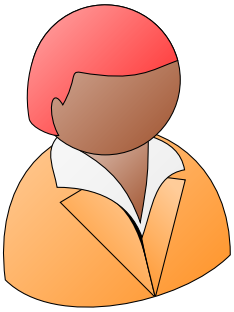
Grundlagen der Programmierung

Rechnen und Rechnen Lassen

Skript zur Vorlesung

Ralf Hinze
Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau
Fachbereich Informatik
AG Programmiersprachen



Wintersemester 2024/2025
Lisa Lista Edition — 1. Oktober 2024

Vorwort

Eine paar Worte vorneweg.

Worte des Willkommens Herzlich willkommen an der Rheinland-Pfälzischen Technischen Universität (RPTU) Kaiserslautern-Landau im Fachbereich Informatik (FBI).

> welkom, mirë se vini, welkomma, bel bonjou, مرحبا, أهلا وسهلا, bari galoust, xos gelmissiniz, i bisimila, akwaba, ongi etorri, Шчыра запрашаем, swagata, amrehba sisswène, ani kié, dobro došli, degemer mad, добре дошъл, kyo tzo pa eit, benvinguts, marsha vog'iyla, ulihelisdi, 欢迎你来, bonavinuta, dobrodošli, vítejte, velkommen, pô la bwam/bepôyédi ba bwam, welkom, welcome, bonvenon, tere tulemast, woezon, vælkomin, tervetuloa, welkom, bienvenue, wolkom, binvignut, awaa waa atuu, benvido, bin la v'nu, mobrdzandit/ketili ikhos tkveni mobrdzaneba, herzlich willkommen, Καλώς ήλθατε, eguahé porá, mikouabô, bienvéni, e komo mai, baroukh haba/brouha aba-a/ברוך הבא על לא דבר, üdvözlet, velkomin, fáilte, benvenuto/benvenuta, yôkoso, welkum, wëllkom, witaj, bem-vindo, mishto-avilian tú, bine ai venit, добро пожаловать, bienvenido/bienvenida, välkommen, härzliche wöikomme, ยินดีต้อนรับ, tashi delek, malo e lelei, difika dilenga, hoş geldiniz, gazhasa oetiśkom, Ласкаво просимо, khush amdeed, hush kelibsiz, chào mừng ông/bà/cô mới ðến, bénvnou/wilicome, croeso, dalal ak diam, ékouabô/ékabô

Wir hoffen, dass Sie sich an Ihrer neuen Wirkungsstätte wohlfühlen und mit viel Spaß, großem Interesse und Begeisterung studieren.

Einführende Worte Das vorliegende Skript ist parallel zur gleichnamigen Vorlesung im Wintersemester 2018/2019 entstanden und wird mit jeder Iteration der Veranstaltung aktualisiert, ergänzt, korrigiert und überarbeitet. Das Skript versteht sich in erster Linie als Hilfsmittel beim Vor- und Nacharbeiten der Vorlesung, ist aber mit gewissen Einschränkungen auch für das Selbststudium geeignet.

Die Vorlesung »Grundlagen der Programmierung« beschäftigt sich, wie der Titel andeutet mit grundlegenden *Konzepten* von Programmiersprachen, Programmierparadigmen und Programmiertechniken. Um gleich ein häufiges Missverständnis auszuräumen: Es handelt sich *nicht* um einen Programmierkurs (»Einführung in die Programmiersprache XYZ«). Zwar werden die eingeführten Konzepte in einer konkreten Programmiersprache eingeübt, aber es stehen die Konzepte im Vordergrund, die unabhängig und von allgemeiner Natur sind, und nicht die Features und Feinheiten einer speziellen Programmiersprache.

Die 14 Wochen des Wintersemesters sind lang, schränken aber dennoch die Stoffauswahl ein: Wir beschränken uns auf sequentielle Programmierung mit kurzen Exkursionen in die Algorithmik und in die formalen Sprachen; Konzepte paralleler, nebenläufiger oder verteilter Systeme werden später in höheren Semestern vermittelt.

Worte der Orientierung In der Schule wurde Ihnen das Wissen in kleinen wohldosierten Dosen verabreicht. Es war in der Regel klar, was gerade gelernt wurde und jedes Konzept wurde

hinreichend lange eingeübt. Das ist an der Universität anders. Zum einen ist hier das Tempo der Wissensvermittlung höher. Zum anderen steht das selbstständige Lernen im Vordergrund. Sie müssen selbst das für Sie passende Lehrmaterial auswählen. Sie müssen selbst überprüfen, was Sie bereits gut und was noch nicht so gut verstanden haben, um dann gezielt an den Problemstellen zu arbeiten. Sie müssen lernen, kritisch mit sich selbst zu sein, eigene Fragen formulieren zu Sachverhalten, die Sie nicht richtig verstehen und dann gezielt nach Antworten auf diese Fragen suchen, durch Selbstdenken, auf den Folien, im Skript, in Büchern, bei Ihren Mitstudenten/Mitstudentinnen, Tutoren/Tutorinnen oder Dozenten/Dozentinnen — aber bitte *nicht*, zumindest nicht ohne einen sehr kritischen Blick, im Internet. Wir machen vielfältige Angebote, um Sie bei diesem Prozess zu unterstützen. Nehmen Sie diese wahr!

Das benötigte Vorwissen insbesondere im Hinblick auf mathematische Sachverhalte ist minimal. Die mathematischen Grundlagen legen wir selbst in Kapitel 2. Anhang B fasst mathematisches Basis- und Hintergrundwissen zusammen — sollten Ihnen zum Beispiel die Notation $\{1, 2\}$ oder $A \cup B$ nichts sagen, werden Sie dort fündig.

Neben den Folien und dem Skript stellen wir Ihnen Programme zum Ausprobieren und Experimentieren zur Verfügung — Hinweise der Form ***module*** *Values.Area* im Seitenrand verweisen auf die entsprechenden Dateien.

Abschnitte, die mit einem oder zwei Sternen ⋆ gekennzeichnet sind, enthalten vertiefenden, ergänzenden oder weiterführenden Lehrstoff. Lesen Sie den einen oder anderen Abschnitt, wenn Sie den Dingen auf den Grund gehen möchten (»Daß ich erkenne, was die Welt Im Innersten zusammenhält, …«), wenn Sie wissbegierig sind oder gelangweilt (»… hatte ich schon alles im Info LK …«). Vielleicht finden Sie die Ausführungen hilfreich und/oder interessant. Anderenfalls überspringen Sie die Abschnitte — weder bauen die darauffolgenden Abschnitte darauf auf, noch ist der Stoff prüfungsrelevant.

> *In den zehn bis 14 Tagen vor dem Rennen auf Kona kann man die Form fast nur noch kaputtmachen. Das ist so, als ob ich mir vor einer Klausur in den letzten Minuten den Lernstoff reinprügele — da bleibt nicht viel hängen.*
>
> — Patrick Lange (1986), *SZ (11. Oktober 2019)*

> *Ich möchte hier die im Laufe der Vorlesung mehrfach — nach meinem Eindruck größtenteils vergeblich — in verschiedener Form getroffene Feststellung wiederholen, daß tieferes Verständnis nicht ohne intensiven Arbeitseinsatz zu erreichen ist, schon gar nicht in einem Gewaltakt in wenigen Tagen oder Wochen. Es ist besser hier dem Rat des Apelles (von Plinius überliefert) zu folgen:* Nulla dies sine linea.
>
> — Gerd Wegner (1938), *Lineare Algebra für Informatiker*

Mahnende Worte »Grundlagen der Programmierung« (INF-02-01-V-2) ist ein umfangreiches Modul, für das Sie 10 Leistungspunkte oder ECTS Credits erhalten (European Credit Transfer System). Im Vollzeitstudium wird davon ausgegangen, dass 60 Leistungspunkte pro akademischem Jahr gesammelt werden, was einem Aufwand von 1500 bis 1800 Stunden entspricht, also circa 45 bis 46 Wochen à 35 bis 40 Lernstunden. Für 10 Leistungspunkte müssen Sie entsprechend 11 bis 14 Stunden pro Woche für das Modul investieren. Dies ist der Natur nach nur ein Richtwert — Lernfortschritt misst sich nicht in Minuten oder Stunden, sondern in der Anzahl der »Aha-Erlebnisse«. Aber ich bin mir sicher: Wenn Sie intensiv und kontinuierlich arbeiten, wird sich dieser Fortschritt auch einstellen. (Fleiß, nicht Intelligenz ist der entscheidende Faktor — der Einfluss der Intelligenz auf den Lernerfolg wird gemeinhin überschätzt. Vergessen Sie nicht: Mit dem Abitur oder einem vergleichbaren Abschluss haben Sie bereits die Studierfähigkeit nachgewiesen.) Lassen Sie sich nicht entmutigen, wenn sich nicht sofort Erfolge einstellen — bleiben Sie am Ball. Im Studium ist eine solide Frustrationstoleranz nicht von Schaden.

Worte zur Didaktik Die Herausforderung bei der Konzeption der Vorlesung und damit ihr Reiz liegt in der Breite und Tiefe des Publikums. »Grundlagen der Programmierung« wird von Studierenden unterschiedlichster Fachrichtungen gehört: Betriebswirtschaftslehre, Informatik, Maschinenbau und Verfahrenstechnik, Mathematik, Physik, Wirtschaftsingenieurwesen und Wirtschaftsmathematik — mit unterschiedlichen Erwartungen und Vorstellungen. Die Vorkenntnisse der Studierenden variieren stark, auch, nein insbesondere die der Informatiker/-innen: Einige sind mit den wissenschaftlichen Grundzügen der Informatik vertraut, mit Algorithmen, Datenstrukturen, Programmiersprachen, Entscheidbarkeit und Komplexität; andere treten das Studium unbeleckt an oder schnuppern erstmal.

Die Vorlesung versucht dem Rechnung zu tragen: der Breite durch Anwendungsbeispiele aus unterschiedlichen Disziplinen, der Tiefe durch das didaktische Konzept. Ein paar Worte dazu. Die Vorlesung erzählt eine Geschichte, sie versucht Konzepte, die Grundlagen der Programmierung, so weit wie möglich *herzuleiten*, zu motivieren und Zusammenhänge zu beleuchten. Konzepte fallen in der Informatik nicht vom Himmel, sie sind nicht gottgegeben oder gar Naturgesetze — das allermeiste ist Menschenwerk. Das ist nicht diffamierend gemeint; auch die Mutter der Informatik, die Mathematik, ist Menschenwerk, allerdings gewachsen, entwickelt, fehlgeleitet, korrigiert und konsolidiert über Jahrtausende. Der Puls der Informatik schlägt schneller; die Zeitskala zeigt Jahrzehnte, nicht Jahrtausende. Genug Zeit für vielfältige Entwicklungen und Fehlentwicklungen, aber auch genug Zeit für Korrekturen und Konsolidierung? Doch, trotz des jugendlichen Alters der Informatik haben sich grundlegende Konzepte herauskristallisiert, Konzepte mit Bestandsgarantie — diese vermittelt die Vorlesung. Und neben den Möglichkeiten der Informatik geht es am Rande auch um deren Grenzen.

Worte des Dankes Ein besonderer Dank gilt Andres Löh für seine Mitwirkung an der Konzeption der Vorlesung. Eine Vorlesung steht und fällt mit der Organisation und Durchführung des Übungsbetriebes. Ich kann mich glücklich schätzen, immer durch ein tolles Team unterstützt worden zu sein bzw. unterstützt zu werden: in Bonn durch Melanie Gnasa und Julia Kuck und in Kaiserslautern durch Alexander Dinges, Markus Heinrich, Sebastian Schloßer und Peter Zeller. Viele Korrekturleserinnen und Leser haben mitgeholfen, Fehler im Skript und auf den Vorlesungsfolien auszumerzen: Fabian Dietrich, Minh Duc Duong (Minh Đức Dương), Timo Höcker (danke für die Farbschemata für Farbenfehlsichtige), Jonas Koch, Maurice Kohl, Gloria Liebl, Xenia Mechler, Sandra Neubauer, Judith Stengel, Lea Stuppy und Tobias Zimmermann.

Eine Bitte zum Schluss Auf die Erstellung der Unterlagen wurde viel Zeit und Sorgfalt verwendet. Falls Ihnen dennoch Fehler im Skript oder auf den Vorlesungsfolien auffallen — Fehler inhaltlicher, grammatikalischer, typographischer oder historischer Natur oder Fehler in Programmen — berichten Sie bitte diese in einer kurzen Email an

support@harry-hacker.org

Ich werde mich bemühen, alle Fehler so schnell wie möglich zu korrigieren.

Ansonsten verbleibt mir nur, Ihnen viel Spaß beim Lesen zu wünschen!

Ralf Hinze

Das Glück stellt sich ein, wenn dein Werk und deine Worte für dich und für andere von Nutzen sind.

— Buddha

Simplicity and elegance are unpopular because they require hard work and discipline to achieve and education to be appreciated.

— Edsger W. Dijkstra (1930–2002)

Habe nun, ach! Philosophie,
Juristerei and Medizin,
Und leider auch Theologie
Durchaus studiert, mit heißem Bemühn.
Da steh' ich nun, ich armer Tor,
Und bin so klug als wie zuvor!
Heiße Magister, heiße Doktor gar,
Und ziehe schon an die zehen Jahr'
Herauf, herab und quer und krumm
Meine Schüler an der Nase herum —
Und sehe, dass wir nichts wissen können!

— Johann Wolfgang von Goethe (1749–1832), *Faust I*

> *Als Peter-André Alt, Präsident der Hochschulrektorenkonferenz, im Juni zum Semesterausklang von Journalisten befragt wurde, sagte er: »Die Studienanfänger erfüllen die Voraussetzungen deutlich schlechter als früher.« Dieses Lamento erklingt jedes Jahr, es erinnert an das bekannte Denkmuster, das immer so beginnt: »Die Jugend von heute ...« - und dann folgt meistens irgendeine Aussage darüber, inwiefern die jüngere Generation defizitär sei im Vergleich zu früheren.*
>
> *Dieses Denkmuster taucht in jedem Kulturkreis auf und reicht belegbar bis in die Antike und wahrscheinlich noch viel weiter in der Menschheitsgeschichte zurück. Es hat, wie die meisten Pauschalurteile, eher was mit einem selbst als mit jenen zu tun, über die man meint urteilen zu müssen.*
>
> *Eine aktuelle Studie aus den USA bestätigt diese These nun. Psychologen von der University of California in Santa Barbara befragten 3458 Männer und Frauen im Alter zwischen 33 und 51 Jahren, ob sie glauben, dass »kids these days« dreister, dümmer und unbelesener sind als früher. Die Antworten fielen je nach persönlichem Hintergrund der Befragten, der ebenfalls geprüft wurde, grob zusammengefasst in etwa so aus: Autoritäre Menschen gaben an, dass es der Jugend an Respekt mangele. Intelligentere sagten, die Jugend sei weniger schlau als früher und die Belesenen beklagten, dass heute zu wenig gelesen werde.*

— Hanno Charisius (1972), *Nichts geht ohne die Jugend von heute (SZ, 19.10.2019, Wissen)*

Die Professoren *sind eher zu Feinden der Sprache geworden: Nie zuvor hat die Wissenschaft uns so rücksichtslos einen so scheußlichen Jargon in so ungeheuren Mengen aufgenötigt. Und die* Computer *stehen im Begriff, unseren Umgang mit den Wörtern ähnlich stark zu verändern wie einst die Schrift, der Buchdruck und das Telegramm.*

— Wolf Schneider (1925), *Deutsch für Kenner (1987)*

1. Einführung ⧹ Rechnen und rechnen lassen

There are two things which I am confident I can do very well: one is an introduction to any literary work, stating what it is to contain, and how it should be executed in the most perfect manner; the other is a conclusion, shewing from various causes why the execution has not been equal to what the author promised to himself and to the public.

— Samuel Johnson (1709–1784), *Boswell Life vol. 1, p. 291 (1755)*

Man kann vorzüglich Rechnen lernen, ohne sich jemals zu fragen, was denn das Rechnen vom sonstigen Gebrauch des Verstandes unterscheidet. Wir stellen diese Frage jetzt und betrachten dazu das Rechnen so, wie es uns im Leben zuerst begegnet — als Umgang mit den Zahlen. Wir werden also die Natur des Rechnens an der Arithmetik studieren und dabei am Ende feststellen, dass die Zahlen bei weitem nicht das Einzige sind, womit wir rechnen können.

Zweifellos ist Rechnen ein besonderer Gebrauch des Verstandes. Eine gewisse Ahnung vom Unterschied zwischen Denken im Allgemeinen und Rechnen im Besonderen hat jeder, der einmal mit seinem/seiner Mathematiklehrer/-in darüber diskutiert hat, ob der Fehler in der Klassenarbeit »bloß« als Rechenfehler oder aber als »logischer« Fehler einzuordnen sei.

Richtig Rechnen heißt Anwendung der Rechenregeln für Addition, Multiplikation usw. Dies allein garantiert das richtige Ergebnis — und neben ihrer Beachtung und Anwendung ist als einzige weitere Verstandesleistung die Konzentration auf diese eintönige Tätigkeit gefragt. Kein Wunder, dass nur wenige Menschen zum Zeitvertreib siebenstellige Zahlen multiplizieren oder die Zahl π auf hundert Stellen bestimmen!

Damit soll nicht etwa das Rechnen diffamiert werden — es entspricht so gerade der Natur dessen, worum es dabei geht, nämlich den Zahlen. Diese sind Größen, abstrakte Quantitäten ohne sonstige Eigenschaft. Bringe ich sie in Verbindung, ergeben sich neue, andere Größen, aber keine andere Qualität. Der Unterschied von 15 und 42 ist 27, und daraus folgt — nichts. Die mathematische Differenz zweier Größen ist, so könnte man sagen, der unwesentliche Unterschied.

Nur zum Vergleich: Stelle ich meinen Beitrag zum Sportverein und meine Einkommensteuer einander gegenüber, so ergibt sich *auch* ein Unterschied im Betrag. Daneben aber auch einer in der Natur der Empfänger, dem Grad der Freiwilligkeit, meiner Einflussmöglichkeiten auf die Verwendung dieser Gelder und vieles andere mehr. Dies sind wesentliche Unterschiede; aus ihnen folgt allerhand. Unter anderem erklären sie auch die Differenz der Beträge und rechnen sie nicht bloß aus.

Für das Rechnen jedoch spielt es keine Rolle, *wovon* eine Zahl die Größe angibt. Jede sonstige Beschaffenheit der betrachteten Objekte ist für das Rechnen mit ihrer Größe ohne Belang. Deshalb kann das Rechnen in starre Regeln gegossen werden und nimmt darin seinen überraschungsfreien Verlauf. Die kreative gedankliche Leistung liegt woanders: Sie manifestiert sich in der Art und Weise, wie man die abstrakten Objekte der Zahlen konkret aufschreibt. Wir sind daran gewöhnt, das arabische Stellenwertsystem zu verwenden. Dieses hat sich im Laufe der Geschichte durchgesetzt, da sich darauf relativ einfach Rechenregeln definieren und auch anwenden lassen. Das römische Zahlensystem mit seinen komplizierten Wertigkeiten und der Vor- und Nachstellung blieb auf der Strecke: Den Zahlen XV und XLII sieht man den Unterschied XXVII nicht an. Insbesondere das Fehlen eines Symbols für die Null macht systematisches Rechnen unmöglich —

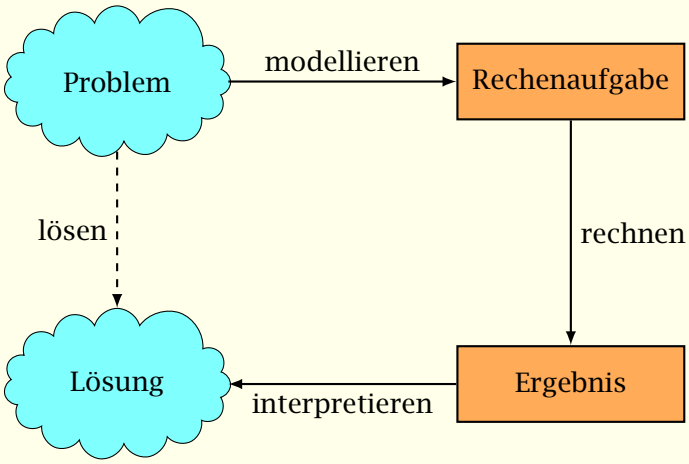


Abbildung 1.1.: Modellbildung in der Informatik.

gerade wegen der Null war das Rechnen mit den arabischen Zahlen im Mittelalter von der Kirche verboten [Kap00].

Einstweiliges Fazit: Das Rechnen ist seiner Natur nach eine äußerliche, gedankenlose, in diesem Sinne mechanische Denktätigkeit. Kaum hatte die Menschheit Rechnen gelernt, schon tauchte die naheliegende Idee auf, das Rechnen auf eine Maschine zu übertragen. Die Geschichte dieser Idee — von einfachen Additionsmaschinen bis hin zu den ersten programmgesteuerten Rechenautomaten — ist an vielen Stellen beschrieben worden und soll hier nicht ausgeführt werden.[1] An ihrem Endpunkt steht der Computer, der bei entsprechender Programmierung beliebig komplexe arithmetische Aufgaben lösen kann — schneller als wir, zuverlässiger als wir und für uns bequemer.

Mit der Existenz dieses Gerätes eröffnen sich plötzlich ganz neue Möglichkeiten: Jetzt, wo wir rechnen *lassen* können, wird es interessant, Aufgaben in Rechenaufgaben zu verwandeln, die es von Natur aus nicht sind und die wir mit unserem Verstand auch nie so behandeln würden. Es gilt, zu einer Problemstellung die richtigen Abstraktionen zu finden, sie durch Formeln und Rechengesetze, genannt Datenstrukturen und Algorithmen, so weitgehend zu erfassen, dass wir dem Ergebnis der Rechnung eine Lösung des Problems entnehmen können (siehe Abbildung 1.1). Wir bilden abstrakte Modelle der konkreten Wirklichkeit, die diese im Falle der Arithmetik perfekt, in den sonstigen Fällen meist nur annähernd wiedergeben. Die Wirklichkeitstreue dieser Modelle macht den Reiz und die Schwierigkeit dieser Aufgabe und die Verantwortung des/der Informatikers/Informatikerin bei der Softwareentwicklung aus.

Die eigentümliche Leistung der Informatik ist es also, Dinge in Rechenaufgaben zu verwandeln, die es von Natur aus nicht sind. Die Fragestellung »Was können wir rechnen lassen?« ist neu in der Welt der Wissenschaften — deshalb hat sich die Informatik nach der Konstruktion der ersten Rechner schnell aus dem Schoße der Mathematik heraus zu einer eigenständigen Disziplin entwickelt. Die Erfolge dieser Bemühung sind faszinierend, und nicht selten, wenn auch nicht ganz richtig, liest man darüber in der Zeitung: »Computer werden immer schlauer«.

[1] Eine beeindruckende Sammlung mechanischer und elektronischer Rechenmaschinen findet man im Bonner Arithmeum (`www.arithmeum.de`). Konrad Zuses Rechenmaschine Z23 ist im Fraunhofer-Institut für Experimentelles Software Engineering ausgestellt (`www.iese.fraunhofer.de`).

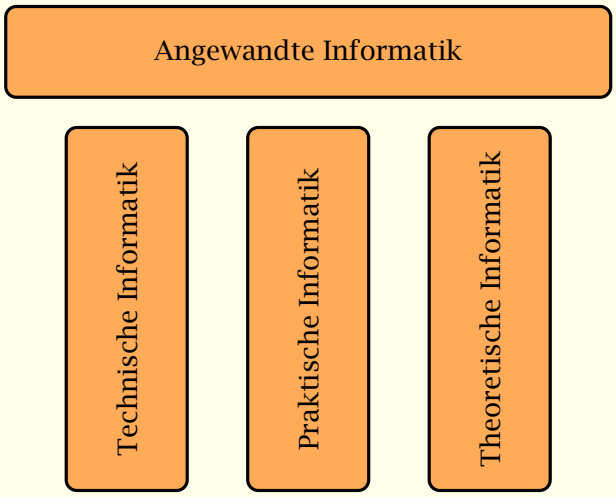


Abbildung 1.2.: Die Aufgabengebiete der Informatik.

1.1. Die Aufgabengebiete der Informatik

Informatik ist die Wissenschaft vom maschinellen Rechnen. Daraus ergeben sich verschiedene Fragestellungen, in die sich die Informatik aufgliedert (siehe Abbildung 1.2).

Zunächst muss sie sich um die Rechenmaschine selbst kümmern. In der *Technischen Informatik* geht es um Rechnerarchitektur und Rechnerentwurf, wozu auch die Entwicklung von Speichermedien, Übertragungskanälen, Aktoren, Sensoren usw. gehört. Der Fortschritt dieser Disziplin besteht in immer schnelleren und kleineren Rechnern bei fallenden Preisen. In ihren elementaren Operationen dagegen sind die Rechner heute noch so primitiv wie zur Zeit ihrer Erfindung. Diese für den Laien überraschende Tatsache erfährt ihre Erklärung in der theoretischen Abteilung der Informatik.

Mit der Verfügbarkeit der Computer erfolgt eine Erweiterung des Begriffs »Rechnen«. Das Rechnen mit den guten alten Zahlen ist jetzt nur noch ein hausbackener Sonderfall. Jetzt werden allgemeinere Rechenverfahren entwickelt, genannt Algorithmen, die aus Eingabe-Daten die Ausgabe-Daten bestimmen. Aber — was genau lässt sich rechnen, und was nicht? Mit welcher Maschine? Die *Theoretische Informatik* hat diese Frage beantwortet und gezeigt, dass es nicht berechenbare Probleme[2] gibt, Aufgaben, zu deren Lösung es keinen Algorithmus gibt. Zugleich hat sie gezeigt, dass alle Rechner prinzipiell gleichmächtig sind, sofern sie über einige wenige primitive Operationen verfügen. Weiterhin erweisen sich die berechenbaren Aufgaben als unterschiedlich aufwändig, so dass die Komplexitätstheorie heute ein wichtiges Teilgebiet der Theoretischen Informatik darstellt.

Zwischen den prinzipiellen Möglichkeiten des Rechnens und dem Rechner mit seinen primitiven Operationen klafft eine riesige Lücke. Die Aufgabe der *Praktischen Informatik* ist es, den Rechner für Menschen effektiv nutzbar zu machen. Die oben erwähnte, sogenannte »semantische Lücke« wird Schicht um Schicht durch Programmiersprachen auf immer höherer Abstraktionsstufe geschlossen. Heute können wir Algorithmen auf der Abstraktionsstufe der Aufgabenstellung entwickeln und programmieren, ohne die ausführende Maschine überhaupt zu kennen. Dies ist nicht nur bequem, sondern auch wesentliche Voraussetzung für die Übertragbarkeit von Programmen

[2] Man kann solche Aufgaben auch als Ja/Nein-Fragestellungen formulieren und nennt sie dann »formal unentscheidbare« Probleme, siehe Anhang B.2.4. Lässt man darin das entscheidende Wörtchen »formal« weg, eröffnen sich tiefsinnige, aber falsche Betrachtungen über Grenzen der Erkenntnis.

zwischen verschiedenen Rechnern. Ähnliches gilt für die Benutzung der Rechner (Betriebssysteme, Benutzungsoberflächen), für die Organisation großer Datenmengen (Datenbanken) und sogar für die Kommunikation der Rechner untereinander (Rechnernetze, Verteilte Systeme). Das World Wide Web (WWW) ist das bekannteste Beispiel für das Schließen der semantischen Lücke: Es verbindet einfachste Benutzbarkeit mit globalem Zugriff auf Informationen und andere Ressourcen in aller Welt. Heute bedarf es nur eines gekrümmten Zeigefingers, um tausend Computer in aller Welt für uns arbeiten zu lassen.

In der *Angewandten Informatik* kommt endlich der Zweck der ganzen Veranstaltung zum Zuge. Sie wendet die schnellen Rechner, effizienten Algorithmen, die höheren Programmiersprachen und ihre Übersetzer, die Datenbanken, Rechnernetze usw. an, um Aufgaben jeglicher Art sukzessive immer weiter und vollkommener zu lösen. Je weiter die Informatik in die verschiedensten Anwendungsgebiete vordringt, desto spezifischer werden die dort untersuchten Fragen. In den vergangenen Jahrzehnten haben wir erlebt, dass sich interdisziplinäre Anwendungen als eigenständige Disziplinen von der »Kerninformatik« abspalten. Wirtschaftsinformatik und Bioinformatik sind zwei Protagonisten dieser Entwicklung. Während es früher Jahrhunderte gedauert hat, bis aus den Erfolgen der Physik zunächst die anderen Natur- und dann die Ingenieurwissenschaften entstanden, so laufen heute solche Entwicklungen in wenigen Jahrzehnten ab.

Wenn die Rechner heute immer mehr Aufgaben übernehmen, für die der Mensch den Verstand benutzt, so ist, insbesondere für Laien, längst nicht mehr erkennbar, auf welche Weise dies erreicht wird. Es entsteht der Schein, dass das analoge Resultat auch in analoger Weise zustande käme. Diesen Schein nennt man künstliche Intelligenz. Es lohnt sich, die Metapher von der Intelligenz des Rechners kurz genauer zu betrachten, weil sie — unter Laien wie unter Informatikern — manche Verwirrung stiftet. Es ist nichts weiter dabei, wenn man sagt, dass ein Rechner (oder genauer eine bestimmte Software) sich intelligent verhält, wenn er (oder sie) eine Quadratwurzel zieht, eine WWW-Seite präsentiert oder ein Flugzeug auf die Piste setzt. Schließlich wurden viele Jahre Arbeit investiert, um solche Aufgaben rechnergerecht aufzubereiten, damit der Rechner diese schneller und zuverlässiger erledigen kann als wir selbst. Nimmt man allerdings die Metapher allzu wörtlich, kommt man zu der Vorstellung, der Rechner würde dadurch selbst so etwas wie eine eigene Verständigkeit erwerben. Daraus entsteht die widersprüchliche Zielsetzung, den Rechner so zu programmieren, dass er sich nicht mehr wie ein programmierter Rechner verhält. Tatsächlich finden wir diese Zielsetzung innerhalb der Informatik wieder, als eigene Arbeitsrichtung »Künstliche Intelligenz«. Der Sache nach gehört sie der Angewandten Informatik an, geht es ihr doch um die erweiterte Anwendbarkeit des Rechners auf immer komplexere Probleme. Andererseits haben diese konkreten Anwendungen immer nur exemplarischen Charakter, als Schritte zu dem abstrakten Ziel, »wirklich« intelligente künstliche Systeme zu schaffen. So leidet diese Arbeitsrichtung unter dem Dilemma, dass ihre Erfolge sich bei Weglassen der metaphorischen Einkleidung stets auch anderen Disziplinen der Informatik zuordnen lassen, während die immer wieder geweckten und dann enttäuschten Erwartungen ganz ihre eigenen bleiben.

Unbeschadet solch metaphorischer Fragen geht der Vormarsch der Informatik in allen Lebensbereichen voran: Aus Textverarbeitung wird DeskTop Publishing, aus Computerspielen wird Virtual Reality, und aus gewöhnlichen Bomben werden »intelligent warheads«. Wie gesagt: die Rechner werden immer schlauer. Und wir?

1.2. Einordnung der Informatik in die Wissenschaftsfamilie

Wir haben gesehen, dass die Grundlagen der Informatik aus der Mathematik stammen, während der reale Ausgangspunkt ihrer Entwicklung die Konstruktion der ersten Rechner war. Mutter die Mathematik, Vater der Computer — wissenschaftsmoralisch gesehen ist die Informatik als ein Bastard aus einer Liebschaft des reinen Geistes mit einem technischen Gerät entstanden.

Die Naturwissenschaft untersucht Phänomene, die ihr ohne eigenes Zutun gegeben sind. Die Gesetze der Natur müssen entdeckt und erklärt werden. Die Ingenieurwissenschaften wenden dieses Wissen an und konstruieren damit neue Gegenstände, die selbst wieder auf ihre Eigenschaften untersucht werden müssen. Daraus ergeben sich neue Verbesserungen, neue Eigenschaften und so weiter.

Im Vergleich dieser beiden Abteilungen der Wissenschaft steht die Informatik eher den Ingenieurwissenschaften nahe: Auch sie konstruiert Systeme, die — abgesehen von denen der Technischen Informatik — allerdings immateriell sind. Wie die Ingenieurwissenschaften untersucht sie die Eigenschaften ihrer eigenen Konstruktionen, um sie weiter zu verbessern. Wie bei den Ingenieurwissenschaften spielen bei der Informatik die Aspekte der Zuverlässigkeit und Lebensdauer ihrer Produkte eine wesentliche Rolle.

Eine interessante Parallele besteht auch zwischen Informatik und Rechtswissenschaft. Die Informatik konstruiert abstrakte Modelle der Wirklichkeit, die dieser möglichst nahe kommen sollen. Das Recht schafft eine Vielzahl von Abstraktionen konkreter Individuen. Rechtlich gesehen sind wir Mieter/-innen, Studenten/Studentinnen, Erziehungsberechtigte, Verkehrsteilnehmer/-innen usw. Als solche verhalten wir uns entsprechend der gesetzlichen Regeln. Der/die Programmierer/-in bildet reale Vorgänge in formalen Modellen nach, der/die Jurist/-in muss konkrete Vorgänge unter die relevanten Kategorien des Rechts subsumieren. Die Analogie endet allerdings, wenn eine Diskrepanz zwischen Modell und Wirklichkeit auftritt: Bei einem Programmfehler behält die Wirklichkeit recht, bei einem Rechtsbruch das Recht.

Eine wissenschaftshistorische Betrachtung der Informatik und ihre Gegenüberstellung mit der hier gegebenen deduktiven Darstellung ist interessant und sollte zu einem späteren Zeitpunkt, etwa zum Abschluss des Informatikstudiums, nachgeholt werden. Interessante Kapitel dieser Geschichte sind das Hilbert'sche Programm, die Entwicklung der Idee von Programmen als Daten, die oben diskutierte Idee der »Künstlichen Intelligenz«, der Prozess der Loslösung der Informatik von der Mathematik, die Geschichte der Programmiersprachen, die Revolution der Anwendungssphäre durch das Erscheinen der Mikroprozessoren und vieles andere mehr.

1.3. Überblick über die Vorlesung

In der Vorlesung beschäftigt uns das »Rechnen lassen«: Wie können wir Aufgaben in Rechenaufgaben verwandeln? Wie können wir einen Rechner programmieren, so dass er diese Aufgaben ohne weiteres Zutun erledigt? Thematisch gehört die Vorlesung somit zur »Praktischen Informatik«. Hier und da werden wir uns allerdings in die anderen Gebiete der Informatik vorwagen, insbesondere in die »Theoretische Informatik«.

Paradoxerweise wird der Rechenknecht selbst, der Computer, bei unserem Streifzug kaum in Erscheinung treten. Dies liegt an der schon angesprochenen semantischen Lücke: zu primitiv sind die Operationen, die ein Computer werksseitig mitbringt. Seine Stärke liegt in der extrem schnellen Ausführung von wenigen einfachen Operationen, nicht in der Bereitstellung ausdrucksstarker Operationen. Aus diesem Grund werden wir im Laufe der Vorlesung unsere eigene Programmiersprache entwickeln: Mini–F#. Eine Sprache, in der sich Rechenregeln bequem und vor allem problemnah formulieren lassen. Dabei geben wir uns der Illusion hin, dass ein entsprechend moderner Rechner diese Programme auch ausführen kann. Tatsächlich ist dies auch möglich: nur nicht nativ (in Hardware), sondern mit Hilfe vieler anderer Programme, die die semantische Lücke schließen (in Software). Der Unterschied ist für den/die Benutzer/-in nicht auszumachen, allenfalls wird die phänomenale Rechengeschwindigkeit moderner Rechner etwas gebremst.

Die Einführung einer eigenen Programmiersprache verfolgt einen Hintergedanken. Sie erlaubt es uns, viele typische Fragestellungen der Praktischen Informatik zu motivieren und zu untersuchen: Wie lässt sich die äußere Form von Programmen festlegen? Wie kann man die Bedeutung

eines Programms präzise definieren? Wie entwickelt man systematisch ein Programm? Wann ist ein Programm korrekt? usw. Auf diese Weise wird die Programmiersprache selbst zum Objekt des Studiums. Wie gesagt: Die Informatik steht den Ingenieurwissenschaften nahe.

Natürlich ist Mini–F#— wie der Name bereits andeutet — keine völlig neue Programmiersprache; sie steht in der Tradition der Algol-Sprachfamilie und ist eng angelehnt an die Sprache F#, die ihrerseits auf Sprachen wie Standard ML oder OCaml aufbaut. F# ist Mitglied der .NET Sprachfamilie, die weitere Programmiersprachen wie Visual Basic und C# umfasst. F# ist eine sogenannte *Multiparadigmensprache*: Sie unterstützt funktionale, imperative und objektorientierte Programmierung — auf diese drei Programmierparadigmen werden wir im Laufe der Vorlesung intensiv eingehen. Mini–F# ist eine sorgfältig ausgewählte Teilmenge von F# — den gesamten Sprachumfang von F# vorzustellen, ist weder zeitlich möglich, noch wünschenswert. Bei der Entwicklung von Mini–F# standen zwei miteinander konkurrierende Ziele im Vordergrund: Mini–F# sollte einfach zu lernen sein und trotzdem einen guten Überblick über bestehende Sprachfamilien und -kulturen vermitteln. Wir hoffen, dass der Balanceakt geglückt ist und Mini–F# sowohl für Anfänger als auch für Fortgeschrittene hinreichend viel Denkstoff bietet. Idealerweise ist jedes Mini–F# Programm ein gültiges F# Programm. Diesem Ideal kommen wir nahe, ganz erreicht wird es nicht: gelegentlich vereinfachen wir etwas, ganz selten mogeln wir (siehe Anhang A).

Gliederung Im Einzelnen ist das vorliegende Skript zur Vorlesung wie folgt gegliedert.

Bevor wir mit dem Programmieren und der wissenschaftlichen Betrachtung des Programmierens loslegen können, benötigen wir etwas Rüstzeug. Dies wird kurz und knapp in Kapitel 2 vermittelt.

Wir nehmen die Metapher des Rechnens zunächst sehr wörtlich: Ein Programm ist einfach ein Ausdruck; rechnen wir den Ausdruck aus, erhalten wir das Ergebnis des Programms. Die elementaren Konstrukte für das Rechnen führen wir in Kapitel 3 ein. Am Ende des Kapitels steht eine Programmiersprache, mit der man die prinzipiellen Möglichkeiten eines Rechners ausschöpfen kann. Das Wörtchen »prinzipiell« ist dabei bedeutsam: Für praktische Belange benötigen wir erheblich mehr Komfort; für diesen wird in den darauffolgenden Kapiteln gesorgt.

Rechner verarbeiten Daten: Personaldaten, Börsendaten, Wetterdaten usw. Was früher in Karteikästen und Aktenordnern verwahrt und aufbewahrt wurde, findet sich heute rechnergerecht aufbereitet auf Speichermedien wieder. Daten machen einen wesentlichen Teil der Modelle aus, die Informatiker/-innen von der Wirklichkeit bilden. Wie man Daten repräsentiert und strukturiert, davon handelt Kapitel 4.

Kenntnis des Vokabulars und der Grammatik einer Sprache macht noch keinen Dichter. Dazu gehört mehr: Kenntnis von Rhythmus und Reim, von Takt und Technik und natürlich Kreativität. Mit dem Programmieren verhält es sich ähnlich: Die kreative, gedankliche Leistung geht dort in das Aufstellen von Rechenregeln. Programmiertechniken, ein Thema von Kapitel 5, helfen Rechenregeln systematisch zu entwickeln. Aufgaben wie Rechenaufgaben lassen sich auf vielfältige Art und Weise lösen. Die resultierenden Rechenregeln können sehr unterschiedlich sein und die Ressourcen eines Rechners, Zeit und Platz, unterschiedlich stark beanspruchen. Auch hier sind Programmiertechniken von Nutzen: Sie helfen Programme zu verbessern, sie schneller und platzsparender zu machen. Werden viele Daten verwaltet, muss man sich überlegen, wie man sie geeignet verknüpft, um auf sie zugreifen und manipulieren zu können: Aus Daten werden Datenstrukturen. Einige einfache Datenstrukturen werden wir in Kapitel 5 kennenlernen.

Bevor wir den Computer rechnen lassen können, müssen Formeln und Rechenregeln, sprich Programme, dem Computer kommuniziert werden. Dabei ist bedeutsam, dass sich der Computer in seinen Aktionen allein von der äußeren Form der Programme leiten lässt. Für einen menschlichen Leser mag es keine große Rolle spielen, ob etwa in einem Roman an einer bestimmten Stelle ein Komma oder ein Semikolon steht. Wird hingegen in einem Programm ein Komma durch ein

Semikolon ersetzt, kann sich die Bedeutung des Programms wesentlich, sogar dramatisch verändern. Aus diesem Grund ist es wichtig, die äußere Form von Programmen präzise und eindeutig festzulegen. Kapitel 6 zeigt, wie dies gemacht werden kann und erzählt dabei eine der großen Erfolgsgeschichten der Informatik.

Kapitel 7 erweitert die Idee des Rechnens. Wurde bis dato ein Programm um des Ergebnisses willen ausgerechnet, kann ein Programm jetzt zusätzlich Effekte haben: Eingaben werden getätigt, Ausgaben erfolgen, Motoren werden gesteuert, Raketen werden abgeschossen usw. Neben diesen, zum Teil spektakulären, externen Effekten betrachten wir auch interne Effekte: Rechnungen werden abgebrochen und wieder aufgenommen, Rechnungen hängen von einem Gedächtnis ab und Rechnungen verändern das Gedächtnis.

Computer dringen immer weiter in unser tägliches Leben vor; immer mehr Aufgaben werden in Rechenaufgaben verwandelt. Die Aufgaben werden zudem anspruchsvoller und umfangreicher. Komplexe Aufgaben resultieren in komplexen Rechenregeln: Aus Programmen werden Softwaresysteme. Um die Entwicklung großer Systeme meistern zu können, muss man sich etwas einfallen lassen. Kapitel 8 zeigt auf, wie sich Programme organisieren lassen: Wie man Rechenregeln konzeptionell zusammenfasst, sie zu größeren Paketen verschnürt und wie man mit diesen Paketen rechnet.

You can never understand one language
until you understand at least two.

— Ronald Searle (1920)

If we spoke a different language,
we would perceive a somewhat different world.

— Ludwig Wittgenstein (1889–1951)

You've remarked that learning many different languages is useful to programming.

Oh yes, it's useful. There is an enormous difference between one who is monolingual and someone who at least knows a second language well, because it makes you much more conscious about language structure in general. You will discover that certain constructions in one language you just can't translate. I was once asked what were the most vital assets of a competent programmer. I said »mathematical inclination« because at the time it was not clear how mathematics could contribute to a programming challenge. And I said »exceptional mastery« of his native tongue because you have to think in terms of words and sentences using a language you are familiar with.

— Philip L. Frana, Thomas J. Misa, *An Interview With Edsger W. Dijkstra, CACM 53(8)*

2. Grundlagen\Vor dem Rechnen

Angling may be said to be so like the mathematics,
that it can never be fully learnt.
— Izaak Walton (1593–1683), *The Compleat Angler (1653)*

Wir haben in der Einleitung angesprochen, dass wir unsere Programmiersprache Mini-F# selbst zum Objekt des Studiums machen. Dazu brauchen wir einige wenige Grundlagen, die wir in diesem Kapitel legen.

Im Einzelnen: Wir setzen elementare Mathematikkenntnisse insbesondere Kenntnisse der naiven Mengenlehre voraus. (Wenn Sie merken, dass Ihnen Vorwissen fehlt, werfen Sie einen Blick in den Anhang B.) Alle weiteren mathematischen Konzepte führt Abschnitt 2.1 ein. Abschnitt 2.2 klärt, was das Studium von Programmiersprachen involviert und motiviert die restlichen Abschnitte dieses Kapitels.

2.1. Endliche Abbildungen und Sequenzen

Endliche Abbildungen Bei der Formalisierung von Mini-F# werden wir häufig Gebrauch von sogenannten ***endlichen Abbildungen*** machen (engl. finite maps). Wie der Name andeutet, bildet eine endliche Abbildung nur endlich viele Elemente aus ihrem Ursprungsbereich auf Elemente des Wertebereichs ab. Der Wertebereich selbst kann unendlich groß sein.

Sind X und Y Mengen, dann bezeichnet $X \to_{\text{fin}} Y$ die Menge aller endlichen Abbildungen von X nach Y. Ist $\varphi \in X \to_{\text{fin}} Y$, dann bezeichnet $\mathit{dom}\ \varphi \subseteq X$ die Menge aller Elemente aus X, auf denen φ definiert ist, den sogenannten ***Definitionsbereich*** von φ (engl. domain). Der Definitionsbereich $\mathit{dom}\ \varphi$ einer endlichen Abbildung muss endlich sein. Die Anwendung einer endlichen Abbildung φ auf ein Element x notieren wir mit $\varphi(x)$.

Die endliche Abbildung

$$\{\mathit{Anja} \mapsto \mathit{Spaghetti}, \mathit{Lisa} \mapsto \mathit{Tortellini}, \mathit{Florian} \mapsto \mathit{Spaghetti}, \mathit{Ralf} \mapsto \mathit{Saltimbocca}\}$$

ordnet zum Beispiel Personen ihre Lieblingsgerichte zu. Ähnlich wie für Abbildungen gilt: Jedem Element x aus $\mathit{dom}\ \varphi$ wird genau ein y aus Y zugeordnet, aber Elemente aus Y können durchaus mehrfach zugeordnet werden.

Um endliche Abbildungen zu konstruieren und zu manipulieren, verwenden wir die folgenden Operationen:

- die ***leere Abbildung*** $\varnothing$ mit
  - $\mathit{dom}\ \varnothing := \varnothing$;
- die ***einelementige Abbildung*** (auch ***Bindung*** genannt) $\{x \mapsto y\}$ mit
  - $\mathit{dom}\ \{x \mapsto y\} := \{x\}$ und
  - $\{x \mapsto y\}(x) := y$;
- die ***Erweiterung*** von φ_1 um φ_2 notiert φ_1, φ_2 (***Kommaoperator***) mit
  - $\mathit{dom}\ (\varphi_1, \varphi_2) := \mathit{dom}\ \varphi_1 \cup \mathit{dom}\ \varphi_2$ und

  - $(\varphi_1, \varphi_2)(x) := \begin{cases} \varphi_2(x) & \text{falls } x \in \mathit{dom}\ \varphi_2 \\ \varphi_1(x) & \text{sonst} \end{cases}$

- die ***Einschränkung*** von φ auf $\mathit{dom}\ \varphi - A$ notiert $\varphi - A$ mit
  - $\mathit{dom}\ (\varphi - A) := \mathit{dom}\ \varphi - A$ und
  - $(\varphi - A)(x) := \varphi(x)$.

Man sieht, dass eine endliche Abbildung jeweils durch zwei Angaben definiert wird: ihrem Definitionsbereich und der eigentlichen Zuordnung von Elementen aus dem Definitionsbereich zu Elementen aus dem Wertebereich. (Nur bei der leeren Abbildung erübrigt sich die Angabe der Zuordnung.)

Der Kommaoperator vereinigt im Prinzip zwei endliche Abbildungen; enthalten beide Abbildungen Bindungen für das gleiche Element, so wird der »rechten« Bindung der Vorzug gegeben:

$$\{\mathit{Anja} \mapsto \mathit{Spaghetti}, \mathit{Ralf} \mapsto \mathit{Pizza}\}, \{\mathit{Ralf} \mapsto \mathit{Eis}\} = \{\mathit{Anja} \mapsto \mathit{Spaghetti}, \mathit{Ralf} \mapsto \mathit{Eis}\}$$
$$\{\mathit{Ralf} \mapsto \mathit{Eis}\}, \{\mathit{Anja} \mapsto \mathit{Spaghetti}, \mathit{Ralf} \mapsto \mathit{Pizza}\} = \{\mathit{Anja} \mapsto \mathit{Spaghetti}, \mathit{Ralf} \mapsto \mathit{Pizza}\}$$

Damit ist der Kommaoperator nicht kommutativ: Die endliche Abbildung φ_1, φ_2 ist in der Regel verschieden von φ_2, φ_1.

Aber der Kommaoperator ist assoziativ: $(\varphi_1, \varphi_2), \varphi_3 = \varphi_1, (\varphi_2, \varphi_3)$, siehe Aufgabe 2.1.2. Deshalb können wir bei mehreren geschachtelten Anwendungen des Kommaoperators die Klammern auslassen und schreiben kurz $\varphi_1, \varphi_2, \varphi_3$. Zusätzlich verwenden wir analog zur Notation von Mengen den Ausdruck $\{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}$ als Abkürzung für die wiederholte Anwendung des Kommaoperators $\{x_1 \mapsto y_1\}, \ldots, \{x_n \mapsto y_n\}$.

Sequenzen Mit Hilfe endlicher Abbildungen lassen sich ***Sequenzen***, endliche Folgen von Elementen, modellieren: Wir nummerieren die Elemente von links nach rechts beginnend mit 0 durch; die Sequenz wird dann durch eine endliche Abbildung repräsentiert, die die »Hausnummer« auf das jeweilige Element abbildet. Die Sequenz *Anja Florian Lisa Ralf* wird zum Beispiel durch $\{0 \mapsto \mathit{Anja}, 1 \mapsto \mathit{Florian}, 2 \mapsto \mathit{Lisa}, 3 \mapsto \mathit{Ralf}\}$ repräsentiert.

Eine Sequenz s von Elementen aus einer Menge A ist somit eine endliche Abbildung des Typs $\mathbb{N} \to_{\text{fin}} A$ mit $\mathit{dom}\ s = \mathbb{N}_n$. Dabei ist $\mathbb{N}_n := \{0, \ldots, n-1\}$ ein Anfangsabschnitt der natürlichen Zahlen. Die Menge aller Sequenzen über A notieren wir mit dem ***Sternoperator***:

$$A^* := \mathbb{N} \to_{\text{fin}} A$$

Ist $\mathit{dom}\ s = \mathbb{N}_n$, dann heißt n die Länge von s, notiert $\mathit{len}\ s := n$.

Die Grundmenge A wird auch manchmal ***Alphabet*** genannt; die Elemente des Alphabets heißen entsprechend Buchstaben und statt von Sequenzen spricht man von ***Wörtern*** über einem Alphabet. Im Kontext von Programmiersprachen verwendet man auch die neutraleren Begriffe Zeichen (engl. characters) und Zeichenketten (engl. strings).

Um Sequenzen zu konstruieren, verwenden wir die folgenden Operationen:

- die ***leere Sequenz*** ε mit
  - $\mathit{dom}\ \varepsilon := \mathbb{N}_0$;

- ist $a \in A$, dann verwenden wir oft das Element a selbst als Abkürzung für die ***einelementige Sequenz*** $\{0 \mapsto a\}$;

- die ***Konkatenation*** von s_1 und s_2 notiert $s_1 \cdot s_2$ mit

- $dom\,(s_1 \cdot s_2) := dom\,s_1 \cup \{i + len\,s_1 \mid i \in dom\,s_2\}$ und
- $(s_1 \cdot s_2)(i) := \begin{cases} s_1(i) & \text{falls } i \in dom\,s_1 \\ s_2(i - len\,s_1) & \text{sonst} \end{cases}$

- die ***n-fache Wiederholung*** von s notiert s^n mit $s^0 := \varepsilon$ und $s \cdot s^n =: s^{n+1} := s^n \cdot s$.

Zum Beispiel ist $\{0 \mapsto \texttt{A}, 1 \mapsto \texttt{n}\} \cdot \{0 \mapsto \texttt{j}, 1 \mapsto \texttt{a}\} = \{0 \mapsto \texttt{A}, 1 \mapsto \texttt{n}, 2 \mapsto \texttt{j}, 3 \mapsto \texttt{a}\}$. Kürzen wir die resultierende Sequenz mit s ab, dann gilt $s(0) = \texttt{A}$ und $s(3) = \texttt{a}$. Da die Konkatenation assoziativ ist, können wir bei geschachtelten Anwendungen die Klammern auslassen: $\texttt{L} \cdot \texttt{i} \cdot \texttt{s} \cdot \texttt{a}$ steht zum Beispiel für die Sequenz $\{0 \mapsto \texttt{L}, 1 \mapsto \texttt{i}, 2 \mapsto \texttt{s}, 3 \mapsto \texttt{a}\}$. Das Symbol für die Konkatenation wird auch oft ausgelassen: $\texttt{L} \cdot \texttt{i} \cdot \texttt{s} \cdot \texttt{a}$ verkürzt sich dann zu `L i s a` oder gar `Lisa` — multiplikative Symbole fallen oft unter den Tisch.

In Mini-F# werden die Zeichen einer Sequenz in doppelte Anführungsstriche gekleidet, aus `Lisa` wird `"Lisa"`, und man spricht von Zeichenketten oder Strings. Ein einzelnes Zeichen wird in einfache Anführungsstriche gesetzt; der String `"Lisa"` besteht aus den vier Zeichen `'L'`, `'i'`, `'s'` und `'a'`. (Der Unterschied macht sich in Mini-F# auch am Typ fest: `"L"` hat den Typ *String*, wohingegen `'L'` vom Typ *Char* ist. Aber wir greifen vor — mehr zu Typen in Kapitel 3.)

Übungen.

Schweißtropfen »💦« kennzeichnen »Drillaufgaben«, mit deren Hilfe Sie eingeführte Konzepte trainieren können — überprüfen Sie, ob Sie die zugrundeliegenden Definitionen wirklich verinnerlicht haben. Mit »📝« werden mathematisch angehauchte Aufgaben gekennzeichnet, die Sie am besten mit Stift und Papier lösen (»pencil and paper exercises«).

💦 **1.** Die folgenden endlichen Abbildungen modellieren das Fressverhalten von Nagetieren:

$\varphi_1 = \{Flecki \mapsto Heu, Fred \mapsto Heu, Hoppel \mapsto Drops\}$
$\varphi_2 = \{Bläcki \mapsto Salat, Flecki \mapsto Möhren, Max \mapsto Gras, Moritz \mapsto Heu\}$

Welche endliche Abbildungen ergeben die folgenden Ausdrücke?

- φ_1, φ_1 und φ_2, φ_2
- φ_1, φ_2 und φ_2, φ_1
- $\varphi_1, \{Hoppel \mapsto Sticks\}, \varphi_2$
- $\varphi_1 - \{Max, Moritz\}$ und $\varphi_2 - \{Max, Moritz\}$
- $(\varphi_1, \varphi_2) - \{Max, Moritz\}$ und $\varphi_1, (\varphi_2 - \{Max, Moritz\})$
- $(\varphi_1, \varphi_2) - \{Fred, Moritz\}$ und $\varphi_1, (\varphi_2 - \{Fred, Moritz\})$

📝 **2.** Zeigen Sie, dass der Kommaoperator assoziativ ist.

$$(\varphi_1, \varphi_2), \varphi_3 \quad = \quad \varphi_1, (\varphi_2, \varphi_3)$$

📝 **3.** Zeigen Sie, dass Sequenzen A^* die algebraischen Eigenschaften eines Monoids erfüllen: Die leere Sequenz ist das neutrale Element der Konkatenation und die Konkatenation ist assoziativ.

$$\varepsilon \cdot s = s = s \cdot \varepsilon \qquad\qquad s_1 \cdot (s_2 \cdot s_3) = (s_1 \cdot s_2) \cdot s_3$$

2.2. Syntax und Semantik

Semantics is a strange kind of applied mathematics; it seeks profound definitions rather than difficult theorems. The mathematical concepts which are relevant are immediately relevant. Without any long chains of reasoning, the application of such concepts directly reveals regularity

in linguistic behaviour, and strengthens and objectifies our intuitions of simplicity and uniformity.
— J.C. Reynolds (1935), *Mathematical Semantics (1980)*

Wenn wir eine Programmiersprache präzise beschreiben wollen, müssen wir zwei Dinge festlegen:

- die äußere Form von Programmen, die ***Syntax***, und
- deren Bedeutung, die ***Semantik***.

Betrachten wir ein Beispielprogramm (ein Teil eines Mini–F# Programms):

```
4711*  (a11 (* speed *) + 815 )
```

Mikroskopisch gesehen besteht das Programm aus einer Folge von Zeichen: der Ziffer 4, gefolgt von der Ziffer 7, gefolgt von der Ziffer 1, gefolgt von der Ziffer 1, gefolgt von einem Asteriskus *, gefolgt von einem Leerzeichen usw. Die Zeichenfolge entspricht im Wesentlichen der Folge von Tasten, die wir betätigen, um das Programm einzugeben.

Als menschlicher/menschliche Leser/-in sind wir gewohnt — bzw. durch jahrelanges Training geschult — mehrere Zeichen, etwa eine Folge von Ziffern, zu einer Einheit zusammenzufassen. Die ersten vier Zeichen werden die meisten unwillkürlich als Zahl viertausendsiebenhundertundelf lesen. Wie Zeichen zu größeren Einheiten, sogenannten ***Lexemen*** (engl. tokens), zusammengefasst werden, wird in der ***lexikalischen Syntax*** einer Programmiersprache festgelegt. Ohne auf Details einzugehen, wird das obige Beispiel in Mini–F# wie folgt gruppiert:

4711	*	(	a11	+	815	)

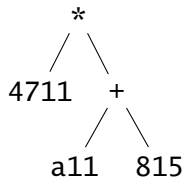
Nicht alle Zeichen sind für den Rechner gedacht: `(* speed *)` ist ein Kommentar, der sich an den menschlichen Leser bzw. an die menschliche Leserin richtet. Ebenso sind Leerzeichen für das Rechnen irrelevant. Lassen wir beides weg, besteht das Programm aus sieben Lexemen.

Nicht jede Folge von Lexemen stellt ein gültiges Programm dar: die Folge

```
) * 4711 815 + ( a11
```

umfasst die gleichen Lexeme, ist aber kein korrektes Mini–F# Programm. In der sogenannten ***kontextfreien Syntax*** einer Programmiersprache wird festgelegt, welche Folgen von Lexemen gültige Programme sind und welche nicht. Die lexikalische und die kontextfreie Syntax bilden zusammen die ***konkrete Syntax*** einer Programmiersprache. Konkret, weil sie genau ausbuchstabiert, wie Programme konkret auszusehen haben. *Wie* die konkrete Syntax definiert wird (und wann sie »kontextfrei« ist), damit beschäftigen wir uns zu einem späteren Zeitpunkt, in Kapitel 6.

Wir haben schon angekündigt, dass wir nicht nur *mit* Mini–F# arbeiten wollen, sondern auch *über* die Sprache reden wollen. Will man eine Programmiersprache selbst zum Gegenstand des Diskurses machen, dann ist die konkrete Syntax als Ausgangspunkt ungeeignet: Sie ist technischen Einschränkungen unterworfen, sie ist das Produkt vieler Kompromisse und spiegelt nicht zuletzt auch den persönlichen Geschmack der Sprachdesigner/-innen wider. Für solche Betrachtungen ist die *hierarchische Struktur* eines Programms relevant. Die hierarchische Struktur unseres Beispielprogramms sieht in etwa so aus:



Das Diagramm verdeutlicht, dass sich der Ausdruck aus mehreren Teilausdrücken zusammensetzt. Man spricht auch von einem ***Rechenbaum*** oder allgemein von einem ***abstrakten Syntaxbaum***. Abstrakt deshalb, weil von den technischen Details der konkreten Syntax abstrahiert wird: In der linearen Folge von Lexemen werden zum Beispiel Klammern verwendet, um Teilausdrücke zu gruppieren. Klammern sind hingegen in der ***abstrakten Syntax*** nicht notwendig; die Baumstruktur legt genau fest, welcher Operand zu welchem Operator gehört.

Der Unterschied zwischen der konkreten und der abstrakten Syntax wird noch deutlicher, wenn man sich die konkrete Syntax des Rechenbaums in anderen Programmiersprachen anschaut. In der Sprache ***Scheme*** zum Beispiel werden die Operatoren *vor* die Operanden geschrieben: `(* 4711 (+ a11 815))`. In der Sprache ***PostScript*** ist es genau anders herum; die Operatoren wandern *hinter* die Operanden: `4711 a11 815 + *`. Zudem müssen keine Klammern verwendet werden, da sich der Rechenbaum eindeutig rekonstruieren lässt. Apropos eindeutig, die oben erwähnten technischen Einschränkungen der konkreten Syntax haben gerade damit zu tun: man möchte aus der linearen Folge von Lexemen die hierarchische Struktur *automatisch* und auf *eindeutige* Weise herauslesen.

In den folgenden drei Kapiteln werden wir uns auf die abstrakte Syntax von Mini–F# konzentrieren und die konkrete nur am Rande behandeln. Mit anderen Worten, wir sind zunächst nicht an Äußerlichkeiten, sondern an den inneren Werten interessiert. (Aber Äußerlichkeiten sind natürlich auch interessant: Abbildung 2.1 berichtet über die Geschichte von Symbolen, die wir heutzutage ganz selbstverständlich verwenden. *Fun Fact:* Das Gleichheitszeichen ist im Laufe der Jahrhunderte verkümmert; aus dem raumgreifenden »═══« im 16. Jahrhundert wurde das stummelige »=« im Computerzeitalter.)

Ist die Struktur von Programmen festgelegt, kann man sich der Bedeutung zuwenden, der ***Semantik*** einer Programmiersprache. Die Semantik legt zum Beispiel fest, dass der Asteriskus `*` die Multiplikation zweier natürlicher Zahlen meint und das Pluszeichen `+` die Addition — das muss nicht notwendigerweise so sein, sondern bedarf in der Tat einer Festlegung. Und was ist die Bedeutung von `a11`? Auch darum muss sich die Semantik kümmern. Wir drücken uns an dieser Stelle vor der Antwort, um nicht zu weit vorzugreifen. Ganz allgemein lässt sich die Semantik mit Hilfe von Auswertungsregeln beschreiben. Zum Beispiel: Wenn `a11` zu 1 auswertet, dann wertet `a11 + 815` zu 816 aus; wenn `a11 + 815` zu 816 auswertet, dann wertet `4711 * (a11 + 815)` zu 3844176 aus. *Die Auswertungsregeln orientieren sich dabei eng an der Struktur eines Programms* — die Bedeutung eines Ausdrucks wird in der Regel auf die Bedeutung der Teilausdrücke zurückgeführt. Deswegen ist es so wichtig, die Struktur vorher präzise festzulegen.

Die beiden folgenden Abschnitte führen das nötige Rüstzeug ein, um die Struktur eines Programms, sprich die abstrakte Syntax, und die Bedeutung eines Programms, sprich die Semantik, zu beschreiben.

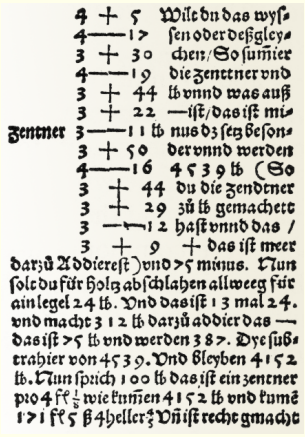
2.3. Abstrakte Syntax\Baumsprachen

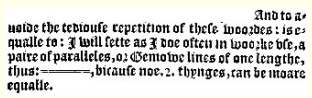
Den hierarchischen Aufbau von Programmen, die abstrakte Syntax, beschreiben wir mit sogenannten ***Baumsprachen***. Die folgende Baumsprache namens *Expr* definiert eine einfache Form von arithmetischen Ausdrücken.

$$
\begin{aligned}
e \in \mathsf{Expr} ::= {} & \mathit{num}\ (\mathbb{N}) \\
\mid {} & \mathit{ident}\ (\mathsf{Ident}) \\
\mid {} & \mathit{add}\ \ (\mathsf{Expr}, \mathsf{Expr}) \\
\mid {} & \mathit{mul}\ \ (\mathsf{Expr}, \mathsf{Expr})
\end{aligned}
$$

Gemäß dieser Definition ist zum Beispiel $\mathit{mul}\ (\mathit{num}\ (\mathtt{4711}), \mathit{add}\ (\mathit{ident}\ (\mathtt{a11}), \mathit{num}\ (\mathtt{815})))$ ein Element von Expr. Dargestellt als Baum:

Der deutsche Mathematiker Johannes Widmann verfasste in jungen Jahren ein Buch über kaufmännisches Rechnen (»Mercantile Arithmetic« oder »Behende und hüpsche Rechenung auff allen Kauffmanschafft«). Das 1489 in Leipzig erschienene Werk gilt als das erste gedruckte Buch, in dem die Symbole »+« und »−« verwendet werden — allerdings in der Funktion als Vorzeichen, nicht als binäre Operatoren. In dieser Bedeutung wurden sie erst 1518 von dem deutschen Mathematiker und Astronomen Heinrich Schreiber (1492–1526) eingeführt.

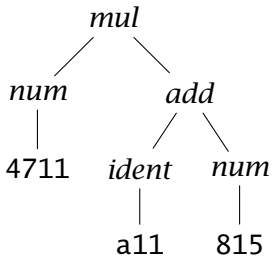

4 + 5 Wilt du das wyſ-
4 — 17 ſen oder deßgley-
3 + 30 chen/ So ſumier
4 — 19 die Zenttner vnd
3 + 44 ℔ vnnd was auß
3 + 22 — iſt/ das iſt mi-
Zentner 3 — 11 ℔ nus dz ſetz beſon-
3 + 50 der vnnd werden
4 — 16 4539 ℔ (So
3 + 44 du die Zendtner
3 + 29 zů ℔ gemachett
3 — 12 haſt vnnd das /
3 + 9 + das iſt meer
darzů Addiereſt) vnd 75 minus. Nun
ſolt du für Holtz abſchlahen allweeg für
ain legel 24 ℔. Vnd das iſt 13 mal 24.
vnd macht 312 ℔ darzů addier das —
das iſt 75 ℔ vnd werden 387. Dye ſub-
trahier von 4539. Vnd bleyben 4152
℔. Nun ſprich 100 ℔ das iſt ein zentner
pro 4 fl. ½ wie kumen 4152 ℔ vnd kume
171 fl. 5 ß 4 heller? Vñ iſt recht gemacht


And to a-
uoide the tedioufe repetition of thefe woordes : is e-
qualle to : I will fette as I doe often in woorke vfe, a
paire of paralleles, or Gemowe lines of one lengthe,
thus: ═══, bicaufe noe. 2. thynges, can be moare
equalle.

And to a-
uoide the tedioufe repetition of thefe woordes : is equalle to : I will fette as I doe often in woorke vfe, a paire of paralleles, or Gemowe lines of one lengthe, thus: ═══, bicaufe noe . 2 . thynges, can be moare equalle.

Im englischsprachigen Raum wurden die beiden Symbole von dem walisischen Arzt und Mathematiker Robert Recorde bekannt gemacht. In seinem 1557 erschienenen Buch mit dem beeindruckenden Titel »The whetstone of witte, whiche is the seconde parte of Arithmetike: containyng thextraction of Rootes: The Coßike practise, with the rule of Equation: and the woorkes of Surde Nombers« erschien auch das erste Mal das moderne Gleichheitszeichen (»keine 2 Dinge können gleicher sein als ein Paar paralleler Linien oder Zwillingslinien«).

Abbildung 2.1.: Johannes Widmann (1460–1498) und Robert Recorde (1510–1558).



Bäume werden in der Informatik in der Regel mit der ***Wurzel*** nach oben und mit den ***Blättern*** nach unten gezeichnet. In unserem Beispiel ist *mul* die Wurzel und 4711, a11 und 815 sind Blätter. Insgesamt hat der Baum acht sogenannte ***Knoten***. Jeder Knoten verzweigt dabei in eine feste Anzahl von Teilbäumen. In der Definition der Baumsprache wird festgelegt, wieviele Teilbäume jede Knotenart hat und von welcher Art die Teilbäume sind: *add* hat zum Beispiel zwei Teilbäume, beide sind wiederum Elemente von Expr; *id* besitzt einen Teilbaum, ein Element aus einer nicht weiter spezifizierten Menge Ident, der Menge von zulässigen Bezeichnern (engl. identifiers).

Die obige Definition führt insgesamt drei verschiedene Dinge ein: einen Namen für die Baumsprache (Expr), Namen für die unterschiedlichen Knotenarten (*num*, *id*, *add* und *mul*) und eine sogenannte ***Metavariable*** (*e*). Das Symbol »::=« trennt den Namen der Baumsprache von den Namen der Knoten; die verschiedenen Knotenarten werden durch das Symbol »|« getrennt. (Diese Vereinbarungen legen die konkrete Syntax von Baumsprachen fest. Verwirrend?)

Umgangssprachlich lässt sich die Definition wie folgt lesen: Ein Element $e \in$ Expr ist entweder von der Form *num* (n) mit $n \in \mathbb{N}$, oder von der Form *ident* (x) mit $x \in$ Ident, oder von der Form *add* (e_1, e_2) mit $e_1, e_2 \in$ Expr oder von der Form *mul* (e_1, e_2) mit $e_1, e_2 \in$ Expr. Man sieht, um arithmetische Ausdrücke zu benennen, verwenden wir die Metavariable *e* (gegebenenfalls mit einem Index versehen). Man spricht von einer *Meta*variablen, da wir mit ihr *über* Elemente der Programmiersprache sprechen; *e* selbst ist *kein* Bestandteil arithmetischer Ausdrücke.

Formal ist die Menge Expr durch eine sogenannte ***induktive Definition*** gegeben. Induktive Definitionen haben stets den gleichen Aufbau: Es gibt Regeln, die bestimmte Teilmengeneigenschaften der definierten Menge festlegen; Regeln, die Abschlusseigenschaften fordern; und schließlich eine Klausel, die fordert, dass die definierte Menge die kleinste Menge mit den genannten Eigenschaften ist. Durch die induktive Brille liest sich unser Beispiel wie folgt. Die Menge Expr ist die *kleinste* Menge mit den folgenden Eigenschaften:

1. ist $n \in \mathbb{N}$, dann ist *num* $(n) \in$ Expr;
2. ist $x \in$ Ident, dann ist *ident* $(x) \in$ Expr;
3. sind $e_1 \in$ Expr und $e_2 \in$ Expr, dann ist auch *add* $(e_1, e_2) \in$ Expr;
4. sind $e_1 \in$ Expr und $e_2 \in$ Expr, dann ist auch *mul* $(e_1, e_2) \in$ Expr.

Wichtig ist, dass Expr die *kleinste* Menge mit diesen Eigenschaften ist; nur Elemente, die sich auf eine der vier Arten bilden lassen, sind in Expr enthalten. Von dieser Eigenschaft machen wir Gebrauch, wenn wir einen Ausdruck "'verarbeiten"'; dann können wir uns darauf verlassen, dass einer der vier Fälle vorliegt.

Wir werden im Laufe der Vorlesung viele Baumsprachen definieren. Dabei nehmen wir uns einige notationelle Freiheiten. So erlauben wir bei der Definition der Knotenarten, Metavariablen stellvertretend für die Baumsprachen selbst zu verwenden. Weiterhin erlauben wir, die Knotennamen in konkreter Syntax oder an die konkrete Syntax angelehnt zu notieren. Mit diesen Konventionen verkürzt sich die Definition von Expr zu:

$n \in \mathbb{N}$
$x \in \mathsf{Ident}$
$e \in \mathsf{Expr} ::= n$
$\quad\mid x$
$\quad\mid e_1 + e_2$
$\quad\mid e_1 * e_2$

Aus dem Knoten *add* (e_1, e_2) ist $e_1 + e_2$ geworden. Es ist wichtig festzuhalten, dass der Unterschied zur ursprünglichen Definition nur ein äußerlicher ist: an Stelle der länglichen Formel *mul* (*num* (`4711`), *add* (*ident* (`a11`), *num* (`815`))) schreiben wir kurz `4711*(a11+815)`, gemeint ist aber stets der gleiche abstrakte Syntax*baum*. Auch wenn wir Ausdrücke linear aufschreiben, zumeist aus Gründen der Bequemlichkeit und der Lesbarkeit, sollte man sich im Geiste stets den jeweiligen Baum vorstellen.

Beispiel: Sequenzen, da capo In Abschnitt 2.1 haben wir ***Sequenzen*** als spezielle endliche Abbildungen modelliert. Alternativ können wir Sequenzen mit Hilfe einer Baumsprache einführen:

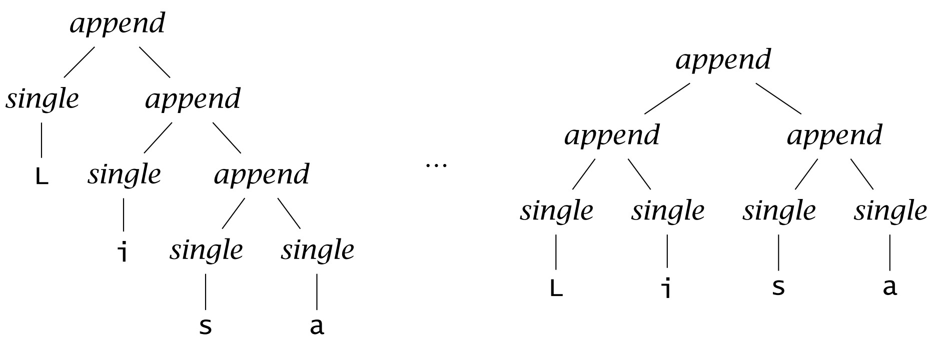
$s \in \mathsf{Sequ} ::= \mathit{single} \quad (A)$
$\quad\mid \mathit{append}\ (\mathsf{Sequ}, \mathsf{Sequ})$

Die Definition beschreibt, wie sich Sequenzen *konstruieren* lassen. *Lies:* Eine Sequenz ist entweder ein einzelnes Zeichen oder besteht aus zwei aneinandergehängten Teilsequenzen. Die Baumsprache `Sequ` modelliert nur nicht-leere Sequenzen. (Warum?) Benötigt man für eine konkrete Anwendung auch die leere Sequenz, so kann man einen weiteren Knotentyp hinzufügen, zum Beispiel, *empty*.

Die Sequenz `Lisa` lässt sich durch fünf verschiedene Bäume darstellen.

append (*single* (`L`), *append* (*single* (`i`), *append* (*single* (`s`), *single* (`a`))))
append (*single* (`L`), *append* (*append* (*single* (`i`), *single* (`s`)), *single* (`a`)))
append (*append* (*single* (`L`), *single* (`i`)), *append* (*single* (`s`), *single* (`a`)))
append (*append* (*single* (`L`), *append* (*single* (`i`), *single* (`s`))), *single* (`a`))
append (*append* (*append* (*single* (`L`), *single* (`i`)), *single* (`s`)), *single* (`a`))

Jeder Baum spiegelt wider, wie die 4-elementige Sequenz konstruiert wurde; die Baumdarstellungen verdeutlichen diesen Punkt noch einmal.



Zum Vergleich: Die in Abschnitt 2.1 eingeführte Konkatenation »·« ist assoziativ, so dass alle fünf Varianten zusammenfallen: `L` · (`i` · (`s` · `a`)) = `L` · ((`i` · `s`) · `a`) = (`L` · `i`) · (`s` · `a`) usw.

Übungen.

📝 **1.** Entwerfen sie Baumsprachen, um Dezimalziffern und Dezimalzahlen zu repräsentieren.

2.4. Beweissysteme

Bei der umgangssprachlichen Beschreibung der Bedeutung arithmetischer Ausdrücke haben wir »wenn-dann« Aussagen formuliert: *wenn* der Teilausdruck $\mathit{ident}\ (\texttt{a11})$ zu der natürlichen Zahl 1 auswertet, *dann* wertet der Ausdruck $\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815}))$ zu 816 aus; *wenn* der Teilausdruck $\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815}))$ zu 816 auswertet, *dann* wertet weiterhin der Ausdruck $\mathit{mul}\ (\mathit{num}\ (\texttt{4711}), \mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})))$ zu 3844176 aus. Wenn-dann Aussagen lassen sich mit Hilfe sogenannter ***Beweisregeln*** formalisieren. Die wenn-dann Aussagen unseres laufenden Beispiels fangen wir mit den beiden folgenden Beweisregeln ein.

$$\frac{\mathit{ident}\ (\texttt{a11}) \Downarrow 1}{\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})) \Downarrow 816}$$

$$\frac{\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})) \Downarrow 816}{\mathit{mul}\ (\mathit{num}\ (\texttt{4711}), \mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815}))) \Downarrow 3844176}$$

Die umgangssprachliche Formulierung »wertet aus zu« symbolisieren wir durch einen nach unten zeigenden Pfeil »$\Downarrow$«. Links von dem Pfeil steht ein arithmetischer Ausdruck, rechts davon eine natürliche Zahl. Über dem Strich der Regeln steht die Voraussetzung oder die Voraussetzungen (der »wenn« Teil); unter dem Strich steht die Schlussfolgerung (der »dann« Teil). Beweisregeln können sowohl von oben nach unten als auch von unten nach oben gelesen werden. Von oben nach unten: Wenn ich $\mathit{ident}\ (\texttt{a11}) \Downarrow 1$ bereits weiß, dann kann ich die Formel $\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})) \Downarrow 816$ schlussfolgern. Von unten nach oben: Wenn ich die Formel $\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})) \Downarrow 816$ zeigen möchte, muss ich zuerst $\mathit{ident}\ (\texttt{a11}) \Downarrow 1$ zeigen.

Beweisregeln lassen sich zu ***Beweisbäumen*** zusammensetzen. Dabei werden die Voraussetzungen einer Regel durch Beweisbäume ersetzt, die die jeweiligen Formeln als finale Schlussfolgerung enthalten. Für unser Beispiel erhalten wir

$$\frac{\dfrac{\dfrac{\vdots}{\mathit{ident}\ (\texttt{a11}) \Downarrow 1}}{\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})) \Downarrow 816}}{\mathit{mul}\ (\mathit{num}\ (\texttt{4711}), \mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815}))) \Downarrow 3844176}$$

Dass dieser Beweisbaum mehr wie ein Strunk und weniger wie ein Baum aussieht, liegt daran, dass jede Regel genau eine Voraussetzung hat. Allerdings haben wir auch etwas gemogelt: Addition wie Multiplikation haben zwei Teilausdrücke und beide Teilausdrücke müssen zunächst ausgewertet werden, wobei Konstanten wie $\mathit{num}\ (\texttt{4711})$ und $\mathit{num}\ (\texttt{815})$ zu sich selbst auswerten.

$$\frac{\dfrac{}{\mathit{num}\ (\texttt{4711}) \Downarrow 4711} \qquad \dfrac{\dfrac{\vdots}{\mathit{ident}\ (\texttt{a11}) \Downarrow 1} \qquad \dfrac{}{\mathit{num}\ (\texttt{815}) \Downarrow 815}}{\mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815})) \Downarrow 816}}{\mathit{mul}\ (\mathit{num}\ (\texttt{4711}), \mathit{add}\ (\mathit{ident}\ (\texttt{a11}), \mathit{num}\ (\texttt{815}))) \Downarrow 3844176}$$

Jetzt sieht man sehr schön die hierarchische Struktur eines Beweisbaumes — der anders als sonst in der Informatik von unten nach oben »wächst«.

Beweisregeln sind ein allgemeines Konzept; ebensowenig wie das Zusammenstellen von Regeln zu Beweisbäumen sind sie auf Auswertungen beschränkt. Ist eine beliebige Menge von Formeln gegeben, etwa durch eine Baumsprache $\phi \in \Phi ::= \cdots$, dann hat eine ***Beweisregel*** die allgemeine Form

$$\frac{\phi_1 \qquad \cdots \qquad \phi_n}{\phi}$$

Über dem Strich der Regeln stehen wie gesagt die Voraussetzungen (n Formeln); unter dem Strich steht die Schlussfolgerung (eine einzige Formel). Ist $n = 0$, so spricht man auch von einem ***Axiom***. Ein ***Beweissystem*** ist eine Menge von Beweisregeln.

Die Menge aller ***Beweisbäume*** ist induktiv definiert: Sind $\mathcal{P}_1, \ldots, \mathcal{P}_n$ Beweisbäume mit den Wurzeln $\phi_1, \ldots, \phi_n$ und ist

$$\frac{\phi_1 \quad \cdots \quad \phi_n}{\phi}$$

eine Beweisregel, dann ist

$$\frac{\mathcal{P}_1 \quad \cdots \quad \mathcal{P}_n}{\phi}$$

ein Beweisbaum mit der Wurzel ϕ. Die Regeln werden zusammengesteckt wie die Klötzchen eines bekannten Spielwarenherstellers. Ist $\mathcal{P}$ ein Beweisbaum mit der Wurzel ϕ, dann sagt man auch $\mathcal{P}$ zeigt oder beweist ϕ.

Kommen wir zurück zu den Auswertungsregeln: Die obigen Beweisregeln sind sehr speziell; allgemeinere Regeln lassen sich mit Hilfe von Metavariablen formulieren.

$$\frac{}{num\,(n) \Downarrow n} \qquad \frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{add\,(e_1, e_2) \Downarrow n_1 + n_2} \qquad \frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{mul\,(e_1, e_2) \Downarrow n_1 \cdot n_2}$$

Die erste Regel — eine Regel ohne Voraussetzungen, ein Axiom — legt fest, dass Konstanten zu sich selbst auswerten. Die beiden anderen Regeln formalisieren, dass zunächst beide Teilausdrücke ausgerechnet werden und dass das Ergebnis die Summe bzw. das Produkt der Teilergebnisse ist. Regeln, die Metavariablen enthalten, heißen auch ***Regelschemata***.

Bevor Regelschemata zu Beweisbäumen zusammengesetzt werden können, müssen die Metavariablen erst durch konkrete Konstanten bzw. Ausdrücke ersetzt werden. Das Ergebnis einer solchen Ersetzung nennt man auch ***Regelinstanz*** oder kurz ***Instanz***. Ein Regelschema steht somit stellvertretend für die Menge aller seiner Instanzen. Für unser laufendes Beispiel benötigen wir zwei Instanzen des Axioms

$$\frac{}{num\,(4711) \Downarrow 4711} \qquad \frac{}{num\,(815) \Downarrow 815}$$

und jeweils eine Instanz der Regeln für die Addition und die Multiplikation:

$$\frac{ident\,(\texttt{a11}) \Downarrow 1 \qquad num\,(815) \Downarrow 815}{add\,(ident\,(\texttt{a11}), num\,(815)) \Downarrow 816}$$

$$\frac{num\,(4711) \Downarrow 4711 \qquad add\,(ident\,(\texttt{a11}), num\,(815)) \Downarrow 816}{mul\,(num\,(4711), add\,(ident\,(\texttt{a11}), num\,(815))) \Downarrow 3844176}$$

Aus diesen Regelinstanzen kann wiederum der obige Beweisbaum zusammengesetzt werden. Man sieht, Instanzen von Axiomen werden zu Blättern eines Beweisbaumes.

Wir haben im letzten Abschnitt angekündigt, dass wir uns bei der Definition der abstrakten Syntax einige Freiheiten herausnehmen, insbesondere, dass wir die Notation der Baumknoten an die konkrete Syntax anlehnen. Das hat den Vorteil, dass wir optisch enger an unserer Programmiersprache arbeiten — die Addition wird in Mini–F# durch $e_1 + e_2$ notiert und nicht durch $add\,(e_1, e_2)$ — und den Nachteil, dass wir optisch sehr eng an die Semantik heranrücken — auch in der Mathematik wird die Addition mit »+« notiert. Betrachten wir als Beispiel die entsprechend adaptierte Regel für die Addition.

$$\frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{e_1 + e_2 \Downarrow n_1 + n_2}$$

Das Pluszeichen tritt zweimal auf, meint aber zwei grundsätzlich verschiedene Dinge: Links ist »+« ein syntaktischer Bestandteil unserer Programmiersprache, rechts bezeichnet »+« das mathematische Konzept der Addition zweier natürlicher Zahlen. Kurz, »+« ist Syntax und »+« ist Semantik. Beides sollte nicht verwechselt werden.

Ganz allgemein haben wir es mit dem Unterschied zwischen ***Objektsprache*** und ***Metasprache*** zu tun. Die Objektsprache, in unserem Fall Mini–F#, ist Objekt des Studiums. Um Eigenschaften der Objektsprache zu formulieren, müssen wir uns einer weiteren Sprache bedienen. Da wir *über* die Objektsprache reden, heißt die andere Sprache *Meta*sprache. Metavariablen sind zum Beispiel ein Element der Metasprache. Als Metasprache verwenden wir die Sprache der Mathematik, angereichert mit deutscher Prosa. Wenn die Objektsprache an die Metasprache angelehnt ist — um zum Beispiel Additionen wie in der Mathematik üblich notieren zu können — besteht die Gefahr der Verwechslung oder zumindest der Verwirrung. Wir sind in diesem Abschnitt der Verwechslungsgefahr etwas entgegengetreten, indem wir unterschiedliche Zeichensätze für Objekt- und Metasprache verwendet haben: »+« ist ein Element der Objektsprache und »+« ein Element der Metasprache. Jetzt, da wir uns den Unterschied klar gemacht haben, werden wir nicht mehr so fein unterscheiden und »+« auch für die Addition von Mini–F# verwenden.

Beispiel: Lindenmayer-Systeme⋆ Wie wäre es zum Abschluss des Kapitels mit einem Beispiel jenseits der Grundschularithmetik? Beweissysteme lassen sich auch verwenden, um natürliche Wachstumsprozesse zu modellieren. Zellgebilde oder Populationen werden dabei durch Wörter über einem Alphabet repräsentiert; das Zellwachstum oder den Übergang von einer zur nächsten Generation spezifizieren Ersetzungsregeln der Form $a \rightsquigarrow s$, wobei a ein einzelner Buchstabe und s ein Wort ist.

Der Klassiker modelliert das Wachstum einer Kaninchenpopulation, siehe auch Abbildung 2.2: ○ ⇝ ● und ● ⇝ ●○. Eine Kaninchenpopulation besteht aus Jungtieren, »○« repräsentiert ein Paar von Jungtieren, und geschlechtsreifen Tieren, »●« steht für ein Paar solcher Tiere. Die Regeln modellieren den Alterungsprozess (die Jungtiere werden geschlechtsreif: ○ ⇝ ●) und die Vermehrung (ein geschlechtsreifes Paar »generiert« ein Paar von Jungtieren und bleibt selbst am Leben: ● ⇝ ●○). Ausgehend von einem Jungtierpaar ergibt sich die unten aufgeführte Populationsfolge.

○

●

●○

●○●

●○●●○

●○●●○●○●

●○●●○●○●●○●●○

●○●●○●○●●○●●○●○●●○●○●

●○●●○●○●●○●●○●○●●○●○●●○●●○●○●●○●●○

●○●●○●○●●○●●○●○●●○●○●●○●●○●○●●○●●○●○●●○●○●●○●●○●○●●○●○●

In jedem Schritt werden die Ersetzungsregeln *gleichzeitig* angewendet, um so die gleichzeitig fortschreitende Entwicklung eines Zellgebildes oder einer Population einzufangen. Die simultane Ersetzung notieren wir mit einem etwas längeren, schlangenförmigen Pfeil, also ●○ ⟿ ●○●, ●○● ⟿ ●○●●○ usw.

Wenden wir uns der Formalisierung zu. Die beiden ursprünglichen Ersetzungsregeln, ○ ⇝ ●

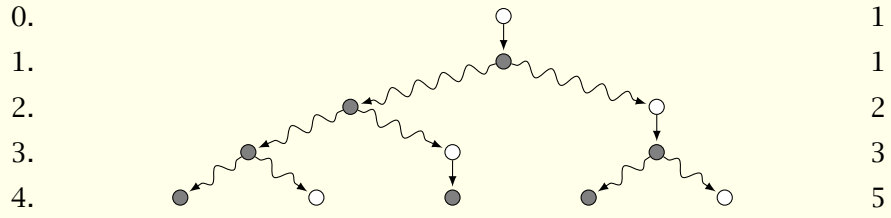
Die Fibonacci-Folge $\mathcal{F}_n$ ist eine unendliche Zahlenfolge, bei der sich ausgehend von 0 und 1 jede weitere Zahl durch Addition ihrer beiden vorherigen Zahlen ergibt, $\mathcal{F}_{n+2} = \mathcal{F}_n + \mathcal{F}_{n+1}$:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots$$

Sie wird als Folge A000045 in der ***On-Line Encyclopedia of Integer Sequences*** (OEIS) gelistet, http://oeis.org, einem unentbehrlichen Nachschlagewerk für Zahlenfreaks.

Die Folge ist nach dem italienischen Mathematiker Leonardo da Pisa (um 1170–1240), alias Fibonacci, benannt, der so das Wachstum einer Kaninchenpopulation modellierte.

> Wie viele Kaninchenpaare entstehen nach n Monaten aus einem einzigen Paar, wenn jedes Paar ab dem 2. Lebensmonat ein weiteres Paar auf die Welt bringt?



Ein weißer Kreis »○« steht für ein *Paar* von Jungtieren; ein grauer »●« symbolisiert ein geschlechtsreifes *Paar*. Nach einem Monat werden die Jungtiere geschlechtsreif und gebären ab diesem Zeitpunkt monatlich ein Paar von Jungtieren, ohne jemals zu sterben. Die Anzahl der Paare in der n-ten Generation ergibt sich somit als

$$●_0 := 0 \qquad ○_0 := 1 \qquad ●_{n+1} := ●_n + ○_n \qquad ○_{n+1} := ●_n$$

Beide Populationsgrößen werden durch die Fibonacci-Folge beschrieben: $●_n = \mathcal{F}_n$ und $○_n = \mathcal{F}_{n-1}$. Notiert man den Übergang von einer zur nächsten Generation mit Vektoren und Matrizen, so erhält man eine wundervolle Formel, um die Folgenglieder effizient zu berechnen: Man potenziert dazu die Übergangsmatrix (siehe Abschnitt 4.1.1).

$$\begin{pmatrix} ●_{n+1} \\ ○_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} ●_n \\ ○_n \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} \mathcal{F}_{n+1} & \mathcal{F}_n \\ \mathcal{F}_n & \mathcal{F}_{n-1} \end{pmatrix} \quad \text{mit } \mathcal{F}_{-1} := 1$$

Fibonacci-Zahlen findet man überall: in der Natur (die Anzahl der links- und rechtsgekrümmten Spiralen in Sonnenblumen sind oft aufeinanderfolgende Fibonacci-Zahlen), in der Architektur (Stichwort: Goldener Schnitt) und in der Kunst (die Skulptur »Seed« von Peter Randall-Page basiert auf der Fibonacci-Folge).

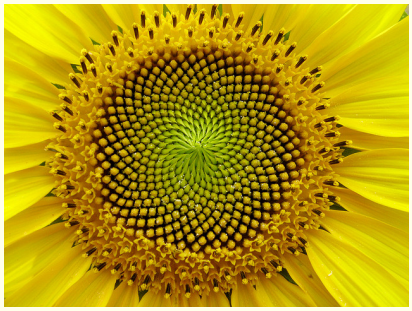


Abbildung 2.2.: Die Fibonacci-Folge.

und ● ⇝ ●○, werden zu Axiomen des Beweissystems,

$$\frac{}{\bigcirc \rightsquigarrow \mathit{single}\ (\bullet)} \qquad \frac{}{\bullet \rightsquigarrow \mathit{append}\ (\mathit{single}\ (\bullet), \mathit{single}\ (\bigcirc))}$$

wobei wir die Baumsprache aus Abschnitt 2.3 für die Repräsentation von Sequenzen heranziehen.

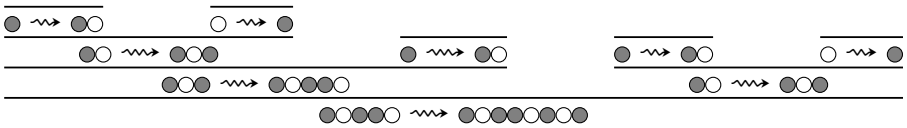
Die simultane Ersetzung wird durch zwei Regelschemata formalisiert.

$$\frac{a \rightsquigarrow s}{\mathit{single}\ (a) \rightsquigarrow s} \qquad \frac{l \rightsquigarrow s \qquad r \rightsquigarrow t}{\mathit{append}\ (l, r) \rightsquigarrow \mathit{append}\ (s, t)}$$

Die erste Regel beschreibt die Ersetzung eines einzelnen Buchstabens; die zweite Regel die Ersetzung eines zusammengesetzten Wortes. Das Beweissystem verwendet zwei verschiedene Formeln:

FORM ::= $a \rightsquigarrow s$	Ersetzung eines Zeichens durch ein Wort
$\mid\ s_1 \rightsquigarrow s_2$	simultane Ersetzung der Zeichen eines Wortes

Man kann die Pfeile entweder als Namen für Baumknoten lesen oder einfach als Trennsymbole, so wie oben der Pfeil » ⇓ « arithmetische Ausdrücke von ihren Werten trennt — analog zur Verwendung von Interpunktionszeichen im Deutschen. Mit Hilfe des Beweissystems können wir zum Beispiel die Formel ●○●●○ ⇝ ●○●●○●○● herleiten,



wobei wir uns wie üblich Freiheiten herausnehmen und die Sequenzen so kompakt wie möglich aufschreiben (anderenfalls sieht man den Wald vor lauter Bäumen nicht).

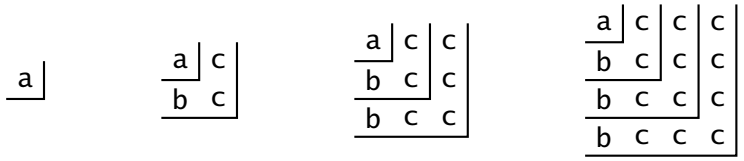
Stehen im obigen Beispiel die Buchstaben für (Paare von) Individuen, so repräsentieren im folgenden Beispiel die Symbole unterschiedliche Zelltypen. Entsprechend modellieren die Ersetzungsregeln Wachstumsvorgänge (die Regeln für ⇝ ändern sich nicht).

$$\frac{}{\mathsf{a} \rightsquigarrow \mathsf{abcc}} \qquad \frac{}{\mathsf{b} \rightsquigarrow \mathsf{bcc}} \qquad \frac{}{\mathsf{c} \rightsquigarrow \mathsf{c}}$$

Typ-a und Typ-b Zellen vermehren sich, Typ-c Zellen hingegen nicht. Erraten Sie, warum die modellierte Spezies ***Quadratwürmer*** genannt werden? (Ich rate davon ab, nach diesem Begriff zu googeln.) Die ersten acht Entwicklungsstadien eines solches Wurms sehen wie folgt aus.

```
a
abcc
abccbcccc
abccbccccbcccccc
abccbccccbcccccbcccccccc
abccbccccbcccccbcccccccbcccccccccc
abccbccccbcccccbcccccccbcccccccccbcccccccccc
abccbccccbcccccbcccccccbcccccccccbcccccccccbcccccccccccc
```

Warum die geometrische Form des Quadrats als Namenspatin dient, sieht man, wenn man die Wörter zweidimensional arrangiert — die Würmer sozusagen aufrollt.



Ein bio*logischer* Beweis, dass die Summe der ersten n ungeraden Zahlen n^2 ergibt.

Die Modellierung von Wachstumsvorgängen mit Hilfe von Ersetzungssystemen geht übrigens auf den ungarischen Biologen Aristid Lindenmayer (1925–1989) zurück, von dem auch das folgende Beispiel stammt. Das System veranschaulicht die Entwicklungsstadien einer ***Rotalge***. Das Alphabet umfasst insgesamt 12 Symbole; die Ziffern repräsentieren unterschiedliche Zelltypen, die restlichen Symbole strukturelle Informationen.

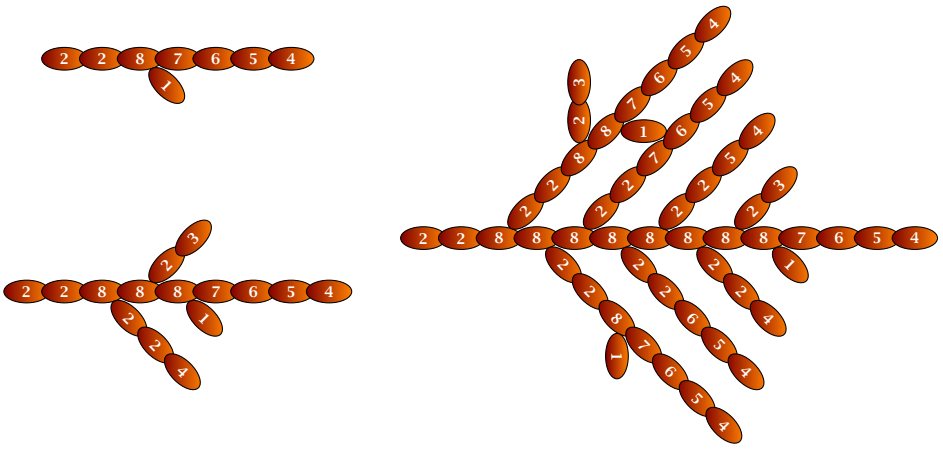
$\overline{1 \rightsquigarrow 23}$ $\overline{2 \rightsquigarrow 2}$ $\overline{3 \rightsquigarrow 24}$ $\overline{4 \rightsquigarrow 54}$ $\overline{5 \rightsquigarrow 6}$ $\overline{6 \rightsquigarrow 7}$

$\overline{7 \rightsquigarrow 8[-1]}$ $\overline{8 \rightsquigarrow 8}$ $\overline{- \rightsquigarrow +}$ $\overline{+ \rightsquigarrow -}$ $\overline{[\rightsquigarrow [}$ $\overline{] \rightsquigarrow]}$

Nach sechs Schritten bildet sich ein Seitenzweig, symbolisiert durch die eckigen Klammern. Dabei gibt das in jedem Schritt wechselnde Vorzeichen, – oder +, die Richtung der Gabelung vor, nach rechts oder nach links.

```
1
23
224
2254
22654
227654
228[-1]7654
228[+23]8[-1]7654
228[-224]8[+23]8[-1]7654
228[+2254]8[-224]8[+23]8[-1]7654
```

Die Entwicklungsstufen lassen sich plastisch darstellen, wenn man die strukturellen Zeichen, –, +, [und], geometrisch interpretiert: Zeichnet man auf einer horizontalen Linie von links nach rechts, so zweigt $[-s]$ in einem $45°$ Winkel nach unten und $[+s]$ entsprechend nach oben ab.



Nach insgesamt 13 Schritten erhält man das auf der rechten Seite dargestellte Entwicklungsstadium. Die acht alternierenden Seitenzweige entsprechen dabei den Stadien 0 bis 7, von rechts nach links.

Übungen.

📝 **1.** Die folgenden Baumsprachen modellieren Dezimalziffern und Dezimalzahlen.

$$\begin{aligned} d \in \mathit{Digit} &::= \mathit{zero} \mid \mathit{one} \mid \mathit{two} \mid \mathit{three} \mid \mathit{four} \mid \mathit{five} \mid \mathit{six} \mid \mathit{seven} \mid \mathit{eight} \mid \mathit{nine} \\ ds \in \mathit{Numeral} &::= \mathit{nil} \\ &\quad \mid \mathit{cons}\,(\mathit{Digit}, \mathit{Numeral}) \end{aligned}$$

Die Dezimalzahl 4711 wird zum Beispiel durch den Baum

$$cons\,(one, cons\,(one, cons\,(seven, cons\,(four, nil))))$$

repräsentiert; die niedrigstwertige Ziffer steht links. Stellen Sie Regelschemata auf, die einem Numeral seinen Wert zuordnen ($ds \Downarrow n$). Konstruieren Sie einen Beweisbaum für die Formel:

$$cons\,(one, cons\,(one, cons\,(seven, cons\,(four, nil)))) \Downarrow 4711$$

Zum Knobeln: Wie müssen die Regeln geändert werden, wenn man vereinbart, dass die Wertigkeit der Ziffern von links nach rechts abnimmt, 4711 also durch

$$cons\,(four, cons\,(seven, cons\,(one, cons\,(one, nil))))$$

repräsentiert wird? *Hinweis:* Stellen Sie Beweisregeln auf, die einem Numeral seine Länge (Anzahl der Ziffern) zuordnen.

2. Erklären Sie die Begriffe

- Beweisregel,
- Axiom,
- Regelschema und
- Regelinstanz

anhand Ihres Beweissystems aus Aufgabe 2.4.1.

3. Harry Hacker hat ein neues Spielzeug erworben: einen programmierbaren Roboter. Um den Roboter zu steuern, kann man ihn mit beliebigen Sequenzen, bestehend aus den Buchstaben `F`, `L` und `R`, füttern. Dabei veranlasst `F` den Roboter, 1 cm in die aktuelle Richtung zu gehen; `L` bzw. `R` drehen den Roboter um 1° nach links bzw. rechts. An dem Roboter lässt sich ein Zeichenstift anbringen, so dass man die Spur des Roboters auf dem Fußboden nachvollziehen kann.

- Die Sequenz `FFFLRF` instruiert den Roboter zum Beispiel 4 cm nach vorne zu gehen.
- Mittels `FFLLLF` geht der Roboter 2 cm nach vorne, dreht sich um 3° nach links und geht von dort aus 1 cm in die neue Richtung.

Nach einigen Tagen des Experimentierens ist Harrys Tastatur — insbesondere die Tasten `F`, `L` und `R` — arg in Mitleidenschaft gezogen. Um der endgültigen Zerstörung des Equipments zuvorzukommen, schlägt Lisa vor, eine Robotersteuerungssprache zu entwickeln, die die gleichen Effekte mit weniger Aufwand erzielt. Sie beschließen keine Zeit auf die konkrete Syntax zu verschwenden und legen gleich die abstrakte Syntax fest:

$n \in \mathbb{N}$

$d \in Draw ::=$	$forward$	1 cm nach vorne
	$\mid left$	1° nach links
	$\mid right$	1° nach rechts
	$\mid d_1; d_2$	Konkatenation
	$\mid repeat\,(n, d)$	Wiederholung

(a) Probieren Sie die Robotersteuerungssprache aus. Schreiben Sie Programme, um

(i) ein Rechteck von 3 cm Breite und 2 cm Länge,

(ii) ein gleichseitiges Dreieck mit einer Seitenlänge von 5 cm und

(iii) das Haus vom Nikolaus

zu zeichnen.

(b) Helfen Sie Lisa und Harry, die Semantik der Robotersteuerungssprache festzulegen. Geben Sie zu diesem Zweck ein Beweissystem an, das einem Programm eine Folge primitiver Instruktionen zuordnet ($Draw \Downarrow \{\mathsf{F}, \mathsf{L}, \mathsf{R}\}^*$).

(c) Wenden Sie das Beweissystem an. Bestimmen Sie mit seiner Hilfe die Bedeutung der Programme aus Teil 1: Geben Sie zu jedem Programm d einen Beweisbaum für $d \Downarrow s$ an, wobei s die Folge der primitiven Instruktionen ist, die Bedeutung von d.

Zusammenfassung und Anmerkungen

DIY: Zusammenfassung

Die Syntax legt den Aufbau von Programmen fest — wie notiere ich eine Rechenvorschrift in einer für den Rechner akzeptablen Form? Die Semantik beschäftigt sich mit der Bedeutung von Programmen — welches Ergebnis erzielt die Rechenvorschrift? Die konkrete Syntax detailliert den Aufbau auf der Ebene von Zeichen und Wörtern. Die abstrakte Syntax löst sich von oft zufälligen Details und beschreibt den hierarchischen Aufbau von Programmen. Die abstrakte Syntax wird mit Hilfe von Baumsprachen festgelegt, die Semantik mit Hilfe von Beweissystemen. Beides hat normativen Charakter.

Was nehmen Sie aus dem Kapitel mit? Was ist merkenswert oder bemerkenswert? Schreiben Sie ihre eigene Zusammenfassung — Do It Yourself. Das Kästchen auf der rechten Seite bietet reichlich Platz.

3. Werte\Elementares Rechnen

Semantics is a strange kind of applied mathematics;
it seeks profound definitions rather than difficult theorems.

— J.C. Reynolds (1980)

Sprachen, natürliche wie künstliche, sind komplexe Gebilde. Eine Sprache wie Deutsch oder Englisch lernt man über viele Jahre hinweg; vollständig beherrscht man sie wohl nie. Für die Vorstellung unserer Programmiersprache steht uns naturgemäß nicht so viel Zeit zur Verfügung. Wir benötigen sie allerdings auch nicht, da Mini-F# bezüglich Struktur, Bedeutung und Verwendung wesentlich einfacher gestrickt ist. Dies liegt zum einen daran, dass eine Programmiersprache nur einem Zweck dient, nämlich einen oder mehrere Rechner zum Rechnen zu bringen, und zum anderen daran, dass sich die Sprache Mini-F# nicht über Jahrhunderte, sondern nur über wenige Jahre hin entwickelt hat.

Wir werden einige Wochen benötigen, um die Sprache vorzustellen und präzise zu definieren. Dabei werden wir die Bestandteile, die sogenannten ***Sprachkonstrukte***, in kleinen, wohlportionierten Dosen verabreichen. Die ersten fünf Dosen erhalten Sie in diesem Kapitel. Am Ende des Kapitels kennen und können wir eine Programmiersprache, die ***berechnungsuniversell*** ist, das heißt, mit der man die prinzipiellen Möglichkeiten eines Rechners ausschöpfen kann. Aus Sicht der Theorie sind die folgenden Kapitel nur Zugabe; aus Sicht der Praxis wird es dann erst interessant.

Jeder Abschnitt in diesem Kapitel und in den meisten der folgenden Kapitel folgt einer einheitlichen Struktur, die in Abbildung 3.1 schematisch dargestellt ist. Prinzipiell wird in jedem Abschnitt *ein* bestimmtes Sprachmerkmal oder neudeutsch Sprachfeature eingeführt.

Zunächst werden jeweils die neuen Sprachkonstrukte motiviert. Oft anhand von Beispielen, die zeigen, dass bestimmte Aufgaben sich mit den bis dato eingeführten Sprachmitteln nicht oder nur schlecht bewerkstelligen lassen. Anschließend wird die Syntax, die äußere Form, und die Semantik, die Bedeutung der Konstrukte, definiert.

Ein Programm in Mini-F# ist technisch gesehen ein ***Ausdruck***; im einfachsten Fall ein arithmetischer Ausdruck wie $4711 + 815$ oder eine Zeichenkette (engl. string) wie `"hello, world"`. Neue Features führen neue Ausdrücke ein: Die syntaktische Kategorie `Expr` der Ausdrücke wird im Laufe der Vorlesung schrittweise um neue Formen erweitert. Um uns nicht in syntaktischen Details zu verlieren, beschreiben wir nur die ***abstrakte Syntax***, nicht die konkrete. Erstere weicht aber wie bereits angekündigt in der Regel nur unwesentlich von der letzteren ab. Wenn es Abweichungen gibt, benennen wir sie kurz. (Anhang A fasst die Unterschiede zusammen.)

Ausdrücke sind beliebig kombinierbar, ein bemerkenswertes Feature unserer Sprache. Nicht alle Kombination ergeben jedoch Sinn. Zum Beispiel lässt das Programm `"hello, world"` $*$ 4711 einen Programmierfehler vermuten. Die ***statische Semantik*** fängt diese sinnlosen Ausdrücke ab (technisch würde man auch von wertlosen Ausdrücken sprechen). Zu diesem Zweck werden Ausdrücke mit Hilfe sogenannter ***Typen*** in Schubladen eingeteilt: Ein arithmetischer Ausdruck erhält zum Beispiel den Typ *Nat*. Die statische Semantik legt dann fest, dass die Multiplikation zwei natürliche Zahlen verarbeitet und eine natürliche Zahl zum Ergebnis hat.

$$\frac{e_1 : \mathit{Nat} \qquad e_2 : \mathit{Nat}}{e_1 * e_2 : \mathit{Nat}}$$

Motivation

Abstrakte Syntax

$e \in \mathsf{Expr} ::= \cdots$ ***Ausdrücke***

Statische Semantik

$t \in \mathsf{Type} ::= \cdots$ ***Typen***

Dynamische Semantik

$\nu \in \mathsf{Val} ::= \cdots$ ***Werte***

Vertiefung

Blick über den Tellerrand

Abbildung 3.1.: Struktur eines Abschnitts.

Für jedes neu eingeführte Konstrukt wird eine ***Typregel*** angegeben. Diese Beweisregeln spezifizieren die zweistellige Relation

$$e : t$$

zwischen Ausdrücken und Typen. *Lies:* »e hat den Typ t«.

Die statische Semantik hat eine wichtige ordnende Funktion: Die meisten Abschnitte führen *einen* neuen Typ oder *ein* neues Typkonstrukt ein, zusammen mit Sprachkonstrukten, die auf diesem Typ arbeiten.

Ein Ausdruck e heißt ***wohlgetypt***, wenn es einen Typ t gibt, so dass sich $e : t$ mit den Regeln der statischen Semantik ableiten lässt. Der Ausdruck $4711 * 2 + 815$ ist wohlgetypt, der Ausdruck `"hello, world"` $* 4711$ ist es hingegen nicht.

Wohlgetypte Ausdrücke können ausgerechnet werden und nur solche. Wie dies geschieht, spezifiziert die ***dynamische Semantik***. Die dynamische Semantik legt zum Beispiel für die Multiplikation fest, dass beide Argumente ausgerechnet werden und dass das Ergebnis das Produkt der Teilergebnisse ist.

$$\frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{e_1 * e_2 \Downarrow n_1 \cdot n_2}$$

Für jedes neu eingeführte Konstrukt wird mindestens eine ***Auswertungsregel*** angegeben. Auswertungsregeln spezifizieren die zweistellige Relation

$$e \Downarrow \nu$$

zwischen Ausdrücken und Werten. *Lies:* »e wertet zu ν aus«. Ein Wert ist das Ergebnis eines Programms; zum Beispiel ist der Wert eines arithmetischen Ausdrucks eine natürliche Zahl. Mit jedem neu eingeführten Typ werden wir auch den Bereich der Werte um entsprechende Elemente erweitern. Ein Typ ist im Prinzip die Menge aller zugehörigen Werte. Da Werte nicht ausgewertet werden müssen, haben die Auswertungsregeln für diese Ausdrücke stets die triviale Form

$$\frac{}{\nu \Downarrow \nu}$$

Ein Programm, sprich ein Ausdruck, wird ausgerechnet, indem die Auswertungsregeln für die einzelnen Bestandteile des Ausdrucks zu einem Beweisbaum kombiniert werden, siehe Abschnitt 2.4. Zur Erinnerung: Für den arithmetischen Ausdruck $4711 * 2 + 815$ erhalten wir zum Beispiel den folgenden Beweisbaum.

$$\dfrac{\dfrac{\overline{4711 \Downarrow 4711} \qquad \overline{2 \Downarrow 2}}{4711 * 2 \Downarrow 9422} \qquad \overline{815 \Downarrow 815}}{4711 * 2 + 815 \Downarrow 10237}$$

Konstanten wie 4711 oder 815 werten zu sich selbst aus — Konstanten *sind* Werte. Die baumartige Darstellung zeigt sehr schön, wie die einzelnen Auswertungsregeln kombiniert werden. Am Anfang der Vorlesung werden wir Beispielrechnungen in aller Ausführlichkeit ohne jedwede Auslassung notieren. Sobald wir etwas Erfahrung gewonnen haben, kürzen wir Teilrechnungen ab oder lassen sie ganz aus.

$$\dfrac{\overline{4711 * 2 \Downarrow 9422}}{4711 * 2 + 815 \Downarrow 10237}$$

Hier sind die trivialen Teilrechnungen für die Konstanten unter den Tisch gefallen.

Jeder Abschnitt schließt mit Anwendungen der neu eingeführten Konstrukte. Da wir in diesem Kapitel nur das Grundvokabular der Sprache vermitteln, sind die Beispielprogramme ebenfalls recht elementar, insbesondere in den ersten Abschnitten. Gelegentlich blicken wir auch über den Tellerrand hinaus und schauen uns an, was andere Programmiersprachen (insbesondere F# selbst) zu dem jeweiligen Thema anbieten.

Praxistipp

Lesen Sie jeweils erst die Motivation und die Vertiefung; nehmen Sie sich erst dann die Theorie vor und wiederholen Sie abschließend noch einmal die Vertiefung.

3.1. Natürliche Zahlen

Die ganze Zahl schuf der liebe Gott,
alles übrige ist Menschenwerk.

— Leopold Kronecker (1823–1891)

Die natürliche Zahl schuf der liebe Gott,
alles übrige ist Menschenwerk.

— Ralf Hinze (1965)

Den Begriff Rechnen werden die meisten mit Zahlen in Verbindung bringen. In diesem Abschnitt führen wir einige elementare Konstrukte zum Rechnen mit natürlichen Zahlen ein. Die Sprachunterstützung ist zunächst recht spartanisch; »liebgewonnene« Operationen wie etwa die Potenzfunktion oder die Quadratwurzel werden erst in einem späteren Abschnitt formal definiert. Was heißt »formal definiert«? Wir zeigen später, wie man diese Operationen programmieren kann.

Abstrakte Syntax Unser erstes Sprachfeature umfasst insgesamt sechs Konstrukte: Neben den natürlichen Zahlen selbst führen wir zwei gängige und drei nicht so gängige arithmetische Operatoren ein.

$n \in \mathbb{N}$	$::= 0 \mid 1 \mid 2 \mid \cdots$	***natürliche Zahlen***
$e \in \mathsf{Expr}$	$::=$	***Arithmetische Ausdrücke:***
	$\mid n$	natürliche Zahl
	$\mid e_1 + e_2$	Addition
	$\mid e_1 \dot{-} e_2$	natürliche Subtraktion (»monus«)
	$\mid e_1 * e_2$	Multiplikation
	$\mid e_1 \div e_2$	natürliche Division
	$\mid e_1 \,\%\, e_2$	Divisionsrest

Die Subtraktion auf den natürlichen Zahlen (»monus«) und die Subtraktion auf den ganzen oder reellen Zahlen (»minus«) haben sehr unterschiedliche Eigenschaften. Aus diesem Grund ist es hilfreich, sie einfach syntaktisch unterscheiden zu können. Gleiches gilt für die Division. Mehr dazu in Kürze. Die konkrete Syntax für $\dot{-}$ ist `-` und für $\div$ ist `/`.

Statische Semantik Ein arithmetischer Ausdruck hat den Typ *Nat*.

$t \in \mathsf{Type}$	$::=$	***Typen:***
	$\mid \mathit{Nat}$	Typ der natürlichen Zahlen

Um Typen gut von Ausdrücken und Werten unterscheiden zu können, verwenden wir Farben: Typen werden in königsblau (engl. royal blue) gesetzt, Ausdrücke und Werte in kohlschwarz (engl. coal black). Die Farben sind bewusst gewählt. Sie erinnern uns stets daran, dass Typen und Werte eine Zweiklassengesellschaft bilden: Die Oberschicht, die Aristokratie, ordnet und dirigiert; die Unterschicht, die Arbeiterklasse, erledigt die eigentliche Arbeit. Die zwei Schichten korrespondieren zu den zwei Phasen der Programmabarbeitung: Überprüfung der statischen Semantik zur ***Übersetzungszeit*** und Ausführung der dynamischen Semantik zur ***Laufzeit***.

Die arithmetischen Operatoren erwarten jeweils zwei Argumente vom Typ *Nat* und haben ein Ergebnis vom Typ *Nat*.

$$\frac{}{n : \mathit{Nat}} \qquad \frac{e_1 : \mathit{Nat} \qquad e_2 : \mathit{Nat}}{e_1 + e_2 : \mathit{Nat}} \qquad \frac{e_1 : \mathit{Nat} \qquad e_2 : \mathit{Nat}}{e_1 \dot{-} e_2 : \mathit{Nat}} \qquad \text{usw.}$$

Dynamische Semantik Ein arithmetischer Ausdruck wertet, wenig überraschend, zu einer natürlichen Zahl aus.

$v \in \mathsf{Val}$	$::=$	***Werte:***
	$\mid n$	natürliche Zahlen

Da alle Operatoren auf den natürlichen Zahlen und nicht etwa auf den ganzen, rationalen oder gar reellen Zahlen arbeiten, müssen wir bei der Formulierung der Auswertungsregeln Vorsicht walten lassen. Zum Beispiel evaluiert $0 \dot{-} 1$ zu 0 (*lies:* 0 monus 1 ergibt 0). Die Metavariablen k, q und r rangieren jeweils über den natürlichen Zahlen: $k, q, r \in \mathbb{N}$.

$$\frac{}{n \Downarrow n} \qquad \frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{e_1 + e_2 \Downarrow n_1 + n_2} \qquad \frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{e_1 * e_2 \Downarrow n_1 \cdot n_2}$$

$$\frac{e_1 \Downarrow n + k \qquad e_2 \Downarrow n}{e_1 \dot{-} e_2 \Downarrow k} \qquad \frac{e_1 \Downarrow n \qquad e_2 \Downarrow n + k}{e_1 \dot{-} e_2 \Downarrow 0}$$

Die Differenz zweier Ausdrücke ist 0, wenn das zweite Argument größer ist als das erste.

Die Operatoren »÷« und »%« implementieren die Division mit Rest: $a \div b$ ist der Quotient von a und b und $a \,\%\, b$ ist der Divisionsrest.

$$\frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{e_1 \div e_2 \Downarrow q} \qquad n_1 = q \cdot n_2 + r \text{ und } r < n_2$$

$$\frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{e_1 \,\%\, e_2 \Downarrow r} \qquad n_1 = q \cdot n_2 + r \text{ und } r < n_2$$

Die Auswertungsregeln haben jeweils eine Nebenbedingung, die neben der Regel aufgeführt ist. Die Nebenbedingung formuliert Einschränkungen an die Belegung der Metavariablen. So ist zum Beispiel $47 \,\%\, 11 \Downarrow r$ nur ableitbar, wenn $47 = 11 \cdot q + r$ und $r < 11$ gilt. Da q und r natürliche Zahlen sein müssen, schränkt die Nebenbedingung r auf 3 und q auf 4 ein. Für $b > 0$ gelten stets die ***Divisionsregeln***:

$$a = (a \div b) * b + (a \,\%\, b) \quad \text{und} \quad 0 \leqslant a \,\%\, b < b \tag{3.1}$$

Jede natürliche Zahl a lässt sich eindeutig in einen Quotienten und in einen Rest zerlegen (für ein festes $b > 0$). Das ist eine merkenswerte Eigenschaft, von der wir wiederholt Gebrauch machen werden.

Ist $b = 0$, dann ist keine der Operationen definiert — die obigen Regeln sind nicht anwendbar, da es kein r mit $r < 0$ gibt. Dies ist natürlich keine befriedigende Lösung; wir werden auf dieses Problem erst in einem sehr viel späteren Abschnitt zurückkommen. Ein *Problem* ist das undefinierte Verhalten tatsächlich, hatten wir doch vollmundig angekündigt, dass alle wohlgetypten Ausdrücke ausgerechnet werden können. Nun ist zum Beispiel das Programm $1 \div 0$ wohlgetypt; die dynamische Semantik ordnet ihm aber keinen Wert zu — das wird sich in Abschnitt 7.4 ändern.

Vertiefung Unsere Programmiersprache hat die Funktionalität eines einfachen Taschenrechners. Lassen wir ihn, den ***Interpreter*** für Mini–F#, also rechnen. Die Benutzungsschnittstelle des Interpreters ist einfach und intuitiv. Man gibt einen Ausdruck ein, der Interpreter wertet den Ausdruck aus und gibt den resultierenden Wert aus. Dann geht es von vorne los — dieser Zyklus des Einlesens, Auswertens und Ausgebens heißt im Englischen ***read-eval-print loop*** (kurz ***REPL***).

```
⋙ 4711 * 2 + 815
10237
```

Die Zeichenfolge »⋙ «, das sogenannte ***Prompt***, fordert die Benutzerin oder den Benutzer auf, eine Eingabe zu tätigen; das Ergebnis wird in der nächsten Zeile ausgegeben.

```
⋙ 11 * 11
121
⋙ 111 * 111
12321
⋙ 111111111 * 111111111
12345678987654321
```

F# Interpreter

Der *reale* F# Interpreter unterscheiden sich in einigen Details vom *virtuellen* Mini–F# Interpreter: Natürliche Zahlen müssen mit dem Suffix `N` gekennzeichnet werden; Eingaben werden mit `;;` abgeschlossen.

```
> 11N * 11N ;;
val it : Nat = 121N
> it * it ;;
val it : Nat = 14641N
```

Mehr dazu im Anhang A.

Die Ergebnisse werden mit mathematischer Genauigkeit berechnet, so wie die Semantik es vorsieht. (Die Genauigkeit ist insbesondere nicht auf die native Genauigkeit von Rechnern, sei es 32 Bit oder 64 Bit, eingeschränkt: Wir rechnen mit mathematischen Zahlen, nicht mit Maschinenzahlen.)

Die meisten von Ihnen werden gewohnt sein, mit den rationalen oder den reellen Zahlen zu rechnen. Bei Umformungen etwa beim Lösen von Gleichungen vertrauen wir darauf, dass die elementaren arithmetischen Operationen Umkehroperationen besitzen: $(a - b) + b$ vereinfacht sich stets zu a. Beim Rechnen mit den natürlichen Zahlen müssen wir etwas aufpassen: $\dot{-}$ ist nicht die Umkehroperation von $+$ und $\div$ ist nicht invers zu $*$. Zum Beispiel wertet $(4 \dot{-} 7) + 7$ zu 7 aus und nicht etwa zu 4, der Ausdruck $(7 \div 4) * 4$ ergibt 4, nicht 7. Wir wollen es an dieser Stelle bei einer Warnung belassen und uns nicht in die algebraischen Eigenschaften der natürlichen Subtraktion und Division vertiefen. Wenn Sie aber Interesse an dem mathematischen Hintergrund haben, sei Ihnen Anhang B.5, speziell Abschnitt B.5.1, ans Herz gelegt.

Übungen.

1. Die dynamische Semantik schreibt vor, dass beide Argumente der arithmetischen Operationen ausgewertet werden. Muss das zwangsläufig so sein?

3.2. Boolesche Werte

Nicht-triviale Programme treffen viele Entscheidungen. Im einfachsten Fall wird überprüft, ob ein bestimmter Sachverhalt wahr oder falsch ist: Ist das Konto überzogen? Ist Florian größer als Lisa? usw. Das Ergebnis einer solchen Überprüfung repräsentieren wir durch einen ***Wahrheitswert***: *true* oder *false*. In Abhängigkeit von einem Wahrheitswert kann die Rechnung dann einen bestimmten Verlauf nehmen. Das linguistische Konstrukt, das eine abhängige Berechnung realisiert, ist die ***Alternative***:

if e_1 ***then*** e_2 ***else*** e_3

Wertet der Ausdruck e_1, die sogenannte ***Bedingung***, zu *true* aus, dann wird mit der Auswertung von e_2 fortgefahren; wertet e_1 zu *false* aus, dann wird e_3 ausgewertet. Im folgenden Beispiel werden zwei Alternativen ausgewertet:

$$\dfrac{\dfrac{\dfrac{}{4711 < 815 \Downarrow \mathit{false}} \qquad \dfrac{}{\mathit{true} \Downarrow \mathit{true}}}{\textbf{\textit{if}}\ 4711 < 815\ \textbf{\textit{then}}\ \mathit{false}\ \textbf{\textit{else}}\ \mathit{true} \Downarrow \mathit{true}} \qquad \dfrac{}{\texttt{"yes"} \Downarrow \texttt{"yes"}}}{\textbf{\textit{if}}\ (\textbf{\textit{if}}\ 4711 < 815\ \textbf{\textit{then}}\ \mathit{false}\ \textbf{\textit{else}}\ \mathit{true})\ \textbf{\textit{then}}\ \texttt{"yes"}\ \textbf{\textit{else}}\ \texttt{"no"} \Downarrow \texttt{"yes"}}$$

Alternativen dürfen beliebig geschachtelt werden. Im obigen Beispiel ist die Bedingung der äußeren Alternative wiederum eine Alternative. Die freie Kombinierbarkeit gilt nicht nur für Alternativen, sondern wie gesagt für alle Ausdrücke, die wir im Laufe der Vorlesung kennenlernen. (Die Entwicklung unserer Programmiersprache befindet sich noch in einem embryonalen Stadium, dementsprechend belanglos sind die Beispiele.)

Abstrakte Syntax Neben den Wahrheitswerten und der Alternative kommen ***Vergleichsoperatoren*** zur Syntax hinzu.

Der englische Mathematiker George Boole entwickelte in seiner Schrift »The Mathematical Analysis of Logic« von 1847 den ersten algebraischen Logikkalkül und begründete damit die moderne mathematische Logik.

Boole stellte die Wahrheitswerte durch die Zahlen 0 und 1 dar und drückte die logischen Operationen entsprechend durch arithmetische Operationen aus.

56 OF HYPOTHETICALS.

1st. Disjunctive Syllogism.

Either X is true, or Y is true (exclusive),	$x + y - 2xy = 1$
But X is true,	$x = 1$
Therefore Y is not true,	$\therefore y = 0$
Either X is true, or Y is true (not exclusive),	$x + y - xy = 1$
But X is not true,	$x = 0$
Therefore Y is true,	$\therefore y = 1$

Abbildung 3.2.: George Boole (1815–1864).

$e ::= \cdots$	***Boolesche Ausdrücke:***
$\mid$ *false*	falsch
$\mid$ *true*	wahr
$\mid$ ***if*** e_1 ***then*** e_2 ***else*** e_3	Alternative
$\mid e_1 < e_2$	kleiner
$\mid e_1 \leqslant e_2$	kleiner gleich
$\mid e_1 = e_2$	gleich
$\mid e_1 <> e_2$	ungleich
$\mid e_1 \geqslant e_2$	größer gleich
$\mid e_1 > e_2$	größer

Das Auslassungszeichen (⋯) soll deutlich machen, dass wir die syntaktische Kategorie $e \in \mathsf{Expr}$ *erweitern*: die oben aufgeführten Konstrukte kommen zu den im vorherigen Abschnitt eingeführten hinzu. Die Ausdrücke rund um die Wahrheitswerte sind nach dem englischen Mathematiker George Boole benannt, siehe Abbildung 3.2.

Der Teilausdruck e_1 nach dem Schlüsselwort[1] ***if*** heißt ***Bedingung***; die Teilausdrücke e_2 und e_3 heißen ***Zweige*** der Alternative.

In der konkreten Syntax bestehen die Vergleichsoperatoren $\leqslant$ und $\geqslant$ jeweils aus zwei Zeichen: <= und >=.

Statische Semantik Ein Boolescher Ausdruck hat den Typ *Bool*.

$t ::= \cdots$	***Typen:***
$\mid$ *Bool*	Typ der Booleschen Werte

Die Wahrheitswerte *false* und *true* sind vom Typ *Bool*.

$$\frac{}{\mathit{false} : \mathit{Bool}} \qquad \frac{}{\mathit{true} : \mathit{Bool}}$$

[1] Ein Schlüsselwort ist ein Konzept der lexikalischen Syntax: eine Folge von Buchstaben, die reserviert ist und somit nicht als Bezeichner verwendet werden kann. Schlüsselwörter heben wir farblich hervor.

$$\frac{e_1 : \mathit{Bool} \qquad e_2 : t \qquad e_3 : t}{\textbf{\textit{if}}\ e_1\ \textbf{\textit{then}}\ e_2\ \textbf{\textit{else}}\ e_3 : t}$$

Die Bedingung e_1 muss ein Boolescher Ausdruck sein; die Zweige der Alternative müssen den gleichen Typ besitzen, dieser ist auch der Typ der gesamten Alternative. Die Vergleichsoperatoren erwarten zwei Argumente vom Typ *Nat*, geben aber ein Element vom Typ *Bool* zurück.

$$\frac{e_1 : \mathit{Nat} \qquad e_2 : \mathit{Nat}}{e_1 < e_2 : \mathit{Bool}} \qquad \frac{e_1 : \mathit{Nat} \qquad e_2 : \mathit{Nat}}{e_1 \leqslant e_2 : \mathit{Bool}} \qquad \text{usw.}$$

Die statische Semantik bringt Ordnung in die Welt der Programme: Ausdrücke werden hier zunächst unterteilt in arithmetische Ausdrücke vom Typ *Nat* und in Boolesche Ausdrücke vom Typ *Bool*. Auf diese Weise werden unsinnige Ausdrücke wie zum Beispiel $\mathit{false} + 4711$ oder $\textbf{\textit{if}}\ 0\ \textbf{\textit{then}}\ 0\ \textbf{\textit{else}}\ \mathit{true}$ abgefangen. Diese Ausdrücke sind unsinnig, da die dynamische Semantik ihnen keinen Wert zuordnet.

Die Umkehrung gilt übrigens nicht: $1 + (\textbf{\textit{if}}\ \mathit{true}\ \textbf{\textit{then}}\ 0\ \textbf{\textit{else}}\ \mathit{false})$ wertet zu 1 aus, ist aber nicht wohlgetypt, da beide Zweige der Alternative einen unterschiedlichen Typ besitzen. Dieses Phänomen ist typisch für statische Typsysteme. Dynamische Eigenschaften von Programmen zählen in der Regel zu den formal unentscheidbaren Problemen. Aus diesem Grund ist die statische Semantik nur eine Annäherung an das tatsächliche Verhalten, allerdings von der sicheren Seite. Wertlose Programme, denen die dynamische Semantik keinen Wert zuordnet, werden von den Typregeln herausgefischt; in den Maschen bleiben aber auch Programme hängen, deren Wert definiert ist. Mehr zu unentscheidbaren Problemen erfahren Sie in späteren Semestern aus der Abteilung der Theoretischen Informatik.

Dynamische Semantik Boolesche Ausdrücke werten zu den Wahrheitswerten *false* und *true* aus, um die wir den Bereich der Werte erweitern.

$\nu ::= \cdots$	***Boolesche Werte:***
$\mid \mathit{false}$	falsch
$\mid \mathit{true}$	wahr

Die Wahrheitswerte *false* und *true* werten zu sich selbst aus. Dies gilt wie gesagt allgemein für alle Werte.

$$\frac{}{\mathit{false} \Downarrow \mathit{false}} \qquad \frac{}{\mathit{true} \Downarrow \mathit{true}}$$

$$\frac{e_1 \Downarrow \mathit{true} \qquad e_2 \Downarrow \nu}{\textbf{\textit{if}}\ e_1\ \textbf{\textit{then}}\ e_2\ \textbf{\textit{else}}\ e_3 \Downarrow \nu} \qquad \frac{e_1 \Downarrow \mathit{false} \qquad e_3 \Downarrow \nu}{\textbf{\textit{if}}\ e_1\ \textbf{\textit{then}}\ e_2\ \textbf{\textit{else}}\ e_3 \Downarrow \nu}$$

Die dynamische Semantik der Alternative wird mit Hilfe zweier Regeln spezifiziert; diese legen fest, dass die Bedingung ausgewertet wird und in Abhängigkeit vom Ergebnis dieser Auswertung *genau* einer der beiden Zweige.

Für jede Vergleichsoperation gibt es zwei Auswertungsregeln.

$$\frac{e_1 \Downarrow n+k \qquad e_2 \Downarrow n}{e_1 < e_2 \Downarrow \mathit{false}} \qquad \frac{e_1 \Downarrow n \qquad e_2 \Downarrow n+k+1}{e_1 < e_2 \Downarrow \mathit{true}} \qquad \text{usw.}$$

Wertet e_1 zu $n+k$ und e_2 zu n aus, dann ist $e_1 < e_2$ äquivalent zu $n+k < n$, einer falschen Aussage, da k vereinbarungsgemäß eine natürliche Zahl ist.

Vertiefung: Logische Verknüpfungen Ein Boolescher Ausdruck modelliert einen Sachverhalt oder eine Aussage. Wir sind gewohnt, einfache Aussagen zu komplexen Aussagen zusammenzusetzen: Der Kunde ist *nicht* kreditwürdig (***Negation***). Das Konto ist überzogen *und* der Kunde ist nicht kreditwürdig (***Konjunktion***). Das Netzteil ist defekt *oder* die Leitung ist unterbrochen (***Disjunktion***). Diese sogenannten Booleschen Verknüpfungen lassen sich mit Hilfe der Alternative programmieren. Ist e ein Boolescher Ausdruck, dann programmiert

if e *then false else true*

die ***Negation*** von e. Die ***Konjunktion*** von e_1 und e_2 wird durch

if e_1 *then* e_2 *else false*

und die ***Disjunktion*** durch

if e_1 *then true else* e_2

realisiert.

Boolesche Verknüpfungen werden oft mit Hilfe von sogenannten Wahrheitstafeln eingeführt, die das Ein-/Ausgabeverhalten tabellieren.

	Negation
false	*true*
true	*false*

Konjunktion	*false*	*true*
false	*false*	*false*
true	*false*	*true*

Disjunktion	*false*	*true*
false	*false*	*true*
true	*true*	*true*

Wir können uns leicht davon überzeugen, dass die Miniprogramme die entsprechenden Verknüpfungen realisieren. Wertet zum Beispiel e zu *false* aus, dann wertet der Ausdruck für die Negation *if* e *then false else true* zu *true* aus usw.

Negation, Konjunktion und Disjunktion werden häufig bei der Formulierung von Bedingungen eingesetzt. Deshalb erlauben wir auch abkürzende Schreibweisen:

- *not* e statt *if* e *then false else true*,
- e_1 && e_2 statt *if* e_1 *then* e_2 *else false* und
- e_1 || e_2 statt *if* e_1 *then true else* e_2.

Es ist lohnenswert, sich mit den Eigenschaften der logischen Verknüpfungen vertraut zu machen: Anhang B.1 führt in die Grundbegriffe der Logik ein; Abschnitte B.1.2 und B.4.3 beleuchten die mathematische Struktur Boolescher Verknüpfungen aus zwei unterschiedlichen Perspektiven.

Übungen.

1. Machen Sie sich noch einmal den Unterschied zwischen Syntax und Semantik klar.

(a) Wieviele Boolesche Ausdrücke gibt es?

(b) Wieviele Boolesche Werte gibt es?

2. Die dynamische Semantik schreibt vor, dass beide Argumente der Vergleichsoperationen ausgewertet werden. Muss das zwangsläufig so sein?

3. Mit Hilfe der dynamischen Semantik kann man zeigen, dass zwei Ausdrücke äquivalent sind, dass beide Ausdrücke zum gleichen Wert ausrechnen, etwa $(2+3)*4$ und $2*4+3*4$. (Zu diesem Zweck kann auch der Mini-F# Interpreter herangezogen werden.) Es lassen sich darüber hinaus auch allgemeine Aussagen

über ***Ausdrucksschemata*** treffen, das sind Ausdrücke, die Metavariablen enthalten. Zum Beispiel gilt das Distributivgesetz:

$$(e_1 + e_2) * e_3 \quad = \quad (e_1 * e_3) + (e_2 * e_3)$$

für beliebige Ausdrücke e_1, e_2 und e_3. Dazu muss man zeigen, dass sich jeder Beweisbaum für $(e_1 + e_2) * e_3 \Downarrow \nu$ in einen Beweisbaum für $(e_1 * e_3) + (e_2 * e_3) \Downarrow \nu$ überführen lässt und umgekehrt. Da es für »+« und »*« nur jeweils eine Auswertungsregel gibt, ist der Beweis recht einfach: Ist $\mathcal{P}_i$ ein Beweisbaum mit der Wurzel $e_i \Downarrow \nu_i$, dann lassen sich die Beweisbäume

$$\dfrac{\dfrac{\mathcal{P}_1 \qquad \mathcal{P}_2}{e_1 + e_2 \Downarrow \nu_1 + \nu_2} \qquad \mathcal{P}_3}{(e_1 + e_2) * e_3 \Downarrow (\nu_1 + \nu_2) \cdot \nu_3} \qquad \text{und} \qquad \dfrac{\dfrac{\mathcal{P}_1 \qquad \mathcal{P}_3}{e_1 * e_3 \Downarrow \nu_1 \cdot \nu_3} \qquad \dfrac{\mathcal{P}_2 \qquad \mathcal{P}_3}{e_2 * e_3 \Downarrow \nu_2 \cdot \nu_3}}{(e_1 * e_3) + (e_2 * e_3) \Downarrow \nu_1 \cdot \nu_3 + \nu_2 \cdot \nu_3}$$

direkt ineinander überführen. (Dass $(\nu_1 + \nu_2) \cdot \nu_3 = \nu_1 \cdot \nu_3 + \nu_2 \cdot \nu_3$ ist, folgt aus den algebraischen Eigenschaften der Addition und der Multiplikation.) Zeigen Sie auf ähnliche Art und Weise die Äquivalenz der folgenden Ausdrucksschemata.

$$\begin{aligned}
&\textit{if } \textit{true } \textit{then } e_1 \textit{ else } e_2 && = && e_1 \\
&\textit{if } \textit{false } \textit{then } e_1 \textit{ else } e_2 && = && e_2 \\
&\textit{if } e \textit{ then } \textit{true } \textit{else } \textit{false} && = && e \\
&\textit{if } (\textit{if } e_1 \textit{ then } e_2 \textit{ else } e_3) \textit{ then } e_4 \textit{ else } e_5 && && \\
&\qquad && = && \textit{if } e_1 \textit{ then if } e_2 \textit{ then } e_4 \textit{ else } e_5 \textit{ else if } e_3 \textit{ then } e_4 \textit{ else } e_5 \\
&(\textit{if } e_1 \textit{ then } e_2 \textit{ else } e_3) * e_4 && = && \textit{if } e_1 \textit{ then } e_2 * e_4 \textit{ else } e_3 * e_4
\end{aligned}$$

Lassen sich die letzten beiden Regeln verallgemeinern?

3.3. Wertedefinitionen

> *The primary purpose of the* `DATA` *statement is to give names to constants; instead of referring to* π *as 3.141592653589793 at every appearance, the variable* `PI` *can be given that value with a* `DATA` *statement and used instead of the longer form of the constant. This also simplifies modifying the program, should the value of* π *change.*
>
> — FORTRAN *manual for Xerox computers*

Rechnungen sind in der Regel nicht linear, sie enthalten Zwischen- oder Hilfsrechnungen: Soll zum Beispiel der Flächeninhalt eines Quadrats berechnet werden, wird man zunächst die Länge einer Seite bestimmen und dann das Ergebnis mit sich selbst multiplizieren. Ein modularer Aufbau von Rechnungen ist auch für unsere Programmiersprache wünschenswert. Um das Ergebnis einer Zwischenrechnung gegebenenfalls mehrfach verwenden zu können, geben wir ihm einen Namen. Ist e der Ausdruck, der die Länge der Seite berechnet, dann wird mit

$$\textit{let } s = e$$

der Name oder im Fachjargon der ***Bezeichner*** s an den *Wert* von e gebunden. Aus diesem Grund heißt $\textit{let } s = e$ auch ***Wertedefinition*** oder ***Wertebindung***.

Die Syntax ist an die natürlichsprachliche Formulierung angelehnt, die man häufig in handschriftlichen Rechnungen oder in mathematischen Texten findet: »sei $d = 2\pi$, …«. Nur ist, wie in der Programmierwelt üblich, das Schlüsselwort *let* dem Englischen entnommen.

Ein Bezeichner ist ein Ausdruck und kann somit überall dort verwendet werden, wo ein Ausdruck verlangt wird. Der Ausdruck

$$s * s$$

berechnet zum Beispiel den gewünschten Flächeninhalt des Quadrats. Der Bezeichner s wird in diesem Ausdruck zweimal verwendet.

Woher wissen wir, welche Bezeichner wir in einem Ausdruck verwenden können? Oder anders ausgedrückt, wie verbinden wir die Definition ***let*** $s = e$ mit dem Ausdruck $s * s$, in dem s verwendet wird? Die Antwort ist einfach: Wir führen ein weiteres linguistisches Konstrukt ein, das den Zusammenhang herstellt.

let $s = e$ ***in*** $s * s$

Die vor dem Schlüsselwort ***in*** aufgeführte Wertedefinition darf in dem Ausdruck, der nach dem Schlüsselwort aufgeführt wird, verwendet werden. Man sagt auch, die definierten Bezeichner sind dort ***sichtbar***. In unserem Beispiel erstreckt sich der Sichtbarkeitsbereich (engl. scope) des Bezeichners s auf den Ausdruck $s * s$.

Die Einschränkung der Sichtbarkeit von Bezeichnern hat den Vorteil, dass wir an verschiedenen Stellen im Programm den gleichen Bezeichner — gegebenenfalls auch für unterschiedliche Zwecke — verwenden können, ohne dass sich die verschiedenen Vorkommen ins Gehege kommen, eine wichtige Hygienemaßnahme. (Die Bedeutsamkeit dieses Features lässt sich erahnen, wenn man sich vergegenwärtigt, dass größere Softwaresysteme aus Millionen von Programmzeilen bestehen. Der Linux Kernel umfasste zum Beispiel im Jahre 2017 circa 25 Millionen Codezeilen.)

Der ***in***-Ausdruck ist, wie der Name sagt, ein Ausdruck und kann somit überall dort verwendet werden, wo ein Ausdruck verlangt wird:

(***let*** $s = e$ ***in*** $s * s$) + 1

In diesem Beispiel ist der erste Summand ein ***in***-Ausdruck. Beachte, dass der Bezeichner s im zweiten Summanden *nicht* sichtbar ist. Wollen wir s auch dort verwenden, müssen wir die Addition in die Klammern schieben bzw. diese weglassen:

let $s = e$ ***in*** $s * s + s$

Teilausdrücke zu benennen und mit Hilfe der vergebenen Namen wiederzuverwenden, gehört zu den grundlegenden Eigenschaften jeder Programmiersprache. Die Bezeichner können dabei frei gewählt werden: ***let*** $s = e$ ***in*** $s * s$ ist gleichwertig zu

let *size* = *e* ***in*** *size* ∗ *size*

oder auch

let *seitenlänge* = *e* ***in*** *seitenlänge* ∗ *seitenlänge*

Für das Ausrechnen und somit auch für den Rechner spielen Namen keine Rolle, wohl aber für den menschlichen Betrachter eines Programms. Deshalb sollte man sich bemühen, möglichst aussagekräftige Bezeichner zu vergeben. Wer viel programmiert, weiß, dass dies nicht immer leicht ist. Allgemein gilt: Je größer der Sichtbarkeitsbereich eines Namens, desto mehr Sorgfalt sollte man bei der Namenswahl walten lassen.

Wir haben bereits angemerkt, dass die gleichen Namen an unterschiedlichen Stellen eines Programms verwendet werden dürfen und auch Unterschiedliches meinen können. Wenn sich die Sichtbarkeitsbereiche *nicht* überlappen, ist dies kein Problem:

(***let*** $s = 4711$ ***in*** $s * s$) + (***let*** $s = 815$ ***in*** $s * s$)

Wenn sich die Sichtbarkeitsbereiche überlagern wie in

$$\textbf{\textit{let}}\ s = 4711\ \textbf{\textit{in}}\ (\textbf{\textit{let}}\ s = 815\ \textbf{\textit{in}}\ (s * s))$$

dann müssen wir festlegen, auf welche Definition sich der Bezeichner s in $s * s$ bezieht. Wir vereinbaren, dass jeweils die nächste Definition — von innen nach außen gelesen — die Bedeutung eines Bezeichners festlegt. Wir werden später sehen, dass dies tatsächlich die einzig sinnvolle Festlegung ist. Das obige Programm ist somit zu

$$\textbf{\textit{let}}\ s_1 = 4711\ \textbf{\textit{in}}\ (\textbf{\textit{let}}\ s_2 = 815\ \textbf{\textit{in}}\ (s_2 * s_2))$$

gleichwertig.

Abstrakte Syntax Wir führen eine neue syntaktische Kategorie ein: ***Deklarationen***. Fürs Erste ist eine Deklaration eine nicht-leere Sequenz von Wertedefinitionen.

$x \in \mathsf{Ident}$	***Bezeichner***
$d \in \mathsf{Decl} ::=$	***Deklarationen:***
$\mid$ $\textbf{\textit{let}}\ x = e$	Wertedefinition
$\mid$ $d_1\ d_2$	Sequenz von Deklarationen

Der Bereich der Bezeichner wird später in der lexikalischen Syntax in Kapitel 6 genau definiert. Dem vorausgreifend halten wir fest, dass ein Bezeichner mit einem Buchstaben anfängt; danach können weitere Buchstaben, Ziffern und Sonderzeichen wie ein Unterstrich oder ein Apostroph folgen.

Sequenzen von Deklarationen werden in der *konkreten* Syntax untereinander geschrieben: Aus dem Einzeiler $\textbf{\textit{let}}\ s = 4711\ \textbf{\textit{let}}\ a = s * s$ wird zum Beispiel der Zweizeiler

$$\begin{array}{l}\textbf{\textit{let}}\ s = 4711\\ \textbf{\textit{let}}\ a = s * s\end{array}$$

Die Kategorie der Ausdrücke wird um Bezeichner und lokale Definitionen erweitert.

$e ::= \cdots$	***lokale Definitionen:***
$\mid$ x	Bezeichner
$\mid$ $d\ \textbf{\textit{in}}\ e$	lokale Definition

Ein ***in***-Ausdruck verknüpft eine Definition mit einem Ausdruck. Der Teilausdruck e heißt Rumpf des ***in***-Ausdrucks.

Statische Semantik Die Semantikregeln, statische wie dynamische, sind idealerweise *kompositional*. Die Bedeutung eines Ausdrucks wird auf die Bedeutung seiner Teilausdrücke zurückgeführt. Diese wünschenswerte Eigenschaft stellt uns bei der Typisierung von ***in***-Ausdrücken wie $\textbf{\textit{let}}\ s = 4711 + 815\ \textbf{\textit{in}}\ s * s$ vor ein Problem: Wenn wir den Teilausdruck $s * s$ typisieren, woher kennen wir den Typ von s? Technisch gesprochen enthält der isolierte Ausdruck $s * s$ einen sogenannten *freien* Bezeichner, ein Bezeichner, der in dem Ausdruck selbst nicht definiert wird. Nun kann ein Bezeichner wie gesagt an unterschiedlichen Stellen im Programm Unterschiedliches bedeuten und insbesondere auch einen unterschiedlichen Typ besitzen.

$$(\textbf{\textit{let}}\ s = \mathit{true}\ \textbf{\textit{in}}\ s)\ \&\&\ (\textbf{\textit{let}}\ s = 815\ \textbf{\textit{in}}\ s * s > 4711)$$

Die Lösung dieses Problems ist vielleicht naheliegend: Wir müssen uns die Typen der jeweils sichtbaren Bezeichner merken. Diesem Zweck dient eine sogenannte *Signatur* (engl. signature oder interface), eine endliche Abbildung von Bezeichnern auf Typen.[2]

[2] Wir verwenden den griechischen Buchstaben Σ für Signaturen: Σ; der gleiche Buchstabe wird in der Mathematik auch als Summationszeichen verwendet: $\sum_{i=1}^{n} i = n \cdot (n+1)/2$. Die Farbe macht deutlich, was jeweils gemeint ist.

$\Sigma \in \mathsf{Sig} = \mathsf{Ident} \to_{\mathrm{fin}} \mathsf{Type}$ ***Signatur***

Wir erweitern unsere Typregeln entsprechend um Signaturen. Aus der zweistelligen Relation $e : t$ wird die dreistellige Relation

$$\Sigma \vdash e : t$$

zwischen Signaturen, Ausdrücken und Typen. *Lies:* »bezüglich der Signatur Σ hat e den Typ t«. (Der Hammer »$\vdash$« dient traditionell als Trennsymbol, ähnlich wie ein Punkt oder ein Semikolon im Deutschen.) Die ursprüngliche Relation $e : t$ gilt ab sofort als Abkürzung für $\varnothing \vdash e : t$ — wir nehmen an, dass die Signatur leer ist.

Unser Ausgangsbeispiel lässt sich somit wie folgt behandeln (etwas vereinfacht).

$$\dfrac{\dfrac{\dfrac{}{\varnothing \vdash 4711 : \mathit{Nat}} \quad \dfrac{}{\varnothing \vdash 815 : \mathit{Nat}}}{\varnothing \vdash 4711 + 815 : \mathit{Nat}} \quad \dfrac{\dfrac{}{\{s \mapsto \mathit{Nat}\} \vdash s : \mathit{Nat}} \quad \dfrac{}{\{s \mapsto \mathit{Nat}\} \vdash s : \mathit{Nat}}}{\{s \mapsto \mathit{Nat}\} \vdash s * s : \mathit{Nat}}}{\varnothing \vdash (\textbf{\textit{let}}\ s = 4711 + 815\ \textbf{\textit{in}}\ s * s) : \mathit{Nat}}$$

Die rechte Seite der lokalen Definition ***let*** $s = 4711 + 815$ wird bezüglich der leeren Signatur überprüft: Da $4711 + 815$ den Typ Nat besitzt, wird dem definierten Bezeichner dieser Typ zugewiesen: $\{s \mapsto \mathit{Nat}\}$. Bezüglich dieser Signatur wird anschließend der Rumpf des ***in***-Ausdrucks untersucht: Die Multiplikation erwartet zwei natürliche Zahlen als Argument; laut Signatur ist der Bezeichner s eine natürliche Zahl. Kurzum: Der Ausdruck ist wohlgetypt.

Alle bisherigen Typregeln müssen angepasst werden, zum Beispiel:

$$\dfrac{\Sigma \vdash e_1 : \mathit{Bool} \qquad \Sigma \vdash e_2 : t \qquad \Sigma \vdash e_3 : t}{\Sigma \vdash \textbf{\textit{if}}\ e_1\ \textbf{\textit{then}}\ e_2\ \textbf{\textit{else}}\ e_3 : t}$$

In den Zweigen der Alternative sind die gleichen Bezeichner sichtbar wie in der Alternative selbst.

Kommen wir zu den Wertedefinitionen. Die statische Semantik ordnet einem Ausdruck einen Typ zu: Dem Ausdruck $4711 + 815$ wird zum Beispiel der Typ Nat zugeordnet. Analog wird einer Wertedefinition eine Signatur zugeordnet: Der Definition ***let*** $s = 4711 + 815$ wird zum Beispiel die Signatur $\{s \mapsto \mathit{Nat}\}$ zugeordnet. Eine Signatur repräsentiert — ähnlich wie ein Typ — das, was wir über eine Definition statisch wissen wollen.

$$\dfrac{\Sigma \vdash e : t}{\Sigma \vdash (\textbf{\textit{let}}\ x = e) : \{x \mapsto t\}} \qquad \dfrac{\Sigma \vdash d_1 : \Sigma_1 \qquad \Sigma, \Sigma_1 \vdash d_2 : \Sigma_2}{\Sigma \vdash d_1\ d_2 : \Sigma_1, \Sigma_2}$$

Die Typregel für die Sequenz von Deklarationen verdient besondere Beachtung. Wir haben schon besprochen, dass in einer Folge von Deklarationen die späteren Deklarationen die früheren »sehen«: In ***let*** $s = e$ ***let*** $a = s * s$ bezieht sich s in $s * s$ auf die vorangegangene Bindung ***let*** $s = e$. Die gesamte Deklaration wird wie folgt typisiert:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \varnothing \vdash e : \mathit{Nat}\end{array}}{\varnothing \vdash (\textbf{\textit{let}}\ s = e) : \{s \mapsto \mathit{Nat}\}} \quad \dfrac{\dfrac{\dfrac{}{\{s \mapsto \mathit{Nat}\} \vdash s : \mathit{Nat}} \quad \dfrac{}{\{s \mapsto \mathit{Nat}\} \vdash s : \mathit{Nat}}}{\{s \mapsto \mathit{Nat}\} \vdash s * s : \mathit{Nat}}}{\{s \mapsto \mathit{Nat}\} \vdash (\textbf{\textit{let}}\ a = s * s) : \{a \mapsto \mathit{Nat}\}}}{\varnothing \vdash (\textbf{\textit{let}}\ s = e\ \textbf{\textit{let}}\ a = s * s) : \{s \mapsto \mathit{Nat}, a \mapsto \mathit{Nat}\}}$$

In der Signatur vor dem Symbol »$\vdash$« wird protokolliert, welche Bezeichner in einem Ausdruck oder einer Deklaration sichtbar sind. Wir starten »unten« mit der leeren Signatur $\varnothing$. Die erste Wertedefinition resultiert in der Signatur $\{s \mapsto \mathit{Nat}\}$. Die zweite Wertedefinition wird bezüglich $\varnothing, \{s \mapsto \mathit{Nat}\} = \{s \mapsto \mathit{Nat}\}$ typisiert und resultiert in der Bindung $\{a \mapsto \mathit{Nat}\}$. Zusammen erhalten wir $\{s \mapsto \mathit{Nat}\}, \{a \mapsto \mathit{Nat}\} = \{s \mapsto \mathit{Nat}, a \mapsto \mathit{Nat}\}$. Das Komma ist der Kommaoperator aus Abschnitt 2.1.

Spätere Wertedefinitionen können frühere »verschatten«, wenn sie die gleichen Bezeichner verwenden. Der Deklaration ***let*** s = *false* ***let*** $s = 4711$ wird die Signatur $\{s \mapsto Nat\}$ zugeordnet. Man spricht von Verschattung, weil die erste Definition prinzipiell zwar sichtbar ist, aber nicht mehr auf sie zugegriffen werden kann, da der Bezeichner s inzwischen anderweitig verwendet wird. Formal wird die Verschattung durch den Kommaoperator implementiert: In Σ_1, Σ_2 werden bei Überschneidungen den Bindungen in Σ_2 Vorrang eingeräumt.

$$\frac{\dfrac{\overline{\varnothing \vdash false : Bool}}{\varnothing \vdash (\textbf{let}\ s = false) : \{s \mapsto Bool\}} \qquad \dfrac{\overline{\{s \mapsto Bool\} \vdash 4711 : Nat}}{\{s \mapsto Bool\} \vdash (\textbf{let}\ s = 4711) : \{s \mapsto Nat\}}}{\varnothing \vdash (\textbf{let}\ s = false\ \textbf{let}\ s = 4711) : \{s \mapsto Nat\}}$$

Die Signatur der zwei Bindungen ist $\{s \mapsto Nat\}$, da $\{s \mapsto Bool\}, \{s \mapsto Nat\} = \{s \mapsto Nat\}$.

Wenden wir uns den Ausdrücken zu, die wir um Bezeichner und ***in***-Ausdrücke erweitert haben. Der Typ eines Bezeichners wird in der Signatur nachgeschlagen.

$$\frac{}{\Sigma \vdash x : \Sigma(x)} \qquad x \in dom\ \Sigma$$

Zur Erinnerung: Σ ist eine endliche Abbildung; damit $\Sigma(x)$ definiert ist, muss x im Definitionsbereich von Σ enthalten sein. Mit anderen Worten, zu jedem Bezeichner muss eine definierende Bindung existieren. Der Ausdruck $4711 * (a11 + 815)$ aus Abschnitt 2.2 ist zum Beispiel nicht wohlgetypt (bezüglich der leeren Signatur $\varnothing$), da der Bezeichner $a11$ nicht definiert ist. Als Teil eines größeren Programms, zum Beispiel ***let*** $a11 = 271828$ ***in*** $4711 * (a11 + 815)$, ist der Ausdruck aber okay.

Die Typregel für lokale Definitionen ähnelt der Regel für die Sequenz von Deklarationen.[3]

$$\frac{\Sigma \vdash d : \Sigma' \qquad \Sigma, \Sigma' \vdash e : t}{\Sigma \vdash (d\ \textbf{in}\ e) : t}$$

Der Kommaoperator hat einen weiteren Auftritt: Der Rumpf des ***in***-Ausdrucks wird bezüglich der erweiterten Signatur Σ, Σ' typisiert.

Kommen wir noch einmal auf unser Ausgangsbeispiel zurück:

$$\frac{\dfrac{\dfrac{\overline{\varnothing \vdash 4711 : Nat} \quad \overline{\varnothing \vdash 815 : Nat}}{\varnothing \vdash 4711 + 815 : Nat}}{\varnothing \vdash \textbf{let}\ s = 4711 + 815 : \{s \mapsto Nat\}} \qquad \dfrac{\overline{\{s \mapsto Nat\} \vdash s : Nat} \quad \overline{\{s \mapsto Nat\} \vdash s : Nat}}{\{s \mapsto Nat\} \vdash s * s : Nat}}{\varnothing \vdash (\textbf{let}\ s = 4711 + 815\ \textbf{in}\ s * s) : Nat}$$

Wie schon besprochen wird der Definition ***let*** $s = 4711 + 815$ die Signatur $\{s \mapsto Nat\}$ zugeordnet. Die leere Signatur wird um diese Signatur erweitert: $\varnothing, \{s \mapsto Nat\} = \{s \mapsto Nat\}$. (Zur Erinnerung: $\varnothing$ ist das neutrale Element des Kommaoperators.) Bezüglich dieser kombinierten Signatur wird dann der Rumpf $s * s$ typisiert. Dabei kommt das Axiom für Bezeichner zweimal zum Einsatz: $\{s \mapsto Nat\} \vdash s : Nat$ da $\{x \mapsto Nat\}(s) = Nat$.

Fassen wir zusammen:

Statische Semantik

Die *statische Semantik* ordnet

- einem Ausdruck einen Typ zu, $\Sigma \vdash e : t$, und
- einer Definition eine Signatur, $\Sigma \vdash d : \Sigma'$.

[3] Der Apostroph hat nichts mit dem Ableitungsoperator aus der Analysis zu tun; Σ' bezeichnet wie Σ eine Umgebung.

Die statische Semantik typisiert nur Ausdrücke und Definitionen, deren freie Bezeichner in der Signatur aufgeführt werden. Bevor ein Teilausdruck, der freie Bezeichner enthält, typisiert wird, wird zunächst die Signatur um die Typen der freien Bezeichner erweitert. Dies ist die große ***Invariante der statischen Semantik***.

Dynamische Semantik Die dynamische Semantik ordnet einem Ausdruck einen Wert zu: $4711 + 815$ wird zum Beispiel der Wert 5526 zugeordnet. Analog wird der Wertebindung ***let*** $x = 4711 + 815$ die sogenannte ***Umgebung*** $\{x \mapsto 5526\}$ zugeordnet. Ähnlich wie eine Signatur ist eine Umgebung (engl. environment) eine endliche Abbildung; im Unterschied zur Signatur bildet eine Umgebung Bezeichner auf Werte ab.

$\delta \in \mathsf{Env} = \mathsf{Ident} \to_{\mathrm{fin}} \mathsf{Val}$ ***Umgebung***

Wir erweitern unsere Auswertungsregeln entsprechend um Umgebungen. Aus der zweistelligen Relation $e \Downarrow \nu$ wird die dreistellige Relation

$$\delta \vdash e \Downarrow \nu$$

zwischen Umgebungen, Ausdrücken und Werten. *Lies:* »bezüglich der Umgebung δ wertet e zu dem Wert ν aus«. Die ursprüngliche Relation $e \Downarrow \nu$ dient ab sofort als Abkürzung für $\varnothing \vdash e \Downarrow \nu$ — wir nehmen an, dass die Umgebung leer ist. Die bisherigen Auswertungsregeln müssen entsprechend angepasst werden, zum Beispiel:

$$\frac{\delta \vdash e_1 \Downarrow \mathit{true} \qquad \delta \vdash e_2 \Downarrow \nu}{\delta \vdash \mathit{if}\ e_1\ \mathit{then}\ e_2\ \mathit{else}\ e_3 \Downarrow \nu} \qquad \frac{\delta \vdash e_1 \Downarrow \mathit{false} \qquad \delta \vdash e_3 \Downarrow \nu}{\delta \vdash \mathit{if}\ e_1\ \mathit{then}\ e_2\ \mathit{else}\ e_3 \Downarrow \nu}$$

Die Zweige der Alternative werden bezüglich der gleichen Umgebung ausgewertet wie die Alternative selbst.

Für jedes neu eingeführte Konstrukt gibt es jeweils eine Auswertungsregel.

$$\frac{\delta \vdash e \Downarrow \nu}{\delta \vdash (\mathit{let}\ x = e) \Downarrow \{x \mapsto \nu\}} \qquad \frac{\delta \vdash d_1 \Downarrow \delta_1 \qquad \delta, \delta_1 \vdash d_2 \Downarrow \delta_2}{\delta \vdash d_1\ d_2 \Downarrow \delta_1, \delta_2}$$

$$\frac{}{\delta \vdash x \Downarrow \delta(x)} \qquad \frac{\delta \vdash d \Downarrow \delta' \qquad \delta, \delta' \vdash e \Downarrow \nu}{\delta \vdash (d\ \mathit{in}\ e) \Downarrow \nu}$$

In der Auswertungsregel für Bezeichner ist durch die statische Semantik sichergestellt, dass der Bezeichner x stets definiert ist: $x \in \mathit{dom}\ \delta$. In der Regel für ***in***-Ausdrücke regelt der Kommaoperator analog zur statischen Semantik Überschneidungen.

Für unser laufendes Beispiel erhalten wir

$$\frac{\dfrac{\dfrac{\vdots}{\varnothing \vdash e \Downarrow 4711}}{\varnothing \vdash \mathit{let}\ s = e \Downarrow \{s \mapsto 4711\}} \qquad \dfrac{\dfrac{\{s \mapsto 4711\} \vdash s \Downarrow 4711 \qquad \{s \mapsto 4711\} \vdash s \Downarrow 4711}{\{s \mapsto 4711\} \vdash s * s \Downarrow 22193521}}{\{s \mapsto 4711\} \vdash \mathit{let}\ a = s * s \Downarrow \{a \mapsto 22193521\}}}{\varnothing \vdash \mathit{let}\ s = e\ \mathit{let}\ a = s * s \Downarrow \{s \mapsto 4711, a \mapsto 22193521\}}$$

Die erste Wertedefinition ***let*** $s = e$ resultiert in der Umgebung $\{s \mapsto 4711\}$. Bezüglich dieser Umgebung wird die zweite Wertedefinition ***let*** $a = s * s$ ausgerechnet. Abschließend werden beide Umgebungen mit dem Kommaoperator verknüpft. Fassen wir zusammen:

Dynamische Semantik

Die *dynamische Semantik* ordnet

- einem Ausdruck einen Wert zu, $\delta \vdash e \Downarrow \nu$ und
- einer Definition eine Umgebung, $\delta \vdash d \Downarrow \delta'$.

Die dynamische Semantik legt nur die Bedeutung von Ausdrücken und Definitionen fest, deren freie Bezeichner in der Umgebung aufgeführt werden. Bevor ein Teilausdruck, der freie Bezeichner enthält, ausgewertet wird, wird zunächst die Umgebung um die Werte der freien Bezeichner erweitert. Dies ist die große ***Invariante der dynamischen Semantik***.

Ich habe keinen Namen
Dafür. Gefühl ist alles,
Name Schall und Rauch.
Umnebelnd Himmelsglut.

— Johann Wolfgang von Goethe (1749–1832), *Faust I*

nomen atque omen

— Titus Maccius Plautus (um 254–184 v. Chr.), *Persa*

Vertiefung: Umbenennung Wir haben schon angesprochen, dass Bezeichner frei gewählt werden können: *let* $s = e$ *in* $s * s$ ist gleichwertig zu

let $size = e$ *in* $size * size$ oder *let* $seitenlaenge = e$ *in* $seitenlaenge * seitenlaenge$

Dass Namen Schall und Rauch sind, ist vielleicht klar, wenn wir die obigen Ausdrücke isoliert für sich betrachten. Die Bedeutung der Ausdrücke bleibt aber ebenso unverändert, wenn sie *Teil* eines größeren Programms sind. Zum Beispiel: Der Bezeichner s im rechten *in*-Ausdruck

let $s = 4711$ *in let* $s = 815$ *in* $s * s$

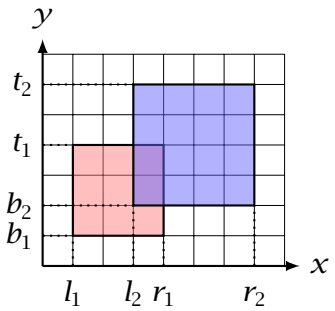
kann zu *size* umbenannt werden,

let $s = 4711$ *in let* $size = 815$ *in* $size * size$

ohne die Bedeutung des Programms zu ändern. Das liegt daran, dass die Auswertungsregeln »neuen« Definitionen Vorrang einräumen. (Ein Gedankenexperiment: Würden wir in der Auswertungsregel für *in*-Ausdrücke die beiden Argumente des Kommaoperators vertauschen, aus $\delta, \delta' \vdash e \Downarrow \nu$ wird $\delta', \delta \vdash e \Downarrow \nu$, dann hätten die beiden Ausdrücke tatsächlich eine unterschiedliche Bedeutung — eine grausame Vorstellung.)

module Values.Area

Vertiefung: Wohnfläche Obwohl unsere Programmiersprache noch vergleichsweise spartanisch ausgestattet ist, können wir mit ihrer Hilfe schon erste kleinere Aufgaben lösen. Schauen wir uns ein — nur auf den ersten Blick einfaches — Beispiel an. Die Fläche einer Wohnung mit dem unten skizzierten Grundriss soll berechnet werden.



let $l_1 = 1$
let $r_1 = 4$
let $b_1 = 1$
let $t_1 = 4$
let $l_2 = 3$
let $r_2 = 7$
let $b_2 = 2$
let $t_2 = 6$

Geometrisch gesehen besteht die zu berechnende Fläche aus zwei sich überlappenden Quadraten. (Das ist aller Wahrscheinlichkeit nach eine Vereinfachung, das Ergebnis des schon angesprochenen Abstraktionsprozesses, mit dem wir Aufgaben in Rechenaufgaben verwandeln.) Wir nehmen weiterhin an, dass die Quadrate durch die eingezeichneten x- und y-Koordinaten gegeben sind (*l*eft, *r*ight, *b*ottom, *t*op).

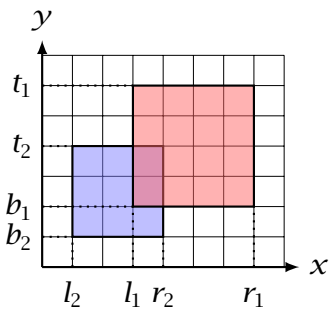
Die Gesamtfläche ergibt sich dann als Summe der beiden Quadratflächen minus der Schnittfläche, die die Form eines Rechtecks hat. Ausgedrückt in Mini–F#:

```
let s1 = r1 - l1
let s2 = r2 - l2
let w = r1 - l2
let h = t1 - b2
s1 * s1 + s2 * s2 - w * h
```

Für die Seitenlänge der Quadrate (*s*ize) führen wir zwei Bezeichner ein, ebenso für die Breite (*w*idth) und Höhe des Rechtecks (*h*eight). Letzteres dient dazu, die Lesbarkeit des Programms zu verbessern; ersteres vermeidet Mehrfachberechnungen: Formuliert man $(r_1 - l_1) * (r_1 - l_1)$ statt $s_1 * s_1$, wird die Teilrechnung $r_1 - l_1$ zweimal durchgeführt. Die vier Bezeichner werden dann in der Flächenformel verwendet. (Allerdings benötigen wir weder b_1 noch t_2. Warum?)

```
>>> ...
>>> s1 * s1 + s2 * s2 - w * h
23
```

Die Wohnfläche beträgt somit $23\,m^2$ — ein kurzer Blick auf den Grundriss bestätigt das Ergebnis. Ändern wir die Daten, indem wir zum Beispiel die Koordinaten der beiden Quadrate »vertauschen«,

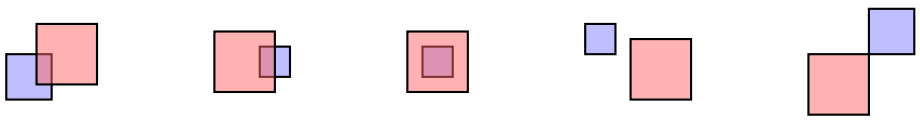



```
let l1 = 3
let r1 = 7
let b1 = 2
let t1 = 6
let l2 = 1
let r2 = 4
let b2 = 1
let t2 = 4
```

erleben wir eine unangenehme Überraschung.

```
>>> ...
>>> s1 * s1 + s2 * s2 - w * h
0
```

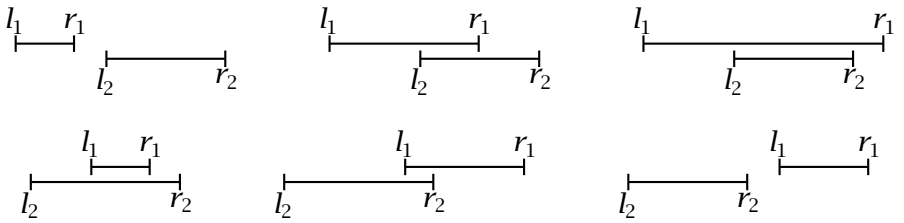
Was läuft schief? Nun, wir haben uns zu sehr von der Skizze des Grundrisses leiten lassen: Unser Programm macht unausgesprochene Annahmen über die relative Lage der beiden Quadrate. (Welche?) Wollen wir das Programm »robuster« machen, müssen wir die Lage der Quadrate berücksichtigen. Das Problem ist nur, dass viele unterschiedliche Konstellationen denkbar sind. Hier ist eine kleine Auswahl:



Wie werden wir Herr oder Frau der Lage?

Die entscheidende Einsicht ist, dass wir Überschneidungen *getrennt* für jede der beiden Koordinatenachsen ausrechnen können und auf diese Weise ein 2-dimensionales Problem auf ein 1-dimensionales Problem zurückführen können. Jedes Quadrat definiert ein Intervall auf der x-Achse, in unserem Fall (l_1, r_1) bzw. (l_2, r_2), und ein Intervall auf der y-Achse, (b_1, t_1) bzw. (b_2, t_2). Die beiden Quadrate überlappen sich genau dann, wenn sich sowohl die beiden x-Intervalle als auch die beiden y-Intervalle überlappen.

Konzentrieren wir uns auf die x-Achse — die folgenden Überlegungen gelten entsprechend für die y-Achse. Wenn wir annehmen, dass $l_1 < r_1$ und $l_2 < r_2$ gilt, dann ergeben sich sechs mögliche Konstellationen:



Die beiden Intervalle haben also einen *leeren* Durchschnitt genau dann, wenn die rechte Grenze des einen vor der linken Grenze des anderen Intervalls liegt: $r_1 < l_2 \;||\; r_2 < l_1$. Umgekehrt liegt eine Überschneidung vor, wenn $r_1 \geqslant l_2 \;\&\&\; r_2 \geqslant l_1$. Hier kommen die Gesetze der Logik und der Arithmetik zum Einsatz: Die eine Formel ergibt sich aus der anderen durch Negation, Anwendung der ***De Morganschen Gesetze***,

$$not\ (a \;\&\&\; b) = not\ a \;||\; not\ b \tag{3.2a}$$
$$not\ (a \;||\; b) = not\ a \;\&\&\; not\ b \tag{3.2b}$$

und der Beziehungen zwischen nicht-strikten und strikten Ordnungen:

$$not\ (a \leqslant b) = a > b \tag{3.3a}$$
$$not\ (a < b) = a \geqslant b \tag{3.3b}$$

Nun sind wir nicht nur an der Frage interessiert, ob es eine Überschneidung gibt, sondern wir benötigen insbesondere die Länge der Überschneidung. Diese ist gegeben durch die Formel $min\ r_1\ r_2 \doteq max\ l_1\ l_2$, wobei $min\ a\ b$ das Minimum von a und b und $max\ a\ b$ entsprechend deren Maximum berechnet. Der Ausdruck $min\ a\ b$ ist eine Abkürzung für die Alternative ***if*** $a \leqslant b$ ***then*** a ***else*** b und $max\ a\ b$ kürzt entsprechend ***if*** $a \leqslant b$ ***then*** b ***else*** a ab. Nach diesen Vorarbeiten ergibt sich das folgende Programm.

```
let s1 = r1 ÷ l1
let s2 = r2 ÷ l2
let w = min r1 r2 ÷ max l1  l2
let h = min t1  t2 ÷ max b1 b2
s1 * s1 + s2 * s2 ÷ w * h
```

Jetzt erhalten wir für beide Datensätze das gleiche Ergebnis: 23.

Wir werden auf das Problem der Berechnung der Wohnfläche zu einem späteren Zeitpunkt noch einmal zurückkommen — wenn wir etwas mehr Vokabular zur Verfügung haben, um die Lösung flexibler und modularer zu gestalten.

Vertiefung: Rechnen mit Programmen Bisher haben wir Auswertungen mit Hilfe von Beweisbäumen illustriert. Die baumartige Darstellung zeigt jeweils sehr schön, wie die einzelnen Auswertungsregeln kombiniert werden. Leider sind Beweisbäume für größere Rechnungen in der Regel zu unhandlich. Kompakter lässt sich eine Rechnung als Folge von Gleichungen notieren. Dabei verwenden wir das folgende Format.

$$
\begin{aligned}
& e_1 \\
= \quad & \{ \text{ Rechtfertigung } \} \\
& e_2
\end{aligned}
$$

Innerhalb der geschweiften Klammern geben wir an, warum die Umformung $e_1 = e_2$ gültig ist. Auf diese Weise wird jeder einzelne Rechenschritt hoffentlich leicht nachvollziehbar.

Die folgende Rechnung illustriert, wie die Wohnfläche bestimmt wird.

$$
\begin{aligned}
& \textit{let } s_1 = r_1 \div l_1 \textit{ let } s_2 = r_2 \div l_2 \textit{ let } w = \mathit{min}\ r_1\ r_2 \div \mathit{max}\ l_1\ l_2 \textit{ let } h = \mathit{min}\ t_1\ t_2 \div \mathit{max}\ b_1\ b_2 \\
& \textit{in } s_1 * s_1 + s_2 * s_2 \div w * h \\
= \quad & \{ \text{ Definition Monus mit } r_1 = 7 \text{ und } l_1 = 3 \} \\
& \textit{let } s_2 = r_2 \div l_2 \textit{ let } w = \mathit{min}\ r_1\ r_2 \div \mathit{max}\ l_1\ l_2 \textit{ let } h = \mathit{min}\ t_1\ t_2 \div \mathit{max}\ b_1\ b_2 \\
& \textit{in } 4 * 4 + s_2 * s_2 \div w * h \\
= \quad & \{ \text{ Definition Monus mit } r_2 = 4 \text{ und } l_2 = 1 \} \\
& \textit{let } w = \mathit{min}\ r_1\ r_2 \div \mathit{max}\ l_1\ l_2 \textit{ let } h = \mathit{min}\ t_1\ t_2 \div \mathit{max}\ b_1\ b_2 \textit{ in } 4 * 4 + 3 * 3 \div w * h \\
= \quad & \{ \text{ Definition } \mathit{min} \text{ und } \mathit{max} \} \\
& \textit{let } w = 4 \div 3 \textit{ let } h = \mathit{min}\ t_1\ t_2 \div \mathit{max}\ b_1\ b_2 \textit{ in } 4 * 4 + 3 * 3 \div w * h \\
= \quad & \{ \text{ Definition Monus } \} \\
& \textit{let } h = \mathit{min}\ t_1\ t_2 \div \mathit{max}\ b_1\ b_2 \textit{ in } 4 * 4 + 3 * 3 \div 1 * h \\
= \quad & \{ \text{ Definition } \mathit{min}, \mathit{max} \text{ und Monus mit } b_1 = 2,\ t_1 = 6,\ b_2 = 1 \text{ und } t_2 = 4 \} \\
& 4 * 4 + 3 * 3 \div 1 * 2 \\
= \quad & \{ \text{ Arithmetik } \} \\
& 23
\end{aligned}
$$

Die Darstellung hat den Vorteil, dass wir den Detaillierungsgrad variieren können: Wichtige Rechnungen können ausführlich dargestellt werden; leichte Routinerechnungen lassen sich abkürzen. In jedem Schritt wird »Gleiches durch Gleiches« ersetzt. Im ersten Schritt rechnen wir $r_1 \div l_1$ aus und setzen das Ergebnis 4 für s_1 im Rumpf des ***in***-Ausdrucks ein. (Zum Vergleich: In einem Auswertungsbaum wird die Einsetzung mit Hilfe von Umgebungen und dem Axiom $\delta \vdash x \Downarrow \delta(x)$ bewerkstelligt.) Der Wert von w wird in zwei Schritten berechnet; die analoge Rechnung für h kürzen wir ab, ebenso die Auswertung des finalen Ausdrucks.

Die Auswertungsrelation $\delta \vdash e \Downarrow \nu$ ordnet einem Ausdruck einen Wert zu. Die Gleichung $e_1 = e_2$ setzt aber zwei Programme zueinander in Beziehung. Plaziert man zwei parallele Linien zwischen zwei mathematische Objekte (siehe Abbildung 2.1), sollte man klären, was eigentlich damit gemeint ist. Hier ist die *semantische* Gleichheit gemeint; $e_1 = e_2$ bedeutet, dass beide Programme zu dem gleichen Wert auswerten: $\delta \vdash e_1 \Downarrow \nu \iff \delta \vdash e_2 \Downarrow \nu$ für alle typkonformen Werte ν und für alle Umgebungen δ. (Alternativ könnte $e_1 = e_2$ bedeuten, dass die Ausdrücke syntaktisch gleich sind — das ist hier aber *nicht* intendiert.)

Insbesondere dürfen die Programme freie Bezeichner enthalten, so dass wir auch über Pro-

grammfragmente argumentieren können, wie oben bereits geschehen:

$$
\begin{aligned}
& \mathit{not}\ (r_1 < l_2\ ||\ r_2 < l_1) \\
= \quad & \{\ \text{De Morgansche Gesetze (3.2b)}\ \} \\
& \mathit{not}\ (r_1 < l_2)\ \&\&\ \mathit{not}\ (r_2 < l_1) \\
= \quad & \{\ \text{nicht-strikte und strikte Ordnungen (3.3b)}\ \} \\
& r_1 \geqslant l_2\ \&\&\ r_2 \geqslant l_1
\end{aligned}
$$

Hier rechnen wir sozusagen *mit* Programmen, das heißt, Programme selbst werden zum Objekt der Umformungen. Das ist angezeigt, wenn wir Programme umschreiben, verbessern, optimieren wollen oder wenn wir Programme systematisch herleiten. Aber wir greifen auf spätere Kapitel vor …

Übungen.

📝 **1.** Geben Sie für jeden der folgenden Ausdrücke an, welche Bezeichner er beinhaltet, und welche der Bezeichner frei bzw. gebunden sind.

- *let* $a = c$ *in if* a *then* b *else* *true*,
- *let* $a = 1$ *in let* $b =$ *true* *in if* b *then* $a + 1$ *else* $c + 1$,
- *let* $a = c$ *in let* $b =$ *true* *in if* b *then* $a + 1$ *else* $d + 1$,
- *let* $a =$ *true* *in if* a *then* 1 *else* 2.

📝 **2.** Werten Sie die folgenden Ausdrücke nacheinander mit dem Mini–F# Interpreter aus:

- *let* $b = 5$ *in let* $a = 4$ *in* $a * b$,
- *let* $d =$ *true* *in let* $b = d$ *in let* $a =$ *false* *in let* $c =$ *true* *in if* b *then* a *else* c,
- *let* $c = 7$ *in let* $b = 5$ *in let* $c = 4$ *in* $b + c$.

Geben Sie für jeden Ausdruck die vollständige Rechnung in Form eines Beweisbaums an.

3.4. Funktionsdefinitionen

Im letzten Abschnitt haben wir mit Hilfe des Programms

let $s = e$ *in* $s * s$

den Flächeninhalt eines Quadrats mit der Seitenlänge e berechnet. Wir können das obige Programm verallgemeinern, indem wir von der gegebenen Seitenlänge e ***abstrahieren***. Aus dem Ausdruck $s * s$ wird eine ***Funktion*** in s.

let $\mathit{area}\ (s : \mathit{Nat}) : \mathit{Nat} = s * s$

Der Bezeichner *area* ist der Name der Funktion, s ist der ***formale Parameter*** und $s * s$ heißt ***Rumpf*** der Funktion. Um jetzt den Flächeninhalt für eine gegebene Seitenlänge e zu berechnen, wenden wir die Funktion auf e an.

$\mathit{area}\ (e)$

Den Ausdruck e nennen wir das Argument oder den ***aktuellen Parameter*** der Funktion.

Ein Funktionsaufruf wie $\mathit{area}\ (e)$ wird ausgerechnet, indem im Rumpf der formale Parameter durch den aktuellen Parameter ersetzt und der resultierende Ausdruck dann ausgewertet wird. Mit anderen Worten, der Funktionsaufruf $\mathit{area}\ (e)$ ist gleichwertig zu dem Ausdruck *let* $s =$

e ***in*** $s * s$, dem Ausgangspunkt unserer Überlegungen. Der Vorteil einer Funktionsdefinition ist, dass die Funktion mehrfach angewendet werden kann.

$$area\ (e_1) + area\ (e_2)$$

Ohne Funktionen im Repertoire müssten wir formulieren

$$(\textbf{\textit{let}}\ s = e_1\ \textbf{\textit{in}}\ s * s) + (\textbf{\textit{let}}\ s = e_2\ \textbf{\textit{in}}\ s * s)$$

Je größer der Funktionsrumpf und je öfter man eine Funktion verwendet, desto größer ist die Ökonomie einer Funktionsdefinition.

Funktionsdefinitionen gehören wie Wertedefinitionen zu den Deklarationen und können wie diese in ***in***-Ausdrücken verwendet werden.

$$\begin{array}{l}\textbf{\textit{let}}\ area\ (s : Nat) : Nat = s * s \\ \textbf{\textit{in}}\ \ area\ (e_1) + area\ (e_2)\end{array}$$

Die Sichtbarkeit des Funktionsbezeichners *area* erstreckt sich auf den Rumpf des ***in***-Ausdrucks; der formale Parameter s ist hingegen *nur* im Funktionsrumpf $s * s$ sichtbar.

Funktionen kennen wir aus der Mathematik; die Funktionsdefinitionen in diesem und in den nächsten drei Kapiteln beschreiben Funktionen im mathematischen Sinne — dies wird sich in den darauffolgenden Kapiteln ändern.[4] Liebgewonnene Funktionen aus Kurvendiskussionen wie $f(x) = 2 \cdot x^2 + x$ lassen sich in unserer Sprache einfach nachprogrammieren.

$$\textbf{\textit{let}}\ f\ (x : Nat) : Nat = 2 * x * x + x$$

Der einzige Unterschied ist, dass unsere Funktionen auf den natürlichen Zahlen arbeiten, und nicht auf den reellen Zahlen. Reelle Zahlen lassen sich auf dem Rechner nur unvollkommen nachbilden; es gibt einfach zu viele davon (siehe Anhang B.2.4). Deshalb beschränken wir uns in der Vorlesung im Wesentlichen auf die natürlichen Zahlen.

Abstrakte Syntax Wir erweitern Deklarationen um Funktionsdefinitionen und Ausdrücke um Funktionsapplikationen (das ist der vornehme Name für Funktionsaufrufe oder Funktionsanwendungen).

$f \in \mathsf{Ident}$

$d ::= \cdots$	***Deklarationen:***
$\mid\ \textbf{\textit{let}}\ f\ (x : t_1) : t_2 = e$	Funktionsdefinition
$e ::= \cdots$	***Funktionsausdrücke:***
$\mid\ f\ (e)$	Funktionsapplikation

Statische Semantik Eine Funktion mit dem Argumenttyp t_1 und dem Ergebnistyp t_2 erhält den Typ $t_1 \to t_2$. *Lies:* t_1 nach t_2. In der Mathematik würde man statt vom Argument- und Ergebnistyp, vom Definitions- und Wertebereich sprechen.

$t ::= \cdots$	***Typen:***
$\mid\ t_1 \to t_2$	Funktionstyp

[4] Eine Ausnahme gibt es auch in diesem Kapitel: Die instrumentierte Version von *player-A* in Abschnitt 3.6 ist keine Funktion im mathematischen Sinne.

Bei der Definition einer Funktion müssen der Argument- und der Ergebnistyp angegeben werden.

$$\frac{\Sigma, \{x_1 \mapsto t_1\} \vdash e_2 : t_2}{\Sigma \vdash (\textbf{\textit{let}}\ f\ (x_1 : t_1) : t_2 = e_2) : \{f \mapsto t_1 \to t_2\}}$$

$$\frac{\Sigma \vdash e_1 : t_1}{\Sigma \vdash f\ (e_1) : t_2} \qquad f \in dom\ \Sigma \text{ und } \Sigma(f) = t_1 \to t_2$$

Der Rumpf einer Funktion wird in der um den formalen Parameter erweiterten Signatur getypt (»,« ist der Kommaoperator). Bei der Funktionsanwendung schlagen wir den Typ der Funktion in der Signatur nach und stellen dann sicher, dass der aktuelle Parameter den gleichen Typ hat wie der formale. Der Typ der Funktionsanwendung entspricht dem Ergebnistyp der Funktion.

Dynamische Semantik Was ist der Wert einer Funktion? Können wir Funktionen überhaupt auswerten? Die Antwort ist vielleicht überraschend: Da wir die Bindung des formalen Parameters bei der Definition nicht kennen, ist es nicht möglich, eine Funktion auszurechnen; allerdings ist dies auch nicht notwendig. Wir verzögern die Auswertung einfach, bis wir den aktuellen Parameter kennen. Mit anderen Worten, eine Funktion wertet im Wesentlichen zu sich selbst aus.

»Im Wesentlichen«, weil wir noch berücksichtigen müssen, dass der Rumpf einer Funktionsdefinition möglicherweise freie Bezeichner enthält, deren Werte in der Umgebung protokolliert sind. Das folgende Beispiel zeigt das Problem auf.

$$\frac{\dfrac{\overline{\varnothing \vdash 2 \Downarrow 2}}{\varnothing \vdash \textbf{\textit{let}}\ d = 2 \Downarrow \{d \mapsto 2\}} \qquad \overline{\{d \mapsto 2\} \vdash \textbf{\textit{let}}\ next\ (n) = n + d \Downarrow \{next \mapsto ?\}}}{\varnothing \vdash \textbf{\textit{let}}\ d = 2\ \textbf{\textit{let}}\ next\ (n) = n + d \Downarrow \{d \mapsto 2, next \mapsto ?\}}$$

Wenn wir die Auswertung der Funktion *next* »einfrieren«, um sie zu einem späteren Zeitpunkt fortzusetzen (»aufzutauen«), müssen wir uns nicht nur die Funktionsdefinition selbst, sondern auch die aktuelle Umgebung $\{d \mapsto 2\}$ merken.

Die Kombination aus Umgebung und Funktionsdefinition heißt ***Funktionsabschluss*** (engl. function closure). Der Bereich der Werte wird um Funktionsabschlüsse erweitert.

$\nu ::= \cdots$	***Werte:***
$\mid \langle \delta, x, e \rangle$	Funktionsabschluss

Ein Funktionsabschluss besteht aus einer Umgebung, dem formalen Parameter und dem Rumpf der definierten Funktion. Mit der Einführung von Funktionsabschlüssen hängt der Bereich der Werte somit vom Bereich der Ausdrücke ab!

Damit können wir das obige Beispiel vervollständigen:

$$\frac{\dfrac{\overline{\varnothing \vdash 2 \Downarrow 2}}{\varnothing \vdash \textbf{\textit{let}}\ d = 2 \Downarrow \{d \mapsto 2\}} \qquad \overline{\{d \mapsto 2\} \vdash \textbf{\textit{let}}\ next\ (n) = n + d \Downarrow \{next \mapsto \gamma\}}}{\varnothing \vdash \textbf{\textit{let}}\ d = 2\ \textbf{\textit{let}}\ next\ (n) = n + d \Downarrow \{d \mapsto 2, next \mapsto \gamma\}}$$

wobei $\gamma = \langle \{d \mapsto 2\}, n, n + d \rangle$

Der Funktionsabschluss repräsentiert eine Funktion, die ihr Argument um 2 erhöht.

Eine Funktionsdefinition wertet somit zu einer Bindung aus, in der der Funktionsname an einen Funktionsabschluss gebunden ist.

$$\overline{\delta \vdash (\textbf{\textit{let}}\ f\ (x) = e) \Downarrow \{f \mapsto \langle \delta, x, e \rangle\}}$$

$$\frac{\delta \vdash e_1 \Downarrow v_1 \qquad \delta', \{x_1 \mapsto v_1\} \vdash e \Downarrow v}{\delta \vdash f\ (e_1) \Downarrow v} \qquad \delta(f) = \langle \delta', x_1, e \rangle$$

Wenn eine Funktion aufgerufen wird, haben wir alles beisammen, um die verzögerte Berechnung fortzusetzen: den formalen Parameter x_1, den aktuellen Parameter e_1 und den Funktionsrumpf e. Der Funktionsaufruf $f\ (e_1)$ mit $f\ (x_1) = e$ ist gleichwertig zu ***let*** $x_1 = e_1$ ***in*** e und wird entsprechend ausgewertet. (Die statische Semantik stellt bereits sicher, dass $f \in \mathit{dom}\ \delta$.)

Das folgende Beispiel illustriert die einzelnen Auswertungsschritte.

$$\frac{\dfrac{}{\varnothing \vdash \textbf{\textit{let}}\ \mathit{area}\ (s) = s * s \Downarrow \delta} \qquad \dfrac{\dfrac{}{\delta \vdash 4711 + 815 \Downarrow 5526} \quad \dfrac{}{\{s \mapsto 5526\} \vdash s * s \Downarrow 30536676}}{\delta \vdash \mathit{area}\ (4711 + 815) \Downarrow 30536676}}{\varnothing \vdash \textbf{\textit{let}}\ \mathit{area}\ (s) = s * s\ \textbf{\textit{in}}\ \mathit{area}\ (4711 + 815) \Downarrow 30536676}$$

wobei $\delta = \{\mathit{area} \mapsto \langle \varnothing, s, s * s \rangle\}$

Der Bezeichner *area* wird an den Funktionsabschluss $\langle \varnothing, s, s * s \rangle$ gebunden. Der Abschluss repräsentiert eine Funktion, die jeder natürlichen Zahl ihren Quadratwert zuordnet.

Auf die Funktion *area* werden wir im Folgenden des Öfteren zurückgreifen. Deswegen benennen wir sie in *square* um — *area* ist mehrdeutig und könnte auch den Flächeninhalt eines Kreises berechnen.

let *square* $(n : \mathit{Nat}) : \mathit{Nat} = n * n$

Vertiefung: Neunerprobe Programmieren ist ein kreativer Prozess, wie das Schreiben von Texten oder das Komponieren von Musikstücken. Man konzipiert, man skizziert, man schreibt, man verwirft, man schreibt um, man redigiert, man verzweifelt, man triumphiert, man feilt und man poliert. Zwei wichtige Instrumente, die uns bei diesem Prozess unterstützen, haben wir soeben kennengelernt: Funktionsdefinitionen und Funktionsapplikationen. Mit Hilfe von Funktionsdefinitionen vergrößern wir unser Vokabular, unseren Wortschatz, mit dem wir Probleme und deren Lösungen beschreiben und so einer rechnerischen Lösung zuführen. Mit Hilfe von Funktionsapplikationen komponieren wir die eingeführten Vokabeln und setzen sie zu größeren Einheiten zusammen. Aus Wörtern werden Sätze, aus Sätzen Kapitel und aus Kapiteln Romane — Algorithmen, Programmbibliotheken und Softwaresysteme.

Aber fangen wir klein an und versetzen uns für erste Fingerübungen in die Zeit, als man noch von Hand rechnete. Sind die Zahlen groß und die Rechnungen lang, so schleichen sich gerne Fehler ein. Um die Gewissheit zu erhöhen, dass man eine Rechnung fehlerfrei zu Ende geführt hat, kann man die sogenannte ***Neunerprobe*** machen: Dabei werden die gleichen Rechenschritte durchgeführt, aber mit Ziffern statt mit Zahlen: An die Stelle der Zahlen treten ihre ***Neunerreste***. Die Rechnung $815 + 4711$ wird zum Beispiel durch $5 + 4$ kontrolliert. Um die Neunerreste zu bestimmen, bildet man die ***Quersummen***, gegebenenfalls mehrfach, bis man eine Ziffer erhält: $8 + 1 + 5 = 14$, $1 + 4 = 5$ und $4 + 7 + 1 + 1 = 13$, $1 + 3 = 4$. Wenn die Neunerreste der Rechnung und der Kontrollrechnung identisch sind, hat man *wahrscheinlich* fehlerfrei gerechnet; sind sie aber unterschiedlich, so *muss* sich ein Fehler eingeschlichen haben. Im obigen Beispiel erhalten wir $815 + 4711 = 5526$ mit $5 + 5 + 2 + 6 = 18$, $1 + 8 = 9$, kontrolliert und für gut befunden durch $5 + 4 = 9$. Rechnen wir $4711 \cdot 4711 = 22183521$ mit $2 + 2 + 1 + 8 + 3 + 5 + 2 + 1 = 24$, so schlägt die Kontrollrechnung Alarm: $5 \cdot 5 = 25$. (Anhang B.5.5 beleuchtet den mathematischen Hintergrund der Neunerprobe.)

Wie können wir die Schritte zur Bestimmung des Neunerrests mit Rechenregeln nachbilden (*ohne* die Abkürzung $n \,\%\, 9$ zu nehmen)? Die folgende Funktion bestimmt die Quersumme einer vierziffrigen Zahl — wir fangen, wie gesagt, klein an.

```
let digit-sum (n : Nat) : Nat =                    // Quersumme einer vierziffrigen Zahl
  (n ÷ 1) % 10 + (n ÷ 10) % 10 + (n ÷ 100) % 10 + (n ÷ 1000) % 10
```

Um die Dezimalziffern zu extrahieren, dividieren wir durch aufeinanderfolgende Zehnerpotenzen und bestimmen jeweils den Zehnerrest. (Überlegen Sie schon einmal, wie man die Quersumme einer *beliebig* großen Zahl bestimmt.)

```
⋙ digit-sum 4711
13
⋙ digit-sum 13
4
```

Bei der Berechnung des Divisionsrests nutzt man aus, dass der Neunerrest einer Zahl mit dem Neunerrest ihrer Quersumme übereinstimmt. Bildet man die Quersumme der Quersumme der Quersumme, so erhält man eine einziffrige Zahl, deren Neunerrest sich mittels einer einfachen Fallunterscheidung bestimmen lässt.

```
let mod9 (n : Nat) : Nat =                         // Neunerrest einer vierziffrigen Zahl
  let s = digit-sum (digit-sum (digit-sum n))
  if s = 9 then 0 else s
```

Die kleinste Zahl, für die drei Schritte zwingend notwendig sind, ist 199 mit $1 + 9 + 9 = 19$, $1 + 9 = 10$ und $1 + 0 = 1$. Für viele Zahlen genügen bereits zwei Schritte oder gar ein einziger. Aber, drei Iterationen schaden nicht: Wendet man *digit-sum* auf einen Neunerrest an, so erhält man diesen als Ergebnis zurück: *digit-sum* $n = n$ für $n < 9$; man sagt auch, n mit $n < 9$ ist ein ***Fixpunkt*** der Funktion *digit-sum*.

Berechnet man Neunerreste von Hand, so überspringt man Neunerziffern einfach: Der Neunerrest von 9719 ist $7 + 1 = 8$ (engl. casting out nines). Diese clevere Vereinfachung können wir nachbilden, indem wir eine »ignorierende« Variante der Addition definieren,

```
let add (a : Nat, b : Nat) : Nat =
  if b = 9 then a else a + b
```

und diese in *digit-sum* verwenden:

```
let digit-sum (n : Nat) : Nat =                    // Quersumme einer vierziffrigen Zahl
  add (add (add (add (0, (n ÷ 1) % 10), (n ÷ 10) % 10), (n ÷ 100) % 10), (n ÷ 1000) % 10)
```

Die Addition ist eine binäre Operation, sie hängt von *zwei* Argumenten ab. Wir erweitern entsprechend Funktionendefinitionen und Funktionsapplikationen auf mehrparametrige Funktionen. Die Formalisierung dieser Erweiterung holen wir in Abschnitt 4.1.1 nach.

Vertiefung: IBAN Das Konzept der ***Prüfsumme*** hört sich nach einem Relikt aus längst vergangenen Zeiten an. Tatsächlich aber sind Prüfsummen aus der Informatik nicht wegzudenken; sie werden überall dort verwendet, wo Übertragungen von Daten möglicherweise fehlerbehaftet sind, etwa wenn Daten über Kupfer- oder Glasfaserkabel gesendet werden oder wenn Daten manuell von einem Blatt Papier in die Eingabemaske eines Programms übertragen werden. Ein selbstvalidierendes Datum, das Sie wahrscheinlich schon häufiger verwendet haben, ist die Internationale Bankkontonummer, kurz IBAN (engl. *I*nternational *B*ank *A*ccount *N*umber). Diese »Nummer« identifiziert auf eindeutige Weise Bankkonten, nicht nur in Deutschland, sondern weltweit. Die IBAN setzt sich aus drei Komponenten zusammen: der Länderkennung, einer zweistelligen Prüfsumme und der sogenannten BBAN (engl. *B*asic *B*ank *A*ccount *N*umber), der länderspezifischen Kontonummer, zum Beispiel `DE72700700100700038301` mit der Länderkennung `DE` für

Deutschland und der Prüfsumme 72. Der Trick: Nicht alle Zeichenfolgen sind gültige IBANs; die Prüfsumme ermöglicht es, ungültige Eingaben zu erkennen, etwa wenn man sich an einer Stelle vertippt hat, und verhindert so Fehlüberweisungen.

Für die Validierung werden zunächst die Buchstaben der Länderkennung in Zahlen umgewandelt: Aus `A` wird 10, aus `B` wird 11 usw. Buchstaben und andere Zeichen werden in Mini–F# durch Elemente des Typs *Char* repräsentiert; Zeichen werden dabei in einfache Anführungsstriche gesetzt, um so die Zahl 3 von dem Zeichen `'3'` unterscheiden zu können: also $3 : Nat$, aber `'3'` : *Char*.

```
let ord (c : Char) : Nat =
  10 + Nat.ord c – Nat.ord 'A'
```

Mini–F# verfügt bereits über eine vordefinierte Funktion, die ein einzelnes Zeichen in eine natürliche Zahl überführt, der Position des Zeichens in dem Zeichensatz (die vordefinierte Bibliotheksfunktion erkennt man an dem zusammengesetzen Namen: *Nat.ord*).

```
>>> Nat.ord 'A'
65
>>> ord 'A'
10
```

Aus historischen Gründen steht der Buchstabe `'A'` an der 65. Stelle des Alphabets. Unsere Funktion rechnet diese Position in das gewünschte Ergebnis um.

Mit Hilfe von *ord* wird die IBAN in eine natürliche Zahl umgewandelt; die Länderkennung und die Prüfsumme wandern dabei an das »Ende« der Zahl. (Auch die BBAN darf übrigens Buchstaben enthalten, aber das ignorieren wir an dieser Stelle.)

```
let valid (d : Char, e : Char, pp : Nat, bban : Nat) : Bool =          // Validierung einer IBAN
  let n = bban * 1000000 + ord d * 10000 + ord e * 100 + pp
  n % 97 = 1
```

Durch geeignete Multiplikationen mit Zehnerpotenzen werden die verschiedenen Bestandteile »aneinandergehängt«. Eine IBAN ist gültig, wenn sich bei der Division durch 97 ein Rest von 1 ergibt.

```
>>> valid ('D', 'E', 72, 700700100700038301)
true
>>> valid ('D', 'E', 72, 700700100700038307)
false
>>> valid ('D', 'E', 72, 700700100700038107)
true
```

Man sieht, dass die Prüfsumme eine gewisse, aber natürlich (?) keine absolute Sicherheit bietet. Vertippt man sich beim letzten Zeichen — aus der 1 wird eine 7 — schlägt die Validierung fehl. Zwei Tippfehler aber werden nicht erkannt. Wie bei unserem ersten Beispiel, den Kontrollrechnungen, muss man die Ergebnisse zu interpretieren wissen: Schlägt die Validierung fehl, so ist die Eingabe fehlerhaft; ist die Validierung erfolgreich, dann ist die Eingabe *wahrscheinlich*, aber eben nicht hundertprozentig korrekt.

Vertiefung: Abkürzungen versus Funktionsdefinitionen In Abschnitt 3.2 haben wir gezeigt, wie sich Boolesche Verknüpfungen mit Hilfe von Fallunterscheidungen programmieren lassen. Es ist verlockend, die dort eingeführten Abkürzungen *not e*, e_1 && e_2 und e_1 || e_2 (Konstrukte der

Metasprache) durch ordentliche Funktionsdefinitionen (Konstrukte der Objektsprache Mini–F#) zu ersetzen.

let *not* $(a : \mathit{Bool}) : \mathit{Bool} =$ ***if*** *a* ***then*** *false* ***else*** *true*

Formal gesehen tritt an die Stelle der Metavariablen e — in Abschnitt 3.2 haben wir den Ausdruck ***if*** *e* ***then*** *false* ***else*** *true* für die Berechnung der Negation eingeführt — der Bezeichner *a* der Programmiersprache — ***if*** *a* ***then*** *false* ***else*** *true* im Rumpf der Funktion.

let *and-also* $(a : \mathit{Bool}, b : \mathit{Bool}) : \mathit{Bool} =$ ***if*** *a* ***then*** *b* ***else*** *false*
let *or-else* $(a : \mathit{Bool}, b : \mathit{Bool}) : \mathit{Bool} =$ ***if*** *a* ***then*** *true* ***else*** *b*

Sind die programmierten Funktionen ein gleichwertiger Ersatz für die liebgewonnenen Abkürzungen? Im Fall der Negation ja; bei den binären Operationen ergeben sich Unterschiede. Zunächst einmal syntaktische. Wenn wir mehr als eine Bedingung konjunktiv verknüpfen, müssen wir die Aufrufe von *and-also* entsprechend schachteln:

and-also $(e_1,$ *and-also* $(e_2, e_3))$

oder alternativ

and-also $($*and-also* $(e_1, e_2), e_3)$

Beide Ausdrücke haben stets das gleiche Ergebnis: Die Konjunktion ist ***assoziativ***. Assoziative Funktionen notiert man vorteilhafter ***infix***: Der Funktionsname kommt zwischen die Argumente.

e_1 && e_2 && e_3

Neben diesem syntaktischen Unterschied gibt es noch einen gewichtigeren semantischen Unterschied zwischen && und *and-also*. Damit beschäftigt sich Aufgabe 3.4.3. Wir greifen die Diskussion auch im nächsten Abschnitt noch einmal auf.

Übungen.

Die Tastatur »⌨« kennzeichnet Programmieraufgaben (»get your hands dirty«).

⌨ **1.** Die Vergleichsoperationen (<, ⩽, =, <>, ⩾, >) arbeiten auf den natürlichen Zahlen. Übertragen Sie die Operationen auf Boolesche Werte unter der Prämisse, dass *false* < *true*. Für die Operation »⩽« definieren Sie zum Beispiel eine Funktion

let *leq* $(a : \mathit{Bool}, b : \mathit{Bool}) : \mathit{Bool}$

die die folgende Wahrheitstabelle implementiert:

		b	
	$a \leqslant b$	*false*	*true*
a	*false*	*true*	*true*
	true	*false*	*true*

Zu welchen Booleschen Verknüpfungen korrespondieren die Vergleichsoperationen?

⌨ **2.** Definieren Sie eine Funktion

let *total-area* $(l_1, r_1, b_1, t_1, l_2, r_2, b_2, t_2) : \mathit{Nat}$

die die Gesamtfläche einer aus zwei *Rechtecken* bestehenden Fläche berechnet — wie im Beispiel aus Abschnitt 3.3 können sich die Flächen überlappen. Verallgemeinern Sie die Funktion auf *drei* sich möglicherweise überlappende Rechtecke.

📝 **3.** Wir haben e_1 && e_2 als Abkürzung für ***if*** e_1 ***then*** e_2 ***else*** *false* eingeführt. Was ist der Unterschied zwischen e_1 && e_2 und dem Funktionsaufruf *and-also* (e_1, e_2)? *Hinweis:* Bestimmen Sie die Semantik beider Ausdrücke für $e_1 =$ *false* und $e_2 = 1 \div 0$.

3.5. Funktionsausdrücke

Für die Auswertung von Funktionen haben wir Funktionsabschlüsse eingeführt. Ein Funktionsabschluss repräsentiert im Prinzip eine anonyme Funktion. Es bietet sich an, anonyme Funktionen dem/der Programmierer/-in auch explizit zur Verfügung zu stellen: ***fun*** $n \to 2 * n + 1$ bezeichnet solch eine namenslose Funktion; sie ordnet dem Argument n den Funktionswert $2 * n + 1$ zu. Wir werden im Laufe der Vorlesung sehen, dass anonyme Funktionen sehr bequem sind — sie befreien uns von der Last, sich für jede Funktion einen Namen überlegen zu müssen.

Im gleichen Atemzug verallgemeinern wir die Syntax für die Funktionsanwendung. Da Funktionen normale Werte sind, können sie auch durch einen Ausdruck berechnet werden: Aus $f\ (e_1)$ wird $e_2\ (e_1)$, an Stelle des Funktionsbezeichners f tritt ein vollwertiger Ausdruck e_2.

Binder

Der Ausdruck ***fun*** $x \to e$ führt den Bezeichner x ein — man sagt auch, x wird gebunden — seine Sichtbarkeit ist auf e beschränkt. Binder kennen wir aus der Mathematik:

$$f(x) = x^2 \qquad \int x^3 \,\mathrm{d}x$$

$$\sum_{x=1}^{n} x^4 \qquad \exists\, x \,.\, 5 \cdot x \geqslant x^5$$

Jedes der Konstrukte bindet die Variable x: Einmal dient sie als Parameter, einmal als Integrationsvariable bzw. als Summationsvariable und einmal als Unbekannte.

Abstrakte Syntax Wir erweitern die abstrakte Syntax um die folgenden Konstrukte:

$e ::= \cdots$	***Funktionsausdrücke:***
$\mid$ ***fun*** $(x : t) \to e$	Funktionsabstraktion
$\mid\ e\ e_1$	Funktionsapplikation

Der Ausdruck ***fun*** $(x : t) \to e$ heißt anonyme Funktion (oder λ-Ausdruck), da er eine Funktion bezeichnet, diese aber keinen Namen hat. Der formale Parameter der Funktion ist x, der Pfeil »→« trennt den formalen Parameter vom Funktionsrumpf e, der durch einen Ausdruck gegeben ist. Beachte, dass wir die Funktionsanwendung nunmehr ohne Klammern schreiben: $e\ e_1$. *Lies:* e von e_1 *oder* e angewendet auf e_1. (Klammern sind ein Hilfsmittel der konkreten Syntax.)

Statische Semantik Die Funktionsabstraktion führt ein Element vom Typ $t_1 \to t_2$ ein; die Funktionsapplikation eliminiert ein Element dieses Typs.

$$\frac{\Sigma, \{x_1 \mapsto t_1\} \vdash e : t_2}{\Sigma \vdash (\textbf{\textit{fun}}\ (x_1 : t_1) \to e) : t_1 \to t_2} \qquad \frac{\Sigma \vdash e : t_1 \to t_2 \qquad \Sigma \vdash e_1 : t_1}{\Sigma \vdash e\ e_1 : t_2} \tag{3.4}$$

Wenn der Typ des formalen Parameters x_1 aus dem Kontext abgeleitet werden kann — etwa weil x_1 als Argument einer arithmetischen Operation verwendet wird — lassen wir die Typangabe oft weg und schreiben kurz ***fun*** $x \to e$.

Dynamische Semantik Eine anonyme Funktion wertet zu einem Funktionsabschluss aus.

$$\frac{}{\delta \vdash (\textbf{\textit{fun}}\ x \to e) \ \Downarrow\ \langle \delta, x, e \rangle}$$

Die Auswertung der Funktionsapplikation $e\ e_1$ ist jetzt etwas umfangreicher, da zusätzlich die Funktion e ausgerechnet werden muss — vorher stand an dieser Stelle ein Bezeichner, den wir nur in der Umgebung nachschlagen mussten.

$$\frac{\delta \vdash e \ \Downarrow\ \langle \delta', x_1, e' \rangle \qquad \delta \vdash e_1 \ \Downarrow\ v_1 \qquad \delta', \{x_1 \mapsto v_1\} \vdash e' \ \Downarrow\ v'}{\delta \vdash e\ e_1 \ \Downarrow\ v'} \tag{3.5}$$

Die Auswertung vollzieht sich in drei Schritten:

(1) Die Funktion e wird ausgerechnet; das Ergebnis ist ein Funktionsabschluss.

(2) Das Argument e_1 wird ausgerechnet; das Ergebnis ist ein Wert.

(3) Der Funktionsrumpf e' wird in der Umgebung $\delta', \{x_1 \mapsto \nu_1\}$ ausgerechnet. Die in dem Funktionsabschluss abgelegte Umgebung wird um die Parameterbindung erweitert: Dem formalen Parameter x_1 wird der *Wert* ν_1 des aktuellen Parameters zugeordnet. Das Ergebnis dieser Rechnung ν' ist der Wert des Funktionsaufrufs $e\ e_1$.

Wir sehen, die Anwendung einer Funktion auf ein Argument ist aufwändig. Zwei Punkte verdienen besondere Beachtung.

Zunächst ist es wichtig festzuhalten, dass der Parameter einer Funktion immer ausgerechnet wird. Da an die Funktion der *Wert* des Parameters übergeben wird, spricht man im Englischen auch von »***call by value***«. Welche alternativen Parameterübergabemechanismen sind denkbar? Wir könnten alternativ den aktuellen Parameter unausgewertet, das heißt den Ausdruck selbst, an den formalen Parameter binden. Warum wäre das eine sinnvolle Alternative? Nun, die Funktion benötigt das Argument vielleicht nicht immer. Wir würden das Argument erst ausrechnen, wenn es im Rumpf der Funktion tatsächlich benötigt wird. Man spricht auch von bedarfsgetriebener Auswertung oder etwas plakativer von »fauler« Auswertung (engl. call by need oder lazy evaluation). Wir haben im letzten Abschnitt die Unterschiede zwischen e_1 && e_2 und *and-also* (e_1, e_2) diskutiert. Schauen wir uns ein konkretes Beispiel an:

$$(b > 0)\ \&\&\ (a \div b \geqslant 10) \quad \text{versus} \quad \textit{and-also}\ (b > 0, a \div b \geqslant 10)$$

In der Umgebung $\{a \mapsto 99, b \mapsto 0\}$ wertet der linke Ausdruck zu *false* aus; der rechte Ausdruck hingegen ist undefiniert: Da Parameter call-by-value übergeben werden, wird der Wert sowohl von $b > 0$ als auch von $a \div b \geqslant 10$ benötigt — die dynamische Semantik ordnet letzterem aber keinen Wert zu. Mit anderen Worten: Im Falle der Funktion *and-also* würden wir von einer »faulen« Auswertung profitieren. Das ist auch der Grund, warum Disjunktion und Konjunktion *Abkürzungen* für ***if***-Ausdrücke sind und *keine vordefinierten Bibliotheksfunktionen*.

Der zweite Punkt, der Beachtung verdient, betrifft den Geltungsbereich von Bezeichnern. Die Auswertungsregel (3.5) involviert zwei verschiedene Umgebungen: δ, die aktuelle Umgebung, bezüglich der die *Anwendung* der Funktion ausgerechnet wird, und δ', die Umgebung, die bei der *Definition* der Funktion aktuell war und die im Funktionsabschluss abgelegt wurde. Der Funktionsrumpf wird bezüglich der erweiterten Umgebung $\delta', \{x_1 \mapsto \nu_1\}$ abgearbeitet, *nicht* $\delta, \{x_1 \mapsto \nu_1\}$. Der Unterschied ist bedeutsam, wenn der Rumpf der Funktion freie Bezeichner enthält. Greifen wir noch einmal ein Beispiel aus Abschnitt 3.4 auf.

```
let d = 2
let next (n) = n + d
…
… let d = 4711 in next (1) …
… let d = 0815 in next (1) …
```

Der Bezeichner d wird insgesamt dreimal definiert: einmal vor der Definition von *next* und zweimal vor der Anwendung von *next*. Welcher Wert von d ist im Rumpf gemeint? Darauf gibt die Semantik eine präzise Antwort. Es ist der Wert, der *statisch* bei der Definition von *next* an d gebunden ist, also 2. Würden wir in der Auswertungsregel die dritte Voraussetzung durch $\delta, \{x_1 \mapsto \nu_1\} \vdash e' \Downarrow \nu'$ ersetzen (in diesem Fall müssen wir in Funktionsabschlüssen die Bindung nicht mehr mitführen), dann wäre d jeweils der Wert, der *dynamisch* beim jeweiligen Aufruf an d gebunden ist, also 4711 bzw. 0815. Man sieht, ein Apostroph macht einen großen Unterschied! Im ersten

Fall spricht man übrigens von statischer Bindung (engl. static binding), im zweiten Fall von dynamischer Bindung (engl. dynamic binding). Mini–F# verwendet statische Bindung und das aus einem guten Grund: Programme sind einfacher zu lesen und zu verstehen. Wird zum Beispiel eine Funktion mit den gleichen Argumenten aufgerufen, so erhält man den gleichen Wert — mit dynamischer Bindung gilt das nicht, siehe obiges Beispiel. Allgemein sind statische Eigenschaften ungleich einfacher zu verstehen, zu vermitteln und zu verifizieren als dynamische Eigenschaften. Für erstere genügt ein Blick in den Programmtext; für letztere muss man alle möglichen Rechnungen betrachten, alle Verläufe, die ein Programm nehmen kann — das sind, wie wir später sehen werden, in der Regel unendlich viele.

> *My second remark is that our intellectual powers are rather geared to master static relations and that our powers to visualize processes evolving in time are relatively poorly developed. For that reason we should do (as wise programmers aware of our limitations) our utmost to shorten the conceptual gap between the static program and the dynamic process, to make the correspondence between the program (spread out in text space) and the process (spread out in time) as trivial as possible.*
>
> — Edsger W. Dijkstra (1930–2002), *Go To Statement Considered Harmful*

Vertiefung: Funktionsabstraktionen versus Funktionsdefinitionen Mit der Einführung von Funktionsabstraktionen benötigen wir Funktionsdefinitionen streng genommen nicht mehr. Die Funktionsdeklaration

$$\textbf{\textit{let}}\ not\ (a : Bool) : Bool = \textbf{\textit{if}}\ a\ \textbf{\textit{then}}\ false\ \textbf{\textit{else}}\ true$$

entspricht exakt der folgenden Wertedeklaration.

$$\textbf{\textit{let}}\ not = \textbf{\textit{fun}}\ (a : Bool) \to \textbf{\textit{if}}\ a\ \textbf{\textit{then}}\ false\ \textbf{\textit{else}}\ true$$

Funktionen sind Werte!

Umgekehrt entspricht die Funktionsabstraktion

$$\textbf{\textit{fun}}\ (x_1 : t_1) \to e$$

exakt dem ***in***-Ausdruck

$$\textbf{\textit{let}}\ f\ (x_1 : t_1) : t_2 = e\ \textbf{\textit{in}}\ f$$

Beide Konstrukte sind also austauschbar. Für welches Konstrukt man sich bei der Programmierung entscheidet, ist daher eine Frage des guten Geschmacks, über den sich ja bekanntlich nicht streiten lässt.

Vertiefung: HOFs Funktionsabstraktionen können auch geschachtelt oder ***gestaffelt*** werden.

$$\textbf{\textit{let}}\ add = \textbf{\textit{fun}}\ (m : Nat) \to \textbf{\textit{fun}}\ (n : Nat) \to m + n$$

Die Funktion *add* hat den merkwürdigen Typ $Nat \to (Nat \to Nat)$. Sie bildet eine natürliche Zahl vom Typ Nat auf eine Funktion vom Typ $Nat \to Nat$ ab. Wenden wir *add* an, müssen entsprechend die Funktionsaufrufe gestaffelt werden: $(add\ 815)\ 4711$. Der Teilausdruck $add\ 815$ berechnet eine Funktion, die dann auf 4711 angewendet wird. In der konkreten Syntax erlauben wir, die Klammern auszulassen und $(add\ 815)\ 4711$ bzw. allgemein $(e\ e_1)\ e_2$ kurz als $add\ 815\ 4711$ bzw. $e\ e_1\ e_2$ aufzuschreiben. Naiv lässt sich eine solche Abfolge lesen als Anwendung der Funktion e auf die zwei Parameter e_1 und e_2. In Wirklichkeit handelt es sich, wie gesagt, um eine

gestaffelte Funktionsanwendung: e wertet zu einer Funktion aus, diese wird auf e_1 angewendet, die Anwendung resultiert wiederum in einer Funktion, die ihrerseits auf e_2 angewendet wird.

Noch eine Bemerkung zur konkreten Syntax: so wie wir $(e\ e_1)\ e_2$ zu $e\ e_1\ e_2$ abkürzen, so erlauben wir auch den Typ $t_1 \to (t_2 \to t_3)$ kurz als $t_1 \to t_2 \to t_3$ aufzuschreiben. *Beachte:* Die Funktionsanwendung ist *nicht* assoziativ: $e\ (e_1\ e_2)$ ist völlig verschieden von $(e\ e_1)\ e_2$; ebenso ist $(t_1 \to t_2) \to t_3$ ein völlig anderer Typ als $t_1 \to (t_2 \to t_3)$, siehe auch Aufgabe 3.5.2.

Eine gestaffelte Funktion vom Typ $Nat \to (Nat \to Nat)$ ist im Vergleich zu einer mehrparametrigen Funktion vom Typ $Nat * Nat \to Nat$ flexibler (den »Paartyp« $t_1 * t_2$ führen wir im nächsten Kapitel ein). Sie kann zunächst nur mit einem Parameter versorgt werden: *add* 815 ist ein gültiger Ausdruck, der überall dort verwendet werden kann, wo eine Funktion des Typs $Nat \to Nat$ verlangt wird. Im Gegensatz dazu muss eine mehrparametrige Funktion stets mit allen Parametern aufgerufen werden.

Eine Funktion, die eine Funktion als Argument erwartet oder — wie *add* — als Ergebnis zurückgibt, heißt ***Funktion höherer Ordnung*** oder kurz ***HOF*** (engl. *h*igher-*o*rder *f*unction). Im Laufe der Vorlesung werden uns einige dieser Exemplare über den Weg laufen, die ersten begegnen uns im nächsten Paragraphen — wir werden sehen: Auch mit Funktionen lässt sich trefflich rechnen.

HOFs in Mathe

Erinnern Sie sich an die Summenregel der Differentialrechnung?

$$(f + g)' = f' + g'$$

Merkwürdig: »+« summiert zwei Funktionen. Tatsächlich meint »+« die Funktion *sum*, eine HOF.

$$\textit{let}\ sum\ (f, g) = \textit{fun}\ x \to f\ x + g\ x$$

Das Pluszeichen steht in der Mathematik für verschiedene, wenn auch verwandte Operationen, es ist ***überladen***.

module Projects.Rastergraphics

Vertiefung: Rastergrafik Unternehmen wir einen kurzen Ausflug in das letzte Jahrhundert, genauer in die neunziger Jahre des letzten Jahrhunderts.

```
Kommen Sie näher! Wenn Sie den Text, den Sie gerade lesen, aus der Nä-
he betrachten, werden Sie vielleicht feststellen, dass die Buchstaben
aus einzelnen Quadraten zusammengesetzt sind, arrangiert auf einem 8x8
Raster. So oder so ähnlich sah die Computerschrift aus, als die Rech-
ner das Heim eroberten. Die sogenannten Heimcomputer wurden in der Re-
gel an den Fernseher, einen Röhrenfernseher, angeschlossen. Dieser Zei-
chensatz war speziell für dieses Ausgabemedium konzipiert und optimiert.
```

Zurück ins 21. Jahrhundert. Bis jetzt kam das Rechnen etwas hausbacken daher, als Manipulation von Zahlen oder Wahrheitswerten. Aber nicht nur mit diesen Größen, sondern auch mit Bildern kann man vorzüglich rechnen. Zu diesem Zweck erweitern wir unsere Programmiersprache im Folgenden Schritt für Schritt um neues Vokabular, mit dessen Hilfe sich Bilder beschreiben, manipulieren und komponieren lassen.

Wir stellen Bilder durch sogenannte ***Rastergrafiken*** (engl. bitmaps) dar. Eine Rastergrafik besteht aus rasterförmig angeordneten Bildpunkten, sogenannten ***Pixeln***, denen jeweils eine Farbe zugeordnet ist. Der Einfachheit halber beschränken wir uns auf Schwarz-Weiß Bilder: Ein Pixel ist entweder an oder aus. Eine Rastergrafik gibt somit für jede Position, bestehend aus einer x- und einer y-Koordinate, an, ob der zugehörige Bildpunkt leuchtet oder eben nicht. Mit anderen Worten, eine Rastergrafik ist nichts anderes als eine Funktion, die Koordinaten auf Wahrheitswerte abbildet: $Int * Int \to Bool$. Aus Gründen der Zukunftssicherheit legen wir uns nicht auf eine bestimmte Auflösung fest und erlauben als Koordinaten nicht nur beliebig große natürliche Zahlen, sondern auch negative Zahlen — Int ist der Typ der ganzen Zahlen. (Warum wir uns nicht auf natürliche Zahlen beschränken, werden wir später sehen.)

Mini-F# erlaubt es, Abkürzungen für Typen einzuführen, sogenannte ***Typsynonyme***, ein Feature, von dem wir gerne Gebrauch machen, um etwas Tipparbeit zu sparen.

$$\textit{type}\ Raster = Int * Int \to Bool$$

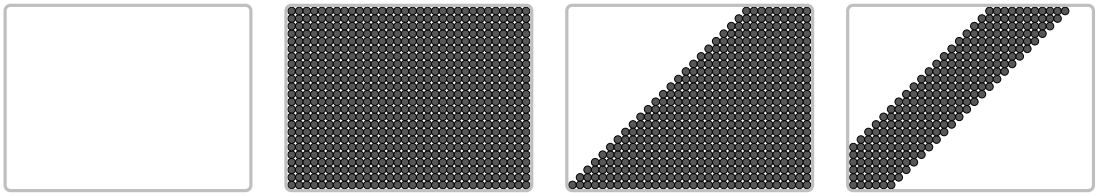
Typsynonyme sind bequem, aber nicht notwendig: Wir könnten überall statt $Raster$ etwas länglicher $Int * Int \to Bool$ verwenden. Aber abgesehen vom erhöhten Arbeitsaufwand würde auch

die Lesbarkeit des Programmtextes leiden — wohlgewählte Typsynonyme erhöhen die Lesbarkeit und tragen zur Selbstdokumentation von Programmen bei.

Wenden wir uns den Bildern und ihrer Komposition zu. Die einfachsten Rastergrafiken sind komplett weiß oder komplett schwarz. Da der Hintergrund weiß ist, werden nur schwarze Punkte, durch *true* repräsentiert, gezeichnet — eine willkürliche Festlegung.

```
let white : Raster = fun (x : Int, y : Int) → false
let black : Raster = fun (x : Int, y : Int) → true
```

Um etwas 90iger Jahre Feeling aufkommen zu lassen und damit Sie die einzelnen Bildpunkte identifizieren können, zeigen wir nur einen winzigen Ausschnitt der Rastergrafiken, die Pixel (x, y) mit $0 \leqslant x < 32$ und $0 \leqslant y < 24$ — sozusagen Mini-QVGA Auflösung.[5]



white *black* *hill* *dstripe*

Interessantere Grafiken erhalten wir, wenn wir die beiden Koordinaten zueinander in Beziehung setzen (*abs* berechnet den Absolutwert einer ganzen Zahl).

```
let hill    : Raster = fun (x : Int, y : Int) → x ⩾ y
let dstripe : Raster = fun (x : Int, y : Int) → abs (x − y) ⩽ 5
```

Wir können auch nur einen einzigen Punkt setzen: Das Bild $at\ (47, 11)$ ist vollständig weiß, mit Ausnahme des Pixels an der angegebenen Position.

```
let at (px : Int, py : Int) : Raster =
  fun (x : Int, y : Int) → px = x && py = y
```

Jetzt wird es spannend — wie setzen wir zwei oder mehr Punkte? Dieses Problem gehen wir etwas allgemeiner an, indem wir eine Funktion definieren, die zwei Bilder miteinander kombiniert.

```
let union (f : Raster, g : Raster) : Raster =
  fun (x : Int, y : Int) → f (x, y) || g (x, y)
```

So wie »+« zwei Zahlen nimmt und deren Summe zurückgibt, so nimmt *union* zwei Rastergrafiken und gibt deren Vereinigung zurück: Der Punkt (x, y) ist in $union\ (f, g)$ gesetzt, wenn er in f oder in g gesetzt ist oder in beiden Teilgrafiken. Zum Beispiel ist das Bild $union\ (at\ (1, 2), at\ (4, 3))$ vollständig weiß mit Ausnahme der beiden angegebenen Pixel. Wenn wir mehr als zwei Bilder vereinigen, müssen wir die Aufrufe schachteln:

$$union\ (f, union\ (g, h))$$

oder alternativ

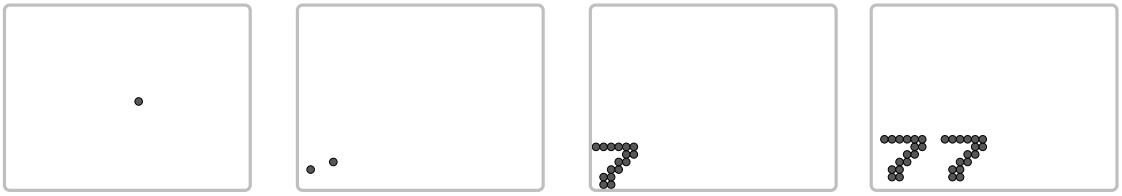
$$union\ (union\ (f, g), h)$$

Macht das einen Unterschied? Nein, die Vereinigung von Bildern ist assoziativ, eine Eigenschaft, die sie von der Disjunktion erbt. Wir haben im letzten Abschnitt schon angesprochen, dass man

[5] Quarter VGA (Video Graphics Array) umfasst 320×240 Pixel und damit ein Viertel des VGA-Formats 640×480.

assoziative Funktionen vorteilhafter infix notiert. Das wollen wir hier auch so halten (Abbildung 3.3 zeigt, wie man den Infixoperator ∧|∧ selbst definieren kann):

$$f \wedge|\wedge g \wedge|\wedge h$$



$at\ (17,11)$ $at\ (1,2) \wedge|\wedge at\ (4,3)$ *seven* *seventy-seven*

Solchermaßen gewappnet können wir einzelne Zeichen auf den Bildschirm bringen, zum Beispiel die Ziffer 7. Die Codierung ist reine Fleißarbeit, die attraktive Formatierung des Programmtextes hingegen eine Kunst:

$$\begin{array}{l}
\textbf{\textit{let}}\ seven \\
\quad = \ at\ (0,5) \wedge|\wedge at\ (1,5) \wedge|\wedge at\ (2,5) \wedge|\wedge at\ (3,5) \wedge|\wedge at\ (4,5) \wedge|\wedge at\ (5,5) \\
\wedge|\wedge \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad at\ (4,4) \wedge|\wedge at\ (5,4) \\
\wedge|\wedge \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad at\ (3,3) \wedge|\wedge at\ (4,3) \\
\wedge|\wedge \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad at\ (2,2) \wedge|\wedge at\ (3,2) \\
\wedge|\wedge \qquad\qquad\qquad\quad at\ (1,1) \wedge|\wedge at\ (2,1) \\
\wedge|\wedge \qquad\qquad\qquad\quad at\ (1,0) \wedge|\wedge at\ (2,0)
\end{array}$$

(An dieser Stelle wird vielleicht klar, warum die Vereinigung infix notiert wird — wenn Sie noch nicht überzeugt sind, versuchen Sie doch einmal, die Definition mit Hilfe von *union* umzuformulieren.)

Aber, wie bekommen wir die Zahl 77, also zwei Kopien der Ziffer 7, auf den Bildschirm? Die Rastergrafik *seven* zeigt die Pixel in der linken unteren Ecke an. Natürlich könnten wir die Definition duplizieren und die Koordinaten entsprechend verändern, aber das wäre nicht nur unökonomisch, sondern auch fehleranfällig. Koordinaten erhöhen — Rechnen mit Zahlen — kann ein Rechner zuverlässiger als wir, so dass wir das Problem etwas verallgemeinern und eine Funktion definieren, die eine gegebene Rastergrafik verschiebt. Zum Beispiel bewegt $move\ (9,1)\ seven$ die Ziffer 7 um neun Pixel nach rechts und einen Pixel nach oben.

$$\begin{array}{l}
\textbf{\textit{let}}\ move\ (dx : Int, dy : Int)\ (f : Raster) : Raster = \\
\quad \textbf{\textit{fun}}\ (x : Int, y : Int) \to f\ (x - dx, y - dy)
\end{array}$$

Da wir nach rechts und nach oben verschieben, müssen wir den Versatz von den Koordinaten *abziehen*. (Geometrisch gesehen handelt es sich bei (x, y) um einen Ortsvektor und bei (dx, dy) um einen Verschiebungsvektor.) Mit einem negativen Versatz können wir ein Bild nach links und/oder nach unten verschieben. Aus diesem Grund verwenden wir ganze und nicht natürliche Zahlen als Koordinaten.

Die Funktion *move* ist ein wundervolles Beispiel für eine HOF, eine Funktion höherer Ordnung. Versorgen wir *move* mit nur einem Argument,

$$move\ (9,1) : Raster \to Raster$$

erhalten wir eine Funktion, die eine Transformation von Rastergrafiken beschreibt. Wenden wir diese Funktion auf eine konkrete Rastergrafik an,

$$move\ (9,1)\ seven : Int * Int \to Bool$$

erhalten wir eine Rastergrafik, also eine Funktion von Koordinaten nach Wahrheitswerten. Wenn wir diese Funktion auf konkrete Koordinaten anwenden, erhalten wir schließlich einen Wahrheitswert.

```
move (9,1) seven (11,6) : Bool
```

Jede der gestaffelten Anwendungen stellt einen gültigen Ausdruck dar und beschreibt ein interessantes Konzept: eine Transformation, eine Rastergrafik oder einen Wahrheitswert.

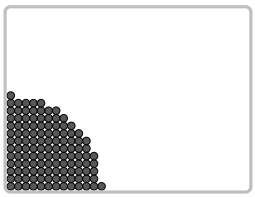
Nach diesen Vorarbeiten lässt sich 77 leicht definieren. (Ein Detail am Rande: Da die Zahl 7 im Unterschied etwa zum kleinen 9 keine Unterlänge besitzt, schieben wir sie um einen Pixelzeile nach oben.)

```
let seventy-seven = move (1,1) seven ^|^ move (9,1) seven
```

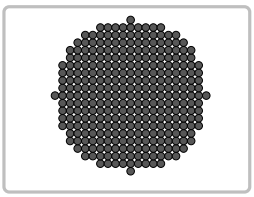
Jede Rastergrafik hat sozusagen ihr eigenes Koordinatensystem. Erst wenn man Bilder vereint, muss man sich Gedanken über die relative Lage der Punkte machen. Das nutzen auch die folgenden Funktionen aus, die einfache geometrische Figuren beschreiben.

```
let disc (r : Int) : Raster =                    // Kreis mit dem Durchmesser 2 · r + 1
  fun (x : Int, y : Int) → x * x + y * y ⩽ r * r
let rectangle (w : Int, h : Int) : Raster =      // Rechteck der Breite 2 · w + 1
  fun (x : Int, y : Int) → abs x ⩽ w && abs y ⩽ h // und der Höhe 2 · h + 1
```

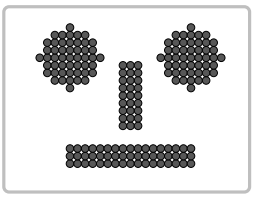
Die Funktion *disc r* zeichnet ein Kreis mit Radius r um den Ursprung des Koordinatensystems. Die Formel basiert auf dem alten Pythagoras: Der Punkt (x, y) liegt *auf* dem Kreis, wenn $x^2 + y^2 = r^2$ erfüllt ist; für Punkte *innerhalb* des Kreises gilt entsprechend $x^2 + y^2 \leqslant r^2$. *Beachte:* Der Kreis *disc r* enthält $2 \cdot r + 1$ Punkte auf der x- und auf der y-Achse, also immer eine ungerade Anzahl von Punkten. Gleiches gilt für Rechtecke.



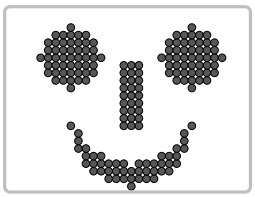
disc 12



move (16, 12) (*disc* 10)



move (16, 12) *frowny*



move (16, 12) *smiley*

Dass wir die Beschreibung von geometrischen Objekten und deren Platzierung in der Ebene logisch voneinander trennen können, liegt auch daran, dass wir ganze Zahlen als Koordinaten verwenden. Beschränkt man sich auf natürliche Zahlen, dann geht die Modularität verloren und die Formulierung wird umständlicher — probieren Sie es aus!

Mit Kreisen und Rechtecken können wir bereits einfache Emoticons (Kontraktion aus engl. *emotion* »Gefühl« und *icon* »Bild«) gestalten.

```
let frowny
    = move (−8, 5) (disc 4)          // left eye
  ^|^ move (8, 5)  (disc 4)          // right eye
  ^|^ move (0, 0)  (rectangle (1,4)) // nose
  ^|^ move (0, −8) (rectangle (8,1)) // mouth
```

Aber wie zeichnen wir den lächelnden Mund des Smileys? Überlegen Sie einen Moment, bevor Sie weiterlesen. Während Sie tüfteln, wenden wir uns vorübergehend der Gestaltung von »Hintergrundmustern« zu.

Periodisch wiederkehrende Muster wie vertikale oder horizontale Streifenmuster lassen sich mit der Modulo Operation realisieren.

```
let vstripes = fun (x : Int, y : Int) → x % 2 = 0
let hstripes = fun (x : Int, y : Int) → y % 2 = 0
```

Leuchten nur Punkte mit einer ungeraden x-Koordinate, erhalten wir vertikale Streifen, von der Breite eines Pixels. Wir können die Streifen verbreitern, indem wir die Grafik skalieren.

```
let scale (n : Int) (f : Raster) : Raster =
  fun (x : Int, y : Int) → f (x ÷ n, y ÷ n)
```

Wie *move* ist auch *scale* eine HOF: *scale* 5 ist eine Transformation, *scale* 5 *vstripes* eine Rastergrafik und *scale* 5 *vstripes* (4, 7) ein Wahrheitswert. Um eine Grafik zu vergrößern, müssen wir durch den Skalierungsfaktor *dividieren*. (Eine Grafik zu verkleinern ist wesentlich schwieriger. Warum?)

Können wir vertikale und horizontale Streifen zu einem Schachbrettmuster kombinieren? Man überlegt sich schnell (oder probiert es aus), dass die Vereinigung nicht ganz das gewünschte Ergebnis liefert. Auch der Durchschnitt führt nicht zum Ziel — wie die Vereinigung notieren wir auch den Durchschnitt bevorzugt infix: f ^&^ g für *intersect* (f, g).

```
let intersect (f : Raster, g : Raster) : Raster =
  fun (x : Int, y : Int) → f (x, y) && g (x, y)
```

Der gewünschte Effekt lässt sich mit der »Gleichheit« erzielen — da *equal* assoziativ ist, erlauben wir auch für diese Operation Infixnotation: f ^=^ g für *equal* (f, g).

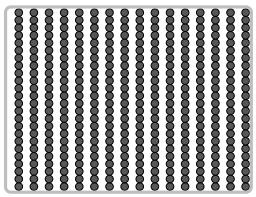
```
let equal (f : Raster, g : Raster) : Raster =
  fun (x : Int, y : Int) → f (x, y) = g (x, y)
```

Der Name *equal* ist vielleicht irreführend: Es wird *nicht* überprüft, ob zwei Rastergrafiken gleich sind — da Rastergrafiken Funktionen sind, ist diese Eigenschaft formal unentscheidbar. Vielmehr tested *equal* (f, g), ob korrespondierende Pixel in f und g gleich sind und setzt entsprechend das Pixel im Ergebnis — *equal* ist die *punktweise Gleichheit*. Was wir bisher noch nicht erwähnt haben: Nicht nur Zahlen, sondern auch Wahrheitswerte können auf (Un-) Gleichheit[6] getestet werden (siehe Aufgabe 3.4.1). Die zweidimensional arrangierten Wahrheitstabellen zeigen ein Schachbrettmuster,

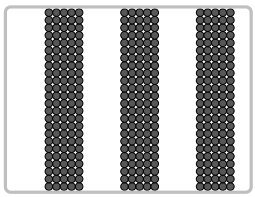
Gleichheit	*false*	*true*
true	*false*	*true*
false	*true*	*false*

Ungleichheit	*false*	*true*
true	*true*	*false*
false	*false*	*true*

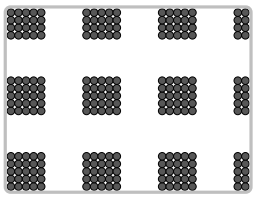
das man in der Grafik periodisch wiederfindet.



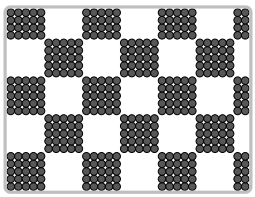
vstripes



scale 5 *vstripes*



scale 5 (*vstripes* ^&^ *hstripes*)



scale 5 (*vstripes* ^=^ *hstripes*)

[6] In der Logik spricht man statt von Gleichheit auch von Äquivalenz, siehe Anhang B.1. Technische Informatiker/-innen kennen die Ungleichheit unter dem Namen XOR (engl. exclusive *or*), der ausschließenden Disjunktion.

Mit der punktweisen Gleichheit lassen sich interessante, grafische Effekte erzielen. Bevor wir uns ein paar Beispiele anschauen, ist es hilfreich, kurz einige Eigenschaften der Operation zu diskutieren. Wir haben bereits erwähnt, dass ^=^ assoziativ ist; das neutrale Element von ^=^ ist *black*.

$$black \mathbin{\hat{=}\hat{}} f \;=\; f \;=\; f \mathbin{\hat{=}\hat{}} black \qquad\qquad (f \mathbin{\hat{=}\hat{}} g) \mathbin{\hat{=}\hat{}} h \;=\; f \mathbin{\hat{=}\hat{}} (g \mathbin{\hat{=}\hat{}} h)$$

Beide Gesetze leiten sich aus Eigenschaften der zugrundeliegenden Operation auf den Wahrheitswerten ab: = ist assoziativ mit *true* als neutralem Element.[7] Mit Hilfe von *white* lässt sich eine Grafik invertieren: schwarze Punkte in f sind weiß in $f \mathbin{\hat{=}\hat{}} white$ und umgekehrt. Invertieren wir zweimal erhalten wir die ursprüngliche Grafik zurück:

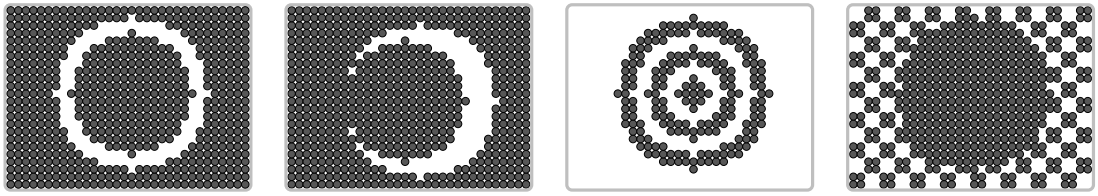
$$\begin{aligned}
& (f \mathbin{\hat{=}\hat{}} white) \mathbin{\hat{=}\hat{}} white \\
= \quad & \{\ \hat{=}\hat{} \text{ ist assoziativ}\ \} \\
& f \mathbin{\hat{=}\hat{}} (white \mathbin{\hat{=}\hat{}} white) \\
= \quad & \{\ (white \mathbin{\hat{=}\hat{}} white) = black, \text{ da } (false = false) = true\ \} \\
& f \mathbin{\hat{=}\hat{}} black \\
= \quad & \{\ black \text{ ist das neutrale Element von } \hat{=}\hat{}\ \} \\
& f
\end{aligned}$$

Algebra ist nützlich!

Kommen wir zu den Beispielen. Verknüpfen wir zwei Kreise unterschiedlicher Größe,

$$\textbf{let}\ ring = move\ (16,12)\ (disc\ 8 \mathbin{\hat{=}\hat{}} disc\ 10)$$

erhalten wir einen weißen Ring auf schwarzem Hintergrund.



ring *moon* *rings* *pond*

Versetzen wir die Kreise etwas, erscheint eine Mondsichel. Mehrere ineinander geschachtelte Kreise ergeben konzentrische Ringe; der Hintergrund in *rings* ist weiß, da eine ungerade Anzahl von Bildern mit ^=^ verknüpft wird — mit jeder Verknüpfung wird der ursprünglich weiße Hintergrund invertiert.

$$\begin{aligned}
&\textbf{let}\ moon \;&&= move\ (15,11)\ (disc\ 8 \mathbin{\hat{=}\hat{}} move\ (2,0)\ (disc\ 10)) \\
&\textbf{let}\ rings \;&&= move\ (16,12)\ (disc\ 2 \mathbin{\hat{=}\hat{}} disc\ 4 \mathbin{\hat{=}\hat{}} disc\ 6 \mathbin{\hat{=}\hat{}} disc\ 8 \mathbin{\hat{=}\hat{}} disc\ 10) \\
&\textbf{let}\ checker \;&&= vstripes \mathbin{\hat{=}\hat{}} hstripes \\
&\textbf{let}\ pond \;&&= scale\ 2\ checker \mathbin{\hat{|}\hat{}} move\ (16,12)\ (disc\ 10)
\end{aligned}$$

Abbildung 3.3 fasst das »Vokabular« noch einmal zusammen — die Typinformationen haben wir weggelassen (das ist tatsächlich möglich), um die Konzentration auf das Wesentliche zu erleichtern: Funktionsausdrücke und Funktionsapplikationen. Eine solche Sammlung von Funktionen nennt man im Fachjargon auch ***Bibliothek***. Man sieht: Mit vergleichsweise wenigen Zutaten

[7] Studenten/Studentinnen mit Kenntnissen imperativer Programmiersprachen testen erstaunlich häufig Wahrheitswerte und schreiben *if test = true then dies else das* statt kürzer *if test then dies else das*.

```
// Boolesche Algebra.
let white       = fun (x, y) → false
let black       = fun (x, y) → true
let at (px, py) = fun (x, y) → px = x && py = y
let invert f    = fun (x, y) → not (f (x, y))
let (^|^) f g   = fun (x, y) → f (x, y) || g (x, y)
let (^&^) f g   = fun (x, y) → f (x, y) && g (x, y)
let (^=^) f g   = fun (x, y) → f (x, y) = g (x, y)
// Transformationen.
let scale n          = fun f → fun (x, y) → f (x ÷ n, y ÷ n)
let move (dx, dy) = fun f → fun (x, y) → f (x − dx, y − dy)
// Geometrische Figuren.
let disc r           = fun (x, y) → x * x + y * y ⩽ r * r
let rectangle (w, h) = fun (x, y) → abs x ⩽ w && abs y ⩽ h
// Periodische Muster.
let vstripes = fun (x, y) → x % 2 = 0
let hstripes = fun (x, y) → y % 2 = 0
```

Abbildung 3.3.: Eine Bildbeschreibungssprache für Rastergrafiken.

lassen sich Rastergrafiken *kompositional* beschreiben. Ausgehend von »atomaren« oder »primitiven« Bildern wie *white*, *at* (47, 11) usw. werden Bilder mit *invert*, ^|^ , ^&^ und ^=^ *kombiniert* und mit *move* und *scale transformiert*. Eine Rastergrafik ist eine Funktion von Punkten auf Wahrheitswerte; die Transformationen manipulieren die Argumente dieser Funktionen; die Kombinatoren deren Ergebnisse.

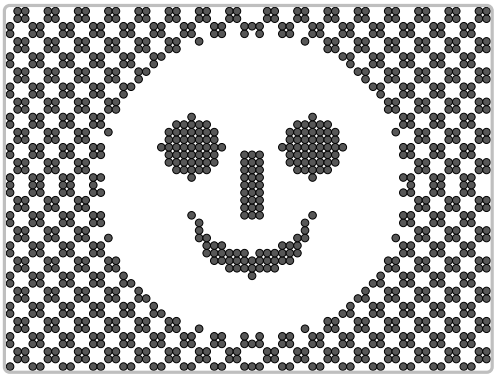
Es bleibt noch nachzutragen, wie der lächelnde Mund des Smileys komponiert wird. Die Mondsichel dient als Inspiration: Wir verschieben zwei Kreise vertikal gegeneinander und setzen alle Punkte, die im unteren aber nicht im oberen Kreis enthalten sind.

```
let smiley
    =  move (−8, 5) (disc 4)                                    // left eye
  ^|^ move (8, 5)   (disc 4)                                    // right eye
  ^|^ move (0, 0)   (rectangle (1, 4))                          // nose
  ^|^ move (0, −4) (disc 8 ^&^ invert (move (0, 3) (disc 8)))   // mouth
```

Der Ausdruck *f* ^&^ *invert g* berechnet die *Differenz* der Bilder *f* und *g* (vergleiche die Grafik mit den Venn-Diagrammen für die Mengendifferenz in Abschnitt B.2.1). Ein weiteres nützliches Idiom ist die »Alternative« (*mask* ^&^ *fore*) ^|^ (*invert mask* ^&^ *back*) — in Abhängigkeit von einer Maske wird ein Vorder- mit einem Hintergrundbild kombiniert. Im folgenden Beispiel dient ein großer Kreis als Maske.

```
let framed-smiley =
  let mask = disc 20
  in (mask ^&^ smiley) ^|^ (invert mask ^&^ scale 2 checker)
```

Der Smiley wird innerhalb des Kreises gezeichnet, das schachbrettartige Hintergrundmuster außerhalb.



move (32, 24) *framed-smiley*

Zwei Gedanken zum Schluß. Der Ausflug in die neunziger Jahre illustriert sehr schön das ingenieursmäßige Herangehen in der Informatik: Wir erschaffen unsere eigenen Welten und untersuchen anschließend deren Eigenschaften. Auch die Bedeutung der Sichtbarkeitsregeln wird uns plastisch vor Augen geführt: Jede der insgesamt dreizehn Funktionen in Abbildung 3.3 verwendet x und y als Parameternamen — die Sichtbarkeitsregeln sorgen für die nötige Hygiene und halten die Vorkommen auf Abstand.

Vertiefung: Gleichheit von Funktionen Gilt tatsächlich $(white \wedge\!=\!\wedge\, white) = black$? Um die Frage zu beantworten, müssen wir zunächst klären, wann zwei Funktionen gleich sind: $f_1 = f_2$? In Abschnitt 3.3 haben wir uns auf den Standpunkt gestellt, dass zwei Ausdrücke gleich sind, $e_1 = e_2$, wenn sie stets zu dem gleichen Wert auswerten. Da Funktionen »zu sich selbst auswerten«, müssten wir festlegen, wann zwei Funktionsabschlüsse gleich sind — damit würden wir das Problem im Prinzip nur verschieben, nicht lösen. (Sind die Abschlüsse $\langle \{ q \mapsto 2 \},\ n,\ n * q \rangle$ und $\langle \varnothing,\ n,\ n + n \rangle$ gleich?)

Wir legen fest, dass zwei Funktionen gleich sind, wenn sie im mathematischen Sinne gleich sind: Wenn sie gleiche Argumente auf gleiche Werte abbilden.

$$f_1 = f_2 \quad \Longleftrightarrow \quad \forall\ x\ .\ f_1\ x = f_2\ x$$

Die Eingangsfrage können wir somit mit »Ja!« beantworten, wie die folgende Rechnung demonstriert.

$$\begin{aligned}
& (white \wedge\!=\!\wedge\, white)\ (x, y) \\
= \quad & \{ \text{ Definition von } \wedge\!=\!\wedge \ \} \\
& white\ (x, y) = white\ (x, y) \\
= \quad & \{ \text{ Definition von } white \ \} \\
& false = false \\
= \quad & \{ \text{ Gleichheit von Wahrheitswerten } \} \\
& true \\
= \quad & \{ \text{ Definition von } black \ \} \\
& black\ (x, y)
\end{aligned}$$

Übungen.

📝 **1.** Werten Sie die folgenden Ausdrücke bzw. Deklarationen nacheinander mit dem Mini–F# Interpreter aus:

- $(\textbf{\textit{fun}}\ (n : Nat) \to n)\ 4711$,

Abbildung 3.4.: ATASCII Zeichensatz (ATARI Standard Code for Information Interchange).

- $(\textbf{\textit{fun}}\ (n : \mathit{Nat}) \to n * n)\ 4711$,
- $\textbf{\textit{let}}\ \mathit{twice} = \textbf{\textit{fun}}\ (f : \mathit{Nat} \to \mathit{Nat}) \to \textbf{\textit{fun}}\ (x : \mathit{Nat}) \to f\ (f\ x)$,
- $\mathit{twice}\ (\textbf{\textit{fun}}\ (n : \mathit{Nat}) \to n * n)\ 4711$,
- $\mathit{twice}\ (\mathit{twice}\ (\textbf{\textit{fun}}\ (n : \mathit{Nat}) \to n * n))\ 4711$.

Geben Sie für jeden Ausdruck die vollständige Rechnung als Beweisbaum an. Beachten Sie, dass die letzten beiden Ausdrücke die Definition $\textbf{\textit{let}}\ \mathit{twice} = \cdots$ sehen.

2. Finden Sie zu jedem der folgenden Typen einen passenden Ausdruck:

(a) $\mathit{Bool} \to \mathit{Bool}$,

(b) $\mathit{Bool} * \mathit{Bool} \to \mathit{Bool}$,

(c) $\mathit{Bool} \to (\mathit{Bool} \to \mathit{Bool})$,

(d) $(\mathit{Bool} \to \mathit{Bool}) \to \mathit{Bool}$.

Um die Aufgabe etwas interessanter zu machen, verlangen wir, dass alle formalen Parameter im jeweiligen Funktionsrumpf auch verwendet werden müssen. Somit scheidet $\textbf{\textit{fun}}\ (x{:}\mathit{Bool}) \to \mathit{false}$ als Lösung für Teil 1 aus. Wie viele semantisch unterschiedliche Funktionen gibt es jeweils? *Hinweis:* Die Typregeln $\Sigma \vdash e : t$ spezifizieren eine *Relation* zwischen Signaturen, Ausdrücken und Typen. Wenn wir mit ihrer Hilfe die Frage »Ist mein Programm wohlgetypt?« beantworten, so sind Σ und e gegeben und t wird gesucht. Jetzt sind Σ und t vorgegeben und wir suchen passende Ausdrücke e.

3. Erweitern Sie die Bibliothek aus Abbildung 3.3 um Funktionen für die Darstellung von Text.

(a) Realisieren Sie den Asteriskus ✱ als Rastergrafik, siehe Abbildung 3.4. Wenn Sie mögen, codieren Sie weitere Zeichen aus dem ATASCII Zeichensatz.

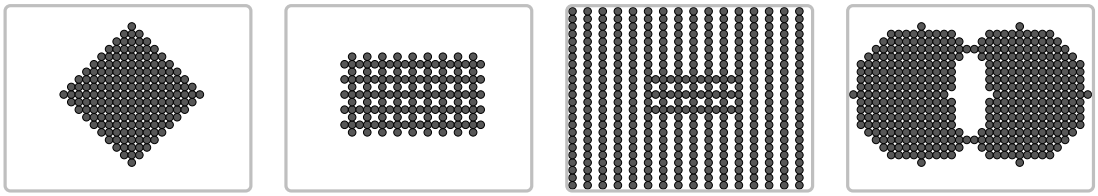
(b) Definieren Sie einen Operator, um Text »auf dem Bildschirm auszugeben«. Die Ausgabe

wird zum Beispiel mit Hilfe der folgenden Definition auf den Bildschirm gezaubert.

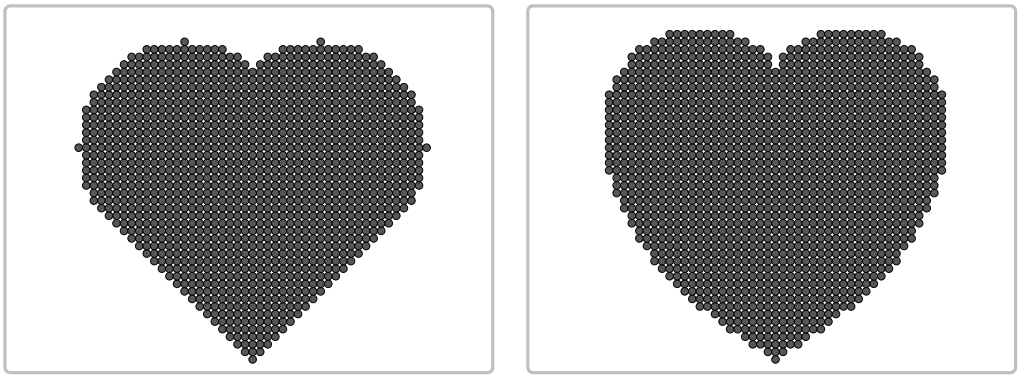
$\textbf{\textit{let}}\ \mathit{hello\text{-}world} =$
$104\ \hat{}\hat{}\ 101\ \hat{}\hat{}\ 108\ \hat{}\hat{}\ 108\ \hat{}\hat{}\ 111\ \hat{}\hat{}\ 12\ \hat{}\hat{}\ 0\ \hat{}\hat{}\ 119\ \hat{}\hat{}\ 111\ \hat{}\hat{}\ 115\ \hat{}\hat{}\ 101\ \hat{}\hat{}\ 100\ \hat{}\hat{}\ 1\ \hat{}\hat{}\ \mathit{white}$

Jedes Zeichen wird durch seinen ***Zeichencode*** spezifiziert, der Position innerhalb des ATASCII Zeichensatzes. Überlegen Sie zunächst, welchen Typ der Operator ^^ besitzt. *Hinweis:* Gehen Sie davon aus, dass Sie eine Funktion $\mathit{atascii} : \mathit{Nat} \to \mathit{Raster}$ zur Verfügung haben, die jedem Zeichencode die entsprechende Rastergrafik zuordnet.

⌨ **4.** Versuchen Sie die folgenden Rastergrafiken mit Hilfe der Kombinatoren aus Abbildung 3.3 zu beschreiben.



Falls Sie nach einer Herausforderung suchen …



Hinweis: googeln Sie nach Kardioid oder Herzkurve (engl. heart curve).

📝 **5.** Beweisen Sie die folgenden Gesetze:

(a) Die Vereinigung von Bildern ist assoziativ mit dem leeren Bild als neutralem Element.

$$\begin{aligned} \mathit{white} \mathbin{\wedge|\wedge} f &= f = f \mathbin{\wedge|\wedge} \mathit{white} \\ (f \mathbin{\wedge|\wedge} g) \mathbin{\wedge|\wedge} h &= f \mathbin{\wedge|\wedge} (g \mathbin{\wedge|\wedge} h) \end{aligned}$$

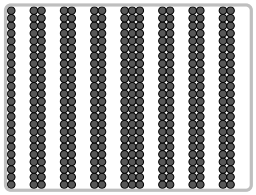
(b) Logische Verknüpfungen und geometrische Transformationen »kommen sich nicht ins Gehege«.

$$\begin{aligned} \mathit{scale}\ n\ (f \mathbin{\wedge|\wedge} g) &= (\mathit{scale}\ n\ f) \mathbin{\wedge|\wedge} (\mathit{scale}\ n\ g) \\ \mathit{move}\ (dx_1, dy_1)\ (\mathit{move}\ (dx_2, dy_2)\ f) &= \mathit{move}\ (dx_1 + dx_2, dy_1 + dy_2)\ f \end{aligned}$$

Finden Sie jeweils weitere Gesetze. *Hinweis:* Zwei Funktionen sind gleich, wenn sie gleiche Argumente auf gleiche Werte abbilden.

6. Harry ist beim Experimentieren mit Graphiken auf eine Merkwürdigkeit gestoßen.

$$\mathit{move}\ (16, 12)\ (\mathit{scale}\ 2\ \mathit{vstripes})$$



Warum befinden sich in der Mitte und nur dort drei vertikale Linien? Studieren Sie Anhang B.5.2 und erleuchten Sie Harry.

7. Harry hat zufällig eine Unterhaltung zwischen Studenten/Studentinnen der Mathematik mitbekommen und einige Sätze aufgeschnappt:

(a) »*at* ist die curryfizierte Gleichheit von Paaren«;

(b) »Rastergrafiken sind Endorelationen«;

(c) »Rastergrafiken formen eine Boolesche Algebra«.

Erklären Sie Harry, was jeweils gemeint ist. Stöbern Sie dazu im Anhang und im Index.

3.6. Rekursive Funktionen

To iterate is human;
to recurse, divine.
— L Peter Deutsch (1946)

Brexit means Brexit.
— Theresa May (1956)

Wir fahr'n fahr'n fahr'n auf der Autobahn,
Fahr'n fahr'n fahr'n auf der Autobahn
Jetzt schalten wir ja das Radio an
Aus dem Lautsprecher klingt es dann:
(Wir fahr'n auf der Autobahn …)
— Kraftwerk (Ralf Hütter, Florian Schneider-Esleben), *Autobahn*

Die letzte und wichtigste Erweiterung in diesem Kapitel motivieren wir mit einer Knobelaufgabe: Wieviele Möglichkeiten gibt es, n verschiedene Objekte in einer Reihe zu arrangieren? Nun, für die erste Position können wir zwischen n Objekten auswählen, die zweite Position lässt sich mit $n-1$ Objekten besetzen usw. Für die letzte Position bleibt schließlich nur ein einziges Objekt übrig. Da die jeweiligen Entscheidungen für ein bestimmtes Objekt unabhängig voneinander sind, ergibt sich als Gesamtzahl aller Arrangements das Produkt der Zahlen von 1 bis n, als Formel $n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$. Diese Zahl heißt auch n ***Fakultät***.

Im Folgenden wollen wir überlegen, wie wir die Fakultätsfunktion in Mini-F# programmieren können.

module Values.Factorial

```
let factorial (n : Nat) : Nat =
```

Wenn wir wissen, welchen konkreten Wert der formale Parameter n hat, können wir das Ergebnis jeweils einfach angeben:

```
if n = 0 then 1
else   if n = 1 then 1
  else if n = 2 then 1 * 2
  else if n = 3 then 1 * 2 * 3
  else …
```

Der Fall für $n = 0$ bedarf noch einer kurzen Klärung. Der Wert von 0 Fakultät ist 1, da das leere Produkt von Zahlen vereinbarungsgemäß 1 ist. Und in der Tat: 0 Objekte können auf genau eine Art und Weise angeordnet werden, als leeres Arrangement.

Die Ellipse (…) zeigt an, dass wir noch kein vollständiges Programm vor uns haben. Trotzdem lässt sich bereits ein Muster ausmachen: In jedem der Fälle $n > 0$ ist der letzte Faktor die Zahl n selbst. (Klar, oder?)

```
if n = 0 then 1
else   if n = 1 then n
  else if n = 2 then 1 * n
  else if n = 3 then 1 * 2 * n
  else …
```

Mit Hilfe der Eigenschaft *if* e_1 *then* $e_2 * e$ *else* $e_3 * e = ($*if* e_1 *then* e_2 *else* $e_3) * e$ können wir das Programm bzw. den Funktionsrumpf umschreiben. Der Faktor n wird sozusagen aus den Zweigen der Alternativen »herausgezogen«.

```
if n = 0 then 1
else ( if n = 1 then 1
  else if n = 2 then 1
  else if n = 3 then 1 * 2
  else ...) * n
```

Der geklammerte Ausdruck sieht dem ursprünglichen Funktionsrumpf sehr ähnlich, nur dass die Bedingungen $n = 1$, $n = 2$ usw. lauten, statt $n = 0$, $n = 1$ usw. Wir können die Konstanten in Übereinstimmung bringen, indem wir links und rechts jeweils 1 subtrahieren. (Dabei ist Vorsicht geboten, da $0 \div 1 = 0$.)

```
if n = 0 then 1
else ( if n ÷ 1 = 0 then 1
  else if n ÷ 1 = 1 then 1
  else if n ÷ 1 = 2 then 1 * 2
  else ...) * n
```

Somit entspricht der geklammerte Ausdruck dem Aufruf *factorial* $(n \div 1)$. Erlauben wir bei der Definition einer Funktion den Rückgriff auf die definierte Funktion selbst (!), so erhalten wir das folgende, kompakte Programm.

```
let rec factorial (n : Nat) : Nat =
  if n = 0 then 1 else factorial (n ÷ 1) * n
```

In Worten ausgedrückt: Die Fakultät von 0 ist 1; ist $n > 0$, dann ist n Fakultät gleich dem Produkt von $n \div 1$ Fakultät und n. Greift man — wie hier — bei der Definition auf das definierte Objekt selbst zurück, spricht man von einer ***rekursiven*** Definition. Rekursive Definitionen werden mit dem Schlüsselwort ***rec*** gekennzeichnet. (Warum?)

Abbildung 3.5 illustriert die Abarbeitung des Funktionsaufrufs *factorial* (3). Um uns nicht in Details zu verlieren, haben wir die Auswertung als Folge von Gleichungen notiert: *factorial* (3) = ⋯ = 6. Da *factorial* eine Funktion im mathematischen Sinne ist, können wir einen Funktionsaufruf ausrechnen, indem wir wiederholt die linke Seite der Definition durch die rechte Seite ersetzen und dabei für die formalen Parameter die aktuellen Parameter einsetzen. (Wenn eine Mini-F# Funktion keine mathematische Funktion ist, dann ist das nicht möglich — in Kapitel 7 verlassen wir den Pfad der Tugend.)

Zwei Phasen lassen sich bei der Abarbeitung von *factorial* ausmachen: Beim ***rekursiven Abstieg*** wird Schritt für Schritt ein Turm von Multiplikationen aufgebaut; beim ***rekursiven Aufstieg*** wird dieser Turm Schritt für Schritt wieder abgebaut. (Bei der Herleitung der Funktion haben wir im letzten Schritt die Definition »eingeklappt«. Bei der Abarbeitung der Funktion wird die Definition sozusagen wieder »ausgeklappt«, gegebenenfalls mehrfach.) Bei der Darstellung in Abbildung 3.5 vereinfachen bzw. mogeln wir bewusst: Die formalen Parameter werden nicht durch die aktuellen Parameter *textuell* ersetzt, sondern die jeweiligen Bindungen werden mit Hilfe von Umgebungen protokolliert. Dazu in Kürze mehr.

Abstrakte Syntax Deklarationen werden um rekursive Funktionsdefinitionen erweitert.

$d ::= \cdots$	***Deklarationen:***
$\mid$ ***let rec*** $f\ (x_1 : t_1) : t_2 = e$	rekursive Funktionsdefinition

Die Gleichung ***let rec*** $f\ (x) = e$ definiert genau wie ***let*** $f\ (x) = e$ eine Funktion, mit dem Unterschied, dass in e zusätzlich der Bezeichner f selbst sichtbar ist.

$$
\begin{aligned}
& \mathit{factorial}\ (3) \\
= & \quad \{ \text{Definition von } \mathit{factorial} \} \\
& \textbf{\textit{if}}\ 3 = 0\ \textbf{\textit{then}}\ 1\ \textbf{\textit{else}}\ \mathit{factorial}\ (3 \dot{-} 1) * 3 \\
= & \quad \{ \text{Auswertung der Alternative} \} \\
& \mathit{factorial}\ (3 \dot{-} 1) * 3 \\
= & \quad \{ \text{Definition der natürlichen Subtraktion} \} \\
& \mathit{factorial}\ 2 * 3 \\
= & \quad \{ \text{Definition von } \mathit{factorial} \} \\
& (\textbf{\textit{if}}\ 2 = 0\ \textbf{\textit{then}}\ 1\ \textbf{\textit{else}}\ \mathit{factorial}\ (2 \dot{-} 1) * 2) * 3 \\
= & \quad \{ \text{Auswertung der Alternative} \} \\
& (\mathit{factorial}\ (2 \dot{-} 1) * 2) * 3 \\
= & \quad \{ \text{Definition der natürlichen Subtraktion} \} \\
& (\mathit{factorial}\ 1 * 2) * 3 \\
= & \quad \{ \text{Definition von } \mathit{factorial} \} \\
& ((\textbf{\textit{if}}\ 1 = 0\ \textbf{\textit{then}}\ 1\ \textbf{\textit{else}}\ \mathit{factorial}\ (1 \dot{-} 1) * 1) * 2) * 3 \\
= & \quad \{ \text{Auswertung der Alternative} \} \\
& ((\mathit{factorial}\ (1 \dot{-} 1) * 1) * 2) * 3 \\
= & \quad \{ \text{Definition der natürlichen Subtraktion} \} \\
& ((\mathit{factorial}\ 0 * 1) * 2) * 3 \\
= & \quad \{ \text{Definition von } \mathit{factorial} \} \\
& (((\textbf{\textit{if}}\ 0 = 0\ \textbf{\textit{then}}\ 1\ \textbf{\textit{else}}\ \mathit{factorial}\ (0 \dot{-} 1) * 0) * 1) * 2) * 3 \\
= & \quad \{ \text{Auswertung der Alternative} \} \\
& ((1 * 1) * 2) * 3 \\
= & \quad \{ \text{Definition der Multiplikation} \} \\
& (1 * 2) * 3 \\
= & \quad \{ \text{Definition der Multiplikation} \} \\
& 2 * 3 \\
= & \quad \{ \text{Definition der Multiplikation} \} \\
& 6
\end{aligned}
$$

Abbildung 3.5.: Auswertung des Funktionsaufrufs *factorial* (3).

Statische Semantik Die Typregel für die rekursive Funktionsdefinition entspricht der Regel für ihr nicht-rekursives Gegenstück mit dem Unterschied, dass nicht nur der formale Parameter x_1, sondern auch der Funktionsname f im Funktionsrumpf e_2 sichtbar ist.

$$\frac{\Sigma, \{f \mapsto t_1 \to t_2, x_1 \mapsto t_1\} \vdash e_2 : t_2}{\Sigma \vdash (\textbf{\textit{let rec}}\ f\ (x_1 : t_1) : t_2 = e_2) : \{f \mapsto t_1 \to t_2\}}$$

Dynamische Semantik Eine rekursive Funktionsdefinition wertet ähnlich wie eine nicht-rekursive im Wesentlichen zu sich selbst aus. Die Deklaration der Fakultätsfunktion ergibt zum Beispiel die Umgebung

$$\{\mathit{factorial} \mapsto \langle \varnothing, \mathit{factorial}, n, \ \textbf{\textit{if}}\ n = 0\ \textbf{\textit{then}}\ 1\ \textbf{\textit{else}}\ \mathit{factorial}\ (n \dot{-} 1) * n \rangle\}$$

An die Stelle eines Funktionsabschlusses ist ein ***rekursiver Funktionsabschluss*** getreten, in dem *zusätzlich* der Name der rekursiven Funktion aufgeführt wird. Bei der Anwendung einer rekursiven Funktion auf ein Argument müssen wir den formalen Parameter an den Wert des aktuellen Parameters *und* zusätzlich den Funktionsbezeichner an den rekursiven Funktionsabschluss binden.

Wir erweitern den Bereich der Werte um rekursive Funktionsabschlüsse.

$\nu ::= \cdots$	***Werte:***
$\mid \langle \delta, f, x, e \rangle$	rekursiver Funktionsabschluss

Eine rekursive Funktionsdefinition wertet zu einer Bindung aus, in der der Funktionsname an einen rekursiven Funktionsabschluss gebunden ist.

$$\frac{}{\delta \vdash (\textbf{\textit{let rec}}\ f\ x = e) \ \Downarrow\ \{f \mapsto \langle \delta, f, x, e \rangle\}}$$

Schließlich benötigen wir eine weitere Regel für die Funktionsapplikation, die sich um rekursive Funktionen kümmert.

$$\frac{\delta \vdash e \ \Downarrow\ \nu \qquad \delta \vdash e_1 \ \Downarrow\ \nu_1 \qquad \delta', \{f \mapsto \nu, x_1 \mapsto \nu_1\} \vdash e' \ \Downarrow\ \nu'}{\delta \vdash e\ e_1 \ \Downarrow\ \nu'} \quad \text{mit } \nu = \langle \delta', f, x_1, e' \rangle$$

Wie auch bei nicht-rekursiven Funktionsabschlüssen vollzieht sich die Auswertung in drei Schritten:

(1) Die Funktion e wird ausgerechnet; die obige Regel kommt zur Anwendung, wenn das Ergebnis ein rekursiver Funktionsabschluss ist.

(2) Das Argument e_1 wird ausgerechnet; das Ergebnis ist ein Wert.

(3) Der Funktionsrumpf e' wird in der Umgebung $\delta', \{f \mapsto \nu, x_1 \mapsto \nu_1\}$ ausgerechnet. Der Bezeichner f wird an den rekursiven Funktionsabschluss gebunden, in dem f selbst aufgeführt wird. (Aus der Rekursion wird ein zyklisches Geflecht.) Zusätzlich wird dem formalen Parameter x_1 der *Wert* ν_1 des aktuellen Parameters zugeordnet. Das Ergebnis dieser Rechnung ist der Wert des Funktionsaufrufs $e\ e_1$.

Schauen wir uns die Abarbeitung des Aufrufs *factorial* (3) noch einmal und jetzt im Detail an — konstruieren wir einen Beweisbaum. Damit die Formeln nicht zu groß geraten, kürzen wir

factorial mit *fac* ab. Weiterhin vereinbaren wir Abkürzungen für den rekursiven Funktionsabschluss und für die beteiligten Umgebungen.

$$\gamma := \langle \varnothing,\ fac,\ n,\ \ \textit{if}\ n = 0\ \textit{then}\ 1\ \textit{else}\ fac\ (n \dot{-} 1) * n \rangle$$
$$\delta := \{\, fac \mapsto \gamma \,\}$$
$$\delta_i := \varnothing, \{\, fac \mapsto \gamma, n \mapsto i \,\} = \{\, fac \mapsto \gamma, n \mapsto i \,\}$$

Wir haben bereits in Abbildung 3.5 gesehen, dass der initiale Aufruf *fac* (3) drei weitere Aufrufe nach sich zieht. Entsprechend mächtig gerät der Beweisbaum — tatsächlich der größte Beweisbaum, der uns in diesem Skript unterkommen wird. Wie für jeden Auswertungsbaum gilt: Die Form der Teilbäume wird jeweils durch die Form der Teilausdrücke bestimmt. Für die meisten Ausdrücke gibt es genau eine Auswertungsregel — damit ist klar, welche Regel zur Anwendung kommt. Ausnahmen von dieser Faustregel sind die Alternative und die Vergleichsoperationen. Für sie gibt es jeweils zwei Auswertungsregeln; entsprechend unterschiedlich können die Beweisbäume aussehen. Beim initialen Aufruf kommen die Auswertungsregeln für rekursive Funktionsdefinitionen und für Aufrufe rekursiv definierter Funktionen zum Tragen.

$$\dfrac{\dfrac{}{\varnothing \vdash \textit{let rec}\ fac\ (n) = \cdots \Downarrow \delta} \quad \dfrac{\dfrac{}{\delta \vdash fac \Downarrow \gamma} \quad \dfrac{}{\delta \vdash 3 \Downarrow 3} \quad \dfrac{\vdots}{\delta_3 \vdash \textit{if}\ n = 0 \cdots \Downarrow 6}}{\delta \vdash fac\ (3) \Downarrow 6}}{\varnothing \vdash \textit{let rec}\ fac\ (n) = \textit{if}\ n = 0\ \textit{then}\ 1\ \textit{else}\ fac\ (n \dot{-} 1) * n\ \textit{in}\ fac\ (3) \Downarrow 6}$$

Die Auswertung des Funktionsaufrufs umfasst wie bereits angesprochen drei Schritte: zunächst wird der Bezeichner *fac* in der Umgebung δ nachgeschlagen; dann wird der aktuelle Parameter ausgerechnet, und schließlich wird der Funktionsrumpf in der Umgebung δ_3 ausgewertet. Diese Umgebung ergibt sich als Erweiterung der im Funktionsabschluss abgelegten Umgebung — diese ist leer — um Bindungen für den Namen der rekursiv definierten Funktion und deren Parameter. Entwickeln wir den Beweisbaum für den Funktionsrumpf weiter — im obigen Baum durch das Auslassungszeichen markiert.

$$\dfrac{\dfrac{}{\delta_3 \vdash n = 0 \Downarrow \textit{false}} \quad \dfrac{\dfrac{}{\delta_3 \vdash fac \Downarrow \gamma} \quad \dfrac{}{\delta_3 \vdash n \dot{-} 1 \Downarrow 2} \quad \dfrac{\vdots}{\delta_2 \vdash \textit{if}\ n = 0 \cdots \Downarrow 2}}{\delta_3 \vdash fac\ (n \dot{-} 1) \Downarrow 2} \quad \dfrac{}{\delta_3 \vdash n \Downarrow 3}}{\delta_3 \vdash fac\ (n \dot{-} 1) * n \Downarrow 6}}{\delta_3 \vdash \textit{if}\ n = 0\ \textit{then}\ 1\ \textit{else}\ fac\ (n \dot{-} 1) * n \Downarrow 6}$$

Die Auswertung zieht einen weiteren Aufruf der Fakultätsfunktion nach sich. Die Abarbeitungsschritte für den Rumpf sind jeweils gleich, nur dass die Umgebung eine andere ist: Aus δ_3 wird δ_2. Sie protokolliert den Wert des Parameters *n* beim rekursiven Abstieg.

$$\dfrac{\dfrac{}{\delta_2 \vdash n = 0 \Downarrow \textit{false}} \quad \dfrac{\dfrac{}{\delta_2 \vdash fac \Downarrow \gamma} \quad \dfrac{}{\delta_2 \vdash n \dot{-} 1 \Downarrow 1} \quad \dfrac{\vdots}{\delta_1 \vdash \textit{if}\ n = 0 \cdots \Downarrow 1}}{\delta_2 \vdash fac\ (n \dot{-} 1) \Downarrow 1} \quad \dfrac{}{\delta_2 \vdash n \Downarrow 2}}{\delta_2 \vdash fac\ (n \dot{-} 1) * n \Downarrow 2}}{\delta_2 \vdash \textit{if}\ n = 0\ \textit{then}\ 1\ \textit{else}\ fac\ (n \dot{-} 1) * n \Downarrow 2}$$

Es erfolgt ein weiterer rekursiver Aufruf — der resultierende Beweisbaum ist vom Aufbau wiederum identisch; nur die Umgebungen und berechneten Werte sind unterschiedlich.

$$\dfrac{\dfrac{}{\delta_1 \vdash n = 0 \Downarrow \textit{false}} \quad \dfrac{\dfrac{}{\delta_1 \vdash fac \Downarrow \gamma} \quad \dfrac{}{\delta_1 \vdash n \dot{-} 1 \Downarrow 0} \quad \dfrac{\vdots}{\delta_0 \vdash \textit{if}\ n = 0 \cdots \Downarrow 1}}{\delta_1 \vdash fac\ (n \dot{-} 1) \Downarrow 1} \quad \dfrac{}{\delta_1 \vdash n \Downarrow 1}}{\delta_1 \vdash fac\ (n \dot{-} 1) * n \Downarrow 1}}{\delta_1 \vdash \textit{if}\ n = 0\ \textit{then}\ 1\ \textit{else}\ fac\ (n \dot{-} 1) * n \Downarrow 1}$$

Vergleicht man die drei obigen Beweisbäume, sieht man, dass zum Beispiel der Teilausdruck n, das zweite Argument der Multiplikation, insgesamt dreimal ausgewertet wird, aber jeweils in unterschiedlichen Umgebungen: $\delta_3 \vdash n \Downarrow 3$, $\delta_2 \vdash n \Downarrow 2$ und $\delta_1 \vdash n \Downarrow 1$. Der letzte Aufruf mit $n = 0$ führt schließlich unmittelbar zum Ziel: Die Alternative wird zu 1 ausgewertet.

$$\frac{\overline{\delta_0 \vdash n = 0 \Downarrow \mathit{true}} \qquad \overline{\delta_0 \vdash 1 \Downarrow 1}}{\delta_0 \vdash \mathbf{if}\ n = 0\ \mathbf{then}\ 1\ \mathbf{else}\ \mathit{fac}\ (n \dot{-} 1) * n \Downarrow 1}$$

Eigentlich müsste man jetzt alle fünf Beweisbäume zusammenstecken; davon wollen wir aus Platzgründen absehen.

Die Fakultät wächst übrigens sehr schnell, wie die folgenden Beispielaufrufe zeigen.

```
⋙ factorial 10
3.628.800
⋙ factorial 100
93.326.215.443.944.152.681.699.238.856.266.700.490.715.968.264.381.621.468.592.
963.895.217.599.993.229.915.608.941.463.976.156.518.286.253.697.920.827.223.758.
251.185.210.916.864.000.000.000.000.000.000.000.000
```

Die Zahl der Atome im sichtbaren Weltall wird auf ungefähr 10^{79} geschätzt; *factorial* 100 mit seinen 158 Stellen übersteigt diese Zahl um ein Vielfaches.

3.7. Entwurfsmuster

Few things are harder to put up with than the annoyance of a good example.
— Mark Twain (1835–1910), *Pudd'nhead Wilson (1894)*

Der Schritt von den nicht-rekursiven zu den rekursiven Funktionen ist ein gewaltiger. Nunmehr ist unsere Sprache ***berechnungsuniversell***. Mit ihr können wir die prinzipiellen Möglichkeiten eines Rechners ausnutzen. Mehr dazu später in der Theoretischen Abteilung der Informatik. Wir wenden uns an dieser Stelle den vergnüglichen Dingen zu, der Programmierung.

3.7.1. Peano Entwurfsmuster

Bei der Auflistung der vordefinierten arithmetischen Operatoren in Abschnitt 3.1 fehlt unter anderem die Potenzfunktion. Vervollständigen wir unser Repertoire an arithmetischen Funktionen, indem wir ein Programm dafür schreiben. Bevor wir die Aufgabe angehen, ist es hilfreich, sich noch einmal die Definition der Fakultät ins Gedächtnis zu rufen.

module Values.Peano

```
let rec factorial (n : Nat) : Nat =
  if n = 0 then 1
           else factorial (n ∸ 1) * n
```

Die Definition macht Gebrauch von der Tatsache, dass eine natürliche Zahl entweder 0 oder größer als 0 ist. Im ersten Fall können und müssen wir unmittelbar die Lösung angeben (***Rekursionsbasis*** oder Rekursionsverankerung). Im zweiten Fall bestimmen wir rekursiv eine Lösung für $n \dot{-} 1$ und erweitern dann die Teillösung zu einer Gesamtlösung für n (***Rekursionsschritt***). Wenden wir dieses Schema auf die Potenzfunktion x^n an.

```
let rec power (x : Nat, n : Nat) : Nat =
  if n = 0 then …
           else … power (x, n ∸ 1) …
```

(Beachte, dass wir über n rekurrieren, nicht über x. Warum?) Die Rekursionsbasis ist einfach: x^0 ist 1. Der Rekursionsschritt ist nicht viel schwieriger: Der rekursive Aufruf ermittelt $x^{n \dot{-} 1}$; wir erweitern die Teillösung zur Gesamtlösung x^n, indem wir $x^{n \dot{-} 1}$ mit x multiplizieren. Insgesamt erhalten wir das folgende Programm.

$$
\begin{array}{l}
\textbf{\textit{let rec}}\ \mathit{power}\ (x : \mathit{Nat}, n : \mathit{Nat}) : \mathit{Nat} = \\
\quad \textbf{\textit{if}}\ n = 0\ \textbf{\textit{then}}\ 1 \\
\qquad\qquad \textbf{\textit{else}}\ \ x * \mathit{power}\ (x, n \dot{-} 1)
\end{array}
$$

Die Potenzfunktion wird auf wiederholte Multiplikation zurückgeführt. Auf die gleiche Art und Weise können wir auch die Multiplikation auf die Addition zurückführen

$$
\begin{array}{l}
\textbf{\textit{let rec}}\ \mathit{mul}\ (m : \mathit{Nat}, n : \mathit{Nat}) : \mathit{Nat} = \\
\quad \textbf{\textit{if}}\ m = 0\ \textbf{\textit{then}}\ 0 \\
\qquad\qquad \textbf{\textit{else}}\ \ n + \mathit{mul}\ (m \dot{-} 1, n)
\end{array}
$$

und die Addition auf die Nachfolgerfunktion.

$$
\begin{array}{l}
\textbf{\textit{let rec}}\ \mathit{add}\ (m : \mathit{Nat}, n : \mathit{Nat}) : \mathit{Nat} = \\
\quad \textbf{\textit{if}}\ m = 0\ \textbf{\textit{then}}\ n \\
\qquad\qquad \textbf{\textit{else}}\ \ 1 + \mathit{add}\ (m \dot{-} 1, n)
\end{array}
$$

Die Beispielprogramme zeigen, dass wir theoretisch mit einigen wenigen vordefinierten Funktionen auskommen: der Zahl 0, dem Test »gleich 0«, der Nachfolger- und der Vorgängerfunktion. Praktisch gesehen ist »+« allerdings vorteilhafter als *add*, da schneller: $4711 + 815$ benötigt einen Auswertungsschritt, $\mathit{add}\ (4711, 815)$ hingegen mehrere zehntausend Schritte. (Die Anzahl der Rechenschritte entspricht der Größe des Beweisbaums für $\delta \vdash e \Downarrow n$ — aus wievielen Regeln bzw. Regelinstanzen setzt sich der Baum zusammen?)

Die Exkursion war noch aus einem anderen Grund lehrreich, zeigt sie uns doch ein allgemeines ***Entwurfsmuster*** (engl. design pattern) auf, um Funktionen über den natürlichen Zahlen zu programmieren: Haben wir die Aufgabe eine Funktion $f : \mathit{Nat} \to t$ zu erstellen, dann sieht ein erster Entwurf folgendermaßen aus.

Peano Entwurfsmuster

$$
\begin{array}{lll}
\textbf{\textit{let rec}}\ f\ (n : \mathit{Nat}) : t = & & \\
\quad \textbf{\textit{if}}\ n = 0\ \textbf{\textit{then}}\ \ldots & & \textit{Rekursionsbasis} \\
\qquad\qquad \textbf{\textit{else}}\ \ \ldots f\ (n \dot{-} 1) \ldots & & \textit{Rekursionsschritt}
\end{array}
$$

Die Ellipsen müssen wir sodann mit Leben füllen: An die Stelle des ersten Auslassungszeichens muss ein Ausdruck des Typs t treten (Rekursionsbasis); die zweite Stelle müssen wir mit einem Ausdruck füllen, der die Teillösung $f\ (n \dot{-} 1)$ vom Typ t zu einer Gesamtlösung vom Typ t erweitert (Rekursionsschritt). Der Parameter n heißt übrigens auch ***Rekursionsvariable***.

Um uns später auf dieses Entwurfsmuster beziehen zu können, geben wir ihm einen Namen: ***Peano Entwurfsmuster*** nach dem italienischen Mathematiker Giuseppe Peano, der sich mit der Axiomatisierung der natürlichen Zahlen beschäftigt hat, siehe Abbildung 3.6.

Wenden wir das Peano Entwurfsmuster auf ein weiteres Beispiel an. Der Aufruf *square-root n* soll die Quadratwurzel der Zahl n bestimmen. Die Wurzel geht nicht immer glatt auf, so dass wir die Aufgabe präzisieren müssen: Gesucht wird die *größte* Zahl r, so dass $r * r$ kleiner oder

Der italienische Mathematiker und Logiker Giuseppe Peano entwickelte, an die Algebra der Logik von Boole, Jevons, Schröder und Porezki anknüpfend, die mathematische Logik weiter.

Von Peano stammt ein bekanntes und noch heute verwendetes ***Axiomensystem*** für die natürlichen Zahlen:

- 0 ist eine natürliche Zahl.
- Für alle n gilt, dass, wenn n eine natürliche Zahl ist, auch die auf n folgende Zahl eine natürliche Zahl ist.
- Wenn auf zwei Zahlen dieselbe Zahl folgt, sind sie identisch.
- 0 kann nicht auf eine natürliche Zahl folgen.
- Das Induktionsaxiom: Wenn 0 eine Eigenschaft hat und wenn jede auf eine natürliche Zahl folgende Zahl die Eigenschaft besitzt, sofern die Zahl selbst die Eigenschaft hat, dann haben alle natürlichen Zahlen die betreffende Eigenschaft.

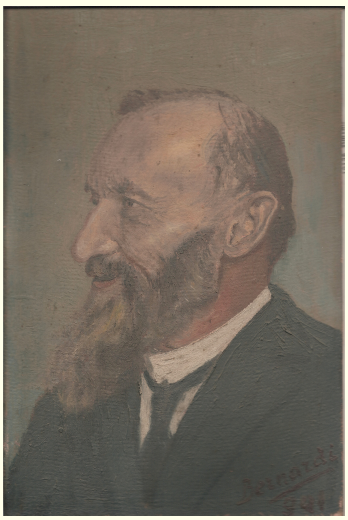


Abbildung 3.6.: Giuseppe Peano (1858–1932).

gleich n ist. Zum Beispiel gilt *square-root* 143 = 11 und *square-root* 144 = 12. In eine Formel gegossen suchen wir $\lfloor\sqrt{n}\rfloor$.[8] Das Entwurfsmuster gibt das Skelett vor:

```
let rec square-root (n : Nat) : Nat =
  if n = 0 then …
           else … square-root (n ∸ 1) …
```

Die Wurzel von 0 ist 0, somit ist die Rekursionsbasis abgehakt. Zum Rekursionsschritt: Wenn wir die Wurzel von $n \dot{-} 1$ kennen, wie lässt sich daraus die Wurzel von n herleiten? Nun, die Quadratwurzel von n ist entweder identisch zur Quadratwurzel von $n \dot{-} 1$ oder um eins größer (Aufgabe 3.7.2 fragt nach einem Beweis). Um herauszufinden, welcher Fall vorliegt, testen wir einfach, ob wir mit der Erhöhung über das Ziel hinausschießen.

```
let rec square-root (n : Nat) : Nat =
  if n = 0 then 0
           else let r = square-root (n ∸ 1)
                in if n < square (r + 1) then r else r + 1
```

Dem Ergebnis des rekursiven Aufrufs geben wir einen Namen, r, da dieser mehrfach benötigt wird. Die Berechnung von *square-root* $(n \dot{-} 1)$ ist aufwändig, es ist keine gute Idee, *if* $n <$ *square* (*square-root* $(n \dot{-} 1)+1$) *then square-root* $(n \dot{-} 1)$ *else square-root* $(n \dot{-} 1)+1$ zu schreiben, da so die aufwändige Rechnung doppelt durchgeführt wird.

Das Peano Entwurfsmuster als HOF Wenden wir uns noch einmal dem Peano Entwurfsmuster selbst zu. Interessanterweise können wir das Peano Entwurfsmuster selbst als Programm formulieren. Aus einem informellen Schema wird eine wiederverwendbare Funktion, eine sogenannte ***Bibliotheksfunktion***! Die wesentliche Einsicht ist, dass die Erweiterung der Teillösung zu einer Gesamtlösung der Natur nach eine Funktion ist. Geben wir also den fehlenden Programmteilen im Schema einen Namen.

```
let rec f (n : Nat) : Nat =
  if n = 0 then zero
           else succ (f (n ∸ 1))
```

Da wir uns auf keine konkreten Werte für die Bezeichner *zero* und *succ* festlegen wollen — wir entwickeln ja ein Lösungs*schema*, nicht eine Lösung für *ein* konkretes Problem — machen wir sie zum Parameter einer Funktion. Der Abstraktionsschritt ist der gleiche wie bei der Einführung der Funktion *area*, nur dass jetzt von zwei Werten abstrahiert wird und dass der eine Wert selbst eine Funktion ist.

```
let peano-pattern (zero : Nat, succ : Nat → Nat) : Nat → Nat =
  let rec f (n : Nat) : Nat =
        if n = 0 then zero
                 else succ (f (n ∸ 1))
  in f
```

Die Funktion *peano-pattern* ist ein weiteres Beispiel für eine Funktion ***höherer Ordnung***: Sie nimmt als Argument eine Funktion (*succ*) und gibt als Ergebnis eine Funktion (f) zurück. Mit Hilfe von *peano-pattern* können wir *power* usw. sehr viel kürzer aufschreiben.

[8] Die Gaußklammer $\lfloor x \rfloor$ (engl. floor function) bezeichnet die größte ganze Zahl, die kleiner oder gleich der reellen Zahl x ist, siehe Anhang B.5.2.

```
let power (x,  n) = (peano-pattern (1, fun s → x * s)) n
let mul   (m, n) = (peano-pattern (0, fun s → n + s)) m
let add   (m, n) = (peano-pattern (n, fun s → 1 + s)) m
```

Der aktuelle Parameter für *succ* wird jeweils durch eine anonyme Funktion spezifiziert. Man sieht sehr schön, wie jeweils die Teillösung *s* (wie *s*olution) zu einer Gesamtlösung erweitert wird. Die rechten Seiten der Funktionsdefinitionen sind eine weitere Betrachtung wert; wir finden jeweils eine *geschachtelte* Funktionsapplikation vor: im Fall von *power* zum Beispiel $(e\ e_1)\ e_2$ mit e = *peano-pattern*, $e_1 = (1, \textbf{fun}\ s \to x * s)$ und $e_2 = n$. Aus den Typen der Ausdrücke lässt sich ablesen, dass $e\ e_1$ in der Tat zu einer Funktion auswertet; die resultierende Funktion wird dann auf e_2 angewendet.

Die Arbeitsweise von *peano-pattern* lässt sich veranschaulichen, wenn man die treibende Kraft der Rekursion, die natürliche Zahl *n*, in »unärer Form« schreibt, als wiederholte Anwendung der Nachfolgerfunktion auf die Zahl Null.

$$\begin{array}{c} 1 + (1 + (1 + (\cdots(1 + (1 + 0))\cdots))) \\ \Big\downarrow \textit{peano-pattern}\ (\textit{zero}, \textit{succ}) \\ \textit{succ}\ (\textit{succ}\ (\textit{succ}\ (\cdots(\textit{succ}\ (\textit{succ}\ \textit{zero}))\cdots))) \end{array}$$

Die Zahl 0 wird sozusagen durch *zero* ersetzt (so erklärt sich der Name des Parameters) und jeder Aufruf der Nachfolgerfunktion durch *succ* (daher die Wahl des Bezeichners). Zum Beispiel wird im konkreten Fall der Potenzfunktion 0 durch 1 und *succ n* durch das Produkt mit der Basis $x * n$ ersetzt.

$$\begin{array}{c} 1 + (1 + (1 + (1 + (1 + (1 + 0))))) \\ \Big\downarrow \textit{peano-pattern}\ (1, \textbf{fun}\ n \to x * n) \\ x * (x * (x * (x * (x * (x * 1))))) \end{array}$$

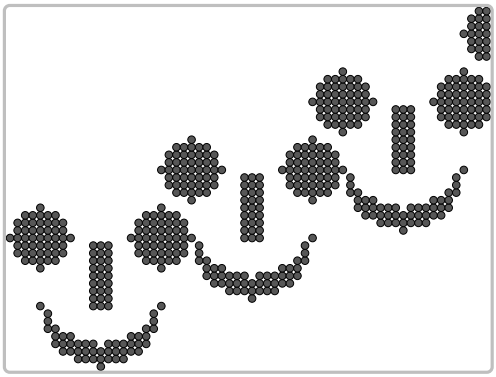
Ganz perfekt ist die Umsetzung des Entwurfsmusters allerdings nicht. Bei der Angabe der Parameterliste haben wir $\textit{zero} : \textit{Nat}$ und $\textit{succ} : \textit{Nat} \to \textit{Nat}$ spezifiziert. Diese Festlegung ist relativ willkürlich, genausogut könnten die Argumente auf Wahrheitswerten operieren, $\textit{zero} : \textit{Bool}$ und $\textit{succ} : \textit{Bool} \to \textit{Bool}$, oder auf Rastergrafiken!

```
let generate (zero : Raster, succ : Raster → Raster) : Nat → Raster =
  let rec f (n : Nat) : Raster =
        if n = 0 then zero
                 else succ (f (n – 1))
  in  f
```

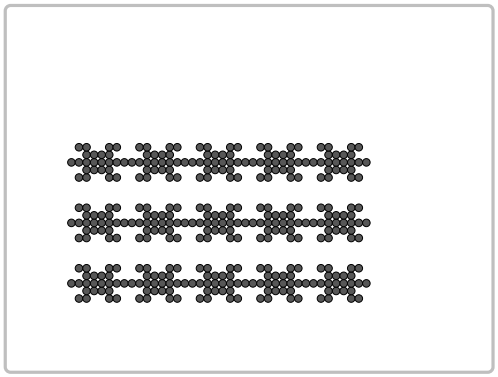
(Wir haben die Funktion *peano-pattern* in *generate* umbenannt, damit wir die ursprüngliche Definition nicht verschatten.) Mit Hilfe dieser Variante können wir zum Beispiel Rastergrafiken vervielfältigen, mehrere Kopien eines Bildes neben- oder übereinander platzieren. Die abgeleitete Funktion *spread* verallgemeinert diese Idee etwas:

```
let spread (n : Nat) (dx : Int, dy : Int) (f : Raster) : Raster =
  generate (white, fun g → f ^|^ move (dx, dy) g) n
```

Ausgehend vom leeren, weißen Bild wird in jedem Schritt die Zwischenlösung um den angegebenen Versatz verschoben, *move* $(dx, dy)\ g$, und dann das zu vervielfältigende Bild hinzugefügt, $f \mathbin{\hat{}|\hat{}} \cdots$.



move (12, 12) *smileys*



move (8, 8) *block*

Das zweidimensionale Layout des Asteriskus ✱ (siehe Aufgabe 3.5.3) — die Grafik erinnert etwas an »Space Invaders« — wird mit einem geschachtelten Aufruf von *spread* erzeugt.

```
let smileys = spread 4 (20, 9) smiley
let block =
  spread 3 (0, 8) (
    spread 5 (8, 0) asteriskus)
```

Die Ausführungen verdeutlichen, dass die Funktion *peano-pattern* eigentlich für beliebige Typen funktioniert: $zero : t$ und $succ : t \to t$. Und in der Tat, bei der Besprechung des Entwurfsmusters haben wir uns auf keinen bestimmten Typ kapriziert. Dieses Manko in der Umsetzung können wir mit unseren bisherigen Sprachmitteln nicht beheben; wir kommen aber später in Abschnitt 4.3.2 darauf zurück. Es gibt noch ein weiteres Manko, das die Ausdruckskraft von *peano-pattern* betrifft: Nicht alle bisher betrachteten Funktionen lassen sich damit definieren. Ein Negativbeispiel ist die Fakultätsfunktion. Versuchen Sie es einmal. Aufgabe 3.7.5 geht der Ursache auf den Grund und weist einen Ausweg.

3.7.2. Leibniz Entwurfsmuster

module Values.Leibniz

Eine Funktion, die mit Hilfe des Peano Entwurfsmusters erstellt oder die direkt mit Hilfe von *peano-pattern* definiert wurde, benötigt für die Lösung eines Problems n rekursive Aufrufe. Das Problem für n wird auf das Problem für $n \div 1$ zurückgeführt, dieses wird auf das Problem für $n \div 2$ zurückgeführt usw. Ist diese Vorgehensweise zwingend? Keineswegs. Wir können zum Beispiel alternativ versuchen, das Problem für n auf das Problem für $n \div 2$ zurückzuführen, also in jedem Schritt n zu halbieren. Das heißt umgekehrt, dass wir aus einer Lösung für $n \div 2$ eine Lösung für n ableiten müssen. Bevor wir loslegen, sei daran erinnert, dass »÷« die Division auf den natürlichen Zahlen bezeichnet: $4 \div 2 = 2$ und $5 \div 2 = 2$. Programmieren wir die Potenzfunktion neu.

```
let rec power (x : Nat, n : Nat) : Nat =
  if n = 0 then …
           else … power (x, n ÷ 2) …
```

Können wir aus $x^{n \div 2}$ das gewünschte Ergebnis x^n ableiten? Ja, dazu greifen wir auf die Divisionsregel $n = (n \div 2) \cdot 2 + (n \,\%\, 2)$ (3.1) und etwas Schulmathematik zurück (Potenzgesetze).

$$x^n = x^{(n \div 2) \cdot 2 + (n \% 2)} = (x^{n \div 2})^2 * x^{n \% 2}$$

Wir müssen *power* $(x, n \div 2)$ quadrieren und das Ergebnis mit $x^{n \% 2}$ multiplizieren. Dieser Faktor ist entweder 1 oder x, je nachdem, ob n gerade ($n \,\%\, 2 = 0$) oder ungerade ($n \,\%\, 2 = 1$) ist.

$$\begin{array}{l}\textbf{\textit{let rec}}\ power\ (x : Nat, n : Nat) : Nat = \\ \quad \textbf{\textit{if}}\ n = 0\ \textbf{\textit{then}}\ 1 \\ \qquad \textbf{\textit{else if}}\ n\,\%\,2 = 0\ \textbf{\textit{then}}\ square\ (power\ (x, n \div 2)) \\ \qquad\qquad \textbf{\textit{else}}\ square\ (power\ (x, n \div 2)) * x\end{array}$$

Wieviele rekursive Aufrufe benötigt $power\ (x, n)$ jetzt? In jedem Schritt wird n halbiert; das können wir insgesamt $\lg n$ mal machen.[9] Möchte man die Anzahl der Rechenschritte nur grob klassifizieren, so sagt man, *power* hat eine ***logarithmische Laufzeit***, im Unterschied zur ersten Version, die eine ***lineare Laufzeit*** hat. Die folgende Tabelle zeigt, dass Programme mit logarithmischer Laufzeit einen erheblichen Geschwindigkeitsvorteil gegenüber Programmen mit linearer Laufzeit haben.

n	$\lg n$
100	$\approx 6,6$
1.000	$\approx 10,0$
10.000	$\approx 13,3$
100.000	$\approx 16,6$
1.000.000	$\approx 20,0$

Für eine Million Elemente ist die binäre Herangehensweise also 50.000 mal schneller als die lineare Implementierung der Potenzfunktion. Natürlich ist das nur eine Abschätzung; für eine präzise Aussage müsste man die tatsächliche Anzahl der Rechenschritte ermitteln. Da uns der binäre Logarithmus wiederholt begegnen wird, lohnt es sich die Tabelle einzuprägen. Dazu reicht ein Fakt, $\lg 1.000 \approx 10,0$, und eine Formel, $\lg(a \cdot b) = \lg a + \lg b$. Zum Beispiel ist $\lg 1.000.000 = 2 \cdot \lg 1.000 \approx 20,0$. Die Approximation ist recht ordentlich, da $2^{10} = 1.024$.

Mit dem gleichen Entwurfsmuster lässt sich auch die Multiplikation verbessern.

$$m * n = (2 * (m \div 2) + (m\,\%\,2)) * n = 2 * ((m \div 2) * n) + (m\,\%\,2) * n$$

Jetzt müssen wir die Teillösung verdoppeln und gegebenenfalls n addieren.

$$\begin{array}{l}\textbf{\textit{let rec}}\ mul\ (m : Nat, n : Nat) : Nat = \\ \quad \textbf{\textit{if}}\ m = 0\ \textbf{\textit{then}}\ 0 \\ \qquad \textbf{\textit{else if}}\ m\,\%\,2 = 0\ \textbf{\textit{then}}\ 2 * mul\ (m \div 2, n) \\ \qquad\qquad \textbf{\textit{else}}\ 2 * mul\ (m \div 2, n) + n\end{array}$$

Es ist übrigens wichtig, dass wir das Ergebnis verdoppeln, nicht etwa die Rechnung: Der Ausdruck $mul\ (m \div 2, n) + mul\ (m \div 2, n)$ würde $mul\ (m \div 2, n)$ zweimal ausrechnen und damit den Geschwindigkeitsvorteil wieder zunichte machen.

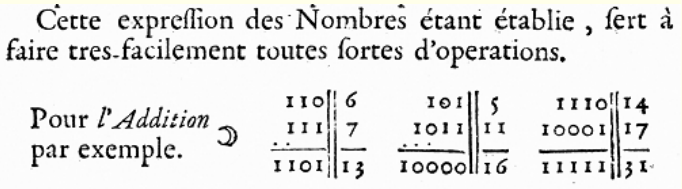
Die obige Implementierung der Multiplikation ist sehr hardware-nah; ähnlich geht auch der Computer vor — die Operationen $e*2$, $e \div 2$, $e\%2$ sind sehr leicht in Hardware zu implementieren, da die Arithmetik eines Computers auf dem sogenannten ***Dualsystem*** basiert. Mehr dazu später aus der Technischen Abteilung der Informatik (siehe auch Abschnitt 4.2.2 und Anhang B.5.3).

Auch dem neuen Entwurfsmuster geben wir einen Namen: ***Leibniz Entwurfsmuster*** nach dem deutschen Universalgelehrten Gottfried Wilhelm Leibniz, der unter anderem das Dualsystem entwickelt hat, siehe Abbildung 3.7.

[9] Mit lg wird der ***binäre Logarithmus*** bezeichnet: $\lg x = \log_2 x$.

Gottfried Wilhelm Leibniz war ein deutscher Philosoph, Wissenschaftler, Mathematiker, Diplomat, Physiker, Historiker, Bibliothekar und Doktor des weltlichen und des Kirchenrechts. Er gilt als der universale Geist seiner Zeit und war einer der bedeutendsten Philosophen des ausgehenden 17. und beginnenden 18. Jahrhunderts.

Auszug aus »Explication de l'Arithmétique Binaire« [Lei03]:


Cette expreſſion des Nombres étant établie, ſert à faire tres-facilement toutes ſortes d'operations.

Pour *l'Addition* par exemple.

110	6		101	5		1110	14
111	7		1011	11		10001	17
1101	13		10000	16		11111	31

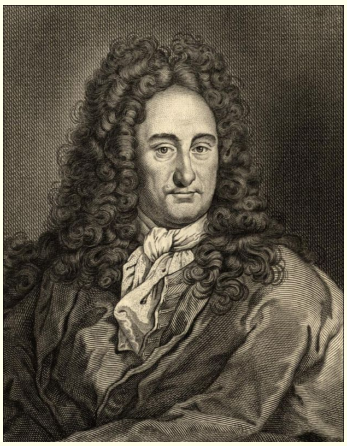


Abbildung 3.7.: Gottfried Wilhelm Leibniz (1646–1716).

Leibniz Entwurfsmuster

```
let rec f (n : Nat) : t =
  if n = 0 then ...                    Rekursionsbasis
           else ... f (n ÷ 2) ...      Rekursionsschritt
```

Versuchen wir das Leibniz Entwurfsmuster auf die Wurzelfunktion anzuwenden. Können wir aus $\lfloor\sqrt{n \div 2}\rfloor$ das gewünschte Ergebnis $\lfloor\sqrt{n}\rfloor$ ableiten? Vielleicht, unmittelbar drängt sich jedoch keine Lösung auf. Nun ist es nicht zwingend durch zwei zu dividieren, die Zerlegung $n = (n \div b) * b + (n \,\%\, b)$ gilt für jedes beliebige $b > 0$. Für unser Problem ist eine Quadratzahl, zum Beispiel vier, eine geschickte Wahl. Da weiterhin $2\lfloor\sqrt{n \div 4}\rfloor$ und $\lfloor\sqrt{n}\rfloor$ höchstens um eins differieren (Aufgabe 3.7.2 fragt nach einem Beweis), können wir unsere ursprüngliche Lösung einfach adaptieren.

```
let rec square-root (n : Nat) : Nat =
  if n = 0 then 0
           else let r = 2 * square-root (n ÷ 4)
                in if n < square (r + 1) then r else r + 1
```

Diese Implementierung ist schon recht ordentlich, einzig die in jedem Rekursionsschritt durchgeführte Multiplikation bremst das Programm etwas aus — unser Rechenmodell setzt für eine Multiplikation einen Rechenschritt an, Multiplikationen sind aber teure Operationen in Hardware. Fürs Erste haben wir genug Arithmetik betrieben; wenden wir uns spielerischen Dingen zu.

3.7.3. Projekt: Lineare und binäre Suche

Programmieren wir ein kleines Spiel: Spieler A denkt sich eine Zahl aus, höchstens sechsstellig, die Spielerin B erraten muss. Spielerin B darf dazu Fragen der Form »Ist die gesuchte Zahl gleich oder kleiner als 815?« stellen, die Spieler A wahrheitsgemäß beantworten muss. Unsere Aufgabe ist es, die Logik von Spielerin B zu entwerfen und zu implementieren.

module Values.Game

Bevor wir mit der Programmierung beginnen, müssen wir uns zunächst Gedanken über die Schnittstelle machen. Spieler A muss zu einem gegebenen n Auskunft geben, ob die gesuchte Zahl gleich oder kleiner als n ist. Wir können ihn somit durch eine Funktion des Typs $Nat \to Bool$ repräsentieren, ein sogenanntes ***Orakel***. Zum Beispiel:

```
let player-A (guess : Nat) : Bool = 4711 ⩽ guess
```

Das Orakel machen wir Spielerin B bekannt, die somit durch eine Funktion höherer Ordnung des Typs $(Nat \to Bool) \to Nat$ implementiert wird: Ein Orakel wird abgebildet auf die gesuchte Zahl. Die Repräsentation des Orakels stellt dabei sicher, dass keine der beteiligten Parteien mogelt: Die gesuchte Zahl ist fest verdrahtet — Spieler A kann sie nicht nachträglich ändern — kann aber auch nicht eingesehen werden — Spielerin B kann das Orakel nur auf eine Zahl anwenden und aus dem Ergebnis ihre Schlüsse ziehen.

Kommen wir zur Logik von Spielerin B. Wir können systematisch alle Zahlen beginnend mit 0 durchprobieren, bis das Orakel eine positive Antwort liefert.

```
let player-B (oracle : Nat → Bool) : Nat =
  let rec search (n : Nat) : Nat =
    if oracle n then n
                else search (n + 1)
  in search 0
```

Dieser Ansatz sieht dem Peano Entwurfsmuster ähnlich, ist es aber nicht: Um das Problem für n zu lösen, wird auf die Lösung für $n+1$ zurückgegriffen! Auch die Rekursionsbasis ist nicht erkennbar. Ein mulmiges Gefühl ist in der Tat angebracht. Der Funktionsaufruf *player-B* (***fun*** $k \to$ *false*) hat keinen Wert. Der Aufruf *search* 0 führt zum Aufruf *search* 1, dieser zu *search* 2 usw. Man sagt auch, dass Programm ***terminiert nicht***. Die Semantik ordnet dem Aufruf entsprechend keinen Wert zu. Um einen Beweisbaum für *search* 0 zu konstruieren, benötigen wir einen Beweisbaum für *search* 1; für die Konstruktion dieses Beweisbaums benötigen wir einen Beweisbaum für *search* 2 usw. Ein unendlicher Regress.

Mit dem Konstrukt der Rekursion haben wir uns das Problem der Nichtterminierung eingehandelt. An dieser Stelle kommt wieder das Peano Entwurfsmuster ins Spiel. Es bändigt die Rekursion und stellt insbesondere die Terminierung sicher: Das Problem für n wird auf das Problem für $n \dot{-} 1$ zurückgeführt; irgendwann wird auf diese Weise der Basisfall $n = 0$ erreicht. Auf unser Beispiel übertragen heißt das, dass wir die Suche nach oben beschränken müssen. In der Aufgabenstellung war von einer höchstens sechsstelligen Zahl die Rede, also müssen wir nur die Zahlen bis maximal 999.999 abklappern. Um das Programm flexibel zu halten, parametrisieren wir *player-B* mit der oberen sowie der unteren Grenze des Suchintervalls.

```
let player-B (oracle : Nat → Bool,
              lower : Nat, upper : Nat) : Nat =
  let rec search (n : Nat) : Nat =
    if n = upper then upper
                 else if oracle n then n
                                  else search (n + 1)
  in search lower
```

Was machen wir, wenn die Suche die obere Grenze erreicht hat? Wir geben einfach die Grenze selbst zurück — im Vertrauen darauf, dass Spieler A nicht mogelt und sich tatsächlich eine Zahl im Suchintervall ausgedacht hat.

Terminiert die neue Version von *player-B stets*? Vielleicht. Wir können ganz sichergehen, indem wir das Peano Entwurfsmuster beherzigen und nicht über den Ratekandidaten selbst rekurrieren, sondern über den *Abstand* des Kandidaten zur oberen Schranke.

```
let player-B (oracle : Nat → Bool,
              lower : Nat, upper : Nat) : Nat =
  let rec search (d : Nat) : Nat =
    if d = 0 then upper
             else if oracle (upper ∸ d) then upper ∸ d
                                        else search (d ∸ 1)
  in search (upper ∸ lower)
```

Voilà. Die Terminierung ist sichergestellt. Die Terminierung der ursprünglichen Version damit auch? Leider nein! Diese weicht in einem kleinen Detail ab. Der Aufruf *player-B* (**fun** $k \to 2 \leqslant k, 9, 0$) terminiert zum Beispiel nicht. Die »untere« Schranke liegt über der »oberen«, somit wertet der Test $n = \mathit{upper}$ nie zu wahr aus. Glücklicherweise ist das einfach zu reparieren: Wir ersetzen den Test $n = \mathit{upper}$ durch $n \geqslant \mathit{upper}$. In der letzten Version von *player-B* wird dieser Fall automatisch mitbehandelt, da $\mathit{upper} \dot{-} \mathit{lower}$ zu 0 auswertet, wenn die untere Schranke über der oberen liegt. (Zur Erinnerung: »$\dot{-}$« ist »monus«, die Subtraktion auf den natürlichen Zahlen, nicht »minus«.)

Einstweiliges Fazit: nie ohne guten Grund von den Entwurfsmustern abweichen! Programmierfehler sind oft sehr subtil und aus einem Programmierfehler wird heutzutage schnell ein »Sicherheitsloch«.

Probieren wir das Programm aus.

```
⋙ player-B (player-A, 0, 999.999)
4711
⋙ player-B (fun k → 815 ⩽ k, 0, 999)
815
```

Es klappt! Werden wir etwas wagemutiger: Spieler A kann sich natürlich auch eine Zahl ausdenken, die durch eine Formel gegeben ist.

```
⋙ player-B (fun k → 815 < square (k + 1), 0, 999)
28
```

Jetzt hat Spielerin B die natürliche Quadratwurzel von 815 bestimmt: $28^2 = 784 \leqslant 815 < 841 = 29^2$. Diese Erkenntnis können wir als Programm festhalten.

```
let square-root (n : Nat) : Nat =
  linear-search ((fun k → n < square (k + 1)), 0, n)
```

Da aus der Implementierung eines Spiels ein Programmstück von allgemeinem Nutzen geworden ist, haben wir *player-B* in *linear-search* umbenannt. Der Name charakterisiert die Suchstrategie: Das Suchintervall wird linear von links nach rechts durchforstet. (Da alle Elemente nacheinander betrachtet werden, heißt der Algorithmus im Englischen auch *British Museum Search*.) Im schlimmsten Fall benötigt *linear-search* n rekursive Aufrufe, durchschnittlich werden immerhin noch $n \div 2$ Rekursionsschritte benötigt.

Können wir die Laufzeit mit Hilfe des Leibniz Entwurfsmusters verbessern? Das Entwurfsmuster sieht vor, den Parameter, in unserem Fall die Größe des Suchintervalls (l, u), in jedem Rekursionsschritt zu halbieren. Die Mitte des Suchintervalls ist durch $m = l + (u \dot{-} l) \div 2$ oder gleichwertig durch $m = (l + u) \div 2$ gegeben (falls $l \leqslant u$). Welche Schlüsse können wir aus der Befragung des Orakels an der Stelle m ziehen? Wertet der Aufruf *oracle* m zu wahr aus — die gesuchte Zahl ist gleich oder kleiner als die geratene — dann müssen wir im Intervall (l, m) suchen, anderenfalls muss die gesuchte Zahl im Intervall $(m + 1, u)$ liegen. Der Basisfall ist erreicht, wenn die untere und die obere Intervallgrenze zusammenfallen.

```
let binary-search (oracle : Nat → Bool,
                   lower : Nat, upper : Nat) : Nat =
  let rec search (l : Nat, u : Nat) : Nat =
    if l ⩾ u then u
             else let m = (l + u) ÷ 2
                  in if oracle m then search (l,     m)
                                 else search (m + 1, u)
  in search (lower, upper)
```

Es ist lehrreich, sich die Abfolge der Rateversuche anzuschauen. Zu diesem Zweck lassen wir Spieler A die geratenen Zahlen am Bildschirm ausgeben. (Wir greifen hier etwas vor: Ausgaben werden erst in Abschnitt 7.1 besprochen, da es sich um einen Effekt handelt.)

```
let player-A (guess : Nat) : bool =
  putline ("Geratene Zahl: " ^ show guess)
  4711 ⩽ guess
```

Die Funktion *putline* gibt einen String auf dem Bildschirm aus; *show* wandelt eine natürliche Zahl in einen String um und »^« konkateniert zwei Strings.

Testen wir die Implementierung mit der instrumentierten Version von *player-A*.

```
⋙ binary-search (player-A, 0, 999999)
Geratene Zahl : 499999
Geratene Zahl : 249999
Geratene Zahl : 124999
Geratene Zahl : 62499
Geratene Zahl : 31249
Geratene Zahl : 15624
Geratene Zahl : 7812
Geratene Zahl : 3906
Geratene Zahl : 5859
Geratene Zahl : 4883
Geratene Zahl : 4395
Geratene Zahl : 4639
Geratene Zahl : 4761
Geratene Zahl : 4700
Geratene Zahl : 4731
Geratene Zahl : 4716
Geratene Zahl : 4708
Geratene Zahl : 4712
Geratene Zahl : 4710
Geratene Zahl : 4711
4711
```

Die gesuchte Zahl wird systematisch eingekreist; nach 20 Versuchen ist sie erraten.

Mit der verbesserten Suchstrategie lässt sich auch *square-root* auf eine logarithmische Laufzeit beschleunigen.

```
let square-root (n : Nat) : Nat =
  binary-search ((fun k → n < square (k + 1)), 0, n)
```

Fassen wir zusammen: Das gleiche Problem lässt sich auf verschiedene Art und Weise lösen. Hier liegt die kreative gedankliche Leistung der Programmiererin oder des Programmierers. Die Entwurfsmuster helfen einen ersten Ansatz systematisch zu entwickeln. Beiden Entwurfsmustern ist gemeinsam, dass Probleme auf Teilprobleme reduziert werden. Programmieren wir eine rekursive Funktion »freihändig«, müssen wir selbst darauf achten, dass die Parameter der rekursiven Aufrufe kleiner werden, so dass die Terminierung sichergestellt ist. Und noch einmal: Programmierfehler sind oft sehr subtil und aus einem Programmierfehler wird heutzutage schnell ein »Sicherheitsloch«.

Schauen wir uns die Funktion *binary-search* noch einmal durch die Terminierungsbrille an. Die Intervallgröße muss stets schrumpfen: Im Rekursionsschritt wird ein Intervall der Größe $n = r \dot{-} l + 1$ in zwei Intervalle der Größen $(n+1) \div 2$ und $n \div 2$ unterteilt — es gilt stets $n = (n+1) \div 2 + n \div 2$. Nun ist $(n+1) \div 2$ nur echt kleiner als n, wenn n echt größer als 1 ist. Das bedeutet, dass $n = 1$ nicht im Rekursionsschritt behandelt werden darf, sondern neben $n = 0$ einen weiteren Basisfall darstellt. Im Programm fängt der Test $l \geqslant r$ beide Basisfälle ab; im Rekursionsschritt werden nur Suchintervalle behandelt, die mindestens zwei Elemente umfassen.

Übungen.

Das Symbol »🧠« kennzeichnet schwierige Aufgaben.

1. Folgt die folgende Version der Potenzfunktion

```
let power (x : Nat, n : Nat) : Nat =
  if n = 0 then 1
           else if n % 2 = 0 then power (x * x, n ÷ 2)
                             else power (x * x, n ÷ 2) * x
```

dem Leibniz Entwurfsmuster?

🧠 **2.** Die nach den Entwurfsmustern konstruierten Implementierungen von *square-root* beruhen auf den folgenden Eigenschaften:

(a) $0 \leqslant \lfloor\sqrt{n}\rfloor - \lfloor\sqrt{n-1}\rfloor \leqslant 1$ für alle $n > 0$,

(b) $0 \leqslant \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\sqrt{n \div 4}\rfloor \leqslant 1$ für alle $n \geqslant 0$.

Zeigen Sie die Eigenschaften.

⌨ **3.** Programmieren Sie zwei Funktionen *even* : *Nat* → *Bool* und *odd* : *Nat* → *Bool*, die bestimmen, ob eine Zahl gerade bzw. ungerade ist. Geben Sie für jede Funktion zwei verschiedene Definitionen an:

- Gehen Sie einmal *streng* nach dem Peano Entwurfsmuster vor.
- Programmieren Sie »freihändig« unter Zuhilfenahme der Operatoren ÷ und %.

⌨ **4.** Schreiben Sie eine rekursive Funktion, die die Quersumme einer Zahl ermittelt.

5. Warum kann man die Funktion *factorial* nicht mit Hilfe von *peano-pattern* definieren? Lässt sich die Funktion *peano-pattern* erweitern, so dass dies möglich wird?

⌨ **6.** Die Funktion *binary-search* setzt voraus, dass die Größe des zu untersuchenden Bereichs bekannt ist. Natürlich gibt es auch Fälle, in denen der Suchbereich vorher nicht eingeschränkt werden kann. In diesem Fall muss zunächst die obere Grenze des Suchintervalls bestimmt werden. Diese Aufgabe übernimmt die Funktion *exponential-search*: In exponentiell wachsenden Schritten (1, 2, 4, 8, 16, 32 …) wird der Bereich bestimmt, in dem das gesuchte Element liegen muss. Nachdem das Suchintervall gefunden wurde, kann dieses mit der Funktion *binary-search* durchsucht werden. Implementieren Sie die Funktion *exponential-search*.

Zusammenfassung und Anmerkungen

DIY: Zusammenfassung

Mini–F# ist erwachsen geworden — am Ende dieses Kapitels verfügen wir über eine berechnungsuniverselle Programmiersprache, mit der wir die prinzipiellen Möglichkeiten eines Rechners ausschöpfen können. Probleme, die sich durch Rechengesetze erfassen lassen, können mit Mini–F# gelöst werden. Einige, wenige Zutaten genügen: *Natürliche Zahlen und Wahrheitswerte*, um Daten zu repräsentieren; *Definitionen*, um Rechnungen zu modularisieren und Mehrfachrechnungen zu vermeiden; *Funktionen*, um unser Problemlösungsvokabular zu vergrößern; und *Rekursion*, um Probleme auf die Lösung kleinerer Probleme zurückzuführen.

Rekursion birgt die Gefahr der Nichtterminierung; *Entwurfsmuster* bannen diese Gefahr und unterstützen den/die Programmierer/-in bei der systematischen Lösung von Problemen.

Die Bedeutung der Sprachkonstrukte wird normativ durch *statische* und *dynamische Semantik* festgelegt. Die Zweiklassengesellschaft der Programmierung: Typen klassifizieren Ausdrücke und Werte. Die statische Semantik formalisiert die Klassifikation mit Hilfe von *Typregeln*. Die dynamische Semantik beschreibt die Dynamik des Rechenprozesses. *Auswertungsregeln* detaillieren, wie ein Ausdruck zu einem Wert ausgerechnet wird.

4. Datentypen⧹Rechnen mit Daten

I think that I shall never see
A poem lovely as a tree.

— Joyce Kilmer (1886–1918), *Trees*

Informatikerinnen und Informatiker bilden Modelle der Wirklichkeit; einen nicht unwesentlichen Teil dieser Modelle machen Daten aus. Daten repräsentieren alles Wissenswerte über einen Weltausschnitt, alles was für die jeweilige Anwendung relevant ist oder relevant erscheint. So werden aus Personen Stammdaten, aus An- und Verkäufen Börsendaten, aus Wolken Luftströmungen und aus pittoresken Sonnenuntergängen Wetterdaten.

Modellbildung ist immer Vereinfachung, Beschränkung und Abstraktion. Für die Verwaltung eines Unternehmens wird zum Beispiel eine Mitarbeiterin oder ein Mitarbeiter auf einige wenige Angaben reduziert. In der Regel werden Name, Geburtsdatum, Geschlecht und Familienstand erfasst; vielleicht die Dauer des Beschäftigungsverhältnisses oder die Stellung im Unternehmen; eher unwahrscheinlich ist die Erfassung von Statur, Bekannten- oder Freundeskreis oder des Lieblingsrestaurants.

In diesem Kapitel beschäftigen wir uns damit, wie man Daten strukturiert und verarbeitet. Die Modellbildung selbst wird dabei eine eher untergeordnete Rolle spielen. Zu diesem Thema erfahren Sie im weiteren Verlauf des Studiums mehr aus der Abteilung »Software Engineering«. (Wir beschäftigen uns im Wesentlichen mit der »Programmierung im Kleinen«; die »Programmierung im Großen« streifen wir nur gelegentlich, siehe aber Kapitel 8.) Unser bisheriges Repertoire an Datentypen ist bescheiden: Wir haben Boolesche Werte, natürliche Zahlen, Funktionen und Zeichenketten im Angebot. Was uns fehlt, sind Möglichkeiten

- mehrere Daten zu einem Datum[1] zusammenzufassen: etwa einen Straßennamen, eine Postleitzahl und einen Ortsnamen zu einer Adresse;
- mehrere alternative Angaben als Einheit zu behandeln: etwa den Familienstand mit den Alternativen ledig, verheiratet mit Angabe des Datums der Trauung oder geschieden ebenfalls mit Datumsangabe.

Wenn größere Datenmengen zusammengefasst werden, wird die Frage interessant, wie bequem oder auch wie schnell man auf ein einzelnes Datum zugreifen kann. Die Organisation von Daten tritt in den Vordergrund: Aus Daten werden Datenstrukturen. Zwei grundlegende Datenstrukturen lernen wir ebenfalls in diesem Kapitel kennen: Listen und Arrays.

4.1. Records

4.1.1. Binäre Tupel⧹Paare

Mit Hilfe der Alternative können wir von zwei gegebenen Zahlen einfach das Minimum (die kleinere Zahl) und das Maximum (die größere Zahl) bestimmen.

[1] Datum ist der Singular von Daten.

$$\textbf{\textit{let}}\ \mathit{minimum}\ (a : \mathit{Nat}, b : \mathit{Nat}) = \textbf{\textit{if}}\ a \leqslant b\ \textbf{\textit{then}}\ a\ \textbf{\textit{else}}\ b$$
$$\textbf{\textit{let}}\ \mathit{maximum}\ (a : \mathit{Nat}, b : \mathit{Nat}) = \textbf{\textit{if}}\ a \leqslant b\ \textbf{\textit{then}}\ b\ \textbf{\textit{else}}\ a$$

Benötigen wir beide Informationen auf einen Schlag — das heißt, wollen wir die Argumente a und b der Größe nach ordnen — müssen wir ein ***Paar*** von Zahlen zurückgeben.

$$\textbf{\textit{let}}\ \mathit{sort2}\ (a : \mathit{Nat}, b : \mathit{Nat}) : \mathit{Nat} * \mathit{Nat} =$$
$$\quad \textbf{\textit{if}}\ a \leqslant b\ \textbf{\textit{then}}\ (a, b)\ \textbf{\textit{else}}\ (b, a)$$

Paare erlauben es uns, Daten zu aggregieren, zwei verschiedene Daten als Einheit zu behandeln. Die zwei Komponenten eines Paares müssen nicht den gleichen Typ besitzen: $(\texttt{"Lisa"}, 9)$ vom Typ $\mathit{String} * \mathit{Nat}$ fasst zum Beispiel einen String und eine natürliche Zahl zusammen, etwa Name und Alter einer Person; $(7, \textbf{\textit{fun}}\ (i : \mathit{Nat}) \to 2 * i)$ vom Typ $\mathit{Nat} * (\mathit{Nat} \to \mathit{Nat})$ aggregiert eine natürliche Zahl und eine Funktion und repräsentiert vielleicht eine endliche Abbildung.

Paare sind tatsächlich kein neues Konzept; sie sind uns schon in einem früheren Abschnitt begegnet, nämlich als Argumente von Funktionen. Wir haben uns bisher auf den Standpunkt gestellt, dass Funktionen wie *minimum* und *maximum* zwei Argumente erhalten (a und b). Eine alternative Sichtweise ist, dass Funktionen stets genau ein Argument verarbeiten, im Fall von *minimum* und *maximum* ist dieses eine Argument eben das Paar (a, b). Da die zweite Sichtweise vorteilhafter ist, werden wir sie uns zu eigen machen. Mehr zu diesem Thema im Abschnitt 4.1.2.

Zurück zu unserem einleitenden Beispiel: Wir haben die Funktion *sort2* »von Grund auf« neu programmiert; alternativ können wir bei der Definition auf *minimum* und *maximum* zurückgreifen.

$$\textbf{\textit{let}}\ \mathit{sort2}\ (a : \mathit{Nat}, b : \mathit{Nat}) : \mathit{Nat} * \mathit{Nat} = (\mathit{minimum}\ (a, b), \mathit{maximum}\ (a, b))$$

Der Programmtext ist etwas kürzer, hat aber den kleinen Nachteil, dass beim Ausrechnen *zwei* Alternativen abgearbeitet werden müssen.

Lassen sich umgekehrt *minimum* und *maximum* auch mit Hilfe von *sort2* programmieren? Ja! So geht's:

$$\textbf{\textit{let}}\ \mathit{minimum}\ (a : \mathit{Nat}, b : \mathit{Nat}) : \mathit{Nat} = \mathit{fst}\ \ (\mathit{sort2}\ (a, b))$$
$$\textbf{\textit{let}}\ \mathit{maximum}\ (a : \mathit{Nat}, b : \mathit{Nat}) : \mathit{Nat} = \mathit{snd}\ (\mathit{sort2}\ (a, b))$$

Ist e ein Ausdruck, der zu einem Paar auswertet, so kann mit $\mathit{fst}\ e$ auf die erste und mit $\mathit{snd}\ e$ auf die zweite Komponente zugegriffen werden. Die alternativen Definitionen von *minimum* und *maximum* sind ebenfalls etwas prägnanter, haben aber den kleinen Nachteil, dass *sort2* ein Paar konstruiert, von dem stets nur eine Komponente benötigt wird.

Im Folgenden formalisieren wir Syntax und Semantik von Paaren oder 2-Tupeln. Alle Konstrukte verallgemeinern sich in natürlicher Weise auf ***Tupel***, Aggregationen von n verschiedenen Komponenten. In den Beispielprogrammen werden wir ausgiebig Gebrauch von Tupeln machen.

Abstrakte Syntax Wir erweitern Ausdrücke um Sprachkonstrukte, die Paare konstruieren und analysieren.

$e ::= \cdots$	***Paarausdrücke:***
$\mid (e_1, e_2)$	Konstruktion\Paarbildung
$\mid \mathit{fst}\ e$	Projektion auf die erste Komponente
$\mid \mathit{snd}\ e$	Projektion auf die zweite Komponente

Die Ausdrücke e_1 und e_2 heißen ***Komponenten*** des Paares (e_1, e_2).

Statische Semantik Im Typ eines Paares wird festgehalten, von welchem Typ die Komponenten sind. Mit anderen Worten, der Typ eines Paares ist ein Paar von Typen, das sogenannte kartesische Produkt der Typen.

$t ::= \cdots$	***Typen:***
$\mid t_1 * t_2$	Paartyp

Die Typregeln für Paare sind vergleichsweise einfach: Ein Paar erhält den Paartyp $t_1 * t_2$; Projektionen erwarten einen Ausdrucks des Typs $t_1 * t_2$ und selektieren die entsprechende Komponente.

$$\frac{\Sigma \vdash e_1 : t_1 \qquad \Sigma \vdash e_2 : t_2}{\Sigma \vdash (e_1, e_2) : t_1 * t_2} \qquad \frac{\Sigma \vdash e : t_1 * t_2}{\Sigma \vdash \mathit{fst}\ e : t_1} \qquad \frac{\Sigma \vdash e : t_1 * t_2}{\Sigma \vdash \mathit{snd}\ e : t_2}$$

Dynamische Semantik Wir erweitern den Bereich der Werte um Paare von Werten.

$\nu ::= \cdots$	***Werte:***
$\mid (\nu_1, \nu_2)$	Paare

Die Auswertungsregeln folgen der statischen Semantik.

$$\frac{\delta \vdash e_1 \Downarrow \nu_1 \qquad \delta \vdash e_2 \Downarrow \nu_2}{\delta \vdash (e_1, e_2) \Downarrow (\nu_1, \nu_2)} \qquad \frac{\delta \vdash e \Downarrow (\nu_1, \nu_2)}{\delta \vdash \mathit{fst}\ e \Downarrow \nu_1} \qquad \frac{\delta \vdash e \Downarrow (\nu_1, \nu_2)}{\delta \vdash \mathit{snd}\ e \Downarrow \nu_2}$$

Bevor wir uns den Beispielprogrammen zuwenden, überlegen wir noch kurz, wie die Konstrukte und Regeln allgemein für n-Tupel aussehen.

Ist $n = 0$, so hat das Tupel keine Komponenten und entsprechend gibt es keine Projektionsfunktionen. Mit anderen Worten, der 0-Tupeltyp, genannt *Unit*, umfasst genau ein Element, nämlich $()$. Zum jetzigen Zeitpunkt ist der 0-Tupeltyp von keinem großen Nutzen; später in Kapitel 7 werden wir ihn als Platzhaltertyp verwenden: Programme, die um ihres Effektes und nicht um des Wertes willen ausgerechnet werden, geben oft »$()$« als Dummywert zurück. Aber wir greifen vor.

Im Fall $n = 1$ haben wir ein 1-Tupel und eine einzige Projektionsfunktion. Dieser Fall ist als einziger wenig sinnvoll, da anstelle des 1-Tupels stets die einzige Komponente treten kann. Dieser Fall wird auch von der konkreten Syntax nicht unterstützt, da »(e)« zur Gruppierung bzw. Klammerung von Ausdrücken dient.

Ist $n = 3$, so konstruieren wir 3-Tupel oder Tripel und analysieren diese mit Hilfe dreier Projektionsfunktionen.

Ist $n = 4$, so konstruieren wir 4-Tupel oder Quadrupel …

Vertiefung: Sortieren Die Funktion *sort2* ordnet zwei natürliche Zahlen; wie lassen sich drei natürliche Zahlen sortieren?

```
let sort3 (a : Nat, b : Nat, c : Nat) : Nat * Nat * Nat =
  if a ⩽ b then
    if b ⩽ c then (a, b, c)
             else if a ⩽ c then (a, c, b) else (c, a, b)
  else
    if a ⩽ c then (b, a, c)
             else if b ⩽ c then (b, c, a) else (c, b, a)
```

Die obige Lösung benötigt bis zu drei Vergleiche: *sort3* $(1, 3, 2)$ zum Beispiel testet zunächst $1 \leqslant 3$, dann $3 \leqslant 2$ und schließlich $1 \leqslant 2$. Gibt es eine Lösung, die mit weniger Vergleichen

auskommt? Nein! Drei Zahlen können auf 3 Fakultät Arten angeordnet werden: 3! = 6. Mit zwei ineinander geschachtelten Alternativen können aber nur vier Fälle unterschieden werden. Ergo werden im schlechtesten Fall drei Vergleiche benötigt. Gleichwohl lässt sich *sort3* etwas kompakter aufschreiben, indem wir auf *sort2* zurückgreifen.

```
let sort3 (a : Nat, b : Nat, c : Nat) : Nat * Nat * Nat =
  let x = sort2 (a, b)
  in  if snd x ⩽ c then (fst x, snd x, c)
                   else  if fst x ⩽ c then (fst x, c, snd x)
                                      else  (c, fst x, snd x)
```

Diese Version, die exakt dieselben Vergleiche durchführt wie die ursprüngliche, macht die Vorgehensweise deutlich: Zunächst werden *a* und *b* geordnet, dann wird die Position von *c* bestimmt. Je größer und umfangreicher ein Programm wird, desto wichtiger ist ein *modularer* Aufbau.

module Datatypes.Matrix

Vertiefung: Matrizen und Fibonacci-Zahlen Tupel erlauben es uns, wie schon erwähnt, mehrere Daten zu einer Einheit zusammenzufassen. Das kennen wir aus der Mathematik: Mit Hilfe von Vektoren und Matrizen können wir zum Beispiel ein System von Gleichungen als Einheit betrachten. (Abbildung 4.1 fasst die wichtigsten Fakten zu Matrizen zusammen.)

$$\begin{aligned} a_{11} \cdot x_1 + a_{12} \cdot x_2 &= b_1 \\ a_{21} \cdot x_1 + a_{22} \cdot x_2 &= b_2 \end{aligned} \qquad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

Aus dem Gleichungssystem auf der linken Seite wird eine einzelne Gleichung auf der rechten Seite. Tupel sind etwas allgemeiner als Vektoren, da die Komponenten eines Tupels nicht den gleichen Typ besitzen müssen. Somit können wir Vektoren und Matrizen mit Hilfe von Tupeln repräsentieren, zum Beispiel, 2×2-Matrizen durch 4-Tupel. Um diese Wahl zu dokumentieren, führen wir ein Typsynonym ein.

```
type Matrix = Nat * Nat * Nat * Nat          // 2 × 2-Matrizen
let unit = (1, 0, 0, 1)
let F    = (1, 1, 1, 0)
```

Dabei wird die Matrix $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ durch das Tupel $(a_{11}, a_{12}, a_{21}, a_{22})$ dargestellt. Zum Beispiel ist *unit* die Einheits- oder Identitätsmatrix, das neutrale Element der Matrizenmultiplikation. Die Matrizenmultiplikation selbst wird durch die folgende Funktion realisiert.

```
let (^*^) (a11, a12, a21, a22) (b11, b12, b21, b22) : Matrix =
  (a11 * b11 + a12 * b21, a11 * b12 + a12 * b22,
   a21 * b11 + a22 * b21, a21 * b12 + a22 * b22)
```

So wie »*« zwei Zahlen nimmt und deren Produkt zurückgibt, so nimmt »^*^« zwei Matrizen und gibt deren Produkt zurück. Da die Matrizenmultiplikation assoziativ ist, haben wir uns für Infixnotation entschieden. Dazu müssen wir bei der *Definition* den symbolischen Bezeichner in runde Klammern setzen und den Argumenten voranstellen — Infixnotation bei der *Definition*, also **let** *a* ^*^ *b* = ⋯, ist leider nicht zulässig. Infixnotation ist immer dann vorteilhaft, wenn man Operationen schachtelt oder aneinanderreiht.

```
⋙ F ^*^ F
(2, 1, 1, 1)
⋙ F ^*^ F ^*^ F ^*^ F ^*^ F ^*^ F ^*^ F ^*^ F ^*^ F ^*^ F
(89, 55, 55, 34)
```

Eine ***Matrix*** ist eine rechteckige Anordnung von Elementen, ein 2-dimensionales Array.

$$A = \begin{pmatrix} 0 & 47.11 & 0 & 0 \\ 2.765 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0.815 \end{pmatrix} \qquad \begin{aligned} A_{12} &= 47.11 \\ A_{21} &= 2.765 \end{aligned} \qquad 3 \times 4\text{-Matrix}$$

Eine solche Matrix repräsentiert eine Abbildung des Typs $I \times J \to X$, wobei I und J endliche Indexmengen sind. Als Indexmengen werden oft Anfangsabschnitte der positiven, ganzen Zahlen verwendet: $I = \{1, \ldots, m\}$ und $J = \{1, \ldots, n\}$. Da der Typ der Elemente (auch Einträge, Komponenten oder Skalare genannt) in der Regel aus dem Kontext ersichtlich ist ($X := \mathbb{R}$ im obigen Beispiel), beschränkt man sich bei der Typangabe auf die Indexmengen oder ***Dimensionen***: Man spricht kurz von einer $I \times J$-Matrix oder noch kürzer von einer $m \times n$-Matrix (sprich m-Kreuz-n Matrix). Ist $m = n$, so spricht man von einer ***quadratischen Matrix***.

Eine $1 \times n$-Matrix heißt auch ***Zeilenvektor***, eine $n \times 1$-Matrix ***Spaltenvektor***.

Die Anwendung einer Matrix A auf ein Indexpaar (i, j) wird kompakt mit A_{ij} notiert. In der tabellarischen Darstellung ist A_{ij} der Eintrag in der i-ten Zeile und j-ten Spalte.

Matrizen passender Dimensionen können multipliziert werden: Ist A eine $I \times J$-Matrix und B eine $J \times K$-Matrix, dann ist $C = A \cdot B$ eine $I \times K$-Matrix.

$$C_{ik} = \sum_{j \in J} A_{ij} \cdot B_{jk}$$

Die Multiplikation lässt sich mit Hilfe von Zeilen- und Spaltenvektoren visualisieren.

$$\begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \end{pmatrix} \cdot \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \\ B_{41} & B_{42} & B_{43} \end{pmatrix}$$

Der Eintrag C_{ik} des Matrixprodukts ergibt sich als ***Skalarprodukt*** des i-ten Zeilenvektors von A mit dem k-ten Spaltenvektor von B. Beim Skalarprodukt werden die korrespondierenden Komponenten der Vektoren multipliziert und die Ergebnisse aufaddiert, zum Beispiel, $C_{12} = A_{11} \cdot B_{12} + A_{12} \cdot B_{22} + A_{13} \cdot B_{32} + A_{14} \cdot B_{42}$.

Die Matrizenmultiplikation ist assoziativ, aber nicht kommutativ. Sie besitzt ein neutrales Element, die quadratische ***Diagonalmatrix*** $\mathbf{1}$.

$$\mathbf{1}_{ij} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases} \qquad \mathbf{1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Die Einträge auf der Hauptdiagonalen (von links oben nach rechts unten) sind 1, alle anderen Einträge sind 0.

Abbildung 4.1.: Matrizen und Matrixoperationen.

Kommen Ihnen die Werte bekannt vor? Die Potenzen von F setzen sich aus aufeinanderfolgenden ***Fibonacci-Zahlen*** zusammen, siehe Abbildung 2.2. Diese Eigenschaft kann man ausnutzen, um die Fibonacci-Zahlen rasend schnell zu berechnen. Die notwendigen Zutaten haben wir bereits zusammen: In Abschnitt 3.7.2 haben wir diskutiert, wie man natürliche Zahlen effizient potenziert. Den nach dem Leibniz Entwurfsmuster gestrickten Algorithmus können wir relativ einfach adaptieren, um statt natürlicher Zahlen, Matrizen von natürlichen Zahlen zu potenzieren.

```
let square (x : Matrix) : Matrix = x ^*^ x
let rec power (x : Matrix) (n : Nat) : Matrix =
  if n = 0 then unit
           else if n % 2 = 0 then square (power x (n ÷ 2))
                             else square (power x (n ÷ 2)) ^*^ x
```

Was hat sich geändert? Die natürliche Multiplikation ist der Matrizenmultiplikation gewichen und entsprechend wurde das neutrale Element der Multiplikation angepasst: 1 ist durch *unit* ersetzt worden.

```
⋙ power F 10
(89, 55, 55, 34)
⋙ power F 100
(573147844013817084101, 354224848179261915075,
 354224848179261915075, 218922995834555169026)
```

Aber was heißt rasend schnell? Zum Vergleich: Wird das Bildungsgesetz der Fibonacci-Zahlen unmittelbar für die Definition herangezogen (eine üble Idee),

```
let rec fibonacci (n : Nat) : Nat =
  if n ⩽ 1 then n
           else fibonacci (n − 1) + fibonacci (n − 2)
```

dann benötigt die Berechnung von $\mathscr{F}_{50}$ fast $2\frac{1}{2}$ Stunden (!), während die schnelle Potenzierung das Ergebnis in 2 Millisekunden liefert. Wir haben die Definition wenig wissenschaftlich als »übel« diffamiert, aber warum ist die rekursive Definition so langsam? Finden Sie eine wissenschaftliche Antwort (siehe Aufgabe 4.1.6).

4.1.2. Unwiderlegbare Muster

Binden wir ein Paar an einen Bezeichner, so ist es bequem, nicht nur einen Namen für das Paar selbst, sondern auch Namen für die beiden Komponenten vergeben zu können. Die folgende Version von *sort3* nutzt dieses Feature.

```
let sort3 (a : Nat, b : Nat, c : Nat) : Nat * Nat * Nat =
  let (small, big) = sort2 (a, b)
  in  if big ⩽ c then (small, big, c)
                 else if small ⩽ c then (small, c, big)
                                   else (c, small, big)
```

Selbst vergebene Namen für Komponenten, hier *small* und *big*, sind in der Regel prägnanter als Projektionen wie *fst x* und *snd x*.

Namen für die Komponenten eines Tupels vergeben zu können, ist insbesondere für n-Tupel mit $n \geqslant 3$ wichtig, da für diese keine vordefinierten Projektionsfunktionen angeboten werden. Die schnelle Berechnung der Fibonacci-Zahlen macht davon Gebrauch:

$$\begin{array}{l}\textbf{\textit{let}}\ \mathit{fibonacci}\ (n : \mathit{Nat}) : \mathit{Nat} = \\ \quad \textbf{\textit{let}}\ (f_{11}, f_{12}, f_{21}, f_{22}) = \mathit{power}\ F\ n\ \textbf{\textit{in}}\ f_{12}\end{array}$$

Die rechte, obere Ecke der 2×2-Matrix enthält das gewünschte Ergebnis.

Abstrakte Syntax Wir verallgemeinern Bezeichner in Bindungspositionen zu sogenannten ***Mustern*** (engl. patterns).

$d ::= \cdots$	***Deklarationen:***
$\mid$ **_let_** $p = e$	verallgemeinerte Wertedefinition

Entsprechend lassen sich alle Konstrukte verallgemeinern, die Bezeichner binden: Funktionsdefinitionen, Funktionsabstraktionen usw.

Um die abstrakte Syntax von Mustern präzise zu beschreiben, führen wir eine neue Baumsprache ein.

$p \in \mathsf{Pat} ::=$	***Muster:***
$\mid \_$	anonymer Bezeichner\»don't care« Muster
$\mid x$	Bezeichner
$\mid p_1 \,\&\, p_2$	konjunktives Muster
$\mid (p_1, p_2)$	Paarmuster

Mit Hilfe des Musters $p_1 \,\&\, p_2$ werden sowohl die Bezeichner in p_1 als auch in p_2 an die entsprechenden Werte gebunden. Ein konjunktives Muster kann zum Beispiel verwendet werden, um sowohl einen Namen für ein Paar als auch für dessen Komponenten zu vergeben: **_let_** $x \,\&\, (\mathit{small}, \mathit{big}) = \mathit{sort2}\ (e_1, e_2)$. Das Muster »_« markiert Komponenten, an denen man nicht interessiert ist: **_let_** $(\_, f_{12}, \_, \_) = \mathit{power}\ F\ n$.

Statische Semantik Eine verallgemeinerte Wertedefinition bindet mehrere Bezeichner, unter Umständen auch keine.

$$\frac{\Sigma \vdash e : t \qquad p \sim t : \Sigma'}{\Sigma \vdash (\textbf{\textit{let}}\ p = e) : \Sigma'}$$

In der Voraussetzung der Regel wird von einer neuen Relation Gebrauch gemacht, die sicherstellt, dass der ***Musterabgleich*** (engl. pattern matching) $p = e$ wohlgetypt ist. Zum Beispiel ist **_let_** $(\mathit{small}, \mathit{big}) = 4711$ keine sinnvolle Wertedefinition. Die Relation

$$p \sim t : \Sigma'$$

»ermittelt« die Signatur aller Bezeichner, die bei dem Musterabgleich gebunden werden. *Lies:* der Abgleich eines Wertes vom Typ t mit dem Muster p ergibt die Signatur Σ'. (Die Tilde $\sim$ soll den Musterabgleich symbolisieren.) Zum Beispiel werden beim Abgleich des Musters $x \,\&\, (\mathit{small}, \mathit{big})$ mit einem Element des Typs $\mathit{Nat} * \mathit{Nat}$ Bindungen des Typs $\{x \mapsto \mathit{Nat} * \mathit{Nat}, \mathit{small} \mapsto \mathit{Nat}, \mathit{big} \mapsto \mathit{Nat}\}$ erzeugt. Die Muster heißen übrigens ***unwiderlegbar*** (engl. irrefutable), weil die statische Semantik garantiert, dass der Wert stets auf das Muster passt. In Abschnitt 4.2.3 lernen wir Muster kennen, auf die das nicht mehr zutrifft, sogenannte widerlegbare Muster (engl. refutable patterns).

$$\frac{}{\_ \sim t : \varnothing} \qquad \frac{}{x \sim t : \{x \mapsto t\}}$$

$$\frac{p_1 \sim t : \Sigma_1 \qquad p_2 \sim t : \Sigma_2}{(p_1 \,\&\, p_2) \sim t : \Sigma_1, \Sigma_2} \qquad \frac{p_1 \sim t_1 : \Sigma_1 \qquad p_2 \sim t_2 : \Sigma_2}{(p_1, p_2) \sim t_1 * t_2 : \Sigma_1, \Sigma_2}$$

Konjunktive Muster und Paarmuster binden unter Umständen mehrere Bezeichner; mögliche Überschneidungen werden wie immer durch den Kommaoperator aufgelöst.

Dynamische Semantik Bei der Abarbeitung einer verallgemeinerten Wertedefinition wird zunächst die rechte Seite evaluiert; der resultierende Wert wird dann mit dem Muster auf der linken Seite abgeglichen.

$$\frac{\delta \vdash e \Downarrow \nu \qquad p \sim \nu \Downarrow \delta'}{\delta \vdash \textbf{\textit{let}}\ p = e \Downarrow \delta'}$$

Der ***Musterabgleich*** (engl. pattern matching) selbst wird mit Hilfe der Relation

$$p \sim \nu \Downarrow \delta$$

formalisiert. *Lies:* der Abgleich des Musters p mit dem Wert ν ergibt die Umgebung δ. Die Auswertungsregeln folgen den Typregeln.

$$\frac{}{\_ \sim \nu \Downarrow \varnothing} \qquad \frac{}{x \sim \nu \Downarrow \{x \mapsto \nu\}}$$

$$\frac{p_1 \sim \nu \Downarrow \delta_1 \qquad p_2 \sim \nu \Downarrow \delta_2}{(p_1 \,\&\, p_2) \sim \nu \Downarrow \delta_1, \delta_2} \qquad \frac{p_1 \sim \nu_1 \Downarrow \delta_1 \qquad p_2 \sim \nu_2 \Downarrow \delta_2}{(p_1, p_2) \sim (\nu_1, \nu_2) \Downarrow \delta_1, \delta_2}$$

Beim Abgleich eines konjunktiven Musters wird der *gleiche* Wert zweimal abgeglichen. Bei einem Paarmuster werden die Komponenten des Paares mit den Komponenten des Musters abgeglichen — durch die statische Semantik ist sichergestellt, dass der Wert tatsächlich ein Paar ist.

Vertiefung: Mehrparametrige Funktionen Schauen wir uns noch einmal die Sortierfunktion an.

$$\textbf{\textit{let}}\ sort2\ (a : Nat, b : Nat) : Nat * Nat =$$
$$\quad \textbf{\textit{if}}\ a \leqslant b\ \textbf{\textit{then}}\ (a, b)\ \textbf{\textit{else}}\ (b, a)$$

Der Typ von *sort2* ist $Nat * Nat \to Nat * Nat$; die Funktion *sort2* bildet also ein Paar auf ein Paar ab. Die Parameterliste $(a : Nat, b : Nat)$ entspricht im Prinzip einem Paarmuster mit der kleinen Abweichung, dass die Typangaben zu den Komponenten gerückt sind: $(a : Nat, b : Nat)$ statt $(a, b) : Nat * Nat$.

Funktionen auf Paaren haben gegenüber mehrparametrigen Funktionen den Vorteil, dass der aktuelle Parameter nicht syntaktisch ein Paar sein muss, sondern ein Ausdruck sein kann, der zu einem Paar auswertet. Nehmen wir zum Beispiel an, dass wir ein Paar von Zahlen nicht auf- sondern absteigend ordnen wollen. Das lässt sich unter anderem bewerkstelligen, indem wir das von *sort2* geordnete Paar umdrehen: $swap\ (sort2\ (e_1, e_2))$, wobei *swap* wie folgt definiert ist.

$$\textbf{\textit{let}}\ swap\ (a : Nat, b : Nat) : Nat * Nat = (b, a)$$

Wäre *swap* eine mehrparametrige Funktion, so dass wir gezwungen wären zwei Parameter anzugeben, müssten wir länglicher formulieren $\textbf{\textit{let}}\ (small, big) = sort2\ (e_1, e_2)\ \textbf{\textit{in}}\ swap\ (small, big)$.

4.1.3. Records

Bei Paaren sowie allgemein bei Tupeln spielt die Reihenfolge der Komponenten eine Rolle: Das Tupel $(12, 1, 2006)$ ist etwas anderes als $(1, 12, 2006)$; (`"Stefan"`, `"Thomas"`) unterscheidet sich von (`"Thomas"`, `"Stefan"`). Beide Beispiele machen deutlich, dass die *Rolle* einer Komponente nur implizit festgelegt ist: Programmierkonvention.

Wir erlauben, die Rolle auch explizit zu machen, indem man die Komponenten benennt: $\{day = 12; month = 1; year = 2006\}$ und {*forename* = `"Stefan"`; *surname* = `"Thomas"`}. Die sogenannten ***Labels*** machen deutlich, dass 12 der Tag ist und nicht der Monat bzw. `"Stefan"` der Vor- und

nicht der Nachname. Weiterhin bezeichnen $\{ month = 1; day = 12; year = 2006 \}$ bzw. $\{ surname = \texttt{"Thomas"}; forename = \texttt{"Stefan"} \}$ die gleichen Werte; das heißt, die Reihenfolge, in der die benannten Komponenten aufgeschrieben werden, ist irrelevant. Mit Hilfe der Labels können Komponenten auch extrahiert werden: *date.year* oder *person.surname*. Tupel mit benannten Komponenten heißen ***Records***.

Bevor Records verwendet werden können, müssen sie zunächst mit einer sogenannten *Typdefinition* bekannt gemacht werden.

$$\textbf{\textit{type}}\ Date = \{ day : Nat; month : Nat; year : Nat \}$$
$$\textbf{\textit{type}}\ Name = \{ forename : String; surname : String \}$$

So wie eine Wertedefinition einen Bezeichner für einen Wert einführt, so führt eine Typdefinition einen Bezeichner für einen Typ ein — eine neue Schublade, in die wir Werte stecken können. Dieser Typname kann in anderen Typdefinitionen sowie in Typangaben verwendet werden. Im Unterschied zu einer Wertedefinition und zu einem Typsynonym hat die rechte Seite der Typdefinition allerdings *keine* eigenständige Bedeutung, sie kann insbesondere *nicht* in Typangaben verwendet werden: $Date \to Nat$ ist ein gültiger Typ, *nicht* aber $\{ day : Nat; month : Nat; year : Nat \} \to Nat$.

Neben dem Namen für den Typ selbst, *Date* und *Name*, führt eine Typdefinition Namen ein, um Komponenten eines Records zu extrahieren: *day*, *month*, *year*, *forename* und *surname*. Diese Bezeichner heißen wie gesagt ***Recordlabels*** oder kurz ***Labels***. Die zwei obigen Definitionen führen somit zusammen sieben neue Bezeichner ein.

Wie auch bei Paaren beschränken wir uns auf den binären Fall und formalisieren nur Records mit exakt 2 Komponenten; alle Konstrukte verallgemeinern sich in naheliegender Weise auf Records mit n Komponenten.

Abstrakte Syntax Ein Recordtyp wird durch eine Definition eingeführt.

$T \in \mathsf{TypeIdent}$	***Typbezeichner***
$\ell \in \mathsf{Lab}$	***Labels***
$d ::= \cdots$	***Deklarationen:***
$\mid$ ***type*** $T = \{ \ell_1 : t_1; \ell_2 : t_2 \}$	Recordtypdefinition ($\ell_1 \neq \ell_2$)

Der Bezeichner T wird durch die Definition neu eingeführt, ebenso die Labels ℓ_1 und ℓ_2. Die beiden Labels müssen verschieden sein: $\ell_1 \neq \ell_2$.

Die Kategorie der Typen wird um Typbezeichner erweitert. (Im Prinzip sind auch *Bool* und *Nat* Bezeichner für Typen.)

$t ::= \cdots$	***Typen:***
$\mid T$	Typbezeichner

Fürs Erste stehen Typbezeichner für Recordtypen; im Laufe der Vorlesung werden weitere »Sorten« von Typen hinzukommen: Variantentypen, Schnittstellentypen usw.

Wir erweitern Ausdrücke um Sprachkonstrukte, die Records konstruieren und analysieren.

$e ::= \cdots$	***Recordausdrücke:***
$\mid \{ \ell_1 = e_1; \ell_2 = e_2 \}$	Konstruktion ($\ell_1 \neq \ell_2$)
$\mid e.\ell$	Projektion\Extraktion

Die Ausdrücke e_1 und e_2 heißen ***Recordkomponenten*** oder kurz ***Komponenten***.

Da ein Label für sich alleine *kein* Ausdruck ist, kommen sich Labels und Bezeichner übrigens nicht ins Gehege. Die gleiche Abfolge von Buchstaben kann aus diesem Grund gleichzeitig als Bezeichner und als Label verwendet werden: ***let*** *year* = *date.year*. Das erste Vorkommen von *year* ist ein Bezeichner, das zweite ein Label. Ähnliches gilt für den Ausdruck $\{ day = day; month = month; year = year \}$: Das erste Vorkommen ist jeweils ein Label, das zweite ein Bezeichner.

Statische Semantik: Vorüberlegungen ⋆ Bei der Besprechung von Wertedefinitionen haben wir gesehen, dass der gleiche Bezeichner für verschiedene Werte verwendet werden kann: ***let*** *s* = *false* ***let*** *s* = 4711. Die zweite Definition verschattet die erste. Das gleiche Phänomen kann auch bei Typdefinitionen auftreten: ***type*** *Oh* = {*je* : *Bool*} ***type*** *Oh* = {*je* : *Nat*}. Auch hier verschattet die zweite Definition die erste. Im Unterschied zu Wertedefinitionen können wir das nicht auf die leichte Schulter nehmen. Warum? Nun, Typen bringen Ordnung in die Welt der Werte. Wenn wir Unordnung in der Welt der Typen stiften, indem wir den gleichen Namen für unterschiedliche Recordtypen verwenden, dann bricht Chaos aus. In unserem Beispiel: Der Typbezeichner *Oh* kann — und wird in der Regel — in Typangaben vorkommen. Zum Beispiel:

let *na-und* (*oh* : *Oh*) : *Bool* = *not* (*oh*.*je*)

Die Funktion erhält den Typ $Oh \to Bool$. Wird der Typ *Oh* nach der Definition von *na-und* redefiniert, dann stimmt der Typ von *na-und* nicht mehr; der neue Typ und der alte Typ müssen ja nichts miteinander zu tun haben. Das folgende, vollständige Beispiel illustriert, was schieflaufen kann.

```
type Oh = {je : Bool}
let na-und (oh : Oh) : Bool = not (oh.je)
type Oh = {je : Nat }
let egal = na-und {je = 4711}
```

Wir schmuggeln eine natürliche Zahl an eine Stelle, an der ein Boolescher Wert erwartet wird und das Unglück nimmt seinen Lauf.

Was ist zu tun? Die Lösung ist so einfach, wie einschränkend: Wir erlauben es *nicht*, Typen zu redefinieren. Aus einem ähnlichen Grund lassen wir auch keine lokalen Typdefinitionen zu. In einem Mini–F# Modul dürfen Typdefinition nur auf dem »top-level« des Moduls eingeführt werden, *nicht* aber lokal mit ***in***-Ausdrücken. (Ein Modul fasst Ausdrücke und Deklarationen zu einer größeren konzeptionellen Einheit zusammen, siehe auch Anhang A.)

Statische Semantik Die folgenden Typregeln setzen voraus, dass die Typdefinition

type T = {$\ell_1 : t_1; \ell_2 : t_2$}

bekannt ist. Die Regeln unterscheiden sich nicht wesentlich von den korrespondierenden Regeln für Paare: An die Stelle des anonymen Typs $t_1 * t_2$ tritt der benannte Typ T.

$$\frac{\Sigma \vdash e_1 : t_1 \qquad \Sigma \vdash e_2 : t_2}{\Sigma \vdash \{\ell_1 = e_1; \ell_2 = e_2\} : \mathrm{T}} \qquad \frac{\Sigma \vdash e_1 : t_1 \qquad \Sigma \vdash e_2 : t_2}{\Sigma \vdash \{\ell_2 = e_2; \ell_1 = e_1\} : \mathrm{T}}$$

$$\frac{\Sigma \vdash e : \mathrm{T}}{\Sigma \vdash e.\ell_i : t_i} \quad i \in \{1, 2\}$$

Bei der Konstruktion eines Records müssen stets alle Komponenten angegeben werden; Komponenten dürfen aber nicht doppelt aufgeführt werden: $\ell_1 \neq \ell_2$. Auf diese Weise wird sichergestellt, dass Projektionen stets wohldefiniert sind. Der Ausdruck {*day* = 30}.*year* ist zum Beispiel nicht wohlgetypt. Es gibt zwei Regeln für die Konstruktion eines Records, da die Reihenfolge, in der die beiden Komponenten aufgeführt werden, keine Rolle spielt.

Ein Label ist einer Funktion nicht unähnlich. Der Typ nach dem Label korrespondiert zum Ergebnistyp, der deklarierte Recordtyp korrespondiert zum Argumenttyp: *year* hat im Prinzip den Typ $Date \to Nat$ und *surname* den Typ $Name \to String$. Im Unterschied zu einer Funktion hat ein Label aber keine Definition; es steht sozusagen für sich selbst. An die Stelle der Funktionsanwendung tritt die Punktnotation: *date*.*year* oder *person*.*surname*.

Dynamische Semantik Typdefinitionen können in der dynamischen Semantik ignoriert werden. Wir erweitern den Bereich der Werte um Records, deren Komponenten Werte sind.

$\nu ::= \cdots$	***Werte:***
$\mid \{\ell_1 = \nu_1; \ell_2 = \nu_2\}$	Records $(\ell_1 \neq \ell_2)$

Die Auswertungsregeln korrespondieren zu den Regeln für Paare, nur dass an die Stelle der Projektionsfunktionen *fst* und *snd* die Punktnotation tritt.

$$\frac{\delta \vdash e_1 \Downarrow \nu_1 \qquad \delta \vdash e_2 \Downarrow \nu_2}{\delta \vdash \{\ell_1 = e_1; \ell_2 = e_2\} \Downarrow \{\ell_1 = \nu_1; \ell_2 = \nu_2\}}$$

$$\frac{\delta \vdash e_1 \Downarrow \nu_1 \qquad \delta \vdash e_2 \Downarrow \nu_2}{\delta \vdash \{\ell_2 = e_2; \ell_1 = e_1\} \Downarrow \{\ell_1 = \nu_1; \ell_2 = \nu_2\}}$$

$$\frac{\delta \vdash e \Downarrow \{\ell_1 = \nu_1; \ell_2 = \nu_2\}}{\delta \vdash e.\ell_i \Downarrow \nu_i} \quad i \in \{1, 2\}$$

Vertiefung: Ganze Zahlen Mini-F# bietet von Haus aus keine ganzen Zahlen an. Um mit ganzen Zahlen rechnen zu können (wie wir das bereits in Abschnitt 3.5 gemacht haben), müssen wir sie implementieren. Natürliche Zahlen haben wir mit Hilfe der Metasprache eingeführt; ganze Zahlen werden mit Hilfe der Objektsprache definiert. Beim ersten Ansatz hat der/die Sprachdesigner/-in die Arbeit, beim zweiten der/die Programmierer/-in.

Wir können eine ganze Zahl als Differenz zweier natürlicher Zahlen repräsentieren: -4 wird zum Beispiel durch $0 - 4$, $5 - 9$ oder $4711 - 4715$ dargestellt; $+4$ entsprechend durch $4 - 0$, $9 - 5$ oder $4715 - 4711$. Wir stellen somit eine ganze Zahl durch *zwei* natürliche Zahlen dar, ein Fall für Recordtypen.

$$\textbf{\textit{type}}\ \mathit{Int} = \{\mathit{pos} : \mathit{Nat}; \mathit{neg} : \mathit{Nat}\}$$

Die Bedeutung von $\{\mathit{pos} = p; \mathit{neg} = n\}$ ist $p - n$, wobei »–« die *mathematische* Subtraktion auf den ganzen Zahlen meint. Kurz: $\{\mathit{pos} = p; \mathit{neg} = n\}$ ist Syntax, $p - n$ ist Semantik. Da jede ganze Zahl verschiedene Repräsentationen besitzt, haben wir es mit einer *redundanten* Zahlendarstellung zu tun. (Wenn führende Nullen zugelassen werden, ist auch das uns vertraute Dezimalsystem redundant: Die Ziffernfolgen `815`, `0815` und `00815` repräsentieren jeweils die gleiche Zahl, nämlich 815.)

Wie können wir mit ganzen Zahlen rechnen? Wir müssen entsprechende Rechenregeln aufstellen, indem wir die arithmetischen Operationen und Vergleichsoperationen für ganze Zahlen zurückführen auf Operationen über den natürlichen Zahlen. Fangen wir mit der Addition an:

$$\begin{array}{l}\textbf{\textit{let}}\ \mathit{add}\ (i : \mathit{Int}, j : \mathit{Int}) : \mathit{Int} = \\ \quad \{\mathit{pos} = i.\mathit{pos} + j.\mathit{pos}; \mathit{neg} = i.\mathit{neg} + j.\mathit{neg}\}\end{array}$$

Die Bedeutung von $\mathit{add}\ (i, j)$ ist

$$(i.\mathit{pos} - i.\mathit{neg}) + (j.\mathit{pos} - j.\mathit{neg}) = (i.\mathit{pos} + j.\mathit{pos}) - (i.\mathit{neg} + j.\mathit{neg})$$

Durch Umordnen und Zusammenfassen positiver wie negativer Komponenten erhalten wir das gewünschte Ergebnis. Auf ähnliche Art und Weise lässt sich auch die Multiplikation implementieren (zur Übung). Interessanter wird es, wenn wir Operationen betrachten, die auf den natürlichen Zahlen nicht unterstützt werden: Negation und Subtraktion. Die Implementierung der Negation ist verblüffend einfach: Da

$$-(i.\mathit{pos} - i.\mathit{neg}) = i.\mathit{neg} - i.\mathit{pos}$$

müssen wir lediglich die Komponenten vertauschen.

```
let negate (i : Int) : Int =
  {pos = i.neg; neg = i.pos}
let sub (i : Int, j : Int) : Int =
  {pos = i.pos + j.neg; neg = i.neg + j.pos}
```

Wann sind zwei ganze Zahlen gleich? Da wir ein redundantes Zahlensystem vor uns haben, müssen wir etwas aufpassen. (Wäre die Darstellung eindeutig, würde gelten: Zwei Zahlen sind gleich, wenn sie gleich aussehen, $i = j \iff i.pos = j.pos \wedge i.neg = j.neg$. Kurz: zwei Zahlen sind semantisch gleich, wenn sie syntaktisch gleich sind.) Die Bedeutung von i ist $i.pos - i.neg$; die Bedeutung von j entsprechend $j.pos - j.neg$. Die semantischen Werte müssen gleich sein:

$$i.pos - i.neg = j.pos - j.neg \quad \iff \quad i.pos + j.neg = i.neg + j.pos$$

Somit erhalten wir:

```
let equal (i : Int, j : Int) : Bool =
  i.pos + j.neg = i.neg + j.pos
```

Die anderen Vergleichsoperationen lassen sich analog implementieren (zur Übung).

Jetzt da Mini-F# über zwei Zahlentypen verfügt, stellt sich die Frage, wie wir Elemente des einen Typs in den anderen Typ überführen (im Fachjargon: Typkonversion). Eine natürliche Zahl in eine ganze zu überführen, ist einfach:

```
let int (n : Nat) : Int =
  {pos = n; neg = 0}
```

Die umgekehrte Richtung geht mit einem Informationsverlust einher: Die ganze Zahl i wird auf ihren Betrag $\mathrm{abs}\, i$ abgebildet.

```
let abs (i : Int) : Nat =
  if i.pos ⩽ i.neg then i.neg ∸ i.pos
                   else i.pos ∸ i.neg
```

Etwas kürzer können wir formulieren:

```
let abs (i : Int) : Nat =
  (i.neg ∸ i.pos) + (i.pos ∸ i.neg)
```

Die rechte Seite regt zum Nachdenken an: Gilt nicht $(i.neg \dot{-} i.pos) + (i.pos \dot{-} i.neg) = 0$? Weit gefehlt! Das Symbol »$\dot{-}$« ist Syntax für die Subtraktion natürlicher Zahlen (»monus« nicht »minus«) und es gilt: $(a \dot{-} b) + (b \dot{-} a) = \mathrm{abs}(a - b)$, siehe auch Anhang B.5.1.

module Datatypes.Area

Vertiefung: Wohnfläche Kommen wir noch einmal auf ein Problem zurück, das wir bereits in Abschnitt 3.3 bearbeitet haben: die Berechnung einer Wohnfläche. Abstrakt gesehen gilt es, die Gesamtfläche zweier gegebener Rechtecke zu berechnen — in der ursprünglichen Aufgabenstellung ist von Quadraten die Rede, aber das ist eine unnötige Einschränkung. (Abbildung 4.2 enthält ein paar grundlegende Überlegungen zur Berechnung von Flächeninhalten.) Jetzt da wir die Möglichkeit haben, Daten zu aggregieren, verschiedene Daten zu einer Einheit zusammenzufassen, können wir die Aufgabe professioneller angehen. Erinnern wir uns: Ein Rechteck ist durch zwei Intervalle gegeben, einen Abschnitt der x-Achse und einen Abschnitt der y-Achse.

Sei $\|P\|$ der Flächeninhalt einer Menge von Punkten P.[a] Flächenberechnungen basieren auf zwei grundlegenden Annahmen: (1) Die Fläche des Einheitsquadrates ist 1; (2) die Fläche zweier *disjunkter* Punktmengen entspricht der Summe der Einzelflächen: $\|A \cup B\| = \|A\| + \|B\|$, falls $A \cap B = \varnothing$. Wenn die Mengen nicht disjunkt sind, müssen wir sie entsprechend in disjunkte Teilmengen aufteilen, zum Beispiel mit Hilfe einer der folgenden Eigenschaften:

$$\begin{aligned} A &= (A - B) \cup (A \cap B) \\ B &= (B - A) \cup (A \cap B) \\ A \cup B &= (A - B) \cup (A \cap B) \cup (B - A) \end{aligned}$$

Die Mengen auf den rechten Seite sind jeweils disjunkt, somit gilt:

$$\|A\| = \|A - B\| + \|A \cap B\| \tag{4.1a}$$
$$\|B\| = \|B - A\| + \|A \cap B\| \tag{4.1b}$$
$$\|A \cup B\| = \|A - B\| + \|A \cap B\| + \|B - A\| \tag{4.1c}$$

Die Formel für $\|A \cup B\|$ verwendet die *Mengendifferenz* auf der rechten Seite; diese Mengenoperation lässt sich vermeiden, wie die folgende Rechnung zeigt :

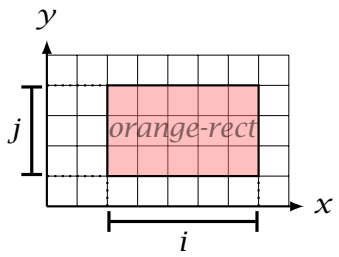
$$\begin{aligned} & \|A\| + \|B\| \\ = & \quad \{ \text{ siehe oben (4.1a) und (4.1b) } \} \\ & \|A - B\| + \|A \cap B\| + \|B - A\| + \|A \cap B\| \\ = & \quad \{ \text{ siehe oben (4.1c) } \} \\ & \|A \cup B\| + \|A \cap B\| \end{aligned}$$

Durch Umstellen erhalten wir

$$\|A \cup B\| = \|A\| + \|B\| - \|A \cap B\|$$

Abbildung 4.2.: Berechnung von Flächeninhalten.

[a] Einer *beliebigen* Punktmenge eine Fläche zuzuordnen, ist tatsächlich ein unlösbares mathematisches Problem. Wenn Sie mathematisch interessiert sind, erfahren Sie dazu mehr in der Maßtheorie. Wir ignorieren diese Probleme grundsätzlicher Natur, sind aber auch auf der sicheren Seite, da unsere Punktmengen bzw. Flächen sehr einfach gestrickt sind.




```
let orange-rect =
  let i = { lo = 2; hi = 7 }
  let j = { lo = 1; hi = 4 }
  { x = i; y = j }
```

Im Folgenden führen wir die notwendigen Typdefinitionen ein, so dass das orangene Rechteck durch die Wertedefinition auf der rechten Seite repräsentiert werden kann. (Die Intervalldarstellung ist natürlich nicht die einzig denkbare Repräsentation von Rechtecken. Welche Alternativen gibt es? Welche Vor- und Nachteile haben die verschiedenen Darstellungen? Wenn Sie Lust haben, lösen Sie die Aufgabe ein zweites Mal unter Verwendung Ihrer favorisierten Darstellung.)

Wenden wir uns zunächst der Darstellung von Intervallen zu. Ein Intervall wird durch die beiden Intervallgrenzen festgelegt.

```
type Interval = { lo : Nat; hi : Nat }          // low und high
```

Die Länge eines Intervalls ergibt sich als Differenz der Intervallgrenzen.

```
let length (i : Interval) : Nat = i.hi ∸ i.lo
```

Da Längen nicht-negativ sind, ist die natürliche Subtraktion »∸« die richtige Wahl. Würden wir zum Beispiel ganze Zahlen als Intervallgrenzen verwenden, müssten wir »monus« nachprogrammieren und die Länge als $max\ 0\ (i.hi - i.lo)$ definieren.

Jetzt können wir die 1-dimensionale Variante unseres ursprünglichen Problems lösen und die Gesamtlänge zweier Intervalle berechnen. Überlappen sich die Intervalle nicht, ist die Gesamtlänge die Summe der Einzellängen. Im Fall einer Überschneidung müssen wir von der Summe die Länge der Überlappung abziehen. Mathematisch betrachtet entspricht die Überlappung einem Mengendurchschnitt.

Bildet man den Durchschnitt zweier Intervalle, erhält man wieder ein Intervall (das klappt bei der Vereinigung von Intervallen nicht).

```
let intersection (i : Interval, j : Interval) : Interval =
  { lo = max i.lo j.lo; hi = min i.hi j.hi }
```

Es ist nützlich sich zu überlegen, welche Eigenschaften eine Funktion hat. Die Funktion *intersection* ist zum Beispiel kommutativ, $intersection\ (i, j) = intersection\ (j, i)$, da sowohl *min* als auch *max* kommutativ sind. Gibt es noch weitere merkenswerte oder bemerkenswerte Eigenschaften?

Jetzt haben wir das Vokabular zusammen, um die umgangssprachliche Lösung in Mini–F# zu transliterieren: Die Gesamtlänge zweier Intervalle ist die Summe der Einzellängen minus der Länge des Durchschnitts.

```
let length2 (i : Interval, j : Interval) =
  length i + length j ∸ length (intersection (i, j))
```

Um unser ursprüngliches Problem zu lösen, müssen wir die 1-dimensionalen Konzepte im Wesentlichen in den 2-dimensionalen Raum übertragen. Fangen wir mit der Darstellung von Rechtecken an: Ein Rechteck wird durch zwei Intervalle festgelegt.

```
type Rectangle = { x : Interval; y : Interval }
```

Der Flächeninhalt eines Rechtecks ergibt sich als Produkt der Intervalllängen.

```
let area (r : Rectangle) = length r.x * length r.y
```

Analog zum 1-dimensionalen Fall definieren wir den Durchschnitt zweier Rechtecke.

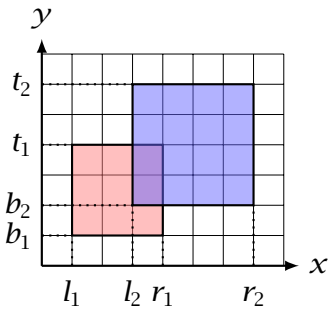
```
let Intersection (r : Rectangle, s : Rectangle) =
  {x = intersection (r.x, s.x);
   y = intersection (r.y, s.y)}
```

Der Durchschnitt wird koordinatenweise berechnet und stützt sich auf die entsprechende Funktion für Intervalle ab. Somit »erbt« *Intersection* die Eigenschaften ihrer kleinen Schwester, zum Beispiel, *Intersection* (r, s) = *Intersection* (s, r) — die Funktion ist kommutativ. Insgesamt erhalten wir für die Gesamtfläche zweier Rechtecke:

```
let area2 (r : Rectangle, s : Rectangle) =
  area r + area s - area (Intersection (r, s))
```

Wie im 1-dimensionalen Fall transliterieren wir die umgangssprachliche Formulierung in Mini–F#. Man erkennt die Fortschritte, die wir erzielt haben, wenn man das obige Programm mit dem Code aus Abschnitt 3.3 vergleicht. Letzterer löst eine spezielle Probleminstanz; der Code besteht aus einem monolithischen Block. Im Gegensatz dazu löst das obige Programm das Problem im Allgemeinen; es ist modular aufgebaut und besteht aus mehreren, kleinen Bausteinen. Der kompositionale Aufbau bringt viele Vorteile mit sich: Jeder Baustein, jede Typdefinition und jede Funktion, kann isoliert betrachtet, verstanden, getestet und verifiziert werden. Je größer ein Programm, je schwieriger ein Problem, je größer ein Softwaresystem, je umfangreicher die Anforderungen, desto wichtiger wird ein modularer Aufbau.

Schauen wir uns das Programm bzw. die Funktionen in Aktion an. Der Grundriss aus Abschnitt 3.3 wird durch zwei Rechtecke beschrieben.



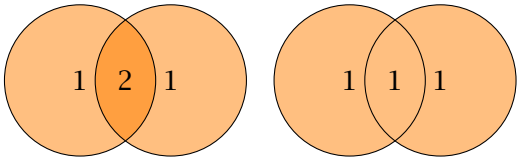

```
let shift (d : Nat, i : Interval) =
  {lo = i.lo + d; hi = i.hi + d}
let red-rect =
  let i = {lo = 1; hi = 4}
  {x = i; y = i}
let blue-rect =
  let i = {lo = 2; hi = 6}
  {x = shift (1, i); y = i}
```

Der Durchschnitt der Quadrate ergibt das kleine, violette Rechteck in der Mitte.

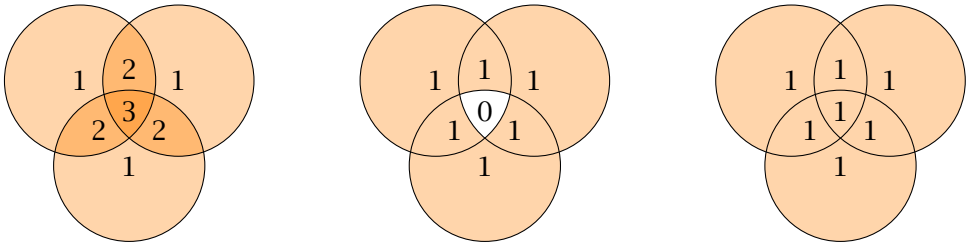
```
>>> Intersection (red-rect, blue-rect)
{x = {lo = 3; hi = 4}; y = {lo = 2; hi = 4}}
>>> area2 (red-rect, blue-rect)
23
>>> area2 (blue-rect, red-rect)
23
```

Es ist beruhigend, dass es keine Rolle spielt, in welcher Reihenfolge wir die Rechtecke an *area2* übergeben. Vielleicht erinnern Sie sich: Der erste Ansatz aus Abschnitt 3.3 funktionierte für eine Reihenfolge, versagte aber bei der anderen. Es gilt allgemein: *area2* (r, s) = *area2* (s, r). Mit anderen Worten, auch *area2* ist kommutativ, eine Eigenschaft, die sich schnell nachweisen lässt. (Versuchen Sie es.)

Werden wir etwas ambitionierter: Wie können wir die Gesamtfläche von *drei* Rechtecken bestimmen? Machen wir uns noch einmal klar, wie wir im Fall von zwei Rechtecken vorgegangen sind. Unserem Programm liegt das ***Prinzip der Einschließung und Ausschließung*** zugrunde (Inklusion und Exklusion). Wenn wir die Fläche von $A \cup B$ berechnen, indem wir die Summe der Einzelflächen addieren, dann wird die Schnittfläche doppelt gezählt, muss also wieder abgezogen werden.



Wenn wir drei Flächen addieren, dann werden die Schnitte von zwei Flächen doppelt, der Schnitt von allen drei Flächen wird dreifach gezählt.



Wenn wir die doppelt gezählten Flächen wieder abziehen, geht aber die gemeinsame Schnittfläche verloren; diese müssen wir dann wieder hinzufügen. Man sieht: Die Flächen werden alternierend ein- und ausgeschlossen, daher der Name des Prinzips. Damit ergibt sich das folgende Mini–F# Programm.

```
let Intersection3 (r : Rectangle, s : Rectangle, t : Rectangle) =
  Intersection (r, Intersection (s, t))
let area3 (r : Rectangle, s : Rectangle, t : Rectangle) =
  area r + area s + area t
  ÷ area (Intersection (r, s)) ÷ area (Intersection (r, t)) ÷ area (Intersection (s, t))
  + area (Intersection3 (r, s, t))
```

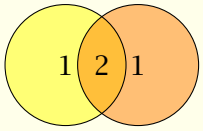
Das Programm ist schon etwas umfangreicher. Das Prinzip der Einschließung und Ausschließung lässt sich auch anwenden, um die Gesamtfläche von vier oder mehr Rechtecken auszurechnen. Aber ist das auch eine gute Idee? (Abbildung 4.3 erklärt das Prinzip noch einmal aus dem Blickwinkel der Kombinatorik.)

module Datatypes.Golden

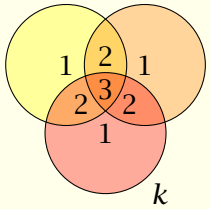
Vertiefung: Goldene Arithmetik und Fibonacci-Zahlen⋆ Wenden wir uns zum Abschluss des Abschnitts noch einmal den Zahlen zu. Vom Taschenrechner ist Ihnen wahrscheinlich das Rechnen mit Fließ- oder Gleitkommazahlen vertraut (in der Exponentialschreibweise, auch bekannt als »wissenschaftliches Format«). Auch F# bietet wie fast jede andere Programmiersprache Fließkommaarithmetik an.

```
⋙ 8122.0 * 3.085677581e+16
2.506187331e+20 : float
⋙ 8122 * 30856775810000000
250618733128820000000 : Nat
```

Etwas Kombinatorik gefällig? Gegeben seien n nicht notwendigerweise disjunkte Flächen A_1, …, A_n. Wir wollen die Gesamtfläche $\|A_1 \cup \cdots \cup A_n\|$ bestimmen. (Um die folgenden Formeln kompakt zu halten, verwenden wir zum Beispiel $\|134\|$ als Abkürzung für die Schnittfläche $\|A_1 \cap A_3 \cap A_4\|$.) Ein systematischer Ansatz zur Bestimmung der Gesamtfläche beruht auf dem ***Prinzip der Einschließung und Ausschließung***, nachfolgend illustriert für die beiden einfachsten, nichttrivialen Probleminstanzen.



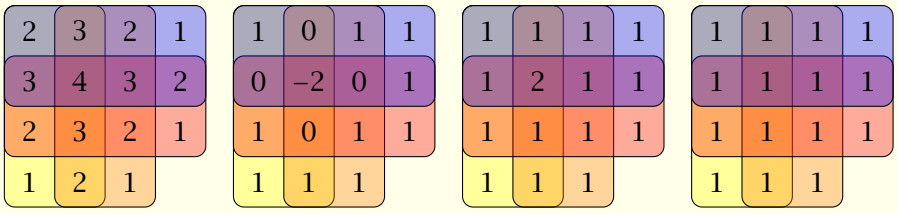
	k	1	2
$\|1\| + \|2\|$		+1	+2
$-\|12\|$			−1



	k	1	2	3
$\|1\| + \|2\| + \|3\|$		+1	+2	+3
$-\|12\| - \|13\| - \|23\|$			−1	−3
$+\|123\|$				+1

Betrachten wir eine Teilfläche, die in *genau k* der Flächen $A_1, \ldots, A_n$ enthalten ist. Ihr Beitrag zur Gesamtfläche ist jeweils in der k-ten Spalte aufgeführt. Ist zum Beispiel $n = 3$ und $k = 2$, dann wird die Fläche doppelt in $\|1\| + \|2\| + \|3\|$ und einfach in $\|12\| + \|13\| + \|23\|$ gezählt. Addiert man die k-te Spalte auf, erkennt man, dass diese Fläche summa summarum genau einmal gezählt wird.

Für $n = 4$ ergibt sich das folgende Bild — die Illustration der Überschneidungen mit Hilfe von Venn-Diagrammen stößt langsam aber sicher an ihre Grenzen.



	k	1	2	3	4
$\|1\| + \|2\| + \|3\| + \|3\|$		+1	+2	+3	+4
$-\|12\| - \|13\| - \|14\| - \|23\| - \|24\| - \|34\|$			−1	−3	−6
$+\|123\| + \|124\| + \|134\| + \|234\|$				+1	+4
$-\|1234\|$					−1

Die Diagramme, von links nach rechts gelesen, illustrieren wie oft eine Fläche gezählt wird, wenn die Flächenformel von oben nach unten abgearbeitet wird. Bleibt zu klären, warum die Summe jeder Spalte 1 ergibt. Die Einträge sind sogenannte Binomialkoeffizienten (warum?); die Summe alternierender Koeffizienten ist 0, eine Konsequenz aus dem Binomischen Satz (die Formel berechnet 1 *minus* der Summe der Spalte):

$$(-1)^0\binom{k}{0} + (-1)^1\binom{k}{1} + (-1)^1\binom{k}{2} + \cdots + (-1)^k\binom{k}{k} = (1-1)^k = 0$$

Abbildung 4.3.: Das Prinzip der Einschließung und Ausschließung.

Um Fließkommazahlen von den natürlichen Zahlen zu unterscheiden, werden erstere mit einem Dezimalpunkt und/oder einem Exponenten geschrieben. Auch der Typ ist ein anderer: *float* statt *Nat*. Rechnet man mit großen Zahlen wie der Entfernung zum Zentrum der Milchstraße, ist man daran gewöhnt, dass das Ergebnis ungenau ist — schließlich verfügt der Taschenrechner nur über eine »endliche« Anzeige mit einer begrenzten Anzahl von Stellen. Aber auch bei kleinen Zahlen ist Vorsicht geboten (Bezeichner dürfen in Mini-F# nicht nur aus lateinischen, sondern auch aus griechischen Buchstaben bestehen):

```
>>> 1.0 - 0.9 = 0.1
false
>>> let φ = (1.0 + sqrt 5.0) / 2.0
val φ : float = 1.618033989
>>> 165580141.0 * φ = 267914296.0
true
```

Beide Antworten sind falsch: 1.0 – 0.9 ist offensichtlich 0.1, aber der Rechner bestreitet das. Der sogenannte *Goldene Schnitt* φ ist eine irrationale Zahl; das Produkt einer natürlichen und einer irrationalen Zahl ist wieder irrational, kann also nicht gleich einer natürlichen Zahl sein, aber der Rechner sieht das anders. Warum verrechnet sich der Interpreter? Zum einen wird mit beschränkter Genauigkeit gerechnet. Zum anderen werden die Dezimalzahlen binär repräsentiert: Dem Dezimalbruch $(0{,}1)_{10}$, also ein Zehntel, entspricht der *periodische* Binärbruch $(0{,}0\overline{0011})_2$ — da mit beschränkter Genauigkeit gerechnet wird, fallen zwangsläufig Binärstellen unter den Tisch. Im F#-Interpreter sollte man sich übrigens nicht von der Ausgabe täuschen lassen:

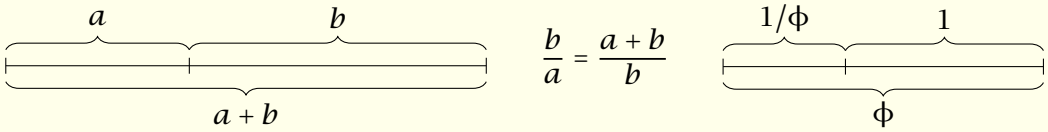
```
>>> 1.0 - 0.9
0.1
>>> printf "%.55f" (1.0 - 0.9)
0.0999999999999999977795539507496869191527366638183593750 0
>>> printf "%.55f" 0.1
0.1000000000000000055511151231257827021181583404541015625
```

Der Ausgabe geht eine Umwandlung binär nach dezimal voraus, bei der typischerweise auf sechs Dezimalstellen gerundet wird. Die ausgegebene Ziffernfolge entspricht also *nicht* der repräsentierten Zahl; das wird deutlich, wenn man sich weitere Dezimalstellen ausgeben lässt. Kurz und gut: Bei der Verwendung von Fließkommazahlen ist Vorsicht geboten.

Aber, müssen wir zwangsläufig mit diesen Einschränkungen leben? Schließlich können wir ja auch mit beliebig großen ganzen Zahlen rechnen, warum nicht auch mit reellen Zahlen? Hier stoßen wir an die Grenzen des mechanischen Rechnens: Da die Menge der reellen Zahlen ***überabzählbar*** ist, lassen sich reelle Zahlen und Operationen auf ihnen nicht in voller Schönheit auf den Rechner bringen. (Anhang B.2.4 berichtet von diesem faszinierenden Kapitel der Mathematik und erklärt die Begriffe abzählbar und überabzählbar.)

Das bedeutet allerdings nicht, dass sich nicht mit irrationalen Zahlen rechnen lässt. (Aufgabe 4.1.4 beschäftigt sich mit der Implementierung von rationalen Zahlen.) Zum Beispiel können wir prima mit *Goldenen Zahlen* rechnen, das sind Zahlen, die den Goldenen Schnitt φ involvieren, siehe Abbildung 4.4.

Ein ***Goldener Schnitt*** unterteilt eine Strecke, so dass das Verhältnis der größeren zur kleineren Teilstrecke dem Verhältnis der Gesamtstrecke zur größeren Teilstrecke entspricht.



Das Verhältnis $x := \frac{b}{a}$ ergibt sich als Lösung einer quadratischen Gleichung.

$$\frac{b}{a} = \frac{a+b}{b} \quad \Longleftrightarrow \quad \frac{b}{a} = \frac{a}{b} + 1 \quad \Longleftrightarrow \quad x = \frac{1}{x} + 1 \quad \Longleftrightarrow \quad x^2 = 1 + x$$

Die Gleichung besitzt eine positive Lösung, den Goldenen Schnitt $\phi = (1+\sqrt{5})/2 \approx 1{,}618$, und eine negative Lösung, den negativen Goldenen Schnitt $\hat{\phi} = (1-\sqrt{5})/2 \approx -0{,}618$. Die folgenden Beziehungen zwischen den Lösungen sind merkenswert:

$$\phi + \hat{\phi} = 1 \qquad \phi - \hat{\phi} = \sqrt{5} \qquad \phi \cdot \hat{\phi} = -1$$

Jede Potenz der Schnitte ergibt sich als Summe der beiden vorhergehenden Potenzen, $x^{n+2} = x^n + x^{n+1}$. Das Bildungsgesetz erinnert an die Fibonacci-Zahlen, $\mathscr{F}_{n+2} = \mathscr{F}_n + \mathscr{F}_{n+1}$. Ein einfacher Induktionsbeweis präzisiert den Zusammenhang (mit $\mathscr{F}_{-1} := 1$):

$$\phi^n = \mathscr{F}_{n-1} + \mathscr{F}_n \cdot \phi \qquad \hat{\phi}^n = \mathscr{F}_{n-1} + \mathscr{F}_n \cdot \hat{\phi} \tag{4.2}$$

Subtrahieren wir die Gleichungen voneinander, erhalten wir eine geschlossene Formel für die Fibonacci-Zahlen, die Formel von Moivre-Binet.

$$\phi^n - \hat{\phi}^n = \mathscr{F}_n \cdot \phi - \mathscr{F}_n \cdot \hat{\phi} \quad \Longleftrightarrow \quad \mathscr{F}_n = \frac{\phi^n - \hat{\phi}^n}{\phi - \hat{\phi}} \approx \phi^n/\sqrt{5}$$

Die Folge $\hat{\phi}^n$ konvergiert gegen 0 für $n \to \infty$, da $-1 < \hat{\phi} < 0$. Damit strebt das Verhältnis zweier aufeinanderfolgender Fibonacci-Zahlen gegen den Goldenen Schnitt.

$$\frac{\mathscr{F}_{n+1}}{\mathscr{F}_n} = \frac{\phi^{n+1} - \hat{\phi}^{n+1}}{\phi^n - \hat{\phi}^n} \to \phi \quad \text{für } n \to \infty$$

Abbildung 4.4.: Der Goldene Schnitt.

```
⋙ 165580141 * ϕ = 267914296
false
⋙ ϕ * ϕ
1 + 1 · ϕ
⋙ power ϕ 10
34 + 55 · ϕ
⋙ power ϕ 100
21892295834555169026 + 35422484817926191507 5 · ϕ
```

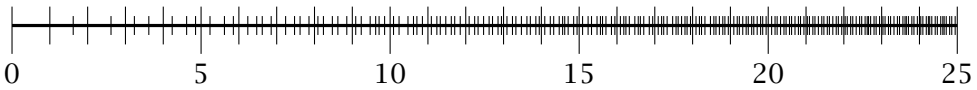
»Prima rechnen« meint exakt, ohne Rundungsfehler und mit beliebiger Genauigkeit. Die Ausgabe deutet bereits an, wie Goldenen Zahlen repräsentiert werden. Eine Goldene Zahl besteht aus einem rationalen Anteil, einer natürlichen Zahl, und einem irrationalen Anteil, einem natürlichen Vielfachen des Goldenen Schnitts: $r + i \cdot \phi$.

```
type Golden = {rat : Nat; irr : Nat}          // r + i · ϕ
let ϕ : Golden = {rat = 0; irr = 1}
```

Falls Sie sich wundern — ja, fast genauso haben wir auch die ganzen Zahlen repräsentiert. Die zugrundeliegende Idee ist in der Tat die gleiche: Eine Zahl jenseits der natürlichen Zahlen wird durch eine Linearkombination repräsentiert: $r + i \cdot a$ für eine vorher festgelegte Konstante a. Im Fall der ganzen Zahlen wählen wir $a := -1$, für Goldene Zahlen $a := \phi$. Die Funktion *golden* bettet die natürlichen Zahlen in die Goldenen Zahlen ein:

```
let golden (n : Nat) : Golden = {rat = n; irr = 0}
```

Zwischen 0 und 25 gibt es insgesamt 214 Goldene Zahlen (inklusive der Grenzen); je weiter wir auf dem Zahlenstrahl nach rechts rücken, desto enger liegen die Zahlen.



Kommen wir zu den arithmetischen Operationen. Zwei Goldene Zahlen werden addiert, indem man getrennt die rationalen und die irrationalen Anteile addiert. Interessanter wird es bei der Multiplikation — um Fehler zu vermeiden, leiten wir die Implementierung her:

$$
\begin{aligned}
& (r + i \cdot \phi) \cdot (s + j \cdot \phi) \\
= \quad & \{ \text{ Distributiv- und Kommutativgesetz } \} \\
& r \cdot s + i \cdot s \cdot \phi + r \cdot j \cdot \phi + i \cdot j \cdot \phi^2 \\
= \quad & \{ \text{ Goldener Schnitt: } \phi^2 = 1 + \phi \ \} \\
& r \cdot s + i \cdot s \cdot \phi + r \cdot j \cdot \phi + i \cdot j \cdot (\phi + 1) \\
= \quad & \{ \text{ Distributiv- und Kommutativgesetz } \} \\
& (r \cdot s + i \cdot j) + (r \cdot j + s \cdot i + i \cdot j) \cdot \phi
\end{aligned}
$$

Im zweiten und entscheidenden Schritt fließt die definierende Eigenschaft des Goldenen Schnitts ein. Damit ergeben sich die folgenden Implementierungen.

```
let (^+^) (a : Golden) (b : Golden) : Golden =
  {rat = a.rat + b.rat; irr = a.irr + b.irr}
let (^*^) (a : Golden) (b : Golden) : Golden =
  let ij = a.irr * b.irr
  {rat = a.rat * b.rat + ij; irr = a.rat * b.irr + b.rat * a.irr + ij}
```

Die Definition der Multiplikation hat eine interessante Konsequenz: *Jede* Potenz des Goldenen Schnitts ϕ^n lässt sich als Linearkombination $r + i \cdot \phi$ darstellen. Die Koeffizienten r und i sind alte Bekannte — vielleicht sind Ihnen die Ergebnisse von *power* ϕ 10 und *power* ϕ 100 in der obigen Interaktion bekannt vorgekommen.

$$\phi^n = \mathscr{F}_{n-1} + \mathscr{F}_n \cdot \phi$$

Damit kommen wir zum wohl schnellsten Programm zur Berechnung der Fibonacci-Zahlen.

```
let square (x : Golden) : Golden = x ^*^ x
let rec power (x : Golden) (n : Nat) : Golden =
  if n = 0 then golden 1
           else if n % 2 = 0 then square (power x (n ÷ 2))
                             else square (power x (n ÷ 2)) ^*^ x
let fibonacci (n : Nat) : Nat = (power φ n).irr
```

Wir potenzieren den Goldenen Schnitt und extrahieren anschließend den irrationalen Anteil. Ganz ähnlich sind wir auch in Abschnitt 4.1.1 bzw. 4.1.2 vorgegangen. Sie erinnern sich? Dort haben wir die Fibonacci-Funktion auf die Potenzierung von 2×2-Matrizen zurückgeführt. Beiden Implementierungen ist gemeinsam, dass sie $\mathscr{F}_n$ mit einer logarithmischen Anzahl an arithmetischen Grundoperationen berechnen. Im direkten Vergleich gewinnt die obige Implementierung: Sie ist rund doppelt so schnell, da 2×2-Matrizen aus vier Komponenten bestehen, Goldene Zahlen aber nur aus zwei.

Abbildung 4.5 fasst die Definitionen rund um die Goldene Arithmetik noch einmal zusammen — mit einem kleinen Twist, der es ermöglicht, die Operationen =, +, und $*$ auch für Goldene Zahlen zu verwenden.

Übungen.

⌨ **1.** (a) Schreiben Sie eine Funktion *minimum4*, die von vier natürlichen Zahlen das Minimum bestimmt.

```
let minimum4 (a : Nat, b : Nat, c : Nat, d : Nat) : Nat
```

(b) Schreiben Sie eine Funktion *sort4*, die vier natürliche Zahlen sortiert.

```
let sort4 (a : Nat, b : Nat, c : Nat, d : Nat) : Nat * Nat * Nat * Nat
```

Wie viele Vergleiche werden im schlechtesten Fall benötigt? Ist Ihre Definition optimal? Wie viele Vergleiche benötigt das beste Programm im schlechtesten Fall?

📝 **2.** Der Musterabgleich wird durch die Relation $p \sim \nu \Downarrow \delta$ formalisiert. Welche Umgebungen werden beim Abgleich der folgenden Werte und Muster jeweils erzeugt?

p	$\sim$	ν	$\Downarrow$	δ
a & b	$\sim$	4711	$\Downarrow$	
_ & b	$\sim$	4711	$\Downarrow$	
_	$\sim$	(4711, "Lisa")	$\Downarrow$	
$(n, \_)$	$\sim$	(4711, "Lisa")	$\Downarrow$	
(n, s)	$\sim$	(4711, "Lisa")	$\Downarrow$	
p & (n, s)	$\sim$	(4711, "Lisa")	$\Downarrow$	
t	$\sim$	(4711, (*false*, 815))	$\Downarrow$	
$(\_, p)$	$\sim$	(4711, (*false*, 815))	$\Downarrow$	
t & $(\_, p$ & $(\_, n))$	$\sim$	(4711, (*false*, 815))	$\Downarrow$	
t & $(m, p$ & $(b, n))$	$\sim$	(4711, (*false*, 815))	$\Downarrow$	

```
[< StructuralEquality; StructuredFormatDisplay ("{rat}+{irr}·ϕ") >]
type Golden =
  { rat : Nat; irr : Nat }
  static member (+) (a, b) =
    { rat = a.rat + b.rat; irr = a.irr + b.irr }
  static member (*) (a, b) =
    let ij = a.irr * b.irr
    { rat = a.rat * b.rat + ij; irr = a.rat * b.irr + b.rat * a.irr + ij }
```

Innerhalb der »Metaklammern« [<···>] werden der Typdefinition sogenannte ***Attribute*** (engl. attributes) vorangestellt, die die Handhabung des Recordtyps beeinflussen.

Das Attribut *StructuralEquality* erweitert den Gleichheitstest auf den Typ *Golden*: Zwei Goldene Zahlen sind gleich, $a = b$, wenn sie die gleichen Komponenten besitzen, $a.rat = b.rat$ && $a.irr = b.irr$. Man sagt auch, die Records sind strukturell gleich.

Das Attribut *StructuredFormatDisplay* (`"{rat}+{irr}·ϕ"`) legt die Ausgabe von Goldenen Zahlen fest: Statt der sonst üblichen Recordschreibweise $\{rat = r; irr = i\}$ wird das Format $r + i \cdot \phi$ verwendet.

Addition und Multiplikation sind hier Bestandteil der Typdefinition, angezeigt durch die Einrückung. Ähnlich wie der Gleichheitstest werden auf diese Weise die vordefinierten Operationen + und * auf den Typ *Golden* erweitert (die Definition wird jeweils statt mit **let** durch die Schlüsselwörter **static member** eingeläutet).

```
let ϕ : Golden = { rat = 0; irr = 1 }
let golden (n : Nat) : Golden = { rat = n; irr = 0 }
module NumericLiteralG =
  let FromZero ()          = golden 0
  let FromOne ()           = golden 1
  let FromInt32 (i : int)  = golden (Nat.nat i)
  let FromInt64 (l : int64) = golden (Nat.nat l)
  let FromString (s : string) = golden (Nat.nat s)
```

Das Modul *NumericLiteralG* dient ausschließlich der Bequemlichkeit; es ermöglicht, Konstanten des Typs *Golden* durch Anhängen des Buchstabens *G* zu notieren: Statt *golden* 4711 schreibt man kurz und bequem 4711*G*. Die folgenden Definitionen illustrieren die Abkürzungen.

```
let square (x : Golden) : Golden = x * x
let rec power (x : Golden) (n : Nat) : Golden =
  if n = 0 then 1G
       else if n % 2 = 0 then square (power x (n ÷ 2))
                         else square (power x (n ÷ 2)) * x
```

Abbildung 4.5.: Implementierung der Goldenen Zahlen.

3. Was ist der Unterschied zwischen

```
let x = e in … x …
```

und

```
let x () = e in … x () …
```

⌨ **4.** Nichtnegative rationale Zahlen können durch Paare von natürlichen Zahlen, den Zähler und den Nenner, repräsentiert werden.

```
type Ratio = {numerator : Nat; denominator : Nat}
```

Implementieren Sie die üblichen arithmetischen Operationen und die üblichen Vergleichsoperationen auf diesem Typ.

```
let add (a : Ratio, b : Ratio) : Ratio
…
let less (a : Ratio, b : Ratio) : Bool
```

Jede *positive* rationale Zahl hat eine eindeutige Darstellung, wenn man vereinbart, dass Nenner und Zähler teilerfremd sind. Erweitern Sie Ihre Implementierung, so dass die Rechenergebnisse stets gekürzt vorliegen. Wie kann die Null behandelt werden?

📝 **5.** Sei T ein beliebiger Typ, $e : T$ ein Element dieses Typs und $\circledast : T \to T \to T$ eine binäre Verknüpfung. Die n-te Potenz eines Elements, also die wiederholte Multiplikation mit sich selbst, lässt sich nach dem Peano oder nach dem Leibniz Entwurfsmuster berechnen.

```
let rec slow-power (x : T) (n : Nat) : T =
  if n = 0 then e
           else x ⊛ slow-power (x, n ÷ 1)
let square (x : T) : T = x ⊛ x
let rec fast-power (x : T) (n : Nat) : T =
  if n = 0 then e
           else if n % 2 = 0 then square (fast-power x (n ÷ 2))
                             else square (fast-power x (n ÷ 2)) ⊛ x
```

Welche Bedingungen müssen an e und $\circledast$ geknüpft werden, damit das Ergebnis identisch ist: *slow-power x n* = *fast-power x n*?

6. Wieviele Rechenschritte benötigt die naive Definition der Fibonacci-Funktion

```
let rec fibonacci (n : Nat) : Nat =
  if n ⩽ 1 then n
           else fibonacci (n − 1) + fibonacci (n − 2)
```

um $\mathscr{F}_n$ auszurechnen? Zählen Sie entweder die Anzahl der rekursiven Aufrufe oder die Zahl der durchgeführten Additionen.

📝 **7.** Zeigen Sie, dass die beiden Implementierungen der Fibonacci-Funktion, mittels Matrizenmultiplikation in Abschnitt 4.1.2 und mittels Goldener Zahlen in Abschnitt 4.1.3, im Wesentlichen die gleichen Rechnungen durchführen, und dass bei der Matrizenmultiplikation eine Teilrechnung doppelt durchgeführt wird.

8. Zeigen Sie die Beziehung zwischen den Goldenen Schnitten und den Fibonacci-Zahlen (4.2) mittels natürlicher Induktion.

4.2. Varianten

module Datatypes.Person

Eine Person ist entweder weiblich oder männlich[2]; eine männliche Person hat Attribute, die eine weibliche nicht hat (und vielleicht umgekehrt, das modellieren wir aber nicht).

```
type Woman = {name : String}
type Man   = {name : String; bald : Bool}
```

Daten, die unterschiedliche Ausprägungen besitzen, können wir in unserer Programmiersprache mit sogenannten ***Varianten*** modellieren. Ein einfacher Variantentyp für Personen ist zum Beispiel

```
type Person =
  | Female of Woman
  | Male   of Man
```

Variantentypen ähneln der Notation, mit der wir die abstrakte Syntax unserer Programmiersprache beschreiben. Diese Ähnlichkeit ist nicht zufällig. Die abstrakte Syntax beschreibt Alternativen: Ein Ausdruck ist *entweder* eine Boolesche Konstante *oder* eine Alternative *oder* eine Funktionsabstraktion *oder* eine Funktionsapplikation usw.

Zurück zu unserem Beispiel: Die Deklaration legt fest, dass eine Person *entweder* weiblich *oder* männlich ist; beide haben einen Namen, bei männlichen Personen wird zusätzlich der Zustand des Haupthaares modelliert.

Ähnlich wie Records müssen auch Varianten mit einer *Typdefinition* bekannt gemacht werden. Eine Variantentypdefinition führt zwei Arten von Bezeichnern ein. Zunächst wird nach dem Schlüsselwort ***type*** ein Typbezeichner festgelegt, in unserem Beispiel *Person*. Dieser Typname kann in anderen Typdefinitionen sowie in Typangaben verwendet werden. Auf der rechten Seite werden dann Bezeichner für die Elemente des neu definierten Variantentyps eingeführt, in unserem Beispiel *Female* und *Male*. Diese Bezeichner heißen auch ***Datenkonstruktoren*** oder kurz ***Konstruktoren***, da mit ihrer Hilfe Elemente des Variantentyps konstruiert werden: *Female* angewendet auf ein Element vom Typ *Woman* ist ein Element vom Typ *Person*; analog für *Male*. Hier sind zwei Beispielausdrücke vom Typ *Person*.

```
Female {name = "Lisa"}
Male {name = "Florian"; bald = false}
```

Wie immer können wir Ausdrücke auch an Bezeichner binden.

```
let ralf    = Male   {name = "Ralf";    bald = true}
let melanie = Female {name = "Melanie"}
let julia   = Female {name = "Julia"}
let andres  = Male   {name = "Andres"; bald = false}
```

Ein Variantentyp beschreibt Alternativen; mit Hilfe der ***Fallunterscheidung match*** können wir in einem Programm feststellen, welche konkrete Alternative vorliegt. Das folgende Programm bestimmt zum Beispiel in Abhängigkeit vom Geschlecht eine Anrede.

[2] Erinnern wir uns: Informatiker/-innen bilden abstrakte Modelle der konkreten Wirklichkeit. Die Wirklichkeitstreue dieser Modelle macht den Reiz und die Verantwortung bei der Softwareentwicklung aus. Dieses Modell dient als einführendes Beispiel und ist aus diesem Grund bewusst einfach gehalten, auf Kosten der Wirklichkeitstreue. Auch das Recht konstruiert Modelle der Wirklichkeit. Ende 2018 wurde im Zuge der Reform des Personenstandsgesetzes die zusätzliche Geschlechtsoption »divers« geschaffen, die Identitäten jenseits des binären Geschlechtermodells abdecken soll.

```
let dear (person : Person) : String =
  match person with
    | Female female → "Liebe " ^ female.name
    | Male   male   → (if male.bald
                         then "Lieber glatzköpfiger "
                         else "Lieber ") ^ male.name
```

Nach dem Schlüsselwort ***match*** steht der Ausdruck, der analysiert werden soll; die Zweige der Fallunterscheidung führen die verschiedenen Fälle des Variantentyps auf. Wertet etwa der Parameter *person* zu *Female* { *name* = "Lisa" } aus, dann wird mit der Auswertung des ersten Zweigs fortgefahren: *female* wird an { *name* = "Lisa" } gebunden und anschließend der Ausdruck nach dem Pfeil ausgerechnet.

```
  dear (Female { name = "Lisa" })
=   { Definition von dear }
  match Female { name = "Lisa" } with ···
=   { Auswertung der Fallunterscheidung }
  "Liebe " ^ "Lisa"
=   { Definition der Konkatenation }
  "Liebe Lisa"
```

Die Fallunterscheidung ist der Alternative ***if*** e_1 ***then*** e_2 ***else*** e_3 sehr ähnlich; wir werden später sehen, dass die Fallunterscheidung die Alternative verallgemeinert.

4.2.1. Binäre Varianten

Wie auch bei den Tupeln und Records führen wir nur die binäre Version der Varianten ein; alle Konstrukte verallgemeinern sich in naheliegender Weise auf Varianten mit n Alternativen.

Abstrakte Syntax Ein Variantentyp (engl. union oder variant type) wird durch eine *Definition* eingeführt.

$C \in \mathsf{Con}$	***Datenkonstruktoren***
$d ::= \cdots$	***Deklarationen:***
$\mid$ ***type*** T = $\mid C_1$ ***of*** t_1	Variantentypdefinition ($C_1 \neq C_2$)
$\mid C_2$ ***of*** t_2	

Der Bezeichner T wird durch die Definition neu eingeführt, ebenso die Konstruktoren C_1 und C_2. Die beiden Konstruktoren müssen verschieden sein: $C_1 \neq C_2$. Konstruktornamen müssen im Unterschied zu Bezeichnern mit einem *großen* Buchstaben anfangen. (Zur Erinnerung: Bezeichner können mit einem beliebigen Buchstaben anfangen.) Danach können weitere Buchstaben, kleine und große, Ziffern, und Sonderzeichen wie ein Unterstrich oder ein Apostroph folgen.

Auf Ebene der Ausdrücke führen wir Sprachkonstrukte ein, die Varianten konstruieren und analysieren.

$e ::= \cdots$	***Ausdrücke:***
$\mid C\ e$	Konstruktion\Injektion
$\mid$ ***match*** e ***with*** $\mid C_1\ x_1 \to e_1$	Fallunterscheidung ($C_1 \neq C_2$)
$\mid C_2\ x_2 \to e_2$	

Der Ausdruck e zwischen den Schlüsselwörtern ***match*** und ***with*** heißt ***Diskriminatorausdruck***; $C_1\ x_1 \to e_1$ und $C_2\ x_2 \to e_2$ sind ***Zweige*** der Fallunterscheidung. Die Konstruktoren der beiden Zweige müssen verschieden sein: $C_1 \neq C_2$. Die einzelnen Zweige binden Bezeichner: In $C_i\ x_i \to e_i$ wird der Bezeichner x_i an das Argument des Konstruktors C_i gebunden und ist in e_i sichtbar.

Statische Semantik: Vorüberlegungen ⋆ Wie Recordtypen dürfen auch Variantentypen weder redefiniert noch lokal definiert werden. Das folgende Beispiel, eine Adaption des entsprechenden Programms für Recordtypen, illustriert, was schieflaufen kann.

```
type Oh = | Je of Bool
let na-und (oh : Oh) : Bool = match oh with | Je b → not b
type Oh = | Je of Nat
let egal = na-und (Je 4711)
```

Wieder schmuggeln wir eine natürliche Zahl an eine Stelle, an der ein Boolescher Wert erwartet wird.

Ein ähnliches Problem tritt auf, wenn Typen lokal definiert werden und ein Typbezeichner aus dem lokalen Kontext entweicht.

```
(type Oh = | Je of Bool in fun (oh : Oh) : Bool → match oh with | Je b → not b)
  (type Oh = | Je of Nat in Je 4711)
```

Der erste Teilausdruck der Funktionsanwendung hat den Typ $Oh \to Bool$, der zweite den Typ Oh. Aber wiederum handelt es sich um zwei verschiedene Typen. Deshalb: Variantentypen dürfen *weder* redefiniert *noch* lokal definiert werden.

Statische Semantik Die folgenden Typregeln setzen voraus, dass der Variantentyp

```
type T = | C1 of t1 | C2 of t2
```

bekannt ist. Für jeden Variantentyp gibt es einen entsprechenden Satz von Regeln.

Die Regel für die Fallunterscheidung verallgemeinert im gewissen Sinne die Regel für die Alternative — in der Vertiefung kommen wir darauf noch einmal zurück.

$$\frac{\Sigma \vdash e : t_i}{\Sigma \vdash C_i\ e : \mathrm{T}} \quad i \in \{1, 2\}$$

$$\frac{\Sigma \vdash e : \mathrm{T} \qquad \Sigma, \{x_1 \mapsto t_1\} \vdash e_1 : t' \qquad \Sigma, \{x_2 \mapsto t_2\} \vdash e_2 : t'}{\Sigma \vdash (\textbf{match}\ e\ \textbf{with} \mid C_1\ x_1 \to e_1 \mid C_2\ x_2 \to e_2) : t'}$$

$$\frac{\Sigma \vdash e : \mathrm{T} \qquad \Sigma, \{x_1 \mapsto t_1\} \vdash e_1 : t' \qquad \Sigma, \{x_2 \mapsto t_2\} \vdash e_2 : t'}{\Sigma \vdash (\textbf{match}\ e\ \textbf{with} \mid C_2\ x_2 \to e_2 \mid C_1\ x_1 \to e_1) : t'}$$

Alle Zweige der Fallunterscheidung müssen den gleichen Typ besitzen; dieser ist auch der Typ des gesamten Ausdrucks. Die einzelnen Zweige binden wie gesagt Bezeichner: In $C_i\ x_i \to e_i$ ist der Bezeichner x_i im Rumpf e_i sichtbar. Die Reihenfolge der beiden Zweige ist irrelevant.

Ein Konstruktor ist einer Funktion nicht unähnlich. Der Typ nach dem Konstruktor korrespondiert zum Argumenttyp, der deklarierte Variantentyp korrespondiert zum Ergebnistyp. Der Konstruktor *Female* hat somit im Prinzip den Typ $Woman \to Person$ und *Male* den Typ $Man \to Person$. Im Unterschied zu einer Funktion hat ein Konstruktor aber keine Definition; er steht sozusagen für sich selbst.

Dynamische Semantik Wie Recordtypdefinitionen können auch Variantentypdefinitionen in der dynamischen Semantik ignoriert werden.

Konstruktoren konstruieren Werte, entsprechend müssen wir den Bereich der Werte erweitern.

$v ::= \cdots$	***Werte:***
$\mid C\ v$	Konstruktion\Injektion in einen Variantentyp

Ein Konstruktoraufruf wird ausgerechnet, indem das Argument ausgewertet wird und der resultierende Wert mit dem Konstruktor »markiert« wird (engl. tagging).

$$\frac{\delta \vdash e \Downarrow v}{\delta \vdash C\ e \Downarrow C\ v}$$

In einer Fallunterscheidung wird zunächst der Diskriminatorausdruck ausgerechnet; abhängig vom Ergebnis wird dann genau ein Zweig ausgewertet. Dabei wird der Bezeichner x_i an das Argument von C_i gebunden.

$$\frac{\delta \vdash e \Downarrow C_i\ v_i \qquad \delta, \{x_i \mapsto v_i\} \vdash e_i \Downarrow v}{\delta \vdash (\textbf{\textit{match}}\ e\ \textbf{\textit{with}} \mid C_1\ x_1 \to e_1 \mid C_2\ x_2 \to e_2) \Downarrow v} \quad i \in \{1,2\}$$

$$\frac{\delta \vdash e \Downarrow C_i\ v_i \qquad \delta, \{x_i \mapsto v_i\} \vdash e_i \Downarrow v}{\delta \vdash (\textbf{\textit{match}}\ e\ \textbf{\textit{with}} \mid C_2\ x_2 \to e_2 \mid C_1\ x_1 \to e_1) \Downarrow v} \quad i \in \{1,2\}$$

Bevor wir uns den Beispielprogrammen zuwenden, überlegen wir noch kurz, wie die Konstrukte und Regeln für Varianten mit n Alternativen aussehen.

Ist $n = 0$, so haben wir einen Typ ohne Alternativen, sprich einen *leeren* Typ. Die Fallunterscheidung hat entsprechend keine Zweige: ***match*** *e* ***with***. Es gibt auch keine Auswertungsregeln für die leere Fallunterscheidung — wir können ja keinen Diskriminatorausdruck e konstruieren, der den passenden Typ hat. Allgemein signalisiert die leere Fallunterscheidung ***toten Code***.

```
type Empty = |
let you-cannot-call-me (x : Empty) : Nat = match x with
```

(F# erlaubt keine leeren Variantentypen.)

Ist $n = 1$, so umfasst der Typ genau einen Konstruktor und die Fallunterscheidung entsprechend einen Zweig. Zum Beispiel:

```
type Price    = | Cent of Nat
type Postcode = | Code of Nat
```

Im Gegensatz zu 1-Tupeln sind 1-Varianten sehr nützlich: Sind *Price* und *Postcode* wie oben definiert, so stellt die statische Semantik sicher, dass wir in einem Programm nicht aus Versehen Preise und Postleitzahlen addieren — *Price* und *Postcode* sind unterschiedliche, inkompatible Typen. Auch lässt sich ein Preis p nicht mit $2 * p$ verdoppeln. Zu diesem Zweck müssen wir extra eine Funktion schreiben.

```
let double (price : Price) : Price =
  match price with | Cent n → Cent (2 * n)
```

Der Gewinn an Sicherheit wird mit einem Verlust an Bequemlichkeit erkauft.

Ist $n = 3$, so haben wir drei Alternativen und entsprechend ***match***-Ausdrücke mit drei Zweigen.

Ist $n = 4$, so haben wir vier Alternativen …

Vertiefung: Aufzählungstypen Wir haben schon kurz anklingen lassen, dass Fallunterscheidungen Alternativen verallgemeinern. Der Typ *Bool* kann in der Tat als Variantentyp aufgefasst werden bzw. durch einen Variantentyp implementiert werden.

```
type Bool = | False of Unit | True of Unit
```

Die Wahrheitswerte *false* und *true* werden durch die Ausdrücke *False* () und *True* () repräsentiert. Die Konstruktoren sind sozusagen »nullstellig«, formalisiert durch *Unit*, den Typ des leeren Tupels. Die Alternative *if* e_1 *then* e_2 *else* e_3 kann entsprechend durch die Fallunterscheidung *match* e_1 *with* | *False* () → e_3 | *True* () → e_2 realisiert werden. »Nullstellige« Konstruktoren wie *False* oder *True* kommen relativ häufig vor. Aus diesem Grund erlauben wir, das Dummyargument auch wegzulassen, sowohl bei der Deklaration, als auch bei der Konstruktion und der Analyse. Die Definition der Wahrheitswerte verkürzt sich damit zu

```
type Bool = | False | True
```

Variantentypen, die *nur* nullstellige Konstruktoren umfassen, nennt man auch ***Aufzählungstypen*** (engl. enumeration types), da sie ihre Element gewissermaßen nacheinander aufzählen: Ein Wahrheitswert ist entweder *False* oder *True*.

Vertiefung: Repräsentationswechsel Mit Tupeln bzw. Records und Varianten haben wir zwei grundlegende Strukturierungselemente für Daten kennengelernt. Statt von Tupeln und Varianten spricht man auch von ***Produkten*** und ***Summen***. Produkt deshalb, weil die Anzahl der Elemente von $t_1 * t_2$, die sogenannte ***Kardinalität***, gleich dem Produkt der Kardinalitäten von t_1 und t_2 ist.[3] Summe deshalb, weil die Kardinalität von T mit *type* T = | C_1 *of* t_1 | C_2 *of* t_2, gleich der Summe der Kardinalitäten von t_1 und t_2 ist. Die Korrespondenz zwischen den arithmetischen Operationen und den Typkonstruktoren geht aber noch tiefer: In der gleichen Weise wie Addition und Multiplikation interagieren — ausgedrückt im ***Distributivgesetz*** $(a+b)\cdot c = a\cdot c + b\cdot c$ — so interagieren auch Records und Varianten. Kommen wir noch einmal auf die Definition von *Person* zurück.

```
type Woman = {name : String}
type Man   = {name : String; bald : Bool}
type Person = | Female of Woman | Male of Man
```

Beiden Alternativen von *Person* ist der Name gemeinsam; diesen gemeinsamen »Faktor« können wir mit Hilfe des Distributivgesetzes auch herausziehen und Personen alternativ darstellen durch

```
type Person' = {name : String; gender : Gender}
type Male'   = {bald : Bool}
type Gender = | Female' | Male' of Male'
```

Das Geschlecht umfasst die trennenden Merkmale, die gemeinsamen sind in *Person′* zusammengefasst.

Die Typen *Person* und *Person′* sind wechselseitig austauschbar, sie sind im Fachjargon ***isomorph***: Jedem Element aus *Person* lässt sich eineindeutig[4] ein Element aus *Person′* zuordnen. Die Funktionen *from-Person* und *to-Person* belegen diese Tatsache.

[3] Wir setzen stillschweigend voraus, dass die beteiligten Typen nur endlich viele Elemente enthalten.

[4] Das Adjektiv »eineindeutig« bedeutet umkehrbar eindeutig, eindeutig in beide Richtungen. Eine eineindeutige Abbildung nennt man auch ***Bijektion***, siehe Anhang B.2.3.

```
let from-Person (p : Person) : Person′ =
  match p with
   | Female f  → { name = f.name;  gender = Female′ }
   | Male   m → { name = m.name; gender = Male′ { bald = m.bald } }
let to-Person (p′ : Person′) : Person =
  match p′.gender with
     | Female′  → Female { name = p′.name }
     | Male′ m′ → Male   { name = p′.name; bald = m′.bald }
```

Welcher Repräsentation beim Programmieren der Vorzug gegeben wird, hängt vom Zugriffsmuster ab: Wird oft auf den Namen zugegriffen, dann ist die zweite Version vorteilhaft; hängt vieles vom Geschlecht ab, dann ist die erste Version vorzuziehen.

4.2.2. Rekursive Varianten

Mit den Konstrukten, die wir bisher eingeführt haben, können wir nur eine beschränkte Anzahl von Daten zusammenfassen: Ein 7-Tupel aggregiert 7 Daten, ein 128-Tupel 128 Daten; beide sind ungeeignet um 6, 8, 127 oder 129 Daten aufzunehmen. Nun kommt es häufig vor, dass man zum Zeitpunkt des Programmierens die genaue Anzahl von Daten nicht kennt: Wieviele Personen immatrikulieren sich im WS 2024/2025? Wieviele Unternehmen sind an der Börse notiert? Wieviele Mitarbeiter hat eine Abteilung? usw. Auch wenn man die Anzahl kennt — weil vielleicht nur 128 Personen zum Studium angenommen werden — ist ein n-Tupel zu unhandlich: ein Ausdruck, der ein 128-Tupel konstruiert, hat eben 128 Teilausdrücke, die erst einmal aufgeschrieben werden wollen.

Im Folgenden überlegen wir, wie wir eine beliebige Folge von natürlichen Zahlen repräsentieren können. Wenn wir naiv für jede Länge eine Alternative definieren, erhalten wir den folgenden Variantentyp (wir lassen die Datenkonstruktoren zunächst weg).

```
type Nats = | Unit | Nat | Nat * Nat | Nat * Nat * Nat | ⋯
```

In Worten ausgedrückt: Eine Folge von natürlichen Zahlen ist entweder die leere Folge (ein 0-Tupel vom Typ *Unit*), oder eine einelementige Folge (ein 1-Tupel), oder eine zweielementige Folge (ein 2-Tupel) usw. Das Plural 's' im Bezeichner *Nats* soll andeuten, dass ein Element dieses Typs viele natürliche Zahlen umfasst.

Die Ellipse (⋯) zeigt an, dass wir noch keine vollständige Definition vor uns haben. Wir müssen die Definition noch etwas massieren. Es ist klar, dass alle Alternativen bis auf die erste mindestens eine *Nat* Komponente haben. Wenn wir diese Komponente »herausziehen«, erhalten wir (das ist keine gültige Typdefinition, aber das soll uns im Moment nicht stören):

```
data Nats = | Unit | Nat * (Unit | Nat | Nat * Nat | ⋯)
```

Aus einem $n+1$-Tupel wird jeweils ein n-Tupel. Formal liegt dem »Herausziehen« das Distributivgesetz zugrunde, das uns schon im letzten Abschnitt begegnet ist. Jetzt sind wir fast am Ziel. Der Typ der zweiten Komponente ist identisch mit der rechten Seite der ursprünglichen Definition von *Nats*. Erlauben wir bei der Definition eines Variantentyps den Rückgriff auf den definierten Typ selbst (!), so erhalten wir die folgende, kompakte Definition (jetzt mit Datenkonstruktoren; *Nil of Unit* verkürzt sich zu *Nil*).

```
type Nats = | Nil | Cons of Nat * Nats
```

In Worten ausgedrückt: Eine Folge von natürlichen Zahlen ist entweder die leere Folge *Nil* oder eine mindestens einelementige Folge *Cons* (n, ns) bestehend aus einer natürlichen Zahl n und

einer Folge von natürlichen Zahlen *ns*. Statt von einer Folge von natürlichen Zahlen spricht man auch kurz von einer ***Liste***. Entsprechend heißt die Zahl *n* ***Kopfelement*** der Liste *Cons* (n, ns) und *ns* ***Restliste***. Die Folge der ersten vier Primzahlen wird zum Beispiel durch den Ausdruck *Cons* $(2, \mathit{Cons}\ (3, \mathit{Cons}\ (5, \mathit{Cons}\ (7, \mathit{Nil}))))$ repräsentiert; die natürliche Zahl 2 ist das Kopfelement dieser Liste und *Cons* $(3, \mathit{Cons}\ (5, \mathit{Cons}\ (7, \mathit{Nil})))$ die Restliste. Bei Listen ist wie bei Tupeln die Reihenfolge der Elemente signifikant: *Cons* $(7, \mathit{Cons}\ (2, \mathit{Cons}\ (5, \mathit{Cons}\ (3, \mathit{Nil}))))$ ist eine gänzlich andere Liste.

Listen sind die erste und einfachste ***Datenstruktur***, die uns begegnet. Eine Datenstruktur verwaltet Daten und unterstützt Zugriff und Manipulation dieser Daten.

Rekursive Typen sind für uns eigentlich nichts Neues. Bei der Beschreibung der abstrakten Syntax unserer Programmiersprache sind sie uns schon wiederholt begegnet: Ein Ausdruck ist zum Beispiel eine Alternative, diese besteht aus drei Teilausdrücken; ein Muster hat zum Beispiel die Form $p_1 \,\&\, p_2$, wobei p_1 und p_2 wiederum Muster sind. Fast alle syntaktischen Bereiche sind rekursiv definiert. Mit Hilfe rekursiver Variantentypen haben wir sozusagen Baumsprachen vollständig in unsere Programmiersprache integriert!

Wie gehen wir mit einem rekursiven Variantentyp um? Wir konstruieren und analysieren rekursive Varianten mit Hilfe rekursiver Funktionen! Wenden wir uns zunächst der Verarbeitung von Listen zu und übertragen die Funktion *sort2* bzw. *sort3* auf Listen.

```
⋙ sort (Cons (7, Cons (2, Cons (5, Cons (3, Nil)))))
Cons (2, Cons (3, Cons (5, Cons (7, Nil))))
```

Der Variantentyp gibt das folgende Skelett für die Sortierfunktion vor.

```
let rec sort (nats : Nats) : Nats =
  match nats with
    | Nil          → …
    | Cons (n, ns) → …
```

Die leere Liste zu sortieren ist einfach; sie ist bereits geordnet. Wie aber füllen wir den Fall der mindestens einelementigen Liste mit Leben? Getreu dem Motto »rekursive Funktionen für rekursive Typen« können wir *sort* auf die Restliste *ns* anwenden. Wir erhalten eine geordnete Liste, bei der lediglich das Kopfelement *n* fehlt. (Die Vorgehensweise ist ähnlich wie bei der Definition von *sort3*, nur dass *sort3* sich auf *sort2* abstützt.) Das Element *n* ist aber nicht notwendigerweise das kleinste Element, wir müssen es an die richtige Stelle einordnen. Ein Element in eine geordnete Liste einfügen, das hört sich nach einer anspruchsvolleren Teilaufgabe an. Wir geben dieser Teilaufgabe einen Namen, *insert*, und können damit die Definition von *sort* vervollständigen.

```
let rec sort (nats : Nats) : Nats =
  match nats with
    | Nil          → Nil
    | Cons (n, ns) → insert (n, sort ns)
```

Die Definition der Hilfsfunktion *insert* gehen wir auf die gleiche Art und Weise an.[5]

```
let rec insert (nat : Nat, nats : Nats) : Nats =
  match nats with
    | Nil          → …
    | Cons (n, ns) → …
```

[5] Im tatsächlichen Programmtext muss *insert* vor *sort* definiert werden, da letztere Funktion sich auf erstere abstützt.

Ist die Liste leer, so geben wir die einelementige Liste *Cons* (*nat*, *Nil*) zurück. Im anderen Fall wissen wir, dass das Kopfelement *n* das Minimum der Liste *nats* ist. Wenn nun das einzufügende Element *nat* gleich oder kleiner als *n* ist, müssen wir *nat* an den Anfang der Liste stellen:

```
let rec insert (nat : Nat, nats : Nats) : Nats =
  match nats with
    | Nil          → Cons (nat, Nil)
    | Cons (n, ns) → if nat ⩽ n then Cons (nat, nats)
                                else  …
```

Ist *nat* größer als *n*, so bleibt *n* das kleinste Element: die resultierende Liste hat somit die Form *Cons* (*n*, …). Es verbleibt, *nat* in die Restliste *ns* einzufügen. Getreu dem Motto »rekursive Funktionen für rekursive Typen« können wir dafür *insert* verwenden. Die vollständige Definition von *insert* lautet somit

```
let rec insert (nat : Nat, nats : Nats) : Nats =
  match nats with
    | Nil          → Cons (nat, Nil)
    | Cons (n, ns) → if nat ⩽ n then Cons (nat, nats)
                                else  Cons (n, insert (nat, ns))
```

Die gezeigte Vorgehensweise ist typisch für die Verarbeitung von Listen und lässt sich als Problemlösungsstrategie formulieren: Wir lösen das Problem zunächst für die leere Liste (***Rekursionsbasis***); um das Problem für eine mindestens einelementige Liste zu lösen, bestimmen wir zunächst rekursiv die Lösung für die Restliste und erweitern diese dann zu einer Gesamtlösung (***Rekursionsschritt***). Mit anderen Worten, wir haben ein ***Entwurfsmuster*** gefunden, um listenverarbeitende Funktionen zu definieren.

Struktur Entwurfsmuster

```
let rec f (nats : Nats) : t =
  match nats with
    | Nil          → …                  Rekursionsbasis
    | Cons (n, ns) → … n … f ns …       Rekursionsschritt
```

Da wir uns eng an der Struktur des Listentyps orientieren — eine Liste ist entweder leer oder besteht aus einem Kopf*element* und einer Rest*liste* — nennen wir das Schema ***Struktur Entwurfsmuster*** für *Nats*.

Erproben wir das Struktur Entwurfsmuster. Nehmen wir an, wir wollen eine gegebene Liste nicht aufsteigend, sondern absteigend sortieren. Wir können natürlich das Programm für *sort* hernehmen und »⩽« systematisch durch »⩾« ersetzen. Eine solche Duplizierung des Programmcodes ist aber unökonomisch. Alternativ können wir die Liste zunächst aufsteigend sortieren und sie dann einfach umdrehen.

```
let decreasing-sort (nats : Nats) : Nats = reverse (sort nats)
```

Die Funktion *reverse* ist genau wie *insert* von allgemeinem Nutzen. Wir sehen, die Identifizierung von Teilproblemen und die Programmierung von Teillösungen beschert uns eine Menge nützlicher Funktionen.

```
let rec reverse (nats : Nats) : Nats =
  match nats with
    | Nil          → Nil
    | Cons (n, ns) → … reverse ns …
```

Nachdem wir *reverse* rekursiv auf *ns* anwendet haben, müssen wir noch *n* hinter die resultierende Liste setzen. Listen — wie wir sie definiert haben — sind allerdings asymmetrisch. Auf das erste Element einer Liste können wir direkt zugreifen, auf das letzte Element nicht. Ein Element einer Liste voranzustellen ist einfach; um ein Element hinten anzustellen, müssen wir Aufwand betreiben. Sprich, wir müssen eine entsprechende Funktion programmieren. Da wir mittlerweile schon etwas im Umgang mit Listen geübt sind, hier gleich die vollständige Definition.

```
let rec put-last (nats : Nats, nat : Nat) : Nats =
  match nats with
    | Nil          → Cons (nat, Nil)
    | Cons (n, ns) → Cons (n, put-last (ns, nat))
```

Die Funktion erledigt ihren Job, ist aber unnötig speziell: *put-last* bildet im Basisfall die leere Liste auf eine einelementige Liste ab. Verallgemeinern wir die einelementige Liste zu einer beliebigen Liste, erhalten wir eine flexiblere Funktion.

```
let rec append (nats₁ : Nats, nats₂ : Nats) : Nats =
  match nats₁ with
    | Nil          → nats₂
    | Cons (n, ns) → Cons (n, append (ns, nats₂))
```

Die Funktion *append* hängt zwei Listen aneinander; *put-last* lässt sich einfach mit Hilfe von *append* implementieren: *append* (*nats*, *Cons* (*nat*, *Nil*)). Die Umkehrung gilt nicht.

Somit können wir die Definition von *reverse* vervollständigen.

```
let rec reverse (nats : Nats) : Nats =
  match nats with
    | Nil          → Nil
    | Cons (n, ns) → append (reverse ns, Cons (n, Nil))
```

module Datatypes.Sort

Kommen wir noch einmal auf die ursprüngliche Aufgabenstellung zurück: die absteigende Sortierung einer Liste. Wenn wir die Aufgabenstellung etwas verallgemeinern und von der speziellen Ordnungsrelation abstrahieren, ergibt sich ein weiterer Lösungsansatz. Von einer speziellen Ordnungsrelation abstrahieren heißt, dass wir »⩽« bzw. »⩾« nicht fest im Programm verdrahten, sondern zum Parameter der Sortierfunktion machen.

```
let sort-by (less-equal : Nat * Nat → Bool) : Nats → Nats =
  let rec insert (nat : Nat, nats : Nats) : Nats =
    match nats with
      | Nil          → Cons (nat, Nil)
      | Cons (n, ns) → if less-equal (nat, n) then Cons (nat, nats)
                                              else Cons (n, insert (nat, ns))
  let rec sort (nats : Nats) : Nats =
    match nats with
      | Nil          → Nil
      | Cons (n, ns) → insert (n, sort ns)
  in sort
```

Die Hilfsfunktionen *insert* und *sort* werden mit Hilfe einer lokalen Deklaration eingeführt. Aufgrund der Sichtbarkeitsregeln ist der formale Parameter von *sort-by*, die Ordnungsrelation *less-equal*, auch im Rumpf der Hilfsfunktionen sichtbar. Die Funktion *sort-by* gibt als Ergebnis die für die jeweilige Ordnungsrelation spezialisierte Sortierfunktion zurück.

Die ursprünglichen Sortierfunktionen sind jetzt hausbackene Spezialfälle:

```
let increasing-sort = sort-by (fun (m, n) → m ⩽ n)
let decreasing-sort = sort-by (fun (m, n) → m ⩾ n)
```

Die Funktion *sort-by* ist ein weiteres Beispiel für eine Funktion höherer Ordnung: *sort-by* nimmt eine Funktion als Argument (*less-equal*) und gibt eine Funktion (*sort*) als Ergebnis zurück. Genau wie *append* aus *put-last* hervorgeht, so entsteht *sort-by* aus *sort*: durch Verallgemeinerung der Aufgabenstellung. In beiden Fällen bleibt der Implementierungsaufwand der gleiche; wir erhalten aber Funktionen, die nützlicher und flexibler sind.

Wenden wir uns nach dem Studium der ***listenverarbeitenden*** Funktionen kurz den ***listenerzeugenden*** Funktionen zu. Programmieren wir eine Funktion, die eine Liste aller Elemente in einem gegebenen Intervall erzeugt. In Abschnitt 3.6 haben wir schon etwas Erfahrung im Umgang mit Intervallen gesammelt. Die Lektionen legen nahe, das Peano Entwurfsmuster auf die Intervallgröße anzuwenden.

```
let rec between (l : Nat, u : Nats) : Nats =
  if l > u then Nil
           else Cons (l, between (l + 1, u))
```

Im Basisfall geben wir die leere Liste zurück; im Rekursionsfall setzen wir die linke Intervallgrenze vor die rekursiv erzeugte Liste.

Abstrakte Syntax … Weder die abstrakte Syntax noch die statische oder dynamische Semantik von Varianten ändert sich. Die Tatsache, dass wir einem Variantentyp immer einen eindeutigen Namen geben — was wir ja zum Beispiel bei Tupeltypen der Form $t_1 * t_2$ nicht machen — ermöglicht die problemlose Erweiterung von Variantentypen auf *rekursive* Variantentypen.

Vertiefung: Unäre Zahlendarstellung Im Abschnitt 4.2.1 haben wir gesehen, dass die Booleschen Werte durch einen Variantentyp implementiert werden können. Überraschenderweise gilt dies auch für die natürlichen Zahlen. Die Definition lässt sich leicht motivieren, wenn wir uns noch einmal das Peano Entwurfsmuster ins Gedächtnis rufen. Das Entwurfsmuster basiert auf der Tatsache, dass jede natürliche Zahl entweder 0 oder von der Form $n + 1$ ist, wobei n wiederum eine natürliche Zahl ist. Machen wir Null und die Nachfolgerfunktion zu Datenkonstruktoren, so erhalten wir

```
type Peano =
  | Zero
  | Succ of Peano
```

Die Zahlendarstellung unserer Urahnen: Für jedes erlegte Bison einen Strich. Die Zahl n wird durch n Anwendungen des Konstruktors *Succ* auf den Konstruktor *Zero* repräsentiert. Wir zählen: *Zero*, *Succ Zero*, *Succ* (*Succ Zero*), *Succ* (*Succ* (*Succ Zero*)) usw. Diese Repräsentation heißt auch ***unäre Zahlendarstellung***.

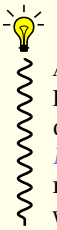
Die Implementierungen von Addition, Multiplikation usw. lassen sich einfach aus Abschnitt 3.6 adaptieren. Die Konstante 0 wird zu *Zero*, der Ausdruck $e + 1$ wird zu *Succ* e und die Alternative *if* $n = 0$ *then* … *else* … $n \div 1$ … wird zur Fallunterscheidung *match* n *with* | *Zero* → … | *Succ* n' → … n' …. Zum Beispiel: Die ursprünglichen Definition der Addition

```
let rec add (m : Nat, n : Nat) : Nat =
  if m = 0 then n
           else add (m ÷ 1, n) + 1
```

lässt sich wie folgt auf die neue Zahlendarstellung übertragen:

```
let rec add (m : Peano, n : Peano) : Peano =
  match m with
    | Zero    → n
    | Succ m' → Succ (add (m', n))
```

Wir halten fest: Der Konstruktor *Zero* korrespondiert zu 0, *Succ e* zu $e + 1$ und das Peano Entwurfsmuster entspricht dem Struktur Entwurfsmuster für den Variantentyp *Peano*.



Erkenntnis

Aus Sicht der Theorie sind mit dem Einzug rekursiver Variantentypen die vordefinierten Typen *Bool* und *Nat* entbehrlich geworden — biedere Spezialfälle. Aus praktischen Erwägungen behalten wir sie aber bei.

Vertiefung: Binäre Zahlendarstellung Können wir aus dem Leibniz Entwurfsmuster eine alternative Darstellung der natürlichen Zahlen ableiten? Überlegen wir: Das Leibniz Entwurfsmuster basiert auf der Tatsache, dass jede natürliche Zahl entweder 0, oder von der Form $2 \cdot n$ bzw. $2 \cdot n+1$ ist, wobei n wiederum eine natürliche Zahl ist.[6] Anders ausgedrückt, eine natürliche Zahl ist entweder Null, gerade oder ungerade. Fangen wir die drei Fälle mit Datenkonstruktoren ein, so erhalten wir

```
type Leibniz =
  | Null
  | Even of Leibniz
  | Odd  of Leibniz
```

Jetzt zählen wir wie folgt: *Null*, *Odd Null*, *Even* (*Odd Null*), *Odd* (*Odd Null*) usw. Um das Bildungsgesetz zu sehen, ist es am einfachsten, wenn wir die Nachfolgerfunktion programmieren.

```
let rec succ (nat : Leibniz) : Leibniz =
  match nat with
    | Null    → Odd Null
    | Even n → Odd n
    | Odd  n → Even (succ n)
```

In Worten und Formeln: der Nachfolger von 0 ist 1, der Nachfolger von $2 \cdot n$ ist $2 \cdot n + 1$, der Nachfolger von $2 \cdot n + 1$ ist $2 \cdot n + 2 = 2 \cdot (n + 1)$. Mit Hilfe von *succ* können wir jede natürliche Zahl in die neue Darstellung überführen, siehe Übung 4.2.2.

Die umgekehrte Fragestellung ist genauso interessant: Welche natürliche Zahl wird zum Beispiel durch *Odd* (*Odd* (*Even* (*Odd Null*))) repräsentiert? Nun, *Even e* repräsentiert $2 \cdot n$, *Odd e* repräsentiert $2 \cdot n + 1$, wenn *e* die Zahl *n* repräsentiert. Somit stellt *Odd* (*Odd* (*Even* (*Odd Null*))) die Zahl 11 dar: $2 \cdot (2 \cdot (2 \cdot (2 \cdot 0 + 1)) + 1) + 1 = 11$. Diese Umformung können wir ebenfalls in Rechenregeln gießen.

```
let rec natural (nat : Leibniz) : Nat =
  match nat with
    | Null    → 0
    | Even n → 2 * natural n
    | Odd  n → 2 * natural n + 1
```

[6] Diese drei Fälle sind nicht disjunkt; in der Vorlesung diskutieren wir eine alternative Darstellung mit disjunkten Fällen: Jede natürliche Zahl ist entweder 0 oder von der Form $2 \cdot n + 1$ bzw. $2 \cdot n + 2$.

Die Funktion *natural* ordnet einer Zahlendarstellung ihren Zahlenwert zu, einer konkreten Repräsentation ihre abstrakte Bedeutung. (Der Typ *Leibniz* ist konkret: Wir kennen seine Definition und wissen welche Elemente er umfasst. Der Typ *Nat* hingegen ist abstrakt: Seine Implementierung ist uns nicht bekannt.)

Die Funktion *natural* hat noch einen anderen Verwendungszweck: Mit ihrer Hilfe können wir arithmetische Operationen auf dem Typ *Leibniz* ***spezifizieren***. Eine Spezifikation beschreibt, *was* eine Funktion leisten soll; im Unterschied zu einer Implementierung, die genau festlegen, *wie* eine Funktion ihr Ergebnis ermittelt. Die Nachfolgerfunktion und die Addition lassen sich wie folgt spezifizieren:

$$natural\ (succ\ e) = natural\ e + 1 \tag{4.3a}$$
$$natural\ (add\ (e_1, e_2)) = natural\ e_1 + natural\ e_2 \tag{4.3b}$$

Die zweite mathematische Gleichung können wir benutzen, um eine Implementierung der Addition *herzuleiten*. Der Typ *Leibniz* gibt zunächst einmal das folgende Schema vor:

```
let rec add (m : Leibniz, n : Leibniz) : Leibniz =
  match m with
    | Null    → …
    | Even m' → …
    | Odd  m' → …
```

Um die Definition für den Basisfall $m = Null$ zu bestimmen, rechnen wir

```
  natural (add (Null, n))
=   { Spezifikation von add (4.3b) }
  natural Null + natural n
=   { Definition von natural }
  0 + natural n
=   { 0 ist das neutrale Element von »+« }
  natural n
```

Es muss also $natural\ (add\ (Null, n)) = natural\ n$ gelten; diese Gleichung können wir erfüllen, wenn wir im Basisfall n zurückgeben. Klar: 0 ist das neutrale Element der Addition. In den beiden anderen Fällen $m = Even\ m'$ und $m = Odd\ m'$ müssen wir eine Fallunterscheidung über das zweite Argument vornehmen:

```
let rec add (m : Leibniz, n : Leibniz) : Leibniz =
  match m with
    | Null    → n
    | Even m' → match n with | Null    → …
                             | Even n' → …
                             | Odd  n' → …
    | Odd  m' → match n with | Null    → …
                             | Even n' → …
                             | Odd  n' → …
```

Die beiden Fälle $n = Null$ sind symmetrisch zum Fall $m = Null$. Sind beide Zahlen gerade, so

können wir herleiten.

$$
\begin{aligned}
& \mathit{natural}\ (\mathit{add}\ (\mathit{Even}\ m', \mathit{Even}\ n')) \\
= & \quad \{\ \text{Spezifikation von } \mathit{add}\ (4.3\text{b})\ \} \\
& \mathit{natural}\ (\mathit{Even}\ m') + \mathit{natural}\ (\mathit{Even}\ n') \\
= & \quad \{\ \text{Definition von } \mathit{natural}\ \} \\
& 2 * \mathit{natural}\ m' + 2 * \mathit{natural}\ n' \\
= & \quad \{\ \text{Distributivgesetz}\ \} \\
& 2 * (\mathit{natural}\ m' + \mathit{natural}\ n') \\
= & \quad \{\ \text{Spezifikation von } \mathit{add}\ (4.3\text{b})\ \} \\
& 2 * (\mathit{natural}\ (\mathit{add}\ (m', n'))) \\
= & \quad \{\ \text{Definition von } \mathit{natural}\ \} \\
& \mathit{natural}\ (\mathit{Even}\ (\mathit{add}\ (m', n')))
\end{aligned}
$$

Die Rechnung legt nahe, dass $\mathit{add}\ (\mathit{Even}\ m', \mathit{Even}\ n')$ zu $\mathit{Even}\ (\mathit{add}\ (m', n'))$ auswerten sollte. Ähnliche Rechnungen ergeben sich, wenn eine Zahl gerade, die andere ungerade ist. Interessant wird es, wenn beide Zahlen ungerade sind.

$$
\begin{aligned}
& \mathit{natural}\ (\mathit{add}\ (\mathit{Odd}\ m', \mathit{Odd}\ n')) \\
= & \quad \{\ \text{Spezifikation von } \mathit{add}\ (4.3\text{b})\ \} \\
& \mathit{natural}\ (\mathit{Odd}\ m') + \mathit{natural}\ (\mathit{Odd}\ n') \\
= & \quad \{\ \text{Definition von } \mathit{natural}\ \} \\
& 2 * \mathit{natural}\ m' + 1 + 2 * \mathit{natural}\ n' + 1 \\
= & \quad \{\ \text{Distributivgesetz}\ \} \\
& 2 * (\mathit{natural}\ m' + \mathit{natural}\ n' + 1) \\
= & \quad \{\ \text{Spezifikation von } \mathit{add}\ (4.3\text{b})\ \} \\
& 2 * (\mathit{natural}\ (\mathit{add}\ (m', n')) + 1) \\
= & \quad \{\ \text{Spezifikation von } \mathit{succ}\ (4.3\text{a})\ \} \\
& 2 * (\mathit{natural}\ (\mathit{succ}\ (\mathit{add}\ (m', n')))) \\
= & \quad \{\ \text{Definition von } \mathit{natural}\ \} \\
& \mathit{natural}\ (\mathit{Even}\ (\mathit{succ}\ (\mathit{add}\ (m', n'))))
\end{aligned}
$$

Die Rechnung legt nahe, dass $\mathit{add}\ (\mathit{Odd}\ m', \mathit{Odd}\ n')$ zu $\mathit{Even}\ (\mathit{succ}\ (\mathit{add}\ (m', n')))$ auswerten sollte. Die Summe zweier ungerader Zahlen ist ebenfalls gerade. Im Unterschied zum vorherigen Fall müssen wir das Ergebnis des rekursiven Aufrufs mit *succ* um eins erhöhen, sprich wir müssen den sogenannten ***Übertrag*** (engl. carry) berücksichtigen. Insgesamt erhalten wir das folgende Programm.

```
let rec add (m : Leibniz, n : Leibniz) : Leibniz =
  match m with
    | Null     → n
    | Even m' → match n with | Null     → m
                             | Even n' → Even (add (m', n'))
                             | Odd  n' → Odd  (add (m', n'))
    | Odd  m' → match n with | Null     → m
                             | Even n' → Odd  (add (m', n'))
                             | Odd  n' → Even (succ (add (m', n')))
```

Der Datentyp *Leibniz* implementiert übrigens das Binär- oder ***Dualsystem***. Wie unser ***Dezimalsystem*** ist das Dualsystem ein ***Stellenwertsystem***; im Unterschied zum Dezimalsystem verwendet es nicht zehn Ziffern, sondern nur zwei. Der Zusammenhang zum Dualsystem wird noch deutlicher, wenn wir den Datentyp *Leibniz* mit Hilfe des Distributivgesetzes umschreiben (wir lassen die Datenkonstruktoren zunächst weg).

$$\begin{aligned} \mathit{Leibniz} &\cong \mathit{Unit} \mid \mathit{Leibniz} \mid \mathit{Leibniz} \\ &\cong \mathit{Unit} \mid \mathit{Unit} * \mathit{Leibniz} \mid \mathit{Unit} * \mathit{Leibniz} \\ &\cong \mathit{Unit} \mid (\mathit{Unit} \mid \mathit{Unit}) * \mathit{Leibniz} \end{aligned}$$

Im vorletzten Schritt nutzen wir aus, dass $\mathit{Unit} * t \cong t$. Vergleichen wir den resultierenden Typ mit der Definition von *Nats*, so sehen wir, dass *Leibniz* im Prinzip ein Listentyp ist. Im Fall von *Nats* sind die Listenelemente natürliche Zahlen, im Fall von *Leibniz* sind sie Bits, Elemente des zweielementigen Typs *Unit* | *Unit*. Eine alternative Definition von *Leibniz* sieht somit folgendermaßen aus (jetzt mit Datenkonstruktoren).

```
type Bit  = | O | I          // 0 und 1
type Bits = | Nil | Cons of Bit * Bits
```

In einem Stellenwertsystem wird eine Zahl durch eine Folge von Ziffern repräsentiert, hier eine Folge von Binärziffern (das englische Wort *bit* ist eine Verschmelzung von *bi*nary und digi*t*). Der Wert einer Ziffer wird durch seine Position in der Liste bestimmt. Die Ziffern im Listenrest wiegen doppelt so viel wie die Ziffer im Listenkopf (siehe Definition von *natural*), daher der Name *Stellenwert*system, siehe auch Anhang B.5.3.

4.2.3. Widerlegbare Muster

Die Zweige einer Fallunterscheidung führen Bezeichner ein. Wie im Fall von Wertebindungen können wir auch hier auf den linken Seiten anstelle eines einzelnen Bezeichners (x in $C\ x$) ein Muster (p in $C\ p$) erlauben. In der Tat lässt sich sogar die gesamte linke Seite als Muster lesen: $C\ p$ ist ein Muster, auf das ein Wert der Form $C\ v$ passt, sofern v auf p passt. Im Unterschied zu den Mustern, die wir bisher kennengelernt haben, kann der Musterabgleich im Fall von $C\ p$ auch fehlschlagen: Der Wert *Male* v passt nicht auf das Muster *Female* x. Man sagt auch, das Muster *Female* x ist ***widerlegbar*** (engl. refutable pattern). Die Fallunterscheidung mit ***match*** lässt sich unter diesem Hintergrund als sukzessives Durchprobieren von Mustern deuten.

Wenn wir Konstruktoranwendungen wie $C\ p$ zu den Mustern hinzunehmen, dann können wir Konstruktoren auch schachteln. Wir werden später sehen, dass dies sehr bequem und nützlich ist.

Abstrakte Syntax Wir erweitern zunächst die Syntax von Fallunterscheidungen.

$e ::= \cdots$	***Ausdrücke:***
$\mid$ ***match*** e ***with*** m	erweiterte Fallunterscheidung

Der Rumpf einer erweiterten Fallunterscheidung ist eine Folge von sogenannten ***Regeln***[7] der Form $p \to e$.

$m \in \mathsf{Match} ::= p \to e$	Regel
$\mid\ m_1 \ \mathsf{I}\ m_2$	Sequenz von Regeln

[7] Verwechseln Sie den Begriff »Regel« nicht mit »Typregel« oder »Auswertungsregel«. Eine Regel ist ein Element der Objektsprache Mini-F#; Typ- und Auswertungsregeln sind Elemente der Metasprache, mit der wir Mini-F# formalisieren.

Schließlich wird der Bereich der Muster um disjunktive[8] Muster und Konstruktoranwendungen erweitert.

$p ::= \cdots$	***Muster:***
$\mid\ p_1 \mid p_2$	disjunktives Muster
$\mid\ C\ p$	Konstruktoranwendung

Eine Regel mit einem disjunktiven Muster $(p_1 \mid p_2) \to e$ entspricht der Regelsequenz $(p_1 \to e) \mid (p_2 \to e)$, hat aber den Vorteil, dass der Ausdruck e nicht dupliziert werden muss. Das Muster $\mathit{Female}\ \{\mathit{name} = s\} \mid \mathit{Male}\ \{\mathit{name} = s; \mathit{bald} = \_\}$ bindet zum Beispiel den Bezeichner s an den Namen einer Person. In einem disjunktiven Muster müssen beide Teilmuster die gleichen Bezeichner enthalten.

Statische Semantik Die Typregeln für die Fallunterscheidung stellen sicher, dass die rechten Seiten der Regeln den gleichen Typ besitzen und dass die Muster dem Typ des Diskriminatorausdrucks entsprechen.

$$\frac{\Sigma \vdash e : t \qquad \Sigma \vdash t\ \mathbf{with}\ m : t'}{\Sigma \vdash \mathbf{match}\ e\ \mathbf{with}\ m : t'}$$

Der Typ des Diskriminatorausdrucks e muss übrigens kein Variantentyp sein — wir werden uns später einige Beispiele dafür anschauen. Die Hilfsrelation $\Sigma \vdash t\ \mathbf{with}\ m : t'$ prüft die einzelnen Zweige der Fallunterscheidung.

$$\frac{p \sim t : \Sigma' \qquad \Sigma, \Sigma' \vdash e : t'}{\Sigma \vdash t\ \mathbf{with}\ p \to e : t'} \qquad \frac{\Sigma \vdash t\ \mathbf{with}\ m_1 : t' \qquad \Sigma \vdash t\ \mathbf{with}\ m_2 : t'}{\Sigma \vdash t\ \mathbf{with}\ m_1 \mid m_2 : t'}$$

Auf der rechten Seite einer Regel sind alle in dem Muster enthaltenen Bezeichner sichtbar.

Die folgenden Typregeln erweitern den Regelsatz für den Musterabgleich, den wir in Abschnitt 4.1.2 eingeführt haben.

$$\frac{p_1 \sim t : \Sigma' \qquad p_2 \sim t : \Sigma'}{(p_1 \mid p_2) \sim t : \Sigma'}$$

Beachte: p_1 und p_2 in dem disjunktiven Muster $p_1 \mid p_2$ müssen die gleiche Signatur Σ' generieren: Sie müssen die gleichen Bezeichner des gleichen Typs binden. Die Typregel für die Konstruktoranwendung setzt voraus, dass der Variantentyp

$$\mathbf{type}\ \mathrm{T} = \mid\ C_1\ \mathbf{of}\ t_1 \mid C_2\ \mathbf{of}\ t_2$$

bekannt ist.

$$\frac{p \sim t_i : \Sigma'}{C_i\ p \sim \mathrm{T} : \Sigma'} \quad i \in \{1, 2\}$$

Wenn t_i der Einheitstyp Unit ist, dann ist C_i selbst ein Muster, da das Dummyargument () wie üblich weggelassen wird. Aus diesem Grund werden übrigens Konstruktoren groß geschrieben: So lässt sich das Muster x in der konkreten Syntax optisch leicht von dem Muster C unterscheiden.

[8] Das Adjektiv »disjunktiv« meint hier nicht, dass die alternativen Muster einander ausschließen (exklusiv). Wie die logische Disjunktion »||« ist auch das alternative Muster einschließend (inklusiv).

Dynamische Semantik Mit der Einführung von Konstruktormustern kann der Abgleich eines Musters mit einem Wert fehlschlagen. Diesen Fall signalisieren wir durch einen Blitz:

$$p \sim \nu \Downarrow \lightning$$

Der Blitz symbolisiert, dass das Muster p *nicht* auf den Wert ν passt.

Die erweiterte Fallunterscheidung wird wie folgt ausgewertet.

$$\frac{\delta \vdash e \Downarrow \nu \qquad \delta \vdash \nu \ \textit{with}\ m \Downarrow \nu'}{\delta \vdash \textit{match}\ e\ \textit{of}\ m \Downarrow \nu'}$$

Die Hilfsrelationen

$$\delta \vdash \nu \ \textit{with}\ m \Downarrow \nu' \quad \text{und} \quad \delta \vdash \nu \ \textit{with}\ m \Downarrow \lightning$$

modellieren das Durchprobieren der Regeln. Trifft keine Regel zu, so ist die Fallunterscheidung undefiniert: Die dynamische Semantik ordnet dem Ausdruck keinen Wert zu — dieses Problem werden wir erst in Abschnitt 7.4 beheben.

$$\frac{p \sim \nu \Downarrow \delta' \qquad \delta, \delta' \vdash e \Downarrow \nu'}{\delta \vdash \nu \ \textit{with}\ p \to e \Downarrow \nu'} \qquad \frac{p \sim \nu \Downarrow \lightning}{\delta \vdash \nu \ \textit{with}\ p \to e \Downarrow \lightning}$$

Die Zweige werden von links nach rechts durchprobiert, bis die erste Regel passt.

$$\frac{\delta \vdash \nu \ \textit{with}\ m_1 \Downarrow \nu'}{\delta \vdash \nu \ \textit{with}\ m_1 \mid m_2 \Downarrow \nu'}$$

$$\frac{\delta \vdash \nu \ \textit{with}\ m_1 \Downarrow \lightning \qquad \delta \vdash \nu \ \textit{with}\ m_2 \Downarrow \nu'}{\delta \vdash \nu \ \textit{with}\ m_1 \mid m_2 \Downarrow \nu'}$$

$$\frac{\delta \vdash \nu \ \textit{with}\ m_1 \Downarrow \lightning \qquad \delta \vdash \nu \ \textit{with}\ m_2 \Downarrow \lightning}{\delta \vdash \nu \ \textit{with}\ m_1 \mid m_2 \Downarrow \lightning}$$

Die folgenden Regeln erweitern den in Abschnitt 4.1.2 eingeführten Regelsatz für den Musterabgleich. Disjunktive Muster werden von links nach rechts durchprobiert, bis das erste Muster passt.

$$\frac{p_1 \sim \nu \Downarrow \delta}{(p_1 \mid p_2) \sim \nu \Downarrow \delta}$$

$$\frac{p_1 \sim \nu \Downarrow \lightning \qquad p_2 \sim \nu \Downarrow \delta}{(p_1 \mid p_2) \sim \nu \Downarrow \delta}$$

$$\frac{p_1 \sim \nu \Downarrow \lightning \qquad p_2 \sim \nu \Downarrow \lightning}{(p_1 \mid p_2) \sim \nu \Downarrow \lightning}$$

$$\frac{}{(C\ p) \sim (C'\ \nu) \Downarrow \lightning} \quad C \neq C'$$

$$\frac{p \sim \nu \Downarrow \delta}{(C\ p) \sim (C'\ \nu) \Downarrow \delta} \quad C = C' \qquad \frac{p \sim \nu \Downarrow \lightning}{(C\ p) \sim (C'\ \nu) \Downarrow \lightning} \quad C = C'$$

Der Abgleich mit einem Konstruktormuster schlägt fehl, wenn der Wert einen unterschiedlichen Konstruktor hat oder wenn die jeweiligen Argumente nicht passen. Die statische Semantik stellt sicher, dass der Wert in den letzten beiden Regeln tatsächlich ein Element eines Variantentyps ist.

Vertiefung Der größte Vorteil der erweiterten Fallunterscheidung ist, dass wir Muster — insbesondere Konstruktoranwendungen — schachteln können. Geschachtelte Muster können oft an die Stelle geschachtelter Fallunterscheidungen treten. Sie helfen, den Programmcode kürzer und klarer zu formulieren. Betrachten wir noch einmal die Implementierung der Addition zweier Binärzahlen. Im Prinzip müssen wir nur vier Fälle unterscheiden: Ein Argument ist Null, beide Argumente sind gerade, ein Argument ist ungerade, beide sind ungerade. Die geschachtelte Fallunterscheidung zwingt uns aber insgesamt sieben Fälle zu behandeln und verschleiert zudem die vorhandene Symmetrie. Mit Hilfe disjunktiver Muster können wir sehr viel natürlicher formulieren:

```
let rec add (m : Leibniz, n : Leibniz) : Leibniz =
  match (m, n) with
    | (Null,     k       )
    | (k,        Null    ) → k
    | (Even m′, Even n′) → Even (add (m′, n′))
    | (Even m′, Odd n′ )
    | (Odd m′,  Even n′) → Odd  (add (m′, n′))
    | (Odd m′,  Odd n′ ) → Even (succ (add (m′, n′)))
```

Auch Konstruktoranwendungen können in Mustern geschachtelt werden. Ein schönes Beispiel hierfür liefert die folgende Implementierung der Funktion *ordered*, die überprüft, ob eine Liste von natürlichen Zahlen aufsteigend geordnet ist. (Zur Erinnerung: *sort* bringt eine Liste in eine aufsteigende Reihenfolge.)

```
let rec ordered (nats : Nats) : Bool =
  match nats with
    | Nil                          → true
    | Cons (_, Nil)                → true
    | Cons (n1, ns & Cons (n2, _)) → n1 ⩽ n2 && ordered ns
```

Zwei benachbarte Listenelemente müssen jeweils in der Relation »⩽« stehen. Das geschachtelte Muster $Cons\ (n_1, Cons\ (n_2, \_))$ passt auf eine mindestens zweielementige Liste; die ersten beiden Listenelemente werden an n_1 und n_2 gebunden. Um die Eigenschaft rekursiv für die Restliste überprüfen zu können, vergeben wir mit Hilfe eines konjunktiven Musters zusätzlich einen Namen für die Liste ohne das erste Element: $Cons\ (n_1, ns\ \&\ Cons\ (n_2, \_))$. Da der Rekursionsfall nur mindestens zweielementige Listen behandelt, wird der Fall der einelementigen Liste, $Cons\ (\_, Nil)$, zu einem weiteren Basisfall.

Die größere Bequemlichkeit bei der Formulierung von Mustern geht mit einer größeren Verantwortung einher: Die Programmiererin oder der Programmierer muss sicherstellen, dass die Muster tatsächlich auch alle Fälle abdecken. Einfache Fallunterscheidungen stellen dies automatisch sicher. Für die Lesbarkeit von Programmen ist es weiterhin wünschenswert, dass die Muster paarweise disjunkt sind, so dass jedes Muster einen anderen Fall abdeckt. Ist das gewährleistet, dann kann man jeden Zweig einzeln für sich lesen und verstehen. Da die Reihenfolge des Musterabgleichs dann keine Rolle spielt, lassen sich die Zweige auch beliebig umordnen.

Übungen.

1. Ganze Zahlen können mit Hilfe des folgenden Variantentyps repräsentiert werden.

```
type Int =
  | Neg of Nat
  | Pos of Nat
```

Dabei repräsentiert ein Wert der Form *Neg n* die Zahl $-n$ und entsprechend *Pos n* die Zahl $+n$. Implementieren Sie die üblichen arithmetischen Operationen und die üblichen Vergleichsoperationen auf diesem Typ. Wie ändern sich die Definitionen, wenn man vereinbart, dass *Neg n* die Zahl $-(n+1)$ repräsentiert? Diese Darstellung hat den Vorteil, dass jede ganze Zahl eine *eindeutige* Repräsentation besitzt.

2. Verwenden Sie das Peano Entwurfsmuster, um eine natürliche Zahl vom Typ *Nat* in ihre Binärdarstellung vom Typ *Leibniz* zu überführen.

```
let leibniz (n : Nat) : Leibniz
```

Programmieren Sie die Funktion ein zweites Mal, diesmal mit Hilfe des Leibniz Entwurfsmusters. Vergleichen Sie die Laufzeit der beiden Versionen.

3. Der folgende rekursive Variantentyp eignet sich zur Repräsentation von arithmetischen Ausdrücken.

```
type Expr =
  | Const of Nat
  | Add   of Expr * Expr
  | Sub   of Expr * Expr
  | Mul   of Expr * Expr
  | Div   of Expr * Expr
```

Die Konstruktoren *Add*, *Sub*, *Mul* und *Div* modellieren die entsprechenden arithmetischen Operatoren, der Konstruktor *Const* dient zur Repräsentation einer natürlichen Zahl.

(a) Schreiben Sie eine Funktion *evaluate*, die einen Ausdruck des Typs *Expr* auswertet.

```
let evaluate (expr : Expr) : Nat
```

(b) Schreiben Sie eine Funktion *pretty-print-infix*, die einen Ausdruck des Typs *Expr* in einen *String* überführt:

```
let pretty-print-infix (expr : Expr) : String
```

Die Operatoren sollen dabei infix notiert werden.

```
>>> pretty-print-infix (Add (Const 4711, Const 815))
"(4711 + 815)"
```

4. Wir erweitern den Datentyp *Expr* aus Aufgabe 4.2.3 um Bezeichner und Wertebindungen.

```
type Expr =
  | Const of Nat
  | Add   of Expr * Expr
  | Sub   of Expr * Expr
  | Mul   of Expr * Expr
  | Div   of Expr * Expr
  | Ident of String
  | Let   of String * Expr * Expr
```

Erweitern Sie entsprechend die Funktion *evaluate*, die einen arithmetischen Ausdruck auswertet.

```
let evaluate (expr : Expr, env : String → Nat) : Nat
```

Ein Ausdruck wird relativ zu einer Umgebung ausgewertet, in der die Werte der freien Bezeichner festgehalten werden. Wir modellieren eine Umgebung als Abbildung von Bezeichnern auf Werte.

4.3. Parametrisierte Typen und Polymorphie

4.3.1. Parametrisierte Typen

Wir haben bisher zwei verschiedene Listentypen eingeführt: Listen von natürlichen Zahlen *Nats* und Listen von Binärziffern *Bits*. Viele andere Listentypen sind denkbar: Listen von Personen, Listen von Adressen, Listen von Listen von natürlichen Zahlen um 2-dimensionale Tabellen zu repräsentieren usw. Für jeden Elementtyp einen neuen Listentyp einzuführen ist mühsam und unökonomisch. Werden in einem Kontext zwei verschiedene Listentypen benötigt, müssen wir uns zudem unterschiedliche Namen für den Typ und insbesondere für die Datenkonstruktoren ausdenken.

Listen sind ein typisches Beispiel für ***Behälter*** (engl. container). Sie enthalten Daten, die sie in einer bestimmten Art und Weise organisieren. Im Fall von Listen werden die Daten linear angeordnet. Da der Typ der Elemente für die Organisation keine Rolle spielt, liegt es nahe von dem Elementtyp zu abstrahieren und ihn zum formalen Parameter einer Typdefinition zu machen.

```
type List ⟨'a⟩ = | Nil | Cons of 'a * List ⟨'a⟩
```

Der formale ***Typparameter*** wird in spitze Klammern gesetzt; die ***Typvariable*** selbst fängt mit einem Apostroph an, um sie von Record- und Variantentypen einfach unterscheiden zu können. Die parametrisierte Typdefinition macht deutlich, dass Listen eine ***homogene*** Datenstruktur sind: Das Kopfelement hat den gleichen Typ wie die Elemente der Restliste.

Da *List* einen Typparameter hat, entspricht *List* im Prinzip einer Funktion auf Typen. Wenden wir *List* auf einen konkreten Typ an, so erhalten wir einen speziellen Listentyp: *List ⟨Nat⟩* umfasst Listen von natürlichen Zahlen, *List ⟨Bit⟩* entsprechend Listen von Binärziffern. Aktuelle ***Typparameter*** werden ebenfalls in spitze Klammern gesetzt, um sie von Werteparametern auf den ersten Blick unterscheiden zu können. Die Typen *List ⟨Nat⟩* und *List ⟨Bit⟩* können wie gewohnt in Typangaben verwendet werden.

```
let rec append (list1 : List ⟨Nat⟩, list2 : List ⟨Nat⟩) : List ⟨Nat⟩ =
  match list1 with
  | Nil          → list2
  | Cons (x, xs) → Cons (x, append (xs, list2))
```

Die speziellen Listentypen können alternativ als Typsynonyme definiert werden.

```
type Nats = List ⟨Nat⟩
type Bits = List ⟨Bit⟩
```

So wie Record- und Variantentypen parametrisiert werden können, so lassen sich auch Typsynonyme parametrisieren.

```
type Oracle ⟨'a⟩ = 'a → Bool
```

Die Funktion *player-A* aus Abschnitt 3.6 erhält damit den Typ *Oracle ⟨Nat⟩* und *player-B* den Typ *Oracle ⟨Nat⟩ → Nat*.

Wir formalisieren im Folgenden nur Typdefinitionen mit *einem* Typparameter. Alle Konstrukte verallgemeinern sich aber in naheliegender Weise auf *n* Typparameter.

Abstrakte Syntax Wir erweitern Deklarationen um parametrisierte Recordtyp- und Variantentypdefinitionen.

$d ::= \cdots$	***Deklarationen:***
$\mid$ ***type*** $\mathrm{T}\langle'a\rangle = \{\ell_1 : t_1; \ell_2 : t_2\}$	parametrisierter Recordtyp
$\mid$ ***type*** $\mathrm{T}\langle'a\rangle =\ \mid C_1$ ***of*** $t_1 \mid C_2$ ***of*** t_2	parametrisierter Variantentyp

Die Typvariablen auf der rechten Seite einer Typdefinition müssen auf der linken Seite eingeführt werden: ***type*** *List* = | *Nil* | *Cons* ***of*** $'a * List$ ist *nicht* zulässig.

Die Kategorie der Typen wird um Typvariablen und Typapplikationen erweitert.

$'a \in \mathrm{TypeVar}$

$t ::= \cdots$	***Typen:***
$\mid\ 'a$	Typvariable
$\mid\ \mathrm{T}\langle t\rangle$	Typapplikation

Mit der Einführung parametrisierter Typen sind nicht mehr alle Typausdrücke wohlgeformt und müssten im Prinzip einer statischen Prüfung unterzogen werden: Zum Beispiel sind $Bool\langle Nat\rangle$ und $List \to Nat$ unsinnig; *Bool* wird mit einem Parameter versorgt, erwartet aber keinen; *List* hingegen benötigt einen Parameter, erhält aber keinen. Wir wollen die Formalisierung an dieser Stelle nicht zu weit treiben und sehen von einer präzisen Definition von »wohlgetypten Typausdrücken« ab.

Statische Semantik Wir beschränken uns im Folgenden auf die Formalisierung von parametrisierten Variantentypen.

Bei einer Konstruktoranwendung wird der Typparameter des Variantentyps mit einem konkreten Typ instantiiert: *Cons* $(1, Nil)$ zum Beispiel hat den Typ $List\langle Nat\rangle$, *Cons* $(false, Nil)$ hat den Typ $List\langle Bool\rangle$. Der formale Typparameter aus der Definition des Variantentyps wird jeweils durch den aktuellen Typparameter ersetzt.

Die textuelle Ersetzung von Typvariablen durch Typen nennt man ***Typsubstitution***. Ist t ein Typ und $\in \mathrm{TypeVar} \to_{\mathrm{fin}} \mathrm{Type}$ eine endliche Abbildung von Typvariablen auf Typen, dann bezeichnet t den Typ, in dem die Typvariablen aus dom durch die zugeordneten Typen ersetzt werden.

$$'a = \begin{cases} (\,'a) & \text{falls } 'a \in dom\,() \\ 'a & \text{sonst} \end{cases}$$

$$\mathrm{T} = \mathrm{T}$$

$$(t_1 * t_2) = t_1 * t_2$$

$$(t_1 \to t_2) = t_1 \to t_2$$

$$(\mathrm{T}\langle t\rangle) = \mathrm{T}\langle t\rangle$$

Für den parametrisierten Variantentyp

type $\mathrm{T}\langle'a\rangle =\ \mid C_1$ ***of*** $t_1 \mid C_2$ ***of*** t_2

muss die Typregel für die Konstruktoranwendung wie folgt angepasst werden.

$$\frac{\Sigma \vdash e : t_i\{'a \mapsto t\}}{\Sigma \vdash C_i\ e : \mathrm{T}\langle t\rangle}$$

Diese Typregel verdient eine nähere Betrachtung. Wenn C_i den Typ $t_i \to \mathrm{T}\langle'a\rangle$ hat, dann erhält $C_i\ e$ den Typ $\mathrm{T}\langle t\rangle$, sofern e den passenden Typ, nämlich $t_i\{'a \mapsto t\}$, hat. Der Typparameter t kann frei gewählt werden und somit kann ein einzelner Ausdruck mehrere, ja unendlich viele Typen besitzen. Dies ist unter anderem dann der Fall, wenn $'a$ in t_i nicht auftritt, wie zum

Beispiel im Fall der leeren Liste *Nil*. (Zur Erinnerung: Ein nullstelliger Konstruktor entspricht einem einstelligen Konstruktor mit dem Argumenttyp *Unit*.) Der Datenkonstruktor *Nil* hat den Typ $List\,\langle t\rangle$ für einen beliebigen Grundtyp t: In *Cons* $(1, Nil)$ zum Beispiel hat *Nil* den Typ $List\,\langle Nat\rangle$, in *Cons* $(false, Nil)$ entsprechend $List\,\langle Bool\rangle$. Der Ausdruck *Cons* (Nil, Nil) hat hingegen unendlich viele Typen: $List\,\langle List\,\langle t\rangle\rangle$ für einen beliebigen Typ t.

$$\dfrac{\dfrac{\overline{\Sigma \vdash Nil : List\,\langle t\rangle} \qquad \overline{\Sigma \vdash Nil : List\,\langle List\,\langle t\rangle\rangle}}{\Sigma \vdash (Nil, Nil) : List\,\langle t\rangle * List\,\langle List\,\langle t\rangle\rangle}}{\Sigma \vdash Cons\ (Nil, Nil) : List\,\langle List\,\langle t\rangle\rangle}$$

Wir sehen, das erste Vorkommen von *Nil* hat den Typ $List\,\langle t\rangle$, das zweite den Typ $List\,\langle List\,\langle t\rangle\rangle$. Der Ausdruck *Cons* (Nil, Nil) ist eine einelementige Liste, dessen einziges Element die leere Liste ist.

Die Regel für die Fallunterscheidung ändert sich nicht wesentlich, nur dass die Buchhaltung etwas aufwändiger ist (die Typvariable $'a$ ist der bei der Deklaration von T spezifizierte Typparameter).

$$\dfrac{\Sigma \vdash e : \mathrm{T}\,\langle t\rangle \qquad \Sigma, \{x_1 \mapsto t_1\} \vdash e_1 : t' \qquad \Sigma, \{x_2 \mapsto t_2\} \vdash e_2 : t'}{\Sigma \vdash (\textbf{\textit{match}}\ e\ \textbf{\textit{with}}\ |\ C_1\ x_1 \to e_1\ |\ C_2\ x_2 \to e_2) : t'} \qquad := \{'a \mapsto t\}$$

Den Bezeichnern x_1 und x_2 werden Instanzen der Argumenttypen von C_1 und C_2 zugeordnet: Hat der Diskriminatorausdruck e zum Beispiel den Typ $List\,\langle Bit\rangle$, dann erhält der Bezeichner x in *Cons* x den Typ $Bit * List\,\langle Bit\rangle$.

Dynamische Semantik Die dynamische Semantik ändert sich nicht.

4.3.2. Polymorphie

Parametrisierte Typen erhöhen — wie auch Funktionen — die Wiederverwendbarkeit von Programmen. Ein parametrisierter Variantentyp wie zum Beispiel *List* kann in vielen verschiedenen Kontexten verwendet werden; im Fall von Listen überall da, wo Folgen von Elementen verwaltet werden müssen. Eine einzige Definition, unendlich viele Verwendungsmöglichkeiten. Kurioserweise halten Funktionen auf parametrisierten Typen mit dieser Entwicklung nicht Schritt. Betrachten wir einmal die Funktion *length*, die die Länge einer Liste bestimmt.

```
let rec length (list : List ⟨Nat⟩) : Nat =
  match list with
    | Nil          → 0
    | Cons (_, xs) → 1 + length xs
```

Der Typ des Parameters, $List\,\langle Nat\rangle$, schränkt die Anwendung von *length* auf Listen von *natürlichen Zahlen* ein. Um zum Beispiel die Länge einer Liste von *Personen* zu bestimmen, müssen wir eine zweite Funktion programmieren.

```
let rec length (list : List ⟨Person⟩) : Nat =
  match list with
    | Nil          → 0
    | Cons (_, xs) → 1 + length xs
```

Diese Definition ist baugleich zur ersten, der Rumpf ist sogar identisch, nur die Typangabe hat sich geändert. Dabei spielt für das Ausrechnen der Listenlänge der Typ der Elemente gar keine

Rolle — die anonyme Variable »_« in dem Muster *Cons* (_, *xs*) macht ja sogar explizit, dass die Elemente ignoriert werden.

Um parametrisierte Typen in ihrer vollen Schönheit genießen zu können, drängt es sich auf, auch Funktionen mit Typen zu parametrisieren.

```
let rec length ⟨'a⟩(list : List ⟨'a⟩) : Nat =
  match list with
    | Nil          → 0
    | Cons (_, xs) → 1 + length xs
```

Die Funktion *length* hat jetzt zwei Parameter: einen Typparameter (*'a*) und einen Werteparameter (*list*). Der Typparameter wird verwendet, um den Typ des Werteparameters, sprich den Elementtyp der Liste, festzulegen. Wird die Funktion *length* aufgerufen, müssen für die formalen Parameter entsprechend aktuelle Parameter angegeben werden: einen Typ und eine Liste mit Elementen des angegebenen Typs. Der Aufruf *length* ⟨*Person*⟩*staff* bestimmt zum Beispiel die Länge einer Liste von Personen, *length* ⟨*Nat*⟩*nats* entsprechend die Länge einer Liste von natürlichen Zahlen. Eine einzige Definition, unendliche viele Anwendungen.

Die Längenfunktion ist natürlich sehr speziell, da sie die Listenelemente gar nicht benötigt. Wenn wir zurückschauen, erkennen wir aber, dass viele Funktionen allgemeiner sind, als die Typangaben es vermuten lassen und die von einer Parametrisierung mit Typen profitieren. Zum Beispiel die Funktion *peano-pattern* aus Abschnitt 3.6:

```
let peano-pattern ⟨'soln⟩(zero : 'soln, succ : 'soln → 'soln) : Nat → 'soln =
```

Bei der Diskussion der Funktion haben wir besprochen, dass der ursprüngliche Typ zu speziell ist. Jetzt haben wir das Sprachmittel in der Hand, um dieses Manko zu beseitigen: Der spezielle Typ wird durch den Typparameter *'soln* ersetzt. Wir können das fleischgewordene Entwurfsmuster zum Beispiel verwenden, um eine natürliche Zahl in eine der Zahlendarstellungen aus Abschnitt 4.2.2 zu überführen.

```
peano-pattern ⟨Peano⟩  (Zero, fun n → Succ n)
peano-pattern ⟨Leibniz⟩(Null, fun n → succ n)
```

Es gibt zahlreiche weitere Beispiele für Funktionen, die sich verallgemeinern lassen:

```
let swap ⟨'a, 'b⟩(x : 'a, y : 'b) : 'b * 'a
let put-last ⟨'a⟩(xs : List ⟨'a⟩, x : 'a) : List ⟨'a⟩
let append ⟨'a⟩(xs₁ : List ⟨'a⟩, xs₂ : List ⟨'a⟩) : List ⟨'a⟩
let reverse ⟨'a⟩(xs : List ⟨'a⟩) : List ⟨'a⟩
let sort-by ⟨'a⟩(less-equal : 'a * 'a → Bool) : List ⟨'a⟩ → List ⟨'a⟩
```

Die Funktion *swap* abstrahiert über zwei Typparameter. Interessanterweise nageln die Typangaben die Implementierung der Funktion eindeutig fest.

```
let swap ⟨'a, 'b⟩(x : 'a, y : 'b) : 'b * 'a = (y, x)
```

Der Rumpf muss die Form (y, x) haben; Tippfehler wie (x, y), (x, x), $(x, 0)$ usw. fallen samt und sonders durch die statische Typprüfung.

Besonders beeindruckend ist die Verallgemeinerung von *sort-by*. Jetzt können wir beliebige Listen sortieren, sofern wir nur eine Ordnungsrelation, eine Vergleichsfunktion, auf den Listenelementen angeben können. Listen von Personen können zum Beispiel wie folgt nach ihrem Nachnamen geordnet werden.

```
sort-by ⟨Person⟩(fun (ann, bob) → ann.surname ⩽ bob.surname)
```

Funktionen, die mit einem oder mehreren Typen parametrisiert sind, heißen auch ***polymorphe*** Funktionen nach dem griechischen Wort πολυμορφια für Vielgestaltigkeit.

Pragmatik Wir sehen davon ab, Syntax und Semantik polymorpher Funktionen formal zu definieren. Stattdessen geben wir uns pragmatisch und erlauben umgekehrt sogar *Typparameter auszulassen*: sowohl bei der Definition polymorpher Funktionen

```
let rec length (list : List ⟨'a⟩) : Nat = ...
let sort-by (less-equal : 'a * 'a → Bool) : List ⟨'a⟩ → List ⟨'a⟩ = ...
```

als auch bei der Anwendung polymorpher Funktionen

```
sort-by (fun (m, n) → m ⩽ n)
sort-by (fun (ns1, ns2) → length ns1 ⩽ length ns2)
```

Insbesondere letzteres stellt eine erhebliche Schreiberleichterung dar.

Tatsächlich ist es möglich, auch die Typen von Funktionsparametern und -ergebnissen auszulassen — die fehlenden Informationen werden automatisch inferiert! Wir können sehr flexibel entscheiden, wie viele Typinformationen wir bereitstellen:

```
let rec length⟨'a⟩(xs : List ⟨'a⟩) : Nat = match xs with ...
let rec length (xs : List ⟨'a⟩) : Nat = match xs with ...
let rec length (xs : List ⟨'a⟩) = match xs with ...
let rec length xs = match xs with ...
let rec length = function ...
```

Der Ausdruck *function m* ist eine beliebte Abkürzung für *fun x → match x with m*. Beliebt, weil man sich keinen Namen für den Funktionsparameter ausdenken muss — neue Namen zu erfinden ist bekanntlich schwer.

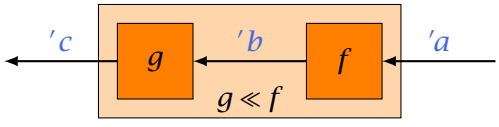
Typinferenz erhöht nicht nur die Bequemlichkeit beim Programmieren, sondern führt gelegentlich auch zu angenehmen Überraschungen, nämlich dann, wenn der inferierte Typ einer Funktion allgemeiner ist als erwartet. Schauen wir uns ein Beispiel an: Die Komposition von Funktionen, $f \circ g$, lässt sich in Mini–F# wie folgt definieren.

```
let compose g f x = g (f x)
```

Entgegen unserer sonstigen Gepflogenheiten haben wir weder die Typen der Argumente noch den Typ des Resultats angegeben. Den Mini–F# Interpreter ficht diese Nachlässigkeit nicht an; er inferiert den folgenden Typ.

```
compose : ('b → 'c) → ('a → 'b) → ('a → 'c)
```

Der hergeleitete Typ enthält drei Typvariablen: $'a$, $'b$ und $'c$. Wenn wir die Funktion g mit f komponieren, dann muss lediglich der Ergebnistyp von f mit dem Argumenttyp von g übereinstimmen; alle anderen Typen sind beliebig. Die Funktionskomposition ist übrigens als Infixoperator vordefiniert: $g \ll f$. *Lies:* g nach f — der »Pfeil« $\ll$ zeigt an, dass das Ergebnis von f in die Funktion g eingespeist wird.



Da die Komposition hochgradig polymorph ist, wäre eine verpflichtende Angabe von Typparametern fatal. Statt *compose reverse sort* oder infix *reverse≪sort* müsste man länglicher formulieren:

compose ⟨*List* ⟨*Nat*⟩, *List* ⟨*Nat*⟩, *List* ⟨*Nat*⟩⟩(*reverse* ⟨*Nat*⟩) *sort*, wahrscheinlich mit dem Ergebnis, dass man *compose* erst gar nicht verwenden würde.

Die Bequemlichkeit der Typinferenz birgt natürlich auch eine Gefahr: Typen gleich vollständig auszulassen. *Zur Erinnerung:* Typen dienen der Dokumentation und sind eine wichtige Hilfe bei der systematischen Erstellung von Programmen (Stichwort: Entwurfsmuster). Wie so oft im Leben gilt es, eine Balance zwischen zwei Extremen zu finden: der vollständigen Angabe aller Typen und dem vollständigen Weglassen aller Typangaben.

Vertiefung: Optionale Werte Listen, so wie wir sie definiert haben, erinnern an Stapel (engl. stacks), zum Beispiel Akten- oder Tellerstapel. Wir können einfach und schnell auf das erste bzw. oberste Element zugreifen. Wenn wir das n-te Element benötigen, müssen wir Aufwand betreiben, sprich, wir müssen eine entsprechende Funktion definieren.

```
let rec nth (list : List ⟨'a⟩, n : Nat) : 'a =
```

Für den zweiten Parameter, den Index, sollte gelten: $0 \leqslant n < \mathit{length}\ \mathit{list}$, eine Eigenschaft, die wir in Mini-F# selbst nicht ausdrücken können. Was machen wir, wenn die Liste weniger als n Elemente enthält? Eine Möglichkeit ist, die beiden möglichen Resultate des Zugriffs, erfolglos und erfolgreich, mit einem Datentyp darzustellen.

```
type Option ⟨'a⟩ = | None | Some of 'a
```

Wie der Name des Typs andeutet, können wir damit optionale Werte repräsentieren. Der Typ *Option* ⟨*Bool*⟩ enthält zum Beispiel drei Elemente: *None*, *Some False* und *Some True*. Der Variantentyp *Option* ist wie *List* ein parametrisierter Typ: der Typparameter legt den Typ der Elemente fest, die im Erfolgsfall zurückgegeben werden. Mit diesem neuen Typ können wir die Signatur von *nth* verfeinern.

```
let rec nth (list : List ⟨'a⟩, n : Nat) : Option ⟨'a⟩ =
```

Für den Fall, dass der Index n zu groß ist, geben wir *None* zurück, anderenfalls *Some x*, wobei x das n-te Element ist. Das Struktur Entwurfsmuster führt unmittelbar zum Ziel:

```
let rec nth (list : List ⟨'a⟩, n : Nat) : Option ⟨'a⟩ =
  match list with
  | Nil          → None
  | Cons (x, xs) → if n = 0 then Some x
                   else  nth (xs, n - 1)
```

Die Rekursionsbasis ist zwingend: Wenn die Liste leer ist, dann ist der Index zu groß — kein Index n erfüllt $0 \leqslant n < \mathit{length}\ \mathit{list} = 0$ — und wir geben *None* zurück. Im Rekursionsschritt führen wir eine zusätzliche Fallunterscheidung über n. (Eine Bitte: Die Funktion *nth* sollte nicht *missbraucht* werden, um über alle Element einer Liste zu iterieren, siehe Aufgabe 4.4.1.)

Vertiefung: Rekursionsmuster Wenn wir zurückblättern, stellen wir fest, dass wir die schnelle Potenzierung nach Leibniz insgesamt dreimal programmiert haben: Einmal, um natürliche Zahlen zu potenzieren; ein zweites Mal, um Matrizen zu potenzieren; und ein drittes Mal, um Goldenen Zahlen zu potenzieren. Die Programme unterscheiden sich dabei nicht im Aufbau, sondern im Wesentlichen durch die Typangaben:

```
let rec power (x : Nat, n : Nat) : Nat = ···
let rec power (x : Matrix) (n : Nat) : Matrix = ···
let rec power (x : Golden) (n : Nat) : Golden = ···
```

module Datatypes.Power

Ein Unterschied ist oberflächlicher Natur: In der ursprünglichen Version haben wir die beiden Parameter als Paar übergeben, später gestaffelt. Der wesentliche Unterschied betrifft den Typ des zu potenzierenden Objekts: *Nat*, *Matrix* oder *Golden* — ein klarer Fall für Polymorphie! Im Unterschied zu dem Prototypen einer polymorphen Funktion, *length*, sind aber im vorliegenden Fall die Funktionsrümpfe nicht identisch. In Abhängigkeit vom Typ werden unterschiedliche Multiplikationsoperationen mit jeweils passendem neutralen Element verwendet. Wenn wir von diesen Zutaten *abstrahieren*, erhalten wir eine ***generische*** Potenzierungsfunktion.

```
let rec generic-power (e:'a, (*):'a → 'a → 'a) (x:'a) (n:Nat):'a =
  let square (x:'a):'a = x * x
  let rec p (k:Nat):'a =
    if k = 0 then e
            else if k % 2 = 0 then square (p (k ÷ 2))
                              else square (p (k ÷ 2)) * x
  p n
```

Als Bezeichner für die *abstrakte* Multiplikation haben wir den Asteriskus gewählt, der damit den *konkreten* Operator für die Multiplikation von Zahlen im Rumpf von *generic-power* verschattet. Ein syntaktisches Detail: Da $*$ infix notiert wird, muss der Bezeichner in der Parameterliste in runde Klammern gesetzt werden.

Die Umkehrung der ***Abstraktion*** ist die ***Spezialisierung***: Indem wir die Parameter *e* und $*$ entsprechend binden, erhalten wir die ursprünglichen Funktionen zurück.

```
>>> generic-power (0, (+)) 7 673
4711
>>> generic-power (1, (*)) 2 10
1024
>>> generic-power (unit, (^*^)) F 10
(89, 55, 55, 34)
>>> generic-power (1G, (*)) ϕ 10
34 + 55 · ϕ
```

Ein amüsanter Spezialfall: Verwenden wir als »Multiplikation« die Addition von Zahlen, dann implementiert der Algorithmus eine schnelle Multiplikation! Das Verfahren ist auch als *Ägyptische Multiplikation* oder als *Russische Bauernmultiplikation* bekannt (engl. peasant algorithm). Die Namen deuten an, dass das Verfahren zur handschriftlichen Multiplikation durch Halbieren und Verdoppeln seit Jahrtausenden in Gebrauch ist. In der Neuzeit findet es sich in Rechnern wieder, als in Silikon gegossene Multiplikation von Binärzahlen. Der Kreis zu Leibniz, dem Vater des Binärsystems, schließt sich.

Über den Tellerrand Listen sind eine der beliebtesten Datenstrukturen. Sie bieten sich bei der Modellierung an, wenn es gilt, Folgen von Objekten, Sequenzen oder Reihungen zu repräsentieren. Listen sind in den meisten höheren Programmiersprachen vordefiniert und werden entsprechend gut unterstützt. F# bildet da keine Ausnahme. Die vordefinierten Listen unterscheiden sich lediglich in der Syntax, nicht aber in der Semantik. Man schreibt

- T *list* statt *List* ⟨T⟩ — an die Stelle der Präfixnotation tritt die Postfixnotation;
- [ ] statt *Nil*; und
- *x* :: *xs* statt *Cons* (*x*, *xs*) — an die Stelle der Präfixnotation tritt die Infixnotation.

Darüber hinaus gibt es eine Menge »***syntaktischen Zucker***«, der das Programmieren erleichtert und versüsst: $[x_1; x_2; x_3; x_4; x_5; x_6]$ ist zum Beispiel eine kompakte Notation für die Liste $x_1 :: (x_2 :: (x_3 :: (x_4 :: (x_5 :: (x_6 :: [\,])))))$; die Intervallschreibweise $[l\,..\,u]$ erzeugt die Liste aller Elemente von l bis einschließlich u. Insbesondere letztere Abkürzung ist beim Testen von listenverarbeitenden Funktionen sehr nützlich.

Wir werden in den folgenden Kapiteln den vordefinierten Listen den Vorzug geben, einfach weil die Syntax angenehmer ist. Lassen Sie uns deshalb ein paar listenverarbeitende Funktionen in F# re-implementieren, damit wir uns an die Syntax gewöhnen. Die Funktion *nth* bestimmt das n-te Element einer Liste:

```
let rec nth (list : 'a list, n : int) : 'a option =
  match list with
  | [ ]     → None
  | x :: xs → if n = 0 then Some x
              else  nth (xs, n - 1)
```

Um auf das n-te Element der Liste xs zuzugreifen, kann man auch kurz $xs.[n]$ schreiben. Im Unterschied zu *nth* wird eine Element vom Typ *'a* zurückgegeben; ist der Index allerdings negativ oder zu groß, bricht die Rechnung mit einer Fehlermeldung ab.

Aus historischen Gründen werden vordefinierte, parametrisierte Typen — dazu gehört auch *option* — postfix notiert: *int option list* ist zum Beispiel eine Liste optionaler ganzer Zahlen (Präfixnotation: *List ⟨Option ⟨Int⟩⟩*); *int list option* ist hingegen eine optionale Liste (Präfixnotation: *Option ⟨List ⟨Int⟩⟩*).

Die Funktion *append* konkateniert zwei Listen:

```
let rec append list ys =
  match list with
  | [ ]     → ys
  | x :: xs → x :: append xs ys
```

Die Listenkonkatenation *append xs ys* ist als Infixoperator vordefiniert: *xs @ ys*, zum Beispiel ist $[4; 7] \,@\, [1; 1] = [4; 7; 1; 1]$. (In der Definition haben wir keine Typen angegeben. Was ist der Typ von *append* bzw. @?)

Die Funktion *contains* ermittelt, ob eine Liste ein gegebenes Element enthält. Was »∈« für Mengen ist, das ist *contains* für Listen.

```
let rec contains key = function
  | [ ]     → false
  | a :: as → key = a || contains key as
```

(*Zum Knobeln:* was ist der Typ von *contains*? Für die Antwort müssten wir weiter ausholen, was wir an dieser Stelle nicht tun wollen.)

4.3.3. Anwendung: Planung von Stromtrassen

Prof. Ventum hat einen lukrativen Beratervertrag mit der Orkankraft GmbH und Co. KG abgeschlossen, die Stromtrassen für die Vernetzung von Windenergieanlagen plant. Bereits bestehende Anlagen, siehe Abbildung 4.6, sollen mit einer Nord-Süd-Trasse vernetzt werden, wobei jede Windkraftanlage über eine West-Ost-Trasse angebunden wird. Prof. Ventum soll herausfinden, wie die Position der Nord-Süd-Trasse gewählt werden muss, so dass die Gesamtlänge der Leitungen möglichst klein wird.

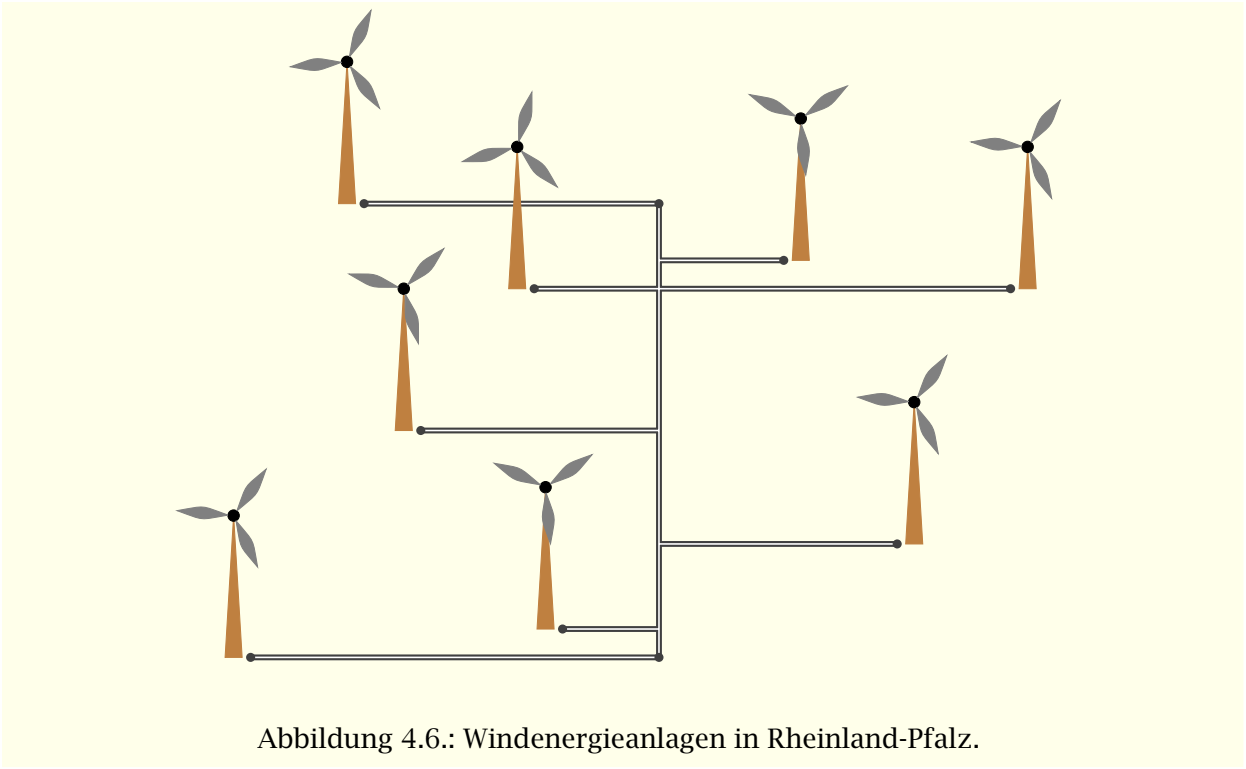


Abbildung 4.6.: Windenergieanlagen in Rheinland-Pfalz.

Die Position der Anlagen ist durch eine *nicht-leere* Liste von Punkten gegeben. Jeder Punkt wird durch eine x- und eine y-Koordinate festgelegt.

```
type Point = {x : Nat; y : Nat}
let wind-farm =
  [{x = 2;  y = 2};  {x = 6;  y = 18};{x = 8;  y = 10};{x = 13;y = 3};
   {x = 12;y = 15};{x = 26;y = 6};  {x = 22;y = 16};{x = 30;y = 15}]
```

Wir nehmen vereinfachend an, dass die y-Koordinaten unterschiedlich sind, so dass jede Anlage über eine separate Trasse angeschlossen werden muss.

Prof. Ventum ist schnell klar, dass sich die Aufgabe in zwei Teilaufgaben zergliedern lässt: (1) die Bestimmung der Länge der Nord-Süd-Trasse; (2) die *Optimierung* der Längen der West-Ost-Trassen. Gehen wir beide Teilaufgaben nacheinander an.

Länge der Nord-Süd-Trasse Für die erste Teilaufgabe müssen die Windkraftanlagen mit der kleinsten bzw. der größten y-Koordinate ermittelt werden. Prof. Ventum verallgemeinert die Aufgabe etwas und programmiert Funktionen, die die Extremelemente einer Liste bezüglich einer beliebigen Prioritätsfunktion bestimmen.

```
let rec minBy (priority : 'a → Nat) : 'a list → 'a = function
  | [x]    → x
  | x :: xs → let m = minBy priority xs in
              if priority x ⩽ priority m then x else m
let rec maxBy (priority : 'a → Nat) : 'a list → 'a = function
  | [x]    → x
  | x :: xs → let m = maxBy priority xs in
              if priority x ⩽ priority m then m else x
```

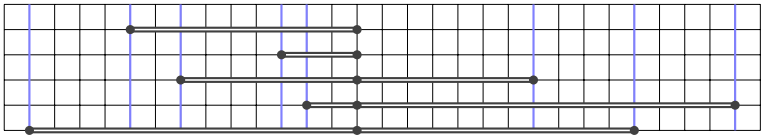
Es fällt auf, dass die Funktionen sich nicht an das Struktur Entwurfsmuster für Listen halten: Der jeweilige Basisfall löst nicht das Problem für die leere Liste, sondern für eine einelementige Liste. Mit anderen Worten, sowohl *minBy f* [ ] als auch *maxBy f* [ ] sind undefiniert. Warum? Betrachten wir den Typ der Funktion *minBy* genauer: Die Funktion erwartet als Argument eine »Prioritätsfunktion« vom Typ *'a → Nat* und gibt als Ergebnis eine »Auswahlfunktion« vom Typ *'a list → 'a* zurück — aus einer gegebenen Liste wird das Element mit der kleinsten Priorität ausgewählt. Ist die Liste nun leer, so steht kein Element zur Auswahl. Und: Wir können kein Element vom Typ *'a erfinden*, da *'a* ein Typparameter ist und kein konkreter Typ. Der polymorphe Typ *('a → Nat) → ('a list → 'a)* verspricht, dass *minBy* funktioniert, unabhängig davon, welcher konkrete Typ für den Typparameter *'a* eingesetzt wird (z.B. *Bool*, *Nat*, *Nat list* oder *Nat → Bool*). Ein Element vom Typ *'a* zu erfinden, käme schwarzer Magie gleich!

Zurück zum Ausgangsproblem: Die Länge der Nord-Süd-Trasse ergibt sich als Differenz der kleinsten und der größten y-Koordinate.

```
let north-south-route ps =
  (maxBy (fun p → p.y) ps).y - (minBy (fun p → p.y) ps).y
```

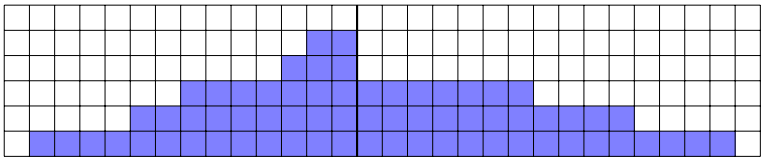
Der Aufruf *maxBy (fun p → p.y) ps* gibt einen Punkt zurück, dessen y-Koordinate anschließend selektiert wird.

Optimierung der West-Ost-Trassen Wenden wir uns dem Optimierungsproblem zu: Wie muss die Position der Nord-Süd-Trasse gewählt werden, so dass die Gesamtlänge der West-Ost-Trassen möglichst klein wird? Prof. Ventum überlegt sich zunächst, dass die vertikale Position der Anlagen für diese Frage keine Rolle spielt. Wenn wir die West-Ost-Trassen entsprechend zusammenschieben, ergibt sich ein aufschlussreiches Bild.

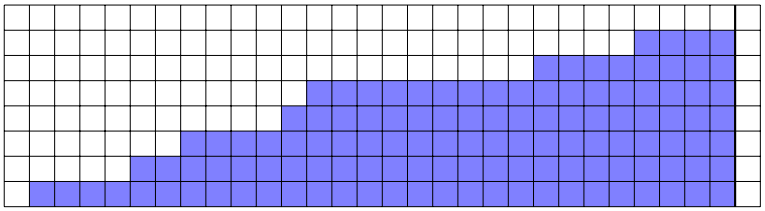


Die x-Achse lässt sich gemäß der x-Koordinaten der Anlagen in verschiedene Intervalle unterteilen. Die Grafik zeigt, dass das Intervall unmittelbar links von der Nord-Süd-Trasse insgesamt 5-mal durchquert wird — 5-mal, da 5 Anlagen links von der Trasse liegen. Das nächste Intervall zur Linken wird 4-mal durchquert usw.

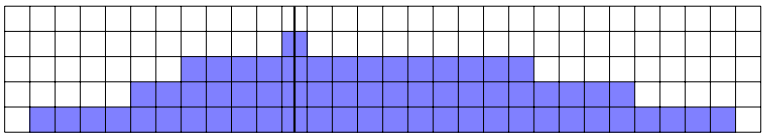
Trägt man auf der y-Achse die Gesamtzahl der Durchquerungen auf, erhält man eine Treppenfunktion. Die Fläche, die die Funktion mit der x-Achse einschließt, entspricht der Gesamtlänge der West-Ost-Trassen.



Wenn wir die Nord-Süd-Trasse weiter nach rechts verschieben, dann vergrößert sich der Flächeninhalt, da die Treppe höher und höher wird. Das folgende Diagramm zeigt den schlechtesten Fall: Die Trasse liegt am rechten Rand.



Das optimale Bild ergibt sich, wenn auf der linken Seite genauso viele Anlagen liegen, wie auf der rechten Seite.



Man beachte, dass die gesuchte Position *weder* die geometrische Mitte *noch* das arithmetische Mittel der x-Positionen ist. Wir suchen stattdessen den Median der x-Positionen. Ist die Folge $x_0, \ldots, x_{n-1}$ mit $n > 0$ der Größe nach geordnet, so ist $x_{\lfloor (n-1)/2 \rfloor}$ der sogenannte ***Untermedian*** und $x_{\lceil (n-1)/2 \rceil}$ der ***Obermedian***. Wenn die Gesamtzahl n der Elemente ungerade ist, fallen Unter- und Obermedian zusammen und man spricht kurz vom ***Median***.[9] Für unsere Anwendung spielt es keine Rolle, ob der Unter- oder der Obermedian verwendet wird oder ein beliebiger Punkt dazwischen. Der (Unter-) Median einer beliebigen Folge lässt sich bestimmen, indem wir die Folge sortieren und dann das mittlere Element herausgreifen.

```
let median xs = (sort xs).[(length xs - 1) / 2]
```

Um die Gesamtlänge der West-Ost-Trassen zu berechnen, müssen die Abstände der Windkraftanlagen vom Median aufsummiert werden. Prof. Ventum liebt Abstraktion und programmiert eine Funktion, die etwas allgemeiner ist.

```
let rec sum-by (cost : 'a → Nat) : 'a list → Nat = function
  | [ ]      → 0
  | x :: xs → cost x + sum-by cost xs
```

Die Funktion *sum-by* erwartet als Argument eine »Kostenfunktion« vom Typ *'a → Nat* und gibt als Ergebnis eine »Summationsfunktion« vom Typ *'a list → Nat* zurück — diese ermittelt die Gesamtkosten für eine gegebene Liste von Elementen. Der Funktionsaufruf *sum-by* (*fun* $x \rightarrow f\ x$) *xs* entspricht in etwa der Summationsformel $\sum_{x \in X} f(x)$ — »in etwa« weil *xs* eine Liste von Elementen ist, X hingegen eine Menge. (In einer Liste können Elemente mehrfach auftreten und werden entsprechend mehrfach addiert; in einer Menge ist das nicht der Fall.) Auch *sum-by* ist eine Funktion höherer Ordnung und als solche vielseitig einsetzbar: *sum-by id* summiert eine Liste von natürlichen Zahlen, *sum-by* (*sum-by id*) eine Liste von Listen von natürlichen Zahlen, *sum-by* (*sum-by* (*sum-by id*)) eine Liste von Listen von Listen von natürlichen Zahlen usw. Ach ja, *id* ist die sogenannte ***Identitätsfunktion*** *fun* $x \rightarrow x$.

Zurück zur Trassenplanung: Die optimale Länge der West-Ost-Trassen lässt sich nach diesen Vorarbeiten wie folgt bestimmen.

```
let west-east-routes ps =
  let m = (median ps).x
  (m, sum-by (fun p → (p.x - m) + (m - p.x)) ps)
```

Für unser ursprüngliches Beispiel ergeben sich die folgenden Werte.

```
>>> north-south-route wind-farm
16
>>> west-east-routes wind-farm
(12, 63)
```

Die Zahl 12 ist der Untermedian der x-Koordinaten: Drei Koordinaten sind kleiner (2, 6 und 8) und vier Koordinaten sind größer (13, 22, 26 und 30). Die Gesamtlänge der Trassen beläuft sich auf 16 + 63 = 79 km.

[9] Wenn die Folgenelemente rationale oder reelle Zahlen sind, wird der Median auch als arithmetisches Mittel von Unter- und Obermedian definiert.

Übungen.

⌨ **1.** Wie muss der Auswerter aus Aufgabe 4.2.4 abgeändert werden, wenn zusätzlich Laufzeitfehler wie Division durch 0 abgefangen werden?

let *evaluate* $(expr : Expr, env : String \to Option\,\langle Nat\rangle) : Option\,\langle Nat\rangle$

Tritt ein Fehler auf, so wird *None* zurückgegeben, anderenfalls ist das Ergebnis *Some value*, wobei *value* der Wert des Ausdrucks ist.

📝 **2.**

(a) Leiten Sie mit den Regeln der statischen Semantik ab, dass der Ausdruck $Cons\ (true, Nil)$ den Typ $List\,\langle Bool\rangle$ hat.

(b) Geben Sie für die folgenden Typen jeweils fünf — möglichst vielfältige — Ausdrücke dieses Typs an.

(i) $List\,\langle Nat\rangle$

(ii) $Option\,\langle Nat\rangle$

(iii) $List\,\langle Option\,\langle Nat\rangle\rangle$

(iv) $Option\,\langle List\,\langle Nat\rangle\rangle$

⌨ **3.** Eine Matrix kann durch eine Liste von Zeilenvektoren dargestellt werden, wobei ein einzelner Zeilenvektor durch eine Liste von natürlichen Zahlen repräsentiert wird. (Die folgenden Definitionen führen ***Typsynonyme*** ein: Der Bezeichner auf der linken Seite ist eine Abkürzung für den Typausdruck auf der rechten Seite.)

type $Vector = List\,\langle Nat\rangle$

type $Matrix = List\,\langle Vector\rangle$

Implementieren Sie die Transposition von Matrizen und die Matrizenmultiplikation auf dieser Darstellung.

let *transpose* $(m : Matrix) : Matrix$

let *mul* $(m_1 : Matrix, m_2 : Matrix) : Matrix$

📝 **4.** Erfinden Sie zu jedem der folgenden Typen einen Ausdruck, der den jeweiligen Typ besitzt.

(a) $'a \to 'a$

(b) $'a * 'a \to 'a$

(c) $'a * 'b \to 'a$

(d) $'a * 'b \to 'b * 'a$

(e) $List\,\langle 'a\rangle \to List\,\langle 'a\rangle$

(f) $List\,\langle 'a * 'b\rangle \to List\,\langle 'b * 'a\rangle$

Wieviele *semantisch verschiedene* Ausdrücke gibt es jeweils? *Beispiel:* ein Ausdruck des Typs $List\,\langle 'a * 'b\rangle \to List\,\langle 'a\rangle * List\,\langle 'b\rangle$ ist *unzip* mit

```
let rec unzip = function
  | Nil              → (Nil, Nil)
  | Cons ((x, y), xys) → let (xs, ys) = unzip xys in (Cons (x, xs), Cons (y, ys))
```

📝 **5.** Zeigen Sie, dass die Funktion *append* bzw. der Operator @ assoziativ ist:

$$(list_1 \mathbin{@} list_2) \mathbin{@} list_3 = list_1 \mathbin{@} (list_2 \mathbin{@} list_3)$$

Unterscheiden Sie in Analogie zum Struktur Entwurfsmuster für Listen zwei Fälle: $list_1 = Nil$ (***Induktionsbasis***) und $list_1 = Cons\ (x_1, xs_1)$ (***Induktionsschritt***). Im zweiten Fall dürfen Sie annehmen, dass die Aussage bereits für xs_1 gilt.

$$(xs_1 \mathbin{@} list_2) \mathbin{@} list_3 = xs_1 \mathbin{@} (list_2 \mathbin{@} list_3)$$

6. Schreiben Sie eine Funktion

let *sublists* $(list : List\langle'a\rangle) : List\langle List\langle'a\rangle\rangle$

die eine Liste aller ***Teillisten*** erzeugt. Die Reihenfolge der Teillisten in der Ergebnisliste ist dabei irrelevant. *Hinweis:* Eine Liste mit n Elementen hat 2^n Teillisten.

7. Schreiben Sie eine Funktion

let *segments* $(list : List\langle'a\rangle) : List\langle List\langle'a\rangle\rangle$

die alle ***Segmente*** einer Liste berechnet. Ein Segment ist eine Teilliste, die nur aufeinanderfolgende Elemente der Ursprungsliste enthält. Die Reihenfolge der Segmente in der Ergebnisliste ist irrelevant. *Hinweis:* Eine Liste mit n Elementen hat $\binom{n+1}{2} = n(n+1)/2$ nicht-leere Segmente.

8. Schreiben Sie eine Funktion

let *max-segment* $(list : List\langle Int\rangle) : List\langle Int\rangle$

die das Segment einer Liste von *ganzen* Zahlen bestimmt, dessen Summe maximal ist.

9. Ändert man die Reihenfolge der Elemente einer Liste, ohne Elemente zu entfernen oder hinzuzunehmen, so erhält man eine ***Permutation***. Zu einer Liste der Länge n existieren n Fakultät verschiedene Permutationen. (Anmerkung: Enthält die Ausgangsliste Duplikate, so sind nicht alle Permutationen verschieden). Schreiben Sie eine Funktion

let *permutations* $(list : List\langle'a\rangle) : List\langle List\langle'a\rangle\rangle$

die eine Liste aller Permutationen der Liste *list* berechnet. Die Reihenfolge der Permutationen in der Ergebnisliste ist irrelevant.

4.4. Arrays\Felder\Reihungen

> *To denote the subsequence of natural numbers* 2, 3, ..., 12 *without the pernicious three dots, four conventions are open to us*
>
> *a)* $2 \leqslant i < 13$
>
> *b)* $1 < i \leqslant 12$
>
> *c)* $2 \leqslant i \leqslant 12$
>
> *d)* $1 < i < 13$
>
> *Are there reasons to prefer one convention to the other? Yes, there are. The observation that conventions a) and b) have the advantage that the difference between the bounds as mentioned equals the length of the subsequence is valid. So is the observation that, as a consequence, in either convention two subsequences are adjacent means that the upper bound of the one equals the lower bound of the other. Valid as these observations are, they don't enable us to choose between a) and b); so let us start afresh.*
>
> *There is a smallest natural number. Exclusion of the lower bound as in b) and d) forces for a subsequence starting at the smallest natural number the lower bound as mentioned into the realm of the unnatural numbers. That is ugly, so for the lower bound we prefer the* $\leqslant$ *as in a) and c). Consider now the subsequences starting at the smallest natural number: inclusion of the upper bound would then force the latter to be unnatural by the time the sequence has shrunk to the empty one. That is ugly, so for the upper bound we prefer* $<$ *as in a) and d). We conclude that convention a) is to be preferred.*
>
> *[...]*
>
> *When dealing with a sequence of length* N*, the elements of which we wish to distinguish by subscript, the next vexing question is what subscript value to assign to its starting element. Adhering to convention a) yields, when starting with subscript 1, the subscript range* $1 \leqslant i < \mathrm{N}+1$*; starting with 0, however, gives the nicer range* $0 \leqslant i < \mathrm{N}$*. So let us let our ordinals start at zero: an element's ordinal (subscript) equals the number of elements preceding it in the sequence. And the moral of the story is that we had better regard — after all those centuries! — zero as a most natural number.*
>
> — Edsger W. Dijkstra (1930–2002), *Why numbering should start at zero — EWD831*

Lassen wir noch einmal die Möglichkeiten, Daten zu aggregieren, Revue passieren. Um eine *feste* Anzahl von Daten *verschiedenen* Typs zusammenzufassen, können wir Tupel bzw. Records verwenden. Um eine *beliebige* Anzahl von Daten des *gleichen* Typs zusammenzufassen, können wir Listen benutzen. Die verschiedenen Typen unterscheiden sich in der Handhabung und bezüglich der Laufzeit elementarer Operationen. Auf eine Komponente eines Tupels bzw. eines Records kann in konstanter Zeit zugegriffen werden, auf ein Element einer Liste in linearer Zeit. Auf der anderen Seite kann der Zugriff auf eine Tupel- bzw. Recordkomponente nicht berechnet werden: Das Label ℓ in $e.\ell$ kann nicht das Ergebnis einer Rechnung sein. Damit gibt es keine Möglichkeit, eine *rekursive* Funktion zu schreiben, die zum Beispiel alle Komponenten eines n-Tupels oder Records aufaddiert. Dass für die Projektion ℓ kein Ausdruck angegeben werden kann, ist keine künstliche Einschränkung, sondern hat einen handfesten Grund:

Tupel wie auch Records sind ***heterogene*** Datenstrukturen: Die Komponenten können einen unterschiedlichen Typ besitzen. Wäre die Projektion durch einen Ausdruck gegeben, wie zum Beispiel in $e.(n\,\%\,2)$, dann würde der *Typ* des gesamten Ausdrucks vom *Wert* des Teilausdrucks $n\,\%\,2$ abhängen. Damit wäre die strikte Trennung zwischen der statischen und der dynamischen Semantik aufgehoben. (Es gibt experimentelle Programmiersprachen, die gerade dies erlauben. So weit wollen wir aber nicht gehen.)

Für Listen gilt diese Einschränkung nicht; sie sind eine ***homogene*** Datenstruktur: Alle Elemente eines Containers besitzen den gleichen Typ. Der Datentyp Liste ist rekursiv definiert, entspre-

chend sind auch listenverarbeitende Funktionen in der Regel rekursiv definiert. Das Struktur Entwurfsmuster gibt einen ersten Ansatz vor. Problematisch, weil langsam, sind Funktionen, die *gegen* die Struktur eines Datentyps ankämpfen. Das Prinzip der binären Suche zum Beispiel lässt sich nicht ohne Weiteres auf Listen übertragen, da der Zugriff auf das mittlere Element einer Liste teuer ist. (Zur Erinnerung: $nth\,(xs, k)$ bzw. $xs.[\,k\,]$ benötigt k Schritte, um das k-te Element der Liste xs zu ermitteln. Wenn wir damit die binäre Suche füttern:

$$binary\text{-}search\,((\textbf{\textit{fun}}\ k \to number \leqslant list.[\,k\,]), 0, length\ list \dot{-} 1)$$

machen wir den Geschwindigkeitsvorteil der binären Suche, $\lg n$ statt n, zunichte. Da das Orakel selbst eine lineare Laufzeit hat, ergibt sich eine Gesamtlaufzeit von $n \lg n$.)

Summa summarum, wir suchen eine Datenstruktur, die sozusagen zwischen Tupeln und Listen angesiedelt ist, die eine beliebige Anzahl von Daten des *gleichen* Typs zusammenfasst, aber einen konstanten Zugriff auf die aggregierten Daten erlaubt. Diese Lücke schließen ***Arrays*** (auch Felder oder Reihungen genannt). Ein Array kann ähnlich wie ein Tupel durch Aufzählung der Elemente konstruiert werden: $[|\ 2;3;5;7;11\ |]$ ist ein Array der Größe 5. Im Unterschied zu Tupeln kann der Zugriff auf Elemente berechnet werden: Ist e ein Ausdruck, der zu einem Array auswertet, und e_1 ein arithmetischer Ausdruck, dann kann mit $e.[\,e_1\,]$ auf die entsprechende Komponente zugegriffen werden. Wertet etwa e_1 zu 3 aus, dann wird die *vierte* Komponente selektiert. Das liegt daran, dass die Arrayelemente beginnend mit 0 durchnummeriert werden.

Abstrakte Syntax Arrays sind Funktionen nicht unähnlich; die sogenannte ***Subskription*** $e.[\,e_1\,]$ korrespondiert zur Funktionsapplikation $e\ e_1$. Im Unterschied zu Funktionen ist der Definitionsbereich stets Int bzw. genauer ein Anfangsstück der natürlichen Zahlen.[10] Auch zur Funktionsabstraktion gibt es ein Gegenstück: $[|\,\textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ 0\,..\,n-1 \to e\,|]$ konstruiert ein Array der Größe n. Zum Beispiel umfasst das Array $[|\,\textbf{\textit{for}}\ i\ \textbf{\textit{in}}\ 0\,..\,99 \to i * i\,|]$ die ersten hundert Quadratzahlen.

$e ::= \cdots$	***Arrays:***
$\mid\ [|\,e_0;\ldots;e_{n-1}\,|]$	Konstruktion durch Aufzählung
$\mid\ [|\,\textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ e_1\,..\,e_2 \to e_3\,|]$	Konstruktion durch Bildungsvorschrift\Arraybeschreibung
$\mid\ e.[\,e_1\,]$	Subskription
$\mid\ e.Length$	Größe eines Arrays

Man sieht: Eckige Klammern mit Strich, $[|$ und $|]$, sind das Markenzeichen der Sprachkonstrukte, die Arrays konstruieren. Die Arraybeschreibung $[|\,\textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ e_1\,..\,e_2 \to e_3\,|]$ führt den Bezeichner x neu ein; x ist in e_3 sichtbar. Der Ausdruck e_1 in $e.[\,e_1\,]$ heißt auch Arrayindex oder kurz ***Index***.

Wie Listen können auch Arrays beliebig viele Elemente umfassen; insbesondere können sie leer sein oder nur ein Element enthalten: $[|\,|]$ oder $[|\,\textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ 1\,..\,0 \to x\,|]$ konstruieren ein leeres Array; die Ausdrücke $[|\,4711\,|]$ oder $[|\,\textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ 0\,..\,0 \to 4711\,|]$ konstruieren ein einelementiges Array.

Statische Semantik Der Typ eines Arrays ist mit dem Typ der Elemente parametrisiert.

$t ::= \cdots$	***Typen:***
$\mid\ Array\,\langle t\rangle$	Arraytyp

Die folgenden Typregeln machen noch einmal deutlich, dass ein Array vom Typ $Array\,\langle t\rangle$ zu einer Funktion des Typs $Int \to t$ korrespondiert.

$$\frac{\Sigma \vdash e_i : t \quad \mid \quad i \in \mathbb{N}_n}{\Sigma \vdash [|\,e_0;\ldots;e_{n-1}\,|] : Array\,\langle t\rangle}$$

[10] Da keine negativen Zahlen als Index zulässig sind, sollte eigentlich Nat als Definitionsbereich verwendet werden. Aus pragmatischen Gründen rückt Mini-F# hier näher an F# heran, das ganze Zahlen als Indizes vorschreibt.

Die Notation $\phi_i \mid i \in \mathbb{N}_n$ ist eine kompakte Schreibweise für eine Regel mit den n Voraussetzungen $\phi_0, \ldots, \phi_{n-1}$.

$$\frac{\Sigma \vdash e_1 : \mathit{Int} \qquad \Sigma \vdash e_2 : \mathit{Int} \qquad \Sigma, \{x \mapsto \mathit{Int}\} \vdash e_3 : t}{\Sigma \vdash [\mid \textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ e_1 \mathinner{..} e_2 \to e_3 \mid] : \mathit{Array}\,\langle t \rangle}$$

$$\frac{\Sigma \vdash e : \mathit{Array}\,\langle t \rangle \qquad \Sigma \vdash e_1 : \mathit{Int}}{\Sigma \vdash e.[e_1] : t} \qquad \frac{\Sigma \vdash e : \mathit{Array}\,\langle t \rangle}{\Sigma \vdash e.\mathit{Length} : \mathit{Int}}$$

Für das leere Array gilt Ähnliches wie für die leere Liste: $[\mid\mid]$ hat den Typ $\mathit{Array}\,\langle t \rangle$ für einen beliebigen Grundtyp t. Entsprechend hat zum Beispiel der Ausdruck $[\mid[\mid\mid]\mid]$ unendlich viele Typen: $\mathit{Array}\,\langle \mathit{Array}\,\langle t \rangle \rangle$ für einen beliebigen Typ t.

Dynamische Semantik Der Wert eines Arrayausdrucks ist eine endliche Abbildung des Typs $\mathbb{N} \to_{\text{fin}} \mathsf{Val}$, mit anderen Worten eine Sequenz vom Typ Val^*. Entsprechend erweitern wir den Bereich der Werte um Sequenzen von Werten.

$s \in \mathsf{Val}^*$

$\nu ::= \cdots$	***Werte:***
$\mid s$	Array von Werten

Ähnlich wie bei Paaren werden bei der Konstruktion eines Arrays zunächst alle Elemente ausgerechnet, dann wird die endliche Abbildung erzeugt.

$$\frac{\delta \vdash e_i \Downarrow \nu_i \mid i \in \mathbb{N}_n}{\delta \vdash [\mid e_0; \ldots; e_{n-1} \mid] \Downarrow \{i \mapsto \nu_i \mid i \in \mathbb{N}_n\}}$$

$$\frac{\delta \vdash e_1 \Downarrow l \qquad \delta \vdash e_2 \Downarrow u \qquad \delta, \{x \mapsto i\} \vdash e_3 \Downarrow \nu_i \mid i \in \{l \mathinner{..} u\}}{\delta \vdash [\mid \textbf{\textit{for}}\ x\ \textbf{\textit{in}}\ e_1 \mathinner{..} e_2 \to e_3 \mid] \Downarrow \{i - l \mapsto \nu_i \mid i \in \{l \mathinner{..} u\}\}}$$

$$\frac{\delta \vdash e \Downarrow s \qquad \delta \vdash e_1 \Downarrow i}{\delta \vdash e.[e_1] \Downarrow s(i)} \quad i < \mathit{len}\ s \qquad \frac{\delta \vdash e \Downarrow s}{\delta \vdash e.\mathit{Length} \Downarrow \mathit{len}\ s}$$

Bei der Konstruktion mittels Bildungsvorschrift werden zunächst die Arraygrenzen ausgerechnet, dann wird der Bezeichner x nacheinander an die Werte $l, \ldots, u$ gebunden und bezüglich jeder Bindung wird der Rumpf e_3 ausgerechnet.

Die Subskription $e.[e_1]$ ist nur definiert, wenn der Index e_1 im Definitionsbereich der endlichen Abbildung liegt. Befindet er sich außerhalb, dann ordnet die dynamische Semantik dem Ausdruck keinen Wert zu — dieses Problem werden wir in Abschnitt 7.4 beheben. (In vielen Programmiersprachen wird *nicht* überprüft, ob der Index innerhalb der Bereichsgrenzen liegt. Die Konsequenzen sind weitreichend; werden die Probleme entdeckt, erscheinen sie oft als sogenannte »Sicherheitslöcher« in den Kolumnen einschlägiger Zeitschriften.)

Vertiefung: Entwurfsmuster Der »Definitionsbereich« des Arrays a ist durch ein Intervall gegeben. Somit können wir die Programmierung von arrayverarbeitenden Funktionen so ähnlich angehen, wie die von Funktionen auf Suchintervallen, siehe Abschnitt 3.6. Die folgende Funktion, die die Elemente eines Arrays von natürlichen Zahlen aufsummiert, illustriert die Vorgehensweise.

```
let sum (a : Array ⟨Nat⟩) : Nat =
  let rec s (i : Int) : Nat =
    if i = a.Length then 0
                    else a.[i] + s (i + 1)
  in s 0
```

Die Definition folgt dem Peano Entwurfsmuster; das Leibniz Entwurfsmuster ist ebenso anwendbar, bringt aber in diesem Fall keinen Vorteil, da jedes Element einmal angefasst werden muss.

```
let sum (a : Array ⟨Nat⟩) : Nat =
  let rec s (l : Int, u : Int) : Nat =
    match u ÷ l with
    | 0 → 0
    | 1 → a.[l]
    | d → let m = l + d ÷ 2 in s (l, m) + s (m, u)
  in s (0, a.Length)
```

Die Definition verwendet übrigens Dijkstras favorisierte Darstellung von natürlichen Intervallen, siehe Zitat am Anfang des Abschnitts. Das Intervall (l, u) umfasst alle natürlichen Zahlen i mit $l \leqslant i < u$. Somit ist $u \div l$ die Größe des Intervalls.

Fassen wir zusammen: Arrays sind zwischen Tupeln und Listen angesiedelt. Sie aggregieren eine *beliebige* Anzahl von Elementen des *gleichen* Typs. Der Zugriff auf Elemente kann berechnet werden und erfolgt in konstanter Zeit. Arrays haben auch ihre Schwächen: Um ein Array um ein Element zu erweitern, muss das komplette Array kopiert werden; der Aufwand ist also linear zur Größe des Arrays. Eine Liste hingegen kann *vorne* in konstanter Zeit erweitert werden.

Übungen.

1. Harry Hacker hat die folgende Funktion geschrieben, um die Elemente einer Liste aufzuaddieren. (Pate für die Funktionsdefinition stand eine entsprechende Funktion für Arrays, siehe Abschnitt 4.4.)

```
let sum (a : List ⟨Nat⟩) : Nat =
  let rec s (i : Int) : Nat =
    if i = length a then 0
                    else nth (a, i) + s (i + 1)
  in s 0
```

Welche Laufzeit hat die Funktion? Was raten Sie Harry?

2. Geben Sie jeweils einen Mini–F# Ausdruck an, um die folgenden Arrays zu konstruieren:

(a) das Array aller ungeraden Zahlen zwischen 0 und 100;

(b) das Array aller Zahlen zwischen 0 und 100, die durch 3 teilbar sind;

(c) das Array der Größe 100, dessen i-tes Element die Summe der ersten i natürlichen Zahlen ist.

4.5. Projekt: Interpreter und Maschinen⋆

Unsere Programmiersprache ist mittlerweile hinreichend ausdrucksstark, um ein kleines Projekt anzugehen: die Implementierung eines Mini–F#-Interpreters in Mini–F# selbst. Wir werden in etwa den in Kapitel 3 eingeführten Sprachumfang realisieren und dabei schrittweise, ähnlich wie in ebendiesem Kapitel, vorgehen. Eine kleine Vereinfachung nehmen wir allerdings vor: Die interpretierte Sprache ist im Unterschied zu Mini–F# nicht statisch, sondern dynamisch getypt: Eine unsinnige Kombination von Ausdrücken wie zum Beispiel *true*+1 wird nicht *vor* der Auswertung entdeckt und moniert, sondern erst *während* der Auswertung. Aus einem statischen Typfehler wird so ein dynamischer Laufzeitfehler.

In Kapitel 3 haben wir die Auswertung von Ausdrücken mit Hilfe von Beweisbäumen formalisiert. Die zugrundeliegenden Auswertungsregeln, aus denen die Bäume zusammengesetzt werden, beschreiben aus mathematischer Sicht eine »ungerichtete« Relation — eine Umgebung, ein Ausdruck und ein Wert werden zueinander in Beziehung gesetzt. In diesem Abschnitt richten wir

den Fokus auf den Konstruktions*prozess*. Aus der Relation $\delta \vdash e \Downarrow v$ wird ein zielgerichteter Algorithmus, der Mini–F#-Interpreter, der zu einer Umgebung δ und einem Ausdruck e den zugehörigen Wert v ermittelt. Am Ende des Abschnitts steht die Einsicht, dass Beweisbäume nicht nur durch scharfes Hinsehen, sondern auch systematisch konstruiert werden können, eine Einsicht — so die Hoffnung — die zu einem tieferen Verständnis der dynamischen Semantik beiträgt.

Die vorgestellten Programmstücke sind etwas länger und umfangreicher, als wir das bisher gewohnt sind. Länger, aber immer noch überschaubar: Die vollständige Formalisierung der abstrakten Syntax und der dynamischen Semantik passt auf zwei DIN A4 Seiten (siehe Abbildungen 4.7 und 4.8). Bei unserem kurzen Exkurs in die Welt des Übersetzerbaus lernen wir Konzepte kennen, mit deren Hilfe wir Phänomene beleuchten können, die sich mit unseren bisherigen Mitteln nicht oder nur schlecht erhellen lassen. So erklären wir, warum bei tiefer Rekursion »Stack Overflows« auftreten, und zeigen auf, wie diese mittels endrekursiver Programme vermieden werden können.

4.5.1. Arithmetische Ausdrücke und natürliche Zahlen⋆

Konzeptionell am einfachsten sind arithmetische Ausdrücke, so dass wir uns diese als Erstes vornehmen. Ausgangspunkt unserer Überlegungen ist wie gewohnt die abstrakte Syntax. In Kapitel 3 haben wir Sprachkonstrukte mit Hilfe von Baumsprachen eingeführt; an die Stelle von Baumsprachen treten jetzt rekursive Variantentypen.

In einem ersten Schritt führen wir numerische Konstanten und eine einzige Operation, die Addition, ein. Die Ausgangssprache ist bewusst einfach gehalten, um die Vorgehensweise verdeutlichen zu können, ohne sich in Details zu verlieren. Diese einfachste aller möglichen »Programmiersprachen« taufen wir auf den Namen Mini^2 (lies: »Mini quadriert«).

```
type Expr =
  | Num of Nat              // n
  | Add  of Expr * Expr     // e1 + e2
```

Wir haben Variantentypen eingeführt, um *Daten* modellieren zu können. Jetzt verwenden wir einen Variantentyp, um *Programme* zu repräsentieren. Die Idee von »Programmen als Daten« spielt eine zentrale Rolle in der Informatik und steht als Geburtshelferin am Anfang ihrer Geschichte. Universelle Rechenmaschinen, Interpreter, Übersetzer, integrierte Entwicklungsumgebungen, sie alle basieren auf der Idee, Programme als Daten aufzufassen und zu verarbeiten.

Da wir uns zunächst auf arithmetische Ausdrücke beschränken, besteht der Bereich der Werte lediglich aus den natürlichen Zahlen.

```
type Value = Nat            // n
```

Metazirkulärer Interpreter In Kapitel 3 haben wir die dynamische Semantik mit Hilfe von Auswertungsregeln festgelegt. Die relevanten Regeln für Mini^2 sind:

$$\frac{}{Num\ n \Downarrow n} \qquad \frac{e_1 \Downarrow n_1 \qquad e_2 \Downarrow n_2}{Add\ (e_1, e_2) \Downarrow n_1 + n_2}$$

Die zweistellige Relation $e \Downarrow n$ ist *funktional*: *Jedem* Ausdruck e wird *genau* ein Wert v zugeordnet. (Wir werden in Kapitel 6 Beweissysteme kennenlernen, denen diese Eigenschaft nicht zu eigen ist, die eine nicht-funktionale Relation zwischen verschiedenen mathematischen Objekten beschreiben.) Damit können wir die Auswertungs*relation* in Mini–F# als Auswertungs*funktion* definieren: Aus $e \Downarrow n$ wird *evaluate e = n*. Das Struktur Entwurfsmuster für den rekursiven Variantentyp *Expr* führt unmittelbar zum Ziel:

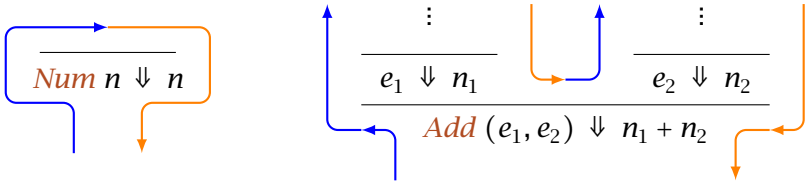
module Interpreter.Naturals

```
let rec evaluate : Expr → Value = function
  | Num n          → n
  | Add (e1, e2)   → evaluate e1 + evaluate e2
```

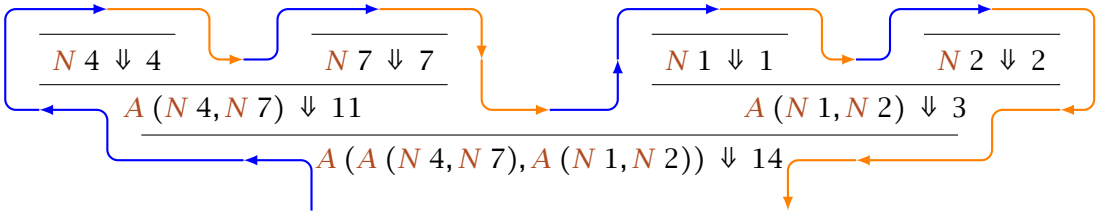
Im Fachjargon nennt man *evaluate* einen ***metazirkulären Interpreter***. Jedes Konstrukt der Objektsprache (Mini^2: *Add*) wird auf das korrespondierende Konstrukt der Metasprache (Mini–F#: +) abgebildet.[11] Im Vergleich zu Kapitel 3 löst Mini–F# somit die Sprache der Mathematik als Metasprache ab.

Um die Bedeutung arithmetischer Ausdrücke zu erklären, verwenden wir eine rekursive Funktionsdefinition. Das ist etwas unbefriedigend, da wir einfache Dinge wie arithmetische Ausdrücke auf komplizierte Dinge wie rekursive Funktionsdefinitionen zurückführen. Im Folgenden beschreiben wir einen alternativen Ansatz, die Auswertung von Ausdrücken mit Hilfe einer ***abstrakten Maschine***. Um diese zu definieren, müssen wir uns zwar etwas mehr abstrampeln, können dann aber als Lohn der Bemühungen einen gegebenen Ausdruck Schritt für Schritt, peu à peu ausrechnen. Die Maschine ist zwar abstrakt — wir abstrahieren von den zahlreichen Details realer Maschinen — zeichnet aber dennoch ein hinreichend realistisches Bild der Wirklichkeit.

Abstrakte Maschine Schauen wir uns noch einmal die Regeln der dynamischen Semantik, die Auswertungsregeln, an.



Die Bedeutung eines komplexen arithmetischen Ausdrucks wird festgelegt, indem Instanzen der Beweisregeln zu einem Beweisbaum zusammengesetzt werden. Der arithmetische Ausdruck *Add* (*Add* (*Num* 4, *Num* 7), *Add* (*Num* 1, *Num* 2)) besteht zum Beispiel aus sieben Knoten; der korrespondierende Beweisbaum entsprechend aus sieben Regelinstanzen (aus Platzgründen haben wir die Konstruktoren mit ihrem ersten Buchstaben abgekürzt).



Jeder Auswerter, menschlich oder maschinell, wird zu einem gegebenen Ausdruck einen solchen Beweisbaum konstruieren und traversieren. In der Regel wird der Beweisbaum dabei nicht *explizit* in Erscheinung treten; er wird nicht als Datum repräsentiert, sondern ist nur gedanklich, zum Beispiel *implizit* durch die Programmstruktur, gegeben — im Fall des metazirkulären Interpreters entspricht der Beweisbaum dem Rekursionsbaum.

Die Pfeile in den obigen Diagrammen sollen die Traversierung des Beweisbaums illustrieren. Entlang der blauen Pfeile klettern wir nach oben: Aus einem zusammengesetzten Ausdruck wird ein Teilausdruck herausgelöst, mit dessen Auswertung dann fortgefahren wird. Im obigen Beispiel klettern wir am Anfang insgesamt dreimal nach oben: Aus dem vorgegebenen Ausdruck *Add* (*Add* (*Num* 4, *Num* 7), *Add* (*Num* 1, *Num* 2)) wird der erste Summand herausgelöst; aus *Add* (*Num* 4, *Num* 7) wird wiederum *Num* 4 herausgelöst.

[11] Das Attribut »zirkulär« deutet darauf hin, dass der Interpreter in der Sprache geschrieben ist, deren Programme er verarbeitet.

In jedem Schritt müssen wir uns merken, was noch zu tun ist, wenn die Auswertung des jeweiligen Teilausdrucks abgeschlossen ist. Also, wenn wir e_1 aus $Add\ (e_1, e_2)$ herauslösen, müssen wir uns den »restlichen« Ausdruck $Add\ (\bullet, e_2)$ merken — der Platzhalter »$\bullet$« symbolisiert dabei die Position, an der wir etwas entfernt haben. Wenn wir den Wert n_1 von e_1 kennen, fahren wir dann mit der Auswertung von e_2 fort. Jetzt müssen wir uns n_1 merken: Aus $Add\ (\bullet, e_2)$ wird $Add\ (n_1, \bullet)$. Wenn die Auswertung von e_2 ebenfalls abgeschlossen ist, können wir schließlich die Addition durchführen und das Resultat zurückgeben, sprich im Beweisbaum entlang der orangenen Pfeile nach unten klettern.

Ausdrücke mit »Löchern«, Einträge auf einer ***Todo-Liste***, repräsentieren wir mit Hilfe des folgenden Datentyps. Die Ziffer gibt jeweils die Position des Platzhalters an.

```
type Frame =
  | Add1 of Expr          // Add1 e2 ≅ Add (•, e2)
  | Add2 of Value         // Add2 v1 ≅ Add (v1, •)
```

Das allgemeine Prinzip lässt sich am besten mit Hilfe einer fiktiven, 3-stelligen Operation verdeutlichen.

$$\frac{e_1 \Downarrow v_1 \qquad e_2 \Downarrow v_2 \qquad e_3 \Downarrow v_3}{Op\ (e_1, e_2, e_3) \Downarrow op\ (v_1, v_2, v_3)}$$

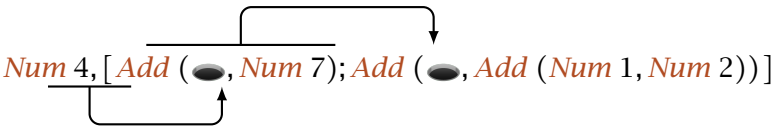
Entsprechend der fiktiven Auswertungsregel vollzieht sich die Auswertung in drei bzw. in vier Schritten — je nachdem, ob man die semantische Operation $op\ (v_1, v_2, v_3)$ als letzten Schritt hinzuzählt oder nicht.

$$Op\ (e_1, e_2, e_3) \rightsquigarrow Op\ (\bullet, e_2, e_3) \rightsquigarrow Op\ (v_1, \bullet, e_3) \rightsquigarrow Op\ (v_1, v_2, \bullet) \rightsquigarrow op\ (v_1, v_2, v_3)$$

Das Loch »$\bullet$« markiert jeweils die Grenze zwischen dem ausgewerteten und dem unausgewerteten Teil des Ausdrucks. Da das Loch an drei Positionen stehen kann, würden wir entsprechend drei Sorten von ***Todo-Einträgen*** zum Variantentyp *Frame* hinzufügen.

```
type Frame =
  | ...
  | Op1 of Expr  * Expr       // Op1 (e2, e3) ≅ Op (•, e2, e3)
  | Op2 of Value * Expr       // Op2 (v1, e3) ≅ Op (v1, •, e3)
  | Op3 of Value * Value      // Op3 (v1, v2) ≅ Op (v1, v2, •)
```

Natürlich genügt es nicht, sich nur *einen* »restlichen« Teilausdruck, ein Element vom Typ *Frame*, zu merken. Ist ein Ausdruck tief verschachtelt, so lösen wir wiederholt Teilausdrücke heraus, die wir uns auf einer ***Todo-Liste*** vom Typ *Frame list* merken. Das obige Beispiel fortführend repräsentiert



die Auswertung nach den ersten drei Schritten. Im Prinzip nehmen wir einen Repräsentationswechsel vor: Aus der Todo-Liste lässt sich der ursprüngliche Ausdruck rekonstruieren, indem wir die Teilausdrücke wie oben angedeutet wieder in die Löcher einsetzen.

Jetzt haben wir fast alle Zutaten beisammen. Unsere abstrakte Maschine befindet sich stets in einem von zwei möglichen Zuständen, je nachdem, ob sie sich im Beweisbaum nach oben oder nach unten bewegt, ob sie einen Ausdruck auswertet, $e \Downarrow \cdots$, oder einen Wert zurückgibt, $\cdots \Downarrow v$.

Auf dem Weg nach unten werden die semantischen Operationen durchgeführt: Aus den *Werten* der Teilausdrücke wird der *Wert* des Gesamtausdrucks berechnet.

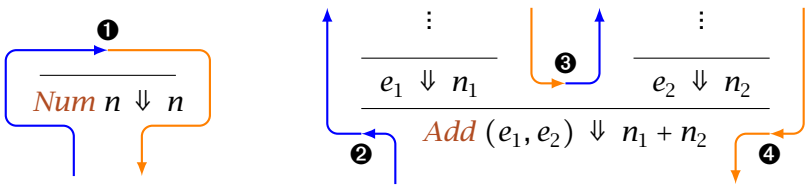
```
type State =
  | Eval of Expr  * Frame list        // e ⇓ ···
  | Ret  of Value * Frame list        // ··· ⇓ v
```

Die beiden Konstruktoren können auch als Instruktionen aufgefasst werden: Die Instruktion $Eval\ (e, stack)$ entspricht einem blauen Pfeil, $Ret\ (v, stack)$ einem orangenen, wobei *stack* jeweils die Todo-Liste repräsentiert. Apropos, die Todo-Liste nennt man im Fachjargon ***Stapel*** (engl. stack), da sie streng von links nach rechts bzw., um im Bild zu bleiben, von oben nach unten abgearbeitet wird — das unterscheidet sie von meinem Todo-Zettel. ***Rahmen*** (engl. frame) ist ein technischer Begriff aus dem Übersetzerbau.

Die Funktion *step* implementiert einen einzelnen Rechenschritt, einen Zustandsübergang der abstrakten Maschine.

```
let step : State → State = function
 // Auswertung (blau)
   | Eval (Num n,          stack) → Ret (n, stack)              // ❶
   | Eval (Add (e1, e2), stack) → Eval (e1, Add1 e2 :: stack)   // ❷
 // Rückgabe (orange)
   | Ret (v, [])                → Ret (v, [])                   // Endzustand
   | Ret (v1, Add1 e2 :: stack) → Eval (e2, Add2 v1 :: stack)   // ❸
   | Ret (v2, Add2 v1 :: stack) → Ret (v1 + v2, stack)          // ❹
```

Da es zwei prinzipielle Zustände gibt, $\rightarrow$ und $\rightarrow$, existieren insgesamt $2 \cdot 2 = 4$ Zustandsübergänge: $\rightarrow\rightarrow$, $\rightarrow\rightarrow$, $\rightarrow\rightarrow$ und $\rightarrow\rightarrow$. Die beiden Auswertungsregeln



illustrieren alle möglichen Arten von Übergängen.

Ist die Todo-Liste leer, so haben wir entweder einen ***Anfangszustand***, $Eval\ (e, [\,])$, oder einen ***Endzustand***, $Ret\ (v, [\,])$, vor uns. Mit Hilfe von *step* können wir einen Mini^2-Ausdruck im Mini-F#-Interpreter schrittweise ausrechnen.

```
>>> step (Eval (Add (Num 4, Num 7), []))
Eval (Num 4, [Add1 (Num 7)])
>>> step it
Ret (4, [Add1 (Num 7)])
>>> step it
Eval (Num 7, [Add2 4])
>>> step it
Ret (7, [Add2 4])
>>> step it
Ret (11, [])
```

Wir rufen *step* solange auf, bis die Todo-Liste leer ist.

Zu unserem laufenden Beispiel korrespondiert die folgende Abfolge von Zuständen.

```
Eval (Add (Add (Num 4, Num 7), Add (Num 1, Num 2)), [ ])
Eval (Add (Num 4, Num 7), [Add1 (Add (Num 1, Num 2))])
Eval (Num 4, [Add1 (Num 7); Add1 (Add (Num 1, Num 2))])
Ret (4, [Add1 (Num 7); Add1 (Add (Num 1, Num 2))])
Eval (Num 7, [Add2 4; Add1 (Add (Num 1, Num 2))])
Ret (7, [Add2 4; Add1 (Add (Num 1, Num 2))])
Ret (11, [Add1 (Add (Num 1, Num 2))])
Eval (Add (Num 1, Num 2), [Add2 11])
Eval (Num 1, [Add1 (Num 2); Add2 11])
Ret (1, [Add1 (Num 2); Add2 11])
Eval (Num 2, [Add2 1; Add2 11])
Ret (2, [Add2 1; Add2 11])
Ret (3, [Add2 11])
Ret (14, [ ])
```

Die Anzahl der Zustände entspricht der Anzahl der Pfeile in dem weiter oben dargestellten Beweisbaum: Insgesamt haben wir sieben blaue und sieben orangene Pfeile.

4.5.2. Boolesche Ausdrücke und Werte⋆

Wir erweitern Mini^2 um Boolesche Ausdrücke. Zusätzlich ersetzen wir die spezielle Additionsoperation durch einen »generischen« binären Operator, so dass wir die zahlreichen arithmetischen und Vergleichsoperationen einheitlich behandeln können.

module Interpreter.Booleans

```
type Op =
  | Add | Sub | Mul | Div | Mod | Lt | Lte | Equ | Neq | Gte | Gt
type Expr =
  | Num of Nat                    // n
  | Bin of Expr * Op * Expr       // e1 + e2, e1 ÷ e2 etc.
  | False                         // false
  | True                          // true
  | If  of Expr * Expr * Expr     // if e1 then e2 else e3
```

Die folgenden Abkürzungen dienen dazu, die Lesbarkeit der abstrakten Syntax zu verbessern.

```
let add (e1, e2) = Bin (e1, Add, e2)
let sub (e1, e2) = Bin (e1, Sub, e2)
let mul (e1, e2) = Bin (e1, Mul, e2)
...
let equ (e1, e2) = Bin (e1, Equ, e2)
...
```

Die Funktionen illustrieren im Kleinen, dass wir Programme in der abstrakten Syntax von Mini^2 auch mit Hilfe von Mini–F#-Funktionen *generieren* können — dabei nutzen wir aus, dass Programme als Daten behandelt werden.

Der Typ der Werte wird entsprechend um Wahrheitswerte erweitert.

```
type Value =
  | Nat  of Nat          // n
  | Bool of Bool         // false oder true
```

Die Werte werden jeweils mit ihrem Typ »getaggt«. Da wir, wie bereits angesprochen, die Typprüfung nicht statisch, sondern dynamisch durchführen, werden sozusagen aus Typen Daten:

Bool false und *Nat* 4711 sind Elemente vom Typ *Value*; der Datenkonstruktor *Bool* bzw. *Nat* verrät jeweils den Typ des Datums.

Die Funktion *primitive* implementiert die verschiedenen Operationen und führt die dynamische Typprüfung durch.

```
let primitive : Value * Op * Value → Value option = function
  | (Nat n1, Add, Nat n2) → Some (Nat (n1 + n2))
  | (Nat n1, Sub, Nat n2) → Some (Nat (n1 - n2))
  | (Nat n1, Mul, Nat n2) → Some (Nat (n1 * n2))
  | (Nat n1, Div, Nat n2) → Some (Nat (n1 / n2))
  | (Nat n1, Mod, Nat n2) → Some (Nat (n1 % n2))
  | (Nat n1, Lt,  Nat n2) → Some (Bool (n1 < n2))
  | (Nat n1, Lte, Nat n2) → Some (Bool (n1 <= n2))
  | (Nat n1, Equ, Nat n2) → Some (Bool (n1 = n2))
  | (Nat n1, Neq, Nat n2) → Some (Bool (n1 <> n2))
  | (Nat n1, Gte, Nat n2) → Some (Bool (n1 >= n2))
  | (Nat n1, Gt,  Nat n2) → Some (Bool (n1 > n2))
  | _                     → None
```

Die Funktion setzt im Prinzip die Regeln der statischen Semantik um: Ein arithmetischer Operator erwartet zwei natürliche Zahlen als Eingabe und gibt eine natürliche Zahl als Ausgabe zurück; ein Vergleichsoperator erwartet die gleichen Eingaben, gibt aber einen Wahrheitswert zurück. Werden die Erwartungen nicht erfüllt, schlägt die Typprüfung fehl und das Ergebnis ist *None*. Man sieht jeweils sehr schön, wie Syntax (*Add* etc.) auf Semantik (+ etc.) abgebildet wird.

Kommen wir zur Auswertung der Alternative. Es ist hilfreich, sich noch einmal die Auswertungsregeln ins Gedächtnis zu rufen.

$$\frac{e_1 \Downarrow \mathit{true} \qquad e_2 \Downarrow v}{\mathit{If}\ (e_1, e_2, e_3) \Downarrow v} \qquad \frac{e_1 \Downarrow \mathit{false} \qquad e_3 \Downarrow v}{\mathit{If}\ (e_1, e_2, e_3) \Downarrow v}$$

Beiden Regeln ist gemeinsam, dass die Bedingung e_1 ausgewertet wird. In Abhängigkeit vom Ergebnis wird genau ein Zweig der Alternative ausgewertet: e_2 oder e_3. Ein weiteres Detail ist bedeutsam: Das Ergebnis v des Zweigs ist auch das Ergebnis der Alternative $\mathit{If}\ (e_1, e_2, e_3)$. Im Unterschied zu den binären Operatoren gibt es nach der Auswertung von e_2 bzw. e_3 nichts mehr zu tun; der berechnete Wert wird einfach »nach unten« weitergereicht (im Fall der Additionsoperation müssen die Werte der Summanden noch addiert werden). Da wir uns auf der Todo-Liste somit nichts merken müssen, enthält *Frame* nur einen Konstruktor für die Alternative, und nicht zwei wie im Fall der binären Operatoren.

```
type Frame =
  | Bin1 of Op * Expr        // Bin (●, op, e2)
  | Bin2 of Value * Op       // Bin (v1, op, ●)
  | If1  of Expr * Expr      // If (●, e2, e3)
```

Im Ein-Schritt-Auswerter gesellen sich zu den Fällen für arithmetische Ausdrücke Fälle für Boolesche Konstanten und die Alternative.

```
let step : State → State = function
 // Auswertung
   | Eval (Num n,           stack)      → Ret (Nat n, stack)
   | Eval (Bin (e1, op, e2), stack)     → Eval (e1, Bin1 (op, e2) :: stack)
   | Eval (False,           stack)      → Ret (Bool false, stack)
   | Eval (True,            stack)      → Ret (Bool true, stack)
   | Eval (If (e1, e2, e3), stack)      → Eval (e1, If1 (e2, e3) :: stack)
 // Rückgabe
   | Ret (v,      [])                   → Ret (v, [])
   | Ret (v1,     Bin1 (op, e2) :: stack) → Eval (e2, Bin2 (v1, op) :: stack)
   | Ret (v2,     Bin2 (v1, op) :: stack) → match primitive (v1, op, v2) with
                                              | Some v → Ret (v, stack)
                                              | None   → error "type mismatch"
   | Ret (Bool b, If1 (e2, e3)  :: stack) → if b then Eval (e2, stack)
                                            else Eval (e3, stack)
   | Ret (_,      If1 (e2, e3)  :: stack) → error "type mismatch"
```

Die beiden Regeln für die Alternative setzen die Auswertungsregeln der dynamischen Semantik buchstabengetreu um. Um $If\ (e_1, e_2, e_3)$ auszurechnen, wird zunächst die Bedingung e_1 ausgewertet; auf der Todo-Liste, dem Stack, merken wir uns die beiden Zweige der Alternative. Ist der Boolesche Wert ermittelt, wird mit der Auswertung eines der beiden Zweige fortgefahren. Die Todo-Liste ist jetzt wieder auf dem ursprünglichen Stand. Dieses kleine Implementierungsdetail hat weitreichende Konsequenzen; es ist ein Mosaikstein einer wichtigen, ja zentralen Optimierung, der sogenannten »***Tail Call Optimization***«. Aber dazu später mehr.

An zwei Stellen brechen wir die Auswertung mit einem ***Typfehler*** ab: Wenn die Typprüfung der primitiven Operationen fehlschlägt oder wenn die Bedingung einer Alternative nicht zu einem Wahrheitswert auswertet.

Schauen wir uns ein Beispiel an: Die Auswertung von (***if*** $4 < 11$ ***then*** 4 ***else*** $11) + 1$ in der konkreten bzw. $Bin\ (If\ (Bin\ (Num\ 4, Lt, Num\ 11), Num\ 4, Num\ 11), Add, Num\ 1)$ in der abstrakten Syntax nimmt den folgenden Verlauf (wir führen lediglich die Zustände der abstrakten Maschine auf; *step* führt uns von einem zum nächsten Zustand).

$$
\begin{aligned}
&Eval\ (Bin\ (If\ (Bin\ (Num\ 4, Lt, Num\ 11), Num\ 4, Num\ 11), Add, Num\ 1), [\,])\\
&Eval\ (If\ (Bin\ (Num\ 4, Lt, Num\ 11), Num\ 4, Num\ 11), [Bin_1\ (Add, Num\ 1)])\\
&Eval\ (Bin\ (Num\ 4, Lt, Num\ 11), [If_1\ (Num\ 4, Num\ 11); Bin_1\ (Add, Num\ 1)])\\
&Eval\ (Num\ 4, [Bin_1\ (Lt, Num\ 11); If_1\ (Num\ 4, Num\ 11); Bin_1\ (Add, Num\ 1)])\\
&Ret\ (Nat\ 4, [Bin_1\ (Lt, Num\ 11); If_1\ (Num\ 4, Num\ 11); Bin_1\ (Add, Num\ 1)])\\
&Eval\ (Num\ 11, [Bin_2\ (Nat\ 4, Lt); If_1\ (Num\ 4, Num\ 11); Bin_1\ (Add, Num\ 1)])\\
&Ret\ (Nat\ 11, [Bin_2\ (Nat\ 4, Lt); If_1\ (Num\ 4, Num\ 11); Bin_1\ (Add, Num\ 1)])\\
&Ret\ (Bool\ false, [If_1\ (Num\ 4, Num\ 11); Bin_1\ (Add, Num\ 1)])
\end{aligned}
$$

An dieser Stelle haben wir die Bedingung der Alternative ausgerechnet und fahren mit der Auswertung des ***else***-Zweigs fort.

$$
\begin{aligned}
&Eval\ (Num\ 11, [Bin_1\ (Add, Num\ 1)])\\
&Ret\ (Nat\ 11, [Bin_1\ (Add, Num\ 1)])\\
&Eval\ (Num\ 1, [Bin_2\ (Nat\ 11, Add)])\\
&Ret\ (Nat\ 1, [Bin_2\ (Nat\ 11, Add)])\\
&Ret\ (Nat\ 12, [\,])
\end{aligned}
$$

Man sieht sehr schön, dass das Ergebnis des ***else***-Zweigs unmittelbar an die Additionsoperation weitergereicht wird. Anhand der Todo-Liste lässt sich nicht mehr nachvollziehen, dass 11 dem

Zweig einer Alternative entstammt. Die letzten fünf Zustände erhalten wir auch, wenn wir zum Beispiel 11 + 1 bzw. *Bin* (*Num* 11, *Add*, *Num* 1) ausrechnen.

4.5.3. Wertedefinitionen⋆

module Interpreter.Definitions

Im nächsten Schritt erweitern wir Mini^2 um Bezeichner und Wertedefinitionen.

```
type Id = String
type Expr =
  | ...
  | Id   of Id                          // x
  | Let of Id * Expr * Expr             // let x1 = e1 in e
```

Bezeichner repräsentieren wir durch Strings. Wertedefinitionen sind im Vergleich zu Mini–F# einfacher gestrickt: *Let* (x_1, e_1, e) entspricht in der konkreten Syntax ***let*** $x_1 = e_1$ ***in*** e, kombiniert also eine Deklaration mit einem ***in***-Ausdruck. (Auf diese Weise sparen wir uns die Einführung einer zweiten syntaktischen Kategorie: Deklarationen zusätzlich zu Ausdrücken. *Ein* Typ für Ausdrücke ist einfacher zu handhaben als *zwei* verschränkt rekursive Typen für Ausdrücke und Deklarationen.)

Die Einführung von Bezeichnern zieht den viel zitierten Rattenschwanz von Änderungen nach sich; nahezu jedes Detail unserer abstrakten Maschine muss angepasst werden.

Ausgangspunkt unserer Überlegungen sind wie immer die Auswertungsregeln der dynamischen Semantik.

$$\frac{}{\delta \vdash Id\ x \Downarrow \delta(x)} \qquad \frac{\delta \vdash e_1 \Downarrow v_1 \qquad \delta, \{x_1 \mapsto v_1\} \vdash e \Downarrow v}{\delta \vdash Let\ (x_1, e_1, e) \Downarrow v}$$

In Mini–F# garantiert die statische Semantik, dass der Bezeichner x in der Umgebung δ definiert wird. In Mini^2 führen wir diese Überprüfung dynamisch zur Laufzeit durch. Eine Wertedefinition wird in zwei Schritten abgearbeitet: Zunächst wird die rechte Seite der Gleichung $x_1 = e_1$ ausgewertet; der erhaltene Wert v_1 wird an x_1 gebunden; in der um diese Bindung erweiterten Umgebung wird der Ausdruck e ausgerechnet. Ähnlich wie im Fall der Alternative ist nach der Auswertung von e für die Wertedefinition nichts mehr zu tun; der berechnete Wert v wird »nach unten« weitergereicht (ein weiteres Mosaikstück der ***Tail Call Optimization***.)

Bevor wir uns den Änderungen an der abstrakten Maschine zuwenden, müssen wir zunächst überlegen, wie wir Umgebungen repräsentieren. Wir erinnern uns: Eine Umgebung ist eine endliche Abbildung von Bezeichnern auf Werte. Mit der Implementierung von endlichen Abbildungen beschäftigen wir uns intensiv in Abschnitt 5.3; dem wollen wir an dieser Stelle nicht vorgreifen, so dass wir eine konzeptionell einfachere Lösung wählen.[12] In der dynamischen Semantik wird eine Umgebung, ausgehend von der leeren endlichen Abbildung, schrittweise mit dem Kommaoperator um Bindungen erweitert. Diese beiden Operationen machen wir zu Konstruktoren eines Datentyps!

```
type Map<'key, 'val> =
  | Empty                               // ∅
  | Comma of Map<'key, 'val> * 'key * 'val   // δ, {x ↦ v}
```

Der Typ ist parametrisiert mit dem Definitions- und dem Wertebereich endlicher Abbildungen: Wenn wir Typen mit Mengen identifizieren, dann entspricht *Map* $\langle X, Y \rangle$ der Menge $X \to_{\text{fin}} Y$ aller

[12] Tatsächlich ist eine ausgefeilte Implementierung nicht notwendig, da Umgebungen nicht sehr groß werden: Die Anzahl der Bindungen hängt *statisch* vom Programmtext ab und nicht *dynamisch* vom Verlauf der Rechnung.

endlichen Abbildungen von X nach Y. Der Konstruktor *Empty* repräsentiert die leere Abbildung; wenn *env* die Umgebung δ repräsentiert, dann repräsentiert *Comma* (env, x, v) die Umgebung $\delta, \{x \mapsto v\}$.

Die Funktion *lookup* entspricht der Anwendung einer endlichen Abbildung; *lookup x env* schlägt den Bezeichner *x* in *env* nach. (Der Zusatz ***when*** *'key* : *equality* drückt aus, dass der Typ *'key* nicht vollkommen beliebig ist: Er muss den Test auf Gleichheit unterstützen.)

```
let rec lookup (x : 'key) : Map⟨'key, 'val⟩ → 'val option when 'key : equality = function
  | Empty →                    None
  | Comma (env, x1, v1) → if x = x1 then Some v1 else lookup x env
```

Repräsentiert *env* die Umgebung δ, dann gilt *lookup x env* = *Some v*, falls $x \in dom\ \delta$ und $\delta(x) = v$; anderenfalls erhalten wir *lookup x env* = *None*. Das Datum

```
Comma (Comma (Empty, "a", Nat 4711), "b", Bool false)
```

repräsentiert zum Beispiel die Umgebung, in der `"a"` an 4711 und `"b"` an *false* gebunden ist: $\emptyset, \{a \mapsto 4711\}, \{b \mapsto false\} = \{a \mapsto 4711, b \mapsto false\}$. Weiter rechts stehende Bindungen verschatten dabei wie gewünscht weiter links stehende Bindungen, da *lookup* gemäß der Struktur des Datentyps von »rechts nach links« vorgeht.

(Der Typ *Map* ⟨*'key*, *'val*⟩ ist übrigens isomorph zu (*'key* ∗ *'val*) *list*, einer Liste von Schlüssel-Wert Paaren. Im Unterschied zu einer Liste werden Einträge nicht vorne mit »::«, sondern hinten mit *Comma* hinzugefügt. Der Grund für die Einführung eines speziellen Typs ist so banal, wie überzeugend: Er erlaubt es uns, die Regeln der dynamischen Semantik buchstabengetreu umzusetzen.)

Todo-Einträge vom Typ *Frame* und Zustände der abstrakten Maschine vom Typ *State* müssen um Umgebungen erweitert werden. Klar: Jeder Teilausdruck kann potentiell einen Bezeichner enthalten, so dass wir Umgebungen für die Auswertung bereitstellen und zu diesem Zweck auf der Todo-Liste vermerken müssen.

```
type Env = Map⟨Id, Value⟩
type Frame =
  | Bin1 of Env ∗ Op ∗ Expr          // δ, Bin (●, op, e2)
  | Bin2 of       Value ∗ Op         // Bin (v1, op, ●)
  | If1  of Env ∗ Expr ∗ Expr        // δ, If (●, e2, e3)
  | Let1 of Env ∗ Id ∗ Expr          // δ, Let (x, ●, e)
```

Jeder Konstruktor erhält die aktuelle Umgebung als zusätzlichen Parameter mit auf den Weg, bis auf eine Ausnahme: Bin_2. Für die Ausführung einer primitiven Operation wird schlicht und einfach keine Umgebung benötigt.

```
type State =
  | Eval of Env ∗ Expr ∗ Frame list      // δ ⊢ e ⇓ ···, stack
  | Ret  of      Value ∗ Frame list      // ··· ⇓ v, stack
```

Die Instruktion *Eval* $(\delta, e, stack)$ weist die Maschine an, den Ausdruck *e* in der Umgebung δ auszuwerten; *Ret* $(v, stack)$ instruiert die Maschine, den Wert *v* zurückzugeben, sprich für die Abarbeitung des nächsten Eintrags auf der Todo-Liste *stack* zu verwenden.

Wenden wir uns der »Schrittfunktion« zu. (Bezeichner dürfen in F# nicht nur aus lateinischen, sondern auch aus griechischen Buchstaben bestehen; an Stelle des Bezeichners *env* verwenden wir im Folgenden stets δ.)

```
let step : State → State = function
 // Auswertung
   | Eval (δ, Num n,          stack) → Ret (Nat n, stack)
   | Eval (δ, Bin (e1, op, e2), stack) → Eval (δ, e1, Bin1 (δ, op, e2) :: stack)
   | Eval (δ, False,          stack) → Ret (Bool false, stack)
   | Eval (δ, True,           stack) → Ret (Bool true, stack)
   | Eval (δ, If (e1, e2, e3), stack) → Eval (δ, e1, If1 (δ, e2, e3) :: stack)
   | Eval (δ, Id x,           stack) → match lookup x δ with
                                       | None   → error ("'" ^ x ^ "' is undefined")
                                       | Some v → Ret (v, stack)
   | Eval (δ, Let (x1, e1, e), stack) → Eval (δ, e1, Let1 (δ, x1, e) :: stack)
```

Die ersten fünf Regeln kennen wir schon — nur, dass wir uns bisher nicht um Umgebungen kümmern mussten. Im Fall von Konstanten können wir die Umgebung ignorieren; bei der Auswertung zusammengesetzter Ausdrücke propagieren wir die Umgebung zu den Teilausdrücken. Die Umgebung kommt schließlich bei der Auswertung von Bezeichnern zum Einsatz; ist der Bezeichner nicht definiert, wird die Rechnung mit einem Laufzeitfehler abgebrochen.

Die beiden Regeln für *let*-Ausdrücke setzen die dynamische Semantik buchstabengetreu um: Zunächst wird die rechte Seite der Gleichung $x_1 = e_1$ ausgewertet (Code oben); der erhaltene Wert v_1 wird an x_1 gebunden; in der um diese Bindung erweiterten Umgebung wird der Ausdruck e ausgerechnet (Code unten).

```
 // Rückgabe
   | Ret (v,  [])                    → Ret (v, [])
   | Ret (v1, Bin1 (δ, op, e2)   :: stack) → Eval (δ, e2, Bin2 (v1, op) :: stack)
   | Ret (v2, Bin2 (v1, op)      :: stack) → match primitive (v1, op, v2) with
                                             | Some v → Ret (v, stack)
                                             | None   → error "type mismatch"
   | Ret (Bool b, If1 (δ, e2, e3) :: stack) → if b then Eval (δ, e2, stack)
                                              else Eval (δ, e3, stack)
   | Ret (_,  If1 (δ, e2, e3)    :: stack) → error "type mismatch"
   | Ret (v1, Let1 (δ, x1, e)    :: stack) → Eval (Comma (δ, x1, v1), e, stack)
```

Schauen wir uns die abstrakte Maschine in Aktion an und werten den geschachtelten Ausdruck *let* $a = 47$ *in let* $b = a + 11$ *in* $a * b$ bzw. in abstrakter Syntax

```
Let ("a", Num 47, Let ("b", Bin (Id "a", Add, Num 11), Bin (Id "a", Mul, Id "b"))) |
```

aus. Um nicht den Überblick zu verlieren, vereinbaren wir zwei Abkürzungen: eine für die vom äußeren *let*-Ausdruck erzeugte Umgebung, δ = *Comma* (*Empty*, "a", *Nat* 47), und eine weitere für den Rumpf des inneren *let*-Ausdrucks, e = *Bin* (*Id* "a", *Mul*, *Id* "b"). (Wie gewohnt geben wir nur die Abfolge der Zustände an.)

```
Eval (Empty, Let ("a", Num 47, Let ("b", Bin (Id "a", Add, Num 11), e)), [])
Eval (Empty, Num 47, [Let1 (Empty, "a", Let ("b", Bin (Id "a", Add, Num 11), e))])
Ret (Nat 47, [Let1 (Empty, "a", Let ("b", Bin (Id "a", Add, Num 11), e))])
Eval (δ, Let ("b", Bin (Id "a", Add, Num 11), e), [])
Eval (δ, Bin (Id "a", Add, Num 11), [Let1 (δ, "b", e)])
Eval (δ, Id "a", [Bin1 (δ, Add, Num 11); Let1 (δ, "b", e)])
Ret (Nat 47, [Bin1 (δ, Add, Num 11); Let1 (δ, "b", e)])
Eval (δ, Num 11, [Bin2 (Nat 47, Add); Let1 (δ, "b", e)])
Ret (Nat 11, [Bin2 (Nat 47, Add); Let1 (δ, "b", e)])
Ret (Nat 58, [Let1 (δ, "b", e)])
Eval (Comma (δ, "b", Nat 58), e, [])
```

An dieser Stelle haben wir die beiden Definitionen abgearbeitet und wenden uns der Auswertung des Rumpfs e zu. Setzen wir die zwei Abkürzungen ein, um den Zustand in voller Schönheit vor uns zu haben.

```
Eval (Comma (Comma (Empty, "a", Nat 47), "b", Nat 58), Bin (Id "a", Mul, Id "b"), [])
```

Die Umgebung besteht aus zwei Einträgen; beide werden benötigt, um den Rumpf auszuwerten. Die Auswertung nimmt jetzt ihren überraschungsfreien Verlauf.

```
Eval (Comma (δ, "b", Nat 58), Id "a", [Bin1 (Comma (δ, "b", Nat 58), Mul, Id "b")])
Ret (Nat 47, [Bin1 (Comma (δ, "b", Nat 58), Mul, Id "b")])
Eval (Comma (δ, "b", Nat 58), Id "b", [Bin2 (Nat 47, Mul)])
Ret (Nat 58, [Bin2 (Nat 47, Mul)])
Ret (Nat 2726, [])
```

Die Bezeichner werden in der Umgebung nachgeschlagen und die Ergebnisse miteinander multipliziert.

4.5.4. Funktionsausdrücke und Funktionsabschlüsse⋆

Was steht als Nächstes auf dem Programm? Funktionsausdrücke und -applikationen!

```
type Expr =
  | ...
  | Fun of Id * Expr              // fun x → e
  | App of Expr * Expr            // e e1
```

module Interpreter.Functions

Die meisten Programmiersprachen, und F# ist da keine Ausnahme, erlauben Schreibvereinfachungen: Zum Beispiel kann die geschachtelte Abstraktion ***fun*** $x_1 \to$ ***fun*** $x_2 \to e$ zu ***fun*** $x_1\ x_2 \to e$ verkürzt werden. Man spricht auch von »***syntaktischem Zucker***« (engl. syntactic sugar), da die verkürzte Notation die Programmerstellung erleichtert und so das Programmierleben versüßt. Für die abstrakte Syntax können wir die gleichen Schreiberleichterungen anbieten, indem wir entsprechende Funktionen programmieren — wir machen an dieser Stelle erneut von der Idee der »Programme als Daten« Gebrauch.

```
let rec funs : Id list * Expr → Expr = function          // fun x1 x2 ··· xn → e
  | ([], e) → e
  | (x :: xs, e) → Fun (x, funs (xs, e))
let rec apps (f : Expr) : Expr list → Expr = function    // e e1 e2 ··· en
  | [] → f
  | e :: es → apps (App (f, e)) es
```

Es lohnt sich, die beiden Funktionsdefinitionen genauer zu studieren: Mehrfachabstraktionen ***fun*** $x_1\ x_2 \cdots x_n \to e$ werden auf nach *rechts* geschachtelte Abstraktionen abgebildet; Mehrfachapplikationen $e\ e_1\ e_2 \cdots e_n$ auf nach *links* geschachtelte Applikationen (f ist ein sogenannter akkumulierender Parameter).

Den Bereich der Werte erweitern wir entsprechend um Funktionsabschlüsse.

```
type Value =
  | ...
  | Closure of Env * Id * Expr    // ⟨δ, x, e⟩
```

Zur Erinnerung: Hier sind die Auswertungsregeln der dynamischen Semantik.

$$\frac{}{\delta \vdash \mathit{Fun}\ (x, e)\ \Downarrow\ \langle \delta, x, e \rangle}$$

$$\frac{\delta \vdash e \Downarrow \langle \delta', x_1, e' \rangle \qquad \delta \vdash e_1 \Downarrow v_1 \qquad \delta', \{x_1 \mapsto v_1\} \vdash e' \Downarrow v'}{\delta \vdash \mathit{App}\ (e, e_1)\ \Downarrow\ v'}$$

Ein Funktionsausdruck wertet zu einem Funktionsabschluss aus. Die Abarbeitung eines Funktionsaufrufs vollzieht sich in drei Schritten: (1) Die Funktion e wird ausgerechnet; das Ergebnis ist hoffentlich ein Funktionsabschluss. (2) Das Argument e_1 wird ausgerechnet. (3) Der Funktionsrumpf e' wird in der erweiterten Umgebung $\delta', \{x_1 \mapsto v_1\}$ ausgerechnet. Ein Detail ist bedeutsam: Das Ergebnis des Funktionsrumpfes ist auch das Ergebnis der Funktionsapplikation. Genau wie bei Alternativen und Wertebindungen wird der berechnete Wert v' einfach »nach unten« weitergereicht (dies ist das dritte und letzte Mosaikstück der ***Tail Call Optimization*** — mit den segensreichen Auswirkungen beschäftigen wir uns im nächsten Abschnitt).

Wir werden sehen, dass die Umsetzung der Regel etwas weniger aufwändig ist, da wir bereits ***let***-Ausdrücke implementiert haben. Aus diesem Grund benötigen wir nur einen Todo-Eintrag vom Typ *Frame*. Da *App* zwei Argumente besitzt, erwartet man vielleicht zwei Konstruktoren, einen für *App* (●, e_1) und einen weiteren für *App* (v, ●) — tatsächlich benötigen wir nur den ersteren.

```
type Frame =
  | ...
  | App1 of Env * Expr          // App (●, e1)
```

Die Schrittfunktion setzt wie immer die Regeln der dynamischen Semantik um.

```
let step : State → State = function
 // Auswertung
  | ...
  | Eval (δ, Fun (x, e),   stack) → Ret (Closure (δ, x, e), stack)
  | Eval (δ, App (e, e1), stack) → Eval (δ, e, App1 (δ, e1) :: stack)
```

Der Funktionsabschluss friert eine Berechnung ein: Wir merken uns alle »Zutaten« im Funktionsabschluss, die aktuelle Umgebung, den formalen Parameter und den Funktionsrumpf. (Alle auf der linken Seite eingeführten Bezeichner, δ, x, e, und *stack*, werden auf der rechten Seite genau einmal verwendet.) Wie schon angedeutet wird eine Funktionsanwendung in zwei, nicht in drei Schritten ausgerechnet. Im ersten Schritt bestimmen wir die Funktion (Code oben).

```
 // Rückgabe
  | ...
  | Ret (Closure (δ', x1, e'), App1 (δ, e1) :: stack) → Eval (δ, e1, Let1 (δ', x1, e') :: stack)
  | Ret (v,                    App1 _      :: stack) → error "type mismatch"
```

Um den zweiten Schritt zu verstehen, ist es hilfreich, sich ins Gedächtnis zu rufen, dass die Wertedefinition ***let*** $x_1 = e_1$ ***in*** e' auch durch (***fun*** $x_1 \to e'$) e_1 ausgedrückt werden kann. Umgekehrt entspricht die Kombination aus einem Funktionsabschluss *Closure* (δ', x_1, e') und einer noch zu tätigen Funktionsanwendung *App*$_1$ (δ, e_1) einer Wertebindung. Diesen Zusammenhang nutzt die Regel aus. Wenn wir den Zustandsübergang für ***let***-Ausdrücke

```
  | Eval (δ, Let (x1, e1, e), stack) → Eval (δ, e1, Let1 (δ, x1, e) :: stack)
```

mit der obigen Regel vergleichen, stellen wir allerdings einen kleinen, aber gewichtigen Unterschied fest: Im Fall der Funktionsanwendung haben wir es mit *zwei* unterschiedlichen Umgebungen zu tun. Dies liegt daran, dass die Definition der Funktion und der Funktionsaufruf räumlich getrennt sind und möglicherweise in unterschiedlichen Umgebungen ausgewertet werden.

Auch bei der Funktionsanwendung $e\ e_1$ kann ein Laufzeitfehler auftreten, nämlich dann, wenn e nicht zu einem Funktionsabschluss auswertet, der Ausdruck $App\ (Num\ 1, Num\ 2)$ ist zum Beispiel nicht wohlgetypt.

Laufzeitmessungen Jetzt da Funktionsausdrücke in Mini^2 zur Verfügung stehen, können wir lange, sehr lange Rechnungen mit wenig Programmieraufwand durchführen lassen[13], so dass wir der interessanten Frage nachgehen wollen, wie sich unser Interpreter im Vergleich zum F# Interpreter schlägt. Die Programmiersprache F# wird ebenfalls mit Hilfe einer abstrakten Maschine implementiert, die die sogenannte »Common Intermediate Language« (CLI) versteht. Unsere Maschine wird somit von einer anderen Maschine ausgeführt, die ihrerseits auf der realen Maschine, der tatsächlichen Hardware, mittels eines Programms emuliert wird. Moderne Prozessoren legen beim Rechnen eine phänomenale Geschwindigkeit an den Tag — aber, wie weit entschleunigen wir die Rechenleistung, wenn wir Abstraktionsschicht um Abstraktionsschicht einziehen?

Wie schnell rechnet der F#-Interpreter? Mit Hilfe der folgenden Funktionen können wir ihn eine Zeitlang beschäftigen.

```
let twice  = fun f x → f (f x)
let thrice = fun f x → f (f (f x))
let succ   = fun n → n + 1
```

Die Funktion *twice* wendet ihr erstes Argument zweimal auf ihr zweites Argument an; *thrice* entsprechend dreimal. Die Funktionen lassen sich auch kombinieren: *twice thrice* ist eine Funktion, die ihr erstes Argument neunmal auf ihr zweites Argument anwendet; *thrice twice* nur achtmal. (Erkennen Sie die Gesetzmäßigkeit?) Mit dem Kommando `#time` instruiert man den F#-Interpreter, zusätzlich zum Rechenergebnis die benötigte Rechenzeit in Sekunden mitzuteilen.

```
⋙ #time
⋙ twice twice twice twice succ 0
CPU: 0.010
65536
⋙ twice twice twice thrice succ 0
CPU: 2.420
43046721
```

Vielleicht ist klar, dass beide Ergebnisse erzielt werden, indem die Nachfolgerfunktion *succ* ausgehend von 0 entsprechend oft angewendet wird. Da wir nur an der Rechenzeit interessiert sind, schweigen wir uns über die weiteren Details aus. An dieser Stelle nur ein kleiner Hinweis:

$$65536 = 2^{16} = 2^{2^{2^2}} \qquad \text{und} \qquad 43046721 = 3^{16} = 3^{2^{2^2}}$$

Also, in rund 2 Sekunden können wir bis 40 Millionen zählen — so hoch hängt die Messlatte.

Hier sind die gleichen Programme in der abstrakten Syntax von Mini^2.

[13] Da Mini^2 als dynamisch getypte Sprache von der Disziplin und von den Zwängen eines statischen Typsystems befreit ist, haben wir *auch ohne rekursive Funktionsdefinitionen* tatsächlich eine ***berechnungsuniverselle*** Sprache vor uns, mit der man die prinzipiellen Möglichkeiten eines Rechners ausschöpfen kann — mehr dazu später aus der Abteilung der Theoretischen Informatik.

```
let Twice  = funs (["f";"x"], App (Id "f", App (Id "f", Id "x")))
let Thrice = funs (["f";"x"], App (Id "f", App (Id "f", App (Id "f", Id "x"))))
let Succ   = Fun ("n", add (Id "n", Num 1))
```

Um den Ausdruck e auszuwerten, wenden wir die Schrittfunktion ausgehend vom Startzustand *Eval* (*Empty*, e, [ ]) solange an, bis wir einen Endzustand der Form *Ret* (v, [ ]) erhalten.

```
let eval (e : Expr) : Value =
  let rec loop = function
    | Ret (v, [ ]) → v
    | state        → loop (step state)
  loop (Eval (Empty, e, [ ]))
```

Wiederholen wir die obigen Rechnungen, diesmal in Mini^2, nicht in F#.

```
⋙ eval (apps Twice [ Twice; Twice; Twice; Succ; Num 0 ])
CPU: 0.070
Nat 65536
⋙ eval (apps Twice [ Twice; Twice; Thrice; Succ; Num 0 ])
CPU: 23.960
Nat 43046721
```

Jetzt benötigen wir rund 20 Sekunden, um bis 40 Millionen zu zählen. Das ist ganz erstaunlich. Es war zu erwarten, dass die zusätzliche Abstraktionsschicht eine Verlangsamung um mehrere Größenordnungen nach sich zieht — die Tests deuten an, dass es nur ein Faktor im einstelligen Bereich ist. Das ist, wie gesagt, ganz erstaunlich.

Um eine Idee davon zu bekommen, wieviele Rechenschritte unser Interpreter benötigt, programmieren wir eine Variante von *eval*, die zusätzlich die Anzahl der Schritte zählt.

```
let count-steps (e : Expr) : Value * Nat =
  let rec loop = function
    | (Ret (v, [ ]), n) → (v, n)
    | (state,        n) → loop (step state, n + 1)
  loop (Eval (Empty, e, [ ]), 0)
```

Anstelle des Zeitnehmers von F# verwenden wir jetzt unseren eigenen Schrittzähler.

```
⋙ count-steps (apps Twice [ Twice; Twice; Twice; Succ; Num 0 ])
(Nat 65536, 917710)
⋙ count-steps (apps Twice [ Twice; Twice; Thrice; Succ; Num 0 ])
(Nat 43046721, 495037500)
```

Um bis 40 Millionen zu zählen, werden rund eine halbe Milliarde (!) Schritte getätigt. Allerdings: Ein Schritt entspricht *nicht* der Anwendung einer Auswertungsregel der dynamischen Semantik; unser Interpreter ist kleinschrittiger: Um eine Regel mit n Voraussetzungen abzuarbeiten, werden $n + 1$ Schritte benötigt. Trotzdem: In der Sekunde schafft unsere Maschine rund 20 Millionen Rechenschritte. Hätten Sie das gedacht?

4.5.5. Rekursive Funktionsdefinitionen⋆

»The world, marm,« said I, anxious to display my acquired knowledge, »is not exactly round, but resembles in shape a flattened orange; and it turns on its axis once in twenty-four hours.«

»Well, I don't know anything about its axes,« replied she, »but I know it don't turn round, for if it did we'd be all tumbled off; and as to its being round, any one can see it's a square piece of ground, standing on a rock!«

»Standing on a rock! but upon what does that stand?«

»Why, on another, to be sure!«

»But what supports the last?«

»Lud! child, how stupid you are! There's rocks all the way down!«

— New-York Mirror

Kommen wir zum krönenden Abschluss, dem großen Finale: der Implementierung rekursiver Funktionsdefinitionen.

```
type Expr =
  | ...
  | Letrec of Id * Id * Expr * Expr          // let rec f x1 = e in e'
```

Ähnlich wie Wertedefinitionen sind rekursive Funktionsdefinitionen im Vergleich zu Mini–F# einfacher gestrickt: der Ausdruck *Letrec* (f, x_1, e, e') entspricht in der konkreten Syntax ***let rec*** $f\ x_1 = e$ ***in*** e', kombiniert also eine rekursive Deklaration mit einem ***in***-Ausdruck.

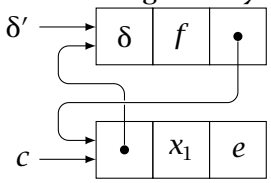
Abweichend von unserem bisherigen Vorgehen wenden wir uns unmittelbar der »Schrittfunktion« zu. Jetzt wird es abenteuerlich:

```
let step : State → State = function
 // Auswertung
  | ...
  | Eval (δ, Letrec (f, x1, e, e'), stack) → let rec δ' = Comma (δ, f, c)
                                             and     c  = Closure (δ', x1, e)
                                             in Eval (δ', e', stack)
```

Der durch die rekursive Funktionsdefinition eingeführte Bezeichner f wird an einen Funktionsabschluss gebunden, der die erweiterte Umgebung als erste Komponente enthält. Dann wird mit der Auswertung von e' weitergemacht. Damit ist die Implementierung des neuen Sprachfeatures abgeschlossen.

Das war's? Yup, mehr ist nicht zu tun! Aber vielleicht stellt sich ein mulmiges Gefühl ein: Die Umgebung δ' enthält den Funktionsabschluss c, der wiederum die Umgebung δ' enthält, die wiederum den Funktionsabschluss c enthält … ein unendlicher Regress.

Im obigen Programmfragment werden die Bezeichner δ' und c durch eine rekursive *Werte*definition eingeführt — ein Feature von F#, das wir bisher aus guten Gründen nicht besprochen haben. Wird die Definition abgearbeitet, entsteht das folgende ***zyklische Geflecht***.



Die meisten rekursiven *Werte*definitionen ergeben keinen Sinn: ***let rec*** $x = x+1$ wird zum Beispiel als fehlerhaft zurückgewiesen, da der Wert von x benötigt wird (rechte Seite), um den Wert von x zu bestimmen (linke Seite). Unser Fall ist aber unproblematisch, da die Konstruktoren Daten konstruieren. Unproblematisch ist vielleicht übertrieben — die Implementierung ist tatsächlich sehr trickreich: Die »Kästchen« in der obigen Grafik werden zunächst provisorisch mit Dummywerten angelegt: $\delta' = \mathit{Comma}\ (\bullet, \bullet, \bullet)$ und $c = \mathit{Closure}\ (\bullet, \bullet, \bullet)$; dann werden die Argumente der Konstruktoren ausgewertet und die Platzhalter anschließend durch die resultierenden Werte ersetzt — den letzten Schritt nennt man auch »***Back Patching***«.

Im Prinzip könnten wir auf diese Weise auch die in Abschnitt 3.6 eingeführten Auswertungsregeln vereinfachen und insbesondere rekursive Funktionsabschlüsse überflüssig machen. Unsere abstrakte Maschine implementiert die unten aufgeführte Auswertungsregel. Der Vorteil des Ansatzes ist, wie gesagt, dass es nur eine Art von Funktionsabschluss gibt und somit nur eine Auswertungsregel für die Funktionsapplikation.

$$\frac{\delta' \vdash e' \Downarrow v}{\delta_0 \vdash \mathit{Letrec}\ (f, x_1, e, e') \Downarrow v} \quad \text{mit} \quad \begin{array}{lcl} \delta' & = & \delta_0, \{f \mapsto c\} \\ c & = & \langle \delta', x_1, e \rangle \end{array}$$

$$\frac{\delta \vdash e_0 \Downarrow \langle \delta', x_1, e \rangle \qquad \delta \vdash e_1 \Downarrow v_1 \qquad \delta', \{x_1 \mapsto v_1\} \vdash e \Downarrow v}{\delta \vdash \mathit{App}\ (e_0, e_1) \Downarrow v}$$

Warum nur »im Prinzip«? Nun, es ist überhaupt nicht klar, was die Definition mathematisch bedeutet — die endliche Abbildung δ' enthält ja sich selbst als Komponente ihres Wertebereichs! Eine Erklärung dieses Phänomens ist möglich, dafür muss man aber schwere mathematische Geschütze auffahren: entweder eine andere Mengenlehre verwenden (»Non-wellfounded Set Theory«) oder die Mengenlehre durch die Theorie der vollständigen Halbordnungen ersetzen (»Domain Theory«). Beide Geschütze werden als zu schwer erachtet.

Wir sind in Abschnitt 3.6 diesem fundamentalen Problem aus dem Weg gegangen, indem wir die Bildung der Umgebung δ' sozusagen verzögern: Sie wird nicht bei der Definition vorgenommen, sondern bei *jedem* Aufruf der rekursiven Funktion, jedes Mal aufs Neue. Zu diesem Zweck haben wir rekursive Funktionsabschlüsse eingeführt und eine zweite Auswertungsregel für Funktionsapplikationen formuliert.

$$\frac{\delta_0, \{f \mapsto \langle \delta_0, f, x_1, e \rangle\} \vdash e' \Downarrow v}{\delta_0 \vdash \mathit{Letrec}\ (f, x_1, e, e') \Downarrow v}$$

$$\frac{\delta \vdash e_0 \Downarrow \langle \delta_0, f, x_1, e \rangle \qquad \delta \vdash e_1 \Downarrow v_1 \qquad \delta_0, \{f \mapsto \langle \delta_0, f, x_1, e \rangle\}, \{x_1 \mapsto v_1\} \vdash e \Downarrow v}{\delta \vdash \mathit{App}\ (e_0, e_1) \Downarrow v}$$

Wenn man die beiden Regelpaare genau studiert, sieht man hoffentlich, dass der Nettoeffekt der gleiche ist.

Tail Call Optimization Kehren wir aus den Sphären der höheren Mathematik zurück in die Niederungen der abstrakten Maschine. Mit Hilfe einer rekursiven Funktionsdefinition können wir zum Beispiel die Fakultätsfunktion programmieren.

```
let Factorial =
  Letrec ("fac", "n", If (equ (Id "n", Num 0),
                          Num 1,
                          mul (Id "n", App (Id "fac", sub (Id "n", Num 1)))), Id "fac")
```

Wenn wir die Fakultät ausrechnen, dann wächst beim rekursiven Abstieg die Todo-Liste stetig an. Abbildung 3.5 illustriert die Auswertung von *factorial* 3 per Hand; unsere abstrakte Maschine durchläuft grob folgende Zustände.

$\ldots; Bin_2\ (Nat\ 3, Mul)\,]\,)$
$\ldots; Bin_2\ (Nat\ 2, Mul); Bin_2\ (Nat\ 3, Mul)\,]\,)$
$\ldots; Bin_2\ (Nat\ 1, Mul); Bin_2\ (Nat\ 2, Mul); Bin_2\ (Nat\ 3, Mul)\,]\,)$
$Ret\ (Nat\ 1, [\,Bin_2\ (Nat\ 1, Mul); Bin_2\ (Nat\ 2, Mul); Bin_2\ (Nat\ 3, Mul)\,]\,)$
$Ret\ (Nat\ 1, [\,Bin_2\ (Nat\ 2, Mul); Bin_2\ (Nat\ 3, Mul)\,]\,)$
$Ret\ (Nat\ 2, [\,Bin_2\ (Nat\ 3, Mul)\,]\,)$
$Ret\ (Nat\ 6, [\,]\,)$

Erst wenn der Basisfall erreicht ist, wird die Todo-Liste wieder peu à peu abgearbeitet. Mit anderen Worten, um $n!$ auszurechnen, benötigen wir nicht nur eine lineare Anzahl an Schritten, sondern wir haben auch einen linearen Platzbedarf für den Stack.

Raum ist im gewissen Sinne eine kostbarere Ressource als Zeit. Man kann ohne große Anstrengungen doppelt so lange warten; den verfügbaren Raum zu verdoppeln, gelingt in der Regel nicht so einfach. Diesem Phänomen begegnet man auch beim Programmieren. Schauen wir uns ein paar Beispielaufrufe an — damit die Zahlen nicht so groß werden, verwenden wir an Stelle der Fakultätsfunktion ihre kleine Schwester.

$$\textbf{\textit{let rec}}\ sum\ n = \textbf{\textit{if}}\ n = 0\ \textbf{\textit{then}}\ 0\ \textbf{\textit{else}}\ n + sum\ (n \div 1)$$

Während die Fakultät dem Produkt der Zahlen von 1 bis n entspricht, berechnet $sum\ n$ deren Summe.[14] Die Tests verlaufen ernüchternd:

```
>>> sum 50000
1250025000
>>> sum 75000
Stack overflow.
```

Wenn wir in die Nähe sechsstelliger Argumente kommen, erhalten wir anstatt des Ergebnisses eine Fehlermeldung, den berüchtigten ***Stack Overflow***. Was ist passiert? Der F#-Interpreter reserviert für die Todo-Liste, den Stack, eine *begrenzte* Menge an Speicherplatz; wenn dieser Platz ausgeschöpft ist, wird die Rechnung gnadenlos abgebrochen. Zum Vergleich: Wenn eine Rechnung viel Zeit in Anspruch nimmt, können wir entscheiden, ob wir sie abbrechen oder nicht. Bei Platzmangel wird uns die Entscheidung abgenommen — es gibt auch keine Möglichkeit, den Platz zu vergrößern und anschließend die Rechnung fortzusetzen.

Wie können wir das Problem lösen? Nun, wir kennen die Ursache für den Abbruch: Die Funktion *sum* erledigt die Hauptarbeit beim rekursiven *Auf*stieg: Nach jedem rekursiven Aufruf, $sum\ (n \div 1)$, ist noch Arbeit zu erledigen, $n +$ ●, die wir uns auf der Todo-Liste merken müssen. Die Programmiertechnik des sogenannten ***Rekursionsparadoxons*** hilft uns an dieser Stelle weiter: Wir programmieren eine Funktion, die die Zahlen von 1 bis n summiert und *zusätzlich* auf das Ergebnis eine weitere Zahl addiert.

$$accumulate\ a\ n = a + sum\ n \tag{4.4}$$

Aus dieser ***Spezifikation*** lässt sich systematisch eine Implementierung herleiten. Analog zur

[14] Natürlich würden wir die Summe so nicht berechnen, da wir mit Hilfe der Gaußschen Summenformel $\sum_{i=1}^{n} i = \binom{n+1}{2} = n \cdot (n+1)/2$ das Ergebnis sehr viel schneller bestimmen können:

$$\textbf{\textit{let}}\ sum\ n = (n * (n+1)) \div 2$$

Funktion *sum* nehmen wir eine Fallunterscheidung über n vor. **Fall** $n = 0$**:**

$$
\begin{aligned}
& \mathit{accumulate}\ a\ 0 \\
= \quad & \{ \text{ Spezifikation von } \mathit{accumulate}\ (4.4) \ \} \\
& a + \mathit{sum}\ 0 \\
= \quad & \{ \text{ Definition von } \mathit{sum} \ \} \\
& a + 0 \\
= \quad & \{ \ 0 \text{ ist das neutrale Element von »+« } \} \\
& a
\end{aligned}
$$

Fall $n > 0$**:**

$$
\begin{aligned}
& \mathit{accumulate}\ a\ n \\
= \quad & \{ \text{ Spezifikation von } \mathit{accumulate}\ (4.4) \ \} \\
& a + \mathit{sum}\ n \\
= \quad & \{ \text{ Definition von } \mathit{sum} \ \} \\
& a + (n + \mathit{sum}\ (n \doteq 1)) \\
= \quad & \{ \text{ »+« ist assoziativ } \} \\
& (a + n) + \mathit{sum}\ (n \doteq 1) \\
= \quad & \{ \text{ Spezifikation von } \mathit{accumulate}\ (4.4) \ \} \\
& \mathit{accumulate}\ (a + n)\ (n \doteq 1)
\end{aligned}
$$

Fassen wir den ersten und den letzten Ausdruck jeweils zu einer Rechenregel zusammen, erhalten wir das folgende Programm.

$$\textit{let rec}\ \mathit{accumulate}\ a\ n = \textit{if}\ n = 0\ \textit{then}\ a\ \textit{else}\ \mathit{accumulate}\ (a + n)\ (n \doteq 1)$$

Die Funktion erledigt die gesamte Arbeit während des rekursiven *Ab*stiegs: Nach dem rekursiven Aufruf $\mathit{accumulate}\ (a+n)\ (n \doteq 1)$ ist nichts mehr zu tun. Der erste Parameter heißt übrigens aus naheliegenden Gründen auch ***Akkumulator***. Der Lohn für unsere Mühen: Der begrenzte Stackplatz bereitet nicht länger Probleme.

```
⋙ accumulate 0 50000
1250025000
⋙ accumulate 0 75000
2812537500
```

Im Fachjargon nennt man *accumulate* eine ***endrekursive*** Funktion (engl. tail recursive), da alle rekursiven Aufrufe an einer ***Endposition*** stehen: direkt in den Zweigen einer Alternative, einer Fallunterscheidung mit ***match*** oder im Rumpf einer Wertebindung. Zum Vergleich: *sum* ist *nicht* endrekursiv, da der rekursive Aufruf Argument einer Additionsoperation ist.

Die Optimierung beliebiger Aufrufe an Endposition nennt man ***Tail Call Optimization*** (TCO); werden nur end*rekursive* Aufrufe optimiert, spricht man von ***Tail Recursion Elimination*** (TRE). Viele gängige Programmiersprachen (z.B. C, C++, Java) unterstützen weder die eine noch die andere Optimierung.[15] Das liegt daran, dass Programmieraufgaben in diesen Sprachen aus historischen Gründen bevorzugt iterativ und nicht rekursiv angegangen werden — Abschnitt 7.3 stellt Kontrollstrukturen für die iterative Programmierung vor.

[15] Im Fall von C und C++ werden die Optimierungen vom Sprachstandard nicht vorgeschrieben. Viele gängige Übersetzer wie z.B. GCC oder Clang implementieren aber die Optimierungen.

Unsere abstrakte Maschine unterstützt wie schon mehrfach angedeutet Tail Call Optimization. Die Definition einer Endposition lässt sich unmittelbar aus den Auswertungsregeln der dynamischen Semantik ableiten. Die Regeln für Alternativen, Wertdefinitionen und Funktionsaufrufe haben alle die gleiche schematische Form:

$$\frac{\delta_1 \vdash e_1 \Downarrow v_1 \qquad \cdots \qquad \delta_n \vdash e_n \Downarrow v}{\delta \vdash e \Downarrow v}$$

Der Wert v des letzten Teilausdrucks wird jeweils unverändert nach unten weitergereicht. Da die abstrakte Maschine die Regeln buchstabengetreu umsetzt, werden Funktionsaufrufe an Endpositionen *ohne zusätzlichen Stackverbrauch* effizient abgearbeitet.

Um die Optimierung plastisch vor Augen zu führen, verwenden wir nicht *accumulate*, sondern die einfachste aller endrekursiven Funktionen, ***let rec*** *forever n = forever n* bzw. in abstrakter Syntax:

```
let Forever = Letrec ("forever", "n", App (Id "forever", Id "n"), Id "forever")
```

Für das zyklische Geflecht aus Umgebung und Funktionsabschluss vereinbaren wir Abkürzungen: δ = *Comma* (*Empty*, `"f"`, *c*) und *c* = *Closure* (δ, `"n"`, *App* (*Id* `"f"`, *Id* `"n"`)).[16] Die Auswertung von *forever* 0 nimmt folgenden Verlauf (wir kürzen *forever* mit *f* ab).

```
Eval (Empty, App (Letrec ("f", "n", App (Id "f", Id "n"), Id "f"), Num 0), [])
Eval (Empty, Letrec ("f", "n", App (Id "f", Id "n"), Id "f"), [App₁ (Empty, Num 0)])
Eval (δ, Id "f", [App₁ (Empty, Num 0)])
Ret (c, [App₁ (Empty, Num 0)])
Eval (Empty, Num 0, [Let₁ (δ, "n", App (Id "f", Id "n"))])
Ret (Nat 0, [Let₁ (δ, "n", App (Id "f", Id "n"))])
```

An dieser Stelle ist die Funktion und ihr Argument ausgerechnet und es wird mit der Auswertung des Funktionsrumpfes fortgefahren.

```
Eval (Comma (δ, "n", Nat 0), App (Id "f", Id "n"), [])
Eval (Comma (δ, "n", Nat 0), Id "f", [App₁ (Comma (δ, "n", Nat 0), Id "n")])
Ret (c, [App₁ (Comma (δ, "n", Nat 0), Id "n")])
Eval (Comma (δ, "n", Nat 0), Id "n", [Let₁ (δ, "n", App (Id "f", Id "n"))])
Ret (Nat 0, [Let₁ (δ, "n", App (Id "f", Id "n"))])
```

Nach fünf weiteren Schritten landen wir wieder im identischen Zustand! Mit anderen Worten, die Auswertung terminiert nicht; sie wird aber auch nicht durch einen »***Stack Overflow***« abgebrochen. Zum Vergleich: Der Aufruf von ***let rec*** *forever n = n + forever n* terminiert zwar in der Theorie nicht, aber in der Praxis ist irgendwann der Stackplatz erschöpft.

Wir haben bisher nicht-terminierende Programme geächtet — dieses Urteil ist aber zu engstirnig. Viele Programme sollen ewig oder zumindest lange laufen: das Betriebssystem eines Rechners, der Webserver eines Online-Shops oder, um ein geläufigeres Beispiel zu nennen, der Kommandozeileninterpreter (CLI) von F#. Damit diese Programme tatsächlich ewig laufen, muss man neben vielen anderen Dingen darauf achten, dass kein Stack Overflow auftritt — verwendet man endrekursive Funktionen, so muss die Programmiersprache TCO oder zumindest TRE unterstützen. (In Abschnitt 7.4.4 schauen wir uns konkrete Beispiele an: Kommandozeileninterpreter für

[16] Man könnte argumentieren, dass diese Definitionen tatsächlich notwendig sind, da man ein zyklisches Geflecht nicht oder zumindest nicht einfach ausgeben kann. Der F#-Interpreter geht diesem Problem mit einem Trick aus dem Weg: Er zeigt Datenstrukturen nur bis zu einer festgelegten Schachtelungstiefe an; ist diese erreicht, wird das Auslassungszeichen »…« ausgegeben.

einfache Taschenrechner.) Diese Beispiele gehören übrigens zur Gruppe der sogenannten ***reaktiven Programme***; sie reagieren auf Stimuli der Umwelt. Von einem reaktiven Programm fordert man zwar nicht, dass es terminiert, aber man wünscht sich, dass es auf einen Stimulus in angemessener oder zumindest in endlicher Zeit reagiert. (Wenn man möchte, kann man Funktionen als Spezialfall reaktiver Programme auffassen: Auf einen Stimulus, den Funktionsaufruf, folgt eine Reaktion, das Funktionsergebnis; damit ist die Interaktion allerdings beendet.) Zu diesem Thema erfahren Sie in höheren Semestern mehr.

Kommen wir zum Schluss noch einmal auf das Ausgangsproblem zurück, dem Stack Overflow als Folge »tiefer« Rekursion. Interessanterweise kann unsere Maschine auch die ursprüngliche Definition von *sum*

```
let Sum =
  Letrec ("sum", "n", If (equ (Id "n", Num 0),
                          Num 0,
                          add (Id "n", App (Id "sum", sub (Id "n", Num 1)))), Id "sum")
```

für beliebig große Argumente ausrechnen.

```
>>> eval (App (Sum, Num 50000))
Nat 1250025000
>>> eval (App (Sum, Num 75000))
Nat 2812537500
>>> eval (App (Sum, Num 1000000))
Nat 500000500000
```

Obwohl unser Interpreter vom F#-Interpreter ausgeführt wird, tritt kein Stack Overflow auf. Wie ist das zu erklären? Zum Ersten ist die Funktion *eval* endrekursiv; somit kann der F#-Interpreter beliebig tiefe rekursive Aufrufe problemlos abarbeiten — sie erinnern sich: eine Milliarde Schritte kommen schnell zusammen. Zum Zweiten wird der Stack in unserer Maschine mittels einer *dynamischen* Datenstruktur verwaltet, einer Liste, die problemlos wachsen und auch schrumpfen kann. Der F#-Interpreter verwendet im Gegensatz dazu eine *statische* Datenstruktur, ein Array, das eine feste, vorher festgelegte Größe hat.

Die Erklärung wirft vielleicht eine andere Frage auf. Wo wird die Liste oder allgemeiner wo werden eigentlich Daten und Datenstrukturen gespeichert? Neben dem Stack gibt es zu diesem Zweck einen zweiten Speicherbereich, den sogenannten ***Heap***[17]. Der Name »Haufen« (engl. heap) deutet die chaotische Organisationsstruktur an: Daten werden dort abgelegt, wo Platz ist; geht der freie Platz zur Neige, räumt man auf und wirft nicht mehr benötigte Daten weg; lässt sich nichts mehr freiräumen, versucht man den Speicherbereich zu vergrößern; erst wenn man an die physischen Grenzen der Hardware stößt, muss man aufgeben und meldet einen »***Heap Overflow***«. (So chaotisch die Struktur des Heaps, so clever und ausgefeilt sind die Algorithmen, die ihn verwalten.)

Abbildungen 4.7 und 4.8 führen den vollständigen Code für die letzte Ausbaustufe unseres Interpreters auf. Das Programm ist erstaunlich kompakt: Um die abstrakte Syntax und die dynamische Semantik von Mini^2 zu definieren, sind lediglich zwei Seiten nötig — immerhin handelt es sich bei Mini^2 um eine berechnungsuniverselle Sprache.

[17] Dieser Heap hat nichts mit der gleichnamigen Datenstruktur zu tun, mit der Prioritätswarteschlangen implementiert werden, siehe Abschnitt 5.4.

```
// endliche Abbildungen
type Map⟨'key,'val⟩ =
  | Empty
  | Comma of Map⟨'key,'val⟩ * 'key * 'val
let rec lookup (x:'key) : Map⟨'key,'val⟩ → 'val option when 'key : equality = function
  | Empty                  → None
  | Comma (env,x1,v1) → if x = x1 then Some v1 else lookup x env
// abstrakte Syntax
type Op =| Add | Sub | Mul | Div | Mod | Lt | Lte | Equ | Neq | Gte | Gt
type Id = String
type Expr =
  | Num   of Nat                    // n
  | Bin   of Expr * Op * Expr       // e1 + e2, e1 ÷ e2 etc.
  | False                           // false
  | True                            // true
  | If    of Expr * Expr * Expr     // if e1 then e2 else e3
  | Id    of Id                     // x
  | Let   of Id * Expr * Expr       // let x1 = e1 in e
  | Fun   of Id * Expr              // fun x → e
  | App   of Expr * Expr            // e e1
  | Letrec of Id * Id * Expr * Expr // let rec f x1 = e in e'
type Value =
  | Bool    of Bool                 // n
  | Nat     of Nat                  // false oder true
  | Closure of Env * Id * Expr      // ⟨δ, x, e⟩
and Env = Map⟨Id,Value⟩
// dynamische Semantik
let primitive : Value * Op * Value → Value option = function
  | (Nat n1,Add, Nat n2) → Some (Nat  (n1 + n2))
  | (Nat n1,Sub, Nat n2) → Some (Nat  (n1 ÷ n2))
  | (Nat n1,Mul, Nat n2) → Some (Nat  (n1 * n2))
  | (Nat n1,Div, Nat n2) → Some (Nat  (n1 ÷ n2))
  | (Nat n1,Mod, Nat n2) → Some (Nat  (n1 % n2))
  | (Nat n1,Lt,  Nat n2) → Some (Bool (n1 < n2))
  | (Nat n1,Lte, Nat n2) → Some (Bool (n1 ⩽ n2))
  | (Nat n1,Equ, Nat n2) → Some (Bool (n1 = n2))
  | (Nat n1,Neq, Nat n2) → Some (Bool (n1 <> n2))
  | (Nat n1,Gte, Nat n2) → Some (Bool (n1 ⩾ n2))
  | (Nat n1,Gt,  Nat n2) → Some (Bool (n1 > n2))
  | _                    → None
```

Abbildung 4.7.: Ein-Schritt-Auswerter für Mini^2 (1. Teil).

```
type Frame =
  | Bin1  of Env * Op * Expr          // δ, Bin (●, op, e2)
  | Bin2  of Value * Op               // Bin (v1, op, ●)
  | If1   of Env * Expr * Expr        // δ, If (●, e2, e3)
  | Let1  of Env * Id * Expr          // δ, Let (x1, ●, e)
  | App1  of Env * Expr               // δ, App (●, e1)
type State =
  | Eval  of Env * Expr * Frame list  // δ ⊢ e ⇓ ···, stack
  | Ret   of Value      * Frame list  // ··· ⇓ v, stack
let step : State → State = function
// Auswertung
  | Eval (δ, Num n,          stack)   → Ret (Nat n, stack)
  | Eval (δ, Bin (e1, op, e2), stack) → Eval (δ, e1, Bin1 (δ, op, e2) :: stack)
  | Eval (δ, False,          stack)   → Ret (Bool false, stack)
  | Eval (δ, True,           stack)   → Ret (Bool true, stack)
  | Eval (δ, If (e1, e2, e3), stack)  → Eval (δ, e1, If1 (δ, e2, e3) :: stack)
  | Eval (δ, Id x,           stack)   → match lookup x δ with
                                          | None   → error ("'" ^ x ^ "' is undefined")
                                          | Some v → Ret (v, stack)
  | Eval (δ, Let (x1, e1, e), stack)  → Eval (δ, e1, Let1 (δ, x1, e) :: stack)
  | Eval (δ, Fun (x, e),     stack)   → Ret (Closure (δ, x, e), stack)
  | Eval (δ, App (e, e1),    stack)   → Eval (δ, e, App1 (δ, e1) :: stack)
  | Eval (δ, Letrec (f, x1, e, e'), stack) → let rec δ' = Comma (δ, f, c)
                                             and     c  = Closure (δ', x1, e)
                                             in Eval (δ', e', stack)
// Rückgabe
  | Ret (v, [])                          → Ret (v, [])
  | Ret (v1, Bin1 (δ, op, e2)   :: stack) → Eval (δ, e2, Bin2 (v1, op) :: stack)
  | Ret (v2, Bin2 (v1, op)      :: stack) → match primitive (v1, op, v2) with
                                              | Some v → Ret (v, stack)
                                              | None   → error "type mismatch"
  | Ret (Bool b, If1 (δ, e2, e3) :: stack) → if b then Eval (δ, e2, stack)
                                               else Eval (δ, e3, stack)
  | Ret (_, If1 (δ, e2, e3)     :: stack) → error "type mismatch"
  | Ret (v1, Let1 (δ, x1, e)    :: stack) → Eval (Comma (δ, x1, v1), e, stack)
  | Ret (Closure (δ', x1, e'), App1 (δ, e1) :: stack) → Eval (δ, e1, Let1 (δ', x1, e') :: stack)
  | Ret (v,                 App1 _      :: stack) → error "type mismatch"
```

Abbildung 4.8.: Ein-Schritt-Auswerter für Mini^2 (2. Teil).

4.5.6. Fortsetzungen⋆⋆

I can resist everything except temptation.

— Oscar Fingal O'Flahertie Wills Wilde (1854–1900), *Lady Windermere's Fan*

> *For a number of years I have been familiar with the observation that the quality of programmers is a decreasing function of the density of go to statements in the programs they produce. More recently I discovered why the use of the go to statement has such disastrous effects, and I became convinced that the go to statement should be abolished from all »higher level« programming languages (i.e. everything except, perhaps, plain machine code). At that time I did not attach too much importance to this discovery; I now submit my considerations for publication because in very recent discussions in which the subject turned up, I have been urged to do so.*
>
> *My first remark is that, although the programmer's activity ends when he has constructed a correct program, the process taking place under control of his program is the true subject matter of his activity, for it is this process that has to accomplish the desired effect; it is this process that in its dynamic behavior has to satisfy the desired specifications. Yet, once the program has been made, the »making« of the corresponding process is delegated to the machine.*
>
> *My second remark is that our intellectual powers are rather geared to master static relations and that our powers to visualize processes evolving in time are relatively poorly developed. For that reason we should do (as wise programmers aware of our limitations) our utmost to shorten the conceptual gap between the static program and the dynamic process, to make the correspondence between the program (spread out in text space) and the process (spread out in time) as trivial as possible.*
>
> — Edsger W. Dijkstra (1930–2002), *Go To Statement Considered Harmful*

Jetzt da wir über eine eigene Implementierung von Mini^2 verfügen, ist die Versuchung groß, zusätzliche Sprachfeatures zu verwirklichen, Konzepte, die weder von Mini–F# noch von F# selbst unterstützt werden. Wenn Sie allerdings Dijkstra zustimmen, dann sollten Sie *jetzt nicht weiterlesen*.

Unsere abstrakte Maschine setzt die Auswertungsregeln der dynamischen Semantik recht buchstabengetreu um. Mit Hilfe der Todo-Liste, des Stacks, wird dabei die Auswertung geschachtelter Ausdrücke sequentialisiert, so dass ein Ausdruck peu à peu abgearbeitet werden kann. Zu jedem Zeitpunkt der Abarbeitung repräsentiert der Stack den »Rest der Rechnung« — wie muss mit der Rechnung fortgefahren werden, wenn die aktuelle Teilaufgabe erledigt ist. Wenn zum Beispiel der Teilausdruck e in $e*3+4$ ausgerechnet wird, dann repräsentiert der Stack das restliche Programm $\bullet * 3 + 4$. Aus naheliegenden Gründen nennt man $\bullet * 3 + 4$ auch ***Fortsetzung***.

Jetzt kommen wir zu einer vielleicht abenteuerlichen Idee: Wir ermöglichen dem/der Programmier/-in, einen Schnappschuss vom Stack zu machen und diesen zu einem späteren Zeitpunkt an Stelle des aktuellen Stacks zu verwenden. Dazu führen wir zwei neue Konstrukte ein: ***letcc*** *x* ***in*** *e* und ***continue*** *e* e_1. Mit Hilfe von ***letcc*** wird die aktuelle Fortsetzung (engl. *c*urrent *c*ontinuation, ein anderer Name für die Todo-Liste) an den Bezeichner *x* gebunden, der im Rumpf *e* sichtbar ist. Zum Beispiel wird der Bezeichner *hop* in dem Ausdruck (***letcc*** *hop* ***in*** $\cdots$) $*$ 3 + 4 an die Fortsetzung $\bullet * 3 + 4$ gebunden. Die eingefangene Fortsetzung kann anschließend mit ***continue*** *hop* e_1 verwendet werden und ersetzt den aktuellen Stack, so dass mit der Auswertung von $e_1 * 3 + 4$ weitergemacht wird. Zum Beispiel wertet

(***letcc*** *hop* ***in*** 1 + ***continue*** *hop* 2) $*$ 3 + 4

zu $2 * 3 + 4 = 10$ aus. Die Rechnung wird also mit Hilfe von ***continue*** faktisch abgebrochen und an einer anderen Stelle fortgesetzt. Da auf diese Weise der Programmablauf kontrolliert bzw. gesteuert wird, nennt man ***letcc*** und ***continue*** ***Kontrolloperatoren***.

Das war ein kleiner Hopser; das nächste Beispiel illustriert einen größeren Sprung aus einer Rekursion heraus.

```
let cross-product n =
  letcc exit
  in let rec f i = if i = 0 then 1
                   else let r = i % 10
                        in if r = 0 then continue exit 0
                                    else r * f (i ÷ 10)
     in f n
```

Die Funktion *cross-product* berechnet das ***Querprodukt*** einer natürlichen Zahl, das Produkt ihrer Ziffern. Das Querprodukt von 4711 ist zum Beispiel $4 \cdot 7 \cdot 1 \cdot 1 = 28$. Das Programm implementiert eine kleine Optimierung — hier kommen die Kontrolloperatoren ins Spiel. Wenn die Ziffer 0 auftritt, wird die Rechnung abgebrochen und unmittelbar 0 als Ergebnis zurückgegeben. Zu diesem Zweck wird direkt im Rumpf der Funktion die aktuelle Fortsetzung eingefangen, also die Stelle im Programm, die *cross-product* aufgerufen hat und an die die Funktion ihr Ergebnis zurückgibt. Wollen wir zum Beispiel 4711 + *cross-product* 10987654321 ausrechnen, dann wird *exit* an 4711 + ⬬ gebunden. Die Arbeitsfunktion f ist nach dem Leibniz Entwurfsmuster gestrickt und baut einen Turm von Multiplikationen auf: Sind die ersten neun Ziffern (von rechts) abgearbeitet, repräsentiert der Stack die Fortsetzung $4711 + (1 * (2 * (3 * (4 * (5 * (6 * (7 * (8 * (9 * (\bullet)))))))))))$. An dieser Stelle der Rechnung trifft f auf die Ziffer 0; anstatt das Produkt mit vorhersehbarem Ausgang auszurechnen, nimmt f den Seitenausgang, so dass mit der Auswertung von $4711 + 0$ fortgefahren wird. (Übrigens, warum definieren wir eine Hilfsfunktion?)

Kommen wir zur Implementierung der Kontrolloperatoren. Wir erweitern zunächst den Datentyp der Ausdrücke um zwei Konstruktoren.

```
type Expr =
  | ...
  | Letcc    of Id * Expr          // letcc x in e
  | Continue of Expr * Expr        // continue e e1
```

Der Typ der Werte wird entsprechend um Fortsetzungen erweitert.

```
type Value =
  | ...
  | Continuation of Frame list
and Env = Map ⟨Id, Value⟩
and Frame =
  | ...
  | Continue1 of Env * Expr        // δ, Continue (⬬, e1)
```

Da ***continue*** ähnlich wie ein Funktionsaufruf schrittweise ausgewertet wird, fügen wir weiterhin einen neuen Todo-Eintrag zum Typ *Frame* hinzu. Die Typen *Value*, *Env* und *Frame* sind verschränkt rekursiv — eine Fortsetzung besteht aus Todo-Einträgen vom Typ *Frame* und umgekehrt enthalten Todo-Einträge Komponenten vom Typ *Value* — somit müssen die Typdefinitionen mit ***and*** verbunden werden.

Die Schrittfunktion setzt die umgangssprachliche Beschreibung der Kontrolloperatoren ***letcc*** und ***continue*** um.

```
let step : State → State = function
 // Auswertung
  | ...
  | Eval (δ, Letcc (x, e),       stack) → Eval (Comma (δ, x, Continuation stack), e, stack)
  | Eval (δ, Continue (e, e1), stack) → Eval (δ, e, Continue1 (δ, e1) :: stack)
```

In der Regel für ***letcc*** *x* ***in*** *e* wird der aktuelle Stack *dupliziert*: Wir fahren mit der Auswertung von *e* bei unverändertem Stack fort; zusätzlich wird *x* an den Stack gebunden. Ähnlich wie bei einem Funktionsaufruf wird im Fall von ***continue*** *e* e_1 zunächst mit der Auswertung von *e* weitergemacht.

```
// Rückgabe
  | ...
  | Ret (Continuation stack, Continue₁ (δ, e₁) :: _) → Eval (δ, e₁, stack)
  | Ret (_,                 Continue₁ (δ, e₁) :: _) → error "type mismatch"
```

Das erste Argument von ***continue*** muss zu einer Fortsetzung auswerten. Ist das gegeben, wird der aktuelle Stack verworfen (anonymer Bezeichner »_«) bzw. durch den vorher eingefangenen Stack ersetzt und mit der Auswertung des zweiten Arguments von ***continue*** fortgefahren.

Schauen wir uns die Auswertung des »Hopsers« an.

$$add\ (mul\ (Letcc\ (\texttt{"hop"}, add\ (Num\ 1, Continue\ (Id\ \texttt{"hop"}, Num\ 2))), Num\ 3), Num\ 4)$$

Aus Gründen der Übersichtlichkeit verwenden wir Abkürzungen für die Fortsetzung, an die *hop* gebunden wird, und die daraus resultierende Umgebung.

$$c = Continuation\ [Bin_1\ (Empty, Mul, Num\ 3); Bin_1\ (Empty, Add, Num\ 4)]$$
$$\delta = Comma\ (Empty, \texttt{"hop"}, c)$$

Zunächst arbeiten wir die arithmetischen Operationen ab, die zu Todo-Einträgen auf dem Stack führen (einige Konstruktoren kürzen wir mit ihrem ersten Buchstaben ab).

$$Eval\ (E, B\ (B\ (Letcc\ (\texttt{"hop"}, B\ (N\ 1, A, Continue\ (Id\ \texttt{"hop"}, N\ 2))), M, N\ 3), A, N\ 4), [\,])$$
$$Eval\ (E, B\ (Letcc\ (\texttt{"hop"}, B\ (N\ 1, A, Continue\ (Id\ \texttt{"hop"}, N\ 2))), M, N\ 3), [Bin_1\ (E, A, N\ 4)])$$
$$Eval\ (E, Letcc\ (\texttt{"hop"}, B\ (N\ 1, A, Continue\ (Id\ \texttt{"hop"}, N\ 2))), [Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$

An dieser Stelle machen wir einen Schnappschuss des Stacks und binden ihn an den Bezeichner *hop*.

$$Eval\ (\delta, B\ (N\ 1, A, Continue\ (Id\ \texttt{"hop"}, N\ 2)), [Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$

Mit der Auswertung des Rumpfs von ***letcc*** geht es weiter.

$$Eval\ (\delta, N\ 1, [Bin_1\ (\delta, A, Continue\ (Id\ \texttt{"hop"}, N\ 2)); Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$
$$Ret\ (Nat\ 1, [Bin_1\ (\delta, A, Continue\ (Id\ \texttt{"hop"}, N\ 2)); Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$
$$Eval\ (\delta, Continue\ (Id\ \texttt{"hop"}, N\ 2), [Bin_2\ (Nat\ 1, A); Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$
$$Eval\ (\delta, Id\ \texttt{"hop"}, [Continue_1\ (\delta, N\ 2); Bin_2\ (Nat\ 1, A); Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$
$$Ret\ (c, [Continue_1\ (\delta, N\ 2); Bin_2\ (Nat\ 1, A); Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$

Der Stack ist etwas angewachsen und enthält neben der Addition auch den unvollendeten Aufruf von ***continue***. Die Ausführung des Kontolloperators bewirkt, dass dieser Stack verworfen wird (insbesondere wird 1 +  vergessen) und durch die Fortsetzung *c* ersetzt wird. Der Rest ist Routine.

$$Eval\ (\delta, N\ 2, [Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$
$$Ret\ (Nat\ 2, [Bin_1\ (E, M, N\ 3); Bin_1\ (E, A, N\ 4)])$$
$$Eval\ (E, N\ 3, [Bin_2\ (Nat\ 2, M); Bin_1\ (E, A, N\ 4)])$$
$$Ret\ (Nat\ 3, [Bin_2\ (Nat\ 2, M); Bin_1\ (E, A, N\ 4)])$$
$$Ret\ (Nat\ 6, [Bin_1\ (E, A, N\ 4)])$$
$$Eval\ (E, N\ 4, [Bin_2\ (Nat\ 6, A)])$$
$$Ret\ (Nat\ 4, [Bin_2\ (Nat\ 6, A)])$$
$$Ret\ (Nat\ 10, [\,])$$

Last thing I remember, I was
Running for the door
I had to find the passage back to the place I was before
'Relax' said the night man,
'We are programmed to receive.
You can check out any time you like,
But you can never leave!'

— Eagles (Glenn Lewis Frey, Don Felder, Donald Hugh Henley), *Hotel California*

Eine Fortsetzung ist einer Funktion nicht unähnlich; ⬬ ∗ 3 + 4 kann als Funktion in dem Platzhalter aufgefasst werden: ***fun*** $x \to x * 3 + 4$. Entsprechend schmeckt ***continue*** nach einem Funktionsaufruf. Kombinieren wir Funktionsabstraktion und ***continue*** können wir die Illusion einer Funktion erzeugen: Ist k eine Fortsetzung, dann ist ***fun*** $x \to$ ***continue*** $k\ x$ eine »normale« Funktion. Dass es sich um eine Illusion handelt, merkt man schnell, wenn man die Funktion aufruft: ***fun*** $x \to$ ***continue*** $k\ x$ ist eine Funktion ohne Wiederkehr, ihren Funktionswert bekommen wir nie zu Gesicht. Vielleicht dämmert es langsam: Mit der Einführung von Kontrolloperatoren verlassen wir die behagliche Welt der mathematischen Funktionen.

Dijkstra mahnt in dem Artikel »Go To Statement Considered Harmful«, die konzeptionelle Lücke zwischen dem statischen Programmtext und dem dynamischen Prozess seiner Auswertung so klein wie möglich zu halten. Die Mathematik macht es vor und treibt es im gewissen Sinne auf die Spitze: Durch ihre Brille ist eine Funktion eine statische Relation zwischen Eingaben und Ausgaben.[18] Der dynamische Prozess, der die Eingaben in die Ausgaben überführt, wird gänzlich ignoriert. (Besonders deutlich wird die Ignoranz, wenn eine Funktion mit ihrem Graphen identifiziert wird.) Im Gegensatz dazu wird in der Informatik das dynamische Wesen einer Funktion betont: Durch ihre Brille ist eine Funktion ein Algorithmus, der präzise beschreibt, wie Ein- in Ausgaben transformiert werden und welche Arbeiten auf diesem Weg zu verrichten sind. Ignoranz ist gemeinhin negativ konnotiert, aber man sollte nicht vergessen, dass sie hilft, Komplexität zu meistern. Um Dijkstras Warnung nachvollziehen zu können, schauen wir uns im Folgenden kurz an, welche weitreichenden Konsequenzen die Einführung der Kontrolloperatoren nach sich zieht, welchen Geist wir aus der Flasche gelassen haben.

Der Ausdruck ***letcc*** k ***in fun*** $v \to$ ***continue*** $k\ v$ fängt die aktuelle Fortsetzung ein und gibt sie unmittelbar als Funktion verkleidet zurück. Wenden wir den Ausdruck auf *sich selbst* an,

(***letcc*** k ***in fun*** $v \to$ ***continue*** $k\ v$) (***letcc*** k ***in fun*** $v \to$ ***continue*** $k\ v$)

erleben wir eine unangenehme Überraschung: Die Auswertung terminiert nicht! Der statische Programmtext ist kurz, aber die Dynamik seiner Ausführung ist unklar. Um eine Idee von dem dynamischen Auswertungsprozess zu bekommen, reichern wir die Funktionsrümpfe mit Ausgabeanweisungen an — ähnlich wie wir das in Abschnitt 3.7 im Kontext des Ratespiels für *player-A* gemacht haben.

```
let yin  = letcc k in fun v → putstring "\n"; continue k v
let yang = letcc k in fun v → putstring "|"  ; continue k v
```

Zur Erinnerung: Die Funktion *putstring* gibt einen String auf dem Bildschirm aus und »;« führt zwei Rechnungen nacheinander aus. Bevor wir einen Testlauf starten können, müssen wir natürlich zunächst unsere abstrakte Maschine erweitern — die Erweiterung ist aber nicht allzu schwer, so dass wir uns die Details sparen.

[18] Siehe Anhang B: Eine Relation $f \subseteq A \times B$ mit der Eigenschaft, dass es zu jedem $x \in A$ genau ein $y \in B$ mit $(x, y) \in f$ gibt, heißt ***Abbildung*** oder ***Funktion***.

```
let Yin  = Letcc ("k", Fun ("v", Seq (Putstring "\n", Continue (Id "k", Id "v"))))
let Yang = Letcc ("k", Fun ("v", Seq (Putstring "|",  Continue (Id "k", Id "v"))))
```

Wenn wir jetzt *yin* auf *yang* anwenden, erleben wir eine faustdicke Überraschung.

```
⋙ eval (App (Yin, Yang))

|
||
|||
||||
|||||
||||||
|||||||
||||||||
|||||||||
…
```

Der nichtterminierende Prozess gibt nacheinander die natürlichen Zahlen in der unären Zahlendarstellung aus — die Zahlendarstellung unserer Urahnen: für jedes erlegte Bison einen Strich! Sehen Sie dem statischen Programmtext diese Dynamik an?

Fortsetzung folgt in Abschnitt 7.3.4.

Zusammenfassung und Anmerkungen

DIY: Zusammenfassung

Die Informatik erschafft Modelle der Wirklichkeit: Statische Aspekte werden durch Typen modelliert, dynamische Aspekte durch Funktionen. Zur Statik: Daten lassen sich mit Hilfe von Records zu einer Einheit zusammenfassen (»… und …«, »sowohl … als auch …«); Varianten repräsentieren alternative Angaben (»entweder … oder …«).

Werte und Typen formen eine Zweiklassengesellschaft, zwei Klassen mit vielen Parallelen: Werte wie Typen können parametrisiert werden; Werte wie Typen dürfen rekursiv definiert werden. Typische Vertreter parametrisierter Typen sind Containertypen wie Listen oder Felder. Polymorphe Funktionen bzw. Werte weichen die Klassengrenzen auf: Funktionen können mit Typen parametrisiert werden und realisieren generische Algorithmen.

↱ hängt ab von →	Wert	Typ
Wert	Funktion	polymorphe Funktion
Typ	—	parametrisierter Typ

Gesprengt werden die Klassengrenzen nicht: Typen dürfen nicht von Werten abhängen — Mini-F# unterstützt keine sogenannten abhängigen Typen (engl. dependent types), ein Feature neuerer, experimenteller Programmiersprachen.

Die Parallelen zwischen den Welten manifestieren sich als Entwurfsmuster. Die Struktur der Daten bestimmt die Struktur der Funktionen, die sie verarbeiten. Als Slogan: Die Funktion folgt stets der Form (engl. function ever follows form).

> *It is the pervading law of all things organic and inorganic, of all things physical and metaphysical, of all things human and all things superhuman, of all true manifestations of the head, of the heart, of the soul, that the life is recognizable in its expression, that form ever follows function.* This is the law.
>
> — Louis H. Sullivan (1856–1924), *The tall office building artistically considered*

calculare
den Wert bestimmen; rechnen; zählen

functio
Verrichtung; Ausführung

fungi
ausüben

Die in den Kapitel 3 und 4 eingeführten Sprachkonstrukte illustrieren das ***funktionale Programmierparadigma***. Wichtige Vertreter funktionaler, werte-orientierter oder applikativer Programmiersprachen sind Clojure, Erlang, F#, Haskell, LISP, OCaml, Racket, Scala, Scheme und Standard ML. Funktionale Programmiersprachen sind »ausdrucksstark«. Ein Problem wird durch einen Ausdruck beschrieben, dessen Auswertung zur Lösung des Problems führt. Die kreative gedankliche Leistung beim Programmieren geht in den Entwurf geeigneten Vokabulars und in die Aufstellung passender Rechenregeln. Im Idealfall besteht das Programm aus vielen, überschaubaren, unabhängigen Einheiten (Typen und Funktionen), die separat gelesen, verstanden, getestet und verifiziert werden können. Der modulare Aufbau wird insbesondere durch zwei Features unterstützt: Funktionale Programmiersprachen sind HOT (*H*igher-*O*rder and *T*yped). Funktionen höherer Ordnung erlauben es, nicht nur von Daten, sondern auch von Algorithmen zu abstrahieren.

5. Algorithmik ⧹ Rechnen mit System

Writing programs needs genius to save the last order or the last millisecond. It is great fun, but it is a young man's game. You start it with great enthusiasm when you first start programming, but after ten years you get a bit bored with it, and then you turn to automatic-programming languages and use them because they enable you to get to the heart of the problem that you want to do, instead of having to concentrate on the mechanics of getting the program going as fast as you possibly can, which is really nothing more than doing a sort of crossword puzzle.

— Christopher Strachey (1916–1975)

In den letzten beiden Kapiteln haben wir den funktionalen Sprachkern von Mini–F# eingeführt. Jetzt machen wir eine Pause vom Sprachentwurf und wenden uns Anwendungen zu. Wir werden einen kleinen Ausflug in die Algorithmik unternehmen, der Lehre vom *systematischen* maschinellen Rechnen.

Wir haben in der Einleitung angesprochen, dass es mit der Existenz von Rechenmaschinen interessant wird, Aufgaben in Rechenaufgaben zu verwandeln, die es von Natur aus nicht sind und die wir mit unserem Verstand auch nie so behandeln würden. Zu einer Problemstellung gilt es, die richtigen Abstraktionen zu finden, sie durch Formeln und Rechengesetze, genannt Datenstrukturen und Algorithmen, so weitgehend zu erfassen, dass wir dem Ergebnis der Rechnung eine Lösung des Problems entnehmen können. Einige Schritte in diese Richtung haben wir bereits unternommen und dabei festgestellt, dass sich die gleiche Problemstellung oft ganz unterschiedlich lösen lässt, so dass die Frage aufkommt, wie wir verschiedene Lösungen miteinander vergleichen können. Welche ist besser, welche schneidet schlechter ab? Bei der Bewertung von Datenstrukturen und Algorithmen spielt allgemein der *Ressourcenverbrauch* eine zentrale Rolle. Wie lang werden die Rechnungen — wieviele Rechenschritte werden benötigt? Wie groß werden die einzelnen Rechenausdrücke — wieviel Platz wird benötigt, um die Rechnung durchzuführen? Werden die Rechnungen auf einem batteriegetriebenen Rechenknecht ausgeführt, wird man sich vielleicht dafür interessieren, den Energieverbrauch zu minimieren. Zu diesem Themen werden Sie sehr viel mehr in der Vorlesung »Algorithmen und Datenstrukturen« erfahren. Gemäß dem Motto »Time is money«, konzentrieren wir uns im Folgenden auf die Ressource »Zeit«, auf die Analyse der Laufzeit von Algorithmen.

Im Gegensatz zum Rechnen ist das Aufstellen von Rechenregeln eine kreative gedankliche Leistung und eine bemerkenswerte dazu. Zur Kreativität gesellen sich aber, wie auch in der Kunst oder im Handwerk, weitere Qualitäten: Erfahrung, Geduld, Ausdauer und die Beherrschung der Werkzeuge. Kreativität lässt sich nur schwer vermitteln; aber wir können Werkzeuge vorstellen und deren Verwendung trainieren. Ein wichtiges Werkzeug für das algorithmische Lösen von Problemen haben wir bereits kennengelernt: *Entwurfsmuster*! Das Peano und das Leibniz Entwurfsmuster haben wir erfolgreich eingesetzt, um Probleme über den natürlichen Zahlen zu lösen. Das Struktur Entwurfsmuster haben wir verwendet, um Funktionen über rekursiv definierten Variantentypen wie zum Beispiel dem Listentyp systematisch zu entwickeln. Zur Erinnerung:

- *Peano Entwurfsmuster:*
  Das Problem für n wird auf das Problem für $n \div 1$ zurückgeführt.

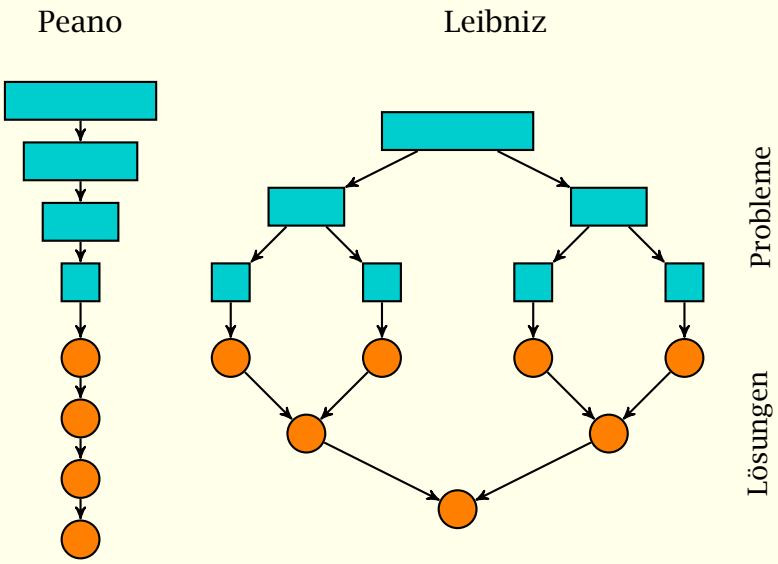


Abbildung 5.1.: Peano und Leibniz Entwurfsmuster.

- *Leibniz Entwurfsmuster:*
  Das Problem für n wird auf das Problem für $n \div 2$ zurückgeführt.

Den Entwurfsmustern ist gemeinsam, dass sie Lösungen für Probleme aus Lösungen für »kleinere« Probleme konstruieren. Daraus lässt sich eine allgemeine Lösungsstrategie, ein allgemeines Prinzip ableiten:

Induktives Problemlösen
Um ein Problem zu lösen, genügt es zu zeigen, dass sich eine Lösung für jede Probleminstanz aus Lösungen kleinerer Probleminstanzen konstruieren lässt.

Mit anderen Worten, es ist nicht nötig, jede Probleminstanz von Grund auf zu lösen. Stattdessen sollte man versuchen, eine Probleminstanz auf kleinere Probleminstanzen zu *reduzieren*. In diesem Sinne lassen sich unsere Entwurfsmuster verallgemeinern:

- *Allgemeines Peano Entwurfsmuster:*
  Ein Problem der Größe n wird auf Probleme der Größe $n \div 1$ zurückgeführt.

- *Allgemeines Leibniz Entwurfsmuster:*
  Ein Problem der Größe n wird auf Probleme der Größe $n \div 2$ zurückgeführt.

Wenn wir einen solchen Ansatz in ein Programm überführen, dann kümmert sich jeweils ein rekursiver Aufruf um die Lösung der Teilprobleme. Abbildung 5.1 illustriert die Vorgehensweise: Beim rekursiven Abstieg wird das Problem sukzessive in Teilprobleme aufgegliedert; sind die Teilprobleme hinreichend einfach, lösen wir sie ad hoc; beim rekursiven Aufstieg werden die Teillösungen zu Gesamtlösungen zusammengeführt. Sowohl die Aufgliederung in Teilprobleme als auch die Zusammenführung von Teillösungen stellt uns oft vor *neue* Aufgaben, die wir sodann auf die gleiche Art und Weise angehen!

Wenn wir Probleminstanzen auf »kleinere« Probleminstanzen zurückführen wollen, müssen wir natürlich überlegen, was die Größe oder die Schwere eines Problems ausmacht. Wie lässt sich der Schwierigkeitsgrad messen? Darauf gibt es keine allgemein gültige Antwort. In der Auseinandersetzung mit einem neuen Problem ist die Festlegung des »Maßes« ein erster wichtiger Schritt.

Im Einzelnen haben wir Folgendes vor. Abschnitt 5.1 zeigt, wie sich die Entwurfsmuster auf das uns schon bekannte Sortierproblem anwenden lassen. Dabei richten wir ein besonderes Augenmerk auf die Analyse der Sortieralgorithmen und überlegen, wie schwierig das Sortierproblem prinzipiell ist. Abschnitt 5.2 widmet sich dem Suchen, einem weiteren klassischen Thema der Algorithmik. Wir vertiefen die Suche in Datenstrukturen und die Suche in »virtuellen Räumen«. Dabei kümmern wir uns insbesondere um die Korrektheit und die Terminierung der Algorithmen. Abschnitt 5.3 erweitert den Blickwinkel und diskutiert, wie man Suchstrukturen konstruiert, modifiziert und traversiert. Aus einer Datenstruktur wird ein abstrakter Datentyp. Abschnitt 5.4 stellt ein weiteres Beispiel für einen abstrakten Datentyp vor: Prioritätswarteschlangen. Abschnitt 5.5 Ein Ausflug in die Welt der Graphen und Graphalgorithmen rundet das Kapitel ab.

5.1. Sortieren

Computer manufacturers of the 1960s estimated that more than 25% of the running time on their computers was spent on sorting, when all their customers were taken into account. In fact, there were many installations in which the task of sorting was responsible for more than half of the computing time. From these statistics we may conclude that either

(i) there are many important applications of sorting, or

(ii) many people sort when they shouldn't, or

(iii) inefficient sorting algorithms have been in common use.

The real truth probably involves all three of these possibilities, but in any event we can see that sorting is worthy of serious study, as a practical matter.

— Donald E. Knuth (1938), *TAOCP 3*

module Algorithmics.Sort

Auch sechzig Jahre später wird das Sortieren von Daten einen nicht unerheblichen Anteil an der gesamten Rechenleistung von Computern ausmachen. Bevor wir uns mit konkreten Sortierverfahren beschäftigen, sollten wir das Sortierproblem zunächst präzise spezifizieren.

Als Eingabe erhalten wir eine Folge von Elementen des gleichen Typs:

$$x_0, x_1, x_2, \ldots, x_{n-1}$$

Die Problemgröße, von der wir vorher gesprochen haben, ist hier die Anzahl der Elemente, also n. Als Ausgabe ist eine Permutation der Eingabe

$$x_{\pi(0)}, x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n-1)}$$

gesucht, so dass

$$x_{\pi(0)} \leqslant x_{\pi(1)} \leqslant x_{\pi(2)} \leqslant \cdots \leqslant x_{\pi(n-1)}$$

Die Abbildung $\pi : \mathbb{N}_n \to \mathbb{N}_n$ ordnet dabei jedem Index i eineindeutig einen Index $\pi(i)$ zu. Mit anderen Worten: Kein Eingabeelement wird vergessen, kein Ausgabeelement erfunden. Da die Eingaben Elemente eines beliebigen Typs sein können, müssen wir weiterhin klären, was »$\leqslant$« bedeutet. Wir setzen folgende Eigenschaften voraus:[1]

1. *reflexiv:* $x \leqslant x$;

[1] Wenn eine Relation total ist, dann ist sie automatisch auch reflexiv: $x \leqslant y$ oder $y \leqslant x$ gilt für beliebige Elemente, somit insbesondere wenn x und y identisch sind.

2. *transitiv:* wenn $x \leqslant y$ und $y \leqslant z$, dann $x \leqslant z$;

3. *total:* $x \leqslant y$ oder $y \leqslant x$.

Diese Eigenschaften definieren eine sogenannte ***totale Quasiordnung*** (engl. total preorder). In Anhang B.4 erfahren Sie mehr zu Ordnungen und Verbänden. Die Ordnung auf den natürlichen Zahlen erfüllt zum Beispiel die geforderten Eigenschaften; die Teilmengenbeziehung erfüllt sie nicht: »⊆« ist zwar reflexiv und transitiv, aber nicht total. Zum Beispiel gilt weder $\{1,2\} \subseteq \{2,3\}$ noch umgekehrt $\{2,3\} \subseteq \{1,2\}$.

Wir verlangen *nicht*, dass die Quasiordnung antisymmetrisch ist: Wenn $x \leqslant y$ und $y \leqslant x$, dann $x = y$. Diese Forderung wäre zu einschränkend: Wenn wir zum Beispiel Personen nach ihrem Alter ordnen, dann gilt nicht, dass es sich bei zwei Personen des gleichen Alters auch um die gleiche Person handeln muss. Eine antisymmetrische Quasiordnung heißt übrigens schlicht und einfach ***Ordnung*** — deswegen spricht man auch von der »Ordnung auf den natürlichen Zahlen«.

In einer totalen Quasiordnung gibt es insgesamt genau *drei* Möglichkeiten, wie zwei Elemente zueinander stehen:

1. sowohl $x \leqslant y$ als auch $y \leqslant x$ gilt (notiert durch $x \sim y$);

2. $x \leqslant y$ gilt, nicht aber $y \leqslant x$ (notiert durch $x < y$); und schließlich

3. $x \leqslant y$ gilt nicht, wohl aber $y \leqslant x$ (notiert durch $x > y$).

Der vierte Fall, weder $x \leqslant y$ noch $y \leqslant x$ gilt, kann nicht auftreten, da die Quasiordnung total ist. Die folgende Tabelle fasst die Fälle noch einmal zusammen.

		$y \leqslant x$ *false*	$y \leqslant x$ *true*
$x \leqslant y$	*false*	—	$x > y$
	true	$x < y$	$x \sim y$

Um Missverständnissen vorzubeugen: Die drei Relationen werden von der Relation »⩽« abgeleitet; sie werden durch die Tabelle definiert. Die Relation »∼« ist eine sogenannte Äquivalenzrelation; »<« und »>« sind sogenannte strikte Ordnungen.

5.1.1. Einfache Sortierverfahren

Wenden wir das verallgemeinerte Peano Entwurfsmuster auf das Sortierproblem an. Um die Problemgröße zu reduzieren, müssen wir ein Element der zu sortierenden Folge zur Seite legen. *Zwei* kanonische Ansätze drängen sich auf: Wir entfernen das erste Element der Eingabe *oder* wir wählen das erste Element der Ausgabe. Zwei Möglichkeiten, zwei Sortierverfahren:

Sortieren durch Einfügen:

- Lege das erste Element zur Seite,
- sortiere die restlichen Elemente,
- *füge* das erste Element in die sortierte Folge *ein*.

Sortieren durch Auswählen:

- *Wähle* das kleinste Element *aus*,
- sortiere die restlichen Elemente,
- setze das kleinste Element vor die sortierte Folge.

Die beiden Verfahren sind im gewissen Sinne »dual« zueinander. Beim Sortieren durch Einfügen ist der erste Schritt einfach und der letzte Schritt aufwändig; beim Sortieren durch Auswählen ist es genau umgekehrt.

Sortieren durch Einfügen Das Verfahren haben wir bereits in Abschnitt 4.2.2 ausführlich besprochen. Die Eingabefolge wird durch eine Liste repräsentiert. Zur Erinnerung:

```
let insertion-sort (⩽) =
  let rec insert k = function
    | [ ]     → [k]
    | x :: xs → if k ⩽ x then k :: x :: xs else x :: insert k xs
  let rec sort = function
    | [ ]     → [ ]
    | x :: xs → insert x (sort xs)
  in sort
```

Die Sortierfunktion ist mit der Quasiordnung »⩽« parametrisiert. (In Abschnitt 4.2.2 haben wir *less-equal* als Bezeichner gewählt, hier verwenden wir einen symbolischen Bezeichner, der den vordefinierten Operator verschattet.)

Ist das Programm korrekt, erfüllt es seine Spezifikation? Wir müssen zeigen, dass die Ausgabe eine Permutation der Eingabe ist. Wenn man den Programmtext genau inspiziert, sieht man, dass kein Eingabeelement vergessen wird und kein Ausgabeelement erfunden wird. Ist die Ausgabe aufsteigend geordnet? Nun, gemäß des Peano Entwurfsmusters erweitert die Hilfsfunktion *insert* eine Teillösung zu einer Gesamtlösung. Mit anderen Worten, wir müssen zeigen, dass, wenn *xs* sortiert ist, dann ist auch *insert k xs* sortiert. Die Korrektheit von *insert* hängt von einer *Vorbedingung* ab. (Wenn die Liste *xs* nicht aufsteigend geordnet ist, lässt sich über das Verhalten von *insert k xs* in der Tat wenig aussagen.) Nach diesen Vorüberlegungen kann man die Korrektheit von *insert* und *sort* mit Hilfe von Induktionsbeweisen nachweisen. Dabei fließt wesentlich die Annahme ein, dass »⩽« sowohl transitiv als auch total ist. (An welchen Stellen?)

Wenden wir uns der Analyse der Laufzeit zu. Sortieren durch Einfügen ist *adaptiv:* »Vorsortierte« Eingaben werden schneller verarbeitet als »unsortierte«. Der beste Fall liegt vor, wenn die Eingabe bereits aufsteigend sortiert ist. In diesem Fall benötigt das Einfügen lediglich einen Vergleich, so dass insgesamt $n-1$ Vergleiche durchgeführt werden. Das ist optimal — schneller kann man nicht sortieren. (Warum?) Der schlechteste Fall liegt vor, wenn *insert* jeweils die gesamte Liste durchlaufen muss, also wenn die Eingabe absteigend sortiert ist.[2] In diesem Fall benötigt das Einfügen $i-1$ Vergleiche, so dass insgesamt $\sum_{i=1}^{n} i-1 = \binom{n}{2} = n \cdot (n-1)/2$ Vergleiche durchgeführt werden. In der Regel interessiert man sich nicht für die präzise Anzahl der Rechenschritte, sondern nur für die Größenordnung, so dass wir festhalten: Die Laufzeit von »Sortieren durch Einfügen« ist im schlechtesten Fall quadratisch.

Sortieren durch Auswählen War vorher die »Lösungserweiterung« aufwändig, so ist es jetzt die »Problemreduktion«. Wir müssen das kleinste Element einer Liste bestimmen; für den rekursiven Aufruf benötigen wir zusätzlich die Liste ohne das kleinste Element. Die Funktion *split-min* erledigt beide Aufgaben in einem Rutsch:

```
split-min : List ⟨'a⟩ → 'a * List ⟨'a⟩
```

Dieser Ansatz führt allerdings noch nicht ganz ans Ziel. Was machen wir im Basisfall, wenn die Eingabeliste leer ist? Es eröffnet sich eine weitere Anwendungsmöglichkeit für den Variantentyp *Option*.

```
split-min : List ⟨'a⟩ → Option ⟨'a * List ⟨'a⟩⟩
```

[2] Wir haben oben das Adjektiv »vorsortierte« in Anführungsstriche gesetzt, da keineswegs klar ist, was genau damit gemeint ist. Man kann mit Fug und Recht behaupten, dass auch eine absteigend geordnete Liste im gewissen Sinne vorsortiert ist.

Das Ergebnis von *split-min* ist ein optionales Paar: Wir erhalten entweder *None* — dann war die Liste leer — oder *Some* (m, ys), wobei m das kleinste Element ist und ys die restlichen Elemente umfasst. Die Definition von *split-min* ergibt sich dann mit dem Struktur Entwurfsmuster für Listen.

```
let selection-sort (⩽) =
  let rec split-min = function
    | [ ]      → None
    | x :: xs → Some (match split-min xs with
                        | None          → (x, xs)
                        | Some (m, ys) → if x ⩽ m then (x, xs) else (m, x :: ys))
  let rec sort xs =
    match split-min xs with
      | None          → [ ]
      | Some (m, ys) → m :: sort ys
  in sort
```

Im Gegensatz dazu folgt die Definition von *sort nicht* dem Struktur Entwurfsmuster: ys ist im Allgemeinen nicht die Restliste von xs.

Ist das Programm korrekt, erfüllt es seine Spezifikation? Aus der obigen Beschreibung von *split-min* lassen sich die Beweispflichten ableiten: Wenn xs nicht leer ist, dann gilt *split-min* xs = *Some* (m, ys), wobei m das kleinste Element von xs ist und ys die restliche Liste. Anderenfalls ist *split-min* xs = *None*. Sind diese Eigenschaften etabliert, folgt die Korrektheit von *sort* auf dem Fuße. Natürlich sollten wir uns noch vergewissern, dass die Ausgabe eine Permutation der Eingabe ist. Eine kurze Inspektion des Programmtextes zeigt wiederum, dass kein Eingabeelement vergessen wird und kein Ausgabeelement erfunden wird.

Wenden wir uns der Analyse der Laufzeit zu. Sortieren durch Auswählen ist im gewissen Sinne »vergesslich« (engl. oblivious): Die Laufzeit hängt nicht von den konkreten Eingabeelementen ab. Das Verfahren benötigt im besten wie im schlechtesten Fall exakt die gleiche Anzahl von Vergleichen. Um jeweils das Minimum zu bestimmen, werden $i - 1$ Vergleiche benötigt. Das ist optimal. (Warum?) Insgesamt werden somit $\sum_{i=1}^{n} i - 1 = \binom{n}{2} = n \cdot (n-1)/2$ Vergleiche getätigt. Kurzum: Die Laufzeit von »Sortieren durch Auswählen« ist ebenfalls quadratisch. Das Attribut »vergesslich« soll andeuten, dass wir bei der Bestimmung des Minimums jeweils von vorne anfangen und keinen Nutzen aus den vorherigen Durchläufen ziehen.

5.1.2. Sortieren durch Mischen

Wenden wir das verallgemeinerte Leibniz Entwurfsmuster auf das Sortierproblem an. Jetzt müssen wir die Problemgröße ungefähr halbieren. Zwei Ansätze bieten sich an:

Sortieren durch Mischen:

- Teile die Eingabefolge in zwei ungefähr gleich große Folgen,
- sortiere jede der Teilfolgen,
- *»mische«* die zwei sortierten Teilfolgen.

(*Sortieren durch Austauschen:*

- Wähle ein »Pivotelement« aus und teile die Eingabeliste in kleinere und größere Elemente,
- sortiere jede der Teilfolgen,
- hänge die beiden sortierten Teilfolgen aneinander.)

Die beiden Verfahren sind im gewissen Sinne »dual« zueinander. Beim Sortieren durch Mischen ist der erste Schritt relativ einfach und der letzte Schritt aufwändig; beim Sortieren durch Austauschen ist es genau umgekehrt. Letzteres Verfahren ist übrigens auch unter dem Namen *Quicksort*

bekannt. Ob Quicksort tatsächlich quick ist, hängt wesentlich von der Wahl des »Pivotelements« ab. Das ist eine Wissenschaft für sich, so dass wir den Ansatz hier nicht weiter verfolgen wollen. (Um die Eingabeliste ungefähr in zwei Teillisten aufzuteilen, wählt man idealerweise den *Median*. Dessen Bestimmung ist aber aufwändig, siehe Abschnitt 5.1.5, so dass man Kompromisse eingeht …)

Beim Sortieren durch Mischen müssen wir die Eingabeliste zunächst in zwei etwa gleich große Listen aufteilen. Das hört sich nach einer »neuen« Aufgabe an. Erfreulicherweise führt das Struktur Entwurfsmuster unmittelbar zum Ziel:

```
// unzip : 'a list → 'a list * 'a list
let rec unzip = function
  | [ ]     → ([ ], [ ])
  | x :: xs → let (xs1, xs2) = unzip xs in (x :: xs2, xs1)
```

Das Verb »unzip« heißt im Englischen »den Reißverschluss von etwas aufmachen« und beschreibt das Verfahren sehr schön: Die Elemente der Eingabeliste werden alternierend den Ergebnislisten zugeschlagen. Der Aufruf *unzip xs* teilt die Liste *xs* somit in die Liste *es* der Elemente an geraden und die Liste *os* der Elemente an ungeraden Positionen. Hat *xs* die Länge n, dann hat *es* die Länge $\lceil n/2 \rceil$ und *os* die Länge $\lfloor n/2 \rfloor$. Mit anderen Worten: Die Teillisten sind entweder gleich lang oder die erste ist um eins länger.

Nach diesen Vorarbeiten lässt sich das Leibniz Entwurfsmuster direkt umsetzen.

```
let merge-sort (⩽) =
  let rec merge = function
    | ([ ], xs) | (xs, [ ]) → xs
    | (x :: xs, y :: ys)    → if x ⩽ y then x :: merge (xs, y :: ys)
                              else  y :: merge (x :: xs, ys)
  let rec sort = function
    | [ ]  → [ ]
    | [x] → [x]
    | xs   → let (xs1, xs2) = unzip xs in merge (sort xs1, sort xs2)
  in sort
```

Die Hilfsfunktion *merge* führt die Teillösungen zu einer Gesamtlösung zusammen: Zwei sortierte Listen werden zu einer sortierten Liste zusammengefügt.[3] Sie hat merkenswerte Eigenschaften: Das Mischen sortierter Listen ist assoziativ mit der leeren Liste als neutralem Element. Letzteres wird durch die Regel $([\,], xs) \mid (xs, [\,]) \to xs$ sehr schön eingefangen. Die Funktion *merge* verallgemeinert *insert*, es gilt: *insert x ys* = *merge* $[x]$ *ys*. Durch die symmetrische Behandlung der Funktionsargumente ist die Implementierung von *merge* eleganter als die von *insert*, obwohl *merge* ein allgemeineres Problem löst.

Die Hilfsfunktion *sort* implementiert die Idee des »divide et impera« (»Teile und Herrsche«, engl. divide and conquer) buchstabengetreu: Die Eingabeliste wird halbiert, beide Teillisten werden sortiert, die Ergebnisse werden zur sortierten Ausgabeliste zusammengeführt. Für die Korrektheit spielt es keine Rolle, dass sich eine Liste nicht immer *exakt* halbieren lässt. Wir müssen nur sicherstellen, dass die Problemgröße tatsächlich reduziert wird: *length* xs_1 < *length xs* und *length* xs_2 < *length xs*. Mit dem Wissen über die Arbeitsweise von *unzip* muss gelten: $\lfloor n/2 \rfloor \leqslant \lceil n/2 \rceil < n$, wobei n die Länge von *xs* ist. Letztere Ungleichung ist aber nur erfüllt für

[3] Die Übersetzung des englischen Begriffs »Mergesort« mit »Sortieren durch Mischen« ist unglücklich. Im Deutschen meint »mischen« oft «etwas in Unordnung bringen«, etwa beim Mischen von Karten. Hier ist das genaue Gegenteil gemeint: *merge* stiftet nicht Unordnung, sondern erhält und vergrößert die Ordnung. Mergesort wird auch mit »Sortieren durch Verschmelzen« übersetzt — das erinnert aber eher an eine innige Liebesbeziehung.

$n \geqslant 2$. Aus diesem Grund behandeln wir zwei Basisfälle: die leere Liste und einelementige Listen — diese sind bereits sortiert.

So wie »Sortieren durch Mischen« das Verfahren »Sortieren durch Einfügen« verallgemeinert, so verallgemeinert sich auch der Nachweis der Korrektheit. Wie im Fall von *insert* hängt die Korrektheit von *merge* von einer Vorbedingung ab:

> Wenn *list1* und *list2* sortiert sind, dann ist auch *merge* (*list1*, *list2*) sortiert.

Versuchen wir uns an einem Induktionsbeweis.

Fall *list1* = [ ] **oder** *list2* = [ ]**:** Als Ergebnis wird die jeweils andere Liste zurückgegeben. Diese ist gemäß der Vorbedingung bereits sortiert.

Fall *list1* = $x :: xs$ **und** *list2* = $y :: ys$**:** Aufgrund der Vorbedingung wissen wir, dass x das kleinste Element von $x :: xs$ ist und entsprechend y das kleinste Element von $y :: ys$. Wenn $x \leqslant y$ gilt (im ***then***-Zweig), dann muss x aufgrund der Transitivität von »$\leqslant$« das Minimum aller Elemente sein. Anderenfalls gilt $y < x$ (im ***else***-Zweig), da »$\leqslant$« total ist. In diesem Fall ist y das Minimum und somit notwendigerweise das Kopfelement der Ergebnisliste. Wenn $x :: xs$ und $y :: ys$ sortiert sind, dann sind es auch xs und ys, so dass wir die Induktionsannahme anwenden können. Damit ist garantiert, dass auch die Restliste *merge* $(xs, y :: ys)$ bzw. *merge* $(x :: xs, ys)$ sortiert ist. Was zu beweisen war.

Wenden wir uns der Analyse der Laufzeit zu. Die schematische Darstellung des Leibniz Entwurfsmusters in Abbildung 5.1 legt die Vorgehensweise nah. Wir müssen uns überlegen, wie tief der »Rekursionsbaum« ist und wie aufwändig die einzelnen Kästchen sind, die das Zerteilen der Probleme und das Zusammenführen der Lösungen symbolisieren. Wir können uns das Leben vereinfachen, wenn wir nicht jeden Schritt isoliert betrachten, sondern den Gesamtaufwand pro »*Rekursionsebene*«, das heißt alle Kästchen auf einer horizontalen Linie zusammenfassen. Der Gesamtaufwand ergibt sich dann als Produkt der Rekursionstiefe und des Aufwands pro Rekursionsebene.

Da wir die Problemgröße wiederholt halbieren, ist die Rekursionstiefe durch den binären Logarithmus gegeben: $\lg n$. Die Laufzeit von *unzip* ist proportional zur Eingabegröße; die Laufzeit von *merge* ist proportional zur Ausgabegröße. Da die Gesamtzahl der Elemente pro Rekursionsebene stets gleich (!), ist der Aufwand pro Ebene somit linear: n. Die Laufzeit von *merge-sort* beträgt entsprechend $n \lg n$. Das Produkt lässt sich als Fläche eines Rechtecks deuten, siehe Abbildung 5.2. Die folgende Tabelle zeigt, dass Programme mit einer linear-logarithmischen Laufzeit einen erheblichen Geschwindigkeitsvorteil gegenüber Programmen mit quadratischer Laufzeit haben.

n	$\lg n$	$n \lg n$	n^2
100	$\approx 6,6$	≈ 660	10.000
1.000	$\approx 10,0$	≈ 10.000	1.000.000
10.000	$\approx 13,3$	≈ 133.000	100.000.000
100.000	$\approx 16,6$	$\approx 1.660.000$	10.000.000.000
1.000.000	$\approx 20,0$	$\approx 20.000.000$	1.000.000.000.000

Für hinreichend große n ist Sortieren durch Mischen somit wesentlich schneller als Sortieren durch Einfügen oder Auswählen.

5.1.3. Komplexität des Sortierproblems

Sortieren durch Mischen hat eine linear-logarithmische Laufzeit. Können wir die Laufzeit weiter verbessern? Lässt sich eine Folge von Elementen in linearer oder gar in logarithmischer Zeit sortieren? Man überlegt sich leicht, dass eine sublineare Laufzeit unmöglich ist. Um nur das Minimum

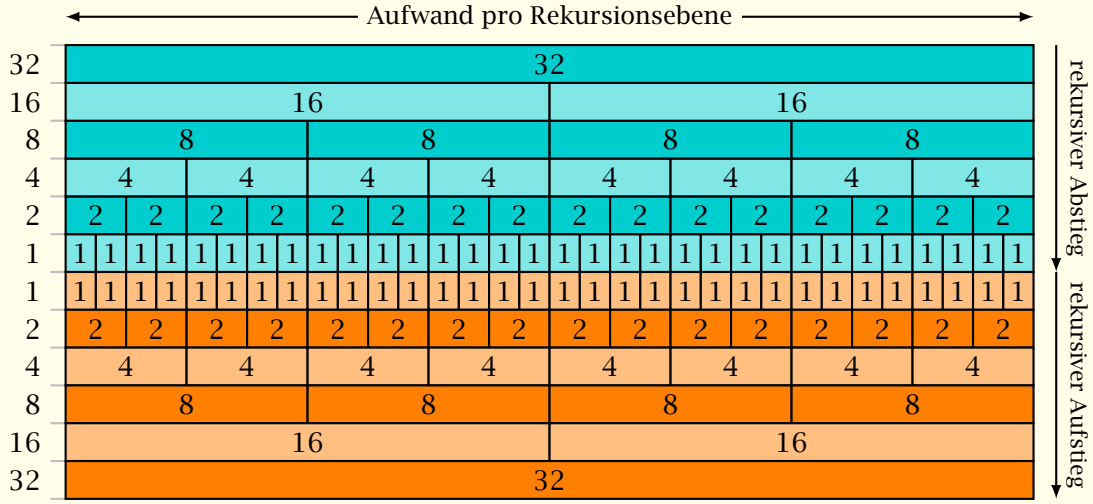


Abbildung 5.2.: Laufzeit von Mergesort.

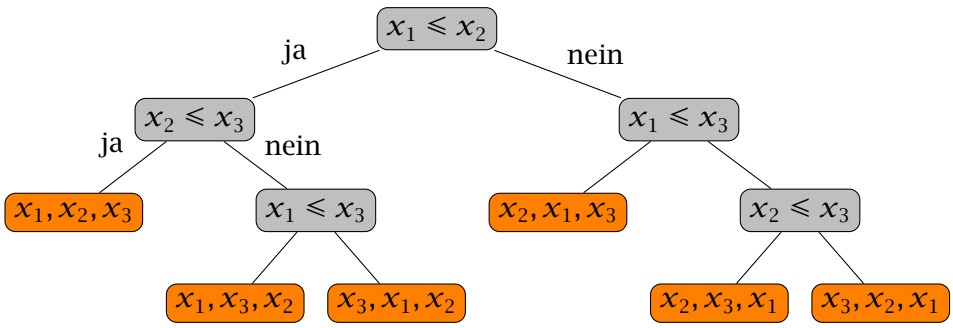
zu bestimmen, müssen wir jedes Element der Eingabe berücksichtigen. Das Sortieren der Eingabe benötigt somit mindestens eine lineare Anzahl von Schritten. Diese Beobachtung lässt sich noch verschärfen. Dazu ist es hilfreich, sich noch einmal die zentrale Annahme ins Gedächtnis zu rufen.

Wir setzen voraus, dass eine Quasiordnung gegeben ist, die der Sortierfunktion als Parameter mit auf den Weg gegeben wird.

$$sort : (\text{'}a \to \text{'}a \to Bool) \to (\text{'}a\ list \to \text{'}a\ list)$$

Die Quasiordnung ist für die Sortierfunktion eine »black box«, ein Orakel. Um Informationen über die relative Anordnung von Elementen zu gewinnen, kann lediglich das Orakel befragt werden, der Funktionsparameter auf zwei Elemente angewendet werden. Da die Sortierfunktion einen polymorphen Typ hat bzw. haben soll, kennen wir noch nicht einmal den konkreten Typ der zu sortierenden Elemente: Sind es natürliche Zahlen, Personendaten oder Musikstücke?

Jedes Sortierprogramm wird wiederholt das Orakel befragen und aus den jeweiligen Antworten seine Rückschlüsse ziehen. Wenn wir uns nur auf die Befragung des Orakels konzentrieren und alle sonstigen buchhalterischen Aktivitäten unter den Tisch fallen lassen, können wir ein Programm durch einen sogenannten ***Entscheidungsbaum*** repräsentieren. Hier ist ein Entscheidungsbaum, um die Folge x_1, x_2, x_3 zu sortieren:



Das repräsentierte Programm testet zunächst ob $x_1 \leqslant x_2$. Ist das der Fall, wird $x_2 \leqslant x_3$ geprüft. Gilt auch dies, lässt sich schließen, dass die Eingabe x_1, x_2, x_3 bereits sortiert ist. Ist hingegen

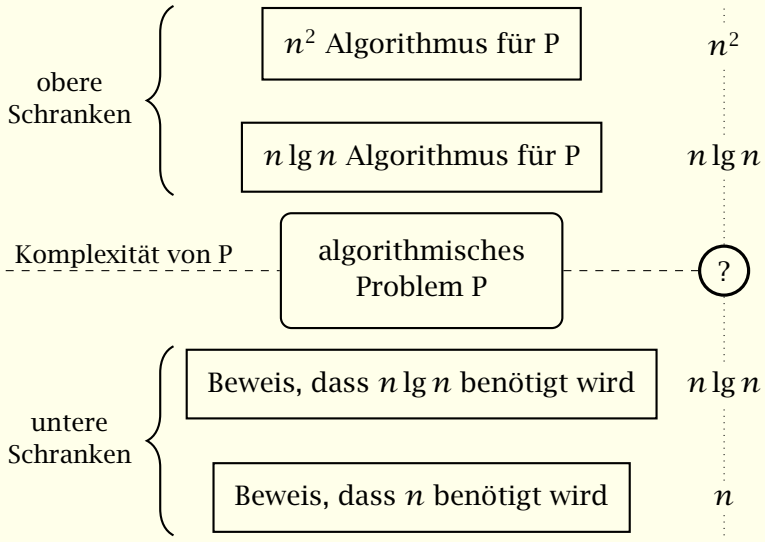


Abbildung 5.3.: Die inhärente Komplexität eines algorithmischen Problems.

$x_2 > x_3$, dann erfolgt ein weiterer Test: Ist $x_1 \leqslant x_3$, dann ist x_1, x_3, x_2 die gesuchte sortierte Ausgabefolge; anderenfalls x_3, x_1, x_2. Und so weiter …

Ein konkreter Lauf des Sortierprogramms, eine konkrete Rechnung korrespondiert zu einem Pfad von der »Wurzel« des Entscheidungsbaums zu einem Blatt, der sortierten Permutation der Eingabe. Drei Elemente lassen sich auf $3! = 6$ Arten anordnen, entsprechend hat der Entscheidungsbaum 6 Blätter. Die maximale Laufzeit des Sortierprogramms entspricht der Länge des längsten Pfades, der sogenannten ***Höhe*** des Entscheidungsbaums. In unserem Beispiel ist die Höhe 3, wir müssen also das Orakel maximal dreimal befragen. Kommen wir auch mit maximal zwei Befragungen aus? Nein! Ein Entscheidungsbaum der Höhe 2 hat höchstens 4 Blätter, wir müssen aber 6 Fälle unterscheiden. Wir halten fest: Mit Hilfe von Entscheidungsbäumen können wir Aussagen über alle denkbaren Sortierprogramme treffen — das sind unendlich (!) viele; neben den naheliegenden, geschickten Programmen gibt es ja auch viele, viele ungeschickte.

Diese Beobachtungen lassen sich auf eine beliebige Anzahl von zu sortierenden Elementen verallgemeinern. Ein Entscheidungsbaum, der n Elemente sortiert, muss notwendigerweise $n!$ Blätter besitzen. Man kann zeigen, dass die Höhe eines solchen Entscheidungsbaums mindestens $n \lg n$ ist (von der Größenordnung, nicht exakt). Mit anderen Worten, jedes Sortierverfahren, *das auf dem Vergleichen von Elementen basiert*, benötigt im schlechtesten Fall mindestens $n \lg n$ Vergleiche. Da wir uns bereits ein Verfahren überlegt haben, das im schlechtesten Fall höchstens $n \lg n$ Vergleiche benötigt, haben wir die ***inhärente Komplexität*** des Sortierproblems ermittelt: $n \lg n$. Damit ist Sortieren durch Mischen ein ***optimales*** Sortierverfahren — bzw. genauer ein ***asymptotisch optimales*** Verfahren, da wir nicht die Anzahl von Vergleichen auf Punkt und Komma bestimmt haben, sondern nur die ungefähre Größenordnung.

Wenn wir den Typ der zu sortierenden Elemente und die zugrundeliegende Quasiordnung kennen, dann können wir tatsächlich schneller sortieren. Ist der Typ zum Beispiel *Unit*, können wir in konstanter Zeit sortieren; ist der Typ *Bool*, dann benötigen wir höchstens lineare Zeit. (Warum?)

Abbildung 5.3 fasst die Diskussion noch einmal zusammen. Um die inhärente Komplexität eines algorithmischen Problems zu bestimmen, kreisen wir das Problem von zwei Seiten ein. Wir überlegen uns Programme, die das Problem lösen und somit obere Schranken für die Laufzeit setzen. Für das Sortierproblem haben wir erst quadratische und dann ein linear-logarithmisches Verfahren entwickelt. Schwieriger ist es, untere Schranken zu setzen, da wir Aussagen über alle

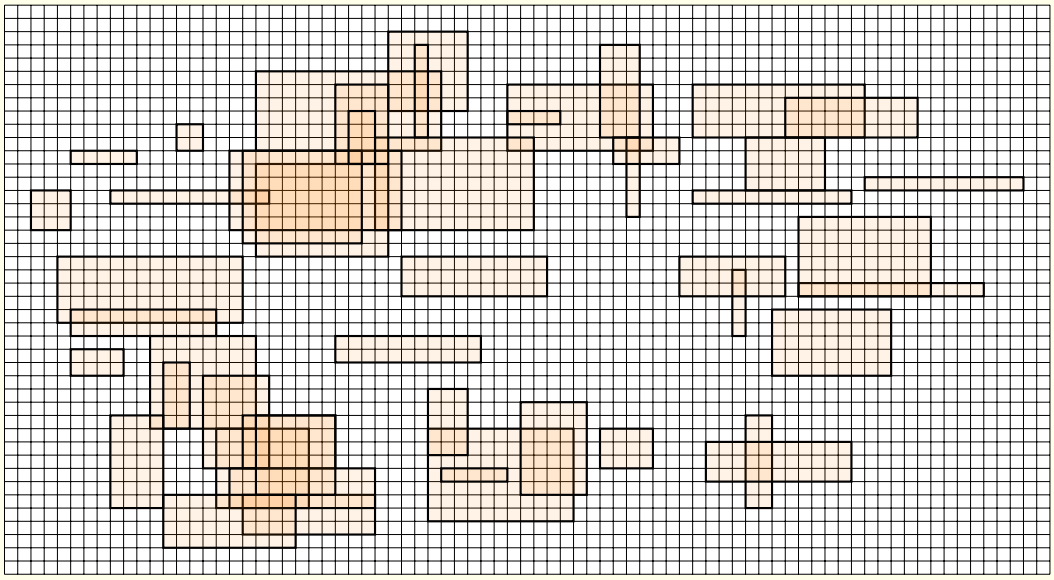


Abbildung 5.4.: Campus der RPTU Kaiserslautern-Landau.

möglichen Programme machen müssen. Für das Sortierproblem lässt sich einfach argumentieren, dass eine lineare Laufzeit notwendig ist. Mit Hilfe eines informationstheoretischen Arguments haben wir eine linear-logarithmische Schranke hergeleitet. Fallen die obere und die untere Schranke zusammen, ist das Problem durchdrungen. Dann wissen wir, wie schwierig es ist, das Problem zu lösen. Das ist der Idealfall — im Laufe des Studiums werden Ihnen viele Probleme begegnen, deren Komplexität nicht bekannt ist, wo die beste untere und die beste obere Schranke weit auseinanderklaffen. (Treiben Sie die Forschung auf diesem Gebiet entscheidend voran, können Sie reich und berühmt werden, siehe http://www.claymath.org/millennium-problems/p-vs-np-problem.)

5.1.4. Anwendung: Bebaute Fläche

Abbildung 5.4 zeigt ein Luftbild des neuen Campus der RPTU Kaiserslautern-Landau. Die schematische Darstellung ist das Ergebnis eines schon mehrfach angesprochenen Abstraktionsprozesses: Gebäude und Gebäudeteile werden dabei durch an den Achsen ausgerichtete Rechtecke repräsentiert. Um zu überprüfen, ob der Campus den neuesten Bestimmungen zur »Beschränkung der Oberflächenversiegelung« genügt, muss die gesamte bebaute bzw. überbaute Fläche berechnet werden.

In Abschnitt 4.1.3 haben wir uns bereits mit den beiden einfachsten, nicht-trivialen Probleminstanzen beschäftigt und die Gesamtfläche von zwei bzw. drei Rechtecken bestimmt. Jetzt wollen wir das Problem in voller Allgemeinheit angehen und die Gesamtfläche von n Rechtecken ausrechnen bzw. ausrechnen lassen.

Rufen wir uns ins Gedächtnis, wie wir das Problem für $n = 2$ bzw. $n = 3$ angegangen sind. Die Programme in Abschnitt 4.1.3 fußen auf dem Prinzip der Ein- und Ausschließung, siehe Abbildung 4.3. Leider skaliert dieser Ansatz nicht: Die Formel für die Gesamtfläche benötigt die Größen sämtlicher Schnittflächen. Das sind viele, zu viele, wenn n hinreichend groß ist: Sind n Flächen gegeben, dann gibt es insgesamt 2^n mögliche Schnitte — jede Fläche kann an einem Schnitt beteiligt sein oder auch nicht. (Die Programme *area2* und *area3* enthalten tatsächlich $2^2 - 1 = 3$ bzw. $2^3 - 1 = 7$ Summanden, da der »leere Schnitt«, bei dem keine Fläche beteiligt ist, nicht benötigt

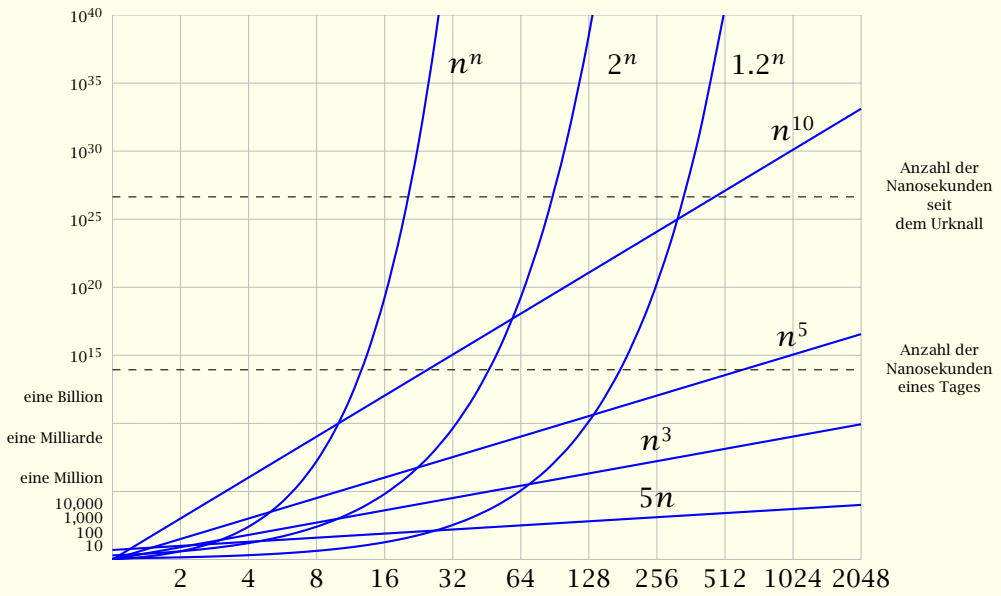


Abbildung 5.5.: Wachstum verschiedener Funktionen (logarithmische Skalen).

wird.) Abbildung 5.5 illustriert, warum es praktisch nicht möglich ist, 2^n Teilprobleme zu lösen: Wenn wir annehmen, dass wir für die Lösung eines Teilproblems eine Nanosekunde benötigen ($1\,ns = 0{,}000\,000\,001\,s$), dann brauchen wir mehr als einen Tag, um 47 Flächen zu bearbeiten; verdoppeln wir deren Anzahl, dann reicht selbst die gesamt Zeit seit dem Urknall nicht!

Das Prinzip der Ein- und Ausschließung gilt für beliebige Flächen. Nun sind Rechtecke, deren Kanten parallel zu den Achsen verlaufen, sehr spezielle, sehr einfache Flächen. So ist es unmöglich, mit n Rechtecken 2^n unterschiedliche Schnittflächen zu konstruieren — Abbildung 4.3 zeigt, dass es mit 4 Rechtecken noch klappt, mit 5 Rechtecken lassen sich höchstens 28 Flächen konstruieren (das ist eine Vermutung). Allgemein ist die Anzahl der Schnittflächen durch $(2 \cdot n + 1)^2$ nach oben begrenzt. (Wenn wir die Kanten jedes Rechtecks ins Unendliche verlängern, dann wird die Ebene in maximal $2 \cdot n + 1$ horizontale Abschnitte und in ebenso viele vertikale Abschnitte unterteilt.) Es besteht also die berechtigte Hoffnung, dass sich das Problem effizienter lösen lässt.

Die Gesamtfläche ließe sich einfach bestimmen, wenn wir davon ausgehen könnten, dass die Rechtecke paarweise disjunkt sind. Eine vielleicht naheliegende Idee ist, genau dafür zu sorgen, indem wir Überlappungen durch Aufteilung von Rechtecken eliminieren — natürlich ohne dabei die Gesamtfläche zu verändern. Zum Beispiel könnten wir den Campus durch vertikale Streifen repräsentieren, siehe Abbildung 5.6, oder alternativ durch horizontale Streifen, siehe Abbildung 5.7. Mit anderen Worten, wir streben einen ***Repräsentationswechsel*** an: Eine Menge von Rechtecken wird durch eine Menge disjunkter Streifen repräsentiert, wobei ein vertikaler Streifen durch *ein* x-Intervall und *eine Menge* von disjunkten y-Intervallen gegeben ist, siehe Abbildung 5.8. Das 2-dimensionale Problem lässt sich durch den Repräsentationswechsel auf seine 1-dimensionale Variante zurückführen: die Gesamtlänge einer Menge von Intervallen zu bestimmen. Wenden wir uns dieser Aufgabe als Erstes zu.

Intervalle Wie in Abschnitt 4.1.3 repräsentieren wir ein Intervall durch die beiden Intervallgrenzen.

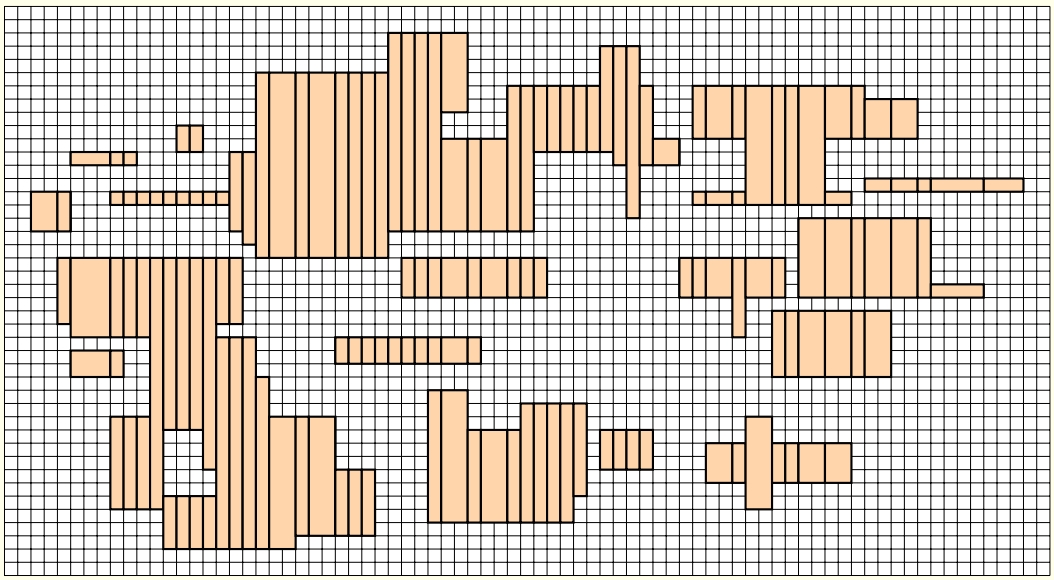


Abbildung 5.6.: Repräsentation des Campus aus Abbildung 5.4 durch vertikale Streifen.

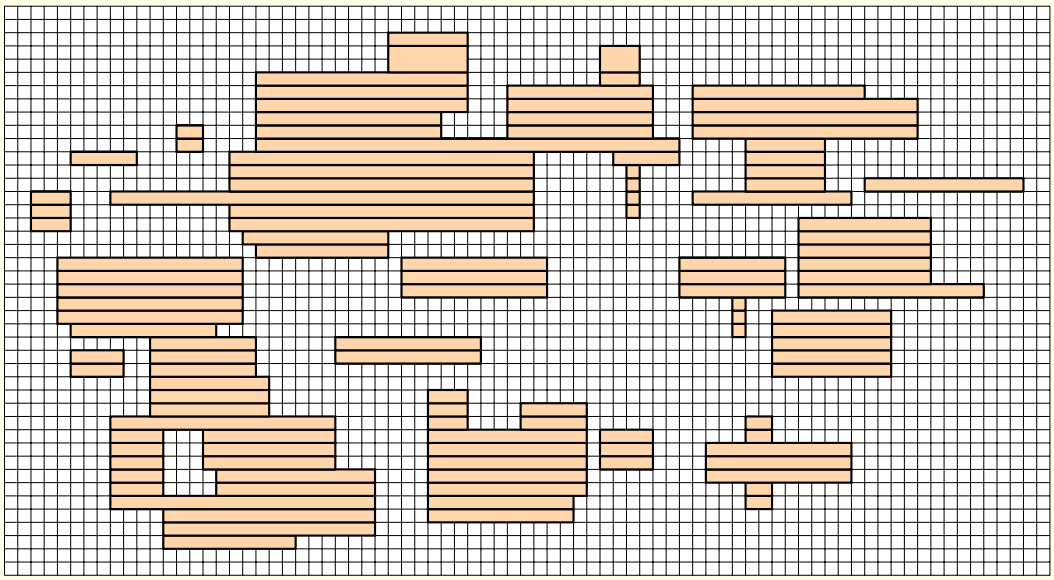


Abbildung 5.7.: Repräsentation des Campus aus Abbildung 5.4 durch horizontale Streifen

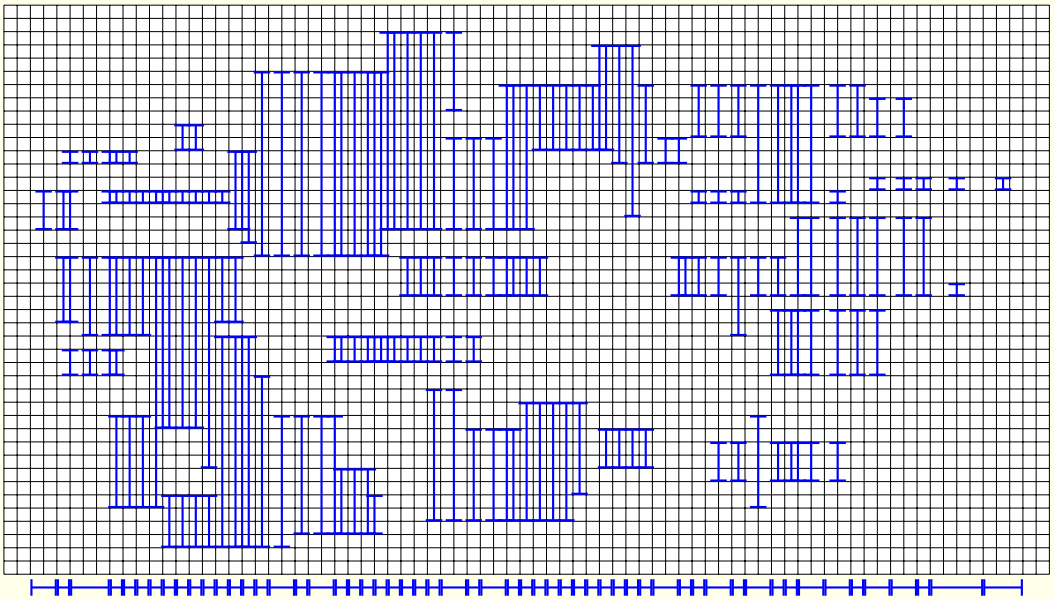


Abbildung 5.8.: x-Intervalle mit assoziierten Listen von y-Intervallen.

```
type Interval = { lo : Int; hi : Int }                    // low und high
module I =
  let length (i : Interval) = max 0 (i.hi − i.lo)         // »monus«
  let union (i : Interval, j : Interval) =
    { lo = min i.lo j.lo; hi = max i.hi j.hi }
```

Das lokale Modul *I* dient dem Zweck, Namenskollisionen zu vermeiden. (In Abschnitt 4.1.3 haben wir auf Tricks wie unterschiedliche Groß- und Kleinschreibung zurückgegriffen.) Die Funktion *union* (i, j) bestimmt das kleinste Intervall, das die Intervalle i und j enthält. Sie implementiert die mengentheoretische Vereinigungen der Punktmengen genau dann, wenn sich die Intervalle überlappen.

Um die Gesamtlänge einer Liste von Intervallen zu berechnen, nehmen wir wie schon angedacht einen ***Repräsentationswechsel*** vor. Wir überführen die gegebene Liste in eine Liste *disjunkter* Intervalle. Um diese Eigenschaft einfach sicherstellen zu können, vereinbaren wir, dass die Listen im folgenden Sinne *geordnet* sind: (1) für jedes in der Liste enthaltene Intervall i gilt $i.lo < i.hi$ — das Intervall ist nicht leer; (2) für zwei aufeinanderfolgende Intervalle i und j gilt $i.hi < j.lo$ — die Intervalle überschneiden sich nicht, sie berühren sich nicht einmal. Mit anderen Worten, die Intervallgrenzen sind von links nach rechts gelesen streng aufsteigend angeordnet.

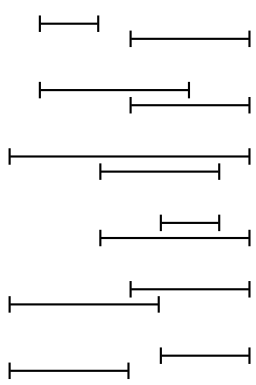
Um den Repräsentationswechsel zu implementieren, verwenden wir das Leibniz Entwurfsmuster (»Teile und Herrsche«, engl. divide and conquer). Ähnlich wie beim Sortieren durch Mischen, müssen wir im Wesentlichen eine Funktion schreiben, die zwei geordnete Intervalllisten vereinigt.

```
union : Interval list * Interval list → Interval list
```

Wir nehmen an, dass die beiden Argumente geordnet sind und erwarten dies auch für das Ergebnis. Unsere Annahmen und Erwartungen werden leider nicht im Typ von *union* reflektiert. Das Typsystem stellt nur sicher, dass die Argumente und das Ergebnis Listen von Intervallen sind.

Das Rekursionsmuster von *union* entspricht im Wesentlichen dem von *merge*: wir betrachten jeweils die beiden ersten Listenelemente und rekurrieren über die Restlisten. Lediglich die

Fallunterscheidung ist etwas umfangreicher, da die Listenelemente nicht Zahlen sind, sondern Intervalle, Paare von Zahlen. Wir haben in Abschnitt 3.3 bereits diskutiert, dass zwei Intervalle, *i* und *j*, auf sechs mögliche Art und Weisen zueinander liegen können.



setzte *i* voran	$i :: union\ (is, j :: js)$
erweitere *j* um *i*	$union\ (is, I.union\ (i, j) :: js)$
ignoriere *j*	$union\ (i :: is, js)$
ignoriere *i*	$union\ (is, j :: js)$
erweitere *i* um *j*	$union\ (I.union\ (i, j) :: is, js)$
setzte *j* voran	$j :: union\ (i :: is, js)$

Zu jedem Fall erhalten wir einen symmetrischen Fall, indem wir die Rollen von *i* und *j* vertauschen. Im Kern müssen wir somit drei Situationen unterscheiden: (1) ein Intervall liegt vor dem anderen; (2) die Intervalle überlappen sich teilweise; (3) ein Intervall liegt vollständig in dem anderen. Im ersten Fall setzen wir das weiter links liegende Intervall der Ergebnisliste voran; im zweiten Fall vereinigen wir die Intervalle; im dritten Fall verwerfen wir das eingeschlossene Intervall.

```
module Is =
  // union : Interval list * Interval list → Interval list
  let rec union = function
    | ([], is) | (is, [])                    → is
    | (i :: is, j :: js) when i.hi < j.lo    → i :: union (is, j :: js)
    | (i :: is, j :: js) when j.hi < i.lo    → j :: union (i :: is, js)
    | (i :: is, j :: js) when i.lo < j.lo && i.hi < j.hi   → union (is, I.union (i, j) :: js)
    | (i :: is, j :: js) when i.lo ⩽ j.lo && i.hi ⩾ j.hi → union (i :: is, js)
    | (i :: is, j :: js) when i.lo ⩾ j.lo && i.hi ⩽ j.hi → union (is, j :: js)
    | (i :: is, j :: js) when i.lo > j.lo && i.hi > j.hi   → union (I.union (i, j) :: is, js)
```

Das Schlüsselwort ***when*** verbindet ein Muster mit einem Booleschen Ausdruck und erlaubt so, die verschiedenen Fälle sehr direkt und übersichtlich in Programmcode zu überführen. Wie beim Musterabgleich üblich, werden die Bedingungen von oben nach unten abgearbeitet. Sind zum Beispiel die ersten drei Bedingungen nicht zutreffend, so wissen wir, dass die Listen nicht leer sind und sowohl $i.hi \geqslant j.lo$ als auch $j.hi \geqslant i.lo$ gilt.

Nach diesen Vorarbeiten ist die Implementierung des Repräsentationswechslers *interval* Routine — so wie die Funktion *union* zu *merge* korrespondiert, so korrespondiert *intervals* zu *merge-sort* (die Funktion *intervals* wird wie union in dem lokalen Modul *Is* definiert).

```
module Is =
  ⋮
  // intervals : Interval list → Interval list
  let rec intervals = function
    | [] → []
    | [i] → [i]
    | is  → let (is1, is2) = unzip is
            union (intervals is1, intervals is2)
```

Auch hier spiegelt sich der Repräsentationswechsel nicht im Typ wider; *interval* bildet tatsächlich eine beliebige Liste von Intervallen auf eine geordnete Liste ab. Da sichergestellt ist, dass die

Intervalle disjunkt sind, ergibt sich sodann die gewünschte Gesamtlänge als Summe der Einzellängen.

```
module Is =
  ⋮
  let total-length = sum-by I.length
```

Die Lösung für das Problem der Berechnung der Gesamtlänge ist somit durch die Funktionskomposition $intervals \gg total\text{-}length : Interval\ list \to Int$ gegeben.

Extrahieren wir alle x-Intervalle bzw. alle y-Intervalle aus der Rechteckliste, die den Campus repräsentiert,

```
⋙ Is.intervals [for r in campus → r.x]
[{lo = 2; hi = 77}]
⋙ Is.intervals [for r in campus → r.y]
[{lo = 2; hi = 41}]
```

erkennen wir, dass die Gebäude »dicht« liegen. Blicken wir in Richtung der Achsen auf das Gelände, sehen wir jeweils einen zusammenhängenden Wall von Wänden. (Letztere Aussage interpretiert die Rechenergebnisse. Aus Sicht des Rechners ist das Ergebnis jeweils eine einelementige Liste, aus Sicht des Stadtplaners vielleicht ein Hinweis auf eine zu dichte Bebauung.) Das Argument von *intervals* ist übrigens eine sogenannte ***Listenbeschreibung*** — eine ähnliche Syntax haben wir auch für die Konstruktion von Arrays verwendet. Ist xs die Liste $[x_1; \ldots; x_n]$ dann bezeichnet $[\textbf{for}\ x\ \textbf{in}\ xs \to f\ x]$ die Liste $[f\ x_1; \ldots; f\ x_n]$; die Funktion f wird auf jedes Element der Liste xs angewendet.

Nach diesen Vorarbeiten sind wir bestens gerüstet, um unser ursprüngliches Problem zu lösen.

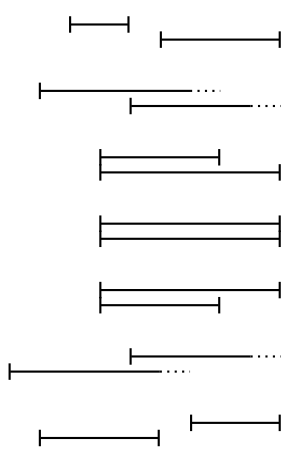
Intervalle von Intervallen Erinnern wir uns an die Idee des Repräsentationswechsels: Wir wollen eine Rechteckmenge bzw. eine Liste von Rechtecken durch eine Liste von vertikalen Streifen repräsentieren, wobei ein vertikaler Streifen durch ein x-Intervall und eine Liste von y-Intervallen gegeben ist. Der Repräsentationswechsler hat somit den Typ:

$$rectangles : Rectangle\ list \to (Interval * Interval\ list)\ list$$

Um sicherzustellen, dass die resultierenden Rechtecke disjunkt sind, muss die äußere Liste bezüglich der x-Intervalle geordnet sein und zusätzlich müssen alle inneren Listen, die Listen der y-Intervallen, geordnet sein. Im Detail verlangen wir für die äußere Liste: (1) für jeden in der Liste enthaltenen Eintrag (i, a) gilt $i.lo < i.hi$ — das Intervall ist nicht leer; (2) für zwei aufeinanderfolgende Einträge (i, a) und (j, b) gilt $i.hi \leqslant j.lo$ — die Intervalle überschneiden sich nicht, sie dürfen sich aber berühren. Wir sind etwas »großzügiger« im Vergleich zu den inneren Listen: Dort sind Berührungen nicht zugelassen (zwei sich berührende Intervalle können ja stets vereinigt werden), hier sehr wohl (eine Vereinigung wäre möglich, aber nur wenn beiden x-Intervallen exakt die gleichen y-Intervalle zugeordnet sind).

Da die Invarianten der Datenstrukturen etwas unterschiedlich sind, müssen wir bei der Vereinigung von x-Intervallen insgesamt sieben Fälle unterscheiden (statt sechs Fälle wie bei den

y-Intervallen).



setzte i voran	$(i, a) :: union\ (is, (j, b) :: js)$
teile i	$(il, a) :: union\ ((ir, a) :: is, (j, b) :: js)$
vereinige Präfix	$(i, a \mathbin{@} b) :: union\ (is, (jr, b) :: js)$
vereinige i und j	$(i, a \mathbin{@} b) :: union\ (is, js)$
vereinige Präfix	$(j, a \mathbin{@} b) :: union\ ((ir, a) :: is, js)$
teile j	$(jl, b) :: union\ ((i, a) :: is, (jr, b) :: js)$
setzte j voran	$(j, b) :: union\ ((i, a) :: is, js)$

Zu jedem Fall erhalten wir einen symmetrischen Fall, indem wir die Rollen von i und j vertauschen. Da der vierte Fall symmetrisch zu sich selbst ist, kommen wir auf insgesamt sieben Fälle. Im Kern müssen wir vier Situationen unterscheiden: (1) ein Intervall liegt vor dem anderen; (2) ein Intervall ragt in das andere hinein; (3) ein Intervall ist ein Präfix des anderen; (4) die beiden Intervalle sind identisch. Im ersten Fall setzen wir das weiter links liegende Intervall der Ergebnisliste voran; im zweiten Fall teilen wir ein Intervall auf; im dritten Fall vereinigen wir zusätzlich die assoziierten y-Intervalle; im vierten Fall müssen wir nicht teilen, sondern nur die assoziierten y-Intervalle vereinigen.

Die Hilfsfunktion *split-at* trennt ein Intervall an einer gegebenen Stelle auf.

```
let split-at x i = ({ lo = i.lo; hi = x }, { lo = x; hi = i.hi })
```

Wir stellen beim Aufruf stets sicher, dass $i.lo < x < i.hi$, so dass ein nicht-leeres Intervall in zwei nicht-leere Intervalle überführt wird.

Die Funktion *union* implementiert die oben detaillierte Fallunterscheidung. Die Fälle sind etwas umgeordnet worden, um die Bedingungen einfacher formulieren zu können.

```
// union : (Interval * 'a list) list * (Interval * 'a list) list → (Interval * 'a list) list
let rec union = function
  | ([], is) | (is, [])                          → is
  | ((i, a) :: is, (j, b) :: js) when i.hi ⩽ j.lo → (i, a) :: union (is, (j, b) :: js)
  | ((i, a) :: is, (j, b) :: js) when j.hi ⩽ i.lo → (j, b) :: union ((i, a) :: is, js)
  | ((i, a) :: is, (j, b) :: js) when i.lo <  j.lo → let (il, ir) = split-at j.lo i
                                                    (il, a) :: union ((ir, a) :: is, (j, b) :: js)
  | ((i, a) :: is, (j, b) :: js) when i.lo >  j.lo → let (jl, jr) = split-at i.lo j
                                                    (jl, b) :: union ((i, a) :: is, (jr, b) :: js)
  | ((i, a) :: is, (j, b) :: js) when i.hi <  j.hi → let (jl, jr) = split-at i.hi j
                                                    (i, a @ b) :: union (is, (jr, b) :: js)
  | ((i, a) :: is, (j, b) :: js) when i.hi = j.hi  → (i, a @ b) :: union (is, js)
  | ((i, a) :: is, (j, b) :: js) when i.hi >  j.hi → let (il, ir) = split-at j.hi i
                                                    (j, a @ b) :: union ((ir, a) :: is, js)
```

Der Typ von *union* ist allgemeiner als erwartet: Die den x-Intervallen zugeordneten Werte müssen lediglich Listen sein, nicht notwendigerweise Listen von y-Intervallen. Das liegt daran, dass wir im Fall von Überlappungen die assoziierten Werte einfach konkatenieren — das klappt für Listen beliebigen Grundtyps.

Der Repräsentationswechsler *rectangles* etabliert die Invarianten getrennt für jede Dimension. Im ersten Schritt, implementiert durch die Hilfsfunktion *union-all*, wird die Liste der Rechtecke in eine geordnete Liste von x-Intervallen überführt. Im zweiten Schritt wird für jedes x-Intervall die Liste der assoziierten y-Intervalle »sortiert«, implementiert durch die Funktion *intervals*.

```
let rec union-all = function
  | [ ]  → [ ]
  | [r] → [(r.x, [r.y])]
  | rs   → let (rs1, rs2) = unzip rs
           union (union-all rs1, union-all rs2)

// rectangles : Rectangle list → (Interval * Interval list) list
let rectangles rs = [for (i, js) in union-all rs → (i, Is.intervals js)]
```

Jetzt sind wir fast am Ziel. Da sowohl die x-Intervalle als auch die y-Intervalle disjunkt sind, ergibt sich die Gesamtfläche als Summe der Flächen der vertikalen Streifen. Die Fläche eines einzelnen Streifens entspricht dem Produkt der Länge des x-Intervalls und der Gesamtlänge der y-Intervalle.

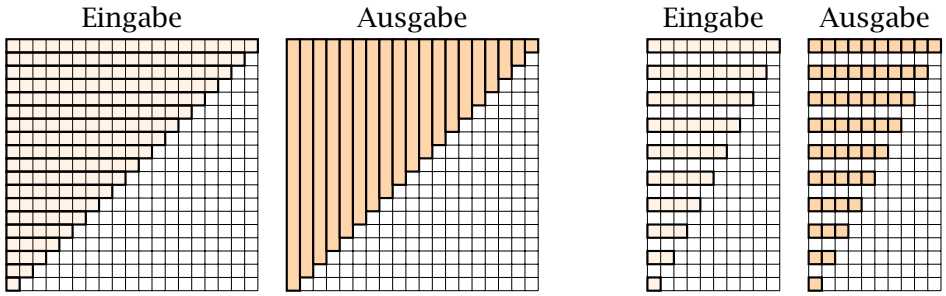
```
let total-area = sum-by (fun (i, js) → I.length i * Is.total-length js)
```

Für den Campus der RPTU Kaiserslautern-Landau ergeben sich die folgenden Werte.

```
>>> length campus
50
>>> let rs = rectangles campus
>>> total-area rs
1124
>>> length rs
56
>>> sum-by (fun (i, js) → length js) rs
156
```

Der aus 50 Rechtecken bestehende Campus wird somit durch 56 x-Intervalle und insgesamt 156 y-Intervalle repräsentiert, siehe Abbildung 5.8.

Analyse der Laufzeit Wie schnell ist unser Algorithmus zur Bestimmung der Gesamtfläche? Die Analyse ist etwas komplizierter als im Fall von *merge-sort*. Das liegt daran, dass wir beim Aufspalten der x-Intervalle Daten verdoppeln (aus (i, a) wird (il, a) und (ir, a)), so dass wir zunächst überlegen müssen, wieviele x-Intervalle und wieviele y-Intervalle maximal generiert werden. Die Zahl der x-Intervalle ist im schlechtesten Fall linear in der Zahl der Rechtecke: Es kann höchstens $2 \cdot n - 1$ x-Intervalle geben, wenn n die Anzahl der Rechtecke ist. (Warum?) Entsprechende Überlegungen gelten für die *einem* x-Intervall zugeordneten y-Intervalle. Summa summarum können somit höchstens quadratisch viele Intervalle generiert werden. Dieser Fall kann tatsächlich auftreten:



Die Eingabedaten sind jeweils lange horizontale Streifen, treppenförmig angeordnet. Im ersten Beispiel werden die horizontale Streifen von *rectangles* in vertikale Streifen überführt — jedem x-Intervall wird also genau ein y-Intervall zugeordnet. Liegen die horizontale Streifen etwas auseinander, erhalten wir eine quadratische Anzahl von y-Intervallen.

Im 1-dimensionalen Fall ist es weniger kompliziert. Um die Gesamtlänge eines Streifens zu berechnen, benötigen wir ungefähr $n \lg n$ Schritte. Da diese Berechnung im 2-dimensionalen Fall für jeden vertikalen Streifen durchgeführt wird, kommen wir auf eine Gesamtlaufzeit von $n^2 \lg n$. Im Vergleich zur exponentiellen Laufzeit eines Verfahrens, das auf dem Prinzip der Ein- und Ausschließung beruht, ist das allerdings eine gigantische Verbesserung, siehe Abbildung 5.5.

5.1.5. Ordnungsstatistik⋆

Wir haben in Abschnitt 4.3.3 gesehen, dass wir für die Berechnung einer optimalen Trassenführung das Minimum, das Maximum und den Median einer Folge von Elementen benötigen. Alle drei Aufgaben lassen sich einfach lösen, indem man die Folge zunächst sortiert und dann auf das erste, das letzte bzw. das mittlere Element zugreift. Die Laufzeit ist damit linear-logarithmisch, da die Sortierung die Laufzeit dominiert. In diesem Abschnitt wollen wir der Frage nachgehen, ob wir die Aufgaben auch direkter und damit effizienter lösen können. Gleichzeitig verallgemeinern wir die Aufgabenstellung etwas: Es gilt, das i-kleinste Element einer Folge von Elementen zu finden, die sogenannte i-te ***Ordnungsstatistik*** oder ***Ordnungsgröße***.

module Algorithmics.Median

Minimum und Maximum Die folgenden Programme lassen sich etwas lesbarer aufschreiben, wenn wir Infixoperatoren für das Minimum bzw. das Maximum zweier Elemente einführen — die beiden Definitionen sind nicht spezifisch für Zahlen, sie funktionieren für beliebige totale Quasiordnungen.

```
let (◁) a b = if a ⩽ b then a else b
let (▷) a b = if a ⩽ b then b else a
```

Statt den Namen voranzustellen, *min a b* bzw. *max a b*, schreiben wir den Bezeichner zwischen die Argumente, $a \triangleleft b$ bzw. $a \triangleright b$. Nur bei der Definition selbst ist das leider nicht möglich; dort muss der Bezeichner in Klammern gesetzt vorangestellt werden. Die Dreiecke können übrigens als Pfeile oder Pfeilspitzen gelesen werden: Wenn wir a und b der Größe nach anordnen, dann ist $a \triangleleft b$ das linke, d. h. das kleinere Element und $a \triangleright b$ das rechte, d. h. das größere Element. Infixnotation ist immer dann vorteilhaft, wenn die Funktion wie im Fall vom Minimum und Maximum ***assoziativ*** ist: $(a \triangleleft b) \triangleleft c = a \triangleleft (b \triangleleft c)$ und $(a \triangleright b) \triangleright c = a \triangleright (b \triangleright c)$. Dann können wir Anwendungen des Operators aneinanderreihen, ohne Klammern setzen zu müssen, zum Beispiel, $a \triangleright b \triangleright c \triangleright d \triangleright e$.

Ordnungsstatistik für $n \leqslant 5$ Fangen wir klein an. Für eine Folge von drei Elementen lässt sich das i-kleinste Element wie folgt bestimmen.

3-kleinste	$(a \triangleright b \triangleright c)$
2-kleinste	$(a \triangleright b) \triangleleft (a \triangleright c) \triangleleft (b \triangleright c)$
1-kleinste	$(a) \triangleleft (b) \triangleleft (c)$

Wie erklärt sich die Formel für den Median, das 2-kleinste Element? Nehmen wir an, wir würden die zwei kleinsten Elemente kennen. Deren Maximum ist der gesuchte Median. Weiterhin ist das Maximum aller anderen 2-elementigen Mengen größer gleich dem Median da $\triangleright$ monoton ist. Somit ergibt sich das 2-kleinste Element als das Minimum der Maxima aller 2-elementigen Teilmengen.

Wenn wir das 3-kleinste Element von vier Elementen bestimmen wollen, können wir entsprechend vorgehen. Wir bestimmen die Maxima aller 3-elementigen Teilmengen; deren Minimum ist das gesuchte Element.

4-kleinste	$(a \triangleright b \triangleright c \triangleright d)$
3-kleinste	$(a \triangleright b \triangleright c) \triangleleft (a \triangleright b \triangleright d) \triangleleft (a \triangleright c \triangleright d) \triangleleft (b \triangleright c \triangleright d)$
2-kleinste	$(a \triangleright b) \triangleleft (a \triangleright c) \triangleleft (a \triangleright d) \triangleleft (b \triangleright c) \triangleleft (b \triangleright d) \triangleleft (c \triangleright d)$
1-kleinste	$(a) \triangleleft (b) \triangleleft (c) \triangleleft (d)$

Allgemein ist das i-kleinste Element das Minimum der Maxima aller i-elementigen Teilmengen. Entsprechend ist das i-größte Element das Maximum der Minima aller i-elementigen Teilmengen. Für $n = 3$:

1-größte	$(a) \triangleright (b) \triangleright (c)$
2-größte	$(a \triangleleft b) \triangleright (a \triangleleft c) \triangleright (b \triangleleft c)$
3-größte	$(a \triangleleft b \triangleleft c)$

Die Klammern umfassen jeweils die Elemente der Teilmengen. Für $n = 4$:

1-größte	$(a) \triangleright (b) \triangleright (c) \triangleright (d)$
2-größte	$(a \triangleleft b) \triangleright (a \triangleleft c) \triangleright (a \triangleleft d) \triangleright (b \triangleleft c) \triangleright (b \triangleleft d) \triangleright (c \triangleleft d)$
3-größte	$(a \triangleleft b \triangleleft c) \triangleright (a \triangleleft b \triangleleft d) \triangleright (a \triangleleft c \triangleleft d) \triangleright (b \triangleleft c \triangleleft d)$
4-größte	$(a \triangleleft b \triangleleft c \triangleleft d)$

Für jede Ordnungsstatistik oder Ordnungsgröße gibt es somit zwei verschiedene Formeln, je nachdem, ob das i-kleinste Element (Min-Max Formel) oder das $(n + 1 - i)$-größte Element (Max-Min Formel) betrachtet wird.

Tatsächlich erhält man viele weitere Formeln, wenn man die Min-Max oder die Max-Min Formel mit Hilfe algebraischer Eigenschaften umformt. Minimum und Maximum erfüllen zum Beispiel die ***Distributivgesetze***:

$$x \triangleleft (y \triangleright z) = (x \triangleleft y) \triangleright (x \triangleleft z) \qquad (x \triangleright y) \triangleleft z = (x \triangleleft z) \triangleright (y \triangleleft z) \tag{5.1a}$$

$$x \triangleright (y \triangleleft z) = (x \triangleright y) \triangleleft (x \triangleright z) \qquad (x \triangleleft y) \triangleright z = (x \triangleright z) \triangleleft (y \triangleright z) \tag{5.1b}$$

Wir können die Anzahl der Operatoren in einem Ausdruck verringern, wenn wir die Gesetze von rechts nach links anwenden — *viele Programmoptimierungen basieren auf einem Distributivgesetz!*

Median für $n \leqslant 5$ Schauen wir uns die Umformungen am Beispiel des Medians an.

Piano $n = 3$: Die Formel für das 2-kleinste Element von 3 Elementen lässt sich wie folgt vereinfachen.

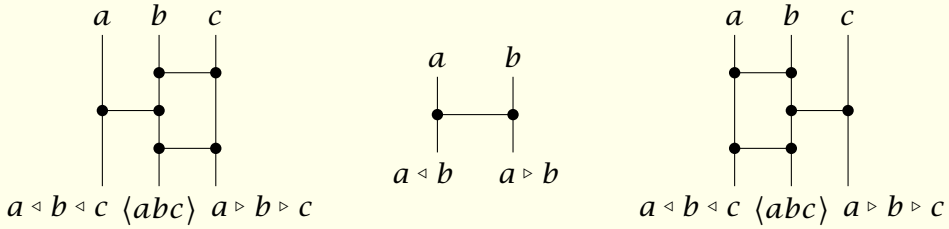
$$\begin{aligned} & (a \triangleright b) \triangleleft (a \triangleright c) \triangleleft (b \triangleright c) \\ = \quad & \{ \text{ Distributivgesetz (5.1b) } \} \\ & (a \triangleright (b \triangleleft c)) \triangleleft (b \triangleright c) \end{aligned}$$

Der resultierende Ausdruck ist optimal in der Anzahl der Operatoren — mit drei Operatoren (Kombinationen von $\triangleleft$ und $\triangleright$) lässt sich der Median nicht bestimmen. Die Formel bestimmt das kleinste der beiden größten Elemente (die Elemente *ohne* das allerkleinste Element $a \triangleleft b \triangleleft c$). Um die umgangssprachliche Deutung zu verstehen, hilft vielleicht die Metapher eines Fußball- oder Tennisturniers, siehe Abbildung 5.9.

$$\textit{let } \textit{median3}\ (a, b, c) = (a \triangleright (b \triangleleft c)) \triangleleft (b \triangleright c)$$

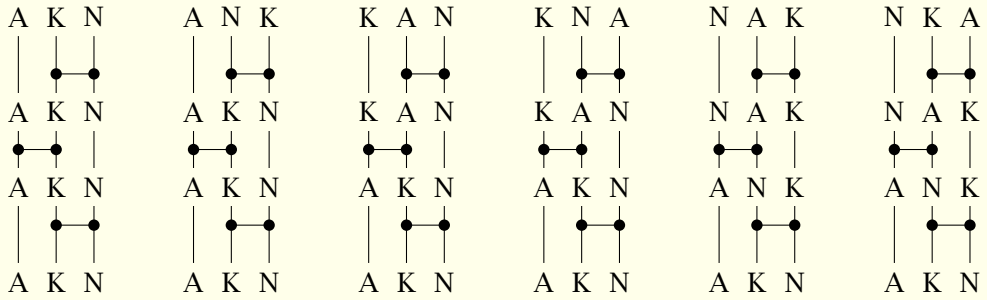
Die Medianfunktion hat viele interessante Eigenschaften. Sie ist zum Beispiel ***selbst-dual***: Die Funktion ändert sich nicht, wenn wir auf der rechten Seite $\triangleleft$ durch $\triangleright$ und umgekehrt $\triangleright$ durch $\triangleleft$

Eine Abfolge von Spielen lässt sich durch ein ***Turnierdiagramm*** repräsentieren. Entsprechend der Anzahl der Teilnehmer gibt es n vertikale Linien. Eine horizontale Linie repräsentiert ein Match. Der Verlierer rückt im Spielplan nach links, der Gewinner nach rechts. Von oben nach unten gelesen ergibt sich der zeitliche Ablauf der Spiele; Spiele auf der gleichen Ebene können parallel ausgetragen werden.

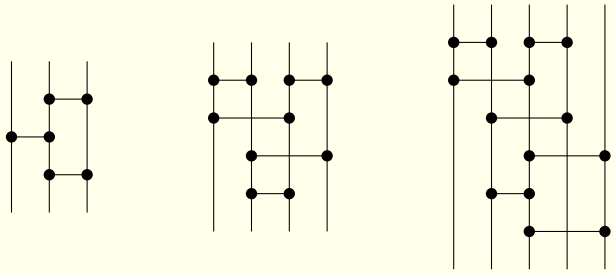


Der linke Spielplan gibt folgende Abfolge von Spielen vor: Zunächst lassen wir b und c gegeneinander antreten; der Verlierer spielt gegen a; der Gewinner dieses Spiels tritt schließlich gegen den Gewinner des ersten Spiels an. (Die Notation $\langle abc \rangle$ ist eine gebräuchliche Abkürzung für den Median von a, b und c.)

Die drei Führenden der Damenweltrangliste im Tennis sind Ashleigh Barty, Karolina Pliskova und Naomi Osaka (Women's Tennis WTA Rankings 2019). Lassen wir sie ein Turnier gemäß dem linken Spielplan austragen, ergeben sich 3! = 6 mögliche Turnierverläufe, je nachdem, in welcher Reihenfolge die Damen aufgestellt werden.



Die Median-Programme korrespondieren zu den folgenden Turnierdiagrammen.



Die ersten beiden Diagramme ermitteln tatsächlich die *vollständige* Rangliste von drei bzw. vier Teilnehmern. Mit anderen Worten, sie sortieren die Eingabe! Das ist beim dritten Diagramm nicht der Fall. (Warum? Welche zusätzlichen Spiele müssen durchgeführt werden, um die Rangliste zu ermitteln?)

Abbildung 5.9.: Turnierdiagramme (auch bekannt unter dem Namen Komparator-Netzwerke, engl. comparator networks).

ersetzen. Probieren Sie es aus! Oben haben wir den Median mit Hilfe vom Minimum und Maximum definiert. Umgekehrt lassen sich Minimum und Maximum auf den Median zurückführen, sofern die totale Quasiordnung über ein kleinstes bzw. ein größtes Element verfügt:

$$a \triangleleft b = median\ (-\infty, a, b)$$
$$a \triangleright b = median\ (a, b, +\infty)$$

wobei $-\infty$ das kleinste und $+\infty$ das größte Element repräsentiert. (Zum Beispiel: Für die Ordnung auf den Wahrheitswerten, $false < true$, spezialisieren sich die obigen Formeln zu $a \,\&\&\, b = median\ (false, a, b)$ und $a \,||\, b = median\ (a, b, true)$. Die Konjunktion entspricht dem Minimum und die Disjunktion dem Maximum zweier Wahrheitswerte.)

Crescendo $n = 4$: Die Formel für das 2-kleinste Element von 4 Elementen lässt sich wie folgt vereinfachen.

$$\begin{aligned}
& (a \triangleright b) \triangleleft (a \triangleright c) \triangleleft (a \triangleright d) \triangleleft (b \triangleright c) \triangleleft (b \triangleright d) \triangleleft (c \triangleright d) \\
= \quad & \{ \text{Distributivgesetz (5.1b), zweimal} \} \\
& (a \triangleright b) \triangleleft (a \triangleright (c \triangleleft d)) \triangleleft (b \triangleright (c \triangleleft d)) \triangleleft (c \triangleright d) \\
= \quad & \{ \text{Distributivgesetz (5.1b)} \} \\
& (a \triangleright b) \triangleleft ((a \triangleleft b) \triangleright (c \triangleleft d)) \triangleleft (c \triangleright d)
\end{aligned}$$

Der resultierende Ausdruck für den Untermedian berechnet das kleinste der drei größten Elemente, siehe auch Abbildung 5.9.

$$\textbf{\textit{let}}\ median4\ (a, b, c, d) = (a \triangleright b) \triangleleft ((a \triangleleft b) \triangleright (c \triangleleft d)) \triangleleft (c \triangleright d)$$

Fortissimo $n = 5$: Wenn die Anzahl der Elemente größer wird, werden die Formeln langsam aber sicher unhandlich. Die Max-Min Formel für das 3-größte Element von 5 Elementen,

$$\begin{aligned}
& (a \triangleleft b \triangleleft c) \triangleright (a \triangleleft b \triangleleft d) \triangleright (a \triangleleft b \triangleleft e) \triangleright (a \triangleleft c \triangleleft d) \triangleright (a \triangleleft c \triangleleft e) \\
& \qquad \triangleright (a \triangleleft d \triangleleft e) \triangleright (b \triangleleft c \triangleleft d) \triangleright (b \triangleleft c \triangleleft e) \triangleright (b \triangleleft d \triangleleft e) \triangleright (c \triangleleft d \triangleleft e)
\end{aligned}$$

besteht aus $\binom{5}{3} = 10$ Min-Gliedern und aus $10 \cdot 2 + 9 = 29$ Operatoren. Glücklicherweise hilft ein modularer Ansatz weiter: Der Median von 5 Elementen lässt sich auf den Median von 3 Elementen zurückführen, wenn wir zwei Elemente »rauskicken«, die für den Median nicht in Frage kommen.

$$\textbf{\textit{let}}\ median5\ (a, b, c, d, e) = median3\ ((a \triangleleft b) \triangleright (c \triangleleft d), (a \triangleright b) \triangleleft (c \triangleright d), e)$$

Das kleinste und das größte Element der ersten vier Elemente können ignoriert werden. Der Median aus den mittleren beiden Elementen und dem Element e ist der gesuchte Median der 5 Elemente, siehe auch Abbildung 5.9. (Schaffen Sie es, das obige Programm aus der Max-Min Formel herzuleiten?)

Für größere n stoßen wir an die Grenzen des Ansatzes: Da es $\binom{n}{k}$ k-elementige Teilmengen einer n-elementigen Menge gibt, enthalten die Min-Max und die Max-Min Formeln insgesamt $k \cdot \binom{n}{k} - 1$ Operatoren. Mit anderen Worten, für die Bestimmung des 1-kleinsten Elements benötigen wir lineare Laufzeit (optimal), für das 2-kleinste Element quadratische Laufzeit (na ja), für das 3-kleinste Element kubische Laufzeit (oh je) usw.

Ordnungsstatistik für $n > 5$ Versuchen wir die allgemeine Lösungsstrategie auf die Ordnungsstatistik anzuwenden und überlegen, wie wir das Problem auf die Lösung kleinerer Probleme zurückführen können.

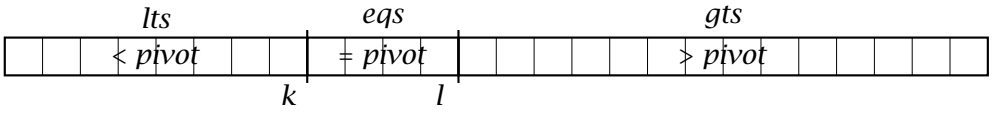
Für das Peano Entwurfsmuster müssen wir ein Element zur Seite legen. Ein beliebiges Element herauszugreifen ist nicht zielführend: Wenn wir zum Beispiel das Element 11 zur Seite legen und 47 ist das i-kleinste Element der restlichen Folge, dann können wir nur schließen, dass 47 das $(i+1)$-kleinste Element der Gesamtfolge ist — das nützt uns aber nichts. Das Entwurfsmuster führt zum Ziel, wenn wir ein Extremelement, das kleinste oder das größte, auswählen. Leider ist das resultierende Verfahren nicht besonders effizient: Um das i-kleinste Element zu bestimmen, benötigen wir $i \cdot n$ Schritte, im Fall des Medians also quadratisch viele Schritte. Im Wesentlichen re-implementieren wir das Sortierverfahren »Sortieren durch Auswählen«. Dessen große Schwester ist das »Sortieren durch Austauschen«, das wir in Abschnitt 5.1.2 haben links liegen lassen. Vielleicht können wir die zugrundeliegende Idee adaptieren?

Im Sinne des Leibniz Entwurfsmusters müssen wir die Problemgröße ungefähr halbieren. Dazu wählen wir ein »Pivotelement« aus und teilen die Eingabefolge in kleinere und größere Elemente. Gibt es insgesamt k kleinere Elemente und ist $i \leqslant k$, dann bestimmen wir das i-kleinste Element unter diesen Elementen, anderenfalls das $(i-k)$-kleinste Element unter den größeren Elementen. Im Unterschied zum »Sortieren durch Austauschen« tätigen wir nur *einen* rekursiven Aufruf.

Die »1 Million €« Frage ist natürlich: Wie wählen wir das Pivotelement? Wir drücken uns für den Moment um die Antwort und nehmen einfach an, dass wir ein ***Orakel*** befragen können. Wenn wir dem Orakel die Folge präsentieren, wählt es für uns ein geeignetes Folgenelement aus. Die Funktion *quickselect*, die das i-kleinste Element einer *nicht-leeren* Liste *xs* von Elementen bestimmt, ist somit zusätzlich mit dem Orakel parametrisiert. (Wir nehmen an, dass der Index i gültig ist: $1 \leqslant i \leqslant \mathit{length}\ \mathit{xs}$.)

```
let rec quickselect (oracle : 'a list → 'a) i xs =          // 1 ⩽ i ⩽ length xs
  let pivot = oracle xs
  let lts   = filter (fun x → x < pivot) xs
  let eqs   = filter (fun x → x = pivot) xs
  let gts   = filter (fun x → x > pivot) xs
  let k     = length lts
  let l     = k + length eqs
  if   i ⩽ k then quickselect oracle i       lts
  elif i ⩽ l then pivot
             else quickselect oracle (i - l) gts
```

Die gegebene Liste *xs* wird tatsächlich in *drei* Teillisten partitioniert: in echt kleinere Elemente, gleiche Elemente und echt größere Elemente.



Wenn $k < i \leqslant l$ gilt, ist das Pivotelement das gesuchte Element; in den beiden anderen Fällen erfolgt ein rekursiver Aufruf.

Die Partitionierung erledigt die vordefinierte Funktion *filter*, die aus einer gegebenen Liste alle »guten« Elemente aussiebt — frei nach Aschenputtel »die guten ins Töpfchen, die schlechten ins Kröpfchen.«

```
let rec filter (good : 'a → Bool) : 'a list → 'a list = function
  | [ ]     → [ ]
  | x :: xs → if good x then x :: filter good xs
                        else     filter good xs
```

Die Funktion *quickselect* folgt einem etwas merkwürdigen Rekursionsschema. Zum Beispiel ist nicht unmittelbar klar, wo der Basisfall behandelt wird. Überlegen wir: Wenn die Eingabeliste einelementig ist, dann wählt *oracle* dieses eine Element aus. Die Listen *lts* und *gts* sind dann leer und wir landen im zweiten Zweig der Fallunterscheidung, in dem das Pivotelement zurückgegeben wird. Für längere Listen ist die Terminierung gewährleistet, da *lts* und *gts* stets weniger Elemente als *xs* enthalten. (Es sei denn das Orakel mogelt: Der Aufruf *quickselect* (**fun** _ → 0) 7 [1 . . 9] terminiert nicht, da das Orakel ein Element zurückgibt, das gar nicht in der Liste enthalten ist.)

Um die Terminierung zu gewährleisten, partitionieren wir übrigens die ursprüngliche Liste in drei Teillisten (<, = und >) und nicht nur in zwei (⩽ und > oder < und ⩾). Die binäre Partitionierung ist problematisch, wenn die Eingabeliste Elemente mehrfach enthält. Sind im Extremfall alle Elemente der Eingabe identisch, dann ist eine Teilliste stets leer und die andere zur Eingabeliste identisch — Nichtterminierung ist die Folge.

Kommen wir zur Analyse der Laufzeit. Nehmen wir zunächst an, dass das Orakel uns nicht wohlgesonnen ist. Im schlechtesten Fall wählt das Orakel ein Extremelement aus, so dass der rekursive Aufruf eine Liste erhält, die nur um ein Element kleiner ist. In diesem Fall ergibt sich eine quadratische Laufzeit.

Wenn uns das Orakel wohlgesonnen ist, dann beschleunigt sich die Rechnung. Im besten Fall wählt das Orakel den *Median* der Eingabefolge, so dass in jedem Schritt die Problemgröße ungefähr halbiert wird. Dann benötigt der Algorithmus insgesamt

$$\frac{1}{1}n + \frac{1}{2}n + \frac{1}{4}n + \frac{1}{8}n + \cdots < 2 \cdot n$$

Schritte, hat also eine lineare Laufzeit, siehe Abbildung 5.10. Das ist asymptotisch optimal — in sublinearer Zeit können wir das *i*-kleinste Element nicht bestimmen, da wir uns zumindest jedes Element anschauen müssen. Halten wir fest: *Wenn* wir den Median in linearer Zeit berechnen können, *dann* lässt sich jede beliebige Ordnungsgröße in linearer Zeit berechnen. (Der Median ist gewissermaßen der schwierigste Spezialfall.) Wenn das Wörtchen »wenn« nicht wäre …

Median der Mediane Zurück zum Ausgangspunkt: Die allgemeine Lösungsstrategie empfiehlt, Probleme auf kleinere Probleme zurückzuführen. Dabei ist es nicht zwingend, die Problemgröße zu halbieren. Wenn wir zum Beispiel in jedem Schritt die Größe um den Faktor $\frac{3}{4}$ verringern, dann hat *quickselect* weiterhin eine lineare Laufzeit, da die ***geometrische Reihe*** $\sum_{k=0}^{\infty} q^k$ für $\operatorname{abs} q < 1$ konvergiert: $\sum_{k=0}^{\infty} q^k = 1/(1-q)$.

$$\frac{1}{1}n + \frac{3}{4}n + \frac{9}{16}n + \frac{27}{64}n + \cdots < 4 \cdot n$$

Die Laufzeit verdoppelt sich lediglich: Wir benötigen jetzt $4 \cdot n$ statt wie vorher $2 \cdot n$ Schritte. Auf unser Problem angewendet heißt das, es genügt ein Pivotelement zu finden, so dass mindestens $\frac{1}{4}$ der Elemente kleiner und mindestens $\frac{1}{4}$ der Elemente größer sind — die Lage der restlichen Elemente zum Pivotelement ist uns egal. Damit wäre garantiert, dass der rekursive Aufruf von *quickselect* auf höchstens $\frac{3}{4}$ der ursprünglichen Elemente angewendet wird. Was uns jetzt noch fehlt ist eine zündende Idee, wie wir ein solches Pivotelement bestimmen.

Das folgende Gedankenexperiment weist den Weg. Wir ordnen die Elemente gedanklich 2-dimensional in einem Rechteck an und bestimmen zunächst den Median jeder einzelnen Zeile und anschließend den Median der Zeilenmediane.

Sei $T(n)$ die Zeit (engl. time), die ein Algorithmus für eine Eingabe der Größe n benötigt. Die Zeitfunktion der binären Suche erfüllt im Rekursionsschritt die Gleichung $T(n) = 1 + T(n/2)$. Wir berechnen eine Zeiteinheit für die Unterteilung des Suchraums und weitere administrative Aufgaben. Der binäre Logarithmus »löst« die Gleichung: $T(n) \sim \lg n$. Die binäre Suche hat somit eine logarithmische Laufzeit.

Im Fall von *quickselect* ist der Aufwand im Rekursionsschritt nicht mehr konstant, sondern linear: $T(n) = n + T(n/2)$. Die Gesamtlaufzeit ist in diesem Fall ebenfalls linear: $T(n) \sim 2 \cdot n$. Der Faktor 2 ergibt sich als Wert der geometrischen Reihe $\sum_{k=0}^{\infty}(1/2)^k$.

Zur Erinnerung: Eine ***geometrische Folge*** a_n hat die Eigenschaft, dass der Quotient aufeinanderfolgender Glieder konstant ist: $a_{n+1}/a_n = q$. Im einfachsten Fall ist $a_n = q^n$. Die dazugehörige Folge der Partialsummen heißt ***geometrische Reihe***: $s_n = \sum_{k=0}^{n-1} a_k$. Eine geschlossene Formel für $s_n = \sum_{k=0}^{n-1} q^k$ lässt sich wie folgt herleiten. Wir betrachten die Summe s_{n+1}; diese lässt sich auf zwei Arten aufschreiben, indem man entweder die ersten n oder die letzten n Summanden zusammenfasst:

$$s_n + q^n = 1 + q + q^2 + q^3 + \cdots + q^{n-1} + q^n = 1 + q \cdot s_n$$

Die resultierende Gleichung lösen wir sodann nach s_n auf:

$$s_n + q^n = 1 + q \cdot s_n \quad \Longleftrightarrow \quad s_n - q \cdot s_n = 1 - q^n \quad \Longleftrightarrow \quad s_n = (1 - q^n)/(1 - q)$$

Ist $\operatorname{abs} q < 1$, dann strebt der Zähler für $n \to \infty$ gegen eins: $\lim_{n\to\infty} s_n = 1/(1 - q)$.

Den Grenzwert einer geometrischen Reihe kann man auch direkt herleiten:

$$\begin{aligned}
& s = 1 + q + q^2 + q^3 + \cdots \\
\Longleftrightarrow \quad & \{ \text{ Distributivgesetz } \} \\
& s = 1 + q \cdot (1 + q + q^2 + \cdots) \\
\Longleftrightarrow \quad & \{ \text{ Definition von } s \} \\
& s = 1 + q \cdot s \\
\Longleftrightarrow \quad & \{ \text{ Arithmetik } \} \\
& s = 1/(1 - q)
\end{aligned}$$

(Eine ähnliche Herleitung haben wir schon einmal gesehen. Erinnern Sie sich wo?)

Die Grenzwerte geometrischer Reihen lassen sich übrigens geometrisch sehr ansprechend als Parkettierungen des Einheitsquadrats deuten.

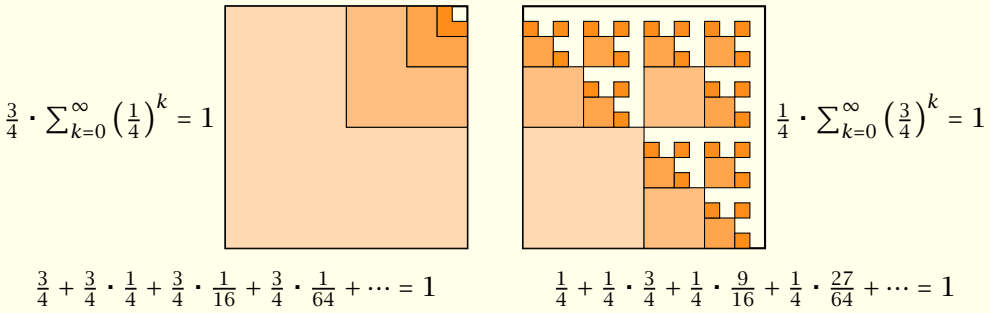
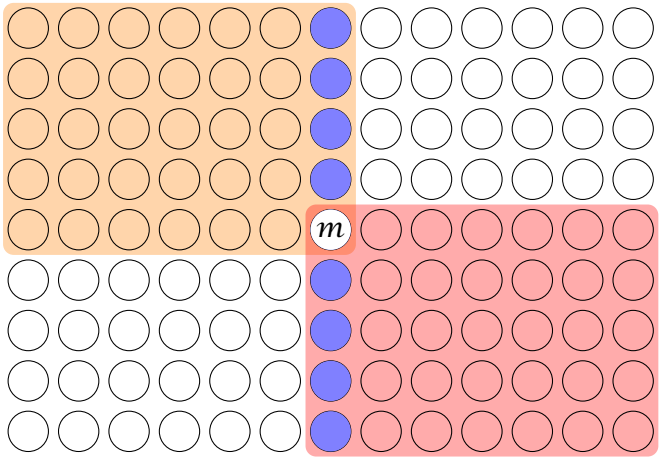


Abbildung 5.10.: Laufzeitanalyse und geometrische Reihen.



Der Median der Zeilenmediane m besitzt die gewünschte Eigenschaft. Um uns davon zu überzeugen, rearrangieren wir die Elemente: In jeder Zeile platzieren wir die kleineren Elemente links und die größeren rechts vom Zeilenmedian, der blau eingefärbt jeweils in der Mitte liegt. Weiterhin platzieren wir die Zeilen, deren Median kleiner ist als m, oberhalb von m und die Zeilen, deren Median größer ist, unterhalb. Aufgrund der Transitivität der Quasiordnung folgt, dass m größer gleich den Elementen in der orange hinterlegten Fläche ist und kleiner gleich den Elementen in der roten Fläche — über die Beziehung der restlichen Element zu m lässt sich allerdings nichts aussagen.

Noch sind wir nicht am Ziel — wir müssen ja noch klären, wie wir die Zeilenmediane und den Median der Zeilenmediane bestimmen. Welche Optionen haben wir? Zunächst einmal spielt die Form des Rechtecks für das obige Argument keine Rolle. Insbesondere können wir eine *konstante*, vorher festgelegte Breite verwenden, wie zum Beispiel 13 in der obigen Grafik. Für die Breite wählen wir geschickterweise ein ungerade Zahl, anderenfalls müssten wir den Unter- oder den Obermedian bestimmen. Aber wie klein können wir sie wählen? Klappt es mit 5 oder gar mit 3 Elementen? Für diese Spezialfälle haben wir ja bereits Lösungen programmiert, die wir für die Berechnung der Zeilenmediane verwenden könnten. Und wie berechnen wir den Median der Zeilenmediane? Nun, dafür tätigen wir einen weiteren rekursiven Aufruf!

Die obige Analyse der Laufzeit ist damit nicht länger gültig, da wir ja ursprünglich von einem, nicht zwei rekursiven Aufrufen ausgegangen sind. Versuchen wir die Laufzeit für die Breite 3 *grob* abzuschätzen. Dazu sei $T(n)$ die Anzahl der Schritte (engl. time), die der Algorithmus für eine Folge von n Elementen benötigt. Im Rekursionsfall erfüllt T die Gleichung $T(n) = n + T\left(\frac{1}{3} \cdot n\right) + T\left(\left(1 - \frac{2}{3} \cdot \frac{1}{2}\right) \cdot n\right)$. Wir tätigen wie gesagt zwei rekursive Aufrufe. Mit dem ersten bestimmen wir den Median von $\frac{1}{3} \cdot n$ Zeilenmedianen. Mit diesem partitionieren wir dann die ursprüngliche Liste. Die Teilliste *lts* enthält somit mindestens $\frac{2}{3} \cdot \frac{1}{2} \cdot n$ Elemente (die orangene Fläche); gleiches gilt für *gts* (die rote Fläche). Die jeweils andere Teilliste hat also höchstens $\left(1 - \frac{2}{3} \cdot \frac{1}{2}\right) \cdot n$ Elemente. (Wir gehen wie immer von dem schlechtesten Fall aus.) Für alle restlichen Arbeiten veranschlagen wir n Schritte.[4] Nun kann man zeigen, dass eine Funktion T mit dieser Eigenschaft leider linear-logarithmisch ist. Das ist die schlechte Nachricht; die gute Nachricht ist, dass der Ansatz für die Breite 5 funktioniert: T mit $T(n) = n + T\left(\frac{1}{5} \cdot n\right) + T\left(\left(1 - \frac{3}{5} \cdot \frac{1}{2}\right) \cdot n\right)$ ist tatsächlich linear. Die folgende Übersicht zeigt: Je größer wir die Breite wählen, desto näher rückt die Laufzeit an den

[4] Das ist natürlich etwas niedrig gegriffen. Es spielt aber tatsächlich keine Rolle, ob wir n, $2n$, $47n$ oder $c \cdot n$ Schritte benötigen — es geht uns ja um Größenordnungen: linear, linear-logarithmisch, quadratisch etc. Solange der Faktor c konstant ist, haben die folgenden Ergebnisse Bestand.

Ausgangspunkt $4 \cdot n$ (nur ein rekursiver Aufruf) heran.

$$\begin{aligned}
\mathrm{T}(n) &= n + \mathrm{T}(n/3) + \mathrm{T}((1-2/6)\cdot n) && \mathrm{T}(n) \sim 3n \cdot \log_{6.75} n \\
\mathrm{T}(n) &= n + \mathrm{T}(n/5) + \mathrm{T}((1-3/10)\cdot n) && \mathrm{T}(n) \sim 10n \\
\mathrm{T}(n) &= n + \mathrm{T}(n/7) + \mathrm{T}((1-4/14)\cdot n) && \mathrm{T}(n) \sim 7n \\
\mathrm{T}(n) &= n + \mathrm{T}(n/9) + \mathrm{T}((1-5/18)\cdot n) && \mathrm{T}(n) \sim 6n \\
&\vdots && \vdots \\
\mathrm{T}(n) &= n + \mathrm{T}(n/99) + \mathrm{T}((1-50/198)\cdot n) && \mathrm{T}(n) \sim 4.125n
\end{aligned}$$

Die Notation $f(n) \sim g(n)$ bedeutet, dass der Quotient der Funktionswerte für hinreichend große n gegen 1 strebt: $\lim_{n\to\infty} f(n)/g(n) = 1$. Ab einer Breite von 5 fällt der zusätzliche rekursive Aufruf nicht signifikant ins Gewicht, so dass wir endlich, endlich zur Implementierung des Verfahrens schreiten können.

Für die Berechnung der Zeilenmediane teilen wir die Eingabeliste in Gruppen zu je 5 Elementen auf.

```
let rec medians-of-5 = function
  | [ ]                          → [ ]
  | [x1 ]                        → [x1 ]
  | [x1;x2 ]                     → [x1 ◁ x2 ]
  | [x1;x2;x3 ]                  → [median3 (x1, x2, x3)]
  | [x1;x2;x3;x4 ]               → [median4 (x1, x2, x3, x4)]
  | x1 :: x2 :: x3 :: x4 :: x5 :: xs → median5 (x1, x2, x3, x4, x5) :: medians-of-5 xs
```

Da die Division durch 5 nicht immer glatt aufgeht, müssen wir insgesamt 5 Basisfälle behandeln. Dazu machen wir ausgiebig Gebrauch von Listenmustern, wobei zum Beispiel $[x_1;x_2;x_3]$ das geschachtelte Muster $x_1 :: x_2 :: x_3 :: [\,]$ abkürzt.

Kommen wir zum großen Finale: Die Funktion *ordselect* berechnet die Ordnungsstatistik in linearer Zeit. Sie spezialisiert *quickselect* mit dem Median der Zeilenmediane als Orakel. Die Medianfunktion selbst wird rekursiv mit Hilfe von *ordselect* definiert.

```
let rec ordselect i xs = quickselect (median ≪ medians-of-5) i xs
and median = function
  | [x1 ]                        → x1
  | [x1;x2 ]                     → x1 ◁ x2
  | [x1;x2;x3 ]                  → median3 (x1, x2, x3)
  | [x1;x2;x3;x4 ]               → median4 (x1, x2, x3, x4)
  | [x1;x2;x3;x4;x5 ]            → median5 (x1, x2, x3, x4, x5)
  | xs                           → ordselect (length xs ÷ 2) xs
```

Das Rekursionsmuster ist jetzt noch merkwürdiger: *ordselect* verwendet *median* und *median* verwendet umkehrt *ordselect*. Im Fachjargon sagt man, die beiden Funktion sind ***verschränkt rekursiv*** definiert. Verschränkt rekursive Funktionsdefinitionen müssen mit dem Schlüsselwort ***and*** verbunden werden, damit jede Funktion jede andere sieht: ***let rec*** $f_1\ (x_1) = e_1$ ***and*** $f_2\ (x_2) = e_2$. Die Bezeichner f_1 und f_2 sind dann sowohl in e_1 als auch in e_2 sichtbar. Im Gegensatz dazu ist in ***let rec*** $f_1\ (x_1) = e_1$ ***let rec*** $f_2\ (x_2) = e_2$ der Bezeichner f_2 nur in e_2 sichtbar, nicht aber in e_1.

Die Funktion *median* verwendet die weiter oben definierten Spezialfunktionen, um den Median für Listen der Länge $n \leqslant 5$ zu bestimmen, behandelt also insgesamt 5 Basisfälle. Somit führt das Orakel nur dann einen rekursiven Aufruf von *ordselect* aus, wenn die ursprüngliche Liste mehr als $5 \cdot 5 = 25$ Element umfasst. (Der Basisfall der einelementigen Liste muss zwingend behandelt werden, um die Terminierung zu gewährleisten.)

Fazit: Mit einer großen Portion Hartnäckigkeit sind wir ans Ziel gekommen. Beim Entwurf von Algorithmen hilft wie bei vielen anderen Tätigkeiten Erfahrung. So haben wir uns wiederholt gefragt, wieviele zusätzliche Rechnungen wir uns erlauben können, ohne das große Ziel, eine lineare Gesamtlaufzeit, aus den Augen zu verlieren bzw. zu gefährden (Verkleinerung der Problemgröße um $\frac{3}{4}$ statt $\frac{1}{2}$; zwei rekursive Aufrufe statt einem). Darüber hinaus gibt es oft einen kreativen Moment, den oft zitierten Geistesblitz. In unserem Beispiel ist das sicherlich die Idee, die Elemente 2-dimensional in einem Rechteck anzuordnen und den Median der Mediane als Privotelement zu verwenden.

Übungen.

1. Die Definition von *split-min* ist nicht ganz zwingend. Die Alternative

$$\textit{if } x \leqslant m \textit{ then } (x, xs) \textit{ else } (m, x :: ys)$$

kann auch durch die symmetrische Formulierung

$$\textit{if } x \leqslant m \textit{ then } (x, m :: ys) \textit{ else } (m, x :: ys)$$

ersetzt werden. (Das resultierende Sortierverfahren hört auf den Namen »Bubble Sort«.) Ändert sich durch diese Modifikation die Laufzeit des Verfahrens?

2. Ein Sortierverfahren heißt ***stabil***, wenn es die relative Reihenfolge von äquivalenten Elemente nicht verändert: Wenn a in der Eingabe vor b auftritt und $a \sim b$ gilt, dann wird auch in der Ausgabe a vor b aufgeführt. (Stabilität ist eine sehr wünschenswerte Eigenschaft, da sie Vorsortierungen erhält: Wenn wir zum Beispiel eine Liste von Personen nach dem Nachnamen sortieren, die Liste aber bereits nach dem Vornamen sortiert ist, dann werden in der Ausgabe Personen mit gleichem Nachnamen nach dem Vornamen angeordnet.) Welche Sortierverfahren sind stabil, welche nicht? Lassen sich letztere gegebenenfalls »stabilisieren«?

3. Ein ***Lauf*** ist eine sortierte Teilliste. Schreiben Sie eine Sortierfunktion *bottom-up-merge-sort*, die auf dem wiederholten Mischen von Läufen basiert. Gehen Sie dabei in vier Schritten vor:

(a) Schreiben Sie eine Funktion *pair-merge*, die eine Liste von n Läufen in eine Liste von $\lceil n/2 \rceil$ Läufen überführt, indem sie jeweils zwei benachbarte Läufe mischt: den 1. Lauf mit dem 2., den 3. mit dem 4. und so weiter.

(b) Definieren Sie eine Funktion *merge-runs*, die eine Liste von Läufen in einen einzigen Lauf überführt, indem sie *pair-merge* so oft aufruft, bis die Liste von Läufen nur noch einen einzigen Lauf enthält.

(c) Implementieren Sie eine Funktion *runs*, die eine ungeordnete Liste in eine Liste von Läufen überführt. Versuchen Sie in der Eingabeliste vorhandene Läufe so weit wie möglich zu verwenden.

(d) Definieren sie *bottom-up-merge-sort* als Komposition von *runs* und *merge-runs*.

Analysieren Sie die Laufzeit des Sortierverfahrens. Wann ist es dem eng verwandten Verfahren aus Abschnitt 5.1.2 vorzuziehen?

5.2. Suchen

module Algorithmics.Search

Im täglichen Leben wie in der Informatik gehört Suchen zu den häufigen, wenn auch nicht immer beliebten Tätigkeiten. Wir suchen nach Schlüsseln, Unterlagen, Waren, Personen .... Beim Schachspielen suchen wir nach einem Gewinnzug, bei unserem Ratespiel aus Abschnitt 3.6 nach einer Zahl.

Bei der ersten Gruppe von Beispielen liegen die zu durchsuchenden Daten konkret vor, zerstreut in einer Wohnung oder wohlorganisiert in einer Datenstruktur auf einem Rechner. In den Abschnitten 5.2.1–5.2.3 schauen wir uns drei mögliche Organisationsformen an: Listen, Suchlisten und Suchbäume.

Bei der zweiten Kategorie von Beispielen sind die Daten virtuell: Nicht alle möglichen Stellungen eines Schachspiels sind explizit repräsentiert; sie ergeben sich implizit mittels der Regeln des Schachspiels. Wir beschreiben den Suchraum in geeigneter Weise und nutzen die Beschreibung bei der Suche. Abschnitt 5.2.4 beschäftigt sich mit dem Suchen in »virtuellen Räumen« und richtet dabei ein besonderes Augenmerk auf Korrektheit und Terminierung.

5.2.1. Listen

Nehmen wir an, wir wollen für die Personalabteilung eines Unternehmens Personaldaten verwalten. Um Personen gleichen Namens einfach auseinanderhalten zu können, erhält jede Mitarbeiterin und jeder Mitarbeiter bei Amtsantritt eine eindeutige Personalnummer. Den Personalstamm können wir dann durch eine Liste von Einträgen des Typs

```
type Entry = {key : Nat; person : Person}
```

repräsentieren. Jeder Eintrag besteht aus einer Personalnummer und den eigentlichen Personaldaten. Vereinbarungsgemäß enthält die Liste, die den Personalstamm repräsentiert, keine zwei Einträge mit der gleichen Personalnummer. Zum Beispiel:

```
let team = [{key = 7;    person = ralf    };
            {key = 815;  person = melanie};
            {key = 4711; person = julia   };
            {key = 4712; person = andres  }]
```

Eine wiederkehrende Aufgabe ist es, zu einer gegebenen Personalnummer die zugehörigen Personaldaten herauszusuchen. Um die Funktion für beliebige Personaldaten verwenden zu können, parametrisieren wir sie mit der Liste der Einträge.

```
lookup (key : Nat, staff : List ⟨Entry⟩) : Person
```

Was machen wir, wenn kein passender Eintrag existiert? Wir stellen die beiden möglichen Resultate einer Suche, erfolglos und erfolgreich, mit Hilfe des Typs *Option* dar.

```
lookup (key : Nat, staff : List ⟨Entry⟩) : Option ⟨Person⟩
```

Der Typ drückt aus, dass die Suche *möglicherweise* eine Person zurückgibt. Schlägt die Suche fehl, wird der Wert *None* zurückgegeben, sonst der Wert *Some p*, wobei *p* die gesuchte Person ist.

Nach diesen Vorarbeiten kommen wir mit dem Struktur Entwurfsmuster für *List* unmittelbar zum Ziel.

```
let rec lookup (key : Nat, staff : List ⟨Entry⟩) : Option ⟨Person⟩ =
  match staff with
  | []              → None
  | entry :: entries → if key = entry.key then Some entry.person
                       else lookup (key, entries)
```

Die Implementierung von *lookup* erinnert an die lineare Suche aus Abschnitt 3.6: Die Liste wird von vorne nach hinten durchsucht, bis ein passender Listeneintrag gefunden wird oder das Listenende erreicht ist. Verbessern lässt sich das Verfahren nicht ohne Weiteres, denn Listen sind der Natur nach linear. (Eine Liste ähnelt wie gesagt einem Akten- oder Tellerstapel: Auf das oberste Objekt kann man direkt zugreifen, auf die darunterliegenden Objekte nicht.)

5.2.2. Suchlisten

Wir können die Suche, zumindest die erfolglose Suche, etwas beschleunigen, wenn wir die Liste nach der Personalnummer ordnen. Eine geordnete oder sortierte Liste nennen wir auch ***Suchliste*** — dies ist allerdings kein etablierter Begriff. Wenn wir von einer Sortierung ausgehen — die Liste *team* ist in der Tat nach der Personalnummer geordnet — lässt sich *lookup* wie folgt verbessern.

```
let rec lookup (key : Nat, staff : List ⟨Entry⟩) : Option ⟨Person⟩ =
  match staff with
  | [ ]                → None
  | entry :: entries → if    key < entry.key    then None
                       elif key = entry.key    then Some entry.person
                       (* key > entry.key *) else  lookup (key, entries)
```

Aus dem 2-Wege Vergleich wird ein 3-Wege Vergleich. Ist die gesuchte Nummer echt kleiner als die des ersten Eintrags, so kann die Suche unmittelbar abgebrochen werden. Die erfolglose Suche wird schneller, die erfolgreiche nicht. Suchen wir zum Beispiel nacheinander nach allen Personalnummern, so benötigen wir in beiden Fällen $1 + 2 + \cdots + n - 1 + n = \binom{n+1}{2} = n \cdot (n+1)/2$ rekursive Aufrufe.

3-Wege Vergleiche sind übrigens das Konstrukt der Wahl, wenn man mit totalen Quasiordnungen arbeitet, da zwei Elemente auf genau drei Arten zueinander in Beziehung stehen können: $a < b$, $a \sim b$ oder $a > b$. Im obigen Programm ist »~« durch »=« gegeben, da die Ordnung auf den natürlichen Zahlen antisymmetrisch ist.

5.2.3. Binäre Suchbäume

module Algorithmics.Tree

Können wir die binäre Suche aus Abschnitt 3.6 adaptieren? Nein, nicht ohne den Geschwindigkeitsvorteil zu verlieren. Im Gegensatz zur Halbierung des Suchintervalls kostet die Halbierung einer Liste viele Rechenschritte. (Wieviele?)

Wenn wir schnell auf das mittlere Element zugreifen wollen, müssen wir die Struktur der Liste ändern. Wir brauchen einen anderen Containertyp!

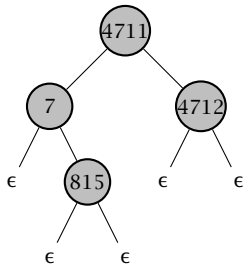
```
type Tree ⟨'a⟩ =
  | Leaf
  | Node of Tree ⟨'a⟩ * 'a * Tree ⟨'a⟩
```

Der Konstruktor *Leaf* tritt an die Stelle von *Nil* bzw. [ ]; wie *Nil* repräsentiert auch *Leaf* die leere Folge. Der Konstruktor *Node* (l, x, r) tritt an die Stelle von *Cons* (x, xs) bzw. $x::xs$ und repräsentiert eine mindestens einelementige Folge, bestehend aus der »linken« Teilfolge l, dem Element x und der »rechten« Teilfolge r. Die Folge 7 815 4711 4712 kann zum Beispiel durch

```
Node (Node (Leaf, 7, Node (Leaf, 815, Leaf)), 4711, Node (Leaf, 4712, Leaf))
```

repräsentiert werden. Neben dieser Möglichkeit gibt es noch 13 andere. (Nachrechnen!)

Elemente des neuen Variantentyps nennen wir auch ***Binärbaume***; Baum wegen der hierarchischen Struktur; *Binär*baum, da jeder nicht-leere Baum in zwei Teilbäume verzweigt. Sind die Elemente von links nach rechts geordnet, so spricht man von einem ***Suchbaum***. Klar, *Tree* soll ja die Suche besser unterstützen als *List*. (Binärbäume haben aber noch viele andere Anwendungen, deswegen lohnt sich ein spezieller Begriff.) Grafisch dargestellt sieht der obige Ausdruck so aus (ϵ repräsentiert jeweils ein Blatt):



Projiziert man die Elemente auf die x-Achse, so erhält man die Ausgangsfolge 7 815 4711 4712. Da diese geordnet ist, handelt es sich bei dem Binärbaum um einen Suchbaum.

Mit Hilfe des Struktur Entwurfsmusters für den Datentyp *Tree* können wir die letzte Definition von *lookup* leicht auf Binärbäume adaptieren — wir gehen davon aus, dass der Personalstamm nicht länger als Liste vorliegt, sondern als Binärbaum.

```
let rec lookup (key : Nat, staff : Tree ⟨Entry⟩) : Option ⟨Person⟩ =
  match staff with
  | Leaf                      → None
  | Node (left, entry, right) → if   key < entry.key   then lookup (key, left)
                                elif key = entry.key   then Some entry.person
                                (* key > entry.key *)  else  lookup (key, right)
```

In einem Suchbaum dient das Element in der ***Wurzel***, dem obersten Knoten (engl. node), als Wegweiser. In unserem Anwendungsfall sind die Einträge nach dem Schlüssel geordnet. Ist der gesuchte Schlüssel kleiner als der Schlüssel des Wegweisers, suchen wir im linken Teilbaum weiter. (Da die Einträge im rechten Teilbaum größer sind als der gesuchte Schlüssel, ist eine Suche im rechten Teilbaum zwar möglich, aber unnötig — sie wäre stets erfolglos.) Der symmetrische Fall, der gesuchte Schlüssel ist größer als der Schlüssel des Wegweisers, wird entsprechend symmetrisch behandelt.

Welche Laufzeit hat die neue Version von *lookup*? Nun, das kommt ganz auf die Form des Suchbaums an. Sind die Elemente links und rechts jeweils gleichmäßig verteilt, ist die Laufzeit logarithmisch. Ein solcher Suchbaum heißt auch ***ausgeglichen*** oder ***balanciert***. Ist hingegen einer der Teilbäume jeweils leer — der Baum degeneriert zur Liste — dann ist die Laufzeit linear.

Im Allgemeinen ist die Laufzeit von *lookup* proportional zur ***Höhe*** des Binärbaums.

```
let rec height = function
  | Leaf          → 0
  | Node (l, x, r) → 1 + max (height l) (height r)
```

Die Höhe entspricht der Länge des längsten Pfades von der Wurzel zu einem ***Blatt*** (engl. leaf), siehe auch Abschnitt 5.1.3.

Die Funktion *lookup* geht davon aus, dass die Stammdaten als Binärbaum vorliegen. Wie aber konstruieren wir einen Binärbaum? Diesem und anderen Themen wenden wir uns in Abschnitt 5.3 ausführlich zu.

5.2.4. Binäre Suche: Korrektheit und Terminierung

Schlag die Nachbarn! Nehmen Sie sich etwas Zeit und versuchen Sie das folgende Problem zu lösen, *bevor* sie weiterlesen.

> Sie sind in der populären Spielshow »Schlag die Nachbarn!« ins Finale gekommen und müssen die letzte Aufgabe meistern. Ihnen wird eine nicht-leere Folge von Schachteln

module Algorithmics.Neighbours

> präsentiert, die jeweils eine für Sie nicht sichtbare Zahl enthalten. Sie müssen eine Schachtel finden, deren Zahl größer ist als die ihrer Nachbarschachteln. Eine Schachtel zu öffnen kostet 100€. Wenn Sie weniger Geld als Ihre Konkurrenten/Konkurrentinnen ausgeben, gewinnen Sie das Finale!

Schauen wir uns eine konkrete Schachtelfolge an (die uns als laufendes Beispiel dienen wird). Aus Gründen der Übersichtlichkeit beschränken wir uns auf zehn Schachteln — wir können davon ausgehen, dass die Gesamtzahl der Schachteln in der Spielshow wesentlich größer ist.

0	1	2	3	4	5	6	7	8	9
0	4	2	7	6	5	3	9	8	1

(5.2)

Die zehn Schachteln sind von 0 bis 9 durchnummeriert, damit wir uns einfach auf sie beziehen können. Eine der Schachteln mit den Hausnummern 1, 3 oder 7 ist gesucht — jede von ihnen schlägt ihre Nachbarn.

Über den Inhalt der Schachteln wissen wir a priori nichts: Die versteckten Zahlen können beliebig klein sein, beliebig groß sein; die Zahlen können alle verschieden sein oder alle gleich. Die letzte Möglichkeit zwingt uns die umgangssprachliche Formulierung »deren Zahl größer ist« zu präzisieren. Um zu garantieren, dass immer eine Lösung existiert, interpretieren wir »größer« als »$\geqslant$« und *nicht* als »>«. Die Schachtel i schlägt somit ihre Nachbarn genau dann, wenn

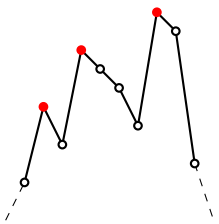
für

	$i-1$	i	$i+1$	
$\cdots$	a	m	b	$\cdots$

gilt: $a \leqslant m \geqslant b$.

Ein zweites Detail bedarf der Klärung: Wann schlagen die Schachteln an den Rändern ihre Nachbarn? Um Spezialfälle zu vermeiden, behelfen wir uns eines Tricks: Wir nehmen an, dass es am linken und am rechten Rand jeweils eine »virtuelle« Schachtel gibt, die $-\infty$ enthält.

−1	0	1	2	3	4	5	6	7	8	9	10
$-\infty$	0	4	2	7	6	5	3	9	8	1	$-\infty$

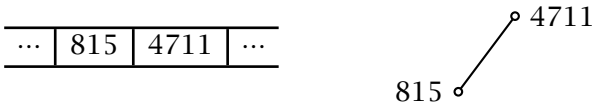


Der Wert $-\infty$ ist keine gültige Zahl *in* Mini-F# (in der Objektsprache); wir verwenden $-\infty$ nur, wenn wir *über* Mini-F# Programme reden (in der Metasprache). Dabei gilt vereinbarungsgemäß $-\infty < n$ für alle ganzen Zahlen n. (Ähnliche Betrachtungen lassen sich für die neu hinzugekommene Hausnummer -1 anstellen. Da wir später im Programm die Schachteln mit den natürlichen Zahlen durchnummerieren, ist -1 keine gültige Hausnummer. Wir verwenden -1 nur, wenn wir über das Programm reden.)

Die Zuordnung von Hausnummern zu Inhalten ist der Natur nach eine endliche Abbildung. Wenn wir ihren Graph plotten (siehe oben; der Übersichtlichkeit halber haben wir die Funktionswerte miteinander verbunden), sehen wir etwas plastischer, wonach wir suchen. Der Graph erinnert an eine Berglandschaft; wir wollen einen Berggipfel besteigen; irgendeinen, nicht notwendigerweise den höchsten Gipfel. Etwas profaner ausgedrückt: Wir suchen ein ***lokales Maximum***, *nicht* ein globales. In unserem Beispiel gibt es insgesamt drei lokale Maxima (und zwei lokale Minima). Um das globale Maximum zu finden, müssen wir notwendigerweise alle Schachteln öffnen. Kommen wir mit weniger Versuchen aus, wenn wir nur ein lokales Maximum suchen?

Das globale Maximum bestimmen wir mit einer linearen Suche; kommen wir für ein lokales Maximum mit der binären Suche ans Ziel? Eine gute Idee, aber nicht unmittelbar zielführend. Wir

öffnen die mittlere Schachtel und sehen, sagen wir, 4711. Was können wir aus dieser Beobachtung schließen? Nichts! Da die Schachteln beliebige Werte enthalten können, benötigen wir einen Referenzwert. Eine vielleicht naheliegende Idee ist, zwei benachbarte Schachteln zu öffnen und aus dem Vergleich ihrer Werte Rückschlüsse über das weitere Vorgehen zu ziehen. Wir öffnen die beiden mittleren Schachteln:



Die positive Steigung verrät, dass wir uns auf einer Flanke links von einem Berggipfel befinden, so dass es naheliegt, rechts von der Mitte weiterzusuchen. Wäre die Steigung negativ, würden wir entsprechend links fortfahren. Das folgende Programm setzt die Idee um.

```
let beat-your-neighbours (box : Nat → Nat) (lower : Nat, upper : Nat) =
  let rec search (l, u) =
    if l = u then u
            else let m = (l + u) ÷ 2
                 if box m ⩽ box (m + 1) then search (m + 1, u)
                                        else search (l,     m)
  in search (lower, upper)
```

Die Schachteln werden durch die Funktion *box* repräsentiert, die Hausnummern im angegebenen Intervall auf die Inhalte abbildet. (Auf diese Weise wird eine endliche Abbildung repräsentiert. Das Intervall gibt den Definitionsbereich an, die Funktion die Zuordnung.)

Die Vorgehensweise ähnelt der binären Suche, ist aber von der »Grundstimmung« eine andere. Bei der binären Suche, so wie bei der Suche in einem binären Suchbaum haben wir in jedem Schritt eine Hälfte des Suchraums ausgeschlossen, da wir garantieren konnten, dass das gesuchte Objekt dort *nicht* zu finden ist (negative Stimmung). Hier suchen wir in der Hälfte weiter, in der die Existenz eines lokalen Maximums garantiert ist (positive Stimmung). In der anderen Hälfte können ebenfalls lokale Maxima existieren, nur garantieren können wir dies eben nicht.

Die Metapher des Bergsteigens lässt plausibel erscheinen, dass das Programm ein lokales Maximum ermittelt. Aber tut es das wirklich? Versuchen wir uns an einem Korrektheitsbeweis. Wir konzentrieren uns auf die Hilfsfunktion *search*, die die eigentliche Arbeit verrichtet.[5] Die Beschreibung des Problems legt nahe, dass

$$box\ (i-1) \leqslant box\ i \geqslant box\ (i+1) \quad \text{wobei} \quad i = search\ (l, u)$$

Leider erfüllt das Programm diese Spezifikation nicht: $search\ (4, 6)$ gibt für unser laufendes Beispiel 4 zurück; der Inhalt der entsprechenden Schachtel, $box\ 4 = 6$, ist aber kein lokales Maximum. Was läuft schief? Im Allgemeinen gibt es drei Möglichkeiten:

1. das Programm ist falsch oder
2. die Spezifikation ist falsch oder
3. beide sind falsch.

In unserem Fall ist die Spezifikation nicht korrekt. Das gewünschte Ergebnis ist an eine Vorbedingung geknüpft: Wir setzen voraus, dass wir uns zwischen einer linken Bergflanke / und einer rechten Bergflanke \ befinden.

$$box\ (l-1) \leqslant box\ l \quad \wedge \quad box\ u \geqslant box\ (u+1)$$

[5] Das Verhältnis zwischen Hauptfunktion und Hilfsfunktionen entspricht dem Verhältnis zwischen Theorem und Lemmata. Letztere machen die ganze Arbeit, während ersteres die Lorbeeren erntet.

Nur wenn diese ***Vorbedingung*** erfüllt ist, dann gilt die obige ***Nachbedingung***. Eine Vorbedingung knüpft Erwartungen an den oder die Parameter einer Funktion. Der/die Aufrufer/-in der Funktion muss diese Bedingung sicherstellen. Eine Nachbedingung beschreibt Eigenschaften des Funktionsresultats — die Funktion selbst muss diese garantieren.

Im Fall einer rekursiven Funktion muss die Vorbedingung für alle rekursiven Aufrufe gelten. Die Parameter mögen sich ändern; die Bedingung bleibt immer erhalten. Aus diesem Grund spricht man auch von einer ***Invariante***.

Invariante von *search* (l, u): $\quad box\,(l-1) \leqslant box\,l \;\wedge\; box\,u \geqslant box\,(u+1)$

Das »Leben« einer Invariante unterteilt sich in drei Phasen:

Invarianten

1. die Invariante wird etabliert (initialer Aufruf);
2. die Invariante wird erhalten (Rekursionsschritt);
3. aus der Invariante folgt das gewünschte Ergebnis (Rekursionsbasis).

Für unser Beispiel ergeben sich die folgenden Überlegungen:
1. Phase: Wir müssen zeigen, dass beim ersten Aufruf der Hilfsfunktion die Invariante etabliert wird, *search* $(lower, upper)$.

$$box\,(lower-1) = -\infty < box\,lower \;\wedge\; box\,upper > -\infty = box\,(upper+1)$$

Hier fließt die Annahme über die virtuellen Schachteln an den Rändern ein.
2. Phase: Wir müssen sicherstellen, dass die zwei rekursiven Aufrufe, *search* $(m+1, u)$ und *search* (l, m), die Invariante erhalten. Die entsprechenden Ungleichungen

$$box\,m \leqslant box\,(m+1) \;\wedge\; box\,u \geqslant box\,(u+1)$$
$$box\,(l-1) \leqslant box\,l \;\wedge\; box\,m \geqslant box\,(m+1)$$

folgen aus der Invariante für *search* (l, u) und der Abfrage $box\,m \leqslant box\,(m+1)$.
3. Phase: Schließlich, und das ist der wichtigste Schritt, müssen wir nachweisen, dass im Basisfall die Invariante die gewünschte Nachbedingung impliziert:

$$box\,(i-1) \leqslant box\,i \geqslant box\,(i+1)$$

folgt aus der Invariante für *search* (l, u) und $l = i = u$.
Abbildung 5.11 stellt die verschiedenen Phasen im Leben unserer Invariante grafisch dar. Man sieht sehr schön, dass die Abfrage $box\,m \leqslant box\,(m+1)$ im nächsten Schritt zu einem Teil der Invariante wird. Bildlich gesprochen werden die linke und die rechte Flanke aufeinander zubewegt, bis sie sich in einem Berggipfel berühren.

Partielle und totale Korrektheit Ist damit die Korrektheit von *beat-your-neighbours* nachgewiesen? Nicht ganz, wir haben lediglich die sogenannte ***partielle Korrektheit*** gezeigt. Für alle zulässigen Eingaben gilt: *Wenn* das Programm terminiert, *dann* produziert es die gewünschte Ausgabe.

Wir werden später sehen, dass *beat-your-neighbours* tatsächlich für alle Eingaben terminiert. Es ist aber ganz lehrreich, sich zu überlegen, was schieflaufen kann. Wenn wir den obigen Beweis Revue passieren lassen, stellen wir fest, dass wir gar nicht von der Tatsache Gebrauch machen, dass der Index m ungefähr in der Mitte zwischen l und u liegt. Ersetzen wir zum Beispiel die lokale

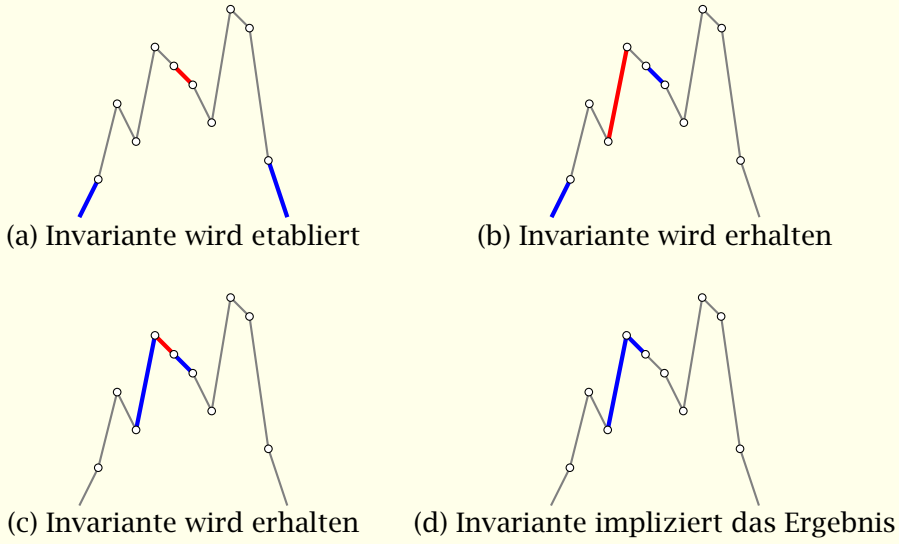


Abbildung 5.11.: Schlag die Nachbarn: Programmablauf von *beat-your-neighbours* für die Eingabe (5.2) — Abfrage jeweils in rot, Invariante in blau.

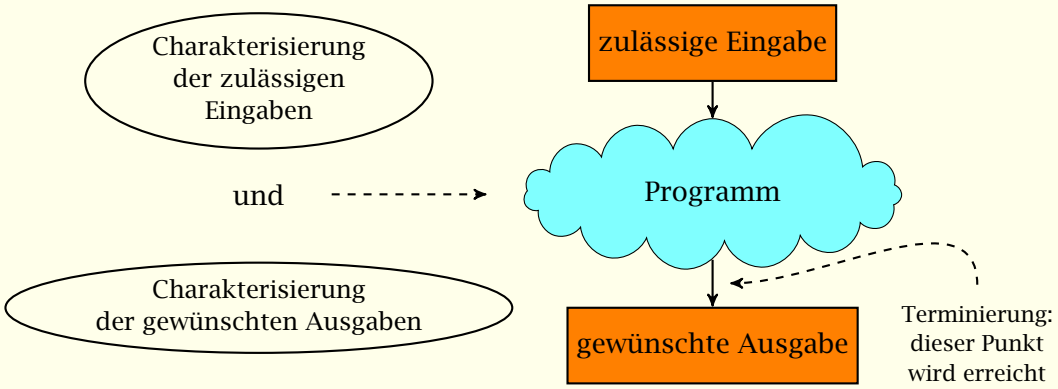


Abbildung 5.12.: Partielle und totale Korrektheit.

Definition ***let*** $m = (l + u) \div 2$ durch ***let*** $m = u$, dann hat der Beweis der partiellen Korrektheit unverändert Bestand. Aber das Programm terminiert nicht mehr für alle Eingaben. Nun ist es vielleicht klar, dass ***let*** $m = u$ keine gute Wahl ist. Terminierungsprobleme können aber auch subtiler daherkommen: Die natürliche Division $a \div b$ rundet nach unten ab, $a \div b = \lfloor a/b \rfloor$; würde sie nach oben runden, $a \div b = \lceil a/b \rceil$, wäre die Terminierung ebenfalls nicht mehr in allen Fällen gewährleistet. (Können Sie ein Beispiel konstruieren?)

Im Allgemeinen sind wir an der ***totalen Korrektheit*** interessiert. Für alle zulässigen Eingaben gilt: Das Programm terminiert *und* es produziert die gewünschte Ausgabe. Um die totale Korrektheit zu zeigen, können wir zum Beispiel einen Induktionsbeweis führen, so wie wir das im Fall von »Sortieren durch Mischen« angedeutet haben. Oder wir teilen uns die Arbeit auf. Wir zeigen in einem ersten Schritt die partielle Korrektheit, etwa mit Hilfe von Invarianten, und kümmern uns dann in einem zweiten Schritt um die Terminierung.

Abbildung 5.12 stellt die Zusammenhänge noch einmal grafisch dar. Es ist wichtig zu betonen, dass die Frage »Ist Programm P korrekt?« für sich isoliert *keinen Sinn* ergibt! Um Aussagen über

die Korrektheit treffen zu können, benötigen wir einen Referenzpunkt, eine ***Spezifikation***, die festlegt, *was* das Programm leisten soll, die unsere Erwartungen an das Programm präzisiert. Ein Programm, das detailliert, *wie* die gewünschten Ergebnisse erzielt werden, ist dann korrekt (oder auch nicht) bezüglich dieser Spezifikation.

Die Spezifikation charakterisiert zum einen die zulässigen Eingaben: statische Eigenschaften mit Hilfe von Typen, dynamische Eigenschaften mit Hilfe von Vorbedingungen. Zum anderen charakterisiert sie die gewünschten Ausgaben: statische Eigenschaften wiederum mit Hilfe von Typen, dynamische Eigenschaften mit Hilfe von Nachbedingungen.

Exerzieren wir die verschiedenen Beweisschritte noch einmal mit einem alten Bekannten durch.

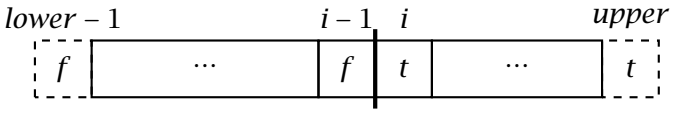
module Algorithmics.BinarySearch

Partielle Korrektheit der binären Suche In Abschnitt 3.6 haben wir uns intensiv mit der Modellierung und Implementierung eines Ratespiels beschäftigt. Sozusagen als Nebenprodukt dieser Auseinandersetzung haben wir eine nützliche Bibliotheksfunktion erhalten: die binäre Suche.

```
let binary-search (oracle : Nat → Bool) (lower : Nat, upper : Nat) : Nat =
  let rec search (l, u) =
    if l ⩾ u then u
             else let m = (l + u) ÷ 2
                  if oracle m then search (l,     m)
                              else search (m + 1, u)
  in search (lower, upper)
```

Der erste Parameter, das sogenannte Orakel, gab ursprünglich zu einem gegebenen n Auskunft, ob die gesuchte Zahl gleich oder kleiner als n ist. Wir haben aber gesehen, dass sich die gesuchte Zahl auch durch eine Formel beschreiben lässt, etwa um die natürliche Quadratwurzel einer Zahl zu berechnen. Im allgemeinen Fall bestimmt die binäre Suche das *kleinste* Argument i, für das *oracle* i wahr ist. Wie können wir diese informelle Spezifikation präzisieren?

Zunächst einmal müssen wir formalisieren, dass das Orakel nicht mogelt. Wenn i das gesuchte Argument ist, dann erwarten wir, dass *oracle* für kleinere Argumente stets *false* und für größere stets *true* zurückgibt. Mit anderen Worten, *oracle* springt nicht willkürlich zwischen den beiden möglichen Funktionswerten *true* und *false* hin und her.



Mathematisch gesehen ist *oracle* eine ***monotone*** Funktion — dabei nehmen wir wie üblich an, dass »falsch« echt kleiner ist als »wahr«: *false* < *true*. Ähnlich wie bei »Schlag die Nachbarn!« machen wir zusätzliche Annahmen über die Ränder: Links ist *oracle* falsch, rechts wahr. Insgesamt stellen wir drei ***Vorbedingungen:***

1. $i \leqslant j \implies \mathit{oracle}\ i \leqslant \mathit{oracle}\ j$ — das Orakel mogelt nicht (Monotonie);
2. $\mathit{lower} \leqslant \mathit{upper}$ — der Suchraum ist nicht leer;
3. $\mathit{oracle}\ (\mathit{lower} - 1) < \mathit{oracle}\ \mathit{upper}$ — eine Lösung existiert stets.

Wenn a und b Boolesche Werte sind, dann bedeutet die Annahme $a < b$ schlicht und einfach, dass a falsch und b wahr ist.

Sind die Vorbedingungen erfüllt, dann garantieren wir die ***Nachbedingung:***

$$\mathit{oracle}\ (i - 1) < \mathit{oracle}\ i \quad \text{wobei} \quad i = \mathit{binary\text{-}search}\ \mathit{oracle}\ (\mathit{lower}, \mathit{upper})$$

Die binäre Suche bestimmt somit die Stelle, an der der Funktionswert von *oracle* umspringt, von *false* auf *true*.

Die Nachbedingung stellt sicher, dass der/die Aufrufer/-in der Bibliotheksfunktion das gewünschte Ergebnis erhält. Der/die Aufrufer/-in hegt aber noch eine weitere Erwartung, die wir noch nicht thematisiert haben. Die Funktion *oracle* repräsentiert zusammen mit dem Intervall $(lower, upper)$ eine endliche Abbildung. Der/die Aufrufer/-in erwartet, dass diese Abbildung nur auf Elemente ihres Definitionsbereichs angewendet wird. Wird die binäre Suche zum Beispiel verwendet, um ein Array zu durchforsten,

$$\mathit{binary\text{-}search}\ (\textbf{\textit{fun}}\ k \to 4711 \leqslant a.[k])\ (0, a.\mathit{Length} - 1)$$

ist die Abbildung tatsächlich für Werte außerhalb des Definitionsbereichs nicht definiert.

Die eigentliche Arbeit erledigt wie so oft eine Hilfsfunktion. Es gilt die algorithmische Idee dieser Funktion, Intervallschachtelung, mit Hilfe einer Invariante einzufangen. Wir müssen bei jedem rekursiven Aufruf, bei jeder Schachtelung sicherstellen, dass der gesuchte Index weiterhin im Suchintervall enthalten ist. Das können wir garantieren, wenn *oracle* am linken Rand falsch und am rechten Rand wahr ist.

1. Invariante von *search* (l, u): $\quad \mathit{oracle}\ (l - 1) < \mathit{oracle}\ u$

Die Invariante ähnelt verdächtig der Nachbedingung, was natürlich kein Zufall ist.

Wir müssen zusätzlich garantieren, dass die Funktion *oracle* nur mit Werten aus ihrem Definitionsbereich aufgerufen wird. Wir fordern, dass die lokalen Intervallgrenzen l und u stets innerhalb der vorgegebenen, globalen Grenzen *lower* und *upper* liegen.

2. Invariante von *search* (l, u): $\quad lower \leqslant l \leqslant u \leqslant upper$

Mit ähnliche Rechnungen wie für »Schlag die Nachbarn!« lassen sich die beiden Invarianten nachweisen, siehe Abbildungen 5.13 und 5.14.

Terminierung der binären Suche Um die totale Korrektheit der binären Suche zu etablieren, steht noch der Nachweis der Terminierung aus. Wir müssen zeigen, dass bei jedem rekursiven Aufruf die Argumente »echt kleiner« werden. Als »Problemgröße« legen wir fest: Die Größe des Intervalls (l, u) ist $u \dot{-} l$.

Um die Terminierung von *search* zu garantieren, müssen wir somit sicherstellen, dass das Intervall (l, u) bei jedem rekursiven Aufruf echt kleiner wird. Im Rekursionsschritt gilt $l < u$; unter dieser Voraussetzung ergeben sich für die Intervallgrößen:

$$\begin{aligned} u \dot{-} (m+1) < u \dot{-} l \quad &\Longleftrightarrow \quad l < m+1 \\ m \dot{-} l < u \dot{-} l \quad &\Longleftrightarrow \quad m < u \end{aligned}$$

Die rechten Seiten folgen jeweils aus der Eigenschaft des »Mittelwerts« m, siehe (5.3).

Verträge: Anforderungen und Garantien Nachdem alle wichtigen Detailfragen geklärt sind, blicken wir noch einmal auf das Zusammenspiel zwischen der Bibliotheksfunktion und ihrem/ihrer Benutzer/-in. Dabei ist die Metapher eines juristischen Vertrags hilfreich. Wir haben zwei Parteien, die ihre Anforderungen (engl. requirements) und ihre Garantien (engl. guarantees) durch einen Vertrag (engl. contract) regeln.

- Der/die Benutzer/-in stellt Anforderungen an das Ergebnis von *binary-search* und
- an die Argumente von *oracle*;

1. Phase: Wir müssen zeigen, dass der initiale Aufruf *search* $(lower, upper)$ die Invariante etabliert:

$$oracle\ (lower - 1) < oracle\ upper$$

Dies folgt unmittelbar aus der 3. Vorbedingung.
2. Phase: Wir müssen sicherstellen, dass die zwei rekursiven Aufrufe, *search* $(m + 1, u)$ und *search* (l, m), die Invariante erhalten. Die entsprechenden Ungleichungen

$$oracle\ m < oracle\ u$$
$$oracle\ (l - 1) < oracle\ m$$

folgen aus der 1. Invariante für *search* (l, u) und der Abfrage *oracle m*.
3. Phase: Wir müssen zeigen, dass die Invariante das gewünschte Ergebnis, die Nachbedingung impliziert. Die Ungleichung

$$oracle\ (i - 1) < oracle\ i$$

folgt aus der 1. Invariante für *search* (l, u) und $l = i = u$. Letzteres folgt aus der Bedingung $l \geqslant u$ und der 2. Invariante.

Abbildung 5.13.: Binäre Suche: Nachweis der 1. Invariante.

1. Phase: Aus der 2. Vorbedingung folgt, dass der initiale Aufruf *search* $(lower, upper)$ die Invariante etabliert. (Zusätzlich verwenden wir, dass »$\leqslant$« reflexiv ist.)
2. Phase: Die rekursiven Aufrufe *search* $(m + 1, u)$ und *search* (l, m) erhalten die Invariante. Die Ungleichungen folgen aus

$$l < u \implies l \leqslant m < m + 1 \leqslant u \quad \text{wobei} \quad m = (l + u) \div 2 \tag{5.3}$$

In den Nachweis fließen Eigenschaften der natürlichen Division ein. Zur Erinnerung: Für den Mittelwert gilt $m = \lfloor (l + u)/2 \rfloor$. (Weiterhin nutzen wir aus, dass »$\leqslant$« transitiv ist.)
3. Phase: Die Invariante in Verbindung mit (5.3) stellt sicher, dass *oracle m* stets definiert ist:

$$lower \leqslant m < upper$$

Wir machen eine interessante Beobachtung: *oracle* wird nie auf die rechte Intervallgrenze angewendet. Dies ist auch nicht notwendig — wir setzen ja voraus, dass *oracle upper* wahr ist.

Abbildung 5.14.: Binäre Suche: Nachweis der 2. Invariante.

- die Bibliotheksfunktion *binary-search* stellt Anforderungen an ihr zweites Argument und
- an die Ergebnisse von *oracle*, ihrem ersten Argument.

Die Gegenseite muss die Anforderungen jeweils garantieren. Im Allgemeinen stellt der/die Benutzer/-in Anforderungen an das Ergebnis; die Bibliotheksfunktion stellt Anforderungen an die Argumente. Für funktionale Argumente wie *oracle* kehren sich Anforderungen und Garantien um! Warum? Nun, der/die Autor/-in einer Funktion formuliert Anforderungen an die Argumente und gibt Garantien für das Ergebnis. Der/die Autor/-in eines funktionalen Arguments wie *oracle* ist aber der/die Benutzer/-in der Bibliotheksfunktion, nicht die Bibliotheksfunktion selbst.

Die Metapher des Vertrags lässt sich noch weiterspinnen. Im Fall einer Vertragsverletzung (engl. contract violation) lässt sich die oder der Schuldige schnell ausmachen: Sind die Anforderungen verletzt, trifft den/die Benutzer/-in die Schuld (engl. blame); werden die Garantien nicht erfüllt, ist die Bibliotheksfunktion zur Rechenschaft zu ziehen. In unserem Beispiel haben wir bewiesen, dass letzteres Problem nicht auftreten kann. Nicht immer lässt sich ein solcher Beweis führen oder mit vertretbarem Aufwand führen. Alternativ kann man Vor- und Nachbedingungen dynamisch beim Rechnen (man sagt auch während der Laufzeit) überprüfen, indem man die Formeln der Metasprache, in der wir die Bedingungen formuliert haben, zu Ausdrücken der Objektsprache macht. Im Fall von Vertragsverletzungen vulgo Programmierfehlern lässt sich dann der Ort der Fehler genau einkreisen. Verträge werden so zu einem integralen Bestandteil beim Entwurf von Programmen, griffig als »design by contract« bezeichnet. Zu diesem Thema erfahren Sie im weiteren Verlauf des Studiums mehr aus der Abteilung »Software Engineering«.

Schlag die Nachbarn, da capo! Beim Beweisen wie beim Programmieren sollte man ein gesundes Misstrauen an den Tag legen. In Beweise als auch in Programme können sich Fehler einschleichen: offensichtliche, subtile, unentdeckte. Eine einfache Plausibilitätsprüfung beim Beweisen besteht darin, zu überprüfen, ob man alle Voraussetzungen, alle Annahmen in dem Beweis auch tatsächlich verwendet hat. Führen wir diese Prüfung für den obigen Korrektheitsbeweis durch, stellen wir (vielleicht) erstaunt fest, dass wir die 1. Vorbedingung, die Annahme, dass das Orakel nicht mogelt, gar nicht benutzt haben!

Ein derartiger Befund kann mehrere Ursachen haben: Der Beweis ist falsch, wir haben ein Detail übersehen; oder das Theorem, das der Beweis zeigt, ist allgemeiner als vermutet. In unserem Beispiel ist letzteres der Fall: Die binäre Suche funktioniert auch wunderbar, wenn das Orakel mogelt!

Wenn das Orakel *nicht* mogelt, die Funktion *oracle* also monoton ist, dann können wir schlussfolgern, dass das Ergebnis i das *kleinste* Argument ist, für das *oracle* i wahr ist. Die Tatsache, dass die binäre Suche den Wert minimiert, ist zum Beispiel für die Berechnung der natürlichen Quadratwurzel essentiell: Das kleinste i mit $n \leqslant i^2$ ist gesucht. Lisa: »Tatsächlich haben wir das größte i mit $i^2 \leqslant n$ gesucht!« Wirklich? Dann müssen wir die Bedingung umschreiben:[6] Wir suchen das kleinste i mit $n < (i+1)^2$.

$$\textit{let}\ \textit{square-root}\ n = \textit{binary-search}\ (\textit{fun}\ k \to n < \textit{square}\ (k+1))\ (0, n)$$

Wir sollten uns noch vergewissern, dass das Orakel tatsächlich monoton ist:

$$i \leqslant j \implies (n < \textit{square}\ (i+1)) \leqslant (n < \textit{square}\ (j+1))$$

Die Ordnung auf den Booleschen Werten ist durch die Implikation gegeben — die Symbole »$\Longrightarrow$« und »$\leqslant$« bezeichnen tatsächlich die gleiche Boolesche Operation. Wir müssen somit zeigen: Wenn

[6] Dabei nutzen wir aus, dass $\mathit{max}\ \{\, n \in \mathbb{Z} \mid \mathrm{P}(n) \,\} = \mathit{min}\ \{\, n \in \mathbb{Z} \mid \neg \mathrm{P}(n+1) \,\}$.

$i \leqslant j$ und $n < \mathit{square}\ (i+1)$ gelten, dann gilt auch $n < \mathit{square}\ (j+1)$. Dies ist der Fall, da *square* auf den natürlichen Zahlen monoton ist.

Wenn das Orakel hingegen mogelt, dann gibt die binäre Suche *irgendein* Argument i mit $\mathit{oracle}\ (i-1) < \mathit{oracle}\ i$ zurück, nicht notwendigerweise das kleinste. Auch für diese Variante haben wir schon einen Anwendungsfall kennengelernt: Schlag die Nachbarn! Und in der Tat: Wenn wir die Arbeitsfunktionen gleichen Namens miteinander vergleichen, stellen wir eine frappierende Ähnlichkeit fest.

```
let rec search (l, u) =
  if l ⩾ u then u
  else
    let m = (l + u) ÷ 2
    if oracle m
      then search (l,     m)
      else search (m + 1, u)
```

```
let rec search (l, u) =
  if l = u then u
  else
    let m = (l + u) ÷ 2
    if box m ⩽ box (m + 1)
      then search (m + 1, u)
      else search (l,     m)
```

Da wir als Vorbedingung $l \leqslant u$ annehmen, sind die beiden Tests $l \geqslant u$ und $l = u$ gleichwertig. Die Zweige der zweiten Alternative lassen sich in Übereinstimmung bringen, indem wir die Bedingung $\mathit{box}\ m \leqslant \mathit{box}\ (m+1)$ negieren. Heureka! Unser Problem »Schlag die Nachbarn!« lässt sich mit Hilfe der binären Suche lösen:

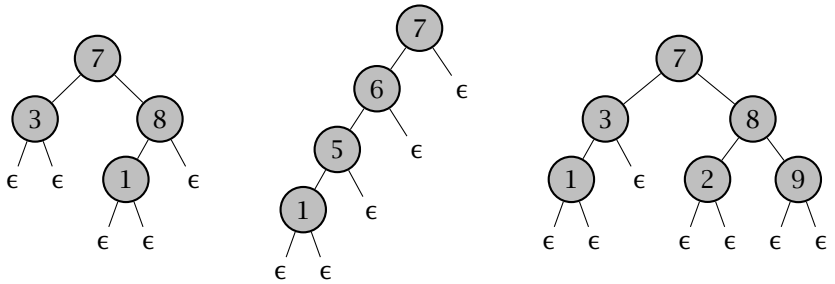
```
let beat-your-neighbours (box : Nat → Nat) =
  binary-search (fun i → box i > box (i + 1))
```

Der/die geneigte Leser/-in sollte sich überzeugen, dass die Vorbedingungen für die binäre Suche tatsächlich erfüllt sind — jede Vorbedingung sollte sich aus den Annahmen für »Schlag die Nachbarn!« herleiten lassen.

Übungen.

1.

(a) Geben Sie zu den folgenden grafischen Darstellungen von Bäumen die zugehörigen Ausdrücke an:



(b) Zeichnen Sie zu den folgenden Ausdrücken die zugehörigen Bäume:

$\mathit{Node}\ (\mathit{Leaf}, 5, \mathit{Leaf})$

$\mathit{Node}\ (\mathit{Node}\ (\mathit{Leaf}, 3, \mathit{Leaf}), 9, \mathit{Node}\ (\mathit{Leaf}, 8, \mathit{Leaf}))$

$\mathit{Node}\ (\mathit{Node}\ (\mathit{Leaf}, 1, \mathit{Node}\ (\mathit{Node}\ (\mathit{Node}\ (\mathit{Leaf}, 2, \mathit{Leaf}), 3, \mathit{Leaf}), 4, \mathit{Leaf})), 5, \mathit{Leaf})$

2. Ein Heap ist ein Binärbaum, der folgende Bedingung erfüllt: Das Element jedes Knotens ist kleiner oder gleich der Elemente seiner Teilbäume. Somit enthält die Wurzel des Heaps stets das kleinste Element. (Die folgende Definition führt ein Typsynonym ein: Der Bezeichner auf der linken Seite ist eine Abkürzung für den Typausdruck auf der rechten Seite.)

```
type Heap = Tree ⟨Nat⟩
```

Schreiben Sie eine Funktion

```
let insert (n : Nat, heap : Heap) : Heap
```

die ein Element in einen Heap einfügt, so dass die Heapeigenschaft erhalten bleibt.

5.3. Endliche Abbildungen

Wenden wir uns wieder dem Projekt aus Abschnitt 5.2.1 zu, der Verwaltung des Personalstamms eines Unternehmens. Zur Erinnerung: Die Stammdaten haben wir durch eine Liste bzw. einen Baum von Einträgen des Typs

```
type Entry = {key : Nat; person : Person}
```

repräsentiert. Wir haben bisher diskutiert, wie man zu einer Personalnummer die entsprechenden Personaldaten heraus*suchen* kann. Neben dem Suchen von Einträgen gibt es eine Reihe weiterer Aufgaben: Zum Beispiel müssen neue Mitarbeiter/-innen zum Personalstamm hinzugefügt werden; umgekehrt wird man einen Eintrag aus dem Personalstamm entfernen, wenn der/die entsprechende Mitarbeiter/-in das Unternehmen verlässt.

Die Zuordnung von Personaldaten zu Personalnummern ist ihrer Natur nach eine endliche Abbildung. Ihr Definitionsbereich wird durch die Menge der aktiven Personalnummern festgelegt; die eigentliche Zuordnung ist implizit durch die jeweils verwendete Datenstruktur gegeben bzw. explizit durch die Funktion *lookup*. Diese Erkenntnis legt nahe, sich von der speziellen Anwendung zu lösen und ganz allgemein endliche Abbildungen zu implementieren. Die Verwaltung von Personaldaten wird durch den Abstraktionsschritt zu einem biederen Spezialfall. Endliche Abbildungen haben vielfältige Anwendungen: Sie lassen sich verwenden, um Bücher nach ISB-Nummern[7], Studierende nach Matrikelnummern oder Telefonnummern nach Spitznamen zu verwalten.

In Abschnitt 2.1 haben wir endliche Abbildungen als Teil des Vokabulars eingeführt, mit dem wir über unsere Programmiersprache reden. Jetzt wollen wir endliche Abbildungen in Mini–F# selbst realisieren. Ähnlich zur Vorgehensweise in Abschnitt 2.1 müssen wir uns zunächst über die ***Schnittstelle*** (engl. interface) Gedanken machen: Welche Operationen wollen wir auf endlichen Abbildungen unterstützen? Inspiriert von unserer ursprünglichen Anwendung legen wir die folgende Schnittstelle fest.

```
type Map⟨'key, 'value when 'key : comparison⟩
val empty    : Map⟨'key, 'value⟩
val add      : 'key * 'value → Map⟨'key, 'value⟩ → Map⟨'key, 'value⟩
val remove   : 'key → Map⟨'key, 'value⟩ → Map⟨'key, 'value⟩
val is-empty : Map⟨'key, 'value⟩ → Bool
val lookup   : 'key → Map⟨'key, 'value⟩ → 'value option
val from-list : ('key * 'value) list → Map⟨'key, 'value⟩
val to-list  : Map⟨'key, 'value⟩ → ('key * 'value) list
```

Da wir von konkreten Anwendungen abstrahieren, werden aus Personalnummern, ISBN-Angaben oder Matrikelnummern ganz allgemein Schlüssel (engl. keys); aus Personaldaten, Büchern und Studierenden werden noch allgemeiner Werte (engl. values). Eine endliche Abbildung bildet somit Schlüssel auf Werte ab. Da wir uns nicht auf konkrete Typen festlegen wollen, ist *Map*, der Typ der

[7] Die Internationale Standardbuchnummer, kurz ISBN für engl. International Standard Book Number, dient der eindeutigen Kennzeichnung von Büchern und anderen Veröffentlichungen.

endlichen Abbildungen, sowohl mit dem Typ der Schlüssel *'key* als auch mit dem Typ der Werte *'value* parametrisiert. Die konkreten Typen für Schlüssel und Werte können je nach Anwendung frei gewählt werden. Mit einer kleinen Einschränkung: Wir setzen voraus, dass sich Schlüssel vergleichen lassen — diese Annahme wird durch den Zusatz ***when*** *'key* : *comparison* ausgedrückt.

Schauen wir uns die Operationen im Detail an. Die Konstante *empty* repräsentiert die leere Abbildung. Mit Hilfe von *add* fügen wir ein Schlüssel-Wert Paar zu einer Abbildung hinzu; *remove* entfernt den Eintrag mit dem angegebenen Schlüssel. Die Funktion *is-empty* überprüft, ob eine endliche Abbildung leer ist. Die Funktion *lookup* verallgemeinert die gleichnamige Operation aus Abschnitt 5.2.1: *lookup* sucht einen Eintrag mit dem angegebenen Schlüssel; ist die Suche erfolgreich, wird der Wert *Some v* zurückgegeben, wobei *v* der mit dem Schlüssel assoziierte Wert ist; schlägt die Suche fehl, wird *None* zurückgegeben. Schließlich stellen wir noch Funktionen zur Verfügung, um eine Liste von Schlüssel-Wert Paaren in eine endliche Abbildung zu konvertieren und umgekehrt. Mit der Funktion *from-list* lässt sich zum Beispiel der Personalstamm aus Abschnitt 5.2.1 einfach in eine endliche Abbildung überführen.

```
let team = from-list [{key = 7;    person = ralf   };
                      {key = 815;  person = melanie};
                      {key = 4711; person = julia  };
                      {key = 4712; person = andres }]
```

Alternativ können wir den Personalstamm auch peu à peu mit Hilfe der Operationen *empty* und *add* aufbauen.

```
let team = empty |> add (7,    ralf   )
                 |> add (815,  melanie)
                 |> add (4711, julia  )
                 |> add (4712, andres )
```

Die Definition verwendet den vordefinierten Operator »|>« für die Postfixapplikation: $x \mid\!> f$ ist alternative Syntax für $f\ x$. Also: *add* $(7, \mathit{ralf})$ wird auf *empty* angewendet; auf das Ergebnis wird *add* $(815, \mathit{melanie})$ angewendet und so weiter.

Ist damit die Bedeutung der Operationen geklärt? Nicht ganz, welche endliche Abbildung bezeichnet zum Beispiel *empty* |> *add* (`"Lisa"`, 4711) |> *add* (`"Lisa"`, 815)? Da Elemente des Typs *Map* endliche Abbildungen repräsentieren, liegt es nahe, die Semantik der Operationen präzise mit Hilfe der Konstrukte aus Abschnitt 2.1 zu beschreiben:

Die leere Abbildung $\varnothing$ wird durch *empty* repräsentiert. Repräsentiert *fm* die endliche Abbildung φ, dann repräsentiert *add* (k, v) *fm* die Erweiterung von φ um $\{k \mapsto v\}$. Wir erinnern uns: Erweiterungen notieren wir mit dem Kommaoperator: $\varphi, \{k \mapsto v\}$. Mit anderen Worten, im Fall von Überschneidungen wird dem »neuen« Eintrag (k, v) Vorrang eingeräumt. Umgekehrt repräsentiert *remove k fm* die Einschränkung von φ auf *dom* $\varphi - \{k\}$, notiert $\varphi - \{k\}$. Repräsentiert *fm* die endliche Abbildung φ, dann testet *is-empty fm*, ob $\varphi = \varnothing$. (Wann sind zwei endliche Abbildungen gleich?) Die Anwendung einer endlichen Abbildung wird durch *lookup* realisiert: *lookup k fm* ergibt *Some* $(\varphi(k))$, wenn $k \in$ *dom* φ und *None* anderenfalls. Unsere Schnittstelle stellt übrigens keine Operation zur Verfügung, um den Definitionsbereich einer endlichen Abbildung direkt zu bestimmen; diesen erhält man nur etwas indirekt mit Hilfe von *to-list*.

Syntax	Semantik
fm	φ
empty	$\varnothing$
add (k, v) *fm*	$\varphi, \{k \mapsto v\}$
remove k fm	$\varphi - \{k\}$
is-empty fm	$\varphi = \varnothing$

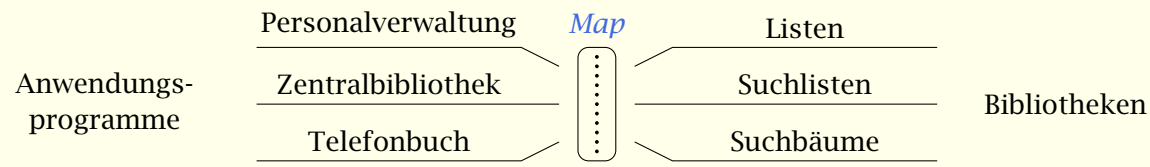


Abbildung 5.15.: Anwendungsprogramme und Bibliotheken »kommunizieren« über eine genormte Schnittstelle.

Die obige Schnittstelle beschreibt, *was* wir mit Elementen des Typs *Map* machen können. Wir haben noch nicht diskutiert, *wie* wir den Typ *Map* und die zugehörigen Operationen konkret realisieren. Wir werden im Folgenden drei Implementierungen der Schnittstelle vorstellen. Bevor wir uns den Details zuwenden, lohnt es sich, die Idee einer Schnittstelle noch einmal genauer zu beleuchten.

Abstrakte Datentypen Der Typ *Map* ist ein Beispiel für einen sogenannten ***abstrakten Datentyp*** (ADT). Zu einem abstrakten Datentyp gehört

- eine ***Schnittstelle*** (engl. interface), die die verfügbaren Typen und Operationen beschreibt (»was«), und
- eine oder mehrere ***Implementierungen*** (engl. implementations), die die Typen und Operationen realisieren (»wie«).

Wohldefinierte Schnittstellen sind in der Softwareentwicklung wie im täglichen Leben nahezu unverzichtbar. Eines der Paradebeispiele für gutes Schnittstellendesign ist *SchuKo* (kurz für Schutz-Kontakt), unser System von Steckern und Steckdosen für die Stromversorgung. Über die genormte Schnittstelle lassen sich verschiedenste elektrische Geräte in weiten Teilen Europas mit Strom versorgen. Solange sich Stromverbraucher und Stromerzeuger an die Schnittstellenvereinbarung halten, spielt es keine Rolle, welches Gerät mit Strom versorgt wird (Kühlschrank, Rasenmäher oder Rechner) oder wie der Strom erzeugt wird (Dieselaggregat, Batterie oder Windkraftanlage).

In der Softwareentwicklung werden aus Stromerzeugern *Bibliotheken*, die eine Schnittstelle implementieren, und aus Stromverbrauchern *Anwendungsprogramme*, die auf die Dienste einer Bibliothek zurückgreifen. Die Vorteile einer Schnittstelle bleiben erhalten: Viele verschiedene Anwendungsprogramme können die gleiche Schnittstelle verwenden; diese kann durch unterschiedliche Bibliotheken realisiert werden, siehe Abbildung 5.15. Die Trennung in Bibliotheken und Anwendungsprogramme (die tatsächlich nicht zu eng zu verstehen ist) ist mit einem beträchtlichen Gewinn an ***Modularität*** verbunden: Beide können unabhängig voneinander entwickelt werden; Bibliotheken lassen sich leicht austauschen; von den Verbesserungen einer Bibliothek profitieren viele Anwendungsprogramme. Die Vorteile kommen auch zum Tragen, wenn es nur eine Anwendung und nur eine Bibliothek gibt. Es ist stets eine gute Idee, Implementierungsdetails hinter einer Schnittstelle zu verbergen.

In den letzten Kapiteln haben wir sowohl konkrete als auch abstrakte Datentypen kennengelernt. Beide »Arten« von Typen verfolgen grundverschiedene Ansätze:

- ein konkreter Datentyp wird durch seine Elemente definiert;
- ein abstrakter Datentyp wird durch seine Operationen definiert.

Ein konkreter Datentyp ist die Summe seiner Elemente. Record- und Variantentypen führen konkrete Typen ein. Die jeweilige Typdefinition beschreibt präzise, welche Elemente der definierte Typ enthält.

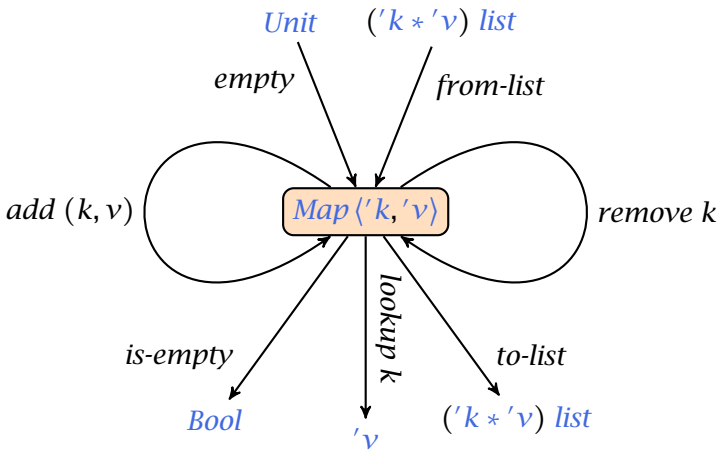
Ein abstrakter Datentyp ist die Summe seines Verhaltens. Die Elemente des ADTs werden nicht offenbart — sie sind abstrakt. Die ersten Typen, die wir eingeführt haben, *Bool* und *Nat*, sind der Natur nach abstrakte Datentypen. Wir haben Operationen festgelegt und präzise beschrieben, mit deren Hilfe wir Wahrheitswerte und natürliche Zahlen konstruieren und analysieren können. Wie diese tatsächlich implementiert werden, verschließt sich uns — die Details sind hinter der jeweiligen Schnittstelle verborgen.

Ein abstrakter Datentyp wird in der Regel durch einen konkreten Datentyp realisiert: Wahrheitswerte können durch einen binären Variantentyp implementiert werden, siehe Abschnitt 4.2.1; für natürliche Zahlen haben wir zwei mögliche Implementierungen diskutiert, eine die auf der unären Zahlendarstellung (*Peano*) und eine die auf der binären Zahlendarstellung (*Leibniz*) basiert, siehe Abschnitt 4.2.2.

Schnittstellen nehmen eine zentrale Rolle bei der Entwicklung von Software ein. Aus diesem Grund sollte ihr Design wohlüberlegt sein. Nachträgliche Änderungen einer Schnittstelle oder unterschiedliche, inkompatible Schnittstellen (andere Steckersysteme für die Stromversorgung im Ausland) sind im besten Fall nur ärgerlich. In der Regel kosten die daraus resultierenden Anpassungen von Anwendungsprogrammen und Bibliotheken Zeit und Geld. Es empfiehlt sich, zumindest eine einfache *Plausibilitätsprüfung* durchzuführen: Die Schnittstelle eines abstrakten Datentyps sollte Operationen bereitstellen

- um Elemente des abstrakten Datentyps zu *konstruieren*;
- um Elemente des abstrakten Datentyps in andere Elemente zu *transformieren*;
- um Elemente des abstrakten Datentyps zu *analysieren*.

Alle drei Aspekte finden sich in der Schnittstelle für endliche Abbildungen wieder. Die Operationen *empty* und *from-list* konstruieren; *add* und *remove* transformieren; und *is-empty*, *lookup* und *to-list* analysieren.



Genug der Vorüberlegungen — wenden wir uns der Implementierung der Schnittstelle zu. In den Abschnitten 5.2.1–5.2.3 haben wir uns mögliche Organisationsformen für endliche Abbildungen angeschaut: Listen, Suchlisten und Suchbäume. Diese greifen wir in den folgenden Abschnitten wieder auf und erweitern sie zu Implementierungen des abstrakten Datentyps *Map*.

5.3.1. Listen

Die einfachste Darstellung von endlichen Abbildungen ist eine ungeordnete Liste von sogenannten ***Schlüssel-Wert Paaren*** (engl. key-value pairs).


```
type Entry ⟨'key, 'value⟩ =
  {key : 'key; value : 'value}
type Map ⟨'key, 'value when 'key : comparison⟩ =
  | Rep of List ⟨Entry ⟨'key, 'value⟩⟩
```

Der Recordtyp *Entry* verallgemeinert den gleichnamigen Typ aus Abschnitt 5.2.1: Das anwendungsspezifische Label *person* haben wir in *value* umbenannt; der Typ ist jetzt sowohl mit dem Schlüsseltyp als auch mit dem Typ der assoziierten Werte parametrisiert.

Die zweite Typdefinition gibt an, wie der abstrakte Typ *Map* konkret implementiert wird. Wir verwenden einen 1-Variantentyp, um den abstrakten Typ und den konkreten Typ einfach auseinander halten zu können (siehe Abschnitt 4.2.1). Der einzige Konstruktor des Typs, *Rep* (engl. für representation), überführt die konkrete Repräsentation, eine ungeordnete Liste von Schlüssel-Wert Paaren, in ein Element des abstrakten Typs, eine endliche Abbildung. *Kurz: list* ist konkret, *Rep list* ist abstrakt. Die endliche Abbildung $\{Anja \mapsto Spaghetti, Ralf \mapsto Pizza\}$ aus Abschnitt 2.1 wird zum Beispiel durch `[{key = "Anja"; value = "Spaghetti"}; {key = "Ralf"; value = "Pizza"}]` repräsentiert — wenn wir Personen und Gerichte durch Zeichenketten darstellen.

Die leere Abbildung wird entsprechend durch die leere Liste implementiert; das Hinzufügen durch »::« — wir müssen lediglich das Paar in ein Record verwandeln.

```
let empty = Rep [ ]
let is-empty (Rep list) = List.is-empty list
let add (key, value) (Rep list) = Rep ({key = key; value = value} :: list)
let lookup key (Rep list) =
  let rec search = function
  | [ ]                 → None
  | entry :: entries → if key = entry.key then Some entry.value
                                          else search entries
  in search list
```

Viele listenverarbeitende Funktionen wie zum Beispiel *is-empty* sind in dem vordefinierten Modul *List* zusammengefasst; mit Hilfe der Punktnotation können die Bibliotheksfunktionen aufgerufen werden. Ein weiteres technisches Detail: Das Muster *Rep list* ist unwiderlegbar; aus diesem Grund können wir es ohne Bedenken als formalen Parameter verwenden.

Die Funktion *lookup*, die wir schon aus Abschnitt 5.2.1 kennen, gibt den Wert des *ersten* Eintrags mit dem passenden Schlüssel zurück. Da *add* vorne, nicht hinten einfügt, werden im Fall von Überschneidungen auf diese Weise den »neueren« Einträgen Vorrang eingeräumt:
lookup 4711 (*add* (4711, `"yes"`) (*add* (4711, `"no"`) *empty*)) ist *Some* `"yes"`, nicht *Some* `"no"`. Mit anderen Worten, der erste Eintrag (4711, `"no"`) wird durch den zweiten Eintrag (4711, `"yes"`) verschattet. Semantisch gesehen entspricht *add* (*key*, *value*) *fm* der Anwendung des Kommaoperators: $\varphi, \{key \mapsto value\}$. So soll es sein, so haben wir es bei der Beschreibung der Schnittstelle festgelegt — jede Implementierung muss diese Vorgaben buchstabengetreu umsetzen.

Beim Entfernen von Einträgen müssen wir aufpassen: Da mehrere Einträge mit dem gleichen Schlüssel auftreten können, müssen wir stets die gesamte Liste durchlaufen. Das ist sozusagen der Preis für die einfache Implementierung von *add*.

```
let remove key (Rep list) =
  let rec del = function
  | [ ]              → [ ]
  | entry :: entries → if key = entry.key then del entries
                                          else entry :: del entries
  in Rep (del list)
```

Wie im Fall von *lookup*, delegiert die Funktion *remove* die eigentliche Arbeit an eine »Arbeiterfunktion« (engl. worker function): *del* arbeitet auf den konkreten Werten, auf der Repräsentation einer endlichen Abbildung; *remove* arbeitet auf den abstrakten Werten.

Die Operationen *from-list* und *to-list* müssen Paare in Einträge verwandeln und umgekehrt.

```
let from-list list =
  Rep (List.map (fun (key, value) → { key = key; value = value }) list)
let to-list (Rep list) =
  List.map (fun entry → (entry.key, entry.value)) list
```

Die vordefinierte Funktion *map* wendet die angegebene Funktion, erstes Argument, auf jedes Element der Liste, zweites Argument, an: *map f* bildet $[x_1; x_2; \ldots; x_n]$ auf $[f\ x_1; f\ x_2; \ldots; f\ x_n]$ ab.

5.3.2. Suchlisten

module Algorithmics.Map.OrdList

Alternativ können wir eine endliche Abbildung durch eine Liste von Schlüssel-Wert Paaren darstellen, die nach dem Schlüssel geordnet ist und die keine zwei Einträge mit dem gleichen Schlüssel enthält. (Die eindeutige Identifizierbarkeit definiert in der Theorie der relationalen Datenbanken gerade einen »Schlüssel«.)

```
type Map ⟨'key, 'value when 'key : comparison⟩ =          // geordnet, ohne Duplikate
  | Rep of List ⟨Entry ⟨'key, 'value⟩⟩
```

Die Typdefinition ändert sich nicht, da wir die zusätzlichen Eigenschaften leider nicht in Mini–F# ausdrücken können. Die geforderten Eigenschaften werden zu einer ***Invariante*** des Typs: Alle Funktionen, die Argumente vom Typ *Map* $\langle' k, 'v\rangle$ entgegennehmen, dürfen annehmen, dass die Invariante gilt; alle Funktionen, die Elemente vom Typ *Map* $\langle' k, 'v\rangle$ zurückgeben, müssen garantieren, dass die Invariante erfüllt ist — daher der Begriff »Invariante«.

Die leere Abbildung wird weiterhin durch die leere Liste implementiert; das Hinzufügen ist jetzt ein Einfügen, wie beim »Sortieren durch Einfügen«.

```
let empty = Rep [ ]
let is-empty (Rep list) = List.is-empty list
let add (key, value) (Rep list) =
  let new-entry = {key = key; value = value}
  let rec ins = function
  | [ ]                → [new-entry]
  | entry :: entries → if   key < entry.key   then new-entry :: entry :: entries
                       elif key = entry.key   then new-entry :: entries
                       (* key > entry.key *) else  entry :: ins entries
  in Rep (ins list)
let lookup key (Rep list) =
  let rec search = function
  | [ ]                → None
  | entry :: entries → if key < entry.key      then None
                       elif key = entry.key    then Some entry.value
                       (* key > entry.key *) else  search entries
  in search list
```

Der 2-Wege Vergleich aus dem letzten Abschnitt ist jeweils einem 3-Wege Vergleich gewichen. Letzterer ist typisch für die Verarbeitung von sortierten Listen *ohne* Duplikate: Beim Einfügen müssen wir Duplikate eliminieren (der neue Eintrag ersetzt den alten); beim Suchen können wir frühzeitig Misserfolg signalisieren. Das Löschen von Einträgen verwendet das exakt gleiche Rekursionsmuster.

```
let remove key (Rep list) =
  let rec del = function
  | [ ]                → [ ]
  | entry :: entries → if   key < entry.key   then entry :: entries
                       elif key = entry.key   then entries
                       (* key > entry.key *) else  entry :: del entries
  in Rep (del list)
```

Die Konvertierungsfunktion *from-list* hat jetzt einen Haufen Arbeit: Sie muss sicherstellen, dass die Liste nach dem Schlüssel geordnet ist und keine Duplikate enthält.

```
let from-list list =
  Rep (List.map (fun (key, value) → {key = key; value = value})
        (List.distinct-by fst
          (List.sort-by fst list)))
let to-list (Rep list) =
  List.map (fun entry → (entry.key, entry.value)) list
```

Die Liste von Schlüssel-Wert Paaren wird zunächst nach dem Schlüssel sortiert, dann werden Duplikate entfernt, und schließlich werden die Paare in Einträge überführt. Die Bibliotheksfunktionen *sort-by* und *distinct-by* erwarten keine Quasiordnung als Argument, sondern eine »Projektionsfunktion«. Die zugrundeliegende Quasiordnung »$\preccurlyeq$« wird von der Projektionsfunktion f abgeleitet: $x \preccurlyeq y \iff f\ x \leqslant f\ y$.

Eine stilistische Anmerkung: Die Definition von *from-list* verwendet auf der rechten Seite vierfach geschachtelte Funktionsaufrufe. Wenn man die resultierenden Klammergebirge vermeiden möchte, kann man alternativ den Operator »|>« für die Postfixapplikation verwenden. Zur Erinnerung: Statt $f\ x$ schreibt man $x \mid\!> f$; das Argument wird vor die Funktion gesetzt. Der Vorteil

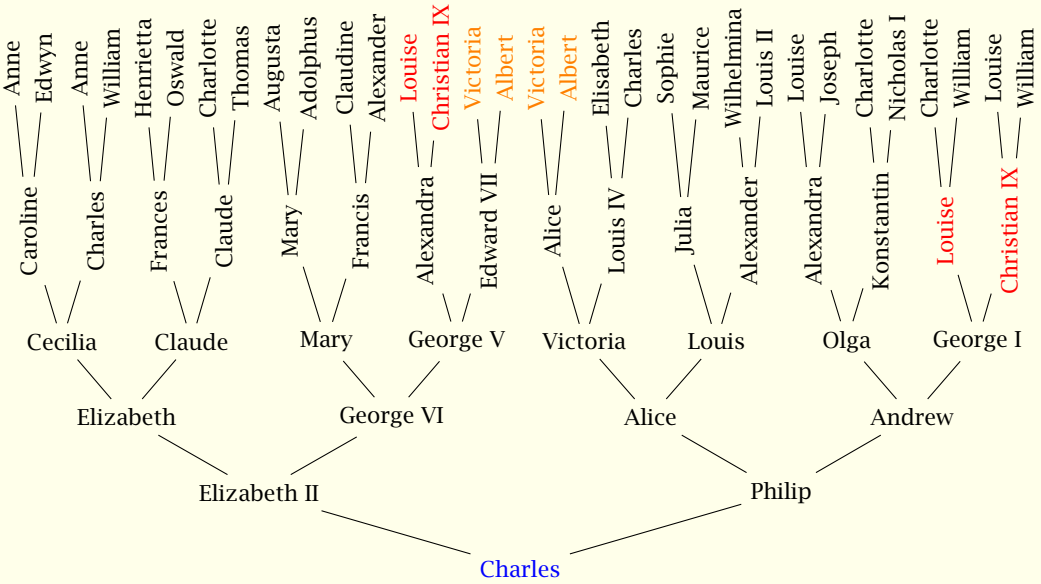


Abbildung 5.16.: Stammbaum von Charles Philip Arthur George, Prince of Wales (Quelle [Knu97, Fig.18(a)]).

erschließt sich, wenn man Applikationen schachtelt: Statt $h\ (g\ (f\ x))$ formuliert man $x |> f |> g |> h$. Im Fall von *from-list* erhalten wir:

```
let from-list list =
  list |> List.sort-by      fst
       |> List.distinct-by fst
       |> List.map          (fun (key, value) → {key = key; value = value})
       |> Rep
```

Wir haben eine Verarbeitungspipeline vor uns: *list* wird in die Pipeline gepumpt und dann in vier Schritten zu einer endlichen Abbildung verarbeitet.

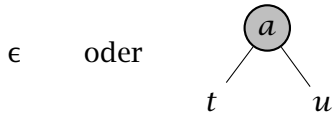
Fassen wir zusammen: Die Konstruktoren eines abstrakten Datentyps müssen die Invariante etablieren; die Transformationen müsssen die Invariante erhalten; die Nutznießerinnen sind die Funktionen, die Elemente des Datentyps analysieren. Im Zusammenspiel dieser drei Parteien entscheidet sich, ob eine Invariante gewinnbringend ist. In unserem Fall ist der Gewinn eher bescheiden: Die (erfolglose) Suche wird beschleunigt, das Einfügen hingegen entschleunigt.

5.3.3. Binäre Suchbäume

module Algorithmics.Tree
module Algorithmics.Map.SearchTree

Neben Listen und Suchlisten haben wir uns Suchbäume als Organisationsform für endliche Abbildungen angeschaut. Bäume im Allgemeinen sind uns in der Vorlesung schon wiederholt begegnet: als abstrakte Syntaxbäume, Beweisbäume, Entscheidungsbäume und Rekursionsbäume. Binäre Bäume lassen sich als fleischgewordene Rekursionsbäume deuten, genauer als die Rekursionsbäume der binären Suche. (Die Rekursionsbäume der linearen Suche sind entsprechend lineare Listen.) Eine Kontrollstruktur wird sozusagen in eine Datenstruktur verwandelt. Neben der naheliegenden Verwendung als Suchstruktur haben Binärbäume noch viele weitere Anwendungen — man verwendet sie zum Beispiel als Stammbäume (siehe Abbildung 5.16), Kodierungsbäume oder Turnierbäume — so dass wir uns die Datenstruktur noch einmal in Ruhe anschauen wollen.

Binärbäume Binärbäume sind induktiv definiert: Ein *binärer Baum* ist entweder ein leeres Blatt oder ein Knoten, der aus einem linken Baum, einem Element und einem rechten Baum besteht. Wenn wir Binärbäume zeichnen, verwenden wir den griechischen Buchstaben ϵ, unser Symbol für die leere Sequenz, für Blätter und Kreise für Knoten.



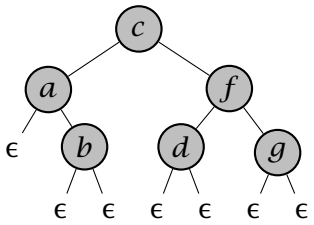
Das Element wird dabei üblicherweise in den Kreis geschrieben — deswegen spricht man auch von einer Knotenmarkierung. In der grafischen Darstellung lässt man die Blätter aus Gründen der Lesbarkeit oft auch weg.

Die induktive Definition entspricht exakt der rekursiven Variantentypdefinition, die wir bereits eingeführt haben.

```
type Tree⟨'elem⟩ =
  | Leaf
  | Node of Tree⟨'elem⟩ * 'elem * Tree⟨'elem⟩
```

Wie Listen sind auch Binärbäume Container: Sie enthalten Elemente. Je nach Typparameter haben wir Bäume von natürlichen Zahlen, *Tree⟨Nat⟩*, Bäume von Zeichenketten, *Tree⟨String⟩*, oder hochkomplexe Gebilde vor uns, etwa *Tree⟨List⟨Tree⟨String⟩⟩⟩*.

Der Binärbaum auf der linken Seite wird durch den Ausdruck bzw. Wert auf der rechten Seite repräsentiert.




```
Node (Node (Leaf,
            "a",
            Node (Leaf, "b", Leaf)),
      "c",
      Node (Node (Leaf, "d", Leaf),
            "f",
            Node (Leaf, "g", Leaf)))
```

Die hierarchische Baumstruktur wird in der linearen Notation etwas unvollkommen durch Einrückung angedeutet. (Das kennen wir von Mini-F# Programmen selbst: Die hierarchische Struktur der abstrakten Syntax wird in der konkreten Syntax idealerweise durch Einrückung reflektiert.) In der Informatik wachsen Bäume typischerweise von oben nach unten, das heißt Bäume werden mit der Wurzel nach oben gezeichnet. Eine Ausnahme haben wir schon kennengelernt: Beweisbäume. Auch Stammbäume werden biologisch korrekt gemalt, siehe Abbildung 5.16.

Nicht zuletzt aufgrund ihrer Popularität gibt es eine Vielzahl von Begriffen, um über Binärbäume zu reden. Nehmen wir den obigen Baum als Beispiel:

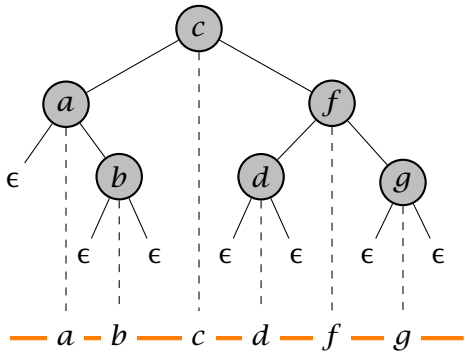
- Der Knoten c ist die ***Wurzel*** des Baums; die leeren Teilbäume sind die ***Blätter***.
- Alle Knoten, mit Ausnahme der Wurzel, haben einen ***Vorgänger***[8]: Der Vorgänger von d ist f; der Vorgänger von f wiederum ist die Wurzel c.
- Knoten können ***Nachfolger*** oder ***Kinder*** haben: f hat die Kinder d und g; der Knoten d hat keine Kinder; a hat ein Kind.

[8] In älteren Informatiktexten wird auch der Begriff Vaterknoten verwendet.

- Die Knoten a und f sind ***Geschwister***; d und g sind ebenfalls Geschwister; b hat keine Geschwister.

Man sieht, die Terminologie ist eine krude Mischung aus Verwandtschaftsbeziehungen (Kind, Geschwister), biologischen Begriffen (Wurzel, Blatt) und Begriffen aus der Graphentheorie (Knoten, Vorgänger, Nachfolger). Leider ist die Terminologie nicht einheitlich: Zum Beispiel werden Knoten, die keine Kinder haben (in unserem laufenden Beispiel b, d und g) oft auch als Blätter bezeichnet. (Gelegentlich sind die Bezeichnungen auch paradox oder irreführend: In Abbildung 5.16 hat der Wurzelknoten »Charles« zwei Kinder: »Elizabeth II« und »Philip«.)

Binäre Suchbäume Sind die Elemente eines Binärbaums von links nach rechts geordnet, spricht man von einem ***binären Suchbaum***. Unser laufendes Beispiel ist ein solcher binärer Suchbaum:




```
Node (Node (Leaf,
            "a",
            Node (Leaf, "b", Leaf)),
      "c",
      Node (Node (Leaf, "d", Leaf),
            "f",
            Node (Leaf, "g", Leaf)))
```

In der linearen Notation lässt sich die Suchbaumeigenschaft besonders einfach überprüfen. In der grafischen Darstellung projiziert man die Elemente auf eine horizontale Linie. Im Fall eines Suchbaums erhalten wir eine aufsteigend geordnete Sequenz.[9]

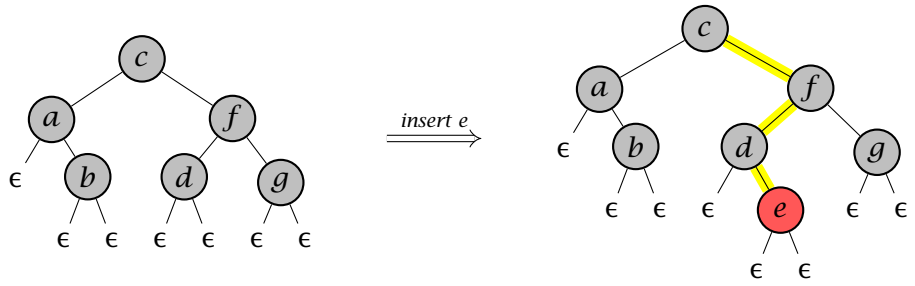
Die Suchbaumeigenschaft lässt sich alternativ auch direkt anhand der Struktur eines Binärbaums festmachen. Für alle Knoten muss gelten, dass die Elemente im linken Teilbaum kleiner sind als das Element in der Wurzel und, in symmetrischer Weise, dass die Elemente im rechten Teilbaum größer sind als das Element in der Wurzel. (Je nach Anwendung meint »kleiner« tatsächlich entweder »<« oder »⩽«.) Auf diese Weise dient das Wurzelelement als *Wegweiser* bei der Suche.

```
// contains : 'key → Tree⟨'key⟩ → Bool  when 'key : comparison
let contains key = function
  | Leaf          → false
  | Node (l, x, r) → if   key < x   then contains key l
                     elif key = x   then true
                     (* key > x *) else  contains key r
```

Die Funktion *contains* überprüft, ob ein Element in einem Binärbaum enthalten ist. Sie ist die Mutter aller Algorithmen auf Suchbäumen. Fast alle anderen Algorithmen orientieren sich an ihrem Rekursionsmuster.

Wie Listen können wir auch Bäume ohne allzu großen Aufwand wachsen oder schrumpfen lassen. So wie wir ein Element in eine Suchliste einfügen, so können wir ein Element in einen Suchbaum einfügen. Dabei folgen wir dem Suchpfad bis zu einem Blatt und ersetzen dieses durch einen Knoten. Wenn wir zum Beispiel e in unseren Binärbaum einfügen, gehen wir erst nach rechts, dann nach links und schließlich wieder nach rechts.

[9] Ob das tatsächlich klappt, hängt von der Zeichnung ab: Schieben wir in unserem Beispiel b ganz nah an d heran, so wechseln b und c möglicherweise die Positionen.

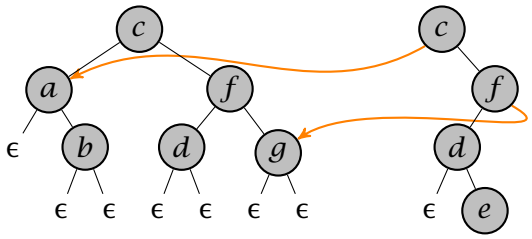


Die algorithmische Idee lässt sich direkt in eine Rechenregel überführen.

```
// insert : 'key → Tree⟨'key⟩ → Tree⟨'key⟩ when 'key : comparison
let rec insert key = function
  | Leaf           → Node (Leaf, key, Leaf)
  | Node (l, x, r) → if   key < x  then Node (insert key l, x, r)
                     elif key = x  then Node (l, key, r)
                     (* key > x *) else  Node (l, x, insert key r)
```

Ein Blatt wird auf einen Minibaum abgebildet, einen Knoten mit leeren Teilbäumen und dem einzufügenden Element als Markierung. Wenn der Schlüssel kleiner ist als der Wegweiser, wird rekursiv in den linken Teilbaum eingefügt. Genauer: Es wird ein Knoten zurückgegeben, der den gleichen rechten Teilbaum und die gleiche Markierung enthält und dessen linker Teilbaum das Ergebnis des rekursiven Aufrufs ist.

Für jeden Knoten entlang des Suchpfades wird somit ein neuer Knoten angelegt. Die Teilbäume, die nicht traversiert werden, sind sowohl Teilbäume im ursprünglichen Baum (der Eingabe) als auch Teilbäume des erweiterten Baums (der Ausgabe). Im Englischen spricht man auch von »sharing«. Es ergibt sich das folgende, interessante Bild:



Das »Teilen« von Datenstrukturen ist bedeutsam, wenn man genauer untersucht, wieviel Speicherplatz für einen Wald benötigt wird. Der Bedarf hängt nicht nur von der Größe der einzelnen Bäume ab, sondern auch vom Grad des »Teilens«. So lässt sich unter Umständen ein Baum von exponentieller Größe in linearem Platz unterbringen, siehe Aufgabe 5.3.3.

Implementierung der Schnittstelle Wenden wir uns nach diesen Vorüberlegungen der Implementierungsarbeit zu. Als Repräsentation wählen wir jetzt Bäume von Einträgen.

```
type Map⟨'key, 'value when 'key : comparison⟩ =
  | Rep of Tree⟨Entry⟨'key, 'value⟩⟩

let empty = Rep Leaf

let is-empty (Rep tree) =
  match tree with
  | Leaf           → true
  | Node (_, _, _) → false
```

Die Funktion *lookup* leitet sich mehr oder weniger direkt von der Funktion *contains* ab, der Mutter aller Algorithmen auf Suchbäumen.

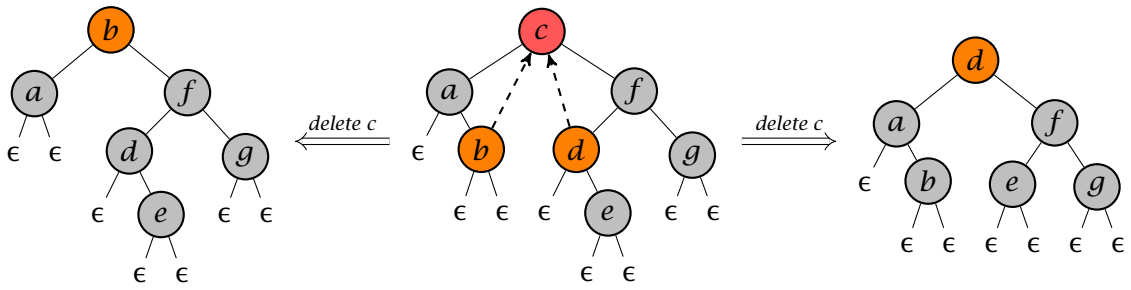
```
let lookup key (Rep tree) =
  let rec search = function
  | Leaf                      → None
  | Node (left, entry, right) → if   key < entry.key   then search left
                                elif key = entry.key   then Some entry.value
                                (* key > entry.key *) else  search right
  in search tree
```

An die Stelle des Ergebnistyps *Bool* ist der Typ *Option* getreten. Wenn man möchte, kann man optionale Werte als konstruktive Varianten der Wahrheitswerte ansehen. Anstatt die Frage »Kennen Sie den Weg zum Audimax?« etwas schroff mit »Ja!« oder »Nein!« zu beantworten, sagt man im positiven Fall »Ja! Betreten Sie das Gebäude durch den Haupteingang, dann halten Sie sich links …«. An die Stelle des Wahrheitswerts *false* tritt *None*, an die Stelle von *true* tritt *Some v*, wobei *v* das erfragte Objekt ist, sozusagen der »Beweis« für die positive Antwort.

Die Schnittstellenfunktion *add* delegiert die Arbeit an eine Arbeitsfunktion, die das eigentliche Einfügen übernimmt. Wie immer achten wir darauf, dass keine zwei Einträge mit dem gleichen Schlüssel vorkommen. Im Fall von Überschneidungen wird wie gefordert dem neuen Eintrag Vorrang eingeräumt.

```
let add (key, value) (Rep tree) =
  let new-entry = {key = key; value = value}
  let rec insert = function
  | Leaf                      → Node (Leaf, new-entry, Leaf)
  | Node (left, entry, right) → if   key < entry.key then Node (insert left, entry, right)
                                elif key = entry.key then Node (left, new-entry, right)
                                (*key > entry.key*) else  Node (left, entry, insert right)
  in Rep (insert tree)
```

Wenden wir uns der nächsten Aufgabe zu, dem Entfernen eines Elements. Entfernen ist im Allgemeinen aufwändiger als Einfügen. Dies ist der Tatsache geschuldet, dass das zu entfernende Element möglicherweise mitten im Baum liegt. (Beim Einfügen operieren wir immer an den Rändern.) Zwei Fälle sind zu unterscheiden: Wenn der Knoten, der das Element enthält, einen leeren Teilbaum besitzt, dann können wir den Knoten einfach durch den anderen Teilbaum ersetzen. Also, *Node* (*Leaf*, *x*, *r*) wird zu *r* und *Node* (*l*, *x*, *Leaf*) entsprechend zu *l*, wobei *x* das zu löschende Element ist. Schwieriger wird es, wenn keiner der Teilbäume leer ist. Dieser Fall liegt zum Beispiel vor, wenn wir das Element *c* in unserem laufenden Beispiel entfernen.



Eine vielleicht naheliegende Idee ist, das zu löschende Element durch ein anderes zu ersetzen. Da wir die Suchbaumeigenschaft nicht kompromittieren dürfen, gibt es genau zwei Wahlmöglichkeiten: das größte Element im linken Teilbaum *oder* das kleinste Element im rechten Teilbaum, den

sogenannten ***Inorder-Vorgänger*** bzw. ***Inorder-Nachfolger***. (Wenn wir die Elemente auf eine horizontale Linie projizieren, sind dies die Elemente direkt vor bzw. direkt hinter dem zu löschenden Element.) Wir entscheiden uns willkürlich für die erste Variante.

Die Funktion *split-max* bestimmt das größte Element in dem angegebenen Binärbaum und gibt zusätzlich den Baum ohne dieses Element zurück. Wie *split-min* vom »Sortieren durch Auswählen«, returniert *split-max* ein optionales Paar. Wenn der Baum leer ist, das heißt ein Blatt vorliegt, dann existiert kein Maximum.

```
// split-max : Tree ⟨'elem⟩ → (Tree ⟨'elem⟩ * 'elem) option
let rec split-max = function
  | Leaf            → None
  | Node (l, a, r)  → Some (match split-max r with
                              | None           → (l, a)        // einfacher Fall: r ist leer
                              | Some (r', max) → (Node (l, a, r'), max))
// (><) : Tree ⟨'elem⟩ → Tree ⟨'elem⟩ → Tree ⟨'elem⟩
let (><) l r =
  match split-max l with
  | None           → r          // einfacher Fall: l ist leer
  | Some (l', max) → Node (l', max, r)
```

Die Operation >< konkatentiert zwei Binärbäume; was *append* bzw. »@« für Listen ist, ist >< für Binärbäume. Keine der beiden Funktionen setzt übrigens voraus, dass die Elemente geordnet sind. Die Funktionen arbeiten problemlos mit Nicht-Suchbäumen; *split-max* bestimmt in diesem Fall das letzte, nicht das größte Element.

Nach diesen Vorarbeiten geht die Implementierung von *remove* leicht von der Hand.

```
let remove key (Rep tree) =
  let rec delete = function
  | Leaf                      → Leaf
  | Node (left, entry, right) → if   key < entry.key then Node (delete left, entry, right)
                                elif key = entry.key then left >< right
                                (*key > entry.key*) else  Node (left, entry, delete right)
  in Rep (delete tree)
```

Wir entfernen den zu löschenden Eintrag und konkatenieren die beiden Teilbäume.

Die Konvertierungsfunktionen sind aufwändiger denn je. Die Funktion *from-list* überführt die Liste von Schlüssel-Wert Paaren zunächst in eine Suchliste, die von der noch zu definierenden Funktion *balanced-tree* in einen Suchbaum überführt wird. Umgekehrt überführt *inorder* einen Suchbaum in eine Suchliste, die sodann in eine Liste von Schlüssel-Wert Paaren überführt wird.

```
let from-list list =
  list |> List.sort-by      fst
       |> List.distinct-by  fst
       |> List.map          (fun (key, value) → {key = key; value = value})
       |> balanced-tree
       |> Rep
let to-list (Rep tree) =
  tree |> inorder
       |> List.map (fun entry → (entry.key, entry.value))
```

Mit der Implementierung der Funktionen *balanced-tree* und *inorder* beschäftigen wir uns im nächsten Abschnitt.

Kommen wir zur Analyse der Laufzeit. Wir haben in Abschnitt 5.2.3 gesehen, dass die Laufzeit von *lookup* proportional zur Höhe des Binärbaums ist. Da *add* und *remove* dem Rekursionsmuster von *lookup* folgen, erben sie auch ihr Laufzeitverhalten. (Was lässt sich über die Laufzeit von *split-min* und >< aussagen?) Das ist eine gute und eine schlechte Nachricht.

Der/die Klient/-in einer Bibliothek interessiert sich zunächst einmal dafür, wie die Laufzeit von der Gesamtzahl der Einträge abhängt, also von der *Größe* der jeweiligen Binärbäume, nicht von der Höhe. (Die Höhe ist eine spezifische Eigenschaft von Suchbäumen, keine, die für alle denkbaren Implementierungen von endlichen Abbildungen Sinn ergibt.)

Die gute Nachricht ist, dass sich die Höhe im besten Fall logarithmisch zur Größe verhält: In einem Binärbaum der Höhe h lassen sich $2^h - 1$ Einträge unterbringen.

Die schlechte Nachricht ist, dass die Höhe im schlechtesten Fall linear zur Größe ist. Ist einer der Teilbäume jeweils leer, dann degeneriert der Suchbaum zu einer Suchliste mit den entsprechenden Konsequenzen für die Laufzeit.

Die wirklich schlechte Nachricht ist, dass der schlechteste Fall nicht unbedingt selten auftritt. Mit den Operationen der Schnittstelle lässt sich leicht ein degenerierter Baum konstruieren, zum Beispiel indem nacheinander Einträge mit aufsteigendem Schlüssel eingefügt werden:

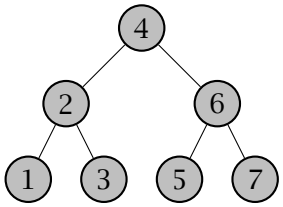
$$\mathit{empty} \mid\!> \mathit{add}\ (0, \texttt{"n"}) \mid\!> \mathit{add}\ (1, \texttt{"e"}) \mid\!> \mathit{add}\ (2, \texttt{"z"}) \mid\!> \mathit{add}\ (3, \texttt{"d"}) \mid\!> \mathit{add}\ (4, \texttt{"v"})$$

Wie lässt sich dieses Problem beheben? Man kann beim Einfügen und beim Löschen Sorge tragen, dass die Binärbäume nicht zu sehr in Schieflage geraten. Ein spezielles Balancierungsschemata wird im nächsten Abschnitt vorgestellt. Mehr zu diesem Thema erfahren Sie in der Vorlesung »Algorithmen und Datenstrukturen«. Ein kleiner Lichtblick: Verwendet die Anwendung *from-list* für die initiale Konstruktion einer endlichen Abbildung und anschließend *add* und *remove* nur sehr sporadisch, dann sind Suchbäume tatsächlich sehr viel effizienter als Suchlisten.

5.3.4. 2-3-Bäume ⋆

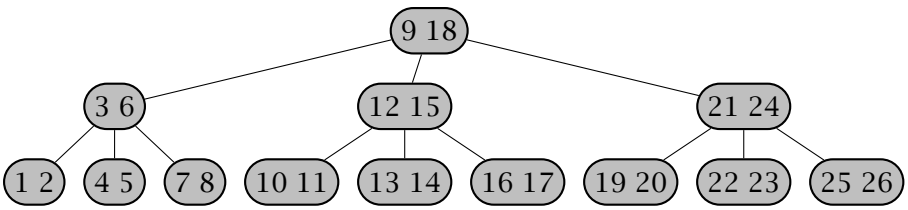
module Algorithmics.Tree23
module Algorithmics.Map.SearchTree23

Wir haben im letzten Abschnitt gesehen, dass Binärbäume die Suche erheblich beschleunigen — sofern sie nicht zu Listen degenerieren. Im Idealfall suchen wir in einem vollständig ausgeglichenen Binärbaum, in einem ***perfekten*** Binärbaum.



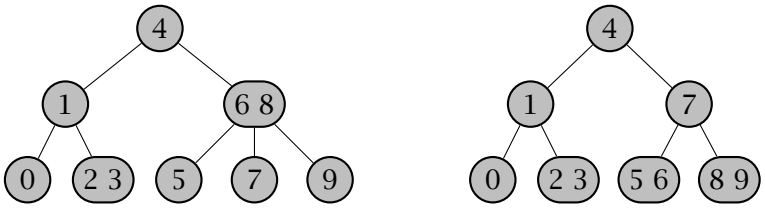
Leider können wir kein Element einfügen oder entfernen, ohne die perfekte Balance zu stören. Aber, wie lässt sich eine Unwucht, eine ungleichmäßige Verteilung der Elemente verhindern, wenn Binärbäume dynamisch wachsen und schrumpfen?

Werden wir kreativ. Als Informatiker/-in fixiert man sich manchmal zu sehr auf das Binäre: 0 und 1, falsch und wahr, weiß und schwarz, Yin und Yang, … Als Erschaffer/-innen unser eigenen Welten sind wir natürlich nicht auf Binärbäume eingeschränkt, wir können alternativ zum Beispiel ***Ternärbäume*** für die Suche in Betracht ziehen.

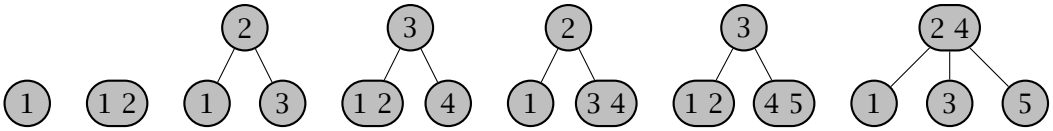


Ein Binärknoten besteht aus zwei Teilbäumen und einem Element; entsprechend besteht ein ***Ternärknoten*** aus drei Teilbäumen und zwei Elementen. (Allgemein besteht ein n-Knoten aus n Teilbäumen und $n-1$ Elementen.) Ein perfekter Binärbaum der Höhe h enthält genau 2^h-1 Elemente, im Beispiel ganz oben: $2^3-1=7$; ein perfekter Ternärbaum enthält entsprechend 3^h-1 Elemente, im Beispiel oben: $3^3-1=26$.

Für sich betrachtet sind allerdings sowohl perfekte Binärbäume als auch perfekte Ternärbäume zu starr, zu unflexibel. Wir gewinnen allerdings erheblich an Flexibilität, wenn wir erlauben, die verschiedenen Knotentypen zu mischen.



Wir erhalten eine neue Spezies: Ein ***2-3-Baum*** besteht aus 2-Knoten und 3-Knoten und ist stets vollständig ausgeglichen. Alle Blätter befinden sich auf der gleichen Ebene, alle Pfade von der Wurzel zu einem Blatt sind gleich lang. Die folgenden Diagramme zeigen alle möglichen Formen bis zu einer Größe von 5.



Zwei Formen der Größe 5 sind möglich: Die Wurzel ist entweder ein 2-Knoten mit zwei 3-Knoten als Kindern oder ein 3-Knoten mit drei 2-Knoten (die kleine Baumarithmetik: $3+3=2\cdot 3=3\cdot 2=2+2+2$). Sind Sie überzeugt, dass sich für jede Größe ein 2-3-Baum konstruieren lässt? Ist die Mischung aus 2- und 3-Knoten hinreichend flexibel? Grübeln Sie ruhig etwas, bevor Sie weiterlesen.

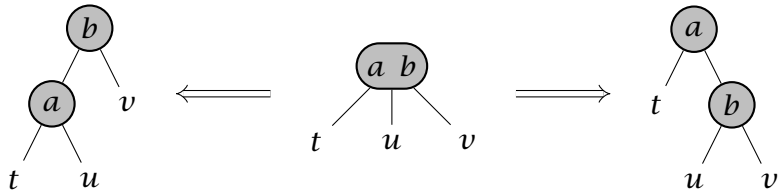
Der Datentyp für 2-3-Bäume erweitert im Prinzip die Typdefinition für Binärbäume um einen weiteren Konstruktor.

```
type Tree23 ⟨'a⟩ =
  | Leaf
  | Node2 of Tree23 ⟨'a⟩ * 'a * Tree23 ⟨'a⟩
  | Node3 of Tree23 ⟨'a⟩ * 'a * Tree23 ⟨'a⟩ * 'a * Tree23 ⟨'a⟩
```

Mit diesem Vokabular lassen sich zum Beispiel die 2-3-Bäume bis zur Größe 5 wie folgt repräsentieren — in der graphischen Darstellung sind die leeren Teilbäume unsichtbar.

```
Node2 (Leaf, 1, Leaf)
Node3 (Leaf, 1, Leaf, 2, Leaf)
Node2 (Node2 (Leaf, 1, Leaf), 2, Node2 (Leaf, 3, Leaf))
Node2 (Node3 (Leaf, 1, Leaf, 2, Leaf), 3, Node2 (Leaf, 4, Leaf))
Node2 (Node2 (Leaf, 1, Leaf), 2, Node3 (Leaf, 3, Leaf, 4, Leaf))
Node2 (Node3 (Leaf, 1, Leaf, 2, Leaf), 3, Node3 (Leaf, 4, Leaf, 5, Leaf))
Node3 (Node2 (Leaf, 1, Leaf), 2, Node2 (Leaf, 3, Leaf), 4, Node2 (Leaf, 5, Leaf))
```

Suchen Sämtliche Beispiele, die wir bisher betrachtet haben, sind ***2-3-Suchbäume***. Die Suchbaumeigenschaft lässt sich am einfachsten an der linearen Darstellung festmachen: Von links nach rechts gelesen bilden die Elemente eine sortierte Folge. Ternäre Knoten werden so gehandhabt als beständen sie aus zwei ineinander geschachtelten binären Knoten:



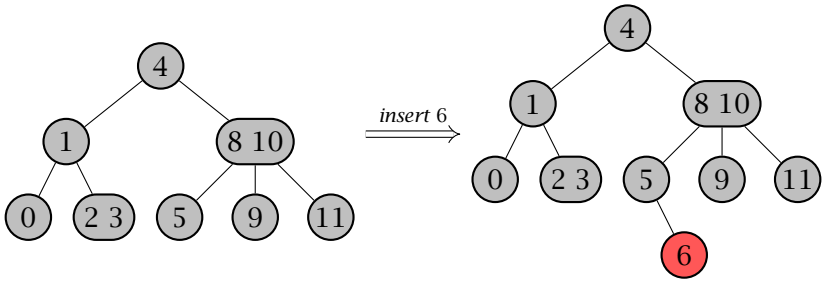
(5.4)

Die Elemente in t sind höchstens so groß wie a, die Elemente in u liegen zwischen a und b und die Elemente in v sind mindestens so groß wie b. Wie bei Binärbäumen dienen die Elemente als *Wegweiser* bei der Suche. Apropos Suche. Die Mutter aller Algorithmen auf 2-3-Suchbäumen erweitert die gleichnamige Funktion aus Abschnitt 5.3.3 um einen Fall für 3-Knoten.

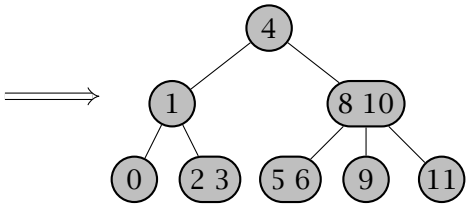
```
type Map ⟨'key, 'value when 'key : comparison⟩ =
  | Rep of Tree23 ⟨Entry ⟨'key, 'value⟩⟩
let lookup key (Rep tree) =
  let rec search = function
    | Leaf                          → None
    | Node2 (t, a, u)     when key < a.key → search t
    | Node2 (t, a, u)     when key = a.key → Some   a.value
    | Node2 (t, a, u)     (* key > a.key *) → search u
    | Node3 (t, a, u, b, v) when key < a.key → search t
    | Node3 (t, a, u, b, v) when key = a.key → Some   a.value
    | Node3 (t, a, u, b, v) when key < b.key → search u
    | Node3 (t, a, u, b, v) when key = b.key → Some   b.value
    | Node3 (t, a, u, b, v) (* key > a.key *) → search v
  search tree
```

Ein zusätzlicher Fall stimmt natürlich nicht so ganz, eigentlich sind es *fünf* Fälle, einen für jeden der fünf Komponenten eines 3-Knoten — so wie wir im Falle eines 2-Knotens mit seinen drei Komponenten drei Fälle unterscheiden. (Wir kombinieren Muster und Bedingungen mit Hilfe von ***when***, um die Symmetrie der Fälle zu betonen.)

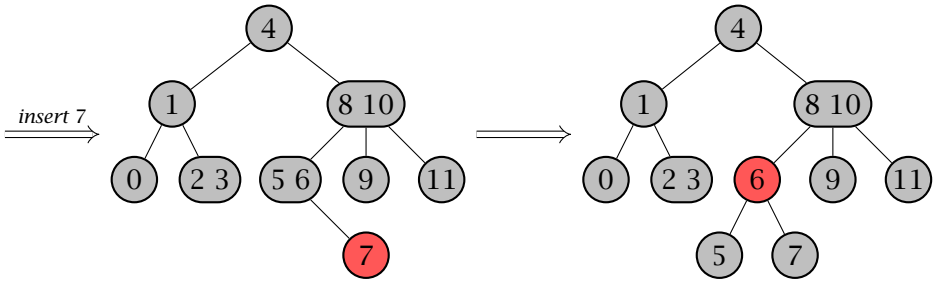
Einfügen Kommen wir zum dynamischen Teil, dem Einfügen. Die Herausforderung besteht darin, eine *globale* Invariante — alle Blätter befinden sich auf der gleichen Ebene — durch *lokale* Transformationen zu erhalten — beim Einfügen bewegen wir uns sehr lokal entlang des Suchpfads von der Wurzel zu einem Blatt. Wenn wir ein Element einfügen, einen leeren Teilbaum durch einen Minibaum ersetzen,



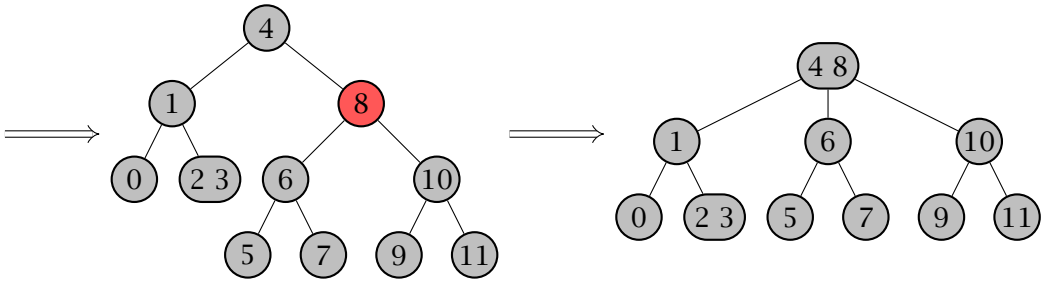
dann ist die Invariante unmittelbar verletzt — angezeigt durch einen rot markierten Knoten. Die Verletzung lässt sich leicht beheben: Der rote Knoten ist Kind eines 2-Knotens, den wir zu einem 3-Knoten vergrößern können (die Arithmetik der 2-3-Bäume: 2 + 1 = 3).



Fügen wir in unmittelbarer Nähe ein weiteres Element ein, so müssten wir der Logik folgend den 3-Knoten zu einem 4-Knoten erweitern (Baumarithmetik: 3 + 1 = 4). Unglücklicherweise haben 2-3-Bäume keine 4-Knoten im Angebot, so dass wir den *virtuellen* 4-Knoten durch einen Minibaum bestehend aus drei 2-Knoten repräsentieren.



Die Wurzel des Minibaums ist rot markiert, da die Invariante weiterhin verletzt ist. Wir haben das Problem der Unwucht nicht gelöst, sondern nur eine Ebene nach oben verschoben. Der rot markierte Knoten ist wiederum Kind eines 3-Knoten so dass wir das gleiche Manöver auf der nächsthöheren Ebene wiederholen.



Jetzt befindet sich der rote Knoten unterhalb eines 2-Knotens, den wir zu einem 3-Knoten erweitern und damit die Transformationen abschließen können.

Abbildung 5.17 fasst die Transformationen zusammen. Die roten Markierungen zeigen jeweils Verletzungen der Invariante an: Teilbäume, deren Wurzel rot markiert ist, sind um eine Ebene zu hoch. Die Verletzungen werden behoben, indem 2-Knoten zu 3-Knoten und 3-Knoten zu *virtuellen* 4-Knoten erweitert werden.

Das Einfügen in einen 2-3-Baum lässt sich konzeptionell in zwei Phasen unterteilen: In der ersten Phase wird die Einfügeposition bestimmt (rekursiver Abstieg); in der zweiten Phase werden die nötigen Rebalancierungen durchgeführt (beim rekursiven Aufstieg). Für die Implementierung der Baumtransformationen verwenden wir sogenannte ***clevere Konstruktoren***, die an Stelle der eigentlichen Datenkonstruktoren zum Einsatz kommen. Ein cleverer Konstruktor konstruiert Daten, erledigt dabei aber noch kleinere Arbeiten, in unserem Fall kümmert er sich um die Rebalancierungen.

Um mögliche Verletzungen der Invariante einfach nachhalten zu können, führen wir einen maßgeschneiderten Datentyp ein.

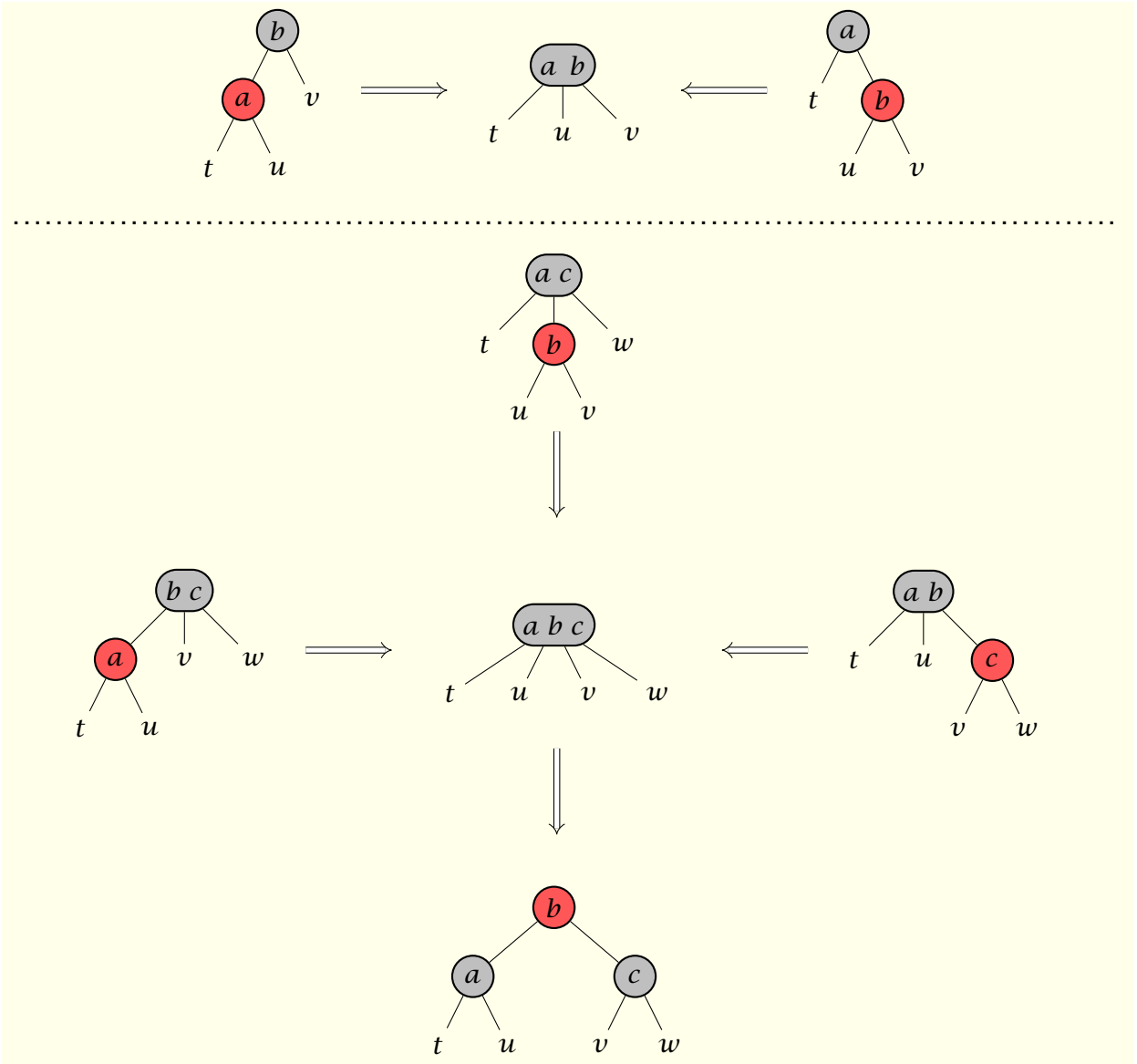


Abbildung 5.17.: 2-3-Bäume: Lokale Baumtransformationen zur Rebalancierung.

```
type Grown⟨'a⟩ =
  | Zero of Tree23⟨'a⟩
  | Succ of Tree23⟨'a⟩ * 'a * Tree23⟨'a⟩          // roter Knoten
```

Elemente des Typs repräsentieren Teilbäume, die durch eine Einfügeoperation *möglicherweise* gewachsen sind: *Zero t* zeigt an, dass die Höhe nicht verändert wurde; *Succ* (t, a, u) entspricht einem roten Knoten und signalisiert Höhenwachstum. Jede der fünf Transformationen aus Abbildung 5.17 wird durch einen cleveren Konstruktor implementiert.

```
node2₁ : Grown⟨'a⟩ * 'a * Tree23⟨'a⟩ → Tree23⟨'a⟩
node2₂ : Tree23⟨'a⟩ * 'a * Grown⟨'a⟩ → Tree23⟨'a⟩

node3₁ : Grown⟨'a⟩ * 'a * Tree23⟨'a⟩ * 'a * Tree23⟨'a⟩ → Grown⟨'a⟩
node3₂ : Tree23⟨'a⟩ * 'a * Grown⟨'a⟩ * 'a * Tree23⟨'a⟩ → Grown⟨'a⟩
node3₃ : Tree23⟨'a⟩ * 'a * Tree23⟨'a⟩ * 'a * Grown⟨'a⟩ → Grown⟨'a⟩

root   : Grown⟨'a⟩ → Tree23⟨'a⟩
```

Die cleveren Konstruktoren »schauen nach unten« zu einem ihrer Teilbäume: Wenn die Höhe des Teilbaums unverändert ist, dann verhalten sie sich wie der entsprechende Datenkonstruktor. Wird aber Höhenwachstum signalisiert, dann setzen sie die Transformationen aus Abbildung 5.17 um.

```
let node2₁ = function
  | (Zero t, a, u)          → Node2 (t, a, u)
  | (Succ (t, a, u), b, v)  → Node3 (t, a, u, b, v)
let node2₂ = function
  | (t, a, Zero u)          → Node2 (t, a, u)
  | (t, a, Succ (u, b, v))  → Node3 (t, a, u, b, v)
```

Im zweiten Fall wird jeweils aus dem 2-Knoten ein 3-Knoten; der rote Knoten verschwindet.

```
let node3₁ = function
  | (Zero t, a, u, b, v)          → Zero (Node3 (t, a, u, b, v))
  | (Succ (t, a, u), b, v, c, w)  → Succ (Node2 (t, a, u), b, Node2 (v, c, w))
let node3₂ = function
  | (t, a, Zero u, b, v)          → Zero (Node3 (t, a, u, b, v))
  | (t, a, Succ (u, b, v), c, w)  → Succ (Node2 (t, a, u), b, Node2 (v, c, w))
let node3₃ = function
  | (t, a, u, b, Zero v)          → Zero (Node3 (t, a, u, b, v))
  | (t, a, u, b, Succ (v, c, w))  → Succ (Node2 (t, a, u), b, Node2 (v, c, w))
```

Im zweiten Fall wird jeweils aus dem 3-Knoten ein virtueller 4-Knoten; der rote Knoten wird nach oben propagiert. Die Funktion *root* wird schließlich verwendet, um einen roten Knoten, der bis zur Wurzel aufgestiegen ist, zu entfärben.

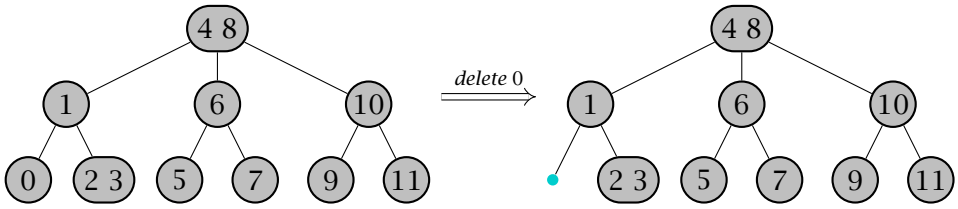
```
let root = function
  | Zero t          → t                  // Höhe ist unverändert
  | Succ (t, a, u)  → Node2 (t, a, u)    // 2-3-Baum ist gewachsen
```

Die Einfügeoperation erweitert die gleichnamige Funktion aus Abschnitt 5.3.3 um die Behandlung von 3-Knoten.

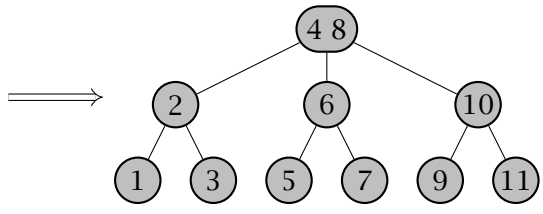
```
let add (key, value) (Rep tree) =
  let new-entry = {key = key; value = value}
  let rec insert = function
    | Leaf                                  → Succ (Leaf, new-entry, Leaf)
    | Node2 (t, a, u)      when key < a.key → Zero (node2₁ (insert t, a, u))
    | Node2 (t, a, u)      when key = a.key → Zero (Node2 (t, new-entry, u))
    | Node2 (t, a, u)      (* key > a.key *) → Zero (node2₂ (t, a, insert u))
    | Node3 (t, a, u, b, v) when key < a.key → node3₁ (insert t, a, u, b, v)
    | Node3 (t, a, u, b, v) when key = a.key → Zero (Node3 (t, new-entry, u, b, v))
    | Node3 (t, a, u, b, v) when key < b.key → node3₂ (t, a, insert u, b, v)
    | Node3 (t, a, u, b, v) when key = b.key → Zero (Node3 (t, a, u, new-entry, v))
    | Node3 (t, a, u, b, v) (* key > b.key *) → node3₃ (t, a, u, b, insert v)
  Rep (root (insert tree))
```

Die Arbeiterfunktion *insert* bildet einen 2-3-Baum vom Typ *Tree23* auf einen möglicherweise gewachsenen Baum vom Typ *Grown* ab. Durch das Typsystem wird sichergestellt, dass wir jeweils die passenden (cleveren) Konstruktoren verwenden. So geben wir im Basisfall *Succ* (*Leaf*, *new-entry*, *Leaf*) zurück, um zu signalisieren, dass der neue Knoten aus dem Baum herausragt. Die zweite Phase wird durch die cleveren Konstruktoren realisiert; vergleichen sie den Code für Binärbäume mit dem für 2-3-Bäume: Aus dem Aufruf *Node2* (*insert t*, *a*, *u*) in Abschnitt 5.3.3 wird hier *Zero* (*node2*$_1$ (*insert t*, *a*, *u*)) — der clevere Konstruktor *node2*$_1$ verarbeitet den rekursiven Aufruf; *Zero* zeigt an, dass der Teilbaum nicht gewachsen ist. In jedem Schritt wird sorgsam die Höhendifferenz nachgehalten.

Löschen Entfernen ist dual zum Einfügen: Beim Einfügen wachsen 2-Knoten zu 3-Knoten und 3-Knoten zu virtuellen 4-Knoten; beim Löschen schrumpft ein 3-Knoten zu einem 2-Knoten und ein 2-Knoten zu einem virtuellen 1-Knoten. Führen wir unser laufendes Beispiel weiter: Wenn wir das Element 0 entfernen,

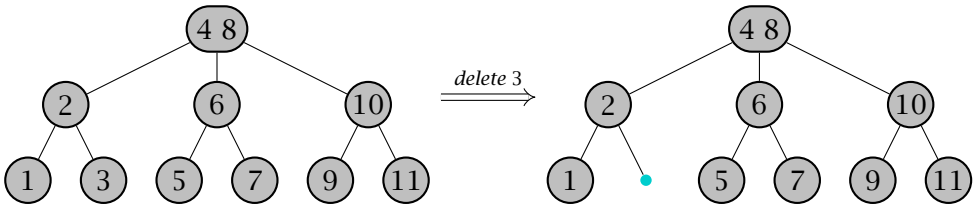


dann ist die Invariante unmittelbar verletzt — angezeigt durch einen blauen[10] 1-Knoten. Zur Erinnerung: Ein 1-Knoten hat genau einen Teilbaum (hier einen unsichtbaren leeren Baum), enthält aber kein Element. Das fehlende Element versuchen wir von das Elter[11] oder den Geschwistern zu stehlen. Im unserem Beispiel ist das Geschwister ein 3-Knoten, so dass wir zwei 2-Knoten bilden können.

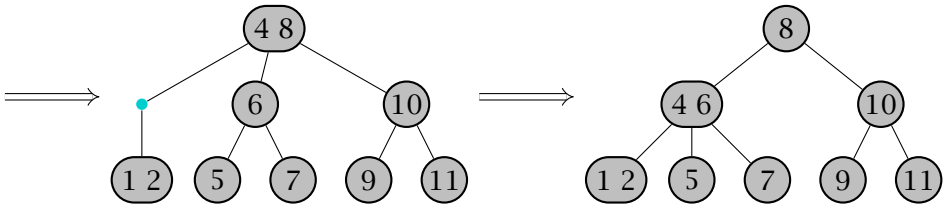


[10] Die Logik der Farben: Rot suggeriert Wärme und zeigt an, dass ein Teil zu dicht ist, zu viele Elemente enthält; blau suggeriert Kälte und signalisiert, dass ein Teil zu licht ist, zu wenig Elemente enthält.
[11] Elter ist der nur fachsprachlich verwendete Singular von Eltern.

Als nächstes entfernen wir die Zahl 3.



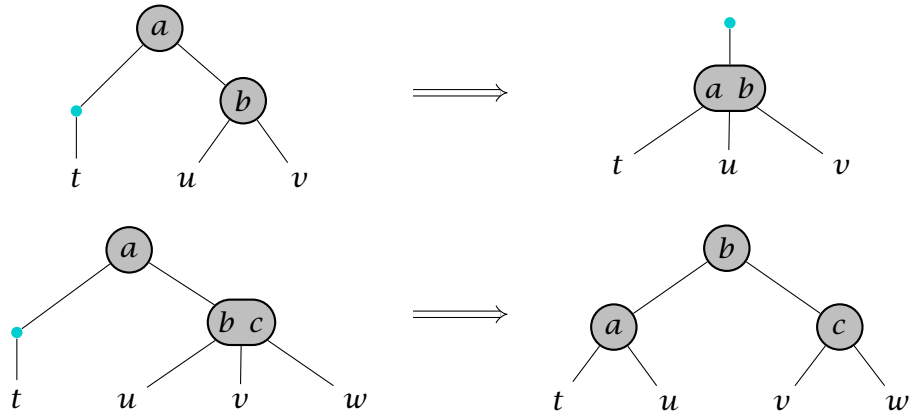
Sowohl der Elternknoten als auch der Geschwisterknoten des blauen Knotens sind 2-Knoten. Mit insgesamt zwei Elementen lässt sich aber kein 2-3-Baum der Höhe 2 konstruieren, so dass wir die beiden 2-Knoten zu einem 3-Knoten mit einem blauen Knoten als Elter zusammenfassen. Wie beim Einfügen verschieben wir das Problem so auf die nächsthöhere Ebene.



Der blaue Knoten liegt jetzt unterhalb eines 3-Knotens, so dass hinreichend viele Elemente vorhanden sind, um den Defekt zu reparieren.

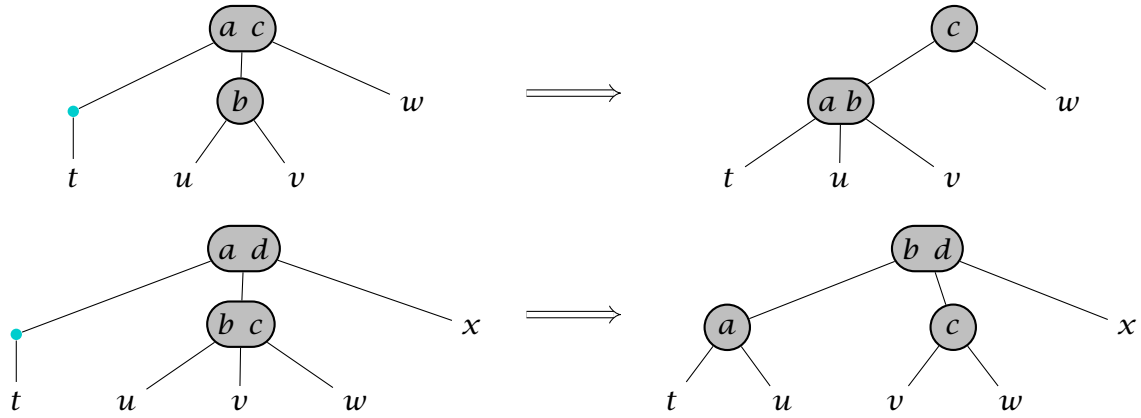
Das Löschen ist wie das Einfügen ein 2-Phasen-Algorithmus: In der ersten Phase wird das zu löschende Element lokalisiert und entfernt; in der zweiten Phase wird die Invariante durch lokale Transformationen entlang des Suchpfads wiederhergestellt. Verglichen mit der Situation beim Einfügen gibt es allerdings doppelt so viele Transformationen, da sowohl der Elternknoten als auch zusätzlich ein Geschwisterknoten berücksichtigt werden müssen.

Wenn das Elter des blauen Knotens ein 2-Knoten ist, dann wird er in Abhängigkeit vom rechten Geschwister entweder zu einem 1-Knoten geschrumpft oder er bleibt erhalten.



Im zweiten Fall müssen die Elemente rearrangiert werden, um die Suchbaumeigenschaft zu erhalten. Die beiden symmetrischen Fälle, in denen der blaue 1-Knoten als rechter Teilbaum auftritt, werden durch symmetrische Transformationen behandelt. Die Transformationen haben eine interessante arithmetische Interpretation: Die erste Umformung setzt die Gleichung $1 + 2 = 3$ um, die zweite $1 + 3 = 2 + 2$. Dabei bestimmt die Wurzel die Anzahl der Summanden, die Summanden selbst entsprechen dem Knotentyp der Kinder.

Ganz entsprechende Umformungen werden durchgeführt, wenn das Elter des blauen Knotens ein 3-Knoten ist: $1 + 2 + n = 3 + n$ und $1 + 3 + n = 2 + 2 + n$ in der Baumarithmetik.



Die restlichen vier Fälle, in denen der blaue 1-Knoten in der Mitte oder rechts auftritt, werden durch symmetrische Transformationen behandelt. Befindet sich der blaue Knoten in der Mitte, so kann man sich aussuchen, ob man das linke oder das rechte Geschwister heranzieht. Die arithmetische Interpretation legt nahe, dass die Transformationen abgesehen von diesem Detail alternativlos sind.

Wie beim Einfügen definieren wir einen Spezialdatentyp, um die Höhenveränderungen nachzuhalten,

```
type Shrunk⟨'a⟩ =
  | Zero' of Tree23⟨'a⟩
  | Pred' of Tree23⟨'a⟩          // blauer Knoten
```

und insgesamt fünf clevere Konstruktoren, um die Transformationen umzusetzen.

```
let node2'1 = function
  | (Zero' t, a, u)                    → Zero' (Node2 (t, a, u))
  | (Pred' t, a, Node2 (u, b, v))      → Pred' (Node3 (t, a, u, b, v))
  | (Pred' t, a, Node3 (u, b, v, c, w)) → Zero' (Node2 (Node2 (t, a, u), b, Node2 (v, c, w)))
let node2'2 = function
  | (t, a, Zero' u)                    → Zero' (Node2 (t, a, u))
  | (Node2 (t, a, u), b, Pred' v)      → Pred' (Node3 (t, a, u, b, v))
  | (Node3 (t, a, u, b, v), c, Pred' w) → Zero' (Node2 (Node2 (t, a, u), b, Node2 (v, c, w)))
let node3'1 = function
  | (Zero' t, a, u, b, v)                    → Node3 (t, a, u, b, v)
  | (Pred' t, a, Node2 (u, b, v), c, w)      → Node2 (Node3 (t, a, u, b, v), c, w)
  | (Pred' t, a, Node3 (u, b, v, c, w), d, x) → Node3 (Node2 (t, a, u), b, Node2 (v, c, w), d, x)
let node3'2 = function
  | (t, a, Zero' u, b, v)                    → Node3 (t, a, u, b, v)
  | (t, a, Pred' u, b, Node2 (v, c, w))      → Node2 (t, a, Node3 (u, b, v, c, w))
  | (t, a, Pred' u, b, Node3 (v, c, w, d, x)) → Node3 (t, a, Node2 (u, b, v), c, Node2 (w, d, x))
let node3'3 = function
  | (t, a, u, b, Zero' v)                    → Node3 (t, a, u, b, v)
  | (t, a, Node2 (u, b, v), c, Pred' w)      → Node2 (t, a, Node3 (u, b, v, c, w))
  | (t, a, Node3 (u, b, v, c, w), d, Pred' x) → Node3 (t, a, Node2 (u, b, v), c, Node2 (w, d, x))
```

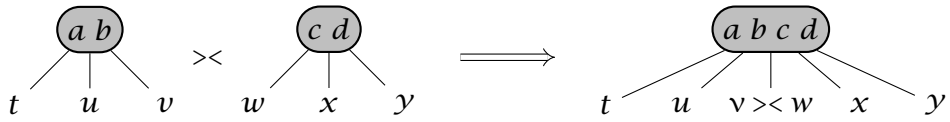
Anhand der textuellen Darstellung der Transformationen kann man übrigens leicht verifizieren, dass die Suchbaumeigenschaft erhalten bleibt. Für jede Regel gilt: Die Teilbäume und Elemente treten auf der linken und der rechten Seite in der exakt gleichen Reihenfolge auf, zum Beispiel t,

a, u, b, v, c, w, d und x in der letzten Regel. Clevere 2-Knoten propagieren möglicherweise den blauen Knoten, während clevere 3-Knoten ihn eliminieren. Schafft der blaue Knoten es bis ganz noch oben, so wird er von der Funktion *root′* verworfen.

```
let root' = function
  | Zero' t → t          // Höhe ist unverändert
  | Pred' t → t          // 2-3-Baum ist geschrumpft
```

Wir haben bereits in Abschnitt 5.3.3 gesehen, dass das Entfernen aufwändiger ist als das Einfügen — das ist hier genauso. Konzeptionell wird das Löschen auf die Konkatenation von Bäumen >< zurückgeführt: Aus *Node2* (t,a,u) wird *node1* $(t >< u)$ und aus *Node3* (t,a,u,b,v) wird $node2_1\ (t >< u,b,v)$, falls a das zu entfernende Element ist.

Die Konkatenation lässt sich auf verschiedene Weisen realisieren. Man kann, wie wir das im Fall der Binärbäume gemacht haben, den Inorder-Vorgänger oder den Inorder-Nachfolger des gelöschten Elements bestimmen und aus den Daten einen 2-Knoten bilden. Alternativ kann man die Bäume im Reißverschlussverfahren miteinander verbinden. Letzteres Verfahren ist zu elegant, als dass wir es Ihnen vorenthalten könnten oder wollten. Die folgende Graphik illustriert die Idee an einem konkreten Beispiel.



Die beiden 3-Knoten werden zu einem virtuellen 5-Knoten kombiniert, indem der rechteste Teilbaum des ersten Arguments mit dem linkesten Teilbaum des zweiten Arguments rekursiv konkateniert wird. Zwei Vorbedingungen sind erforderlich: Die beiden 2-3-Bäume müssen gleich hoch sein (so wie die Stränge eines Reißverschlusses gleich lang sein müssen) und im Fall von 2-3-Suchbäumen müssen die Elemente des ersten Arguments höchstens so groß sein wie die Elemente des zweiten Arguments. Der konkatenierte Baum ist entweder gleich hoch oder eine Ebene höher. Wie immer protokollieren wir sorgsam die Höhenveränderungen mit Hilfe von cleveren Konstruktoren.

```
let node4_2 = function
  | (t,a,Zero u,b,v,c,w)          → Succ (Node2 (t,a,u),b,Node2 (v,c,w))
  | (t,a,Succ (u,b,v),c,w,d,x) → Succ (Node3 (t,a,u,b,v),c,Node2 (w,d,x))
let node4_3 = function
  | (t,a,u,b,Zero v,c,w)          → Succ (Node2 (t,a,u),b,Node2 (v,c,w))
  | (t,a,u,b,Succ (v,c,w),d,x) → Succ (Node2 (t,a,u),b,Node3 (v,c,w,d,x))
let node5_3 = function
  | (t,a,u,b,Zero v,c,w,d,x)          → Succ (Node2 (t,a,u),b,Node3 (v,c,w,d,x))
  | (t,a,u,b,Succ (v,c,w),d,x,e,y) → Succ (Node3 (t,a,u,b,v),c,Node3 (w,e,x,e,y))
```

Da die Höhe der Argumente von >< gleich ist, müssen wir nur fünf Fälle unterscheiden: einen Basisfall, beide Argument sind Blätter, und vier Rekursionsfälle, alle möglichen Kombinationen von 2- und 3-Knoten. (Anderenfalls wären es insgesamt neun Fälle. Warum?)

```
let rec (><) t u =
  match (t,u) with
  | (Leaf,          Leaf)          → Zero Leaf
  | (Node2 (t,a,u), Node2 (v,c,w)) → node3_2 (t,a,u >< v,c,w)
  | (Node2 (t,a,u), Node3 (v,c,w,d,x)) → node4_2 (t,a,u >< v,c,w,d,x)
  | (Node3 (t,a,u,b,v), Node2 (w,d,x)) → node4_3 (t,a,u,b,v >< w,d,x)
  | (Node3 (t,a,u,b,v), Node3 (w,d,x,e,y)) → node5_3 (t,a,u,b,v >< w,d,x,e,y)
```

Im Rekursionsfall wird ein i-Knoten und ein j-Knoten zu einem $(i+j-1)$-Knoten verbandelt. Da nur ein rekursiver Aufruf erfolgt, ist die Laufzeit von $><$ proportional zur Höhe der Bäume.

Nach diesen Vorarbeiten geht das Löschen relativ leicht von der Hand.

```
let node1 = function
  | Zero t          → Pred' t
  | Succ (t, a, u) → Zero' (Node2 (t, a, u))
let remove key (Rep tree) =
  let rec delete = function
    | Leaf                                  → Zero' Leaf
    | Node2 (t, a, u)      when key < a.key → node2'1 (delete t, a, u)
    | Node2 (t, a, u)      when key = a.key → node1 (t >< u)
    | Node2 (t, a, u)      (* key > a.key *) → node2'2 (t, a, delete u)
    | Node3 (t, a, u, b, v) when key < a.key → Zero' (node3'1 (delete t, a, u, b, v))
    | Node3 (t, a, u, b, v) when key = a.key → Zero' (node2'1 (t >< u, b, v))
    | Node3 (t, a, u, b, v) when key < b.key → Zero' (node3'2 (t, a, delete u, b, v))
    | Node3 (t, a, u, b, v) when key = b.key → Zero' (node2'2 (t, a, u >< v))
    | Node3 (t, a, u, b, v) (* key > b.key *) → Zero' (node3'3 (t, a, u, b, delete v))
  Rep (root' (delete tree))
```

Wie immer unterscheiden wir insgesamt acht Fälle. Wird aus einem 3-Knoten ein Element entfernt, dann ändert sich die Höhe garantiert nicht (angezeigt durch die *Zero'* Konstruktoren); im Fall von 2-Knoten ändert sie sich möglicherweise. Am interessantesten ist der dritte Fall; der clevere Konstruktor vom Typ $Grown\langle'a\rangle \to Shrunk\langle'a\rangle$ übersetzt Höhenwachstum in Höhenschrumpfung: Hat $t >< u$ die gleiche Höhe wie t und u, dann fehlt effektiv eine Ebene, signalisiert durch den Konstruktor *Pred'*. Zum Beispiel: Entfernen wir 4711 aus dem Minibaum *Node2* (*Leaf*, 4711, *Leaf*), so erhalten wir *node1* (*Leaf* >< *Leaf*) = *node1* (*Zero Leaf*) = *Pred' Leaf* — aus dem 2-Knoten ist ein blauer 1-Knoten mit einem leeren Teilbaum geworden.

Laufzeitanalyse Haben sich die Anstrengungen gelohnt? Absolut! Alle drei betrachteten Operationen, *lookup*, *add* und *remove*, legen eine logarithmische Laufzeit an den Tag. Wie für ihre Kolleginnen auf Binärbäumen ist die Anzahl der Rechenschritte proportional zur Höhe der Bäume — das liegt daran, dass jede Rebalancierungsoperation nur eine konstante Anzahl an zusätzlichen Schritten benötigt. Im Unterschied zu stinknormalen Binärbäumen ist aber im Fall von 2-3-Bäumen eine logarithmische Höhe garantiert.

$$2^{height\ t} - 1 \leqslant size\ t \leqslant 3^{height\ t} - 1 \qquad \lceil \log_3(size\ t + 1) \rceil \leqslant height\ t \leqslant \lfloor \log_2(size\ t + 1) \rfloor$$

Der *lichteste* 2-3-Baum ist ein perfekter Binärbaum; der *dichteste* 2-3-Baum ist entsprechend ein perfekter Ternärbaum. Die Größe eines 2-3-Baums liegt zwischen diesen beiden Extremen. Formen wir die Ungleichungen um, erhalten wir die gewünschte Abschätzung für die Höhe. (Zur Erinnerung: Logarithmen unterscheiden sich nur in einem konstanten Faktor, $\log_b x = \ln x / \ln b$.) PS: Die Analyse legt vielleicht nahe, dass dichte 2-3-Bäume mit vielen 3-Knoten wegen der geringeren Höhe vorteilhafter sind als lichte 2-3-Bäume, die nur wenige 3-Knoten enthalten. Das stimmt nicht ganz, da 3-Knoten ein asymmetrisches Verhalten bei der Suche hervorrufen: Der 5-Wege-Vergleich wird in der Regel durch zwei ineinandergeschachtelte 3-Wege-Vergleiche implementiert (5.4). Suchen wir in einem dichten Baum nach dem linkesten Element, dann beschleunigt sich die Suche im Vergleich zu einem lichten Baum um den Faktor $\ln 2 / \ln 3 \approx 1{,}585$; suchen wir aber nach dem rechtesten Element so verlangsamt sich die Suche um den Faktor $1{,}585/2 = 0{,}7925$, da auf jeder Ebene zwei 3-Wege-Vergleiche erfolgen.

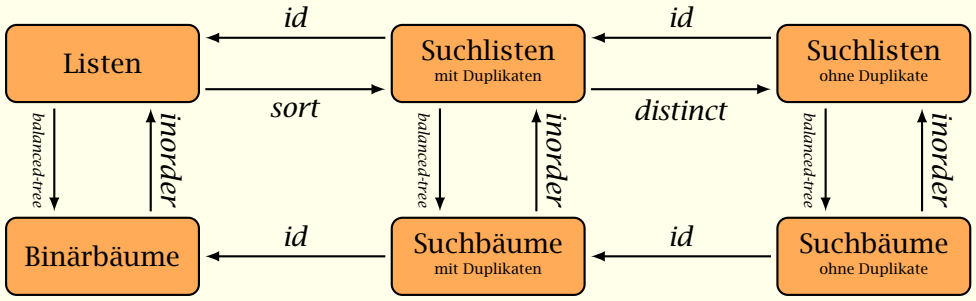


Abbildung 5.18.: Wechsel der Repräsentation.

5.3.5. Wechsel der Repräsentation

Endliche Abbildungen lassen sich auf vielfältige Weisen repräsentieren: unter anderem mit Hilfe von Listen, Suchlisten oder Suchbäumen. Wechselt man im laufenden Betrieb die Repräsentation, müssen die Daten entsprechend konvertiert werden, siehe Abbildung 5.18. Die Überführung von Listen in Binärbäume und umgekehrt ist ein algorithmisches Problem von allgemeinem Interesse, da, wie bereits angedeutet, Binärbäume viele weitere Anwendungen haben.

Linearisierung von Binärbäumen Wie können wir einen Baum in eine Liste überführen? Das Struktur Entwurfsmuster für *Tree* führt fast direkt zum Ziel.

```
let rec inorder (tree : Tree ⟨'elem⟩) : List ⟨'elem⟩ =
  match tree with
  | Leaf                → ...
  | Node (left, x, right) → ... inorder left ... inorder right ...
```

Im Rekursionsfall müssen wir zwei Listen, die Ergebnisse der rekursiven Aufrufe, und ein Element zu einer Liste zusammenfügen. Das Konkatenieren zweier Listen besorgt *append* bzw. »@«, so dass wir formulieren können.

```
let rec inorder (tree : Tree ⟨'elem⟩) : List ⟨'elem⟩ =
  match tree with
  | Leaf                → [ ]
  | Node (left, x, right) → inorder left @ [x] @ inorder right
```

Die relative Reihenfolge der Elemente — erst die Elemente aus dem linken Teilbaum, dann das Wurzelelement, dann die Elemente aus dem rechten Teilbaum — bleibt bei der Transformation erhalten. Auf diese Weise wird ein Suchbaum in eine Suchliste überführt. Weil das Wurzelelement *zwischen* die Elemente des linken und des rechten Teilbaums wandert, heißt die Funktion entsprechend *inorder*. Zwei weitere Alternativen sind geläufig: das Wurzelelement voranzustellen (*preorder*) oder hinten anzuhängen (*postorder*), siehe Aufgabe 5.3.1.

Wie schnell ist *inorder*? Das hängt wie so oft von der Form des Binärbaums ab. Zunächst müssen wir kurz überlegen, wieviele Schritte *append* benötigt, um zwei Listen zu konkatenieren. Rufen wir uns die Definition von *append* ins Gedächtnis.

```
let rec append list ys =
  match list with
  | [ ]     → ys
  | x :: xs → x :: append xs ys
```

Die Funktion rekurriert über das erste Argument, das zweite Argument wird gar nicht inspiziert. Die Laufzeit von *append* ist also proportional zur Länge der ersten Liste.

Also, wenn der linke Teilbaum immer leer ist, dann ist *append* jedes Mal in einem Schritt fertig. Insgesamt erhalten wir für *inorder* eine lineare Laufzeit. Das ist optimal; schneller geht es nicht, da wir jedes Element der Ergebnisliste einmal anfassen müssen. Umgekehrt, wenn der rechte Teilbaum immer leer ist, dann muss *append* ackern: Nacheinander werden Listen der Längen 1, 2, …, $n-2$, $n-1$ durchlaufen. Insgesamt erhalten wir eine Laufzeit von $1+2+\cdots+n-2+n-1 = \binom{n}{2} = n \cdot (n-1)/2$ Schritten — grob gesprochen eine ***quadratische*** Laufzeit.

Das ist vielleicht unerwartet, auf jeden Fall ist es unbefriedigend. Um etwa eine Liste mit zehntausend Elementen zu produzieren — Bäume dieser Größenordnung sind nicht ungewöhnlich — werden hundertmillionen Schritte benötigt. Den Aufwand kann man sehen — sogar hören, falls der Rechner luftgekühlt wird — wenn man den F#-Interpreter entsprechende Testbeispiele rechnen lässt. Zu diesem Zweck schreiben wir zwei Funktionen, eine, die linksschiefe, und eine, die rechtsschiefe Binärbäume generiert.

```
let rec left-skewed (n : Nat, x : 'elem) : Tree ⟨'elem⟩ =
  if n = 0 then Leaf else Node (left-skewed (n − 1, x), x, Leaf)
let rec right-skewed (n : Nat, x : 'elem) : Tree ⟨'elem⟩ =
  if n = 0 then Leaf else Node (Leaf, x, right-skewed (n − 1, x))
```

Um Tipparbeit zu sparen, definieren wir noch eine Funktion, die nacheinander einen Baum generiert, den Baum mit *inorder* in eine Liste überführt und anschließend die Länge der Liste ermittelt.

```
let test (generate, n) = length (inorder (generate (n, "hello, world")))
```

Die Funktion *test* abstrahiert von dem Generator und von der Anzahl der Elemente. Wenn wir alles richtig gemacht haben, sollte *test* (*generate*, *n*) zu *n* auswerten.

```
⋙ test (left-skewed, 50.000)
50.000
⋙ test (right-skewed, 50.000)
50.000
```

Auf dem Rechner des Dozenten benötigt der F#-Interpreter mehr als 2 Minuten, bis das erste Ergebnis ausgerechnet ist; der zweite Aufruf wird hingegen in Nullkommanichts erledigt, in genau 0,15 Sekunden. Je weiter man den zweiten Parameter erhöht, desto deutlicher wird der Laufzeitunterschied.

Was ist zu tun? Versuchen wir *inorder* zu verbessern oder im Fachjargon zu ***optimieren***. (Der Begriff »optimieren« wird in der Programmierung tatsächlich synonym zu verbessern verwendet: Optimal ist das resultierende Programm nicht notwendigerweise. Das ist tatsächlich auch ein schwieriges Feld. Optimierung im eigentlichen Sinn erfordert zu zeigen, dass es ein besseres Programm nicht geben kann. Man muss also die ***Problemkomplexität*** kennen.)

Verbessern oder optimieren sollte man nicht blindlings. Zunächst sollte man den oder die Verbrecher identifizieren, die für die mangelhafte Laufzeit verantwortlich sind (Laufzeit-Cluedo). In unserem Fall ist der Verbrecher leicht ausgemacht: Die Funktion *append* treibt die Laufzeit in die Höhe. Die Funktion *append* selbst lässt sich allerdings nicht verbessern, das liegt an der Natur des Typs *List*. Zur Erinnerung: Listen sind asymmetrisch, auf das erste Element einer Liste können wir unmittelbar zugreifen, auf das letzte Element nicht.

Wenn wir *append* selbst nicht verbessern können, müssen wir versuchen, ohne *append* auszukommen. Das hört sich schwierig an. Der Schlüssel zum Erfolg liegt wie so oft in einer geschickten

Verallgemeinerung der Aufgabenstellung. Die grundlegende Idee ist, eine Funktion zu programmieren, die gleichzeitig linearisiert *und* konkateniert, also zwei Aufgaben auf einen Schlag erledigt. Wir spezifizieren:

$$\mathit{inorder\text{-}append}\ (\mathit{tree}, \mathit{list}) = \mathit{inorder}\ \mathit{tree} \mathbin{@} \mathit{list} \tag{5.5}$$

Die Spezifikation formuliert, dass *inorder-append* das erste Argument, einen Baum, in eine Liste überführt, und *zusätzlich* mit dem zweiten Argument, einer Liste, konkateniert. Wir können die Spezifikation von *inorder-append* benutzen, um die Funktionsdefinition auszurechnen — aus der Spezifikation wird die Implementierung *hergeleitet*! Das Struktur Entwurfsmuster für *Tree* gibt die folgende Fallunterscheidung vor.
Basisfall $\mathit{tree} = \mathit{Leaf}$**:**

$$\begin{aligned}
&\mathit{inorder\text{-}append}\ (\mathit{Leaf}, \mathit{list}) \\
=\ &\{\ \text{Spezifikation von } \mathit{inorder\text{-}append}\ (5.5)\ \} \\
&\mathit{inorder}\ \mathit{Leaf} \mathbin{@} \mathit{list} \\
=\ &\{\ \text{Definition von } \mathit{inorder}\ \} \\
&[\,] \mathbin{@} \mathit{list} \\
=\ &\{\ \text{Definition von } @ \text{ — } [\,] \text{ ist das neutrale Element von »@«}\ \} \\
&\mathit{list}
\end{aligned}$$

Rekursionsfall $\mathit{tree} = \mathit{Node}\ (\mathit{left}, x, \mathit{right})$**:**

$$\begin{aligned}
&\mathit{inorder\text{-}append}\ (\mathit{Node}\ (\mathit{left}, x, \mathit{right}), \mathit{list}) \\
=\ &\{\ \text{Spezifikation von } \mathit{inorder\text{-}append}\ (5.5)\ \} \\
&\mathit{inorder}\ (\mathit{Node}\ (\mathit{left}, x, \mathit{right})) \mathbin{@} \mathit{list} \\
=\ &\{\ \text{Definition von } \mathit{inorder}\ \} \\
&(\mathit{inorder}\ \mathit{left} \mathbin{@} [x] \mathbin{@} \mathit{inorder}\ \mathit{right}) \mathbin{@} \mathit{list} \\
=\ &\{\ @ \text{ ist assoziativ}\ \} \\
&\mathit{inorder}\ \mathit{left} \mathbin{@} ([x] \mathbin{@} \mathit{inorder}\ \mathit{right} \mathbin{@} \mathit{list}) \\
=\ &\{\ \text{Definition von } @\ \} \\
&\mathit{inorder}\ \mathit{left} \mathbin{@} (x :: \mathit{inorder}\ \mathit{right} \mathbin{@} \mathit{list}) \\
=\ &\{\ \text{Spezifikation von } \mathit{inorder\text{-}append}\ (5.5)\ \} \\
&\mathit{inorder\text{-}append}\ (\mathit{left}, x :: \mathit{inorder}\ \mathit{right} \mathbin{@} \mathit{list}) \\
=\ &\{\ \text{Spezifikation von } \mathit{inorder\text{-}append}\ (5.5)\ \} \\
&\mathit{inorder\text{-}append}\ (\mathit{left}, x :: \mathit{inorder\text{-}append}\ (\mathit{right}, \mathit{list}))
\end{aligned}$$

Die Herleitung macht wesentlichen Gebrauch von der Tatsache, dass die Konkatenation von Listen assoziativ ist, siehe Aufgabe 4.3.5.

Insgesamt erhalten wir das folgende Programm.

```
let rec inorder-append (tree : Tree ⟨'elem⟩, list : List ⟨'elem⟩) : List ⟨'elem⟩ =
  match tree with
  | Leaf                  → list
  | Node (left, x, right) → inorder-append (left, x :: inorder-append (right, list))
```

Das ursprüngliche Problem ist jetzt ein biederer Spezialfall:

```
let inorder (tree : Tree ⟨'elem⟩) : List ⟨'elem⟩ = inorder-append (tree, [ ])
```

Hier nutzen wir aus, dass die leere Liste das neutrale Element der Konkatenation ist: $xs \mathbin{@} [\,] = xs$.

Wie hat sich die Rechenzeit verbessert? Beide Aufrufe, sowohl *test* (*left-skewed*, 50.000) als auch *test* (*right-skewed*, 50.000), benötigen jetzt 0,15 Sekunden. Die Laufzeit ist erfreulicherweise unabhängig von der Struktur des zu linearisierenden Binärbaums — sie ist linear zur *Größe* des Binärbaums.

Konstruktion von Binärbäumen Wie können wir einen balancierten Suchbaum aus einer geordneten Liste konstruieren? Oder etwas allgemeiner: Wie können wir einen Binärbaum aus einer Liste konstruieren, so dass der Inorder-Durchlauf wieder die ursprüngliche Liste ergibt?

$$inorder \ll balanced\text{-}tree = id$$

Mathematisch gesehen, suchen wir die Umkehrfunktion von *inorder* bzw. genauer eine ***Rechtsinverse***. Die gespiegelte Beziehung $balanced\text{-}tree \ll inorder = id$ lässt sich nicht erfüllen, da es viele Bäume mit dem gleichen Inorder-Durchlauf gibt. Kurz: *inorder* ist surjektiv, aber nicht injektiv. Die Spezifikation macht auch deutlich, dass die ursprüngliche Aufgabe ein Spezialfall ist: *balanced-tree* überführt eine Suchliste in einen Suchbaum.

Das Konstruktionsverfahren orientiert sich an der Struktur eines Binärbaums: Ist die Liste leer, so haben wir einen leeren Baum. Eine mindestens einelementige Liste teilen wir in drei Teile auf, den linken Teil, das Element und den rechten Teil. Das Verfahren wenden wir rekursiv auf die beiden Teillisten an. Um die Ausgeglichenheit zu gewährleisten, sollten die beiden Teillisten natürlich möglichst gleich lang sein. Aber wie können wir eine Liste halbieren? Wir sehen ja einer Liste die Anzahl der Elemente nicht an. (Die Funktion *unzip* taugt übrigens nicht für diesen Zweck. Warum?)

Statt eine Funktion zu programmieren, die eine Liste genau halbiert, ist es geschickter, die Aufgabe etwas zu verallgemeinern: Wir schreiben eine Funktion, die eine Liste *list* in zwei Teillisten der Längen n und $length\ list - n$ zerteilt falls $n \leqslant length\ list$. Halbierung ist dann ein Spezialfall mit $n = length\ list \div 2$.

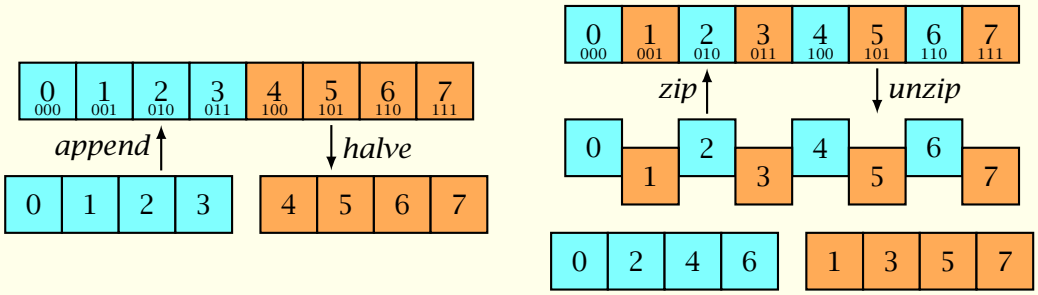
```
let rec split (n : Nat, list : List ⟨'a⟩) : List ⟨'a⟩ * List ⟨'a⟩ =
  if n = 0 then ([ ], list)
           else match list with
                  | [ ]      → ([ ], [ ])
                  | x :: xs → let (xs₁, xs₂) = split (n ÷ 1, xs) in (x :: xs₁, xs₂)
```

Die beiden Parameter n und *list* werden im Tandem verringert. Der Programmcode behandelt zusätzlich den Fall, dass $n > length\ list$. Für diesen speziellen Fall legen wir $split\ (n, list) = (list, [\,])$ fest.

Nach diesen Vorarbeiten können wir uns wieder der ursprünglichen Aufgabe zuwenden.

```
let rec balanced-tree (list : List ⟨'a⟩) : Tree ⟨'a⟩ =
  let n = length list
  if n = 0 then Leaf
           else let (xs₁, x :: xs₂) = split (n ÷ 2, list)
                Node (balanced-tree xs₁, x, balanced-tree xs₂)
```

Die Liste wird im Rekursionsfall halbiert, das Element für die Wurzel wird der zweiten Teilliste entnommen. Man beachte, dass die Fallunterscheidung unvollständig ist: Das Muster $(xs_1, [\,])$ fehlt. Schiefgehen kann aber nichts: Die Länge n der gesamten Liste ist mindestens eins, die

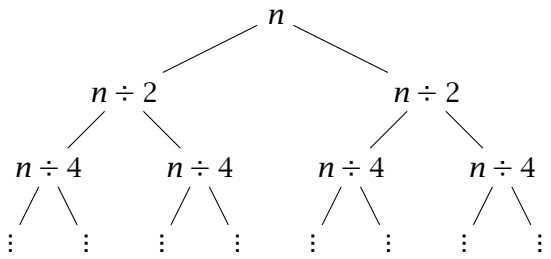


Werden die Elemente ab 0 durchnummeriert, dann teilt *halve* nach dem höchstwertigen Bit, während *unzip* nach dem niedrigstwertigen Bit aufteilt — vorausgesetzt, die Länge der Liste ist eine exakte Zweierpotenz.

Abbildung 5.19.: Teilen einer Liste: *halve* versus *zip*.

zweite Teilliste hat somit die Länge $n - n \div 2 = (n+1) \div 2$, also umfasst sie ebenfalls mindestens ein Element.

Welche Laufzeit hat *balanced-tree*? Die Länge der Liste spielt sicherlich eine zentrale Rolle. Schauen wir uns also die rekursive Aufrufstruktur von *balanced-tree* in Abhängigkeit von der Listenlänge an (die Längen stimmen nicht ganz).



Der ***Rekursionsbaum*** ist — genau wie der erzeugte Suchbaum — ausgeglichen: Der initiale Aufruf führt zu zwei rekursiven Aufrufen, jeder dieser Aufrufe resultiert in zwei weiteren rekursiven Aufrufen usw. Die Höhe des Rekursionsbaumes ist $\lg n$, wenn n die Länge der ursprünglichen Liste ist. Vor jedem rekursiven Aufruf wird das aktuelle Listenargument $1\frac{1}{2}$ mal durchlaufen (1 mal von *length* und $\frac{1}{2}$ mal von *split*). Alle Aufrufe auf einer horizontalen Ebene haben somit *zusammen* eine lineare Laufzeit. Multipliziert mit der Anzahl der Ebenen, der Höhe des Rekursionsbaumes, ergibt sich insgesamt eine Laufzeit von $n \lg n$.

Blättern wir im Skript zurück, merken wir, dass die Laufzeitanalyse im Wesentlichen der Analyse von Mergesort entspricht. Dies überrascht vielleicht nicht, da beide Funktionen nach dem Leibniz Entwurfsmuster gestrickt sind. Sie illustrieren zwei duale Ansätze, die Problemreduktion (in der »Teile«-Phase) zu realisieren: Mergesort trennt die Listen reißverschlussartig mit Hilfe von *unzip* auf, *balanced-tree* trennt in der Mitte mit Hilfe von *halve*, siehe Abbildung 5.19. Je nach Problemstellung wird man dem einen oder dem anderen Verfahren den Vorzug geben.[12] Mergesort funktioniert prinzipiell mit beiden Ansätzen; tatsächlich ist aber vorteilhafter *halve* zu verwenden, siehe Aufgabe 5.1.2.

Zurück zum ursprünglichen Problem: Lässt sich die Laufzeit von *balanced-tree* verbessern? Vielleicht können wir wiederum die Aufgabenstellung geschickt verallgemeinern? Im Fall von *inorder* haben wir die Linearisierung mit der Konkatenation von Listen kombiniert. Jetzt lösen

[12] Die Trennung in der Mitte erscheint auf den ersten Blick natürlicher oder offensichtlicher. Tatsächlich aber verwenden wir oft das Reißverschlussverfahren, da die Mitte manchmal nur schwer abzuschätzen ist: etwa beim Austeilen von Karten, die alternierend an die Mitspieler/-innen vergeben werden.

wir das duale Problem, so dass es naheliegt, die Konstruktion mit dem Aufspalten einer Liste zu kombinieren. Wir spezifizieren:

$$\mathit{balanced\text{-}tree\text{-}of\text{-}size}\ n\ \mathit{list} = (\mathit{balanced\text{-}tree}\ xs, ys) \quad \text{wobei} \quad (xs, ys) = \mathit{split}\ n\ \mathit{list}$$

Der erste Parameter von *balanced-tree-of-size* gibt sozusagen den »erlaubten Verbrauch« an Listenelementen an; nicht benötigte Elemente müssen zurückgegeben werden. Beim initialen Aufruf wird n die Länge der gesamten Liste sein, so dass wir als Vorbedingung annehmen, dass $n \leqslant \mathit{length}\ \mathit{list}$ — es sind stets genügend Elemente vorhanden.

Die ursprüngliche, umgangssprachliche Beschreibung des Konstruktionsverfahrens lässt sich jetzt unmittelbar in Rechenregeln überführen. Ist $n = 0$, so geben wir ein Blatt und alle Listenelemente zurück. Anderenfalls konstruieren wir aus den ersten $m = (n-1) \div 2$ Elementen den linken Teilbaum, entnehmen ein Element für die Wurzel und konstruieren aus den restlichen Elementen den rechten Teilbaum.

```
let rec balanced-tree-of-size n xs =
  if n = 0 then (Leaf, xs)
           else let m = (n ∸ 1) ÷ 2
                let (l, x :: ys) = balanced-tree-of-size m          xs
                let (r, zs)      = balanced-tree-of-size (n ∸ 1 ∸ m) ys
                (Node (l, x, r), zs)
```

Im Rekursionsfall verbrauchen wir wie vorgegeben insgesamt $m + 1 + (n - 1 - m) = n$ Elemente. Aufgrund der Vorbedingung $n \leqslant \mathit{length}\ xs$ kann das widerlegbare Muster $x :: ys$, mit dem wir das Wurzelelement x entnehmen, nicht scheitern.

Das ursprüngliche Problem ist jetzt ein biederer Spezialfall: Wir setzen den »erlaubten Verbrauch« auf den maximalen Wert, die Listenlänge.

```
let balanced-tree x = fst (balanced-tree-of-size (length x) x)
```

Die Laufzeit von *balanced-tree-of-size n list* ist proportional zu n. Somit hat die Funktion *balanced-tree* eine lineare Laufzeit — das ist optimal, da wir jedes Listenelement verarbeiten müssen. Übrigens würde auch *merge-sort* von einem ähnlichen Ansatz profitieren, siehe Aufgabe 5.1.2. Wir können zwar nicht die asymptotische Laufzeit verbessern (an der Größenordnung ändert sich nichts), wohl aber die konkrete Zahl der Rechenschritte.

Fazit: Ein schwierigeres Problem muss nicht schwieriger zu lösen sein. Die Ursache für diese scheinbar paradoxe Tatsache liegt in der Rekursion begründet: Im Rekursionsschritt können wir auf Teillösungen zurückgreifen; die rekursiven Aufrufe lösen aber bereits schwierigere Teilprobleme, so dass der Schritt zur Gesamtlösung oft einfacher ist. Im Fall von *inorder-append* zum Beispiel erledigt der rekursive Aufruf zusätzlich das Aneinanderhängen der Teillisten.

Das ***Rekursionsparadoxon*** stellt eine allgemeine Programmiertechnik dar und firmiert unter verschiedensten Namen: Verallgemeinerung der Aufgabenstellung, akkumulierende Parameter (*inorder*), Tupeltransformation (*balanced-tree*); beim Beweisen, einer dem Programmieren eng verwandten Tätigkeit, spricht man von der Verstärkung der Induktionsannahme, im Englischen auch bekannt unter dem Namen »Inventor's Paradox«.

5.3.6. Laufzeitverhalten der Implementierungen

Wir haben gesehen, dass sich endliche Abbildungen auf mindestens vier verschiedene Arten implementieren lassen (tatsächlich gibt es eine fast unüberschaubare Anzahl von Möglichkeiten).

Bezüglich der funktionalen Eigenschaften, des Ein- und Ausgabeverhaltens, sind die Implementierungen austauschbar — die Spezifikation der Semantik legt das Verhalten präzise fest; die Implementierungen setzen die Anforderungen buchstabengetreu um. Unterschiede treten bezüglich der nichtfunktionalen Eigenschaften auf, bezüglich des Ressourcenverbrauchs. Die folgende Tabelle trägt die einzelnen Ergebnisse zusammen (dabei steht n für die Gesamtzahl der Einträge, h mit $\lceil \lg(n+1) \rceil \leqslant h \leqslant n$ für die Höhe der Binärbäume).

	Listen	Suchlisten	Suchbäume	2-3-Suchbäume
empty	1	1	1	1
add	1	n	h	$\lg n$
remove	n	n	h	$\lg n$
is-empty	1	1	1	1
lookup	n	n	h	$\lg n$
from-list	n	$n \lg n$	$n \lg n$	$n \lg n$
to-list	n	n	n	n

Die linear-logarithmische Laufzeit von *from-list* im Fall von Suchlisten und Suchbäumen erklärt sich durch die Sortierung der Eingabe. (Lässt sich *from-list* auf lineare Laufzeit beschleunigen?)

Qual der Wahl? Nicht wirklich, 2-3-Suchbäume gehen als klare Gewinner aus dem Wettbewerb hervor. Binäre Suchbäume kommen zum Einsatz, wenn die Schlüsselmenge statisch ist (Suchoperationen dominieren Einfüge- und Löschoperationen); Suchlisten, wenn die Schlüsselmenge klein ist (eher 2- als 3-stellig in der Zahl).

Übungen.

1. Programmieren Sie in Analogie zur Funktion *inorder* Funktionen, die einen Baum in Preorder- bzw. Postorder-Reihenfolge in eine Liste überführen. *Zur Erinnerung:* Inorder-Reihenfolge bedeutet, dass das Wurzelelement *zwischen* die Elemente des linken und des rechten Teilbaums wandert. Beim Preorder-Durchlauf wird das Wurzelelement vorangestellt und beim Postorder-Durchlauf hinten angehängt.

```
let preorder  (tree : Tree ⟨'a⟩) : List ⟨'a⟩
let postorder (tree : Tree ⟨'a⟩) : List ⟨'a⟩
```

Lassen sich die ursprünglichen Bäume aus den resultierenden Listen rekonstruieren? Mit anderen Worten, sind die Funktionen injektiv?

2. Programmieren Sie eine Funktion

```
let tree-sort (list : List ⟨Nat⟩) : List ⟨Nat⟩
```

die eine Liste sortiert. Gehen Sie dabei in drei Schritten vor:

(a) Definieren Sie zunächst eine Funktion

```
let insert (n : Nat, tree : Tree ⟨Nat⟩) : Tree ⟨Nat⟩
```

die ein Element in einen ***Suchbaum*** einfügt, so dass die Suchbaumeigenschaft erhalten bleibt.

(b) Schreiben Sie mit Hilfe von *insert* eine Funktion *search-tree*, die aus einer Liste einen Suchbaum konstruiert.

(c) Definieren Sie *tree-sort* als Komposition von *build* und *inorder*. *Zur Erinnerung:* Die Funktion *inorder* überführt einen Suchbaum in eine geordnete Liste.

3. Harry Hacker behauptet eine Funktion definiert zu haben, die einen Binärbaum der Größe n in logarithmischer (!) Zeit konstruiert. Seine Funktion erfüllt die Eigenschaft

```
size (create n) = n
```

wobei *size* wie folgt definiert ist:

```
let rec size = function
  | Leaf          → 0
  | Node (l, a, r) → size l + 1 + size r
```

Genie oder Scharlatan?

4. Weihnachten steht vor der Tür und Lisa Lista und Harry Hacker haben beschlossen, gemeinsam einen Weihnachtsbaum zu schmücken. Für die Repräsentation des Baumes haben sie sich folgende Typdeklaration überlegt:

```
type Christmas-Tree = | Twig | Bauble | Fork of Christmas-Tree * Christmas-Tree
```

Der Konstruktor *Twig* steht für einen leeren Ast des Weihnachtsbaumes; der Konstruktor *Bauble* beschreibt einen Ast des Baumes, der mit einer Christbaumkugel geschmückt ist. Schreiben Sie eine Funktion *decorate*, die einen beliebigen leeren Ast mit einer Christbaumkugel schmückt.

```
let decorate (tree : Christmas-Tree) : Christmas-Tree
```

Wird der gesamte Baum geschmückt, wenn die Funktion wiederholt aufgerufen wird?

5. Erweitern Sie die Schnittstelle für endliche Abbildungen um eine Funktion, die den Kommaoperator implementiert. Realisieren Sie die Operation für Listen, Suchlisten und Suchbäume und analysieren Sie jeweils die Laufzeit.

6. Eine Menge von natürlichen Zahlen kann durch eine geordnete Liste repräsentiert werden, in der kein Element doppelt vorkommt (Suchliste ohne Duplikate).

```
type Set = List ⟨Nat⟩
```

Definieren Sie auf dieser Repräsentation die Vereinigung, den Durchschnitt und die Differenz von Mengen.

```
let union        (set₁ : Set, set₂ : Set) : Set
let intersection (set₁ : Set, set₂ : Set) : Set
let difference   (set₁ : Set, set₂ : Set) : Set
```

Wie ändert sich die Definition der Funktionen, wenn wir statt Mengen von natürlichen Zahlen Mengen von ganzen Zahlen betrachten (vergleiche Aufgabe 4.2.1)?

5.4. Prioritätswarteschlangen

In Abschnitt 5.1.5 haben wir überlegt, wie man das i-kleinste Element einer Folge bestimmen kann, die i-te Ordnungsstatistik. Die Folge ist dabei fest vorgegeben; wenn sich die Folge ändert, dann muss die i-te Ordnungsstatistik neu berechnet werden. Die Algorithmen ziehen dabei keinen Nutzen aus der oder den vorausgegangenen Berechnungen. In diesem Abschnitt wenden wir uns der »dynamischen Variante« dieser Aufgabe zu. Aus einem algorithmischen Problem, der Bestimmung der Ordnungsstatistik, wird ein abstrakter Datentyp, die ***Prioritätswarteschlange*** oder Vorrangwarteschlange (engl. priority queue).

Warteschlangen kennen wir aus dem täglichen Leben. Oft werden sie im »first-in first-out« Modus betrieben: Bei Behördengängen entscheidet in der Regel die Ankunftszeit (»Ziehen Sie bitte eine Wartemarke …«), wann eine Person an der Reihe ist. Bei einer Prioritätswarteschlange ist hingegen nicht die Ankunftszeit, sondern eine vorher festgelegte Priorität ausschlaggebend, zum Beispiel die Wichtigkeit oder die Hilfsbedürftigkeit einer Person. Dieser »Modus Operandi« begegnet einem zum Beispiel beim Boarding eines Flugzeugs (»Wir bitten zunächst Senatoren und Familien mit kleinen Kindern …«). Auch das Betriebssystem eines Rechners verwendet eine Prioritätswarteschlange, um anstehende Rechenaufgaben zu verwalten und diese nach Dringlichkeit abzuarbeiten. Die berühmt-berüchtigten Todo-Listen sind von ähnlicher Natur; die Priorität einer Aufgabe spiegelt deren Dringlichkeit oder die noch verbleibende Zeit bis zum avisierten Fertigstellungstermin wider.

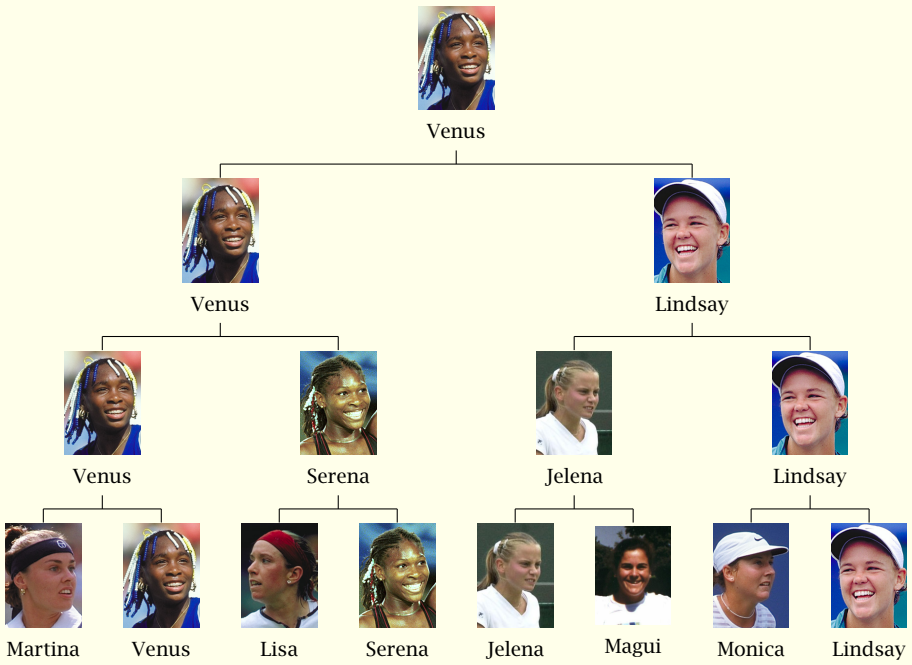


Abbildung 5.20.: Dameneinzel (Wimbledon Championships 2000).

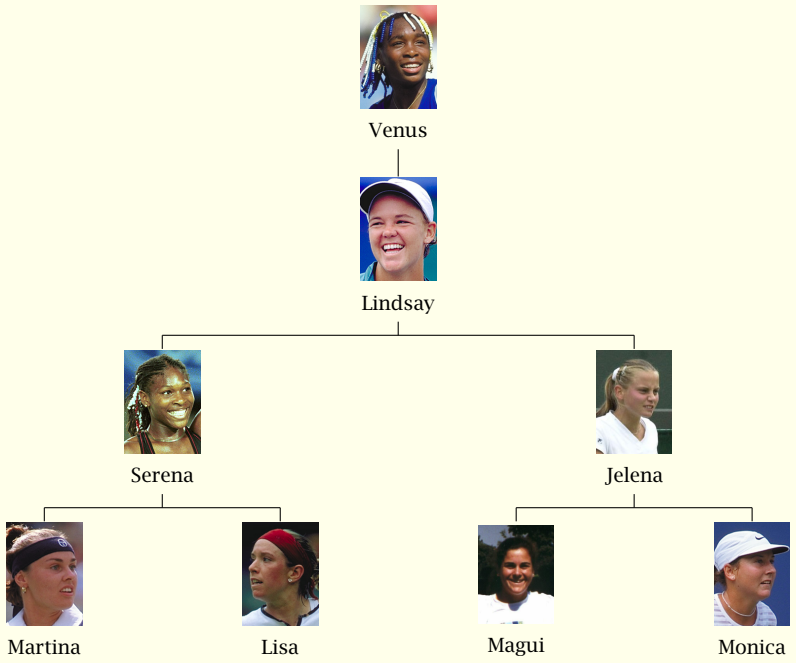


Abbildung 5.21.: Der zu dem Turnierbaum aus Abbildung 5.20 korrespondierende Baum der Verliererinnen mit dem Champion an der Spitze.

Schnittstelle Prioritätswarteschlangen unterstützen die folgenden Operationen.

type $PQueue\,\langle 'elem$ *when* $'elem : comparison\rangle$

empty	$: PQueue\,\langle 'elem\rangle$
single	$: 'elem \to PQueue\,\langle 'elem\rangle$
insert	$: 'elem * PQueue\,\langle 'elem\rangle \to PQueue\,\langle 'elem\rangle$
meld	$: PQueue\,\langle 'elem\rangle * PQueue\,\langle 'elem\rangle \to PQueue\,\langle 'elem\rangle$
split-min	$: PQueue\,\langle 'elem\rangle \to ('elem * PQueue\,\langle 'elem\rangle)\ option$
from-list	$: 'elem\ list \to PQueue\,\langle 'elem\rangle$
to-ord-list	$: PQueue\,\langle 'elem\rangle \to 'elem\ list$

Der abstrakte Datentyp *PQueue* ist mit dem Typ der Elemente *'elem* parametrisiert; der Zusatz *when* $'elem : comparison$ legt fest, dass sich Elemente vergleichen lassen müssen. Die Priorität eines Elements wird also nicht indirekt durch eine Zahl angegeben, sondern direkt durch die zugrundeliegende Ordnung auf den Elementen — wie immer setzen wir eine totale Quasiordnung voraus.

Abstrakt gesehen repräsentieren Warteschlangen Multimengen (engl. bags) oder *geordnete Sequenzen*. Insbesondere können Elemente in einer Warteschlange mehrfach auftreten. Mit Hilfe der ersten vier Operationen werden Warteschlangen konstruiert bzw. transformiert. Die *meld* Operation verdient besondere Beachtung: Im Unterschied zu endlichen Abbildungen können zwei Warteschlangen »verschmolzen«, zu einer Schlange vereinigt werden. (Unsere endlichen Abbildungen bieten eine analoge Operation, sprich den »Kommaoperator«, nicht an, da geeignete Implementierungen wie zum Beispiel Suchbäume die Operation nicht effizient unterstützen.) Um eine Warteschlange zu »dekonstruieren«, steht lediglich die Operation *split-min* zur Verfügung, die eine Schlange in das kleinste Element und die restliche Schlange aufteilt. Die Operation stellt das Herzstück der Signatur dar: Prioritätswarteschlangen sollen ja gerade den Zugriff auf das jeweils kleinste Element effizient unterstützen. Zusätzlich gibt es noch zwei Bulk-Operationen[13], mit denen eine Liste in eine Schlange und umgekehrt eine Schlange in eine *geordnete Liste* überführt werden kann.

Interdefinierbarkeit Die verschiedenen Operationen der Signatur sind nicht unabhängig voneinander; einige lassen sich mit Hilfe der anderen Operationen implementieren. Im Fachjargon sagt man, die Operationen sind ***interdefinierbar***. Zum Beispiel lässt sich *insert* auf *single* und *meld* zurückführen.

let $insert\ (x, q) = meld\ (single\ x, q)$

Können Sie umgekehrt *meld* mit den anderen Operationen der Signatur realisieren?

Warum ist das eine bedeutsame Erkenntnis? Nun, Anwendungsprogrammierer/-innen wünschen sich eine möglichst reichhaltige Schnittstelle; Implementierer/-innen hingegen eine möglichst schmale. Um zwischen den gegenläufigen Interessen zu vermitteln, sind ***Default-Implementierungen*** wie die *insert* nützlich. Sie reduzieren den Implementierungsaufwand, da sie unabhängig von einer speziellen Implementierung arbeiten — zumindest den initialen Implementierungsaufwand, oft lässt sich die betreffende Operation für eine spezielle Implementierung direkter und damit effizienter umsetzen.

Insbesondere lassen sich für die beiden Bulk-Operationen Default-Implementierungen angeben. Um eine Warteschlange in eine geordnete Liste zu überführen, rufen wir *split-min* solange auf, bis die Warteschlange leer ist.

[13] So werden Operationen bezeichnet, die eine »große« Menge von Daten (engl. bulk) verarbeiten.

```
let rec to-ord-list q =
  match split-min q with
  | None        → [ ]
  | Some (x, q') → x :: to-ord-list q'
```

Das Verfahren erinnert an »Sortieren durch Auswählen« mit dem Unterschied, dass die *Eingabe*daten nicht konkret sind, eine Liste von Elementen, sondern abstrakt, eine Prioritätswarteschlange. Dementsprechend führen wir nicht direkt eine Fallunterscheidung über die Eingabe durch, mit den Mustern $[\,]$ und $x :: xs$, sondern diskriminieren die Rückgabe von *split-min*, mit den Mustern *None* und *Some* (x, q'). Von der Syntax abgesehen entsprechen sich die Muster — mit Hilfe von *split-min* kann eine Prioritätswarteschlange peu à peu linearisiert werden.

Umgekehrt können wir eine Liste in eine Prioritätswarteschlange überführen, indem wir nacheinander die Elemente in die anfangs leere Warteschlange einfügen. Das Verfahren erinnert an »Sortieren durch Einfügen« mit dem Unterschied, dass die *Ausgabe*daten nicht konkret sind, sondern abstrakt. Statt das Peano Entwurfsmuster zu verwenden, können wir auch das Leibniz Entwurfsmuster einsetzen und erhalten dann eine abstrakte Variante des »Sortierens durch Mischen«. Im Folgenden wollen wir uns eine weitere Alternative anschauen, die von Tennisturnieren inspiriert ist.

Um die beste Tennisspielerin zu ermitteln, kann man ein Turnier im K.-o.-System austragen (engl. knock-out tournament). Die Gewinnerin eines Spiels zieht in die nächste Runde ein, die Verliererin scheidet aus. Der Turnierverlauf lässt sich durch einen ***Turnierbaum***, einen binären Baum, repräsentieren, siehe Abbildung 5.20. Aus Gründen der Fairness und um möglichst viele Spiele gleichzeitig austragen zu können (Parallelverarbeitung wird auch in der Informatik immer wichtiger), ist der Turnierbaum in der Regel vollständig ausgeglichen. Dies setzt voraus, dass die Gesamtzahl der Spielerinnen eine exakte Zweierpotenz ist.

Die folgenden Funktionen übertragen die Idee des Tennisturniers auf das Problem der Konstruktion einer Prioritätswarteschlange.

```
// play-round : (PQueue ⟨'elem⟩) list → PQueue ⟨'elem⟩ list when 'elem : comparison
let rec play-round = function
  | [ ]          → [ ]
  | [q1 ]        → [q1 ]
  | q1 :: q2 :: qs → meld (q1, q2) :: play-round qs

// tournament : (PQueue ⟨'elem⟩) list → PQueue ⟨'elem⟩ when 'elem : comparison
let rec tournament = function
  | [ ]  → empty
  | [q] → q
  | qs   → tournament (play-round qs)

let from-list (xs : 'elem list) = tournament [for x in xs → single x]
```

Wir überführen die Listenelemente zunächst in einelementige Warteschlangen. In einer Turnierrunde werden jeweils zwei benachbarte Warteschlangen verschmolzen. Wenn die Eingabe von *play-round* die Länge n hat, dann umfasst die Ausgabeliste $\lceil n/2 \rceil$ Warteschlangen. Wir spielen soviele Runden wie nötig; die Funktion *play-round* wird solange aufgerufen, bis nur noch eine einzige Warteschlange übrigbleibt. Ein gewichtiger Unterschied zu einem Tennisturnier fällt vielleicht ins Auge: Wir verwalten eine Liste von Warteschlangen, nicht von Elementen, da wir nicht nur den Champion bestimmen wollen. Mit anderen Worten, Verliererinnen scheiden nicht sofort aus — später mehr dazu. Da der Turnierbaum von unten nach oben aufgebaut wird, spricht man auch von einem »bottom-up« Verfahren. Im Unterschied dazu ist »Sortieren durch Mischen« ein »top-down« Verfahren — Aufgabe 5.1.3 fragt nach einer alternativen »bottom-up« Implementierung.

Wie effizient ist *from-list*? *Wenn* wir davon ausgehen, dass *meld* in konstanter Zeit arbeitet, *dann* ergibt sich das folgende Bild. Die Hilfsfunktion *play-round* hat eine lineare Laufzeit; da sie in jedem Schritt die Anzahl der Warteschlangen ungefähr halbiert, ist die Gesamtlaufzeit ebenfalls linear:

$$\frac{1}{1}n + \frac{1}{2}n + \frac{1}{4}n + \frac{1}{8}n + \cdots < 2 \cdot n$$

Ähnliche Überlegungen haben wir bei Analyse der Laufzeit von *quickselect* angestellt, siehe auch Abbildung 5.10. Aber ist die Annahme, dass *meld* lediglich konstante Zeit benötigt, realistisch? Schauen wir uns ein paar Implementierungsideen an, um ein Gefühl für den Arbeitsaufwand zu bekommen.

Implementierungsideen Vielleicht lassen sich die Implementierungen von endlichen Abbildungen aus Abschnitt 5.3 adaptieren?

- *ungeordnete Listen:* Das Einfügen ist schnell, aber das Auswählen des Minimums ist langsam (siehe »Sortieren durch Auswählen«).
- *Suchlisten:* Vor- und Nachteile kehren sich um; das Einfügen ist langsam (siehe »Sortieren durch Einfügen«), während das Auswählen schnell ist.
- *Suchbäume:* Das kleinste Element in einem Suchbaum ist das linkeste Element. (Wenn wir uns die Größe der Teilbäume merken, dann unterstützen Suchbäume sogar Ordnungsstatistiken.) Einfügen und Auswählen arbeiten somit proportional zur Höhe der Bäume.

Leider unterstützt keine der obigen Datenstrukturen eine effiziente Implementierung von *meld*. Die Laufzeit ist jeweils linear zur Zahl der Elemente (bzw. linear zur Größe der ersten Liste im Fall von @).

Was können wir erwarten? Lässt sich eine geniale Implementierung finden, so dass alle Operationen (mit Ausnahme der Bulk-Operationen) in konstanter Zeit arbeiten? Die Antwort ist ein klares und entschiedenes »Nein!« Warum? Wenn wir die Bulk-Operationen komponieren,

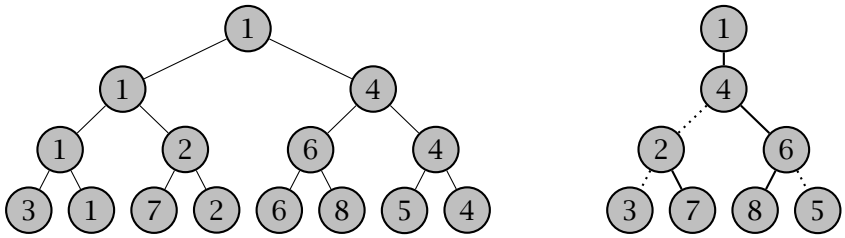
let heap-sort = from-list ≫ to-ord-list

erhalten wir ein abstraktes Sortierverfahren[14], »Sortieren mit Prioritätswarteschlangen«. Hätten sowohl *insert* als auch *split-min* eine konstante Laufzeit (oder *merge* und *split-min*), dann könnten wir in linearer Zeit sortieren. In Abschnitt 5.1.3 haben wir gezeigt, dass eben dies nicht möglich ist. Wir können messerscharf folgern, dass entweder das Einfügen (*insert* und *meld*) oder das Auswählen (*split-min*) mindestens eine logarithmische Laufzeit haben muss. Schade!

5.4.1. Turnierbäume

Wir brauchen eine zündende Idee. Vielleicht können wir Turnierbäume als Datenstruktur für die Implementierung von Prioritätswarteschlangen verwenden? Der linke untere Binärbaum korrespondiert zu dem Turnierbaum aus Abbildung 5.20 — wir haben lediglich die Spielerinnen durch die vermutete Spielstärke ersetzt (je kleiner, desto spielstärker).

[14] Alle bisher eingeführten Sortierverfahren lassen sich als konkrete Instanzen dieses Verfahrens deuten, je nachdem ob man Warteschlangen durch ungeordnete Listen, Suchlisten oder Suchbäume realisiert.



Ein Defekt fällt sofort ins Auge. Der Turnierbaum enthält Elemente mehrfach: Je besser eine Spielerin, je kleiner der numerische Wert, desto öfter tritt sie auf. Können wir die Redundanz eliminieren? In einem K.-o.-Turnier verliert jede Spielerin genau ein Match — mit Ausnahme des späteren Champions — so dass die Idee naheliegt, den Gewinnerbaum durch einen Verliererbaum zu ersetzen, so wie in der Grafik oben rechts, siehe auch Abbildung 5.21.

Der Champion wird zusätzlich oben auf den Verliererbaum gesetzt. Die durchgezogenen Linien deuten jeweils an, aus welcher Turnierhälfte die Verliererin kommt. Diese Information ist bedeutsam. So wissen wir zum Beispiel, dass 4 kleiner ist als alle Werte im rechten Teilbaum — Lindsay hat die rechte Turnierhälfte gewonnen. Über das Verhältnis zu den Werten aus dem linken Teilbaum ist hingegen nichts bekannt — mit den Teilnehmerinnen aus der linken Turnierhälfte hat Lindsay keine Spiele ausgetragen. Den »getoppten« Verliererbaum können wir durch ein Paar bestehend aus einem Element und einem Binärbaum repräsentieren. Diese Kombination nennt man aufgrund der Form auch ***Wimpel*** (engl. pennant). Ein Wimpel entspricht einem nicht-leeren Binärbaum mit einem leeren linken oder leeren rechten Teilbaum.

```
type Pennant ⟨'elem⟩ = 'elem * Tree ⟨'elem⟩
```

Die Funktion *versus* führt ein Spiel durch.

```
// versus : Pennant ⟨'elem⟩ * Pennant ⟨'elem⟩ → Pennant ⟨'elem⟩ when 'a : comparison
let versus ((a, t), (b, u)) =
  if a ⩽ b then (a, Node (u, b, t))        // b dominiert u
           else (b, Node (t, a, u))        // a dominiert t
```

Im Unterschied zu einem K.-o.-Spiel scheidet die Verliererin nicht unmittelbar aus. Ganz im Gegenteil: Mit Hilfe der Verliererbäume protokollieren wir den Turnierverlauf. Ein Detail ist bedeutsam: Wir arrangieren den Verliererbaum jeweils so, dass die Wurzel den *linken* Teilbaum dominiert. Mit anderen Worten, für jeden Knoten gilt, dass die Knotenmarkierung kleiner gleich den Elementen im linken Teilbaum ist. Binarbäume mit dieser Eigenschaft heißen auch ***Semi-Heaps***. (In einem ***Heap*** dominiert die Knotenmarkierung jeweils beide Teilbäume; in einem Semi-Heap nur einen.)

Die Elemente auf einem Pfad entlang der *durchgezogenen* Linien sind jeweils aufsteigend geordnet (von oben nach unten). Während die Elemente in einem Suchbaum *horizontal* angeordnet sind, sind die Elemente in einem Semi-Heap bzw. in einem Heap *vertikal* angeordnet.

Anders als in der Tenniswelt können unsere Turniere auch leer sein: die Operation *empty* soll ja eine leere Warteschlange repräsentieren, so dass wir einen nicht-rekursiven Variantentyp als Implementierungstyp verwenden.

```
type PQueue ⟨'elem when 'elem : comparison⟩ =
  | Inf
  | Min of Pennant ⟨'elem⟩
```

Die leere Warteschlange wird durch *Inf* repräsentiert; eine nicht-leere Warteschlange durch *Min* (a, t), wobei a das kleinste Element ist — a ist der Champion, t der Verliererbaum. (Alternativ hätten wir als Implementierungstyp *Pennant* ⟨*'elem*⟩*option* verwenden können. Die Konstruktornamen *Inf* und *Min* machen den Code etwas lesbarer.) Die Grafiken und die Typdefinition verdeutlichen, dass unsere Warteschlangen Zwitterwesen sind: Sie fangen als Liste an und hören als Binärbaum auf.

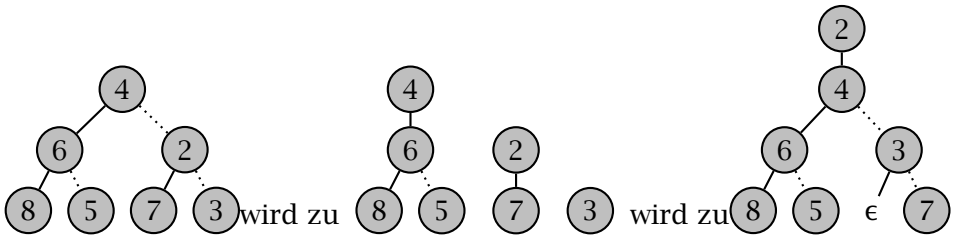
Nach diesen Vorarbeiten können wir zur Implementierung der Operationen schreiten.

```
let empty = Inf

let single x = Min (x, Leaf)

let meld = function
  | (Inf, q) | (q, Inf)          → q
  | (Min (a, t), Min (b, u)) → Min (versus ((a, t), (b, u)))
```

Bei der Implementierung von *meld* nutzen wir aus, dass *empty* das neutrale Element der Vereinigung ist. Wenn beide Warteschlangen nicht-leer sind, tragen wir ein Spiel aus. Vielleicht überraschend: *meld* arbeitet in konstanter Zeit. Mit einer einzigen Vergleichsoperation können wir zwei Warteschlangen verschmelzen.

Da *meld* und somit *insert* eine konstante Laufzeit haben, muss *split-min* notwendigerweise mindestens eine logarithmische Laufzeit an den Tag legen. Bei einem Tennisturnier erhält die Verliererin des Endspiels den zweiten Preis. Das Preisgeld ist vielleicht verdient, aber nicht gerechtfertigt: Die Verliererin dominiert ja nur eine Turnierhälfte; damit ist sie im ungünstigsten Fall lediglich besser als die Hälfte der Teilnehmerinnen.[15] Dieser Fall tritt ein, wenn die besten Spielerinnen »zufällig« in der gleichen Turnierhälfte gesetzt sind — eine Situation, die man mit Hilfe von Ranglisten zu vermeiden versucht.

In unserem Beispiel ist die Verliererin lediglich die 4-beste Spielerin. Welche Spielerinnen kommen für den 2. Preis überhaupt in Frage? Das sind diejenigen, die gegen den späteren Champion verloren haben! In dem Verliererbaum lassen sich die Elemente leicht lokalisieren; sie befinden sich auf dem Pfad von der Wurzel zu dem *rechtesten* Blatt, da vereinbarungsgemäß jede Knotenmarkierung den *linken* Teilbaum dominiert. Zwischen diesen Teilnehmerinnen muss der 2. Platz ausgespielt werden.



(5.6)

Wir machen eine interessante Beobachtung: Ein Binärbaum korrespondiert zu einer Liste von Wimpeln! In der Funktion *second-best* werden diese von rechts nach links miteinander verschmolzen (streng nach dem Struktur Entwurfsmuster für Listen). Die resultierende Warteschlange enthält sieben Elemente und kann somit nicht mehr vollständig ausgeglichen sein: Spielerin 3 ist

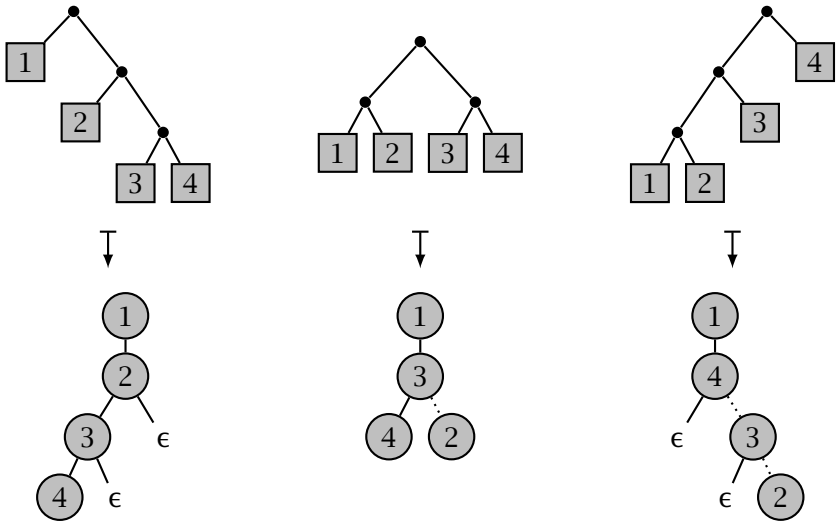
[15] Charles Lutwidge Dodgson besser bekannt als Lewis Carroll hat früh auf dieses Problem hingewiesen und in der Abhandlung »Lawn Tennis Tournaments, The True Method of Assigning Prizes with a Proof of the Fallacy of the Present Method.« eine alternative Turnierplanung entwickelt.

gleich in der 1. Runde gegen den Champion ausgeschieden und dominiert damit einen leeren linken Teilbaum (durch ϵ repräsentiert).

```
// second-best : Tree ⟨'elem⟩ → PQueue ⟨'elem⟩ when 'elem : comparison
let rec second-best = function
  | Leaf          → Inf
  | Node (t, a, u) → meld (Min (a, t), second-best u)
let split-min = function
  | Inf        → None
  | Min (a, t) → Some (a, second-best t)
```

Der Typ von *second-best* verdeutlicht, dass die Funktion einen Verliererbaum in eine Warteschlange überführt. Da der Baum von der Wurzel bis zum rechtesten Blatt traversiert wird, ist die Laufzeit von *second-best* und somit von *split-min* proportional zur Höhe des Verliererbaums. Wie bei Suchbäumen wird die Laufzeit nicht nur von der Gesamtzahl der Knoten beeinflusst, sondern auch von der Gestalt des Binärbaums.

Ist der zugrundeliegende Turnierbaum ausgeglichen, dann ist die Laufzeit logarithmisch — das ist asymptotisch optimal. Erfreulicherweise konstruiert zum Beispiel die Default-Implementierung von *from-list* einen balancierten Turnierbaum. Daraus folgt insbesondere, dass *heap-sort* eine linear-logarithmische Laufzeit hat — das ist ebenfalls asymptotisch optimal. Wo Licht ist, da fällt auch Schatten. Ist der Turnierbaum degeneriert — ist er zum Beispiel links- oder rechtsschief — dann ist auch die resultierende Warteschlange degeneriert. Im Unterschied zu Suchbäumen gilt die Gleichung »degenerierter Baum = schlechte Laufzeit« aber *nicht*. Die folgenden Beispiele illustrieren warum — die schwarzen, inneren Knoten entsprechen einem Aufruf von *meld*, die quadratischen, äußeren Knoten einem Aufruf von *single*.



Die drei resultierenden Warteschlangen enthalten jeweils die gleichen Elemente. Im ersten Fall ist die Warteschlange zwar *links*schief, aber das ist tatsächlich vorteilhaft, da *second-best* stets nach *rechts* läuft! Die durchgezogenen Linien deuten an, dass wir die vollständige Ordnung der Elemente kennen. Der ausgeglichene Baum in der Mitte ist somit weniger vorteilhaft. Am schlechtesten schneidet die *rechts*schiefe Warteschlange ab. Die gestrichelten Linien deuten an, dass wir über die relative Ordnung der Elemente im Verliererbaum überhaupt nichts wissen. Je mehr durchgezogene Linien, desto besser!

Nun mag der/die Leser/-in einwenden, dass man in der Praxis niemals einen unbalancierten Turnierplan aufstellen würde. Das mag für Tennis- oder Fußballturniere gelten, aber nicht für unsere Bibliothek, da wir schlicht und einfach keinen Einfluss darauf haben, wie die Schnittstelle

verwendet wird. Zum Beispiel könnte der/die Anwendungsprogrammierer/-in seine/ihre eigene Variante von *from-list* definieren und dabei streng nach dem Struktur Entwurfsmuster für Listen vorgehen.

```
let rec from-list = function
  | [ ]      → empty
  | x :: xs → meld (single x, from-list xs)        // oder: meld (from-list xs, single x)
```

Wenden wir *from-list* auf eine aufsteigend geordnete Liste an, erhalten wir einen linksschiefen Verliererbaum; für eine absteigend geordnete Liste einen rechtsschiefen Baum. (Warum?)

```
⋙ from-list [1..5]
Min (1, Node (Node (Node (Node (Leaf, 5, Leaf), 4, Leaf), 3, Leaf), 2, Leaf))
⋙ from-list [5..-1..1]
Min (1, Node (Leaf, 5, Node (Leaf, 4, Node (Leaf, 3, Node (Leaf, 2, Leaf)))))
```

Komponieren wir diese Version von *from-list* mit *to-ord-list* — wir wollen Listen sortieren — dann ergeben sich erhebliche Laufzeitschwankungen: Für aufsteigend geordnete Listen ist die Gesamtlaufzeit linear (*heap-sort* verhält sich wie »Sortieren durch Einfügen«), für absteigend geordnete Listen hingegen quadratisch (*heap-sort* verhält sich wie »Sortieren durch Auswählen«).

Wie können wir die Laufzeit von *second-best* verbessern? Wir diskutieren zwei Ansätze; der erste ist einfach zu implementieren, aber schwierig zu analysieren; die Implementierung des zweiten ist aufwändiger, aber dafür leichter zu analysieren.

5.4.2. Pairing-Heaps ⋆

Wie lässt sich die Laufzeit von *second-best* verbessern? Was haben wir für Optionen? Die Funktion geht konzeptionell in zwei Schritten vor (5.6): Im ersten Schritt wird der Verliererbaum in eine Liste von Warteschlangen überführt, die im zweiten Schritt von rechts nach links zu einer einzigen Warteschlange zusammengefasst werden.

```
second-best = spine ≫ right-to-left
```

Die Funktion *spine*, die den ersten Schritt implementiert, nimmt im Prinzip einen Repräsentationswechsel vor. Aufgrund der Invariante — die Verlierer dominieren die jeweils linke Turnierhälfte — ist ihre Definition allerdings in Stein gemeißelt.

```
// spine : Tree ⟨'elem⟩ → PQueue ⟨'elem⟩ list
let rec spine = function
  | Leaf          → [ ]
  | Node (t, a, u) → Min (a, t) :: spine u
```

Der Pfad von der Wurzel bis zu dem rechtesten Blatt wird auch bildhaft das rechte ***Rückgrat*** des Baums genannt (engl. right spine).

```
// right-to-left : (PQueue ⟨'elem⟩) list → PQueue ⟨'elem⟩ when 'elem : comparison
let rec right-to-left = function
  | [ ]      → empty
  | q :: qs → meld (q, right-to-left qs)
```

Die Funktion *right-to-left* ist die große Schwester von *from-list*: Statt einer Folge von Elementen verarbeitet sie eine Folge von Warteschlangen. (Die Implementierung von *from-list* auf Seite 254 lässt sich auf *right-to-left* zurückführen: *from-list* = *map single* ≫ *right-to-left*.) Die Definition von

right-to-left ist alles andere als in Stein gemeißelt, hier können wir mit unseren Optimierungsbemühungen ansetzen. Eine Alternative haben wir bereits implementiert: die Funktion *tournament*, die wiederholt Warteschlangen paarweise kombiniert.

Wäre *tournament* die bessere Wahl? Vielleicht. Die Frage ist tatsächlich schwierig zu beantworten, da wir die Gestalt der zugrundeliegenden Verliererbäume nicht kennen. Sind alle Bäume gleich groß, dann ist *tournament* eine gute Wahl; sind die Bäume absteigend der Höhe nach geordnet, dann sollten wir *right-to-left* den Vorzug geben. Da wir aber im Dunkeln stochern, liegt die Idee nahe, die beiden Strategien zu kombinieren — wie so oft im Leben macht es die gesunde Mischung. (Die Form der Binärbäume zunächst zu analysieren, ist übrigens keine Option — eine Analyse würde schlicht und einfach zu viel Zeit kosten.)

$$\mathit{second\text{-}best} = \mathit{spine} \gg \mathit{play\text{-}round} \gg \mathit{right\text{-}to\text{-}left}$$

Wir fügen einen zusätzlichen Transformationsschritt ein, in dem die Warteschlangen in einer Runde paarweise verschmolzen werden. Dieser zusätzliche Schritt gibt der Datenstruktur ihren Namen: engl. pairing heaps. Die Länge des Pfades von der Wurzel bis zu dem rechtesten Blatt bestimmt die Laufzeit von *second-best*; der Aufruf von *play-round* sorgt dafür, dass sich die Länge des Rückgrats mit jedem Aufruf ungefähr halbiert.

Die drei Schritte lassen sich zu einem zusammenfassen.

```
let rec second-best = function
  | Leaf                    → Inf
  | Node (t, a, Leaf)       → Min (a, t)
  | Node (t, a, Node (u, b, v)) → meld (meld (Min (a, t), Min (b, u)), second-best v)
```

Im Fachjargon sagt man auch, die drei Funktionen werden ***fusioniert***. Fusion ist eine wichtige Programmoptimierung; in unserem Fall sparen wir uns die Erzeugung und Verarbeitung von zwei intermediären Listen. Damit ist die Implementierung von Pairing-Heaps abgeschlossen; alle anderen Operationen übernehmen wir unverändert.

Es ist aufschlussreich, die neue Definition von *second-best* in Aktion zu sehen. Der Pairing-Heap in Abbildung 5.22 dient dabei als Ausgangspunkt. Alle Elemente im Verliererbaum befinden sich auf dem rechten Rückgrat — es liegt somit der schlechteste Fall vor. Wenn wir jetzt mit Hilfe von *split-min* die drei kleinsten Elemente entfernen, erhalten wir die in Abbildung 5.23 dargestellte Abfolge von Pairing-Heaps. Jeder Aufruf von *split-min* halbiert die Wegstrecke; nach der Entnahme von drei Elementen ist der zugrundeliegende Verliererbaum fast vollständig ausgeglichen. Man ist fast versucht zu sagen »auf wundersame Weise«, aber natürlich basiert das »Wunder« ausschließlich auf unseren Rechenregeln. Zum Vergleich: Die Implementierung von *split-min* aus Abschnitt 5.4.1 verkürzt die Wegstrecke jeweils nur um einen Knoten; insbesondere wird die rechtsschiefe Form nicht verändert.

Was haben wir erreicht? Zunächst einmal gilt es zu betonen, dass wir die Laufzeit von *split-min*, die im *schlechtesten* Fall auftritt, *nicht* verbessert haben. *Aber*, der schlechteste Fall wird nicht mehr so häufig auftreten, da die Bäume sich re-organisieren. Betrachtet man nicht isoliert die Laufzeit einer einzelnen Operation, sondern bestimmt die Laufzeit einer Folge von Operationen, so kann man zeigen, dass die über diese Folge ***amortisierte*** Laufzeit im Fall von *insert* und *meld* konstant und im Fall von *split-min* logarithmisch ist.[16] Die Analyse ist schwierig, da die Operationen beliebig geschachtelt werden können; zu schwierig für das erste Semester. Allerdings ist die Performanz von Pairing-Heaps zu gut und die Implementierung zu einfach, als dass wir sie hätten ignorieren wollen.

[16] In Wirklichkeit ist es noch komplizierter. Diese Aussage gilt nicht, wenn die *gleiche* Warteschlange als Eingabe für *mehrere* nachfolgende Operationen verwendet wird. Oder positiv ausgedrückt: Die Aussagen zur Laufzeit setzen voraus, dass jedes Zwischenergebnis höchstens einmal weiterverwendet wird. Man spricht in diesem Fall auch von einer ***ephemeralen*** Verwendung, im Gegensatz zu einer ***persistenten*** Verwendung.

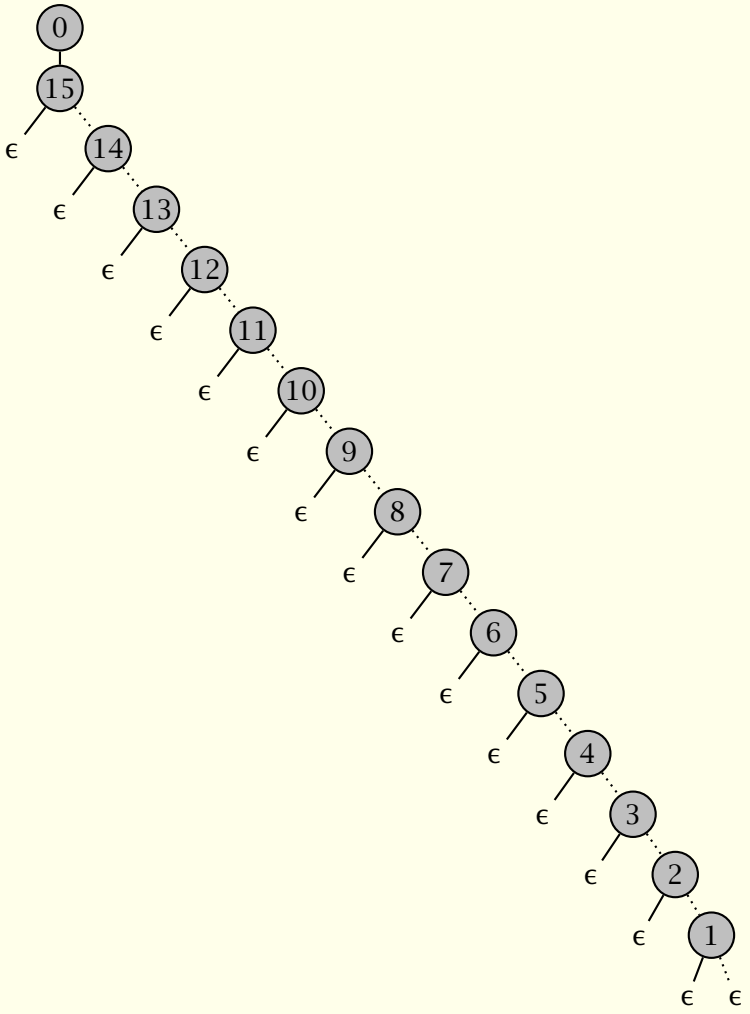


Abbildung 5.22.: Ein rechtsschiefer Pairing-Heap (*from-list* $[15\,..\,{-1}\,..\,0]$).

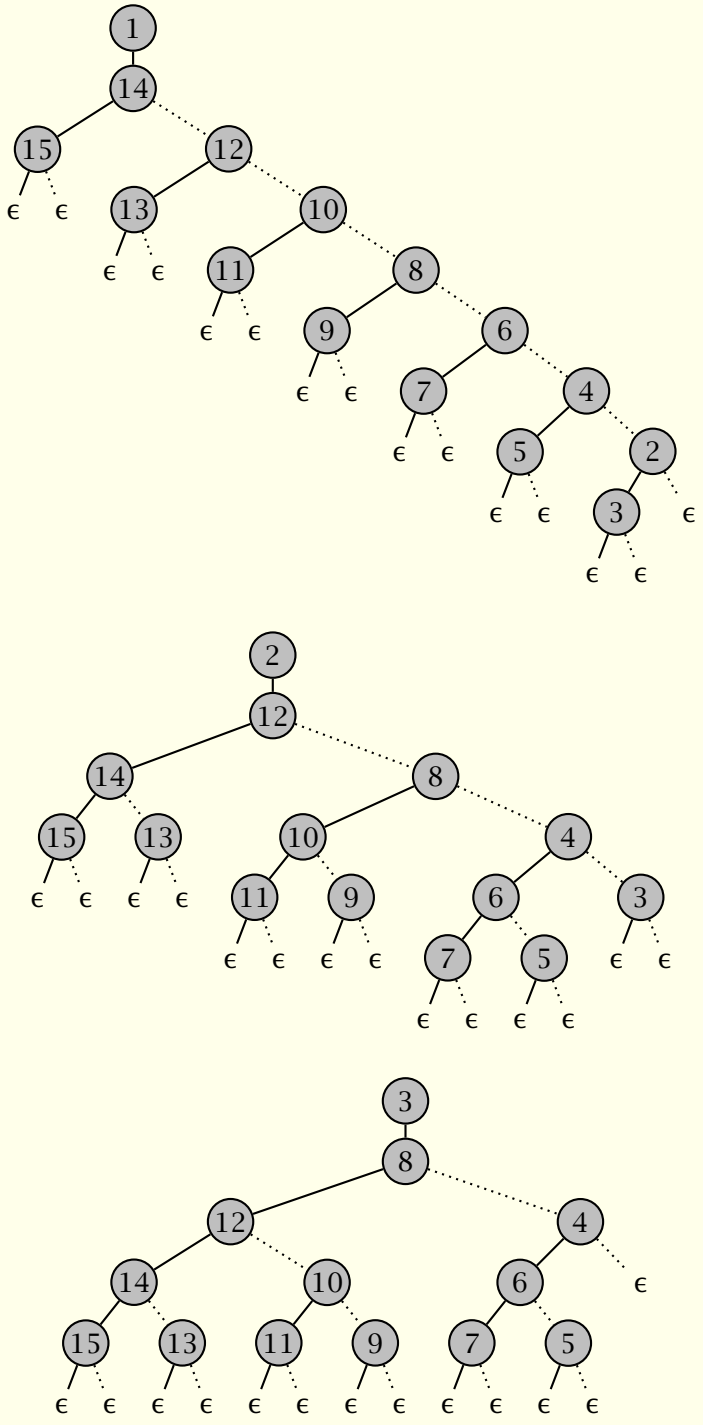


Abbildung 5.23.: Aus dem Pairing-Heap, siehe Abbildung 5.22, werden die drei kleinsten Elemente nacheinander entfernt.

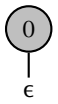
5.4.3. Binomial-Heaps ⋆

Zurück zum Ausgangspunkt. Die Metapher des Tennisturniers hat sich als hilfreich erwiesen, aber tatsächlich hinkt sie etwas. Die Aufstellung eines Turnierbaums ist zumindest konzeptionell einfacher als die Verwaltung einer Prioritätswarteschlange. Die Teilnehmer eines Turniers stehen vor dem Turnierstart fest — in der Regel gibt es eine festgelegte Zahl an Startplätzen, typischerweise eine exakte Potenz von 2, zum Beispiel 2^k. Ein Turnier ist also was die Struktur anbelangt eine eher ***statische*** Angelegenheit. Im Gegensatz dazu ist eine Prioritätswarteschlange ein ***dynamisches*** Gebilde: Elemente können peu à peu hinzugefügt werden; Minima können entfernt werden; Einfüge- und Auswahloperationen dürfen beliebig verschränkt werden.

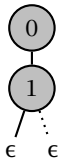
Das folgende Gedankenexperiment spinnt die Metapher etwas weiter mit dem Ziel, den dynamischen Aspekt einzufangen. Stellen wir uns vor, die Teilnehmer eines Turniers treffen zeitversetzt nacheinander ein. Wie können wir das Turnier trotz dieser widrigen Umstände organisieren? Insbesondere sollen die gleichen Spiele wie im statischen Fall ausgetragen werden, sobald 2^k Teilnehmer angekommen sind. Eine vielleicht naheliegende Idee ist, bei jeder Ankunft eines Teilnehmers, so viele Spiele wie möglich auszutragen. Es ergibt sich die folgende Abfolge von Spielen (um die Spiele einfach nachvollziehen zu können, entspricht die Spielstärke jeweils der Ankunftszeit):

Das Turnier beginnt.

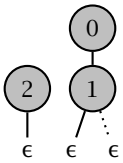
Der erste Spieler kommt.



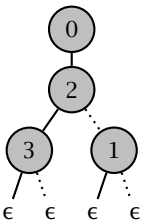
Der zweite Spieler kommt. Ein Spiel wird ausgetragen.



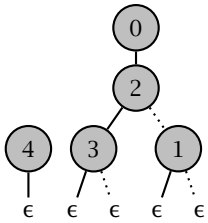
Der dritte Spieler kommt.



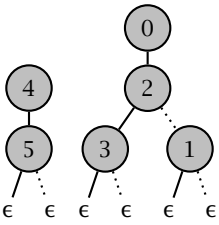
Der vierte Spieler kommt. Zwei Spiele werden ausgetragen.



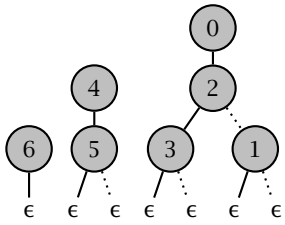
Der fünfte Spieler kommt.



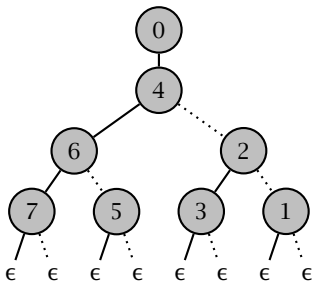
Der sechste Spieler kommt. Ein Spiel wird ausgetragen.



Der siebte Spieler kommt.

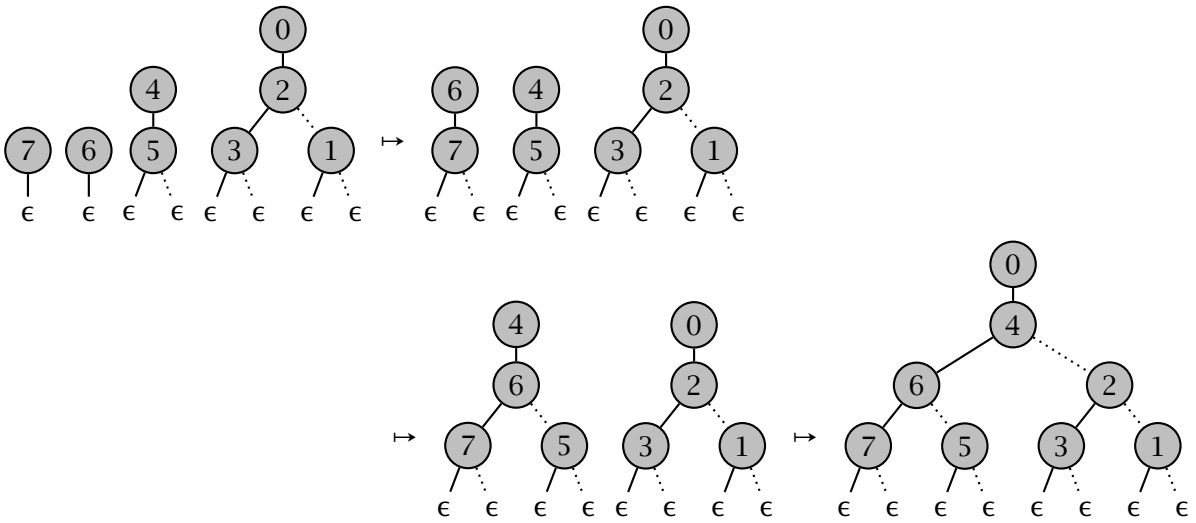


Der achte Spieler kommt. Drei Spiele werden ausgetragen.



Ein Spiel wird nur dann ausgetragen, wenn die beiden beteiligten Wimpel exakt die gleiche Form

besitzen und damit auch die gleiche Anzahl von Elementen enthalten. Jedes Spiel verdoppelt somit die Zahl der Elemente, so dass die Größe jedes Wimpels durch eine exakte Potenz von 2 gegeben ist. Nachdem 7 Teilnehmer eingetroffen sind, erhalten wir zum Beispiel eine Folge von Wimpeln der Größen 2^0, 2^1 und 2^2, da $7 = 1 + 2 + 4 = 2^0 + 2^1 + 2^2$. Trifft der 8. Teilnehmer ein, ergibt sich die folgende Abfolge von Spielen:



Wenn n die Anzahl der Teilnehmer ist, dann wird die Anzahl der Wimpel und deren Größe durch die Binärrepräsentation von n festgelegt. Leibniz lässt grüßen!

Das Gedankenexperiment legt nahe, eine Warteschlange durch eine Folge von Wimpeln darzustellen. Mehr noch: Wir modellieren die Repräsentation und die dazugehörigen Operationen nach dem Binärsystem! Was für eine wundervolle Idee: Ein Zahlensystem dient als Blaupause für einen Containertyp.

```
type Bit ⟨'elem⟩ =
  | O                          // 0
  | I of Pennant ⟨'elem⟩       // 1
type PQueue ⟨'elem⟩ =
  | Rep of List ⟨Bit ⟨'elem⟩⟩
```

Eine Warteschlange wird durch eine Liste von Binärziffern repräsentiert. Diese Datenstruktur hört auf den Namen ***Binomial-Heap*** (engl. binomial heap) — aus Gründen, auf die wir hier nicht näher eingehen wollen.

Das Binärsystem ist ebenso wie das uns vertraute Dezimalsystem ein ***Stellenwertsystem***: Jede Ziffer hat abhängig von ihrer Position in einer Zahl eine festgelegte Wertigkeit. In einem Binomial-Heap gesellen sich zu den Ziffern Datenstrukturen: Hat die Ziffer d die Wertigkeit 2^i, dann wird der Ziffer ein Wimpel der Größe $d \cdot 2^i$ zur Seite gestellt. Fügen wir ein Element zu einem Binomial-Heap hinzu, dann wird die Binärzahl entsprechend inkrementiert (aus Gründen der Lesbarkeit kürzen wir *Leaf* und *Node* durch den ersten Buchstaben ab):

```
>>> from-list [4..-1..0]
Rep [I (4,L);O;I (0,N (N (L,3,L),2,N (L,1,L)))]
>>> insert (5,it)
Rep [O;I (4,N (L,5,L));I (0,N (N (L,3,L),2,N (L,1,L)))]
>>> insert (6,it)
Rep [I (6,L);I (4,N (L,5,L));I (0,N (N (L,3,L),2,N (L,1,L)))]
>>> insert (7,it)
Rep [O;O;O;I (0,N (N (N (L,7,L),6,N (L,5,L)),4,
                   N (N (L,3,L),2,N (L,1,L))))]
```

Im letzten Schritt inkrementieren wir 111 und erhalten die Binärzahl 0001 — die niedrigstwertige Ziffer steht also links (nicht rechts wie im Dezimalsystem). Wir werden sehen, dass jeder Übertrag, 1 + 1 = 01, der Austragung eines Spiels entspricht — aber wir greifen vor.

Ein Binomial-Heap enthält gewissermaßen die Repräsentation seiner Größe. Diese lässt sich ausrechnen, indem wir die zugrundeliegende Binärzahl in eine natürliche Zahl umwandeln.

```
let rec size = function
  | []      → 0
  | O  :: ps → 0 + 2 * size ps
  | I _:: ps → 1 + 2 * size ps
```

Wenden wir uns den Operationen auf Warteschlangen zu. Wie schon angedeutet, verfolgen wir die grundlegende Idee, die korrespondierenden Operationen auf Binärzahlen als Blaupause zu verwenden.

Zahlensystem	*Containertyp*
0	leerer Container
1	einelementiger Container
Nachfolgerfunktion\Inkrement	Einfügen eines Elements
Addition	Vereinigung zweier Container

Die leere Warteschlange wird durch die leere Ziffernfolge repräsentiert; die einelementige Warteschlange entsprechend durch die einelementige Ziffernfolge. Der Ziffer 1 bzw. *I* wird dabei der Wimpel $(a, Leaf)$ zur Seite gestellt.

```
let empty = Rep []
let single a = Rep [I (a,Leaf)]
```

Die Nachfolgerfunktion erhöht ihr Argument um 1. Auch dieser Eins muss ein Wimpel der entsprechenden Größe beigefügt werden. Aus diesem Grund erhält *succ* zwei Argumente: einen Wimpel für den impliziten Übertrag und einen Binomial-Heap.

```
let rec succ p = function
  | []      → [I p]
  | O :: ps  → I p :: ps
  | I q :: ps → O :: succ (versus (p,q)) ps          // 1 + 1 = 01
let insert (a,Rep q) = Rep (succ (a,Leaf) q)
```

Beim initialen Aufruf wird der Nachfolgerfunktion der Wimpel $(a, Leaf)$ mitgegeben — der initiale Übertrag hat das Gewicht $2^0 = 1$. Dieser Wimpel wird in den ersten beiden Fällen der Ziffer 1 bzw. *I* zur Seite gestellt. Ergibt sich eine Übertrag, so tragen wir ein Spiel aus: $versus\ (p, q)$. Dabei ist

sichergestellt, dass die Ziffern das gleiche Gewicht besitzen und sich somit die Größe des Wimpels verdoppelt.

Der Schulalgorithmus für die Addition führt die Addition von Zahlen auf die Addition von Ziffern zurück. Dabei wird sichergestellt, dass die addierten Ziffern jeweils das gleiche Gewicht besitzen. Entsprechend führen wir die Vereinigung von Warteschlangen auf die Vereinigung von Wimpeln zurück.

```
let rec add = function
  | ([ ], ps) | (ps, [ ])  → ps
  | (O   :: ps, O   :: qs) → O   :: add (ps, qs)
  | (O   :: ps, I p :: qs)
  | (I p :: ps, O   :: qs) → I p :: add (ps, qs)
  | (I p :: ps, I q :: qs) → O   :: succ (versus (p, q)) (add (ps, qs))        // 1 + 1 = 01
let meld (Rep q1, Rep q2) = Rep (add (q1, q2))
```

Wenn beide Zahlen mit der Ziffer 1 anfangen, ergibt sich ein Übertrag, 1 + 1 = 01, den wir mit Hilfe von *succ* hinzuaddieren.

Die Implementierung von *split-min* ist am aufwändigsten, siehe Abbildung 5.24. Da ein Binomial-Heap aus einer Liste von Wimpeln besteht, lässt sich das kleinste Element, der Turniersieger, nicht länger in konstanter Zeit bestimmen. Die Wimpelliste repräsentiert ja ein noch nicht vollständig ausgetragenes Turnier. Die Operation *split-min* geht konzeptionell in drei Schritten vor:

1. Der Binomial-Heap wird in den Wimpel mit der kleinsten Wurzel und dem restlichen Heap aufgespalten (*split-min-pennant*). Der extrahierte Wimpel wird dabei durch die Ziffer 0 ersetzt. Die Wurzel des extrahierten Wimpels ist das gesuchte minimale Element.

2. Der Verliererbaum des extrahierten Wimpels wird in eine Liste von Wimpeln überführt (*spine*). Dabei werden die Wimpel der Größe nach *absteigend* angeordnet. Wir erhalten einen Binomial-Heap, indem wir die Liste spiegeln (*rev*) und jeden Wimpel mit der Ziffer 1 »taggen« (*map I*).

3. Die Binomial-Heaps aus den ersten beiden Schritten werden anschließend miteinander verschmolzen (*add*).

Ähnlich wie bei Pairing-Heaps wird *split-min* summa summarum auf *meld* zurückgeführt. Im Unterschied zu Pairing-Heaps wird aber eine Warteschlange nicht mehr durch einen einzigen Wimpel, sondern durch eine Liste von Wimpeln repräsentiert.

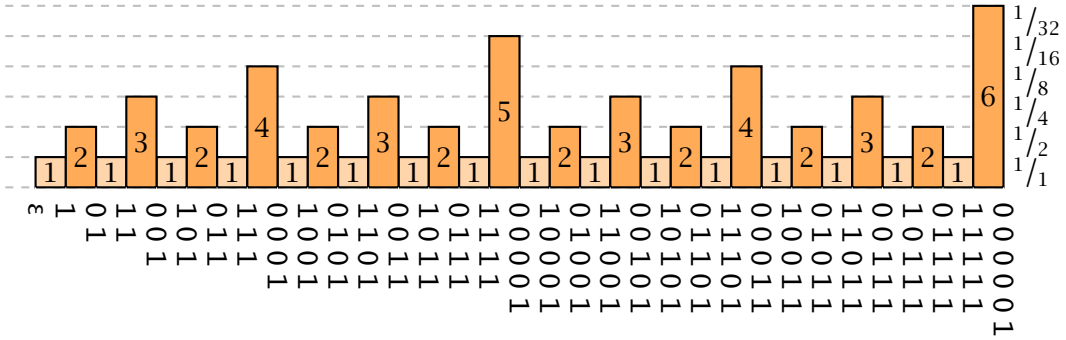
Amortisierte Analyse der Laufzeit Kommen wir zur Analyse der Laufzeit. Da Binomial-Heaps auf dem Binärsystem basieren, »vererben« sich die Eigenschaften des Zahlensystems und seiner Operationen. Zur Erinnerung: Die Zahl n wird im Binärsystem durch $\lceil \lg(n+1) \rceil$ Binärziffern repräsentiert. Entsprechend besteht ein Binomial-Heap der Größe n aus maximal $\lceil \lg(n+1) \rceil$ Wimpeln. Damit ist klar, dass die Operationen *insert*, *meld* und *split-min* im schlechtesten Fall eine logarithmische Laufzeit besitzen. Gegenüber Pairing-Heaps hat sich die Laufzeit von *split-min* verbessert, allerdings auf Kosten der Laufzeit von *meld*.

Vielleicht überraschend ist die Tatsache, dass *insert* in *amortisiert konstanter* Zeit arbeitet. Im schlechtesten Fall ist die Laufzeit von *insert* logarithmisch, nämlich dann, wenn die Binärzahl aus einer Folge von Einsen besteht. In diesem Fall kaskadiert der Übertrag bis an das Ende der Ziffernfolge und hinterlässt dabei eine Folge von Nullen, gefolgt von einer Eins. Damit kann der schlechteste Fall nicht unmittelbar wieder auftreten. Ganz im Gegenteil: Die nächsten Einfügeoperationen sind sehr günstig. Mit anderen Worten, wenn wir die Laufzeit von n Einfügeoperationen

```
let empty = Rep [ ]
let single a = Rep [I (a, Leaf)]
let rec succ = function
  | [ ]       → [I p]
  | O :: ps   → I p :: ps
  | I q :: ps → O :: succ (versus (p, q)) ps
let insert (a, Rep q) = Rep (succ (a, Leaf) q)
let rec add = function
  | ([ ], ps) | (ps, [ ])  → ps
  | (O :: ps, O :: qs)     → O :: add (ps, qs)
  | (O :: ps, I p :: qs)
  | (I p :: ps, O :: qs)   → I p :: add (ps, qs)
  | (I p :: ps, I q :: qs) → O :: succ (versus (p, q)) (add (ps, qs))
let meld (Rep q1, Rep q2) = Rep (add (q1, q2))
let rec split-min-pennant = function
  | [ ]       → None
  | O :: ps → match split-min-pennant ps with
                | None          → None
                | Some (q, [ ]) → Some (q, [ ])
                | Some (q, qs)  → Some (q, O :: qs)
  | I p :: ps → match split-min-pennant ps with
                | None          → Some (p, [ ])
                | Some (q, qs) → if fst p ⩽ fst q then Some (p, O :: ps)
                                                  else Some (q, I p :: qs)
let rec spine = function
  | Leaf           → [ ]
  | Node (t, a, u) → (a, t) :: spine u
let split-min (Rep ps) =
  match split-min-pennant ps with
  | None               → None
  | Some ((a, t), qs) → Some (a, Rep (add (map I (rev (spine t)), qs)))
```

Abbildung 5.24.: Implementierung von Binomial-Heaps.

mit $n \lg n$ abschätzen, ist das viel zu pessimistisch, da der schlechteste Fall nicht in jedem Schritt auftreten kann. Tatsächlich ergibt sich das folgende Bild:

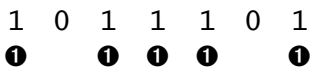


Wir zählen binär von 0 bis $n = 32$. Auf der y-Achse ist jeweils die Laufzeit der Nachfolgerfunktion aufgetragen. Die Gesamtlaufzeit von n Inkrements entspricht der Gesamtfläche aller Balken. Addieren wir die Flächen von unten nach oben auf, erhalten wir eine uns wohlbekannte Formel, siehe auch Abbildung 5.10.

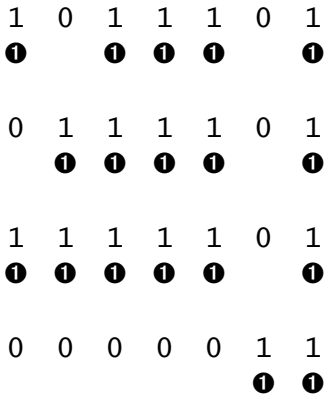
$$\frac{1}{1}n + \frac{1}{2}n + \frac{1}{4}n + \frac{1}{8}n + \cdots < 2 \cdot n$$

Amortisiert über eine Folge von Operationen ist die Laufzeit der Nachfolgerfunktion somit konstant — die Überlegungen gelten gleichermaßen für die Einfügeoperation *insert*. Einzelne »teure« Operationen werden durch viele »günstige« Operationen ausgeglichen.

Die Vorstellung, dass günstige für teure Operationen bezahlen, lässt sich präzisieren, indem wir Ziffern *gedanklich* mit Geldmünzen dekorieren:



Die Münzen repräsentieren Zeitguthaben (Momo und die Grauen Herren lassen grüßen), mit denen Rechenschritte bezahlt werden können. In unserem Fall ist die Ziffer 1 jeweils mit einer 1€ Münze dekoriert. Die Nachfolgerfunktion erhält diese ***Invariante*** und muss dafür 2€ aufwenden. Im Detail: Die Nachfolgerfunktion wandelt eine Folge von 1en in 0en um und eine 0 in eine 1. Die ersten Schritte ($1 \to 0$) bezahlen wir mit den hinterlegten Münzen; für den letzten Schritt ($0 \to 1$) müssen wir 1€ in Rechnung stellen. Zusätzlich müssen wir eine 1€ Münze hinterlegen, mit der zukünftige Operationen bezahlt werden.



Summa summarum entstehen für jeden Aufruf der Nachfolgerfunktion Kosten von 2€. Wir können die Operationen der Schnittstelle auch bunt mischen, zum Beispiel *insert* und *split-min* alternieren — die Analyse hat weiterhin Bestand.

Die vorgestellte Technik zur amortisierten Laufzeitanalyse heißt im Fachjargon ***Bankkonto-Methode*** (engl. banker's method). Die Methode basiert auf einer zentralen Annahme, die wir im letzten Abschnitt bereits zart angedeutet haben. Es wird vorausgesetzt, dass jedes Zwischenergebnis im weiteren Verlauf der Rechnung *höchstens einmal* weiterverwendet wird. Der Grund für diese Einschränkung ist vielleicht klar: Man kann jede Münze nur einmal ausgeben! Besteht eine Warteschlange aus einer Folge von Einsen und wir fügen in diese Warteschlange zwei verschiedene Elemente ein,

```
let q = from-list [1..1023]
in (insert (815, q), insert (4711, q))
```

dann können wir die Kosten der ersten Einfügeoperation aus den hinterlegten Geldmünzen begleichen, nicht aber die der zweiten Operation, oder gegebenenfalls einer dritten und vierten.

5.4.4. Laufzeitverhalten der Implementierungen

Ähnlich wie endliche Abbildungen lassen sich Prioritätswarteschlangen auf vielfältige Art und Weise implementieren. Die folgende Tabelle fasst das Laufzeitverhalten der vorgestellten Implementierungen zusammen.

	Wimpel	Pairing-Heaps	Binomial-Heaps
empty	1	1	1
single	1	1	1
insert	1	1	$1^\star$
meld	1	1	$\lg n$
split-min	n	$\lg n^\star$	$\lg n$
from-list	n	n	n
to-ord-list	$n \lg n$	$n \lg n$	$n \lg n$

* amortisierte Laufzeit

Pairing-Heaps unterscheiden sich von Wimpeln, getoppten Verliererbäumen, nur in der Implementierung der Operation *split-min*. Deren Laufzeit ist für beide Varianten im schlechtesten Fall linear; Pairing-Heaps garantieren allerdings eine *amortisiert* logarithmische Laufzeit. *Merkenswert:* Im Unterschied zu Suchbäumen lassen sich Prioritätswarteschlangen in linearer Zeit konstruieren.

Aber, wie schlagen sich die verschiedenen Implementierungen in der Praxis? Der folgende ***Micro-Benchmark*** vermittelt einen etwas oberflächlichen Eindruck. Wir verwenden Prioritätswarteschlangen, um verschiedene Listen der Länge 100000 zu sortieren.

Prioritätswarteschlange	aufsteigend	absteigend	zufällig	*from-list*
geordnete Listen	0.034	28:34.430	9:42.330	right-to-left
	0.290	0.270	0.430	bottom-up
Wimpel		stack overflow		right-to-left
	1.509	1.418	2.624	bottom-up
Pairing-Heaps	0.146	0.464	2.504	right-to-left
	0.413	0.371	2.556	bottom-up
Binomial-Heaps	1.310	1.329	4.164	right-to-left
	1.511	1.467	4.596	bottom-up
List.sortWith compare	0.018	0.019	0.029	

Die zu sortierenden Listen sind entweder aufsteigend geordnet ([1..100000]), absteigend geordnet ([100000..−1..1]), oder bestehen aus zufällig ausgewählten Elementen. (Mit dem Aufruf ***let*** *random* = *System.Random* (4711) erhält man einen Generator für sogenannte ***Pseudozufallszahlen***. Der Ausdruck [***for*** *i* ***in*** 1..100000 → *random.Next* ()] generiert die verwendete Liste von zufälligen Elementen; *random.Next* () erzeugt dabei bei jedem Aufruf eine neue Pseudozufallszahl, stellt also keine Funktion im mathematischen Sinne dar). Die Laufzeit wird in der obigen Tabelle jeweils in Sekunden angegeben.

Man spricht übrigens von einem Micro-Benchmark, da ein einigermaßen künstliches Anwendungsszenario nachgestellt wird, das nur einen bestimmten Aspekt beleuchtet. Prioritätswarteschlangen unterstützen ja beliebige Abfolgen von Einfüge- und Auswahloperationen; beim Sortieren fügen wir zunächst wiederholt ein, um dann wiederholt auszuwählen — wir mischen die Operationen also nicht. Pairing-Heaps zählen zu den besten Implementierungen von Prioritätswarteschlangen in der Praxis; die Spitzenposition wird auch von der Tabelle bestätigt. Geordnete Listen schneiden allerdings auch prima ab, zumindest wenn die Bottom-up Variante von *from-list* verwendet wird (Seite 249). Das ist auch nicht weiter verwunderlich; in diesem Fall entspricht das Sortierverfahren dem »Sortieren durch Mischen«, einem guten Sortieralgorithmus. Daraus lässt sich nicht folgern, dass geordnete Listen die Datenstruktur der Wahl für Prioritätswarteschlangen sind. Ganz im Gegenteil: Wird die right-to-left Implementierung von *from-list* eingesetzt (Seite 254), dann erhalten wir »Sortieren durch Einfügen« — die Tabelleneinträge belegen die schlechte, da quadratische Laufzeit. Man sieht: Ein einzelner Micro-Benchmark kann in die Irre führen.

5.5. Projekt: Graphen und Graphalgorithmen ⋆

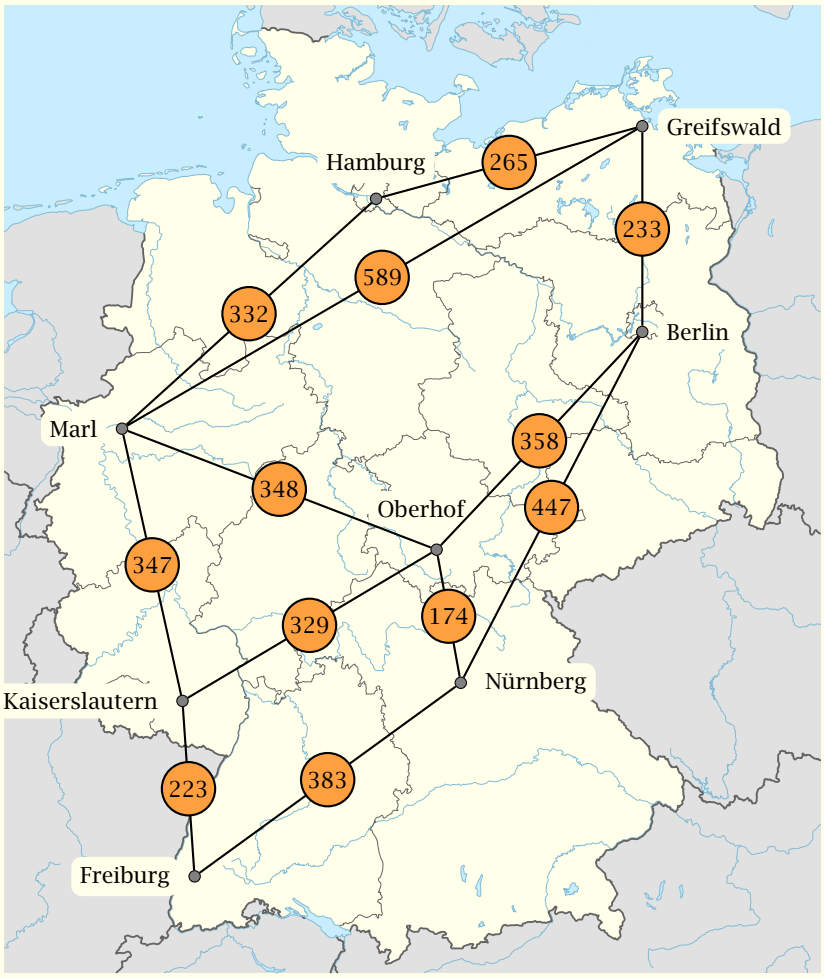
And Now for Something Completely Different.

— Monty Python

Zum Abschluss des Kapitels unternehmen wir einen Ausflug in die Welt der Graphen und Graphalgorithmen. Ein Stammbaum, das U-Bahn-Netz einer Großstadt, ein soziales Netzwerk, das World-Wide-Web — das sind nur einige Beispiele für Graphen. Graphen verallgemeinern baumartige Strukturen und spielen eine wichtige Rolle sowohl bei der Modellierung als auch bei der konkreten Umsetzung dieser Modelle auf dem Rechner. Wir gehen die Schritte von der Modellierung eines Problems bis zur rechnerischen Lösung exemplarisch an einer konkreten Aufgabe durch. Tatsächlich lösen wir nicht nur ein Problem, sondern eine ganze Klasse verwandter Optimierungsprobleme und lernen dabei die Segnungen der Abstraktion kennen: Die Mathematiker/-innen nennen es Algebra, die Informatiker/-innen Schnittstelle (engl. interface).

5.5.1. Eine Familie von Optimierungsproblemen

Kürzeste Wege Harry möchte von Freiburg nach Greifswald reisen und hat sich bei einer Mitfahrzentrale verschiedene Optionen eingeholt. Leider fährt niemand die gesamte Strecke, so dass Harry mehrfach die Mitfahrgelegenheit wechseln muss, siehe Abbildung 5.25. Da die einzelnen Fahrten nach der Weglänge abgerechnet werden und Harry notorisch knapp bei Kasse ist, gilt es, den kürzesten Weg vom Start- zum Zielort zu ermitteln. Ein typisches ***Optimierungsproblem***: Aus verschiedenen Möglichkeiten (hier: unterschiedlichen Reiserouten) muss die beste (hier: die mit der minimalen Gesamtlänge) ausgewählt werden. Im vorliegenden Beispiel ist die Gesamtzahl der Reiserouten noch überschaubar, aber mit steigender Anzahl von Zwischenstopps explodieren die Möglichkeiten. Werden n Zwischenstopps angefahren, dann existieren insgesamt $n!$ Routen,



von \ *nach*	Berlin	Freiburg	Greifswald	Hamburg	Kaiserslautern	Marl	Nürnberg	Oberhof
Berlin			233				447	358
Freiburg					223		383	
Greifswald	233			265		589		
Hamburg			265			332		
Kaiserslautern		223				347		329
Marl			589	332	347			348
Nürnberg	447	383						174
Oberhof	358				329	348	174	

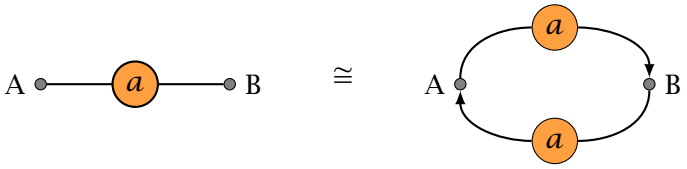
Abbildung 5.25.: Kürzeste Wege, Entfernungstabelle (direkte Wege, Angaben in km).

wenn wir im extremsten Fall davon ausgehen, dass zwischen allen Orten eine direkte Verbindung existiert. Kurzum: Wir haben es mit einem interessanten Problem zu tun.

In Abbildung 5.25 werden die »Rohdaten« auf zwei verschiedene Weisen dargestellt, einmal als ***gewichteter Graph*** und ein zweites Mal mit Hilfe einer Entfernungstabelle. Wir verwenden beide Darstellungen gleichberechtigt nebeneinander: Wir rechnen mit Tabellen (siehe Abschnitte 5.5.2 und 5.5.3), präferieren aber Graphen für kleinere Beispiele und zur Illustration der Rechenoperationen. Die Tabelle aus Abbildung 5.25 führt die Entfernungen der *direkten* Verbindungen auf; unser Ziel ist es, aus diesen Daten die Tabelle der kürzesten Verbindungen, direkt oder indirekt über Zwischenstopps, abzuleiten.[17]

Für die Lösung des Optimierungsproblems spielt es keine große Rolle, ob es sich bei den zugrundeliegenden Daten um Entfernungen (Länge in km), um die Reisezeit (Zeit in min) oder um die Fahrtkosten (Preis in €) handelt — die Markierungen müssen auch nicht notwendigerweise Zahlen sein. Allerdings müssen bestimmte Operationen auf den Daten unterstützt werden und diese Operationen müssen bestimmte Eigenschaften aufweisen, die wir im Folgenden motivieren wollen.

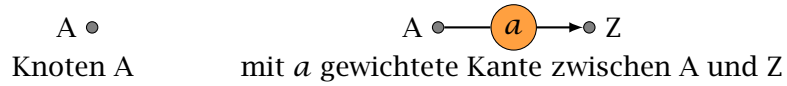
Gerichtete, gewichtete Graphen Ein Graph besteht aus ***Knoten*** ● und ***Kanten*** ●—● zwischen den Knoten, wobei die Kanten mit Markierungen oder ***Gewichten*** a versehen sind. Der Graph in Abbildung 5.25 ist ein sogenannter ***ungerichteter Graph***: Eine Kante zwischen zwei Knoten A und B kann in beide Richtungen durchlaufen werden, von A nach B und von B nach A. Um auch Einbahnstraßen modellieren zu können, betrachten wir allgemeiner ***gerichtete Graphen***: An die Stelle von Verbindungslinien treten Pfeile ●⟶●. Gerichtete Graphen verallgemeinern ungerichtete Graphen, da eine ungerichtete Kante durch zwei gerichtete Kanten ersetzt werden kann.



Sobald Gewichte ins Spiel kommen, sind ungerichtete Kanten eher die Ausnahme als die Regel, da sich Entfernungen, Reisezeiten oder Reisekosten oft für Hin- und Rückfahrt unterscheiden. Fassen wir zusammen: Ein Graph besteht aus Knoten und gerichteten, gewichteten Kanten zwischen Knoten.

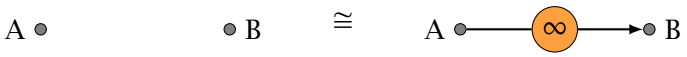
Tripel-G

Gerichtete, gewichtete Graphen verallgemeinern Relationen und besitzen vielfältige Anwendungen. Insbesondere werden sie gerne bei der Modellierung eingesetzt.



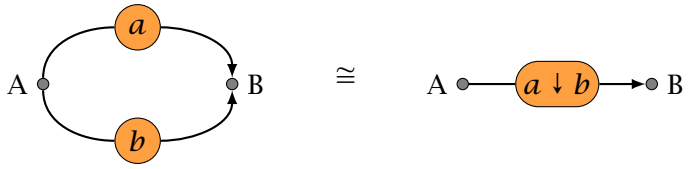
Knoten A — mit a gewichtete Kante zwischen A und Z

In einem Graphen ist nicht notwendigerweise jeder Knoten mit jedem anderen verbunden. Die Entfernungstabelle in Abbildung 5.25 weist zum Beispiel viele leere Einträge auf. Um diese mit Leben füllen zu können, fordern wir, dass es ein Element gibt, mit dem das Gewicht einer nichtexistenten Kante repräsentiert werden kann. Im Fall von Entfernungen fällt der »unendlichen« Entfernung, symbolisiert durch ∞, diese Rolle zu.

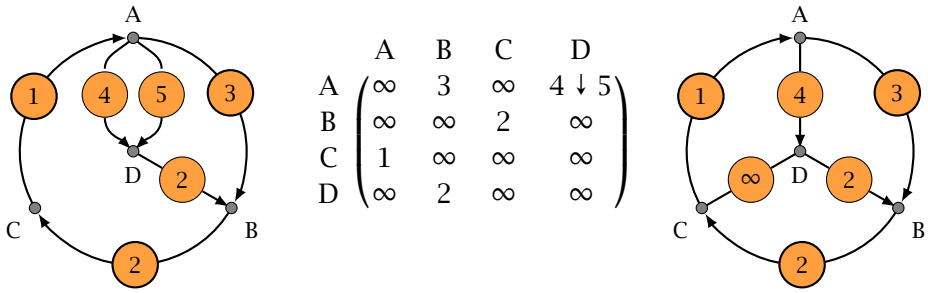


[17] Manchmal ist man auch nur an einem Eintrag oder an einer Zeile dieser Tabelle interessiert, dem »single-source shortest path«-Problem. Wir betrachten im Gegensatz dazu das sogenannte »all-pairs shortest path«-Problem.

Da wir ein Optimierungsproblem lösen, müssen sich Gewichte vergleichen lassen. Im Fall von Entfernungen bedeutet »besser« kürzer, das bessere der Gewichte a und b ist somit durch das Minimum $a \downarrow b$ gegeben.

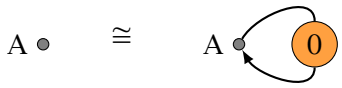


Mit diesen Vereinbarungen lässt sich jeder Graph in eine Tabelle überführen und umgekehrt. Zum Beispiel beschreiben die beiden folgenden Graphen das gleich Wegenetz wie die Tabelle:

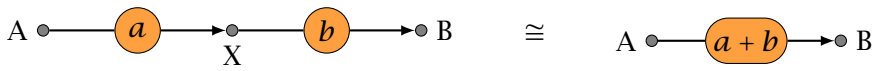


Der gleiche Graph kann ganz unterschiedlich gezeichnet werden, je nachdem, ob Mehrfachkanten zusammengefasst werden und ob »nicht-existente« Verbindungen eingezeichnet werden. (Abgesehen davon können die Knoten auch unterschiedlich plaziert werden oder aus Gründen der Übersichtlichkeit mehrfach gezeichnet werden.)

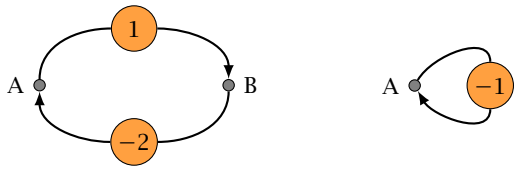
Eine Reise entspricht in der Terminologie von Graphen einem ***Pfad***. Ein Pfad von A nach B ist entweder leer (in diesem Fall gilt A = B), oder eine Kante von A nach B (eine direkte Verbindung) oder ein zusammengesetzter Pfad, bestehend aus einem Pfad von A nach X und einem Pfad von X nach B, wobei X ein Zwischenstopp ist. Die »Algebra der Pfade« detailliert, wie die Gewichte von Pfaden berechnet werden. Um dem leeren Pfad ein Gewicht zuweisen zu können, fordern wir die Existenz eines »kostenneutralen« Gewichts, der Zahl 0 im Fall von Entfernungen.



Um das Gewicht zusammengesetzter Pfade angeben zu können, müssen sich Gewichte »summieren« lassen.



Geringste Kosten Wir haben schon angesprochen, dass die Gewichte auch Kosten repräsentieren können (Preise in € oder ¢). Während Entfernungen nichtnegativ sind, spricht prinzipiell nichts dagegen, auch negative Kosten, sprich Gewinne, zuzulassen. (So wie es umgekehrt auch Negativzinsen für Bankguthaben gibt.) Die Existenz negativ gewichteter Kanten hat allerdings interessante Konsequenzen.



In beiden Graphen führt eine Rundreise von A nach A zu Kosten von -1 €, sprich einem Gewinn von einem Euro. Da eine Rundreise beliebig oft wiederholt werden kann, lassen sich beliebig große Gewinne erzielen. Wie das rechte Beispiel zeigt, tritt das Phänomen auch in Graphen auf, die nur aus einem einzigen Knoten und einer einzigen Kante bestehen — eine Kante mit gleichem Start- und Zielknoten nennt man auch ***Schleife***. Um diese Situation zu modellieren, setzen wir neben ***Vereinigung*** und ***Komposition***, einen dritten Operator auf Gewichten voraus, die ***Wiederholung*** oder den Sternoperator a^*. Für unser laufendes Beispiel, Gewichte als Kosten, ist der Operator wie folgt definiert.

$$a^* = \begin{cases} 0 & \text{falls } a \geqslant 0 \\ -\infty & \text{falls } a < 0 \end{cases}$$

Der Operator a^* ermittelt die geringsten Kosten einer mit a markierten Schleife: 0, wenn a nichtnegativ ist (wir bleiben zuhause), und $-\infty$ sonst (wir drehen uns im Kreis).

Maximale Durchfahrtshöhe Lisas Vater, Leo Lista, arbeitet bei einem Speditionsunternehmen und ist dort für die Routenplanung zuständig. Die Lastwagen fahren überwiegend ländliche Ziele an. Auf den Strecken liegen Brücken und Tunnel, so dass Durchfahrtsbeschränkungen beachtet werden müssen: Nur Fahrzeuge unter einer festgelegten tatsächlichen Höhe dürfen passieren. Leo muss unter allen möglichen Routen von einem Start- zu einem Zielort diejenige mit der *maximalen* Durchfahrtshöhe bestimmen, wobei sich die Höhe einer einzelnen Route als *Minimum* der Durchfahrtshöhen der Streckenabschnitte ergibt. Die Straßenverkehrsordnung kennt verschiedene Beschränkungen: der Masse, der Achslast, der Breite, der Höhe und der Länge (Zeichen 262–266).

Das allgemeine Problem firmiert auch unter dem Namen ***Flaschenhalsproblem*** und ist eng verwandt mit dem Problem der kürzesten Wege.

Arbitrage Harrys Mutter, Helga Hacker, arbeitet bei einer Bank und ist dort für Währungsumrechnungen zuständig. Grundlage ihrer Arbeit sind Tabellen wie die folgende, die für je zwei Währungen den aktuellen Umrechnungskurs angeben (womöglich an verschiedenen Handelsplätzen).

		nach				
		CHF	EUR	GBP	JPY	USD
von	CHF	1	0,9429	0,83931	111,21	1,0327
	EUR	1,0605	1	0,89009	117,96	1,0953
	GBP	1,1913	1,1234	1	132,49	1,2303
	JPY	0,0089886	0,0084774	0,0075469	1	0,0092867
	USD	0,96785	0,91284	0,81264	107,67	1

Zum Beispiel können mit 1000€ rund 890£ erworben werden. Interessanterweise erhält man einen günstigeren Umrechnungskurs, wenn man einen Umweg wählt und zuerst Euros in japanische Yen umtauscht, EUR → JPY → GBP: $117{,}96 \cdot 0{,}0075469 = 0{,}890232324$. Für 1000€ bekommt man dann statt 890,09£ sogar 890,23£, also 14 Pence mehr. Aber es kommt noch besser:

Tauscht man eine Währung in eine andere um und wieder in die ursprüngliche zurück, macht man einen, wenn auch geringen Verlust, zum Beispiel, EUR → GBP → EUR: 0,89009 · 1,1234 = 0,999927106. Der Umweg über den Yen ergibt einen Umrechungsfaktor r, der größer ist als Eins, EUR → JPY → GBP → EUR: 117,96 · 0,0075469 · 1,1234 = 1,0000869927815998 =: r. Das heißt, bei einem Einsatz von 1000€ erzielt man 8¢ Gewinn! Das macht sich bescheiden aus, aber es hindert einen nichts daran, die Transaktion zu wiederholen (außer sich ändernde Kurstabellen). So lässt sich der Gewinn ins Unermessliche steigern: bei 1.000 Transaktionen ergibt sich ein Umrechungsfaktor von $r^{1.000} \approx 1{,}09$, bei 1.000.000 Transaktionen astronomische $r^{1.000.000} \approx 6 \cdot 10^{37}$.

Die Ausnutzung von Kursunterschieden wird ***Arbitrage*** genannt (von lat. arbitratus »freier Wille, Belieben«). Der Umrechnungstabelle sieht man nicht unmittelbar an, ob die Möglichkeit einer solchen Gewinnmitnahme besteht. Verringert sich, zum Beispiel, der Kurs GBP → EUR von 1,1234 auf 1,1233, dann lassen sich keine Gewinne mehr erzielen.

Kleene Algebra Die folgende Tabelle fasst die den Optimierungsproblemen zugrundeliegenden Operationen zusammen: Mit Hilfe der ***Komposition*** »·« werden aus den Gewichten der Kanten die Gewichte der Pfade berechnet; existieren alternative Pfade zwischen zwei Knoten, so wird mit Hilfe der ***Vereinigung*** »⊔« der optimale Pfad ausgewählt.

	kein Pfad	mehrere Pfade	leerer Pfad	Konkatenation von Pfaden	zyklischer Pfad
Kleene Algebra $(\mathbb{K}, \sqsubseteq)$	$\bot$	$a \sqcup b$	1	$a \cdot b$	a^*
Erreichbarkeit $(\mathbb{B}, \Rightarrow)$	*false*	$a \vee b$	*true*	$a \wedge b$	*true*
kürzeste Wege $(\mathbb{N} \cup \{\infty\}, \geqslant)$	∞	$a \downarrow b$	0	$a + b$	0
geringste Kosten $(\mathbb{Z} \cup \{-\infty, +\infty\}, \geqslant)$	$+\infty$	$a \downarrow b$	0	$a + b$	$\begin{cases} 0 & \text{falls } a \geqslant 0 \\ -\infty & \text{falls } a < 0 \end{cases}$
Flaschenhals $(\mathbb{N} \cup \{\infty\}, \leqslant)$	0	$a \uparrow b$	∞	$a \downarrow b$	∞
Arbitrage[a] $(\mathbb{Q}_{\geqslant 0} \cup \{\infty\}, \leqslant)$	0	$a \uparrow b$	1	$a \cdot b$	$\begin{cases} 1 & \text{falls } a \leqslant 1 \\ \infty & \text{falls } a > 1 \end{cases}$

[a] Die Trägermenge der »Arbitragealgebra« ist $\mathbb{Q}_{\geqslant 0} := \{\, q \in \mathbb{Q} \mid q \geqslant 0 \,\}$.

Die »Erreichbarkeitsalgebra« illustriert, dass die Gewichte nicht notwendigerweise Zahlen sein müssen: In einem System von Einbahnstraßen gibt ein Wahrheitswert an, ob eine Verbindung zwischen zwei Knoten *existiert* — dabei ist *eine* Verbindung (*true*) »besser« als *keine* Verbindung (*false*).

Wir haben bereits angedeutet, dass die Operationen nicht völlig beliebig gewählt werden können; formal müssen sie den Anforderungen einer sogenannten ***Kleene Algebra*** genügen. Wir besprechen zum Abschluss des Abschnitts die für unsere Anwendung wichtigsten Eigenschaften; eine ausführliche Motivation und Herleitung der Axiome finden Sie in Anhang B.6. Eine Kleene Algebra kombiniert zwei mathematische Strukturen, eine »Optimierungsalgebra« und eine »Pfadalgebra«, die in geeigneter Weise interagieren müssen.

Zur *Optimierungsalgebra*: Die Vereinigung $\sqcup$ ist assoziativ, kommutativ und idempotent mit $\bot$ als neutralem Element. Oder etwas knackiger im Mathematiksprech: $\sqcup$ und $\bot$ formen ein kommutatives, idempotentes Monoid. Ein derartiges Monoid entspricht einem ***Halbverband*** mit einem

kleinsten Element (siehe Anhang B.4). Die der Optimierung zugrundeliegende Ordnung (was bedeutet »besser«) leitet sich aus der Vereinigung ab:

$$a \sqsubseteq b \quad :\Longleftrightarrow \quad a \sqcup b = b$$

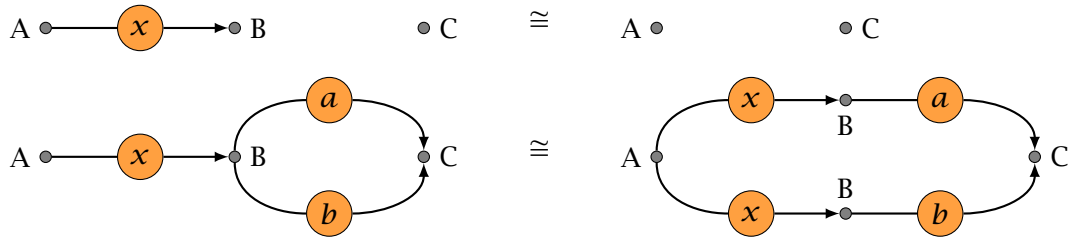
In der Kostenalgebra ist a besser als b, wenn a kleiner ist als b — die Kosten werden minimiert. In der Flaschenhalsalgebra verhält es sich umgekehrt: a ist besser als b, wenn a größer ist als b — die Flaschenhälse werden maximiert. Die algebraischen Eigenschaften haben übrigens die Wahl des Symbols »$\sqcup$« bestimmt: So wird üblicherweise das Supremum in einem Halbverband notiert.

Zur *Pfadalgebra*: Die Komposition »$\cdot$« ist assoziativ mit 1 als neutralem Element; »$\cdot$« und 1 formen ein Monoid. (In den obigen Beispielen hat die Komposition oft noch weitere Eigenschaften, sie ist, zum Beispiel, kommutativ, aber diese Eigenschaften sind nicht zwingend notwendig, um die Optimierungsprobleme zu lösen.) Die Komposition wird bevorzugt multiplikativ geschrieben, da sich dann wiederholte Kompositionen als Potenzen aufschreiben lassen: $a \cdot a =: a^2$ usw.

Kombiniert man zwei mathematische Strukturen (hier: einen Halbverband mit einem Monoid), dann muss man sich Gedanken über die Interaktion der Operationen machen. In unserem Fall wird das Zusammenspiel von Vereinigung und Komposition durch ***Distributivgesetze*** geregelt:

$$x \cdot \bot = \bot \qquad\qquad \bot \cdot x = \bot$$
$$x \cdot (a \sqcup b) = (x \cdot a) \sqcup (x \cdot b) \qquad\qquad (a \sqcup b) \cdot x = (a \cdot x) \sqcup (b \cdot x)$$

Die Distributivgesetze lassen sich ansprechend mit Hilfe von Graphen motivieren: Das Gewicht des optimalen Pfads von A nach C sollte links wie rechts gleich jeweils sein.



Gibt es keinen Pfad von B nach C, dann gibt es auch keinen Pfad von A nach C. Gibt es mehrere Pfade von B nach C, dann gibt es auch mehrere Pfade von A nach C (der Knoten B ist rechts doppelt gezeichnet). Die Kombination aus einem kommutativen Monoid und einem Monoid nennt man auch ***Halbring***. Das bekannteste Beispiel: Die natürlichen Zahlen mit Addition und Multiplikation bilden einen Halbring. (Da die Multiplikation kommutativ ist, haben wir es sogar mit einem kommutativen Halbring zu tun.) Allerdings formen sie *keine* Kleene Algebra, da die Addition *nicht* idempotent ist. (Idempotenz vereinfacht das Rechnen übrigens ungemein:

$$(a \sqcup 1)^2 = a^2 \sqcup a \sqcup 1 \qquad\qquad (a + 1)^2 = a^2 + 2 \cdot a + 1$$

Auf der anderen Seite verlangen wir nicht, dass die Komposition $\cdot$ kommutativ ist. Das Fehlen des Kommutativgesetzes verkompliziert das Rechnen wiederum:

$$(a \sqcup b)^2 = a^2 \sqcup a \cdot b \sqcup b \cdot a \sqcup b^2 \qquad\qquad (a + b)^2 = a^2 + 2 \cdot a \cdot b + b^2$$

Das Kommutativgesetz ermöglicht uns im Zusammenspiel mit dem Distributivgesetz Faktoren zusammenfassen.)

Abbildung 5.26 fasst die Anforderung zusammen. Eine Kleene Algebra ist ein idempotenter Halbring und noch ein bischen mehr: Wir haben uns bisher noch nicht zur dritten Operation, der Wiederholung, geäußert — das holen wir im nächsten Abschnitt nach. In Kapitel 6 lernen wir ein Beispiel für eine Kleene Algebra kennen, bei der die Wiederholung eine zentrale Rolle einnimmt. Aber wir greifen vor …

Ein ***Monoid*** ist eine Menge M mit einem ausgezeichneten Element $0 \in M$ und einer binären Verknüpfung $+ : M \times M \to M$, so dass $+$ assoziativ ist mit 0 als neutralem Element.

$$0 + a = a = a + 0$$
$$(a + b) + c = a + (b + c)$$

Ein ***Halbring*** (engl. semiring) ist eine Menge S mit zwei ausgezeichneten Elementen $0, 1 \in S$ und zwei binären Verknüpfungen $+, \cdot : S \times S \to S$, die die folgenden Eigenschaften erfüllen.[a]

$$a + 0 = a = 0 + a \qquad a \cdot 1 = a = 1 \cdot a \qquad a \cdot 0 = 0 = 0 \cdot a$$
$$a + b = b + a \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad a \cdot (b + c) = a \cdot b + a \cdot c$$
$$a + (b + c) = (a + b) + c \qquad (a + b) \cdot c = a \cdot c + b \cdot c$$

Ein Halbring verbindet ein kommutatives Monoid (das additive Monoid, 1. Spalte) mit einem Monoid (dem multiplikativen Monoid, 2. Spalte); die Distributivgesetze (3. Spalte) regeln die Interaktion zwischen den beiden algebraischen Strukturen.

Die natürlichen Zahlen $\mathbb{N}$ mit Addition und Multiplikation bilden einen Halbring; ebenso die »erweiterten« Zahlen $\mathbb{N} \cup \{\infty\}$ mit Minimum und Addition, den sogenannten »tropischen Halbring« (engl. tropical semiring).

Ist die additive Operation ***idempotent***, $a + a = a$, dann spricht man von einem ***idempotenten Halbring***. Da ein kommutatives, idempotentes Monoid einem ***Halbverband*** mit einem kleinsten Element entspricht (siehe Anhang B.4), verwendet man in diesem Fall statt 0 und $+$ die Symbole $\bot$ (für das kleinste Element) und $\sqcup$ (für das Supremum). Die dem Verband zugrundeliegende Ordnung leitet sich aus dem Supremum ab:

$$a \sqsubseteq b \quad :\Longleftrightarrow \quad a \sqcup b = b$$

Eine ***Kleene Algebra*** K erweitert einen idempotenten Halbring um eine unäre Verknüpfung, den Sternoperator $(\text{-})^* : K \to K$. Die Anforderungen an den Sternoperator werden in Anhang B.6 ausführlich motiviert und präzisiert, siehe insbesondere Abbildung B.16.

Abbildung 5.26.: Monoide, Halbringe und Kleene Algebren.

[a] Die Terminologie ist leider nicht einheitlich; oft werden die Elemente 0 und 1 nicht vorausgesetzt. Ein Halbring in unserem Sinne heißt dann Bewertungshalbring.

5.5.2. Reflexive, transitive Hülle

Die im letzten Abschnitt skizzierten Optimierungsprobleme lassen sich auf *einheitliche* Weise lösen, indem wir die ***reflexive, transitive Hülle*** G^* des gegebenen Graphen G berechnen. Eine *Kante* von A nach B in der Hülle G^* entspricht dabei einem *optimalen Pfad* von A nach B in G. Informell gesprochen ergibt sich die Hülle als Vereinigung aller endlichen »Potenzen«:

$$G^* = G^0 \sqcup G^1 \sqcup G^2 \sqcup G^3 \sqcup \cdots \qquad G^0 := \mathbf{1} \qquad G \cdot G^n =: G^{n+1} := G^n \cdot G$$

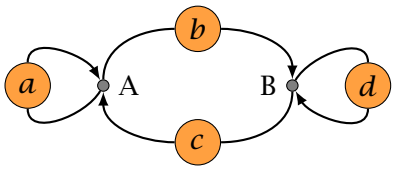
Die Potenz G^n enthält als Kanten die optimalen Pfade der Länge n in G. Vereinigung, Komposition und Wiederholung: Die gleichen Operationen, mit denen wir vorher *Gewichte* manipuliert haben, verwenden wir jetzt für die Manipulation von *Graphen*. Durch die Mathematikbrille betrachtet zeigen wir im Folgenden, dass Graphen eine Kleene Algebra bilden, sofern die Gewichte selbst einer Kleene Algebra entstammen. Mit der Informatikbrille auf der Nase programmieren wir *generische Algorithmen*.

In diesem Abschnitt motivieren wir zunächst die Definition der Operationen und wenden uns dann im nächsten Abschnitt ihrer Implementierung zu. Dabei machen wir uns das Leben leicht und beschränken uns auf Graphen, die genau zwei Knoten enthalten. (Wir werden später sehen — und das ist vielleicht etwas überraschend — dass damit bereits alles gesagt ist.) Zweielementige Graphen sind der kleinste, interessante Spezialfall. Ein Graph mit nur einem Knoten lässt sich mit dem Gewicht der einzigen Kante identifizieren, das heißt, die Operationen auf einelementigen Graphen entsprechen den korrespondierenden Operationen auf den Gewichten. (Auch das ist, wie wir später sehen werden, eine wichtige Erkenntnis.)

$\cong \quad a$

Zurück zum kleinsten, interessanten Spezialfall: Ein Graph mit zwei Knoten enthält vier Kanten und lässt sich kompakt durch eine 2×2-Tabelle repräsentieren.

Graph $\qquad$ 2×2**-Tabelle** $\qquad$ 2×2**-Matrix**

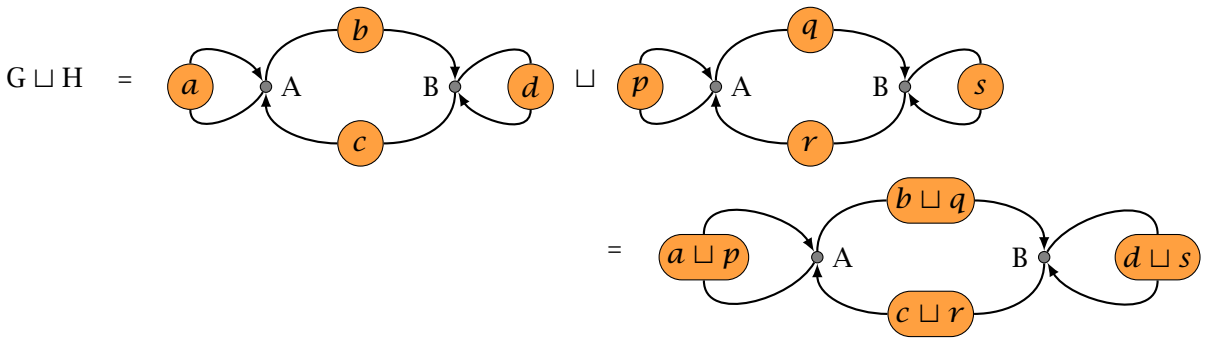


	A	B
A	a	b
B	c	d

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Alle im Folgenden aufgeführten Graphen besitzen die gleichen Knoten und unterscheiden sich nur in den Gewichten. Aus diesem Grund lassen wir die Knoten in der Darstellung oft weg und schreiben die Tabellen kompakter als 2×2-Matrizen.

Nullmatrix und Vereinigung Zwei Matrizen G und H lassen sich vereinigen, indem die korrespondierenden Einträge, sprich Gewichte, vereinigt werden.

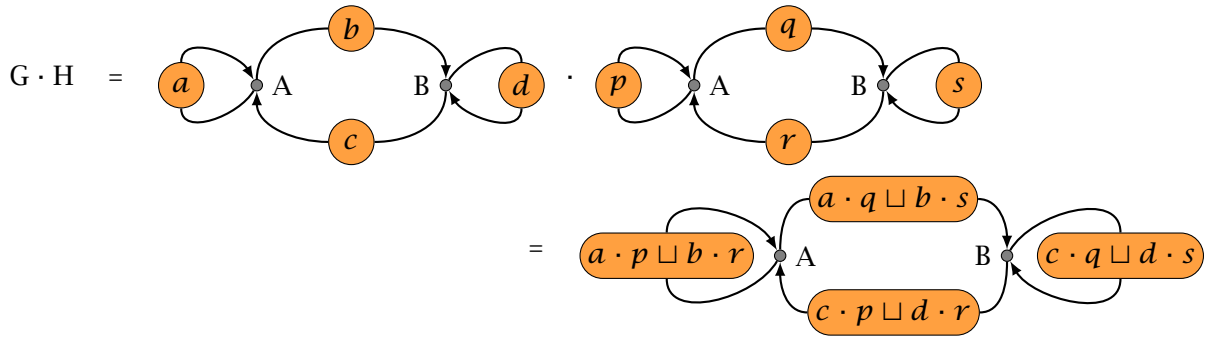


Das neutrale Element der Vereinigung ist die ***Nullmatrix***, deren Einträge dem neutralen Element $\bot$ der zugrundeliegenden Vereinigung entsprechen.

$$\mathbf{0} = \begin{pmatrix} \bot & \bot \\ \bot & \bot \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \sqcup \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} a \sqcup p & b \sqcup q \\ c \sqcup r & d \sqcup s \end{pmatrix}$$

Die Nullmatrix $\mathbf{0}$ entspricht einem leeren Graphen — einem Graphen, der zwar Knoten, aber keine Kanten enthält.

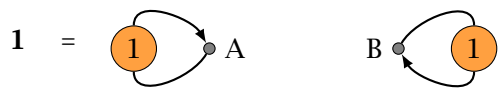
Einheitsmatrix und Multiplikation Im Vergleich zur Vereinigung kommt die Komposition interessanter daher. Eine Kante in $G \cdot H$ entspricht einer Reise mit einem Zwischenstopp, mit dem ersten Segment aus G und dem zweiten aus H.



Zum Beispiel gibt es zwei Möglichkeiten, um von A nach B zu gelangen: Entweder man reist von A nach A in G und dann von A nach B in H oder erst von A nach B in G und dann von B nach B in H. Die bessere Route, $a \cdot q \sqcup b \cdot s$, landet im Produkt $G \cdot H$. Entsprechende Überlegungen gelten für die restlichen drei Kanten.

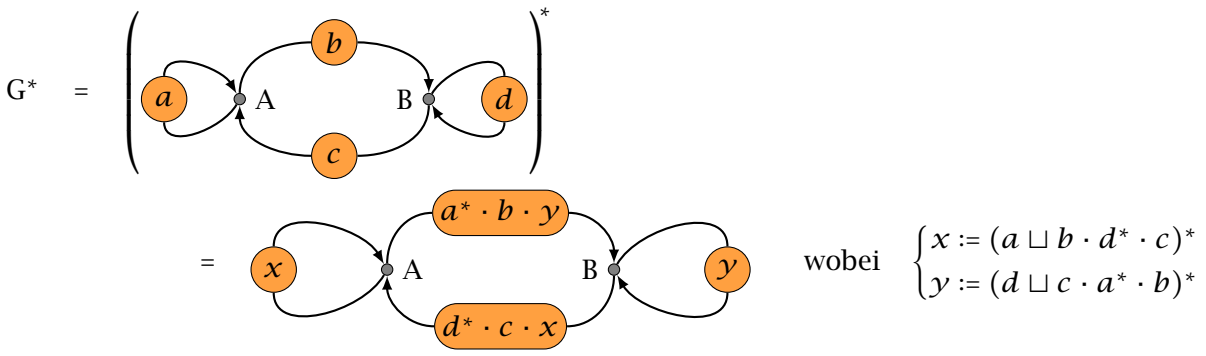
$$\mathbf{1} = \begin{pmatrix} 1 & \bot \\ \bot & 1 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} a \cdot p \sqcup b \cdot r & a \cdot q \sqcup b \cdot s \\ c \cdot p \sqcup d \cdot r & c \cdot q \sqcup d \cdot s \end{pmatrix}$$

Das neutrale Element der Matrixmultiplikation ist die ***Einheitsmatrix***, die auf der Hauptdiagonalen das neutrale Element 1 der zugrundeliegenden Multiplikation enthält und überall sonst das Nullelement $\bot$ der Multiplikation. Die Einheitsmatrix $\mathbf{1}$ entspricht einem Graphen, der nur Schleifen (engl. loops) enthält: Von jedem Knoten führt eine mit 1 markierte Kante zu ebendiesem Knoten zurück.



Conways Formel Kommen wir zur Lösung des Optimierungsproblems. Die reflexive, transitive Hülle des Graphen G lässt sich wie folgt berechnen. (Zur Erinnerung: Eine *Kante* von X nach Y

in G* entspricht einem *optimalen Pfad* von X nach Y in G.)



Für eine Rundreise von A nach A gibt es vielfältige Möglichkeiten: Entweder man fährt eine Schleife oder man reist nach B, fährt dort Schleifen und kehrt anschließend wieder nach A zurück, $a \sqcup b \cdot d^* \cdot c$. Dieses Manöver lässt sich beliebig häufig wiederholen, $x := (a \sqcup b \cdot d^* \cdot c)^*$. Ähnliche Optionen gibt es für eine Reise von B nach A: Man fährt zunächst Schleifen, dann quert man nach A und schließt mit einer Rundreise von A nach A ab, $d^* \cdot c \cdot x$. Diese Überlegungen motivieren die folgende Definition, auch bekannt unter dem Namen ***Conways Formel***.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} x & a^* \cdot b \cdot y \\ d^* \cdot c \cdot x & y \end{pmatrix} \quad \text{wobei} \quad \begin{cases} x := (a \sqcup b \cdot d^* \cdot c)^* \\ y := (d \sqcup c \cdot a^* \cdot b)^* \end{cases}$$

Damit haben wir das Optimierungsproblem für Graphen mit maximal 2 Knoten gelöst. Ein erster Schritt, aber wie gehen wir im allgemeinen Fall vor? Vereinigung und Komposition lassen sich relativ leicht auf beliebig große Graphen verallgemeinern (siehe auch Abbildung 4.1); für die Wiederholung gilt das nicht — probieren Sie es für 3×3-Matrizen aus. Was ist zu tun? Überlegen Sie einen Moment, *bevor* sie weiterlesen.

5.5.3. Kleene Algebren und Blockmatrizen

Nachdem wir hoffentlich ein klares Bild von den Optimierungsproblemen und deren Lösung gewonnen haben, setzen wir die Mathematikbrille ab, die Informatikbrille auf und wenden uns der Implementierungsarbeit zu. Unser Ziel ist, wie bereits erwähnt, ein ***generisches*** Programm zu schreiben, das alle in Abschnitt 5.5.1 detaillierten Optimierungsprobleme auf einen Schlag löst. In einem ersten Schritt kümmern wir uns darum, Kleene Algebren in Mini-F# zu repräsentieren.

Kleene Algebren Allgemein besteht eine mathematische Struktur wie ein Monoid, ein Halbring oder eine Kleene Algebra aus einer sogenannten Trägermenge, Elementen dieser Menge und Funktionen über der Menge, auch Operationen oder innere Verknüpfungen genannt. Die Trägermenge repräsentieren wir in Mini-F# durch einen Typ; die Elemente und Operationen fassen wir in einem Record zusammen. Dass einige der Recordkomponenten Funktionen sind, soll uns nicht stören — Funktionen sind auch Daten.

```
type Algebra<'carrier> =
  {
    bot  : 'carrier                          // ⊥
    join : 'carrier → 'carrier → 'carrier    // a ⊔ b
    one  : 'carrier                          // 1
    mult : 'carrier → 'carrier → 'carrier    // a · b
    star : 'carrier → 'carrier               // a*
  }
```

Die Trägermenge *'carrier* haben wir zum Parameter des Typs *Algebra* gemacht, da diese für jede Probleminstanz verschieden ist und erst festgelegt wird, wenn wir konkrete Elemente des Typs konstruieren — bei der Definition selbst ist die Trägermenge abstrakt. (Eine Bemerkung zur konkreten Syntax: Führt man die Komponenten des Records ordentlich eingerückt *untereinander* auf, so kann das Trennsymbol, das Semikolon »;«, entfallen.)

Die Trägermenge der Wegalgebra ist zum Beispiel die Menge der natürlichen Zahlen, erweitert um den Wert ∞, repräsentiert durch *Infty*.

```
type Distance = | Nat of Nat | Infty
```

Der Konstruktor *Infty* ist das neutrale Element der Vereinigung und das absorbierende Element der Komposition.

```
let shortest-path-algebra : Algebra ⟨Distance⟩ =
  let join a b =
    match a, b with
    | Infty, a | a, Infty → a
    | Nat a, Nat b       → Nat (min a b)
  let mult a b =
    match a, b with
    | Infty, a | a, Infty → Infty
    | Nat a, Nat b       → Nat (a + b)
  let star a = Nat 0
  {
    bot  = Infty
    join = join
    one  = Nat 0
    mult = mult
    star = star
  }
```

Die Komponenten der Algebra werden lokal definiert und abschließend in einem Record gebündelt (wie so oft, machen wir uns das Leben leicht und verwenden die gleichen Namen für Recordlabels und für Funktionsbezeichner).

Wir haben in Abschnitt 5.5.1 motiviert, dass Vereinigung und Komposition bestimmte Eigenschaften besitzen müssen — zu diesem Aspekt schweigt sich die obige Typdefinition aus. Und in der Tat, nicht jedes Element des Typs *Algebra* ⟨T⟩ stellt eine Kleene Algebra dar; so ist zum Beispiel nicht sichergestellt, dass die Vereinigung assoziativ, kommutativ und idempotent ist. Aus diesem Grund vereinbaren wir einen ***Vertrag***: Wenn ein Element des Typs *Algebra* ⟨T⟩ *konstruiert* wird, muss der/die Programmierer/-in sicherstellen, dass die Anforderungen an eine Kleene Algebra erfüllt sind; wenn ein Element des Typs *verwendet* wird, zum Beispiel als Parameter einer Funktion, darf der/die Programmierer/-in davon ausgehen, dass die algebraischen Eigenschaften einer Kleene Algebra gegeben sind. (Falls Sie den Dingen auf den Grund gehen wollen: In Anhang B.6.4 wird gezeigt, dass die Wegalgebra, wie oben definiert, die Anforderungen erfüllt.)

Blockmatrizen Kommen wir zur Auflösung des Puzzles: Wie lässt sich die reflexive, transitive Hülle beliebig großer Graphen berechnen? Erinnern Sie sich noch an den Slogan aus der Einleitung dieses Kapitels?

> Um ein Problem zu lösen, genügt es zu zeigen, dass sich eine Lösung für jede Probleminstanz aus Lösungen kleinerer Probleminstanzen konstruieren lässt.

Lassen wir noch einmal Revue passieren, was wir im letzen Abschnitt gezeigt haben: Wenn die Einträge von 2×2-Matrizen Elemente einer Kleene Algebra sind, dann formen auch 2×2-Matrizen selbst wieder eine Kleene Algebra. Damit können die Elemente insbesondere auch wiederum Matrizen sein! Zum Beispiel können wir die 8×8-Matrix aus Abbildung 5.25 (die Tabelle der direkten Entfernungen) alternativ als 2×2-Matrix von 2×2-Matrizen von 2×2-Matrizen von Entfernungen notieren.

$$\begin{pmatrix} \begin{pmatrix} \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix} & \begin{pmatrix} 233 & \infty \\ \infty & \infty \end{pmatrix} \\ \begin{pmatrix} 233 & \infty \\ \infty & \infty \end{pmatrix} & \begin{pmatrix} \infty & 265 \\ 265 & \infty \end{pmatrix} \end{pmatrix} & \begin{pmatrix} \begin{pmatrix} \infty & \infty \\ 223 & \infty \end{pmatrix} & \begin{pmatrix} 447 & 358 \\ 383 & \infty \end{pmatrix} \\ \begin{pmatrix} \infty & 589 \\ \infty & 332 \end{pmatrix} & \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix} \end{pmatrix} \\ \begin{pmatrix} \begin{pmatrix} \infty & 223 \\ \infty & \infty \end{pmatrix} & \begin{pmatrix} \infty & \infty \\ 589 & 332 \end{pmatrix} \\ \begin{pmatrix} 447 & 383 \\ 358 & \infty \end{pmatrix} & \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix} \end{pmatrix} & \begin{pmatrix} \begin{pmatrix} \infty & 347 \\ 347 & \infty \end{pmatrix} & \begin{pmatrix} \infty & 329 \\ \infty & 348 \end{pmatrix} \\ \begin{pmatrix} \infty & \infty \\ 329 & 348 \end{pmatrix} & \begin{pmatrix} \infty & 174 \\ 174 & \infty \end{pmatrix} \end{pmatrix} \end{pmatrix}$$

Da die Matrix in kleinere Teilblöcke aufgeteilt wird, spricht man von einer ***Blockmatrix***. Da wir die Schachtelungstiefe der Matrizen nicht antizipieren können, führt uns die allgemeine Lösungsstrategie zu dem folgenden, *rekursiven* Typ von Matrizen.

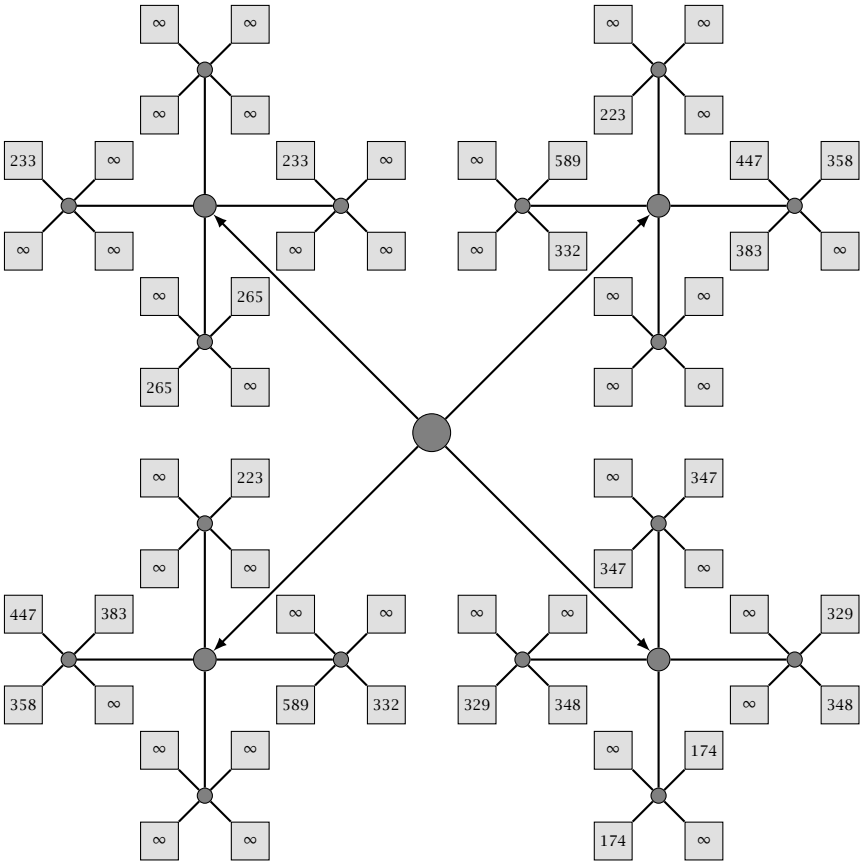
```
type Matrix ⟨'a⟩ =
  | Scalar of 'a
  | Block  of Matrix ⟨'a⟩ * Matrix ⟨'a⟩ * Matrix ⟨'a⟩ * Matrix ⟨'a⟩
```

Eine Matrix ist entweder ein Skalar — wir identifizieren 1×1-Matrizen und Skalare — oder ein Block, der aus vier Matrizen besteht. Im Allgemeinen können die Blöcke eine beliebige Form besitzen; aus Gründen der Einfachheit beschränken wir uns auf quadratische Matrizen und Blöcke, insbesondere müssen die Teilmatrizen *die gleiche Dimension* besitzen, so dass wir nur Matrizen der Dimension $2^k \times 2^k$ repräsentieren können. (Diese ***Invariante*** wird allerdings durch die Typdefinition *nicht* sichergestellt.) Mit anderen Worten, die Anzahl der Knoten eines Graphen muss stets eine exakte Potenz von zwei sein. Das ist aber keine Einschränkung, da wir einen Graphen stets um isolierte Knoten erweitern können, die mit keinem anderen Knoten verbunden sind. Der Graph aus Abbildung 5.25 enthält genau 8 Knoten, so dass sich die Entfernungstabelle wie folgt repräsentieren lässt.

```
let block (a, b, c, d) = Block (Scalar a, Scalar b, Scalar c, Scalar d)

let distances : Matrix ⟨Distance⟩ = Block (
  Block (block (Infty, Infty, Infty, Infty),
         block (Nat 233, Infty, Infty, Infty),
         block (Infty, Infty, Nat 223, Infty),
         block (Infty, Nat 589, Infty, Nat 332),
         block (Infty, Nat 223, Infty, Infty),
         block (Nat 447, Nat 383, Nat 358, Infty),
         block (Infty, Nat 347, Nat 347, Infty),
         block (Infty, Infty, Nat 329, Nat 348)),
  Block (block (Nat 233, Infty, Infty, Infty),
         block (Infty, Nat 265, Nat 265, Infty)),
         block (Nat 447, Nat 358, Nat 383, Infty),
         block (Infty, Infty, Infty, Infty)),
         block (Infty, Infty, Nat 589, Nat 332),
         block (Infty, Infty, Infty, Infty)),
         block (Infty, Nat 329, Infty, Nat 348),
         block (Infty, Nat 174, Nat 174, Infty)))
```

Der Datentyp hört zwar auf den Namen *Matrix*, aber aus Sicht der Informatik handelt es sich eigentlich um einen Baumtyp. Im Unterschied zu den Bäumen, die wir in den letzten Abschnitten kennengelernt haben, besitzt aber jeder Knoten nicht zwei, sondern vier Teilbäume — wir haben es nicht mit Binärbäumen, sondern mit ***Quaternärbäumen***[18] zu tun. Das folgende Diagram stellt den Quaternärbaum *distances* als »Draufsicht« dar.

[18] Quaternärbäume werden auch in der algorithmischen Geometrie verwendet, um Mengen von Punkten in der Ebene zu verwalten.



Operationen auf Blockmatrizen Kommen wir zu den Operationen auf Blockmatrizen. Der vollständige Programmcode ist in Abbildung 5.27 aufgeführt — wir konzentrieren uns im Folgenden auf die »Highlights« der Implementierung. In der Abbildung wird nur eine einzige Funktion definiert — diese erhält damit den Preis für die textuell längste Funktionsdefinition im Skript.

```
let matrix-algebra (algebra : Algebra ⟨'a⟩) (dim : Nat) : Algebra ⟨Matrix ⟨'a⟩⟩ = ···
```

Während *shortest-path-algebra* eine Kleene Algebra ist, haben wir es hier mit einer Funktion auf Kleene Algebren zu tun — da *Algebra* als Komponenten Funktionen enthält, ist *matrix-algebra* moralisch ein weiteres Beispiel für eine ***Funktion höherer Ordnung***. Als zweiter Parameter wird die Dimension der Matrizen spezifiziert; diese Angabe ist notwendig, um die Nullmatrix und die Einheitsmatrix generieren zu können. Die Definition der Funktion *bot* ist eine nähere Betrachtung wert.

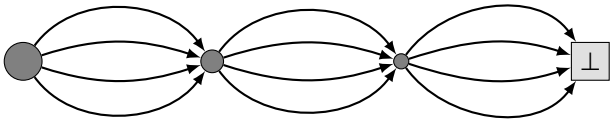
```
let rec bot (n : Nat) =
  if n = 1 then Scalar algebra.bot
           else let g = bot (n ÷ 2)
                Block (g, g, g, g)
```

Die Funktion bringt das Kunststück fertig, eine Datenstruktur mit einer quadratischen Anzahl von Elementen in logarithmischer Zeit und mit logarithmischem Platzbedarf zu erstellen! Zum Beispiel genügen 20 rekursive Aufrufe, um eine Matrix mit $2^{20} \times 2^{20} = 1.099.511.627.776$ Elementen (also rund einer Billion) zu erstellen, bei einem Speicherbedarf von $5 \cdot 20 + 2$ Speicherzellen. Dieses scheinbare Paradoxon — wie lassen sich so viele Elemente in so wenig Speicherplatz unterbringen — löst sich wie folgt auf: Wir nutzen bei der Konstruktion aus, dass die Nullmatrix aus vier identischen Blöcken besteht, Nullmatrizen der halben Dimension. Eine Nullmatrix enthält

```
let matrix-algebra (algebra : Algebra ⟨'a⟩) (dim : Nat) : Algebra ⟨Matrix ⟨'a⟩⟩ =
  let rec bot (n : Nat) =            // Annahme: dim = 2^k
    if n = 1 then Scalar algebra.bot
             else let g = bot (n ÷ 2)
                  Block (g, g, g, g)
  let rec (||) g h =
    match g, h with
    | Scalar x, Scalar y                    → Scalar (algebra.join x y)
    | Block (a, b, c, d), Block (p, q, r, s) → Block (a || p, b || q, c || r, d || s)
  let rec one (n : Nat) =
    if n = 1 then Scalar algebra.one
             else let g = one (n ÷ 2)
                  let h = bot (n ÷ 2)
                  Block (g, h, h, g)
  let rec (*) g h =
    match g, h with
    | Scalar x, Scalar y → Scalar (algebra.mult x y)
    | Block (a, b, c, d), Block (p, q, r, s) →
      Block (a * p || b * r,
             a * q || b * s,
             c * p || d * r,
             c * q || d * s)
  let rec star g =
    match g with
    | Scalar x → Scalar (algebra.star x)
    | Block (a, b, c, d) →
      let A = star a
      let D = star d
      let X = star (a || b * D * c)
      let Y = star (d || c * A * b)
      Block (X, A * b * Y, D * c * X, Y)
  {
    bot  = bot dim
    join = (||)
    one  = one dim
    mult = (*)
    star = star
  }
```

Abbildung 5.27.: Die Kleene Algebra der Blockmatrizen.

eben nicht eine quadratische Anzahl von *verschiedenen* Elementen, sondern eine quadratische Anzahl von *Kopien* des gleichen Elements. Dadurch dass die Teilblöcke nur einmal erzeugt, aber viermal verwendet werden (im Englischen spricht man auch von ***sharing***), sieht zum Beispiel ein Quaternärbaum der Dimension 8 wie folgt aus (*bot* 8).



Jeder innere Knoten enthält vier Verweise auf den identischen Teilbaum. Ganz ähnlich wird im Fall der Einheitsmatrix vorgegangen.

Vereinigung, Komposition und Wiederholung greifen für Skalare auf die korrespondierenden Operationen der Basisalgebra zurück; für Blockmatrizen setzen sie die Formeln aus Abschnitt 5.5.2 symbolgetreu um. Wie der Datentyp selbst sind auch die Operationen rekursiv definiert — getreu unserem Motto »die Funktion folgt der Form«. Aus Gründen der Lesbarkeit verwenden wir für die assoziativen Verknüpfungen Infixnotation: || für die Vereinigung und ∗ für die Komposition. (Die vordefinierten Operationen, Disjunktion und Multiplikation von Zahlen, werden durch diese Definitionen verschattet.[19] Die zwei binären Operationen sind nur definiert, wenn beide Argumente die spezifizierte Dimension *dim* besitzen — eine Anforderung, die sich nicht im Typ widerspiegelt. Aus diesem Grund ist der Musterabgleich unvollständig: »gemischte« Muster wie (*Scalar* x, *Block* (p, q, r, s)) können und müssen nicht behandelt werden.[20]

Nach diesem langen Anlauf wird es höchste Zeit, dass wir uns Beispielen zuwenden und einige der in Abschnitt 5.5.1 detaillierten Optimierungsprobleme lösen. Für Harrys Problem der kürzesten Wege haben wir bereits alle Zutaten beisammen. Wir müssen nur noch den generischen Algorithmus mit der Wegalgebra instantiieren und den resultierenden Sternoperator auf die Matrix der direkten Entfernungen anwenden.

```
>>> let star = (matrix-algebra shortest-path-algebra 8).star
>>> star distances
Block (Block (Block (Scalar (Nat 0), Scalar (Nat 830), Scalar (Nat 830), Scalar (Nat 0)),
              Block (Scalar (Nat 233), Scalar (Nat 498), Scalar (Nat 1063), Scalar (Nat 902)),
              Block (Scalar (Nat 233), Scalar (Nat 1063), Scalar (Nat 498), Scalar (Nat 902)),
              Block (Scalar (Nat 0), Scalar (Nat 265), Scalar (Nat 265), Scalar (Nat 0))), ...
```

Als Ergebnis erhalten wir die Blockmatrix der optimalen Entfernungen. In Sinne von Abbildung 1.1 müssen wir den Zahlensalat im Sachzusammenhang interpretieren, idealerweise als beschriftete Tabelle:

[19] Der F#-Interpreter ist darüber tatsächlich etwas ungehalten und warnt, dass man die Disjunktion eigentlich nicht redefinieren sollte.

[20] Der F#-Interpreter, der unsere Vereinbarung nicht kennt, warnt, dass nicht alle Muster abgedeckt werden.

von \ nach	Berlin	Freiburg	Greifswald	Hamburg	Kaiserslautern	Marl	Nürnberg	Oberhof
Berlin	0	830	233	498	687	706	447	358
Freiburg	830	0	1063	902	223	570	383	552
Greifswald	233	1063	0	265	920	589	680	591
Hamburg	498	902	265	0	679	332	854	680
Kaiserslautern	687	223	920	679	0	347	503	329
Marl	706	570	589	332	347	0	522	348
Nürnberg	447	383	680	854	503	522	0	174
Oberhof	358	552	591	680	329	348	174	0

Da der zugrundeliegende Graph ungerichtet ist, sind die Tabellen der direkten und optimalen Entfernungen jeweils spiegelsymmetrisch an der Hauptdiagonalen: Die Streckenlänge ist identisch für Hin- und Rückfahrt. So beträgt die optimale Distanz von Freiburg nach Greifswald 1063 km. (Die Streckenführung lässt sich leider nicht der Tabelle entnehmen. Ein Blick auf die Karte in Abbildung 5.25 verrät, dass Harry über Nürnberg und Berlin reisen muss.)

Die Algebra der kürzesten Wege erlaubt es uns auch, Varianten des Optimierungsproblems zu lösen, zum Beispiel, den optimalen Weg, wenn man höchstens einmal umsteigen möchte: $\mathbf{1} \sqcup D \sqcup D \cdot D$ für die Matrix D der direkten Distanzen.

```
⋙ let a = matrix-algebra shortest-path-algebra 8
⋙ let (∗)  = a.mult
⋙ let (||) = a.join
⋙ a.one || distances || distances ∗ distances
Block (Block (Block (Scalar (Nat 0), Scalar (Nat 830), Scalar (Nat 830), Scalar (Nat 0)),
              Block (Scalar (Nat 233), Scalar (Nat 498), Scalar Infty, Scalar Infty),
              Block (Scalar (Nat 233), Scalar Infty, Scalar (Nat 498), Scalar Infty),
              Block (Scalar (Nat 0), Scalar (Nat 265), Scalar (Nat 265), Scalar (Nat 0))), ...
```

Aus dem Ergebnis lässt sich ablesen, dass keine Verbindungen zwischen Freiburg und Greifswald der gewünschten Art existiert: Der Eintrag *Nat* 1063 ist dem Wert *Infty* gewichen.

Kommen wir zum Problem optimaler Wechselkurse. Abbildung 5.28 zeigt die Kleene Algebra der Wechselkurse und die Codierung der Umrechnungstabelle aus Abschnitt 5.5.1. Da die Tabelle nur 5×5 Einträge umfasst, ist sie mit »Dummyeinträgen« auf die erforderliche Größe gebracht worden. Die Implementierung der Algebra ähnelt dem Programmcode der Wegalgebra und ist nicht weiter bemerkenswert, mit vielleicht einer Ausnahme: Was ist der Wert von $0 \cdot \infty$? Null oder unendlich? Die Distributivgesetze klären die Frage: 0 ist und bleibt das absorbierende Element der Multiplikation, somit gilt $0 \cdot \infty = 0 = \infty \cdot 0$. Unendlich absorbiert auch, aber nur positive Werte: $x \cdot \infty = \infty = \infty \cdot x$, für $x > 0$. Aus diesem Grund unterscheidet *mult* drei Fälle, siehe Abbildung 5.28.

Berechnen wir die optimalen Wechselkurse, erleben wir eine faustdicke Überraschung.

```
type Rate = | Fin of float | Inf          // nur nichtnegative Wechselkurse
let best-rate-algebra : Algebra⟨Rate⟩ =
  let join a b =
    match a, b with
    | Inf, _ | _, Inf → Inf
    | Fin a, Fin b    → Fin (max a b)
  let mult a b =
    match a, b with
    | Fin 0.0, _  | _, Fin 0.0 → Fin 0.0
    | Inf, _      | _, Inf     → Inf
    | Fin a, Fin b            → Fin (a * b)
  let star = function
    | Inf    → Inf
    | Fin a → if a ⩽ 1.0 then Fin 1.0 else Inf
  {
    bot  = Fin 0.0
    join = join
    one  = Fin 1.0
    mult = mult
    star = star
  }
let dummy = best-rate-algebra.bot
let rates : Matrix⟨Rate⟩ =
  Block (Block (block (Fin 1.0, Fin 0.9429, Fin 1.0605, Fin 1.0),
                block (Fin 0.83931, Fin 111.21, Fin 0.89009, Fin 117.96),
                block (Fin 1.1913, Fin 1.1234, Fin 0.0089886, Fin 0.0084774),
                block (Fin 1.0, Fin 132.49, Fin 0.0075469, Fin 1.0)),
         Block (block (Fin 1.0327, dummy, Fin 1.0953, dummy),
                block (dummy, dummy, dummy, dummy),
                block (Fin 1.2303, dummy, Fin 0.0092867, dummy),
                block (dummy, dummy, dummy, dummy)),
         Block (block (Fin 0.96785, Fin 0.91284, dummy, dummy),
                block (Fin 0.81264, Fin 107.67, dummy, dummy),
                block (Fin 1.0, dummy, dummy, dummy),
                block (dummy, dummy, dummy, dummy)),
         Block (block (dummy, dummy, dummy, dummy),
                block (dummy, dummy, dummy, dummy),
                block (dummy, dummy, dummy, dummy),
                block (dummy, dummy, dummy, dummy)))
```

Abbildung 5.28.: Die Kleene Algebra der Wechselkurse.

```
⋙ let star = (matrix-algebra best-rate-algebra 8).star
⋙ star rates
Block (Block (Block (Scalar Inf, Scalar Inf, Scalar Inf, Scalar Inf),
              Block (Scalar Inf, Scalar Inf, Scalar Inf, Scalar Inf),
              Block (Scalar Inf, Scalar Inf, Scalar Inf, Scalar Inf),
              Block (Scalar Inf, Scalar Inf, Scalar Inf, Scalar Inf)),
       Block (Block (Scalar Inf, Scalar (Fin 0.0), Scalar Inf, Scalar (Fin 0.0)),
              Block (Scalar (Fin 0.0), Scalar (Fin 0.0), Scalar (Fin 0.0), Scalar (Fin 0.0)),
              Block (Scalar Inf, Scalar (Fin 0.0), Scalar Inf, Scalar (Fin 0.0)),
              Block (Scalar (Fin 0.0), Scalar (Fin 0.0), Scalar (Fin 0.0), Scalar (Fin 0.0))), ...
```

Die resultierende Tabelle der optimalen Wechselkurse enthält neben den Dummyeinträgen nur *Infty* Werte! Aber vielleicht sind Sie gar nicht überrascht? Das Ergebnis hat eine einfache, logische Erklärung: Wir haben schon besprochen, dass der Umtausch EUR → JPY → GBP → EUR einen Umrechungsfaktor ergibt, der größer ist als Eins, und dass sich der Gewinn durch Wiederholung der Transaktion ins Unermessliche steigern lässt. Da jede Währung in jede andere umgerechnet werden kann (wir haben einen sogenannten ***vollständigen*** Graphen vor uns), lässt sich mit jedem Umtausch ein unendlicher Gewinn erzielen — zumindest theoretisch — signalisiert durch die ∞-Einträge. (Vielleicht haben Sie erwartet, dass wir den Zyklus mit dem größten Faktor > 1 erhalten — das ist nicht der Fall; dieses Problem ist tatsächlich *sehr* viel schwieriger.)

Laufzeitanalyse Kommen wir zur Analyse der Laufzeit der fünf generischen Algorithmen aus Abbildung 5.27, eine interessante Übung, nicht zuletzt wegen der zum Teil ungewöhnlichen Rekursionsmuster. Als Problemgröße wählen wir jeweils die Gesamtzahl n der Knoten, sprich die Dimension der beteiligten Matrizen.

Wir haben schon angesprochen, dass für die Konstruktion der Nullmatrix eine logarithmische Anzahl von Schritten benötigt wird. Die Zeitfunktion von *bot* kennen wir bereits von der binären Suche; sie erfüllt im Rekursionsschritt die Gleichung $T(2 \cdot n) = 1 + T(n)$, die vom binären Logarithmus gelöst wird: $T(n) \sim \lg n$. Wir haben auch diskutiert, dass dies für den Datentyp *Matrix* eine ungewöhnlich gute Laufzeit darstellt. Ein Graph mit n Knoten hat im schlechtesten Fall n^2 Kanten. Blockmatrizen, so wie wir sie definiert haben, stellen eine sogenannte ***dichte*** Repräsentation dar (engl. dense representation): Auch nicht-existente Kanten werden explizit repräsentiert (abstrakt durch $\perp$ und konkret durch *algebra.bot*) und belegen Speicherplatz. Eine Matrix der Dimension n enthält eine quadratische Anzahl von Elementen und benötigt im Allgemeinen entsprechend viel Speicherplatz. Eine ***lichte*** Repräsentation (engl. sparse representation) würde dies vermeiden.

Für die Konstruktion der Einheitsmatrix wird etwas mehr Zeit benötigt, da *one* auf *bot* zurückgreift. Der Aufwand im Rekursionsschritt ist nicht länger konstant, sondern logarithmisch: $T(2 \cdot n) = \lg n + T(n)$. Gegenüber *bot* quadriert sich somit die Gesamtlaufzeit: $T(n) \sim \frac{1}{2} \lg^2 n$.

Die Matrizenvereinigung kommt im Vergleich dazu fast bieder daher; sie folgt exakt der rekursiven Struktur von Blockmatrizen. Zur Erinnerung: Wir verlangen, dass die beiden Argumente von *join* die gleiche Dimension besitzen. Die Argumente werden parallel bis zu den Blättern durchlaufen; in jedem Rekursionsschritt erfolgen vier rekursive Aufrufe: $T(2 \cdot n) = 4 \cdot T(n)$. Insgesamt ergibt sich eine quadratische Laufzeit: $T(n) \sim n^2$ — Standard für Blockmatrizen.

Die Matrizenmultiplikation legt ein interessanteres Rekursionsmuster an den Tag: Im Rekursionsschritt erfolgen acht rekursive Aufrufe und zusätzlich vier Aufrufe der Matrizenvereinigung: $T(2 \cdot n) = 4 \cdot n^2 + 8 \cdot T(n)$. Der quadratische Aufwand für die Vereinigung fällt allerdings nicht so stark ins Gewicht; die Laufzeit wird von den acht rekursiven Aufrufen dominiert, es ergibt sich insgesamt eine kubische Laufzeit: $T(n) \sim n^3$.

Wir haben gesehen, dass sich die Optimierungsprobleme aus Abschnitt 5.5.1 einheitlich lösen lassen, indem wir die reflexive, transitive Hülle einer Matrix berechnen. Letztlich sind wir also nur an der Laufzeit des Sternoperators interessiert. Aber: Der Sternoperator stützt sich auf die Matrizenmultiplikation ab und diese wiederum auf die Matrizenvereinigung. Da sich die Struktur der Zeitfunktionen an der Struktur der Mini–F# Funktionen orientiert, erhalten wir für die Laufzeit des Sternoperators die folgende Rekurrenz: $T(2 \cdot n) = 8 \cdot n^3 + 4 \cdot T(n)$, insgesamt achtmal wird die Multiplikation aufgerufen und es erfolgen vier rekursive Aufrufe. Hier sind im Gegensatz zur obigen Situation die Aufrufe der »Stützfunktion« nicht zu vernachlässigen. Es ergibt sich insgesamt eine kubische Laufzeit: $T(n) \sim 2 \cdot n^3$. Die Optimierungsprobleme aus Abschnitt 5.5.1 lassen sich somit in kubischer Zeit lösen, das heißt, für jeden der quadratisch vielen Einträge wird eine lineare Laufzeit benötigt. Das ist nicht schlecht, aber ein Blick in die folgende Tabelle zeigt, dass kubische Algorithmen durchaus Skalierungsprobleme haben.

n	$\lg n$	$\lg^2 n$	n^2	n^3
100	$\approx 6,6$	$\approx 44,1$	10.000	1.000.000
1.000	$\approx 10,0$	$\approx 99,3$	1.000.000	1.000.000.000
10.000	$\approx 13,3$	$\approx 176,6$	100.000.000	1000.000.000.000
100.000	$\approx 16,6$	$\approx 275,9$	10.000.000.000	1.000.000.000.000.000
1.000.000	$\approx 20,0$	$\approx 397,3$	1.000.000.000.000	1.000.000.000.000.000.000

Zusammenfassung und Anmerkungen

DIY: Zusammenfassung

Probleme lassen sich auf ganz verschiedene Weise rechnerisch lösen; Problemlösungen konkurrieren hinsichtlich Eleganz, Lesbarkeit, Verständlichkeit und Resourcenverbrauch, Platzbedarf und Rechenzeit. Man unterscheidet zwischen der *Komplexität* eines Problems und der *Laufzeit* eines Programms. Die Frage »Wie schwierig ist das Problem?« hat eine ganz andere Qualität als die Frage »Wie schnell ist das Programm?«. Die Frage, wie lange ein konkretes Programm im schlechtesten aller Fälle rechnet, lässt sich mit einiger Routine oft direkt beantworten. Die Frage nach dem besten aller Programme ist weitaus schwieriger — die Komplexität vieler, vieler Probleme ist auch nach Jahrzehnten der Forschung unbekannt (Stichwort: »P versus NP«).

Das Sortierproblem hat eine linear-logarithmische Komplexität; Sortieren durch Einfügen und Sortieren durch Auswählen haben eine quadratische Laufzeit — damit die Aussagen unabhängig von Programmiersprachen, Rechnerarchitekturen und allgemein dem technologischen Fortschritt sind, beschränkt man sich bei den Angabe in der Regel auf Größenordnungen (konstant, logarithmisch, linear, linear-logarithmisch, quadratisch, kubisch, exponentiell usw.). Sortieren durch Mischen hat im schlechtesten Fall eine linear-logarithmische Laufzeit und ist damit asymptotisch optimal.

Das Mantra des systematischen Rechnens lautet: Um ein Problem zu lösen, genügt es zu zeigen, dass sich eine Lösung für jede Probleminstanz aus Lösungen kleinerer Probleminstanzen

konstruieren lässt. Das allgemeine Peano Entwurfsmuster empfiehlt, die Problemgröße um eins zu reduzieren; das allgemeine Leibniz Entwurfsmuster schlägt eine Halbierung der Problemgröße vor. Am Beispiel des Suchens:

Algorithmus:	lineare Suche	binäre Suche
Datenstruktur:	Suchlisten	binäre Suchbäume

Aus der *Kontrollstruktur* leitet sich jeweils eine *Datenstruktur* ab: Listen inkarnieren die Idee der linearen Suche; Binärbäume leiten sich von der binären Suche ab.

Fasst man Operationen in einer wohldefinierten Schnittstelle zusammen, erhält man einen abstrakten Datentyp (ADT). Ein *konkreter Datentyp* wird durch Angabe seiner Element definiert; ein *abstrakter Datentyp* definiert sich durch die angebotenen Operationen — er ist die Summe seines Verhaltens. Ein abstrakter Datentyp wird durch konkrete Datentypen implementiert: Suchlisten, binäre Suchbäume und 2-3-Suchbäume implementieren den ADT »endliche Abbildung« ; Wimpel, Pairing-Heaps und Binomial-Heaps den ADT »Prioritätswarteschlange«. Implementierungen einer Schnittstelle konkurrieren hinsichtlich Eleganz, Lesbarkeit, Verständlichkeit und Resourcenverbrauch …

6. Grammatiken\Konkrete Syntax

In den letzten drei Kapiteln haben wir uns angeschaut, wie man mit der Sprache Mini–F# Probleme löst: Wie man Probleme in Rechenaufgaben verwandelt und wie man Rechenregeln in Mini–F# formuliert, um diese Rechenaufgaben zu lösen. Aber wir haben nicht nur *mit* Mini–F# programmiert, wir haben auch *über* die Sprache gesprochen; wir haben die abstrakte Syntax und die Bedeutung zahlreicher Konstrukte präzise festgelegt.

In diesem Kapitel wenden wir uns der ***konkreten Syntax*** zu. Wir werden Formalismen kennenlernen, mit denen man die konkrete Syntax einer Sprache — und nicht nur die einer Programmiersprache — ebenso präzise wie die abstrakte Syntax definieren kann. Unsere Programmiersprache wird uns dabei als fortlaufendes Beispiel dienen.

Zur Erinnerung: Die abstrakte Syntax ist durch eine Baumsprache gegeben. Sie beschreibt den *hierarchischen* Aufbau eines Programms, etwa dass der Mini–F# Ausdruck für die Alternative aus drei Teilausdrücken besteht. Die konkrete Syntax beschreibt im Gegensatz dazu, welche *Folgen* von Zeichen ein Lexem und welche *Folgen* von Lexemen ein gültiges Programm darstellen, etwa dass `i` gefolgt von `f` ein Schlüsselwort ist und dass das Schlüsselwort ***if*** gefolgt von einem Ausdruck, gefolgt von dem Schlüsselwort ***then***, gefolgt von einem Ausdruck, gefolgt von dem Schlüsselwort ***else***, gefolgt von einem Ausdruck ebenfalls ein Ausdruck ist. Die konkrete Syntax legt also fest, wie ein Programm, das wir einem Rechner vorlegen wollen, konkret aussehen muss. Kurz: Die abstrakte Syntax beschreibt Bäume, die konkrete Syntax Folgen von Zeichen bzw. Lexemen.

Es ist absehbar, dass die Bedeutung der konkreten Syntax zurückgeht. Entwicklungen wie Strukturediteren, die direkt die Struktur eines Programms erfassen, integrierte Entwicklungsumgebungen (engl. IDE) oder visuelle Programmiersprachen machen ihr den Garaus. Dessen ungeachtet sind die Formalismen, mit denen man die konkrete Syntax beschreibt, bedeutsam. Neben vielfältigen Anwendungsmöglichkeiten jenseits der Programmiersprachen erzählen sie auch eine der großen Erfolgsgeschichten der Informatik: Wie man automatisch von einer deskriptiven Beschreibung zu einem ausführbaren Programm kommt, das diese Beschreibung umsetzt. Der Traum der Informatik: Ich beschreibe »was« ein Programm leisten soll, das »wie« erledigt der Rechner, dazu später mehr in Abschnitt 6.2.

Im Einzelnen haben wir folgendes vor: Abschnitt 6.1 beschäftigt sich mit der Beschreibung der lexikalischen Syntax einer Programmiersprache. Abschnitt 6.2 detailliert den Weg von der Deskription zur Präskription, von der Beschreibung zur Rechenvorschrift. In Abschnitt 6.3 unternehmen wir eine längere, optionale Exkursion in die Welt der Automatentheorie. Abschnitt 6.4 erweitert den Formalismus, so dass die konkrete Syntax von Programmiersprachen beschrieben werden kann. Fast alle Programmiersprachen haben Infixoperatoren im Angebot, Operatoren, die zwischen ihre Argumente geschrieben werden. Mit dem Sinn und Zweck von Operatoren und den damit verbundenen Problemen beschäftigt sich ebenfalls Abschnitt 6.4. Abschnitt 6.5 zeigt schließlich, wie konkrete Syntax automatisch in abstrakte Syntax überführt werden kann.

6.1. Reguläre Ausdrücke\lexikalische Syntax

Eine natürliche Zahl wird in Mini–F# durch ein ***Numeral*** repräsentiert; umgekehrt bezeichnet ein Numeral eine natürliche Zahl. Kurz: Numeral ist Syntax, Zahl ist Semantik. Ein Numeral in Mini–

F# besteht aus einer nicht-leeren Folge von Dezimalziffern. Ein Bezeichner in Mini–F# beginnt mit einem Buchstaben, gefolgt von weiteren Buchstaben, Ziffern und Sonderzeichen, wie dem Unterstrich oder dem Apostroph.

Wie lässt sich die lexikalische Syntax von Numeralen, Bezeichnern und den anderen syntaktischen Bestandteilen von Mini–F# formal beschreiben? Dazu können wir uns zum Beispiel eine Sprache ausdenken — eine Sprache, um Sprachen zu beschreiben. Bevor wir uns dieser Aufgabe zuwenden, klären wir zunächst, was eine Sprache überhaupt ist.

Ist $\mathbb{A}$ eine Menge von Zeichen, ein sogenanntes ***Alphabet***, dann ist eine ***Sprache*** eine Teilmenge von $\mathbb{A}^*$, der Menge der Sequenzen über $\mathbb{A}$ — statt von Sequenzen spricht man in diesem Zusammenhang auch oft von ***Wörtern***. Die Menge aller Sprachen ist $\mathcal{P}(\mathbb{A}^*)$, die Potenzmenge von $\mathbb{A}^*$. Ist $\mathbb{A}$ zum Beispiel das ASCII-Alphabet[1], dann kann eine Sprache über $\mathbb{A}$ die lexikalische Syntax beschreiben, die Menge aller Lexeme. Ist $\mathbb{A}$ hingegen die Menge aller Lexeme, dann kann eine Sprache die kontextfreie Syntax einer Programmiersprache festlegen (den Zusatz »kontextfrei« erklären wir in Abschnitt 6.4).

Kommen wir zur Sprachbeschreibungssprache. In Abschnitt 2.1 haben wir einige Operationen auf Sequenzen eingeführt: die leere Sequenz, die Konkatenation und die Wiederholung. Ziehen wir diese Konstrukte heran, dann können wir bereits Numerale beschreiben. Ist *digit* eine Abkürzung für die Sprache der Ziffern, dann beschreibt

$$\mathit{digit} \cdot \mathit{digit}^*$$

die Syntax von Numeralen. Lies: Ein Numeral ist eine Ziffer gefolgt von einer beliebigen Wiederholung von Ziffern. Wie können wir *digit* definieren? Eine Ziffer ist entweder `0`, oder `1`, oder `2`, oder …. Erfinden wir eine Notation für die Alternative, zum Beispiel »∣«, dann ist

$$\texttt{0} \mid \texttt{1} \mid \texttt{2} \mid \texttt{3} \mid \texttt{4} \mid \texttt{5} \mid \texttt{6} \mid \texttt{7} \mid \texttt{8} \mid \texttt{9}$$

die gesuchte Definition von *digit*. Die lexikalische Syntax von Bezeichnern lässt sich auf ähnliche Art und Weise festlegen:

$$\mathit{letter} \cdot (\mathit{letter} \mid \mathit{digit} \mid \texttt{'} \mid \texttt{\_})^*$$

wobei *letter* durch $\texttt{A} \mid \cdots \mid \texttt{Z} \mid \texttt{a} \mid \cdots \mid \texttt{z}$ gegeben ist.

Jetzt da wir eine erste Vorstellung von der Sprachbeschreibungssprache haben, können wir unser Routineprogramm abspulen. Welches Routineprogramm? Wir definieren die abstrakte Syntax und die Semantik der Sprachbeschreibungssprache! Das mag etwas merkwürdig anmuten — wir wollen ja die neue Sprache gerade dazu verwenden, die Syntax anderer Sprachen zu beschreiben, und jetzt beabsichtigen wir die Syntax der Sprache selbst festzulegen. Aber die Sprachbeschreibungssprache ist nun einmal eine Sprache und als solche müssen wir uns um deren Syntax und Semantik kümmern.

6.1.1. Syntax regulärer Ausdrücke

Abstrakte Syntax Sei $\mathbb{A}$ ein beliebiges ***Alphabet***, eine Menge von Zeichen, Symbolen oder Buchstaben. (Die Begriffe sind sehr allgemein zu verstehen: Ein Alphabet ist einfach eine Menge, zum Beispiel $\{0, 1\}$; ein Buchstabe ist einfach ein Element der Menge.) Die abstrakte Syntax der sogenannten ***regulären Ausdrücke*** über $\mathbb{A}$ ist durch die folgende Baumsprache gegeben.

[1] ASCII steht für American Standard Code for Information Interchange — ist also eigentlich nichts für Europäer — und stellt eine Zeichenkodierung dar, eine Zuordnung von Zeichen zu Zahlen. Die ASCII Zeichenkodierung definiert 33 nicht-druckbare sowie die folgenden 95 druckbaren Zeichen, beginnend mit dem Leerzeichen: ␣!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~.

	Abstrakte Syntax	`grep`	`egrep`
das leere Wort	ε	–	–
einzelnes Zeichen	a	a	a
Konkatenation	$r_1 \cdot r_2$	$r_1\ r_2$	$r_1\ r_2$
die leere Sprache	$\emptyset$	–	–
Alternative	$r_1 \mid r_2$	r_1 `|` r_2	r_1 `|` r_2
Wiederholung	r^*	r`\*`	r`*`
Gruppierung	–	`\(` r `\)`	`(` r `)`
beliebiges Zeichen (außer Zeilenende)	$a_1 \mid \cdots \mid a_n$	`.`	`.`
optionales Vorkommen	$\varepsilon \mid r$	r`\?`	r`?`
mindestens einmalige Wiederholung	$r\ r^*$	r`\+`	r`+`

Abbildung 6.1.: Konkrete Syntax regulärer Ausdrücke.

$a \in \mathbb{A}$	***Alphabet***
$r \in \mathsf{Reg} ::=$	***reguläre Ausdrücke:***
$\mid\ a$	einzelnes Zeichen\Terminalsymbol
$\mid\ \varepsilon$	das leere Wort
$\mid\ r_1 \cdot r_2$	Konkatenation\Sequenz
$\mid\ \emptyset$	die leere Sprache
$\mid\ r_1 \mid r_2$	Alternative
$\mid\ r^*$	Wiederholung

Die Elemente des Alphabets, auch ***Terminalsymbole*** genannt, sind sozusagen die Konstanten der Sprache. Die Notation regulärer Ausdrücke ist eng an die Notation von Sequenzen angelehnt. Man sollte sich aber klarmachen, dass die obige Baumsprache die *Syntax* regulärer Ausdrücke beschreibt. Zum Beispiel ist $\emptyset$ nicht die leere Menge, sondern ein regulärer Ausdruck. Das Symbol $\emptyset$ ist ***überladen***: Je nach Kontext bezeichnet es die leere Menge oder einen regulären Ausdruck, vergleiche die Diskussion am Ende von Abschnitt 2.4. Ebenso sind die Terminalsymbole überladen: a ist entweder ein einzelner Buchstabe oder ein regulärer Ausdruck. (Das Phänomen kennen wir von Booleschen und arithmetischen Ausdrücken: *true* ist sowohl ein Boolescher Wert als auch ein Boolescher Ausdruck; 4711 ist sowohl eine natürliche Zahl als auch ein arithmetischer Ausdruck.) Die Konkatenation oder Sequenz von regulären Ausdrücken $r_1 \cdot r_2$ wird im Folgenden häufig »ohne Syntax« notiert, indem die Ausdrücke r_1 und r_2 einfach hintereinander geschrieben werden: $r_1\ r_2$. Damit folgen wir einer guten (?), alten mathematischen Tradition: Multiplikative Operatoren werden oft ausgelassen; aus $2 \cdot x + 1$ wird $2x + 1$; aus $a \wedge b \vee c$ wird $ab \vee c$.

Konkrete Syntax Auch reguläre Ausdrücke haben eine konkrete Syntax. Wir entwerfen hier keine eigene, sondern schauen uns zwei praktische Beispiele für Syntaxen an, siehe Tabelle 6.1. Kurz zum Hintergrund: Die Programme `grep` und `egrep` durchsuchen Sequenzen (typischerweise Textdateien) nach zusammenhängenden Teilsequenzen, die auf ein bestimmtes, vom Benutzer vorgegebenes Muster passen. Das Muster ist dabei durch einen regulären Ausdruck gegeben. Eine Teilsequenz passt auf ein Muster, wenn die Sequenz in der durch das Muster beschriebenen Sprache enthalten ist.

Die prinzipielle Schwierigkeit, mit der man sich beim Entwurf einer konkreten Syntax konfrontiert sieht, liegt darin, Terminalsymbole von Metasymbolen (`|` oder `*`) zu unterscheiden. Beide Symbole entstammen ja dem gleichen Alphabet, da die lexikalische Syntax regulärer Ausdrücke festgelegt wird. Ein einfacher Trick, dieser Schwierigkeit zu begegnen, ist, ein sogenanntes

Fluchtsymbol (engl. escape symbol) einzuführen, das die jeweilige Kategorie, Terminal- oder Metasymbol, signalisiert. In den Beispielen, Tabelle 6.1, ist \ (engl. backslash) das Fluchtsymbol. In `grep` kennzeichnet es die Metasymbole: `*` ist ein Terminalsymbol, `\*` ist ein Metasymbol. In `egrep` ist es genau umgekehrt: `\*` ist das Terminal- und `*` das Metasymbol.

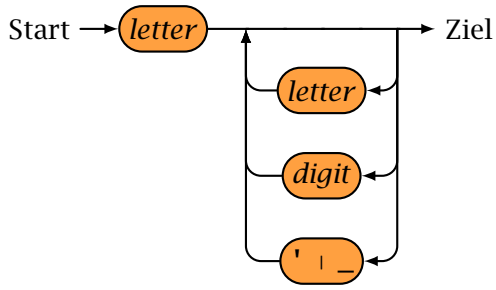
Das Programm `egrep` bietet weiterhin einige bequeme Abkürzungen an: Die lexikalische Syntax von Numeralen kann zum Beispiel durch `[0-9]+` festgelegt werden; entsprechend beschreibt `[A-Za-z][A-Za-z'_]*` die Syntax von Bezeichnern. Der folgende Aufruf von `egrep` durchsucht das Skript nach gültigen Email-Adressen.[2]

```
> egrep "[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}" Skript.tex
  \url{support@harry-hacker.org}
besseren Namen? Vorschläge gerne an \url{support@harry-hacker.org}.
"\nPlease report it as a bug to support@harry-hacker.org.")
\url{support@harry-hacker.org}). Einstweilen verwenden wir einen
```

Das Programm wird mit zwei Argumenten aufgerufen, dem in Anführungsstriche gesetzten regulären Ausdruck und dem Namen einer Datei. Der reguläre Ausdruck enthält drei Punkte, die jeweils für das Terminalsymbol, das Zeichen »`.`«, stehen. Da der Punkt von Haus aus ein Metasymbol für ein beliebiges Zeichen ist, muss das Fluchtsymbol vorangestellt werden. Innerhalb der eckigen Klammern ist das jedoch nicht nötig. Aber: Dort ist »–« ein Metasymbol; meint man das Terminalsymbol, den Bindestrich, muss dieser als letztes, direkt vor der schließenden Klammer aufgeführt werden.

Man sieht, die konkrete Syntax zu entwerfen, ist keine ganz leichte Angelegenheit. Deswegen ist unser Ausgangspunkt allermeistens die abstrakte Syntax. Entgegen vorherrschender (Lehr-) Meinung ist ein abstraktes Konzept nicht schwieriger als ein konkretes. Abstraktion bedeutet ja Vernachlässigung irrelevanter, uninteressanter oder zufälliger Details. Deswegen abstrahieren Informatiker/-innen und Mathematiker/-innen auch so gerne; es macht das Leben leichter.

Syntaxdiagramme Reguläre Ausdrücke lassen sich wunderbar mit Hilfe sogenannter ***Syntaxdiagramme*** (engl. syntax diagrams) bzw. ***Eisenbahndiagramme*** (engl. railroad diagrams) darstellen. Die lexikalische Syntax von Bezeichnern wird zum Beispiel durch das folgende Diagramm eingefangen.



Das Diagramm hat einen »Eingang« auf der linken Seite, den Startpunkt, und einen »Ausgang« auf der rechten Seite, den Zielpunkt. Indem man mit dem Finger von Start- zum Zielpunkt fährt, lassen sich systematisch alle Wörter der Sprache generieren.

Die Konkatenation wird dabei durch hintereinander geschaltete Schienenstränge visualisiert, die Alternative durch parallel geschaltete Schienenstränge. »Loopings« oder Schleifen stellen Wiederholungen dar, wie im folgenden Diagramm.

[2] Die Ausgabe bezieht sich auf die Version des Skripts *bevor* die Ausgabe zum Text hinzugefügt wurde.

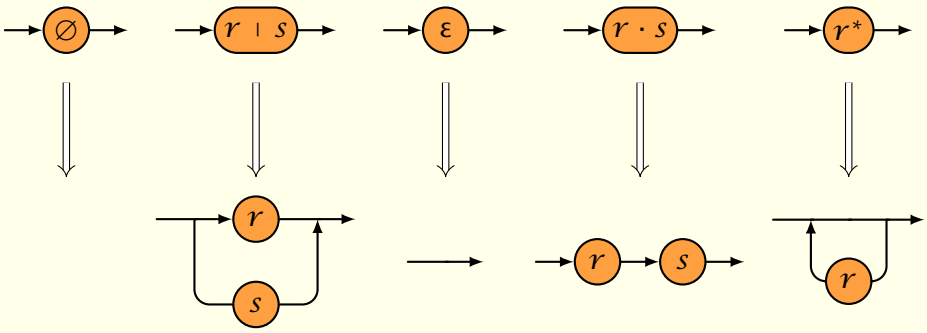
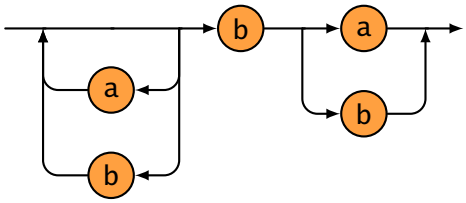
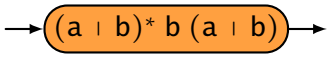


Abbildung 6.2.: Konstruktion von Syntaxdiagrammen.

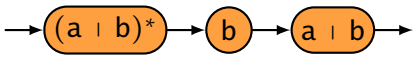


Das Syntaxdiagramm generiert die Sprache aller Wörter über dem Alphabet $\{\mathtt{a}, \mathtt{b}\}$, die an der vorletzten Position ein `b` enthalten. Um zum Beispiel das Wort `ababb` zu generieren, drehen wir uns dreimal im Kreis, fahren dann nach rechts und dann nach rechts unten. Die Sprache wird uns als laufendes Beispiel in diesem Kapitel dienen. Um uns einfach auf sie beziehen zu können, taufen wir sie auf den Namen ***advPieb-Sprache*** (*a*n *d*er *v*orletzten *P*osition *i*st *e*in *b*). Vielleicht finden Sie einen besseren Namen? Vorschläge gerne an support@harry-hacker.org.

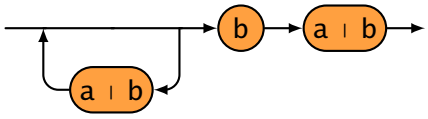
Abbildung 6.2 illustriert, wie man für einen gegebenen regulären Ausdruck systematisch das korrespondierende Syntaxdiagramm konstruiert. Ausgangspunkt ist das Diagramm, dessen einziger »Bahnhof« den regulären Ausdruck enthält.



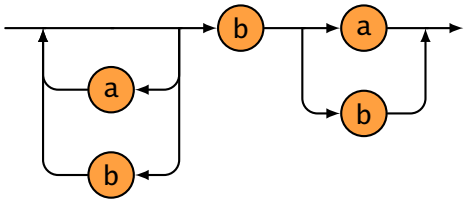
Die Transformationen werden von oben nach unten angewendet; ein Bahnhof wird dabei jeweils durch ein kleines Diagramm ersetzt. In unserem Beispiel expandieren wir gemäß des Aufbaus des regulären Ausdrucks zunächst die Konkatenation.



Anschließend wird die Wiederholung durch einen Looping ersetzt.



Wenn wir schließlich die Alternativen durch parallele Schienenstränge visualisieren, erhalten wir das ursprüngliche Diagramm.



Man kann die Transformationen solange anwenden, bis nur noch mit Buchstaben markierte Bahnhöfe übrig sind. Manchmal hört man aus Gründen der Übersichtlichkeit etwas früher auf, so geschehen im ersten Beispiel, dem Diagramm für Bezeichner.

6.1.2. Semantik regulärer Ausdrücke

In den Kapiteln 3 und 4 haben wir zwischen statischer und dynamischer Semantik unterschieden. Das ist hier nicht notwendig: Reguläre Ausdrücke sind beliebig, ohne jedwede Einschränkungen kombinierbar.

Ein regulärer Ausdruck bezeichnet eine Sprache, eine Teilmenge von $\mathbb{A}^*$. Wir werden zwei verschiedene Ansätze vorstellen, die Semantik regulärer Ausdrücke festzulegen. Der erste Ansatz ordnet einem regulären Ausdruck direkt eine Sprache zu. Der zweite zeigt, wie sich aus einem regulären Ausdruck ein Wort ableiten lässt; die Menge aller ableitbaren Worte entspricht dann der bezeichneten Sprache.

Denotationelle Semantik Kommen wir zum ersten Ansatz. Dieser heißt ***mathematische*** oder ***denotationelle Semantik***, da einem syntaktischen Objekt, in unserem Fall einem regulären Ausdruck, ein mathematisches Objekt, in unserem Fall eine Sprache, zugeordnet wird. Das mathematische Objekt ist die Bedeutung oder im Fachjargon die ***Denotation*** des syntaktischen Objekts.

Was ist die Bedeutung von ε oder eines Terminalsymbols? Nun, der reguläre Ausdruck ε bezeichnet die Sprache $\{\varepsilon\}$ und a entsprechend $\{a\}$, wobei a die einelementige Sequenz $\{0 \mapsto a\}$ abkürzt. (Wer überrascht ist, dass die Bedeutung von ε die Menge $\{\varepsilon\}$ und nicht etwa ε selbst ist, der sei daran erinnert, dass die Bedeutung eines regulären Ausdrucks eine Sprache ist, kein Wort.)

Wir haben die Konkatenation von Wörtern, sprich Sequenzen, bereits eingeführt. Jetzt müssen wir allerdings zwei Mengen konkatenieren: r_1 und r_2 bezeichnen zwei Sprachen, sagen wir L_1 und L_2, diese müssen verknüpft werden. Die Konkatenation von Sprachen lässt sich einfach auf die Konkatenation von Wörtern zurückführen, indem man jedes Wort der einen mit jedem Wort der anderen Menge konkateniert.

$$L_1 \cdot L_2 = \{w_1 \cdot w_2 \mid w_1 \in L_1, w_2 \in L_2\}$$

Das Symbol »·« ist jetzt ***überladen*** (genau wie ∅ und 0 und + und …): Es wird sowohl für die Konkatenation von Wörtern als auch für die Konkatenation von Sprachen verwendet. Der Zusammenhang ist allerdings ein direkter: Man sagt, die Operation oder Funktion »·« wird auf Mengen *fortgesetzt* und drückt damit aus, dass die obige Definition die naheliegende oder im Fachjargon die *kanonische* Wahl ist.

Die n-fache Konkatenation einer Sprache mit sich selbst wird, wie bei Wörtern mit L^n notiert, wobei $L^0 := \{\varepsilon\}$ und $L \cdot L^n =: L^{n+1} := L^n \cdot L$. Damit lässt sich auch die beliebige Wiederholung von Sprachen definieren.

$$L^* = \bigcup\{L^n \mid n \in \mathbb{N}\}$$

Der Operator $\bigcup$ vereinigt eine Menge von Mengen. Enthält L ein nicht-leeres Wort, dann ist L^* eine unendliche Menge.

Jetzt haben wir alle Zutaten beisammen, um die Bedeutung regulärer Ausdrücke zu definieren. Die Semantik wird durch die unten definierte Bedeutungsfunktion angegeben, die einen regulären Ausdruck, ein Element von `Reg`, auf eine Sprache, ein Element von $\mathcal{P}(\mathbb{A}^*)$, abbildet.

$$
\begin{aligned}
[\![a]\!] &= \{a\} \\
[\![\varepsilon]\!] &= \{\varepsilon\} \\
[\![r_1 \cdot r_2]\!] &= [\![r_1]\!] \cdot [\![r_2]\!] \\
[\![\varnothing]\!] &= \varnothing \\
[\![r_1 \mid r_2]\!] &= [\![r_1]\!] \cup [\![r_2]\!] \\
[\![r^*]\!] &= [\![r]\!]^*
\end{aligned}
$$

Die doppelten Klammern sind die sogenannten ***Oxford*** oder ***Strachey Klammern***[3]; sie schließen stets das syntaktische Objekt ein und trennen so Syntax von Semantik.

Jedem regulären Ausdruck r wird mit $[\![r]\!]$ eine Sprache, die Bedeutung des regulären Ausdrucks, zugeordnet. Die Bedeutungsfunktion $[\![-]\!]$ ist ***kompositional***: Die Bedeutung eines Ausdrucks wird auf die Bedeutung seiner Teilausdrücke zurückgeführt. Mit Hilfe der Bedeutungsfunktion können wir die Bedeutung von regulären Ausdrücken ausrechnen. Für die folgenden Beispiele verwenden wir das Alphabet $A = \{\mathsf{a}, \mathsf{b}\}$.

$$
\begin{aligned}
& [\![\mathsf{a\ b} \mid \mathsf{b\ a}]\!] \\
= \ & [\![\mathsf{a\ b}]\!] \cup [\![\mathsf{b\ a}]\!] \\
= \ & ([\![\mathsf{a}]\!] \cdot [\![\mathsf{b}]\!]) \cup ([\![\mathsf{b}]\!] \cdot [\![\mathsf{a}]\!]) \\
= \ & (\{\mathsf{a}\} \cdot \{\mathsf{b}\}) \cup (\{\mathsf{b}\} \cdot \{\mathsf{a}\}) \\
= \ & \{\mathsf{ab}\} \cup \{\mathsf{ba}\} \\
= \ & \{\mathsf{ab}, \mathsf{ba}\}
\end{aligned}
$$

Der reguläre Ausdruck $[\![\mathsf{a\ b} \mid \mathsf{b\ a}]\!]$ bezeichnet somit die Sprache $\{\mathsf{ab}, \mathsf{ba}\}$.

Vertauschen wir Konkatenation und Alternative erhalten wir eine andere Sprache:

$$
\begin{aligned}
& [\![(\mathsf{a} \mid \mathsf{b})\ (\mathsf{b} \mid \mathsf{a})]\!] \\
= \ & [\![\mathsf{a} \mid \mathsf{b}]\!] \cdot [\![\mathsf{b} \mid \mathsf{a}]\!] \\
= \ & ([\![\mathsf{a}]\!] \cup [\![\mathsf{b}]\!]) \cdot ([\![\mathsf{b}]\!] \cup [\![\mathsf{a}]\!]) \\
= \ & (\{\mathsf{a}\} \cup \{\mathsf{b}\}) \cdot (\{\mathsf{b}\} \cup \{\mathsf{a}\}) \\
= \ & \{\mathsf{a}, \mathsf{b}\} \cdot \{\mathsf{b}, \mathsf{a}\} \\
= \ & \{\mathsf{ab}, \mathsf{aa}, \mathsf{bb}, \mathsf{ba}\}
\end{aligned}
$$

Der reguläre Ausdruck $(\mathsf{a} \mid \mathsf{b})\ (\mathsf{b} \mid \mathsf{a})$ bezeichnet die Sprache der Wörter der Länge 2. Klar: Ist das Alphabet $A = \{\mathsf{a}, \mathsf{b}\}$, dann ist $\mathsf{a} \mid \mathsf{b}$ ein einzelner beliebiger Buchstabe und $(\mathsf{a} \mid \mathsf{b})\ (\mathsf{a} \mid \mathsf{b}) = (\mathsf{a} \mid \mathsf{b})\ (\mathsf{b} \mid \mathsf{a})$ sind zwei beliebige Buchstaben hintereinander. Ein letztes Beispiel:

$$
\begin{aligned}
& [\![((\mathsf{a} \mid \mathsf{b})\ (\mathsf{b} \mid \mathsf{a}))^*]\!] \\
= \ & [\![(\mathsf{a} \mid \mathsf{b})\ (\mathsf{b} \mid \mathsf{a})]\!]^* \\
= \ & \{\mathsf{ab}, \mathsf{aa}, \mathsf{bb}, \mathsf{ba}\}^*
\end{aligned}
$$

Die bezeichnete Sprache umfasst alle Wörter gerader Länge.

Eine Sprache $\mathrm{L} \subseteq \mathscr{P}(\mathbb{A}^*)$ heißt ***regulär***, wenn sie von einem regulären Ausdruck r beschrieben wird: $L = [\![r]\!]$. (Falls Sie sich wundern: Nicht jede Sprache ist regulär, dazu später mehr.)

Fassen wir zusammen: In der denotationellen Semantik wird einem syntaktischen Objekt, hier einem regulären Ausdruck, ein mathematisches Objekt, hier eine Sprache, zugeordnet. Die denotationelle Semantik ist nicht auf reguläre Ausdrücke eingeschränkt, sondern kann ganz allgemein

[3] Christopher Strachey (1916–1975), ein britischer Informatiker, war einer der Begründer der denotationellen Semantik.

verwendet werden, um die Bedeutung einer Sprache, insbesondere die einer Programmiersprache, zu beschreiben. Die Sprache Scheme [KCR98] verwendet zum Beispiel eine denotationelle Semantik, um die Bedeutung der Sprachkonstrukte präzise festzulegen.

Mit Hilfe der denotationellen Semantik können wir zeigen, dass zwei reguläre Ausdrücke gleichwertig sind, dass sie die gleiche Sprache bezeichnen: $[\![r_1]\!] = [\![r_2]\!]$. Für derartige Rechnungen ist es hilfreich, wenn wir uns mit den Eigenschaften von Vereinigung, Konkatenation und Wiederholung vertraut machen. Unternehmen wir also einen kleinen Ausflug in die Welt der Algebra.

Die Kleene Algebra der regulären Sprachen Die gleiche Sprache kann durch viele verschiedene reguläre Ausdrücke beschrieben werden, zum Beispiel bezeichnen $\mathtt{a} \mid \mathtt{b}$ und $\mathtt{b} \mid \mathtt{a}$ die gleiche Sprache: $[\![\mathtt{a} \mid \mathtt{b}]\!] = \{\mathtt{a}, \mathtt{b}\} = [\![\mathtt{b} \mid \mathtt{a}]\!]$. Die Situation ist uns von den Zahlen und dem Rechnen mit Zahlen wohlvertraut, zum Beispiel werten $4700 + 11$ und $7 \cdot 673$ zur gleichen Zahl aus: $4700 + 11 = 4711 = 7 \cdot 673$. Die Analogie sollte man allerdings nicht zu weit treiben; die arithmetische Operationen und die Operationen auf Sprachen besitzen nicht die gleichen Eigenschaften. So ist zum Beispiel die Vereinigung idempotent, $L \cup L = L$, nicht aber die Addition von Zahlen, $1 + 1 \neq 1$; die Multiplikation von Zahlen ist kommutativ, $x \cdot y = y \cdot x$, nicht aber die Konkatenation von Sprachen, $\{\mathtt{a}\} \cdot \{\mathtt{b}\} \neq \{\mathtt{b}\} \cdot \{\mathtt{a}\}$. Während die rationalen Zahlen mit Addition und Multiplikation einen sogenannten ***Körper*** (engl. field) bilden, formen die Sprachen eine ***Kleene Algebra***. Über Körper erfahren Sie mehr in den (begleitenden) Mathematikvorlesungen oder von den Kollegen/Kolleginnen der Biologie.

Kleene Algebren haben wir bereits in Verbindung mit Optimierungsproblemen (!) kennengelernt, siehe Abschnitt 5.5.1 (insbesondere Abbildung 5.26). Da der Abschnitt ergänzenden Lehrstoff enthält, fassen wir im Folgenden die wichtigsten Eigenschaften einer Kleene Algebra noch einmal zusammen — eine ausführliche Motivation und Herleitung der Axiome finden Sie in Anhang B.6.

Die Mengenvereinigung ist assoziativ, kommutativ und idempotent mit der leeren Sprache als neutralem Element: $(\mathscr{P}(\mathbb{A}^*), \varnothing, \cup)$ ist ein sogenannter ***Halbverband***.

$$\varnothing \cup R = R = R \cup \varnothing \qquad R \cup S = S \cup R$$
$$(R \cup S) \cup T = R \cup (S \cup T) \qquad R \cup R = R$$

Eine assoziative, kommutative und idempotente Verknüpfung definiert implizit eine Ordnung; in unserem Fall werden Sprachen mittels der Teilmengenbeziehung angeordnet.

$$A \subseteq B \iff A \cup B = B$$

Falls sich die Menge B nicht verändert, wenn wir die Elemente von A hinzufügen, dann ist A eine Teilmenge von B (die Menge A ist kleiner als B).

Die Konkatenation von Sprachen ist assoziativ mit der einelementigen Sprache $\{\varepsilon\}$ als neutralem Element: $(\mathscr{P}(\mathbb{A}^*), \{\varepsilon\}, \cdot)$ ist ein sogenanntes ***Monoid***.

$$\{\varepsilon\} \cdot R = R = R \cdot \{\varepsilon\}$$
$$(R \cdot S) \cdot T = R \cdot (S \cdot T)$$

Die Assoziativgesetze erlauben es uns, drei oder mehr Sprachen zu verknüpfen, ohne Klammern setzen zu müssen: $R \cup S \cup T$ und $R \cdot S \cdot T$ — eine wichtige Schreiberleichterung.

Kombiniert man zwei mathematische Strukturen (hier: einen Halbverband mit einem Monoid), dann muss man sich Gedanken über die Interaktion der Operationen machen. In unserem Fall wird das Zusammenspiel von Vereinigung und Konkatenation durch ***Distributivgesetze*** geregelt:

$$L \cdot \varnothing = \varnothing \qquad \varnothing \cdot L = \varnothing \tag{6.1a}$$
$$L \cdot (R \cup S) = (L \cdot R) \cup (L \cdot S) \qquad (R \cup S) \cdot L = (R \cdot L) \cup (S \cdot L) \tag{6.1b}$$

Die Distributivgesetze sind unentbehrlich für das Rechnen mit Sprachen; von rechts nach links angewendet vereinfachen sie Vereinigungen, indem ein gemeinsamer Faktor herausgezogen wird (suchen Sie nach den Stichworten ***Links-*** bzw. ***Rechtsfaktorisierung***).

Von den drei Operatoren, Vereinigung, Konkatenation und Wiederholung, ist der »Sternoperator« sicherlich der interessanteste. Zum einen weil er es uns erlaubt, unendliche Sprachen zu beschreiben. Zum anderen weil nicht unmittelbar klar ist, welche algebraischen Eigenschaften der Operator erfüllt oder erfüllen sollte. (Versuchen Sie, ein paar Gesetze zu formulieren, bevor Sie weiterlesen.) Wir skizzieren an dieser Stelle nur die Axiomatisierung; die vollständige Geschichte, für die uns leider nicht ausreichend Zeit zur Verfügung steht, erzählt wie gesagt Anhang B.6.

Die Wiederholung L^* kann als Lösung der Gleichung $X = L \cdot X \cup \{\varepsilon\}$ in der Unbekannten X aufgefasst werden: Konkatenieren wir L und L^* und ergänzen $\{\varepsilon\}$, erhalten wir wieder L^*. (Die Invariante erinnert an das Bildungsgesetz von Listen, siehe Abschnitt 4.2.2.) Auch die »gespiegelte« Gleichung $X = \{\varepsilon\} \cup X \cdot L$ wird von L^* erfüllt. Die »Schreib- bzw. Leserichtung« spielt sozusagen keine Rolle: Wir können Wiederholungen von links nach rechts oder von rechts nach links bilden. (Und Listen?)

Allerdings ist L^* in der Regel nicht die einzige Lösung der beiden Gleichungen: So wird zum Beispiel $X = \{\varepsilon, a\} \cdot X \cup \{\varepsilon\}$ nicht nur von $\{\varepsilon, a\}^*$, sondern auch von $\{a, b\}^*$ und von $\{a, b, c\}^*$ gelöst. Da schleicht sich ein ungutes Gefühl ein: Die letzten beiden Lösungen erscheinen willkürlich, da die Symbole b und c in der Gleichung garnicht erwähnt werden. Aus diesem Grund legen wir fest, dass L^* die *kleinste* Lösung der Gleichungen ist.

Die Axiome für den Sternoperator verallgemeinern die Ideen in zwei Richtungen. Zum einen werden *Un*gleichungen statt Gleichungen betrachtet — das liegt nahe, da wir die *kleinste* Lösung auszeichnen. Zum anderen wird nicht L^* selbst axiomatisiert, sondern die Sprachen $A^* \cdot B$ und $B \cdot A^*$ — das kommt etwas überraschend (Anhang B.6.4 legt die Gründe dar).

$$A \cdot (A^* \cdot B) \cup B \subseteq A^* \cdot B \tag{6.2a}$$
$$B \cup (B \cdot A^*) \cdot A \subseteq B \cdot A^* \tag{6.2b}$$
$$A^* \cdot B \subseteq X \iff A \cdot X \cup B \subseteq X \tag{6.2c}$$
$$B \cdot A^* \subseteq X \iff B \cup X \cdot A \subseteq X \tag{6.2d}$$

Das Axiom (6.2a) weist $A^* \cdot B$ als Lösung der Ungleichung $A \cdot X \cup B \subseteq X$ aus; das Prinzip der ***Fixpunkt-Induktion*** (6.2c) besagt, dass $A^* \cdot B$ die *kleinste* aller Lösungen ist.[4] Aus den Axiomen folgen eine Vielzahl weiterer Eigenschaften; auf drei wollen wir kurz eingehen, da sie uns im Folgenden des Öfteren über den Weg laufen.

Alle drei Operatoren, Vereinigung, Konkatenation und Wiederholung, sind ***monoton*** — unentbehrliche Eigenschaften, wenn man mit Ungleichungen rechnet.

$$A_1 \subseteq B_1 \ \wedge \ A_2 \subseteq B_2 \implies A_1 \cup A_2 \subseteq B_1 \cup B_2 \tag{6.3a}$$
$$A_1 \subseteq B_1 \ \wedge \ A_2 \subseteq B_2 \implies A_1 \cdot A_2 \subseteq B_1 \cdot B_2 \tag{6.3b}$$
$$A \subseteq B \implies A^* \subseteq B^* \tag{6.3c}$$

Aufgrund der folgenden Eigenschaften wird L^* auch als ***reflexive, transitive Hülle*** von L bezeichnet.

$$\{\varepsilon\} \subseteq L^* \qquad L^* \cdot L^* \subseteq L^* \qquad L \subseteq L^* \qquad (L^*)^* \subseteq L^* \tag{6.4}$$

[4] Ähnlich wie das Prinzip der ***natürlichen Induktion*** die Menge der natürlichen Zahlen als kleinste Menge mit bestimmten Eigenschaften auszeichnet.

Die letzten beiden Eigenschaften charakterisieren einen Hüllenoperator: L^* enthält die ursprüngliche Menge L; wenden wir den Sternoperator ein zweites Mal an, so bleibt die Hülle unverändert. Die ersten beiden Ungleichungen geben an, um welche Elemente die Menge L erweitert wird: Das leere Wort ist enthalten und jede beliebige Konkatenation von Wörtern — man sagt auch, L^* ist abgeschlossen unter der Konkatenation.

Die sogenannte ***Dekompositionsregel*** erlaubt es schließlich, eine Wiederholung von Vereinigungen umzuschreiben.[5]

$$A^* \cdot (B \cdot A^*)^* = (A \cup B)^* = (A^* \cdot B)^* \cdot A^* \tag{6.5}$$

Reduktionssemantik Kommen wir zum zweiten Ansatz, der ***Reduktionssemantik***. Während die denotationelle Semantik ein globales Bild vermittelt (»Welche Sprache bezeichnet der reguläre Ausdruck?«), bietet die Reduktionssemantik ein lokales Bild (»Wie kann ich ein einzelnes Wort aus dem regulären Ausdruck ableiten?«). Die Reduktionssemantik legt fest, wie ein regulärer Ausdruck schrittweise zu einem Wort reduziert wird. Für die denotationelle Semantik sind Wörter Elemente von $\mathbb{A}^*$; für die Reduktionssemantik sind Wörter besonders einfache reguläre Ausdrücke — so wie Werte besonders einfache Programme sind.

$w ::= a$	einzelnes Zeichen\Terminalsymbol
$\mid \varepsilon$	das leere Wort
$\mid w_1 \cdot w_2$	Konkatenation\Sequenz

Ein Wort zeichnet sich dadurch aus, dass seine Denotation eine einelementige Menge ist.

Die schrittweise Reduktion $r \longrightarrow r'$ (lies: r kann in *einem Schritt* zu r' reduziert werden) wird durch ein Beweissystem formalisiert. Dieses umfasst zunächst einmal die folgenden sogenannten ***Rechenregeln***:

$$\frac{}{r \cdot \varepsilon \longrightarrow r} \qquad \frac{}{\varepsilon \cdot r \longrightarrow r}$$

$$\frac{}{r_1 \mid r_2 \longrightarrow r_1} \qquad \frac{}{r_1 \mid r_2 \longrightarrow r_2}$$

$$\frac{}{r^* \longrightarrow \varepsilon} \qquad \frac{}{r^* \longrightarrow r \cdot r^*}$$

Die ersten beiden Regeln formalisieren, dass ε das neutrale Element der Konkatenation ist. Interessanter sind die letzten vier Regeln; sie haben mit Wahlmöglichkeiten zu tun. Die Alternative $r_1 \mid r_2$ kann entweder zu r_1 oder zu r_2 reduziert werden. Für die Wiederholung r^* gibt es ebenfalls zwei Alternativen: ε oder $r \cdot r^*$.

Für den regulären Ausdruck $\mathsf{a\,b} \mid \mathsf{b\,a}$ existieren somit zwei mögliche Reduktionen.

$$\mathsf{a\,b} \mid \mathsf{b\,a} \longrightarrow \mathsf{a\,b} \qquad \text{und} \qquad \mathsf{a\,b} \mid \mathsf{b\,a} \longrightarrow \mathsf{b\,a}$$

In beiden Fällen ist das Ergebnis direkt ein Wort, somit ist die bezeichnete Sprache $\{\mathsf{ab}, \mathsf{ba}\}$. Um den Ausdruck $(\mathsf{a} \mid \mathsf{b})\,(\mathsf{b} \mid \mathsf{a})$ zu vereinfachen, benötigen wir weitere Regeln. Die obigen Beweisregeln erlauben nur den *gesamten* Ausdruck umzuformen; wir brauchen zusätzlich Regeln, die es uns ermöglichen, einen Ausdruck »mittendrin« zu manipulieren, um etwa $(\mathsf{a} \mid \mathsf{b})\,(\mathsf{b} \mid \mathsf{a})$ zu $\mathsf{a}\,(\mathsf{b} \mid \mathsf{a})$ zu reduzieren. Diese Regeln nennt man auch ***Kongruenz-*** oder ***Kontextregeln***.[6]

$$\frac{r_1 \longrightarrow r_1'}{r_1 \cdot r_2 \longrightarrow r_1' \cdot r_2} \qquad \frac{r_2 \longrightarrow r_2'}{r_1 \cdot r_2 \longrightarrow r_1 \cdot r_2'}$$

[5] Einem ähnlichen Zweck dienen die binomischen Formeln.

[6] Kontextregeln verwenden wir routinemäßig, ohne uns groß darüber bewusst zu werden: Die Gleichungen $1 \cdot x = x = x \cdot 1$ werden in der Umformung $(x+1) \cdot (x-1) = x \cdot x + 1 \cdot x - x \cdot 1 - 1 \cdot 1 = x^2 - 1$ im Kontext einer Summe angewendet.

Die Kontextregeln sind rein bürokratische Regeln. Ihr einziger Zweck ist es, die Rechenregeln auf Teilausdrücke eines größeren Ausdrucks anwenden zu können. Kommen wir zu unserem Beispiel: Für $(a \mid b)\,(b \mid a)$ gibt es insgesamt acht mögliche *Reduktionsfolgen*.

$$\begin{aligned}
&(a \mid b)\,(b \mid a) \longrightarrow a\,(b \mid a) \longrightarrow a\,b && (a \mid b)\,(b \mid a) \longrightarrow (a \mid b)\,b \longrightarrow a\,b\\
&(a \mid b)\,(b \mid a) \longrightarrow a\,(b \mid a) \longrightarrow a\,a && (a \mid b)\,(b \mid a) \longrightarrow (a \mid b)\,b \longrightarrow b\,b\\
&(a \mid b)\,(b \mid a) \longrightarrow b\,(b \mid a) \longrightarrow b\,b && (a \mid b)\,(b \mid a) \longrightarrow (a \mid b)\,a \longrightarrow a\,a\\
&(a \mid b)\,(b \mid a) \longrightarrow b\,(b \mid a) \longrightarrow b\,a && (a \mid b)\,(b \mid a) \longrightarrow (a \mid b)\,a \longrightarrow b\,a
\end{aligned}$$

In zwei Schritten lässt sich jeweils ein Wort ableiten; in jedem Schritt wird eine Rechenregel angewendet. Die bezeichnete Sprache ist somit $\{ab, aa, bb, ba\}$. Wesentlich mehr Möglichkeiten haben wir im dritten Beispiel, nämlich unendlich viele.

$$\begin{aligned}
&((a \mid b)\,(b \mid a))^* \longrightarrow \varepsilon\\
&((a \mid b)\,(b \mid a))^* \longrightarrow (a \mid b)\,(b \mid a)\,((a \mid b)\,(b \mid a))^*\\
&\qquad\qquad\qquad\longrightarrow a\,(b \mid a)\,((a \mid b)\,(b \mid a))^*\\
&\qquad\qquad\qquad\longrightarrow a\,b\,((a \mid b)\,(b \mid a))^*\\
&\qquad\qquad\qquad\longrightarrow a\,b\,\varepsilon\\
&\qquad\qquad\qquad\longrightarrow a\,b\\
&\ldots
\end{aligned}$$

Das Wort w ist aus dem regulären Ausdruck r ***ableitbar***, wenn es eine Reduktionsfolge der Form

$$r \longrightarrow r_1 \longrightarrow \cdots \longrightarrow r_n \longrightarrow w$$

gibt. Die Sprache, die durch einen regulären Ausdruck beschrieben wird, ist die Menge aller *Worte*, die aus dem Ausdruck ableitbar sind. Die Betonung liegt auf Worte, denn eine Reduktionsfolge muss nicht zwangsläufig in einem Wort enden.

$$\varnothing^* \longrightarrow \varnothing\,\varnothing^* \longrightarrow \varnothing\,\varnothing\,\varnothing^* \longrightarrow \cdots$$

Da es keine Regel gibt, $\varnothing$ zu reduzieren, lässt sich mit dieser Reduktionsfolge kein Staat machen. Die einzig mögliche Reduktion ist $\varnothing^* \longrightarrow \varepsilon$. Somit ist die Semantik von $\varnothing^*$ die Sprache $\{\varepsilon\}$. (Auch mit der denotationellen Semantik erhalten wir $[\![\varnothing^*]\!] = \{\varepsilon\}$.)

Überzeugen Sie sich, dass die oben aufgeführten Reduktionsregeln ***korrekt*** sind: Wenn sich $r \longrightarrow r'$ ableiten lässt, dann gilt $[\![r]\!] \supseteq [\![r']\!]$. Die Kongruenzregeln folgen zum Beispiel aus der Monotonie der Konkatenation (6.3b). Warum verkleinert sich die repräsentierte Sprache? Das liegt daran, dass Wahlmöglichkeiten ergriffen werden!

Wie auch die denotationelle Semantik lässt sich die Reduktionssemantik verwenden, um die Gleichheit von zwei regulären Ausdrücken r_1 und r_2 zu klären. Dazu zeigt man, dass es zu jeder Reduktionsfolge $r_1 \longrightarrow \cdots \longrightarrow w$ eine korrespondierende Reduktionsfolge $r_2 \longrightarrow \cdots \longrightarrow w$ gibt und umgekehrt.

Zwei Semantiken, zwei Antworten auf die Frage »Was bedeutet ein regulärer Ausdruck?«. Ist die Antwort in beiden Fällen die gleiche? Ja! Da uns die nötigen Hilfsmittel für den Nachweis dieser Tatsache fehlen, nehmen wir die gute Nachricht so hin.

Wie auch die denotationelle Semantik wird die Reduktionssemantik verwendet, um die Bedeutung von Programmiersprachen festzulegen. Die Reduktionssemantik ist der Semantik von Mini-F#, der sogenannten ***Auswertungssemantik***, sehr ähnlich. Beide werden durch Beweissysteme spezifiziert; beide beschreiben, wie ein Programm ausgerechnet wird. Die Reduktionssemantik beschreibt einen *einzelnen Schritt*; die Auswertungssemantik eine *vollständige Rechnung*. Für reguläre Ausdrücke lässt sich übrigens auch eine Auswertungssemantik angeben, siehe Aufgabe 6.1.7.

6.1.3. Vertiefung: Beispiele

»Paritätische« Sprachen Schauen wir uns weitere Beispiele für reguläre Ausdrücke an. Das zugrundeliegende Alphabet ist im Folgenden weiterhin $A = \{\mathsf{a}, \mathsf{b}\}$. Der Ausdruck

$$(\mathsf{b} \mid \mathsf{a}\,\mathsf{b}^*\,\mathsf{a})^*$$

bezeichnet die Sprache aller Wörter mit einer geraden Anzahl von as und beliebig vielen bs. Ein einzelnes b erfüllt diese Eigenschaft; ebenso ein a, gefolgt von bs, gefolgt von einem weiteren a. Von diesen Wörtern, b oder $\mathsf{a}\ \mathsf{b}^*\ \mathsf{a}$, können wir beliebig viele hintereinandersetzen, ohne die Eigenschaft zu verletzen (die Summe zweier gerader Zahlen ist wiederum gerade).

Wir haben schon diskutiert, dass die gleiche Sprache durch viele verschiedene reguläre Ausdrücke beschrieben werden kann. Zum Beispiel bezeichnet $(\mathsf{a}\,\mathsf{b}^*\,\mathsf{a} \mid \mathsf{b})^*$ die gleiche Sprache wie $(\mathsf{b} \mid \mathsf{a}\,\mathsf{b}^*\,\mathsf{a})^*$. Das ist eine recht offensichtliche Umformung, da die Alternative semantisch eine Vereinigung ist und somit kommutativ. Weniger offensichtlich ist, dass wir die gleiche Sprache auch *ohne* Alternative beschreiben können:

$$\mathsf{b}^*\,(\mathsf{a}\,\mathsf{b}^*\,\mathsf{a}\,\mathsf{b}^*)^*$$

Hier kommt die Dekompositionsregel (6.5) zum Einsatz: An die Stelle der iterierten Alternative tritt eine geschachtelte Wiederholung.

Die Sprache aller Wörter, die eine gerade Anzahl von as *oder* eine ungerade Anzahl von bs haben, lässt sich unter Rückgriff auf das vorherige Beispiel leicht definieren.

$$(\mathsf{b} \mid \mathsf{a}\,\mathsf{b}^*\,\mathsf{a})^* \mid \mathsf{a}^*\,\mathsf{b}\,(\mathsf{a} \mid \mathsf{b}\,\mathsf{a}^*\,\mathsf{b})^*$$

Aber wie beschreibt man die Sprache aller Wörter, die eine gerade Anzahl von as *und* eine ungerade Anzahl von bs enthalten? Die Sprache für reguläre Ausdrücke hat zwar eine Operation für die Vereinigung, nicht aber für den Durchschnitt. Stände ein Pendant zum Durchschnitt bereit, sagen wir &, könnten wir formulieren:

$$(\mathsf{a}\,\mathsf{b}^*\,\mathsf{a} \mid \mathsf{b})^* \,\&\, \mathsf{a}^*\,\mathsf{b}\,(\mathsf{a} \mid \mathsf{b}\,\mathsf{a}^*\,\mathsf{b})^* \tag{6.6}$$

In der Tat spricht nichts dagegen, den Durchschnitt zu der Sprache der regulären Ausdrücke hinzuzufügen, siehe Aufgabe 6.1.8. Interessanterweise ist die Erweiterung zwar bequem, aber nicht notwendig: Sie erhöht nicht die Ausdruckskraft. Mehr dazu später aus der Abteilung der Theoretischen Informatik. Wir versuchen an dieser Stelle einfach, die Sprache mit den bisherigen Bordmitteln zu definieren. Dazu sind zwei Abkürzungen nützlich: $g = (\mathsf{a}\ \mathsf{a})^*$ und $u = \mathsf{a}\ (\mathsf{a}\ \mathsf{a})^*$. Starten wir bescheiden und definieren eine Sprache, die genau ein b und eine gerade Anzahl von as enthält.

$$g\,\mathsf{b}\,g \mid u\,\mathsf{b}\,u$$

Entweder kommen vor und hinter dem b eine gerade Anzahl von as vor oder an beiden Positionen eine ungerade Anzahl. Nächster Schritt: Wir erhöhen die Anzahl der bs auf zwei:

$$g\,\mathsf{b}\,g\,\mathsf{b}\,g \mid g\,\mathsf{b}\,u\,\mathsf{b}\,u \mid u\,\mathsf{b}\,g\,\mathsf{b}\,u \mid u\,\mathsf{b}\,u\,\mathsf{b}\,g$$

Jetzt werden die as über drei Positionen verteilt; entweder befinden sich an allen Stellen eine gerade Anzahl von as oder an exakt zwei Positionen eine ungerade Anzahl. Jetzt sind wir fast am Ziel. Eine ungerade Zahl hat die Form $2 \cdot n + 1$, entsprechend definieren wir als Alternative zu (6.6):

Numeral	*digit digit**
Stringliteral	" (^(?* (" ∣ \) ?*) ∣ \" ∣ \\ ∣ \t ∣ \n ∣ \v ∣ \f ∣ \r)* "
Bezeichner klein	*lower* (*lower* ∣ *upper* ∣ *digit* ∣ ' ∣ _)*
Bezeichner groß	*upper* (*lower* ∣ *upper* ∣ *digit* ∣ ' ∣ _)*
Typparameter	' (*lower* ∣ *upper* ∣ *digit* ∣ _)*
Schlüsselwörter	abstract ∣ and ∣ as ∣ assert ∣ base ∣ begin ∣ class ∣ default ∣ delegate ∣ do ∣ done ∣ downcast ∣ downto ∣ elif ∣ else ∣ end ∣ exception ∣ extern ∣ false ∣ finally ∣ for ∣ fun ∣ function ∣ global ∣ if ∣ in ∣ inherit ∣ inline ∣ interface ∣ internal ∣ lazy ∣ let ∣ match ∣ member ∣ module ∣ mutable ∣ namespace ∣ new ∣ null ∣ of ∣ open ∣ or ∣ override ∣ private ∣ public ∣ rec ∣ return ∣ sig ∣ static ∣ struct ∣ then ∣ to ∣ true ∣ try ∣ type ∣ upcast ∣ use ∣ val ∣ void ∣ when ∣ while ∣ with ∣ yield
Separatoren	(∣) ∣ , ∣ { ∣ }
Symbole	! ∣ % ∣ & ∣ && ∣ * ∣ + ∣ , ∣ - ∣ -> ∣ . ∣ .. ∣ / ∣ : ∣ := ∣ < ∣ <= ∣ <> ∣ = ∣ > ∣ >= ∣ [∣ [∣ ∣] ∣ ^ ∣ _ ∣ ∣ ∣ ∣] ∣ ∣∣
Leerzeichen	∣ \t ∣ \n ∣ \v ∣ \f ∣ \r
Zeilenkommentar	// ^(?* \n ?*) \n
Kommentar	(* ^(?* *) ?*) *)

Abbildung 6.3.: Lexikalische Syntax von Mini–F#.

$$(g\,\mathsf{b}\,g \mid u\,\mathsf{b}\,u)\,(g\,\mathsf{b}\,g\,\mathsf{b}\,g \mid g\,\mathsf{b}\,u\,\mathsf{b}\,u \mid u\,\mathsf{b}\,g\,\mathsf{b}\,u \mid u\,\mathsf{b}\,u\,\mathsf{b}\,g)^*$$

Man sieht, ohne den Durchschnitt müssen wir bei der Formulierung von Sprachen sehr viel mehr Grips investieren.

Das bringt uns zu der Frage, ob wir mit regulären Ausdrücken überhaupt alle Sprachen beschreiben können bzw. wenn das nicht möglich ist, ob wir wenigstens die Syntax von Programmiersprachen festlegen können. Die Antwort auf beide Fragen ist negativ, reguläre Ausdrücke sind in ihren Möglichkeiten stark eingeschränkt — deswegen werden sie tatsächlich nur für die lexikalische Syntax herangezogen. (Die Antwort auf die erste Frage ist übrigens immer negativ, da es sehr viel mehr Sprachen gibt als Ausdrücke, mit denen Sprachen beschrieben werden können, siehe Anhang B.2.4.) Mit Hilfe regulärer Ausdrücke lassen sich zum Beispiel einfache Hygienevorschriften nicht fassen, etwa, dass es in Mini–F# Ausdrücken zu jeder »Klammer auf« eine korrespondierende »Klammer zu« geben muss. Selbst die Sprache, die nur aus ordentlich geschachtelten Klammerpaaren besteht,

$$\{\mathsf{a}^n\,\mathsf{b}^n \mid n \in \mathbb{N}\}$$

ist keine reguläre Sprache — lies a als »(« und b als »)«. Warum das so ist, werden wir im nächsten Abschnitt sehen.

Lexikalische Syntax von Mini–F# Kommen wir zur lexikalischen Syntax von Mini–F#. Abbildung 6.3 fasst die Lexeme der Sprache zusammen. Die dort aufgeführten regulären Ausdrücke verwenden zwei Erweiterungen: »?« steht für ein beliebiges Zeichen und $\hat{}r$ steht für das Komplement von r. Wie auch die Konjunktion erhöhen die neuen Konstrukte die Bequemlichkeit, nicht aber die prinzipielle Ausdruckskraft regulärer Ausdrücke — wir kommen in Abschnitt 6.2 noch

einmal darauf zu sprechen. Ist das Alphabet $\mathbb{A} = \{a_1, \ldots, a_n\}$, dann ist »?« eine Abkürzung für $a_1 \mid \cdots \mid a_n$. Im Komplement $\hat{}r$ sind alle Wörter enthalten, die in r *nicht* enthalten sind. Was Disjunktion (||), Konjunktion (&&) und Negation (*not*) für Boolesche Werte sind, sind Alternative (|), Durchschnitt (&) und Komplement (^) für Sprachen.

Gehen wir die Lexeme in Abbildung 6.3 einmal durch. Ein Numeral ist eine Konstante vom Typ *Nat*. Ein Stringliteral ist eine Konstante vom Typ *String* und bezeichnet einen Text, eine Sequenz von Zeichen. Strings werden in Anführungsstriche (oben) eingeschlossen. Innerhalb der Anführungsstriche darf das Zeichen »"« selbst nicht vorkommen. Soll »"« ein Zeichen des Textes sein, so muss dem doppelten Anführungsstrich das Fluchtsymbol »\« vorangestellt werden. Das Literal `"\"Zitat\""` bezeichnet somit einen Text, der aus sieben Zeichen besteht. Mini–F# kennt noch weitere Fluchtsequenzen, etwa `\n` für den Zeilenvorschub, ein nicht druckbares Zeichen des ASCII-Alphabets.

Wir unterscheiden zwischen drei Arten von Bezeichnern, solchen, die mit einem kleinen Buchstaben anfangen, solchen, die mit einem großen Buchstaben anfangen, und solchen, die mit einem Apostroph anfangen. Kleine Bezeichner werden für Werte (*size*, *area*) und Labels (*day*, *month*) verwendet; große Bezeichner für Konstruktoren (*Nil*, *Cons*) und Typen (*Person*, *List*); Apostrophbezeichner ausschließlich für Typparameter (*'a*, *'soln*).[7] Bestimmte Folgen von kleinen Buchstaben (***let***, ***in*** usw.), sogenannte Schlüsselwörter, sind reserviert und dienen der kontextfreien Syntax als Interpunktionszeichen. Bei der Unterteilung eines Programmtextes werden Lexeme so lang wie möglich gewählt (engl. longest match): `letter` ist ein Bezeichner, `let ter` aber das Schlüsselwort `let` gefolgt von dem Bezeichner `ter`.

Bestimmte Symbole, wie etwa die Klammerpaare `(` und `)`, `{` und `}`, werden als Interpunktionszeichen verwendet, andere Symbole dienen als Bezeichner für Operatoren, wie zum Beispiel `+` und `*`. Die als Separatoren gekennzeichneten Symbole stehen stets für ein einzelnes Lexem, alle anderen Symbole können auch zu größeren Einheiten kombiniert werden: etwa `>` und `=` zu `>=`. Wie auch bei den Schlüsselwörtern gilt, dass Lexeme so lang wie möglich gewählt werden: `>=` ist ein Lexem, `> =` sind zwei Lexeme.

Einzelne Lexeme können durch Leerzeichen oder Kommentare getrennt werden. Mini–F# unterscheidet zwischen Zeilenkommentaren, die mit `//` anfangen und sich bis zum Zeilenende erstrecken, und normalen Kommentaren, die von den Kommentarklammern `(*` und `*)` eingeschlossen werden. (Entgegen der Spezifikation in Abbildung 6.3 dürfen Kommentare auch geschachtelt werden. Ordentlich geschachtelte Klammerpaare lassen sich aber, wie wir bereits wissen, mit regulären Ausdrücken nicht beschreiben.)

Übungen.

1. Welche Sprachen bezeichnen die folgenden regulären Ausdrücke?

(a) `0 (0 | 1)* 0`,

(b) `((ε | 0) 1*)*`,

(c) `(0 | 1)* 0 (0 | 1) (0 | 1)`,

(d) `0* 1 0* 1 0* 1 0*`.

Geben Sie die Sprachen sowohl umgangssprachlich als auch formal an.

2. Geben Sie für die folgenden Sprachen reguläre Ausdrücke an.

(a) Alle Buchstabenfolgen, die die fünf Vokale jeweils genau einmal in der Reihenfolge des Alphabets beinhalten.

(b) Alle Buchstabenfolgen, bei denen die Buchstaben lexikographisch aufsteigend geordnet sind.

[7] Diese Konvention zusammen mit der Farbcodierung erlaubt es, jeden Bezeichner eindeutig einer Kategorie zuzuordnen. (Wir mogeln tatsächlich etwas: In F# können kleine Bezeichner auch für Typen (*int*) und große Bezeichner für Werte und Labels (*Length*) benutzt werden.)

(c) Kommentare, die aus Zeichenketten über dem Alphabet $A = \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{y}, \mathtt{z}, \mathtt{(}, \mathtt{)}, \mathtt{*}, \mathtt{"}\}$ bestehen, die in `(*` und `*)` eingeschlossen sind und die weder `(*` noch `*)` enthalten, es sei denn innerhalb von Anführungszeichen (" ... ").

(d) Alle Folgen von `0` und `1`, bei denen nicht mehrere `1`en direkt nebeneinander stehen.

(e) Alle nicht-leeren Folgen von `0` und `1`, bei denen das erste und das letzte Zeichen identisch sind.

(f) Alle Ziffernfolgen, die keine Ziffer mehrfach enthalten.

(g) Alle Ziffernfolgen, die höchstens eine Ziffer mehrfach enthalten.

(h) Alle Folgen aus `0` und `1`, in denen `001` nicht enthalten ist.

3. Um größere Zahlen besser lesen zu können, setzt man oft einen Punkt zwischen Gruppen aus drei Ziffern: zum Beispiel 4.711 oder 1.234.567. Geben Sie einen regulären Ausdruck für Numerale mit Tausenderpunkt an.

4. Welche Sprache bezeichnet der folgende reguläre Ausdruck?

$$\mathit{riddle} = (\mathtt{a\,a} \mid \mathtt{b\,b})^* \; ((\mathtt{a\,b} \mid \mathtt{b\,a})\,(\mathtt{a\,a} \mid \mathtt{b\,b})^*\,(\mathtt{a\,b} \mid \mathtt{b\,a})\,(\mathtt{a\,a} \mid \mathtt{b\,b})^*)^*$$

Welche Sprachen bezeichnen $\mathtt{a} \setminus \mathit{riddle}$ und $\mathtt{b} \setminus \mathit{riddle}$?

5. Zeige $A \cdot (A^* \cdot B) \cup B = A^* \cdot B$ und $B \cup (B \cdot A^*) \cdot A = B \cdot A^*$.

6. Zeigen Sie die Korrektheit der Reduktionsregeln.

7. Formulieren Sie eine Auswertungssemantik für reguläre Ausdrücke, indem Sie Beweisregeln für die Auswertungsrelation $r \Downarrow w$ aufstellen.

8. Wenn wir Durchschnitt und Komplement zu den regulären Ausdrücken hinzunehmen, lassen sich viele Sprache einfacher formulieren.

$r ::= \cdots$	***reguläre Ausdrücke:***
$\mid r_1 \,\&\, r_2$	Durchschnitt
$\mid \hat{}r$	Komplement

(a) Legen Sie die denotationelle Semantik dieser Erweiterung fest.

(b) Stellen Sie die Reduktionssemantik für diese Erweiterung auf (schwierig).

6.2. Scanner\Akzeptoren

6.2.1. Akzeptoren

Ein regulärer Ausdruck r beschreibt eine Sprache. Wie können wir feststellen, ob ein gegebenes Wort w in der Sprache enthalten ist? Dieses Problem, $w \in [\![r]\!]$, nennt man auch kurz und prägnant ***Wortproblem***. (Bei der Aufteilung eines Programmtextes in einzelne Lexeme ist eine ähnliche Operation gefragt.) Oder besser: Können wir ein Mini-F# Programm schreiben, das uns diese Aufgabe abnimmt? Die Antwort ist diesmal positiv. Ein solches Programm nennt man auch ***Akzeptor***. (Das Programm, das einen Programmtext in Lexeme aufteilt, hört auf den Namen ***Lexer*** oder ***Scanner***.) Im Folgenden gehen wir die einzelnen Schritte exemplarisch für den regulären Ausdruck $r_{00} = (\mathtt{a} \mid \mathtt{b})^*\,\mathtt{b}\,(\mathtt{a} \mid \mathtt{b})$ durch — der Ausdruck beschreibt die ***advPieb-Sprache***, die Sprache aller Wörter, die an der vorletzten Position ein `b` enthalten.

Überlegen wir uns zunächst die Schnittstelle des Programms. Wir gehen davon aus, dass das Alphabet durch eine Variantentypdefinition gegeben ist. Zum Beispiel:

```
type Alphabet = | A | B
let ord-Alphabet (a : Alphabet) : Int =
  match a with | A → 0 | B → 1
```

module Grammar.Alphabet
module Grammar.Compiled

Zu einem Alphabet gehört eine injektive Funktion, die sogenannte Codierungsfunktion, die jedem Zeichen eine ganze Zahl zuordnet, den sogenannten ***Zeichencode***.

Ein Akzeptor ist eine Funktion des folgenden Typs.

$$\mathit{accept\text{-}r_{00}} : \mathit{List}\,\langle \mathit{Alphabet} \rangle \to \mathit{Bool}$$

Die Funktion $\mathit{accept\text{-}r_{00}}$ testet, ob die Eingabe w ein Element der durch r_{00} bezeichneten Sprache ist: $w \in [\![r_{00}]\!]$. Das Struktur Entwurfsmuster für *List* motiviert einen ersten Ansatz:

```
let rec accept-r00 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → …
  | A :: rest → … accept-r00 rest …
  | B :: rest → … accept-r00 rest …
```

Der rekursive Aufruf von $\mathit{accept\text{-}r_{00}}$ hilft uns an dieser Stelle leider nicht weiter. Aus $w \in [\![r_{00}]\!]$ können wir nur bedingt Rückschlüsse auf $a \cdot w \in [\![r_{00}]\!]$ ziehen. Gehen wir die Zweige des ***match***-Ausdrucks der Reihe nach durch. Im Fall $\mathit{input} = [\,]$ müssen wir überlegen, ob das leere Wort in der Sprache enthalten ist: $\varepsilon \in [\![r]\!]$. Wir müssen einen Spezialfall des Wortproblems lösen: das ***ε-Problem***. Können wir dem regulären Ausdruck das ansehen? Können wir eine semantische Eigenschaft — ist ε Element der möglicherweise unendlichen Menge $[\![r]\!]$ — an Hand der Form, das heißt der Syntax von r überprüfen? Ja, so geht's:[8]

$$\begin{aligned}
\mathit{nullable}(a) &= \mathit{false}\\
\mathit{nullable}(\varepsilon) &= \mathit{true}\\
\mathit{nullable}(r_1 \cdot r_2) &= \mathit{nullable}(r_1) \wedge \mathit{nullable}(r_2)\\
\mathit{nullable}(\varnothing) &= \mathit{false}\\
\mathit{nullable}(r_1 \mid r_2) &= \mathit{nullable}(r_1) \vee \mathit{nullable}(r_2)\\
\mathit{nullable}(r^*) &= \mathit{true}
\end{aligned}$$

Die Konkatenation $r_1 \cdot r_2$ enthält ε, wenn sowohl r_1 als auch r_2 das leere Wort ε enthalten; die Alternative $r_1 \mid r_2$ enthält ε, wenn entweder r_1 oder r_2 das leere Wort ε enthalten. Die Wiederholung r^* enthält ε auf jeden Fall. Somit können wir den ersten Zweig von $\mathit{accept\text{-}r_{00}}$ mit Leben füllen: $\mathit{nullable}(r_{00}) = \mathit{false}$, also

```
let rec accept-r00 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → false
  | A :: rest → … accept-r00 rest …
  | B :: rest → … accept-r00 rest …
```

Kommen wir zum Fall $\mathit{input} = A :: \mathit{rest}$. An dieser Stelle wäre es nützlich zu wissen, was von der Sprache »übrigbleibt«, jetzt da wir a bereits gesehen haben. Dann könnten wir die Arbeit an eine weitere Funktion delegieren, den Akzeptor für die »Restsprache«. Diese »Restsprache« heißt im Fachjargon ***Rechtsfaktor*** und ist für ein Wort w wie folgt definiert:[9]

$$w \setminus \mathrm{L} = \{\, x \mid w \cdot x \in \mathrm{L} \,\} \tag{6.7}$$

[8] Die Funktion *nullable* ist eine mathematische Funktion, kein Mini–F# Programm. Der Name ist historisch bedingt und möglicherweise irreführend. Der Nullelement der Kleene Algebra ist ∅; die Sprache $\{\varepsilon\}$ ist ihr Einselement — »unitable« würde es also vielleicht besser treffen. Im Text vermeiden wir die englischen Begriffe und sprechen stattdessen von ε-***haltigen*** und ε-***freien*** Sprachen.

[9] Da die Konkatenation *nicht* kommutativ ist, gibt es zwei verschiedene Divisionsoperationen: $w \setminus \mathrm{L}$ und L / w, Rechts- und Linksfaktoren. Dabei deutet die Neigung der Symbole »\« und »/« Dividend und Divisor an. Wenn die Multiplikation wie im Fall der reellen Zahlen kommutativ ist, muss man nicht so fein unterscheiden und man schreibt wahlweise $b \setminus a$ oder $\frac{a}{b}$ oder a / b.

Der Rechtsfaktor $w \setminus L$ (lies: w dividiert L *oder* L durch w) ist die Menge aller Restworte x, so dass $w \cdot x$ in L enthalten ist. Nun ist L eine reguläre Sprache und wir müssen überlegen, ob $w \setminus L$ ebenfalls regulär ist. Zunächst einmal gilt (beachte die Reihenfolge der Divisionen):

$$\begin{aligned} \varepsilon \setminus L &= L \\ (w_1 \cdot w_2) \setminus L &= w_2 \setminus (w_1 \setminus L) \end{aligned}$$

Das heißt, wir können uns auf die Herleitung von $a \setminus L$ konzentrieren, wobei a ein Terminalsymbol ist. Der schwierigste Fall ist die Konkatenation: $a \setminus (r_1 \cdot r_2)$. Entweder wir entfernen a aus r_1 oder aus r_2; letzteres ist aber nur möglich, wenn der reguläre Ausdruck r_1 ε-haltig ist. Damit erhalten wir

$$\begin{aligned} x \setminus a &= \begin{cases} \varepsilon & \text{falls } a = x \\ \varnothing & \text{sonst} \end{cases} \\ x \setminus \varepsilon &= \varnothing \\ x \setminus (r_1 \cdot r_2) &= \begin{cases} (x \setminus r_1) \cdot r_2 \mid (x \setminus r_2) & \text{falls } \mathit{nullable}(r_1) \\ (x \setminus r_1) \cdot r_2 & \text{sonst} \end{cases} \\ x \setminus \varnothing &= \varnothing \\ x \setminus (r_1 \mid r_2) &= (x \setminus r_1) \mid (x \setminus r_2) \\ x \setminus r^* &= (x \setminus r) \cdot r^* \end{aligned}$$

Die Definition des Rechtsfaktors ist der *Ableitung von Funktionen* sehr ähnlich (lies ε als 1, ∅ als 0, die Alternative als Summe und die Konkatenation als Produkt). Die Regel für die Alternative entspricht exakt der Summenregel der Analysis; die Regel für die Konkatenation entspricht *fast* der Produktregel — die Produktregel der Analysis ist vollkommen symmetrisch: Es gilt $x \setminus (r_1 \cdot r_2) = (x \setminus r_1) \cdot r_2 \mid r_1 \cdot (x \setminus r_2)$.

Halten wir fest: Das Wortproblem lässt sich in zwei Teilaufgaben untergliedern, die Lösung des ε-Problems und die Berechnung von Rechtsfaktoren — diese können peu à peu zeichenweise bestimmt werden.

$$a_1 \ldots a_n \in [\![r]\!] \quad \Longleftrightarrow \quad \mathit{nullable}(a_n \setminus (\cdots (a_1 \setminus r) \cdots)) \tag{6.8}$$

Wie sehen die Rechtsfaktoren für unser Beispiel aus?

$$\begin{aligned} \mathsf{a} \setminus r_{00} &= r_{00} \\ \mathsf{b} \setminus r_{00} &= r_{00} \mid (\mathsf{a} \mid \mathsf{b}) = r_{10} \end{aligned}$$

Wir erhalten r_{00} selbst und einen neuen regulären Ausdruck, den wir auf den Namen r_{10} taufen. Damit können wir endlich die Definition von *accept-r*$_{00}$ vervollständigen.

```
let rec accept-r00 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → false
  | A :: rest → accept-r00 rest
  | B :: rest → accept-r10 rest
```

Ist das erste Zeichen ein A, dann erfolgt ein rekursiver Aufruf; ist das Zeichen ein B, dann wird die weitere Arbeit an *accept-r*$_{10}$ delegiert.

Es verbleibt einen Akzeptor für r_{10} zu schreiben. Diese Aufgabe gehen wir nach dem gleichen Schema wie für r_{00} an.

$$\begin{aligned}
&\mathit{nullable}(r_{10}) = \mathit{false}\\
&\mathsf{a} \setminus r_{10} = r_{00} \mid \varepsilon \qquad\qquad = r_{01}\\
&\mathsf{b} \setminus r_{10} = r_{00} \mid (\mathsf{a} \mid \mathsf{b}) \mid \varepsilon = r_{11}
\end{aligned}$$

Wir erhalten zwei neue reguläre Ausdrücke und rechnen weiter.

$$\begin{aligned}
&\mathit{nullable}(r_{01}) = \mathit{true}\\
&\mathsf{a} \setminus r_{01} = r_{00}\\
&\mathsf{b} \setminus r_{01} = r_{10}\\
&\mathit{nullable}(r_{11}) = \mathit{true}\\
&\mathsf{a} \setminus r_{11} = r_{01}\\
&\mathsf{b} \setminus r_{11} = r_{11}
\end{aligned}$$

In der letzten Runde sind keine neuen regulären Ausdrücke hinzugekommen. Somit können wir unser Programm zusammenpuzzeln. Die Aufrufstruktur ist recht chaotisch: Die Funktion *accept-*r_{00} ruft *accept-*r_{10} auf, diese ruft *accept-*r_{11} auf, diese ruft *accept-*r_{01} auf und diese wiederum *accept-*r_{00}, siehe Abbildung 6.4. Mit anderen Worten, die vier Akzeptoren sind ***verschränkt***

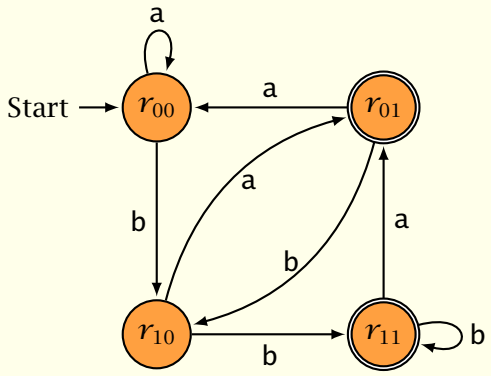


Abbildung 6.4.: Aufrufgraph des Akzeptors.

rekursiv definiert. Zur Erinnerung: Verschränkt rekursive Funktionsdefinitionen müssen mit dem Schlüsselwort ***and*** verbunden werden, damit jede Funktion jede andere sieht: ***let rec*** $f_1\ (x_1) = e_1$ ***and*** $f_2\ (x_2) = e_2$. Die Bezeichner f_1 und f_2 sind sowohl in e_1 als auch in e_2 sichtbar. Das vollständige Programm für *accept-*r_{00} ist in Abbildung 6.5 aufgeführt.

Der reguläre Ausdruck $(\mathsf{a} \mid \mathsf{b})^*\ \mathsf{b}\ (\mathsf{a} \mid \mathsf{b})$ hat vier verschiedene Rechtsfaktoren, der Ausdruck $(\mathsf{b} \mid \mathsf{a}\ \mathsf{b}^*\ \mathsf{a})^*$ hat zwei (welche?). Allgemein kann man zeigen, dass eine Sprache, die durch einen regulären Ausdruck beschrieben wird, nur *endlich* viele verschiedene Rechtsfaktoren besitzt. (Die Umkehrung gilt übrigens auch, mehr dazu in Abschnitt 6.3.5.) Diese Eigenschaft können wir ausnutzen, um zu zeigen, dass eine Sprache *nicht* durch einen regulären Ausdruck beschrieben werden kann. Wir haben im letzten Abschnitt erwähnt, dass $L = \{\mathsf{a}^n\ \mathsf{b}^n \mid n \in \mathbb{N}\}$ eine solche Sprache ist. Die Rechtsfaktoren für Wörter der Form a^k sind gegeben durch:

$$\mathsf{a}^k \setminus L = \{\mathsf{a}^n\ \mathsf{b}^{n+k} \mid n \in \mathbb{N}\}$$

Alle diese Sprachen sind verschieden, also ist L keine reguläre Sprache.

Die Definition des Rechtsfaktors $x \setminus r$ lässt sich übrigens leicht auf die Operationen »&« und »^«, Durchschnitt und Komplement regulärer Ausdrücke, erweitern.

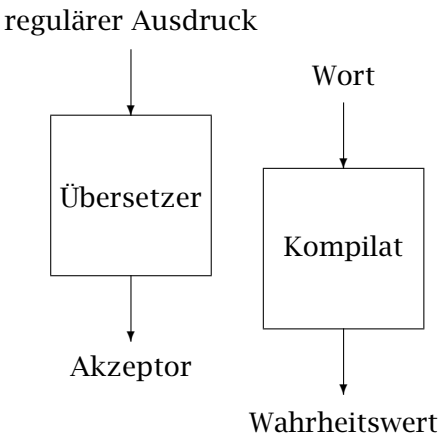
$$\begin{aligned}
x \setminus (r_1 \,\&\, r_2) &= (x \setminus r_1) \,\&\, (x \setminus r_2)\\
x \setminus \hat{}r &= \hat{}(x \setminus r)
\end{aligned}$$

```
let rec accept-r00 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → false                  // nullable(r00) = false
  | A :: rest → accept-r00 rest        // a \ r00 = r00
  | B :: rest → accept-r10 rest        // b \ r00 = r10
and accept-r10 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → false                  // nullable(r10) = false
  | A :: rest → accept-r01 rest        // a \ r10 = r01
  | B :: rest → accept-r11 rest        // b \ r10 = r11
and accept-r01 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → true                   // nullable(r01) = true
  | A :: rest → accept-r00 rest        // a \ r01 = r00
  | B :: rest → accept-r10 rest        // b \ r01 = r10
and accept-r11 (input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → true                   // nullable(r11) = true
  | A :: rest → accept-r01 rest        // a \ r11 = r01
  | B :: rest → accept-r11 rest        // b \ r11 = r11
```

Abbildung 6.5.: Akzeptor für (a | b)* b (a | b).

Auch für diese Erweiterungen gilt, dass die Menge aller Rechtsfaktoren endlich ist. Wenn man gezeigt hat, dass eine Sprache mit endlich vielen Rechtsfaktoren regulär ist, dann ist damit auch klar, dass Durchschnitt und Komplement die Ausdruckskraft regulärer Ausdrücke nicht erhöhen (die erweiterten regulären Ausdrücke haben ja nur endlich viele Rechtsfaktoren).

Übersetzer und Interpreter Kommen wir zurück zu unserer ursprünglichen Aufgabe, der Generierung eines Akzeptors. Da die Anzahl aller Rechtsfaktoren endlich ist, kann man das obige Verfahren verwenden, um aus einem regulären Ausdruck ein Programm zu generieren, das testet, ob ein Wort in der von dem Ausdruck bezeichneten Sprache enthalten ist. Mehr noch: Wir können das Verfahren auch automatisieren, sprich wir können ein Mini-F# Programm schreiben, das uns diese Aufgabe abnimmt! Dieses Mini-F# Programm würde als Eingabe einen regulären Ausdruck verarbeiten (in konkreter oder abstrakter Syntax) und als Ausgabe ein Mini-F# Programm, einen Akzeptor für den regulären Ausdruck, erzeugen (in konkreter Syntax). Ein Mini-F# Programm, das ein anderes Mini-F# Programm erzeugt! Ein solches Programm nennt man ***Übersetzer*** (engl. compiler). In diesem Fall würde man genauer von einem ***Scanner-Generator*** sprechen. Einen Scanner-Generator tatsächlich zu programmieren, würde den Umfang dieser Vorlesung sprengen, so dass wir an dieser Stelle keinen Programmcode angeben. (Am Ende des Kapitels haben wir aber durchaus das nötige Know-how, um ein solches



Projekt anzugehen.) Trotzdem wollen wir das Thema noch etwas vertiefen. Der Übersetzer und der generierte Akzeptor sind zwei getrennte Programme, siehe obige Grafik. Der Übersetzer erzeugt ein Programm, das in einem zweiten Schritt ausgeführt wird. Die beiden Programme können alternativ auch enger miteinander verzahnt werden:

Schauen wir uns das Programm in Abbildung 6.5 noch einmal an. Die Struktur der einzelnen Funktionen ist identisch — das ist nicht weiter verwunderlich, wir haben sie ja nach dem gleichen Schema konstruiert. Eine naheliegende Frage ist, ob sich die vier Funktionen nicht zu einer zusammenfassen lassen? Wir könnten die vier Funktionen zum Beispiel durchnummerieren und die Hausnummer zu einem zusätzlichen Parameter machen.

module Grammar-ByteCode

```
accept (k : Nat, input : List ⟨Alphabet⟩) : Bool
```

Diese allgemeine Funktion müssen wir dann noch mit Informationen ausstatten, welcher Wahrheitswert im [ ]-Zweig zurückgegeben wird und welche Hausnummer als nächstes an der Reihe ist, wenn ein a bzw. ein b gesehen wird. Kurzum: Wir müssen die rekursive Aufrufstruktur des Programms aus Abbildung 6.5 in einer Datenstruktur ablegen — eine *Kontrollstruktur* wird zu einer *Datenstruktur*. Wie kann die Datenstruktur aussehen? Für den [ ]-Zweig müssen wir jeder Hausnummer einen Wahrheitswert zuordnen; im »::«-Zweig müssen wir in Abhängigkeit von dem gelesenen Zeichen und der aktuellen Hausnummer eine neue Hausnummer ermitteln. Beide Zuordnungen können wir durch Arrays beschreiben, ein 1-dimensionales für den [ ]-Zweig und ein 2-dimensionales für den »::«-Zweig.

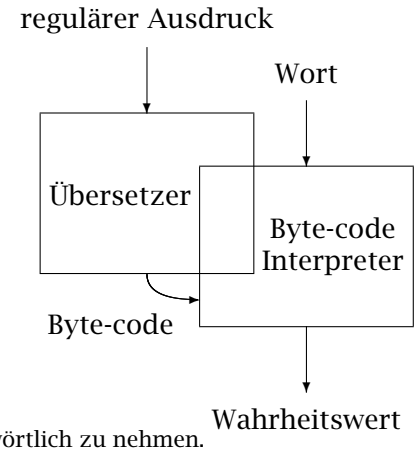
```
type Control = { nullable : Array ⟨Bool⟩;
                 next     : Array ⟨Array ⟨Nat⟩⟩ }
```

Das 2-dimensionale Array wird durch ein geschachteltes Array realisiert. Ein technisches Detail ist noch zu beachten: Arrays werden mit ganzen Zahlen indiziert; wir wollen das *next* Array aber mit einem Element des Alphabets indizieren. Hier kommt die Funktion *ord-Alphabet* ins Spiel, die jedem Zeichen eine ganze Zahl zuordnet. Für unser laufendes Beispiel erhalten wir die folgenden Daten — die Funktionen aus Abbildung 6.5 haben wir fortlaufend von oben nach unten beginnend mit 0 durchnummeriert.

```
let control-r00 = { nullable = [| false; true; false; true |];
                    next     = [| [| 0; 0; 1; 1 |];       (* A *)
                                  [| 2; 2; 3; 3 |] |] }   (* B *)
```

Das vollständige Programm ist in Abbildung 6.6 dargestellt. Der erste Teil ist unabhängig von einem konkreten regulären Ausdruck; der zweite Teil instantiiert das allgemeine Programm mit dem für unser laufendes Beispiel spezifischen Daten.

Verschaffen wir uns noch einmal einen Überblick. Der Übersetzer für reguläre Ausdrücke — den wir nicht angegeben haben — würde in diesem Szenario kein Mini-F# Programm erzeugen, sondern ein Element des Typs *Control*, in dem die Kontrollinformation des Akzeptors codiert ist. Der allgemeine Akzeptor *generic-accept* interpretiert dann diese Kontrollinformation, um zu einem gegebenen Wort zu entscheiden, ob es in der Sprache enthalten ist oder nicht. Bei dem allgemeinen Akzeptor handelt es sich somit um einen Interpreter, genauer um einen ***Byte-code Interpreter***. Byte-code deswegen, weil die Rechtsfaktoren durch kleine Zahlen[10] repräsentiert werden und die Funktionen *nullable*



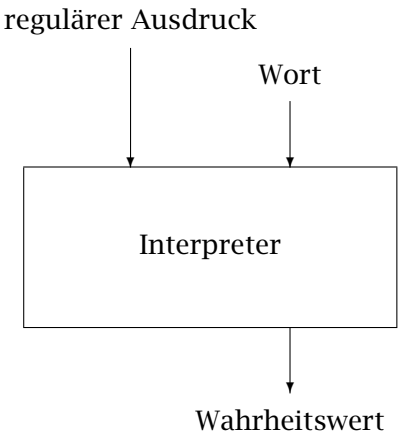
[10] Der Begriff Byte, der für eine Folge von 8 Bits steht, ist hier nicht allzu wörtlich zu nehmen.

```
type Control = { nullable : Array ⟨Bool⟩;
                 next     : Array ⟨Array ⟨Nat⟩⟩ }
let generic-accept (control : Control) : List ⟨Alphabet⟩ → Bool =
  let rec accept (k : Nat, input : List ⟨Alphabet⟩) : Bool =
    match input with
    | [ ]      → control.nullable.[k]
    | a :: rest → accept (control.next.[ord-Alphabet a].[k], rest)
  in fun input → accept (0, input)
(* Beispiele *)
let control-r00 = { nullable = [| false; true; false; true |];
                    next     = [| [| 0;0;1;1 |];      (* A *)
                                  [| 2;2;3;3 |] |] }  (* B *)
let accept-r00 = generic-accept control-r00
```

Abbildung 6.6.: Generischer Akzeptor (Byte-code Interpreter).

und $x \setminus r$ mit Hilfe von *nullable* und *next* codiert werden. Da die beiden Programme, der Übersetzer und der Byte-code Interpreter, über eine Datenstruktur miteinander kommunizieren, können sie in einem Programm zusammengefasst werden, siehe obige Abbildung.

Der Übersetzer generiert Byte-code, den der Byte-code Interpreter abarbeitet. Der Übersetzer hat sozusagen die Aufgabe reguläre Ausdrücke vorzuverdauen. Alternativ können wir einen Akzeptor schreiben, der direkt auf den regulären Ausdrücken arbeitet, sozusagen auf den unverdauten Eingaben. Dann haben wir keinen Byte-code Interpreter mehr vor uns, sondern einen »echten« Interpreter, siehe Abbildung rechts.



Zu diesem Zweck müssen wir reguläre Ausdrücke durch einen Datentyp modellieren und die Funktionen *nullable* und $x \setminus r$ in Mini-F# Programme überführen. Für die erste Aufgabe ziehen wir die abstrakte Syntax regulärer Ausdrücke heran und transliterieren diese in einen rekursiven Variantentyp.

```
type Reg =
  | Sym of Alphabet      einzelnes Zeichen\Terminalsymbol
  | Eps                  das leere Wort
  | Cat of Reg * Reg     Konkatenation\Sequenz
  | Empty                die leere Sprache
  | Alt of Reg * Reg     Alternative
  | Rep of Reg           Wiederholung
```

Der reguläre Ausdruck r_{00} kann jetzt unmittelbar mittels einer Wertebindung definiert werden.

```
let any = Alt (Sym A, Sym B)
let r00 = Cat (Rep any, Cat (Sym B, any))
```

module Grammar.Interpreter

Die Funktion *nullable* lässt sich ebenfalls sehr direkt übertragen: Die sechs Gleichungen werden zu den sechs Zweigen einer Fallunterscheidung.

```
let rec nullable (reg : Reg) : Bool =
  match reg with
  | Eps          → true
  | Sym _        → false
  | Cat (r1, r2) → nullable r1 && nullable r2
  | Empty        → false
  | Alt (r1, r2) → nullable r1 || nullable r2
  | Rep r        → true
```

Ähnlich direkt ist die Umsetzung der mathematischen Funktion $x \setminus r$.

```
let rec divide (x : Alphabet, reg : Reg) : Reg =
  match reg with
  | Eps          → Empty
  | Sym a        → if x = a then Eps else Empty
  | Cat (r1, r2) → if nullable r1
                   then Alt (Cat (divide (x, r1), r2), divide (x, r2))
                   else      Cat (divide (x, r1), r2)
  | Empty        → Empty
  | Alt (r1, r2) → Alt (divide (x, r1), divide (x, r2))
  | Rep r        → Cat (divide (x, r), Rep r)
```

Jetzt können wir uns vom Mini-F# Interpreter ausrechnen lassen, ob r_{00} ε-haltig ist und wie die Rechtsfaktoren von r_{00} aussehen.

```
>>> nullable r00
false
>>> divide (A, r00)
Alt (Cat (Cat (Eps, Rep (Alt (Sym A, Sym B))),
          Cat (Sym B, Alt (Sym A, Sym B))),
     Cat (Empty, Alt (Sym A, Sym B)))
>>> divide (B, r00)
Alt (Cat (Cat (Eps, Rep (Alt (Sym A, Sym B))),
          Cat (Sym B, Alt (Sym A, Sym B))),
     Cat (Eps, Alt (Sym A, Sym B)))
```

Es ist bemerkenswert, dass *divide* (A, r_{00}) einen regulären Ausdruck zurückgibt, der zwar semantisch äquivalent zu r_{00} ist, aber nicht syntaktisch gleich. Das liegt daran, dass bei der Konstruktion des Rechtsfaktors keine algebraischen Vereinfachungen wie etwa $\varepsilon \cdot r = r$ vorgenommen werden. (Bei manuellen Umformungen nehmen wir solche Vereinfachungen fast automatisch vor.) Für die Definition des Akzeptors spielt das aber keine Rolle (warum?).

```
let rec generic-accept (reg : Reg, input : List ⟨Alphabet⟩) : Bool =
  match input with
  | [ ]       → nullable reg
  | a :: rest → generic-accept (divide (a, reg), rest)
```

Hier einige Beispielaufrufe:

```
>>> accept (r00, [A; A; A])
false
>>> accept (r00, [A; B; A])
true
>>> let even-no-of-as = Rep (Alt (Cat (Sym A, Cat (Rep (Sym B), Sym A)), Sym B))
even-no-of-as : Reg
>>> accept (even-no-of-as, [A; B; A])
true
>>> accept (even-no-of-as, [A; B; B])
false
```

In Abbildung 6.7 ist noch einmal der gesamte Mini–F# Code zusammengefasst. Die Funktionen sind etwas allgemeiner als die im Text beschriebenen, da von einem konkreten Alphabet abstrahiert wird. Zudem werden bei der Konstruktion der regulären Ausdrücke einfache algebraische Identitäten ausgenutzt, um die Ausdrücke zu verkleinern. Diese Aufgabe übernehmen die sogenannten ***cleveren Konstruktoren*** *cat* und *alt*.

Fassen wir zusammen: Aus einem regulären Ausdruck lässt sich automatisch ein passender Akzeptor konstruieren. Je nach Verzahnungsgrad kann man mindestens drei Ansätze unterscheiden:

1. reiner Übersetzer,
2. Mischform aus Übersetzer und Interpreter,
3. reiner Interpreter.

Übersetzer und Interpreter sind keineswegs spezifisch für reguläre Ausdrücke, sondern stellen allgemeine Konzepte dar. Im Allgemeinen übersetzt ein Übersetzer ein Wort einer Sprache, der Quellsprache, in ein Wort einer anderen Sprache, der Zielsprache. Ein Interpreter interpretiert ein Wort direkt. In diesem Abschnitt ist die Quellsprache die Sprache der regulären Ausdrücke und die Zielsprache Mini–F# bzw. *Control*. Natürlich kann es sich auch bei der Quellsprache um eine Programmiersprache handeln. Mini–F# zum Beispiel wird von einem Übersetzer in eine Zwischensprache, die wesentlich einfacher als Mini–F# aufgebaut ist, übersetzt. Die Zwischensprache wird dann von einem Interpreter abgearbeitet. Mehr zum Themenkreis Übersetzer und Interpreter erfahren Sie in der Vorlesung Übersetzerbau (siehe auch Abschnitt 4.5).

6.2.2. Scanner

Die Akzeptoren aus dem letzten Abschnitt beantworten die Frage »Ist ein gegebenes Wort in der von einem regulären Ausdruck bezeichneten Sprache enthalten?«. Ein Scanner hingegen unterteilt ein Wort in einzelne Teilwörter, die sogenannten ***Lexeme***. Ausgangspunkt für die Unterteilung ist nicht ein einzelner regulärer Ausdruck, sondern eine Menge regulärer Ausdrücke: $\{r_1, \ldots, r_n\}$. Jeder Ausdruck beschreibt den Aufbau einer Sorte von Lexemen, siehe zum Beispiel Abbildung 6.3. Ein Scanner beantwortet also in konstruktiver Weise die Frage »Ist ein gegebenes Wort in der von $(r_1 \mid \cdots \mid r_n)^*$ bezeichneten Sprache enthalten?«. Die Antwort ist konstruktiv, da eine Aufteilung der Eingabe gleich mitgeliefert wird. Die Aufteilung ist allerdings in der Regel nicht eindeutig; ist zum Beispiel $r_1 = \mathit{digit}^+$ und $r_2 = \mathit{letter}\ (\mathit{letter} \mid \mathit{digit})^*$, dann gibt es für `a11` vier mögliche Aufteilungen: `a|1|1`, `a1|1`, `a|11` und `a11`. Aus diesem Grund vereinbart man zusätzlich, dass jeweils das *längste passende Wort* abgetrennt wird (engl. longest match). In unserem Beispiel wird damit `a11` in genau ein Lexem »unterteilt«. Diese Zusatzvereinbarung macht es etwas mühsam, die Akzeptoren aus dem letzten Abschnitt ohne große Änderungen zu Scannern umzurüsten. Stattdessen

module Grammar.Token

```
type Reg⟨'a⟩ = | Eps
               | Sym of 'a
               | Cat  of Reg⟨'a⟩ * Reg⟨'a⟩
               | Empty
               | Alt  of Reg⟨'a⟩ * Reg⟨'a⟩
               | Rep  of Reg⟨'a⟩

let cat (reg1 : Reg⟨'a⟩, reg2 : Reg⟨'a⟩) : Reg⟨'a⟩ =
  match reg1, reg2 with
  | Eps, r     | r, Eps     → r                 // ε · R = R = R · ε
  | Empty, r | r, Empty → Empty               // ∅ · R = ∅ = R · ∅
  | _                   → Cat (reg1, reg2)

let alt (reg1 : Reg⟨'a⟩, reg2 : Reg⟨'a⟩) : Reg⟨'a⟩ =
  match reg1, reg2 with
  | Empty, r | r, Empty   → r                 // ∅ ∪ R = R = R ∪ ∅
  | _                     → Alt (reg1, reg2)

let rep (reg : Reg⟨'a⟩) =
  match reg with
  | Empty | Eps →    Eps                      // ∅* = ε = ε*
  | Rep r       →    reg                      // (R*)* = R*
  | _           →    Rep reg

let rec nullable = function
  | Eps          → true
  | Sym _        → false
  | Cat (r1, r2) → nullable r1 && nullable r2
  | Empty        → false
  | Alt (r1, r2) → nullable r1 || nullable r2
  | Rep r        → true

let rec divide (x : 'a, reg : Reg⟨'a⟩) : Reg⟨'a⟩ =
  match reg with
  | Eps          → Empty
  | Sym a        → if x = a then Eps else Empty
  | Cat (r1, r2) → if nullable r1 then alt (cat (divide (x, r1), r2), divide (x, r2))
                                  else cat (divide (x, r1), r2)
  | Empty        → Empty
  | Alt (r1, r2) → alt (divide (x, r1), divide (x, r2))
  | Rep r        → cat (divide (x, r), reg)

let rec generic-accept (reg : Reg⟨'a⟩, input : List⟨'a⟩) : Bool =
  match input with
  | [ ]       → nullable reg
  | a :: rest → generic-accept (divide (a, reg), rest)

(* Beispiele *)
let any = Alt (Sym A, Sym B)
let r00 = Cat (Rep any, Cat (Sym B, any))
let accept-r00 = fun input → generic-accept (r00, input)
```

Abbildung 6.7.: Generischer Akzeptor (Interpreter).

schauen wir uns an, wie man für einfach gestrickte lexikalische Syntaxen einen Scanner von Hand programmiert.

Wir nehmen an, dass die Eingabe als Liste von Eingabezeichen gegeben ist. Die Eingabe `(4+7)*11` zum Beispiel wird durch die Liste

```
⋙ explode "(4+7)*11"
['(';'4';'+';'7';')';'*';'1';'1']
```

repräsentiert. (Die Funktion *explode* überführt eine Zeichenkette in eine Liste von Zeichen; umgekehrt wird eine solche Liste von *implode* in eine Zeichenkette überführt.) Wir stellen uns die Aufgabe, einen Scanner für die lexikalische Syntax einfacher arithmetischer Ausdrücke zu schreiben: $\{digit^+, (,), *, +, space\}$ ist die zugrundeliegende Menge regulärer Ausdrücke. Dabei steht *space* für einen beliebigen Zwischenraum (engl. white space), etwa ein Leerzeichen oder einen Zeilenvorschub. Als Ausgabe soll eine Liste von Lexemen erzeugt werden. Lexeme werden mit Hilfe des Variantentyps

```
type Token = | Num of Nat | LParen | RParen | Asterisk | Plus
```

repräsentiert. Die offene Klammer `(` wird zum Beispiel durch den Konstruktor *LParen* dargestellt; das Numeral `4711` durch den Wert *Num* 4711. Das Lexem (engl. token) für Numerale führt sozusagen seinen semantischen Wert mit. Zwischenräume werden in der Ausgabe nicht aufgeführt. Die Eingabe `(4+7)*11` sollte vom Scanner in die Liste

```
[LParen; Num 4; Plus; Num 7; RParen; Asterisk; Num 11]
```

überführt werden.

Die lexikalische Syntax ist besonders einfach, da das erste Zeichen der Eingabe das Lexem eindeutig bestimmt — im Gegensatz zu Mini-F#: `l` kann das erste Zeichen des Schlüsselworts `let` sein oder das erste Zeichen eines Bezeichners. Aus diesem Grund führt das Struktur Entwurfsmuster für Listen fast direkt zum Ziel, siehe Abbildung 6.8. Die einzige »Schwierigkeit« bereiten

```
type Token = | Num of Nat | LParen | RParen | Asterisk | Plus
let rec lex (list : List⟨Char⟩) : List⟨Token⟩ =
  match list with
  | [] → []
  | c :: rest → if c = '(' then LParen :: lex rest
                elif c = ')' then RParen :: lex rest
                elif c = '*' then Asterisk :: lex rest
                elif c = '+' then Plus :: lex rest
                elif Char.IsDigit c then
                  let (xs1, xs2) = split-while Char.IsDigit list
                  in Num (Nat.Parse (implode xs1)) :: lex xs2
                elif Char.IsWhiteSpace c then lex rest
                else panic "illegal character"
```

Abbildung 6.8.: Handgeschriebener Scanner für einfache arithmetische Ausdrücke.

Numerale. Wir müssen die Liste weiterverfolgen, solange wir Ziffern sehen. Diese Aufgabe übernimmt eine nützliche Hilfsfunktion namens *split-while*: Der Aufruf *split-while pred list* teilt *list*

in zwei Listen *list1* und *list2* auf; für alle Elemente *x* in *list1* gilt, dass *pred x* zu *true* auswertet; weiterhin ist *list1* das längste Anfangsstück mit dieser Eigenschaft.

```
⋙ split-while (fun n → n % 2 = 0) (0 :: [2 .. 5])
([0;2],[3;4;5])
⋙ split-while Char.IsDigit (explode "24me")
(['2';'4'],['m';'e'])
⋙ split-while Char.IsWhiteSpace (explode "24me")
([],['2';'4';'m';'e'])
```

Die Bibliotheksfunktion *Char.IsDigit* testet, ob das Argument eine Ziffer ist; entsprechend überprüft *Char.IsWhiteSpace*, ob das Argument ein Zwischenraum ist. Die Definition von *split-while* folgt exakt dem Struktur Entwurfsmuster.

```
let rec split-while (pred : 'a → Bool) = function
  | []      → ([],[])
  | x :: xs → if pred x then let (xs1, xs2) = split-while pred xs in (x :: xs1, xs2)
                        else ([], x :: xs)
```

Bleibt noch zu klären, was *Nat.Parse* und *panic* bedeuten: Die Funktion *Nat.Parse* wird benutzt, um einen Ziffernfolge in eine natürliche Zahl umzuwandeln: Der Aufruf *Nat.Parse* `"4711"` zum Beispiel ergibt 4711. Die Funktion *panic* schließlich bricht eine Rechnung mit einer Fehlermeldung ab (dazu später mehr in Abschnitt 7.4).

Übungen.

1. Zeigen Sie (6.8) durch natürliche Induktion über die Länge der Eingabe.

2. Schreiben Sie Akzeptoren für die folgenden regulären Ausdrücke:
   (a) $(a^* \mid b^*)^*$,
   (b) $a^*\,(\varepsilon \mid b)\,(a\,a^*\,b)^*\,a^*$,
   (c) $(b \mid ab)^*\,a^*$.

6.3. Projekt: Automaten\Rechnen mit Syntaxdiagrammen⋆

In Abschnitt 6.1.1 haben wir reguläre Ausdrücke mit Hilfe von Syntaxdiagrammen bzw. Eisenbahndiagrammen visualisiert. Damit haben wir Syntaxdiagramme tatsächlich etwas unter Wert verkauft — sie können so einiges mehr:

- Wir können Syntaxdiagramme direkt verwenden, um Sprachen zu beschreiben, sie sind *visuelle Sprachbeschreibungssprachen* (»Generatorbrille«: Abschnitte 6.3.1–6.3.2).
- Aus Syntaxdiagrammen lassen sich systematisch Algorithmen ableiten, um das *Wortproblem* für reguläre Sprachen zu lösen (»Akzeptorbrille«: Abschnitte 6.3.3–6.3.6).

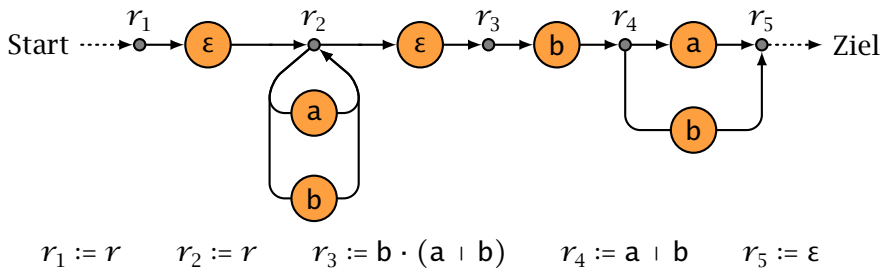
Bei unserem Ausflug in die ***Automatentheorie*** kommt die Algorithmik nicht zu kurz: Wir lernen eine weitere wichtige Datenstruktur kennen, ***Graphen***, und beschäftigen uns mit verschiedenen Graphalgorithmen. Auch die Mathematik kommt auf ihre Kosten: Wir zeigen, dass man mit Syntaxdiagrammen selbst rechnen kann und lernen dabei die zentrale Algebra der Informatik besser kennen: ***Kleene Algebra***. (Wenn Sie Abschnitt 5.5 gelesen haben, werden Ihnen viele Dinge vertraut vorkommen.) Ach ja, fast nebenbei holen wir noch einen Beweis nach und zeigen, dass eine Sprache genau dann regulär ist, wenn sie endlich viele Rechtsfaktoren besitzt.

Es sei noch einmal daran erinnert, dass wir die Notation überladen: Sei $\mathbb{A}$ ein Alphabet. Der griechische Buchstabe ε steht sowohl für das leere Wort, $\varepsilon \in \mathbb{A}^*$, als auch für die Sprache, die nur das leere Wort enthält, $\varepsilon \in \mathcal{P}(\mathbb{A}^*)$. Ebenso steht $a \in \mathbb{A}$ sowohl für ein einzelnes Zeichen, als auch für das Wort, das nur aus diesem Zeichen besteht, $a \in \mathbb{A}^*$, als auch für die Sprache, die nur ebendieses Wort enthält, $a \in \mathcal{P}(\mathbb{A}^*)$. Eine weitere Vereinbarung ist nützlich: Elemente des »erweiterten« Alphabets $\mathbb{A}_\varepsilon = \mathbb{A} \cup \{\varepsilon\}$ nennen wir ***Grundsymbole*** (engl. basic symbols).

6.3.1. Syntaxdiagramme, da capo⋆

Wir können Syntaxdiagramme auch direkt verwenden, um Sprachen zu beschreiben, ohne den »Umweg« über reguläre Ausdrücke zu beschreiten — wir werden sehen, dass Diagramme die Sprachbeschreibung manchmal substantiell vereinfachen.

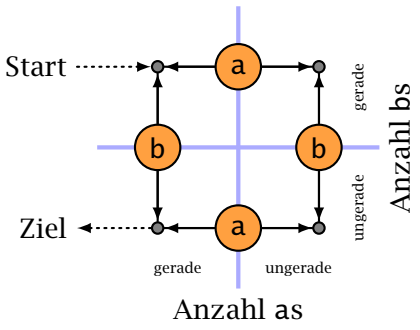
Wenn wir Diagramme zum Gegenstand unserer Untersuchungen machen, müssen wir wie immer die äußere Form (Syntax) und die Bedeutung (Semantik) präzise festlegen. Dazu machen wir zunächst Kreuzungs- bzw. Verbindungspunkte zwischen »Bahnhöfen« explizit. Angereichert um Verbindungspunkte sieht zum Beispiel das Syntaxdiagramm für den regulären Ausdruck $(\mathsf{a} \mid \mathsf{b})^* \cdot \mathsf{b} \cdot (\mathsf{a} \mid \mathsf{b})$ aus Abschnitt 6.1.1 wie folgt aus.



(6.9)

Jeder der sieben Bahnhöfe ⬤ liegt zwischen zwei Punkten ●. Die regulären Ausdrücke $r_1, \ldots, r_5$ spezifizieren die *generierten Sprachen*: Welche Sprache wird ab der jeweiligen Position bis zum Zielpunkt erzeugt? Zum Beispiel: Ausgehend von r_3 bis zum designierten Zielpunkt r_5 wird die Sprache $[\![r_3]\!] = \{\mathsf{ba}, \mathsf{bb}\}$ erzeugt. Das gesamte Diagramm generiert wie gewünscht die *advPieb-Sprache*, die Menge aller Wörter, die an der vorletzten Position ein b enthalten.

Das folgende Beispiel illustriert die Verwendung von Syntaxdiagrammen als »Beschreibungswerkzeug«. In Abschnitt 6.1.3 haben wir uns abgemüht, einen regulären Ausdruck für die Sprache aller Wörter zu finden, die eine gerade Anzahl von as *und* eine ungerade Anzahl von bs enthalten. Diese Sprache lässt sich einfach und elegant mit dem unten dargestellten Syntaxdiagramm beschreiben (die bidirektionalen Verbindungen dienen als Abkürzungen für jeweils zwei unidirektionale Verbindungen).



Wir unterscheiden vier Sprachen, je nachdem, ob die Gesamtzahl der as bzw. bs gerade oder ungerade ist: die gesuchte ***gu-Sprache***, die gg-, die ug- und die uu-Sprache. Ein einzelnes Zeichen dreht die entsprechende Parität von gerade auf ungerade oder umgekehrt.

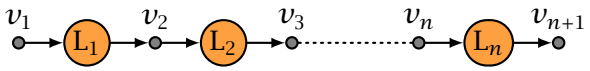
Syntax von Eisenbahndiagrammen Wenn Sie Abschnitt 5.5 studiert haben, werden Ihnen die Diagramme bekannt vorkommen. Mathematisch gesehen entspricht ein Syntaxdiagramm einem ***gerichteten Graphen*** mit ***Kantenmarkierungen*** (oder etwas weniger neutral formuliert: einem gerichteten, *gewichteten* Graphen).

Knoten a mit x beschriftete Kante zwischen a und z

Die Verbindungspunkte eines Syntaxdiagramms werden durch Knoten modelliert und die Bahnhöfe durch Kantenmarkierungen. Die Knoten a und z heißen ***Endknoten*** der Kante.

Semantik von Eisenbahndiagrammen In den bisher betrachteten Beispielen sind die Kantenmarkierungen reguläre Ausdrücke. Im Folgenden nehmen wir an, dass die Kanten mit Sprachen markiert sind — wir wechseln von der Syntax zur Semantik. Der Übergang ist besonders einfach, wenn die Markierungen Grundsymbole sind, wie in den allermeisten Beispielen.

Eine Folge von Knoten, in der aufeinander folgende Knoten durch eine Kante verbunden sind, bezeichnet man als ***Pfad***.



In der Eisenbahnmetapher entspricht ein Pfad einer Zugfahrt. Sind die Kanten mit den Sprachen $L_1, \ldots, L_n$ markiert, dann generiert die Zugfahrt die Sprache $L_1 \cdot \cdots \cdot L_n$, die Konkatenation aller Kantenmarkierungen. Die von einem Diagramm generierte Sprache ergibt sich dann als Vereinigung aller Pfade vom Start- bis zum Zielknoten.

Ein Graph wird durch zwei Angaben festgelegt: durch die Menge V seiner Knoten (engl. vertices) und durch eine Abbildung $M : V \times V \to \mathscr{P}(\mathbb{A}^*)$, die jeder Kante (engl. edge) ihre Markierung aus $\mathscr{P}(\mathbb{A}^*)$ zuordnet. Wir haben in Abschnitt 5.5 erörtert, dass sich ein Graph bequem als quadratische Matrix aufschreiben lässt. Dabei entspricht der Funktionswert $M(i,j)$ dem Eintrag in Zeile i und Spalte j, in Matrixnotation M_{ij}. (Im Folgenden verwenden wir die Begriffe »Graph« und »Matrix« weitestgehend synonym — je nachdem, welche Perspektive wir betonen wollen.) Für unser laufendes Beispiel, die advPieb-Sprache (6.9), erhalten wir:

$$M := \begin{array}{c} \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \end{array} \begin{array}{c} \begin{array}{ccccc} r_1 & r_2 & r_3 & r_4 & r_5 \end{array} \\ \begin{pmatrix} \varnothing & \varepsilon & \varnothing & \varnothing & \varnothing \\ \varnothing & \{\mathsf{a},\mathsf{b}\} & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing & \{\mathsf{b}\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \{\mathsf{a},\mathsf{b}\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix} \end{array}$$

Die Matrix M nennt man auch ***Adjazenzmatrix***, da sie uns verrät, ob zwei Knoten benachbart sind (lat. adiacēns). Im Syntaxdiagramm gibt es zwei gerichtete Kanten von r_4 nach r_5; eine ist mit a markiert, die andere mit b; der Eintrag in der Matrix, $\{\mathsf{a},\mathsf{b}\}$, repräsentiert die Vereinigung der Kantenmarkierungen. Existiert in der graphischen Darstellung keine Kante, zum Beispiel von r_5 nach r_4, so ist der Eintrag die leere Sprache. (Erinnern Sie sich an Abschnitt 5.5.1? Dort wir hier setzen wir voraus, dass die Gewichte bzw. Markierungen die Struktur eines Halbverbandes besitzen.)

In einem Syntaxdiagramm kommt zwei Knoten eine besondere Bedeutung zu: dem ***Startknoten***, dem Eingang in das Syntaxdiagramm, und dem ***Zielknoten***, dem Ausgang. Den Startknoten

merken wir uns in einem Zeilenvektor, den Zielknoten in einem Spaltenvektor, so dass das Syntaxdiagramm für $(\mathsf{a} \mid \mathsf{b})^* \cdot \mathsf{b} \cdot (\mathsf{a} \mid \mathsf{b})$ insgesamt durch drei Angaben festgelegt wird:

$$S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix} \qquad M := \begin{pmatrix} \varnothing & \varepsilon & \varnothing & \varnothing & \varnothing \\ \varnothing & \{\mathsf{a},\mathsf{b}\} & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing & \{\mathsf{b}\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \{\mathsf{a},\mathsf{b}\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix} \qquad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix}$$

In der Regel gibt es genau einen Start- und genau einen Zielknoten. Es spricht aber nichts dagegen, mehrere Start- und mehrere Zielknoten zuzulassen. Im Allgemeinen sind der Startvektor und der Zielvektor ∅-ε-Vektoren: Jeder Eintrag ist entweder ∅ oder ε.

Die Matrixdarstellung ist aus zwei Gründen attraktiv. Zum einen erlaubt sie es uns, irrelevante Details unter den Teppich zu kehren: Wir werden sehen, dass die Natur der Knoten keine große Rolle spielt — in der obigen Darstellung treten die Knoten r_1, …, r_5 bereits nicht mehr explizit in Erscheinung. Zum anderen können wir die Semantik eines Syntaxdiagramms präzise durch Matrixoperationen beschreiben: Das Matrixprodukt aus dem Startvektor S, der ***reflexiven, transitiven Hülle*** der Adjazenzmatrix M und dem Zielvektor F

$$S \cdot M^* \cdot F$$

ist die durch das Syntaxdiagramm *generierte Sprache*. Das Ergebnis ist eine 1×1-Matrix, die wir mit dem Skalar identifizieren. Wir werden sehen, dass auf diese Weise einem Syntaxdiagramm eine reguläre Sprache zugeordnet wird — sofern alle Kantenmarkierungen selbst reguläre Sprachen sind.

Die reflexive, transitive Hülle eines Graphen haben wir in Abschnitt 5.5.2 im Zusammenhang mit Optimierungsproblemen eingeführt. Der folgende Paragraph frischt unser Gedächtnis auf.

Reflexive, transitive Hülle In Abschnitt 6.1.2 haben wir die Wiederholung L^* der Sprache L als Vereinigung aller endlichen Potenzen definiert. Ganz entsprechend gehen wir im Fall der reflexiven, transitiven Hülle eines Graphen vor. Ist A eine quadratische Matrix, dann können wir Potenzen von A bilden:

$$A^0 := \mathbf{1} \qquad\qquad A \cdot A^n =: A^{n+1} := A^n \cdot A$$

Die ***reflexive, transitive Hülle*** von A ist die Vereinigung aller endlichen Potenzen:

$$A^* := \bigsqcup \{ A^n \mid n \in \mathbb{N} \} \tag{6.10}$$

Identifizieren wir Kanten und Pfade mit ihren Markierungen, dann entspricht eine *Kante* in A^n einem *Pfad* der Länge n in A und eine *Kante* in der Hülle A^* einem *Pfad* beliebiger Länge in A. Der Begriff »Hülle« ist durch die folgenden Eigenschaften motiviert, die wir schon von Sprachen kennen.

$$\mathbf{1} \sqsubseteq M^* \qquad M^* \cdot M^* \sqsubseteq M^* \qquad M \sqsubseteq M^* \qquad (M^*)^* \sqsubseteq M^* \tag{6.11}$$

Die Ungleichungen lassen sich anschaulich als Eigenschaften von Pfaden deuten:

- ***Reflexivität***: $\mathbf{1} \sqsubseteq M^*$, der leere Pfad ist ein Pfad;
- ***Transitivität***: $M^* \cdot M^* \sqsubseteq M^*$, die Konkatenation zweier Pfade ist ein Pfad;
- ***Extensivität***: $M \sqsubseteq M^*$, eine Kante ist ein Pfad;

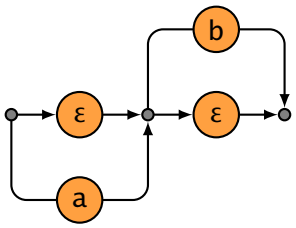
- ***Idempotenz***: $(M^*)^* \sqsubseteq M^*$, ein Pfad von Pfaden ist ein Pfad.

Die letzten beiden Gesetze charakterisieren einen ***Hüllenoperator***: Die Hülle enthält die ursprüngliche Menge (***Extensivität***), wird die Hülle ein zweites Mal gebildet, so bleibt die Menge unverändert (***Idempotenz***). Die ersten beiden Gesetze spezifizieren die Art der Hülle: Der resultierende Graph ist ***reflexiv*** (er enthält Kanten von i nach i) und ***transitiv*** (gibt es Kanten von i nach j und von j nach k, dann auch von i nach k).

Mit der *Berechnung* der reflexiven, transitiven Hülle eines Graphen haben wir uns ebenfalls in Abschnitt 5.5.2 beschäftigt. Abbildungen 6.9 und 6.10 fassen die Ergebnisse zusammen; dabei verdient Conways Formel (6.12) in Abbildung 6.10 besondere Beachtung.

Bevor wir uns der Programmierung zuwenden und zeigen, wie man ein Syntaxdiagramm mechanisch in einen regulären Ausdruck überführen kann, rechnen wir die Semantik einiger Diagramme beispielhaft (und mühsam) von Hand aus.

Beispiele Fangen wir einfach an: mit einem Syntaxdiagramm, das nur endliche Sprachen generiert. Das Diagramm für $(\varepsilon \mid \mathsf{a}) \cdot (\varepsilon \mid \mathsf{b})$ auf der linken Seite wird durch die Matrizen auf der rechten Seite eingefangen.



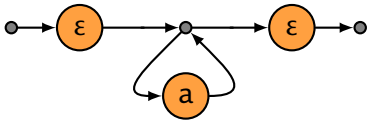
$$S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \quad M := \begin{pmatrix} \varnothing & \{\varepsilon, \mathsf{a}\} & \varnothing \\ \varnothing & \varnothing & \{\varepsilon, \mathsf{b}\} \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \quad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix}$$

Zugfahrten in M umfassen maximal zwei Streckensegmente: $M^n = \varnothing$ für $n > 2$. Daraus folgt, dass die Hülle von A nur endliche Sprachen enthält:

$$M^* = M^0 \sqcup M^1 \sqcup M^2 = \begin{pmatrix} \varepsilon & \varnothing & \varnothing \\ \varnothing & \varepsilon & \varnothing \\ \varnothing & \varnothing & \varepsilon \end{pmatrix} \sqcup \begin{pmatrix} \varnothing & \{\varepsilon, \mathsf{a}\} & \varnothing \\ \varnothing & \varnothing & \{\varepsilon, \mathsf{b}\} \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \sqcup \begin{pmatrix} \varnothing & \varnothing & \{\varepsilon, \mathsf{a}, \mathsf{b}, \mathsf{ab}\} \\ \varnothing & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing \end{pmatrix}$$
$$= \begin{pmatrix} \varepsilon & \{\varepsilon, \mathsf{a}\} & \{\varepsilon, \mathsf{a}, \mathsf{b}, \mathsf{ab}\} \\ \varnothing & \varepsilon & \{\varepsilon, \mathsf{b}\} \\ \varnothing & \varnothing & \varepsilon \end{pmatrix}$$

Das Syntaxdiagramm generiert somit die Sprache $S \cdot M^* \cdot F = \{\varepsilon, \mathsf{a}, \mathsf{b}, \mathsf{ab}\}$ — die Vektoren S und F selektieren die rechte, obere Ecke der Matrix M^*. Der reguläre Ausdruck $(\varepsilon \mid \mathsf{a}) \cdot (\varepsilon \mid \mathsf{b})$ erzeugt alle Teilmengen des Alphabets $\{\mathsf{a}, \mathsf{b}\}$ als »geordnete« Strings (a kommt vor b), so dass wir die generierte Sprache auf den Namen ***Potenzsprache*** taufen.

Damit eine der generierten Sprachen unendlich ist, muss das Syntaxdiagramm wie im folgenden Minimalbeispiel, dem Diagramm für a^*, mindestens eine Schleife enthalten.



$$S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \quad M := \begin{pmatrix} \varnothing & \varepsilon & \varnothing \\ \varnothing & \{\mathsf{a}\} & \varepsilon \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \quad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix} \tag{6.14}$$

Zugfahrten können hier beliebig lang sein, da an der mittleren Station eine Rundreise ins Programm genommen werden kann. Jetzt kommt Conways Formel zum Einsatz, siehe Abbildung 6.10. Dazu teilen wir die 3×3-Matrix M wie folgt auf.

$$M = \begin{pmatrix} \varnothing & \varepsilon & \varnothing \\ \varnothing & \{\mathsf{a}\} & \varepsilon \\ \varnothing & \varnothing & \varnothing \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} \varnothing & \varepsilon \\ \varnothing & \{\mathsf{a}\} \end{pmatrix} & \begin{pmatrix} \varnothing \\ \varepsilon \end{pmatrix} \\ \begin{pmatrix} \varnothing & \varnothing \end{pmatrix} & \begin{pmatrix} \varnothing \end{pmatrix} \end{pmatrix} =: \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

Eine Matrix repräsentiert eine Abbildung des Typs $M : I \times J \to \mathbb{K}$, wobei I und J endliche Indexmengen sind. Dabei entspricht M_{ij} dem Eintrag in Zeile i und Spalte j.

Ist $(\mathbb{K}, \bot, \sqcup, 1, \cdot, (\text{-})^*)$ eine Kleene Algebra, dann bilden die quadratischen Matrizen $V \times V \to \mathbb{K}$ mit $\mathbf{0}$, $\sqcup$, $\mathbf{1}$, $\cdot$ und $(\text{-})^*$ ebenfalls eine Kleene Algebra.

Die Vereinigung und die Multiplikation von Matrizen sowie die neutralen Elemente beider Operationen sind wie folgt definiert.

$$\mathbf{0}_{ij} := \bot \qquad \mathbf{1}_{ij} := \begin{cases} 1 & \text{falls } i = j \\ \bot & \text{sonst} \end{cases}$$

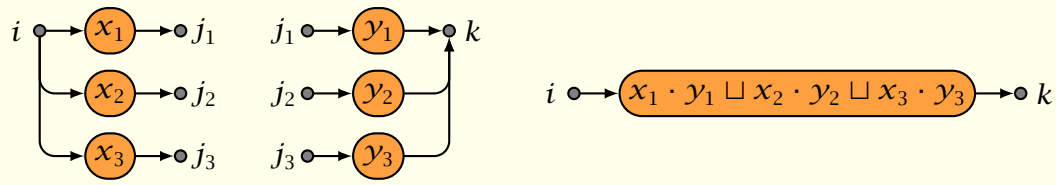
$$(A \sqcup B)_{ij} := A_{ij} \sqcup B_{ij} \qquad (A \cdot B)_{ik} := \bigsqcup_{j \in J} A_{ij} \cdot B_{jk}$$

Die Operationen auf Matrizen (linke Seiten) werden auf die korrespondierenden Operationen der zugrundeliegenden Kleene Algebra $\mathbb{K}$ (rechte Seiten) zurückgeführt.

Die ***Nullmatrix*** $\mathbf{0}$ entspricht einem leeren Graphen — einem Graphen, der zwar Knoten, aber keine Kanten enthält. Zwei Matrizen werden vereinigt, indem die korrespondierenden Einträge vereinigt werden — man sagt auch, die Matrizenvereinigung ist ***komponentenweise*** definiert. Entsprechend sind Matrizen komponentenweise angeordnet:

$$A \sqsubseteq B \quad :\Longleftrightarrow \quad \forall\, i \in I \;.\; \forall\, j \in I \;.\; A_{ij} \sqsubseteq B_{ij}$$

Die ***Diagonalmatrix*** $\mathbf{1}$ enthält nur Schleifen (engl. loops): Von jedem Knoten führt eine mit 1 markierte Kante zu ebendiesem Knoten zurück. Das Matrixprodukt umfasst alle Möglichkeiten, von einem Startknoten zu einem Zielknoten über einen Zwischenstopp zu gelangen. Enthält A eine Kante von i nach j und B eine Kante von j nach k, dann enthält $A \cdot B$ eine Kante von i nach k — der Zwischenstopp j fällt unter den Tisch.



Die Matrixoperationen sind nicht nur für quadratische Matrizen definiert; auch müssen die Endknoten einer Kante nicht notwendigerweise der gleichen Knotenmenge entstammen. Die folgenden »Typregeln« präzisieren die Anforderungen.

$$\frac{}{\mathbf{0} : I \times J \to \mathbb{K}} \qquad \frac{}{\mathbf{1} : I \times I \to \mathbb{K}}$$

$$\frac{A : I \times J \to \mathbb{K} \qquad B : I \times J \to \mathbb{K}}{A \sqcup B : I \times J \to \mathbb{K}} \qquad \frac{A : I \times J \to \mathbb{K} \qquad B : J \times K \to \mathbb{K}}{A \cdot B : I \times K \to \mathbb{K}}$$

Die Matrixvereinigung ist nur für Matrizen der gleichen Dimension definiert; bei der Matrixmultiplikation muss die Anzahl der Spalten der ersten Matrix mit der Anzahl der Zeilen der zweiten Matrix übereinstimmen.

Abbildung 6.9.: Die Kleene Algebra der Matrizen⧹Graphen (1. Teil).

Die reflexive, transitive Hülle kann von quadratischen Matrizen gebildet werden.

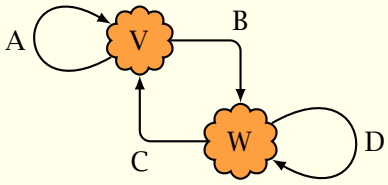
$$\frac{\mathrm{A} : \mathrm{I} \times \mathrm{I} \to \mathbb{K}}{\mathrm{A}^* : \mathrm{I} \times \mathrm{I} \to \mathbb{K}}$$

Erinnern wir uns an ein grundlegendes Prinzip der Algorithmik: Um ein Problem zu lösen, genügt es zu zeigen, dass sich eine Lösung für jede Probleminstanz aus Lösungen kleinerer Probleminstanzen konstruieren lässt. In diesem Sinne wird der Hüllenoperator induktiv über die Größe der Matrix definiert.

Induktionsbasis: Für eine 1×1-Matrix führen wir die Hülle auf den Sternoperator der zugrundeliegenden Kleene Algebra $\mathbb{K}$ zurück: $(a)^* := (a^*)$.

Induktionsschritt: Eine quadratische $(m+n) \times (m+n)$-Matrix mit $m, n > 0$ teilen wir gemäß der Formel $(m+n) \times (m+n) = m \times m + m \times n + n \times m + n \times n$ in zwei quadratische und zwei rechteckige Teilmatrizen auf — eine solche Aufteilung nennt man ***Blockmatrix***.

$$\mathrm{M} =: \begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix} : \begin{pmatrix} m \times m & m \times n \\ n \times m & n \times n \end{pmatrix}$$



Auf diese Weise wird die Knotenmenge des Graphen in zwei Teilmengen, V und W, partitioniert. Die quadratische Teilmatrix A enthält alle Kanten mit Endpunkten aus V; entsprechend umfasst D alle Kanten mit Endpunkten aus W. Die rechteckigen Matrizen enthalten die Transitstrecken: B die Übergänge von V nach W und C in die umgekehrte Richtung von W nach V.

Für eine Zugfahrt von V nach V gibt es zwei Möglichkeiten. Entweder wir fahren ein Segment innerhalb des ersten Teilgraphen oder wir queren in den zweiten Teilgraphen, fahren dort eine beliebige Strecke und kehren dann in den ersten Teilgraphen zurück: $\mathrm{A} \sqcup \mathrm{B} \cdot \mathrm{D}^* \cdot \mathrm{C}$. Das Manöver können wir beliebig oft wiederholen. Diese Überlegungen motivieren das folgende Rechengesetz, ***Conways Formel***.

$$\begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix}^* := \begin{pmatrix} \mathrm{X} & \mathrm{A}^* \cdot \mathrm{B} \cdot \mathrm{Y} \\ \mathrm{D}^* \cdot \mathrm{C} \cdot \mathrm{X} & \mathrm{Y} \end{pmatrix} \quad \text{wobei} \quad \begin{cases} \mathrm{X} := (\mathrm{A} \sqcup \mathrm{B} \cdot \mathrm{D}^* \cdot \mathrm{C})^* \\ \mathrm{Y} := (\mathrm{D} \sqcup \mathrm{C} \cdot \mathrm{A}^* \cdot \mathrm{B})^* \end{cases} \tag{6.12}$$

Wenn wir zwischen V und W nur in eine Richtung reisen können, *entweder* $\mathrm{B} = \mathbf{0}$ *oder* $\mathrm{C} = \mathbf{0}$, dann vereinfacht sich Conways Formel etwas.

$$\begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathbf{0} & \mathrm{D} \end{pmatrix}^* = \begin{pmatrix} \mathrm{A}^* & \mathrm{A}^* \cdot \mathrm{B} \cdot \mathrm{D}^* \\ \mathbf{0} & \mathrm{D}^* \end{pmatrix} \qquad \begin{pmatrix} \mathrm{A} & \mathbf{0} \\ \mathrm{C} & \mathrm{D} \end{pmatrix}^* = \begin{pmatrix} \mathrm{A}^* & \mathbf{0} \\ \mathrm{D}^* \cdot \mathrm{C} \cdot \mathrm{A}^* & \mathrm{D}^* \end{pmatrix} \tag{6.13a}$$

Sind die Teilgraphen nicht verbunden, $\mathrm{B} = \mathbf{0}$ *und* $\mathrm{C} = \mathbf{0}$, so können die Hüllen getrennt voneinander berechnet werden.

$$\begin{pmatrix} \mathrm{A} & \varnothing \\ \varnothing & \mathrm{D} \end{pmatrix}^* = \begin{pmatrix} \mathrm{A}^* & \varnothing \\ \varnothing & \mathrm{D}^* \end{pmatrix} \tag{6.13b}$$

Abbildung 6.10.: Die Kleene Algebra der Matrizen⧹Graphen (2. Teil).

Die Hülle der 2×2-Teilmatrix A berechnen wir »rekursiv« ebenfalls mit Conways Formel. Da ein Eintrag $\varnothing$ ist, kommt eine der vereinfachten Rechenformeln (6.13a) zum Einsatz.

$$A^* = \begin{pmatrix} \varnothing^* & \varnothing^* \cdot \varepsilon \cdot \{a\}^* \\ \varnothing & \{a\}^* \end{pmatrix} = \begin{pmatrix} \varepsilon & \{a\}^* \\ \varnothing & \{a\}^* \end{pmatrix} \qquad A^* \cdot B \cdot D^* = \begin{pmatrix} \{a\}^* \\ \{a\}^* \end{pmatrix} \qquad D^* = \begin{pmatrix} \varepsilon \end{pmatrix}$$

Auch die Berechnung von M^* nutzt eine der vereinfachten Rechenformeln, da $C = \mathbf{0}$ ist.

$$M^* = \begin{pmatrix} A & B \\ C & D \end{pmatrix}^* = \begin{pmatrix} A^* & A^* \cdot B \cdot D^* \\ \varnothing & D^* \end{pmatrix} = \left(\begin{pmatrix} \varepsilon & \{a\}^* \\ \varnothing & \{a\}^* \end{pmatrix} \begin{pmatrix} \{a\}^* \\ \{a\}^* \end{pmatrix} \right) = \begin{pmatrix} \varepsilon & \{a\}^* & \{a\}^* \\ \varnothing & \{a\}^* & \{a\}^* \\ \varnothing & \varnothing & \varepsilon \end{pmatrix}$$

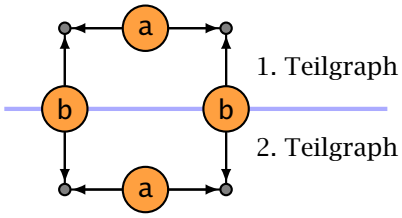
Somit generiert das Syntaxdiagramm die Sprache $S \cdot M^* \cdot F = \{a\}^*$ — wie erwartet.

Für unser laufendes Beispiel, die advPieb-Sprache, erhalten wir die folgende Hülle:

$$M^* = \begin{pmatrix} \varepsilon & \{a,b\}^* & \{a,b\}^* & \{a,b\}^* \cdot \{b\} & \{a,b\}^* \cdot \{b\} \cdot \{a,b\} \\ \varnothing & \{a,b\}^* & \{a,b\}^* & \{a,b\}^* \cdot \{b\} & \{a,b\}^* \cdot \{b\} \cdot \{a,b\} \\ \varnothing & \varnothing & \varepsilon & \{b\} & \{b\} \cdot \{a,b\} \\ \varnothing & \varnothing & \varnothing & \varepsilon & \{a,b\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varepsilon \end{pmatrix}$$

Die Rechnungen sind hier etwas mühsamer, aber — und das ist der entscheidende Punkt — sie können mechanisch durch stupide Anwendung von Conways Formel durchgeführt werden. In der ersten Zeile finden wir die Sprachen, die vom Startknoten r_1 *bis* zu dem jeweiligen Knoten generiert werden (als Formel $S \cdot M^*$); in der letzten Spalte können wir die Sprachen ablesen, die *von* dem jeweiligen Knoten bis zum Zielknoten r_5 generiert werden (als Formel $M^* \cdot F$). Die Vektoren S und F extrahieren die obere, rechte Ecke (als Formel $S \cdot M^* \cdot F$); die von dem Diagramm generierte Sprache ist somit $\{a,b\}^* \cdot \{b\} \cdot \{a,b\}$.

Bereit für die letzte Herausforderung? In Abschnitt 6.3.1 haben wir die Sprache aller Wörter, die eine gerade Anzahl von as und eine ungerade Anzahl von bs enthalten, elegant mit Hilfe eines Syntaxdiagramms beschrieben.



$$S \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix}^* \cdot F := \begin{pmatrix} \varepsilon & \varnothing & \varnothing & \varnothing \end{pmatrix} \cdot \begin{pmatrix} \varnothing & a & b & \varnothing \\ a & \varnothing & \varnothing & b \\ b & \varnothing & \varnothing & a \\ \varnothing & b & a & \varnothing \end{pmatrix}^* \cdot \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \\ \varnothing \end{pmatrix}$$

Jetzt können wir *mechanisch* einen regulären Ausdruck für diese Sprache herleiten. Die Blockmatrizen unterteilen das Diagramm horizontal entlang der blauen Linie. Die Symmetrie des Diagramms spiegelt sich in der Blockmatrix wider: $A = D$ und $B = C$ (aus Platzgründen lassen wir »·« im Folgenden an einigen Stellen weg).

$$A^* = D^* = \begin{pmatrix} \varnothing & a \\ a & \varnothing \end{pmatrix}^* = \begin{pmatrix} (aa)^* & a(aa)^* \\ a(aa)^* & (aa)^* \end{pmatrix} =: \begin{pmatrix} e & o \\ o & e \end{pmatrix}$$

$$\begin{pmatrix} \varnothing & a \\ a & \varnothing \end{pmatrix} \sqcup \begin{pmatrix} b & \varnothing \\ \varnothing & b \end{pmatrix} \cdot \begin{pmatrix} e & o \\ o & e \end{pmatrix} \cdot \begin{pmatrix} b & \varnothing \\ \varnothing & b \end{pmatrix} = \begin{pmatrix} beb & a \cup bob \\ a \cup bob & beb \end{pmatrix} =: \begin{pmatrix} E & O \\ O & E \end{pmatrix}$$

$$X = Y = \begin{pmatrix} E & O \\ O & E \end{pmatrix}^* = \begin{pmatrix} (E \sqcup OE^*O)^* & E^*O(E \sqcup OE^*O)^* \\ E^*O(E \sqcup OE^*O)^* & (E \sqcup OE^*O)^* \end{pmatrix} =: \begin{pmatrix} L_{gg} & L_{ug} \\ L_{ug} & L_{gg} \end{pmatrix}$$

Die Sprache L_{gg} enthält alle zyklischen Pfade — eine Rundreise besucht notwendigerweise eine gerade Anzahl von as und bs. Die Sprache L_{ug} umfasst alle horizontalen Seitenwechsel (Pfade

innerhalb der Teilgraphen), von links nach rechts oder umgekehrt. Vertikale Seitenwechsel (Pfade zwischen den Teilgraphen) werden durch komplexere Ausdrücke beschrieben:

$$A^* \cdot B \cdot Y^* = D^* \cdot C \cdot X^* = \begin{pmatrix} e & o \\ o & e \end{pmatrix} \cdot \begin{pmatrix} b & \varnothing \\ \varnothing & b \end{pmatrix} \cdot \begin{pmatrix} L_{gg} & L_{ug} \\ L_{ug} & L_{gg} \end{pmatrix} = \begin{pmatrix} eb & ob \\ ob & eb \end{pmatrix} \cdot \begin{pmatrix} L_{gg} & L_{ug} \\ L_{ug} & L_{gg} \end{pmatrix}$$
$$= \begin{pmatrix} e \cdot b \cdot L_{gg} \cup o \cdot b \cdot L_{ug} & e \cdot b \cdot L_{ug} \cup o \cdot b \cdot L_{gg} \\ o \cdot b \cdot L_{gg} \cup e \cdot b \cdot L_{ug} & o \cdot b \cdot L_{ug} \cup e \cdot b \cdot L_{gg} \end{pmatrix} =: \begin{pmatrix} L_{gu} & L_{uu} \\ L_{uu} & L_{gu} \end{pmatrix}$$

Die reflexive, transitive Hülle von M enthält jede der vier Sprachen, L_{gg}, L_{ug}, L_{gu} und L_{uu}, genau viermal, siehe unten. Im Syntaxdiagramm haben wir als Startknoten die linke, obere Ecke gewählt. Die Matrix zeigt, dass der Startknoten tatsächlich frei wählbar ist, solange der Zielknoten auf der jeweils vertikal gegenüberliegenden Seite liegt.

$$M^* = \begin{pmatrix} L_{gg} & L_{ug} & L_{gu} & L_{uu} \\ L_{ug} & L_{gg} & L_{uu} & L_{gu} \\ L_{gu} & L_{uu} & L_{gg} & L_{ug} \\ L_{uu} & L_{gu} & L_{ug} & L_{gg} \end{pmatrix}$$

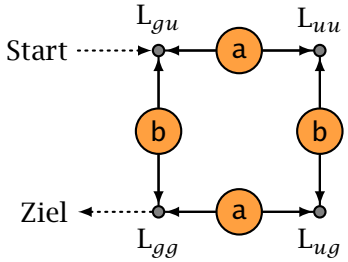
Der gesuchte reguläre Ausdruck ist also L_{gu}. Setzen wir alle verwendeten Abkürzungen ein, erhalten wir einen wahrhaft bombastischen Ausdruck.

$$\begin{aligned} L_{gu} &= e \cdot b \cdot L_{gg} \cup o \cdot b \cdot L_{ug} = eb(g \cup ug^*u)^* \cup obg^*u(g \cup ug^*u)^* \\ &= eb\big((beb) \cup (a \cup bob)(beb)^*(a \cup bob)\big)^* \cup \\ &\quad ob(beb)^*(a \cup bob)\big((beb) \cup (a \cup bob)(beb)^*(a \cup bob)\big)^* \\ &= (aa)^*b\big((b(aa)^*b) \cup (a \cup ba(aa)^*b)(b(aa)^*b)^*(a \cup ba(aa)^*b)\big)^* \cup \\ &\quad a(aa)^*b(b(aa)^*b)^*(a \cup ba(aa)^*b)\big((b(aa)^*b) \cup (a \cup ba(aa)^*b)(b(aa)^*b)^*(a \cup ba(aa)^*b)\big)^* \end{aligned}$$

Die Form des Ausdrucks wird maßgeblich von der Partitionierung des Syntaxdiagramms beeinflusst. Unterteilen wir das obige Diagramm nicht horizontal wie oben, sondern vertikal, ergibt sich ein etwas einfacherer Ausdruck: Wir erhalten im Wesentlichen L_{ug}, nur das a und b vertauscht sind. Während das Diagramm einfach und klar ist, verdient der mechanisch generierte, reguläre Ausdruck die Attribute komplex und verwirrend. Woran liegt das?

To iterate is human;
to recurse, divine.
— L Peter Deutsch (1946)

Kommen wir zum noch einmal zum Ausgangspunkt zurück und beschriften die Knoten des Syntaxdiagramms mit den jeweils generierten Sprachen.




```
let rec gu =     a · uu | b · gg
and     uu =     a · gu | b · ug
and     ug =     a · gg | b · uu
and     gg = ε | a · ug | b · gu    // Ziel
in gu                               // Start
```

Das Syntaxdiagramm ließe sich sehr direkt in einen »regulären Ausdruck« überführen, wenn wir unsere Sprachbeschreibungssprache etwas aufpeppen würden. Wenn wir reguläre Ausdrücke um ***lokale Definitionen*** erweitern, *let* $x = r_1$ *in* r_2, dann entspricht das Diagramm dem Ausdruck auf

der rechten Seite. Da der Graph zyklisch ist, benötigen wir allerdings ***rekursive Definitionen***, sogar verschränkt rekursive Definitionen. Damit lässt sich die obige Frage beantworten: Der aus einem Syntaxdiagramm abgeleitete reguläre Ausdruck ist oft so komplex, da wir *verschränkt rekursive Definitionen auf geschachtelte Iterationen* abbilden! Es ist bemerkenswert, dass dies überhaupt möglich ist. Man sollte nicht überrascht sein, dass die Lesbarkeit leidet, wenn man Definitionen, insbesondere rekursive Definitionen »einsetzt«.

Dieser kurze Exkurs wirft weitere Fragen auf: Man überlegt sich leicht, dass nicht-rekursive Definitionen die Ausdruckskraft regulärer Ausdrücke nicht erhöhen, aber wie sieht es mit *rekursiven* Definitionen aus? Ergeben diese überhaupt immer Sinn? Was wäre die Bedeutung von ***let rec*** x = a · x ***in*** x? Wir lassen die Fragen fürs Erste unbeantwortet im Raum stehen (in Abschnitt 6.4 kommen wir darauf zurück) und wenden uns der Programmierung zu.

Programmierung Zum krönenden Abschluss des Abschnitts zeigen wir, wie sich die Transformation eines Syntaxdiagramms in einen regulären Ausdruck programmieren lässt. Dazu nehmen wir an, dass die Kanten des Syntaxdiagramms mit regulären Ausdrücken markiert sind (im einfachsten Fall mit Grundsymbolen) — wir wechseln also wieder von der Semantik zur Syntax. Überraschenderweise gibt es fast nichts zu tun, da wir den *generischen* Algorithmus aus Abschnitt 5.5.3 zur Berechnung der reflexiven, transitiven Hülle wiederverwenden können! Dabei reift die Erkenntnis, dass der Algorithmus nicht nur Optimierungsprobleme löst.

Dazu müssen wir lediglich reguläre Ausdrücke in eine Kleene Algebra überführen: Die Operationen der Algebra machen quasi nichts, sie setzen einfach reguläre Ausdrücke zusammen (»∪« ist *Alt*, »·« ist *Cat* und $(-)^*$ ist *Rep*). Die Definition in Abbildung 6.11 implementiert eine kleine Verbesserung, indem es statt der Datenkonstruktoren clevere Konstruktoren verwendet, die einfache algebraische Vereinfachungen vornehmen (siehe auch Abschnitt 6.2.1 und Abbildung 6.7). Wir sollten noch anmerken, dass reguläre Ausdrücke nicht die Gesetze einer Kleene Algebra erfüllen: *Alt* (*Empty*, *Sym* `'a'`) ist zum Beispiel nicht gleich *Sym* `'a'`, da es sich um zwei unterschiedliche Syntaxbäume handelt. Allerdings haben die Ausdrücke die gleiche Bedeutung, so dass moralisch gesehen keine Einwände bestehen.

Die folgende Interaktion zeigt den generischen Algorithmus in Aktion.

```
⋙ let a = matrix-algebra regex-algebra 4 : Algebra ⟨Matrix ⟨Reg ⟨Char⟩⟩⟩
⋙ a.star many-as
  Block (Block (Scalar Eps, Scalar (Rep (Sym 'a')), Scalar Empty, Scalar (Rep (Sym 'a'))),
         Block (Scalar (Rep (Sym 'a')), Scalar Empty, Scalar (Rep (Sym 'a')), Scalar Empty),
         Block (Scalar Empty, Scalar Empty, Scalar Empty, Scalar Empty),
         Block (Scalar Eps, Scalar Empty, Scalar Empty, Scalar Eps))
```

Die Bedeutung des einfachsten aller zyklischen Syntaxdiagramme (6.14) ist *Rep* (*Sym* `'a'`) — wie erwartet. Verwenden wir allerdings nicht die cleveren, sondern die normalen Konstruktoren, erhalten wir einen gigantischen Ausdruck bestehend aus insgesamt 702 Konstruktoren!

Zusammenfassung Wenn die Einträge der Matrix M reguläre Sprachen sind, dann sind auch alle Einträge der reflexiven, transitiven Hülle M^* reguläre Sprachen. Insbesondere ist die von einem Syntaxdiagramm generierte Sprache S · M^* · F regulär.

Um diese Sprache zu bestimmen, können wir den gleichen Algorithmus einsetzen, den wir in Abschnitt 5.5.3 eingeführt haben, um Optimierungsprobleme zu lösen. Die Segnungen der Abstraktion: Am Boden sehen die Probleme, Bestimmung der kürzesten Wege und Semantik von Syntaxdiagrammen, sehr verschieden aus. Begibt man sich in die Vogelperspektive, so dass zufällige Details verschwinden und man einen Blick für Strukturen gewinnt, merkt man, dass es sich

```
let cat (reg1 : Reg⟨'a⟩) (reg2 : Reg⟨'a⟩) : Reg⟨'a⟩ =
  match reg1, reg2 with
  | Eps, r     | r, Eps     → r                  // ε · R = R = R · ε
  | Empty, r | r, Empty → Empty                // ∅ · R = ∅ = R · ∅
  | _                    → Cat (reg1, reg2)
let alt (reg1 : Reg⟨'a⟩) (reg2 : Reg⟨'a⟩) : Reg⟨'a⟩ =
  match reg1, reg2 with
  | Empty, r | r, Empty → r                    // ∅ ∪ R = R = R ∪ ∅
  | _                    → Alt (reg1, reg2)
let rep (reg : Reg⟨'a⟩) =
  match reg with
  | Empty | Eps → Eps                          // ∅* = ε = ε*
  | Rep r       → reg                          // (R*)* = R*
  | _           → Rep reg
let regex-algebra : Algebra⟨Reg⟨'a⟩⟩ =
  {
    bot  = Empty
    join = alt
    one  = Eps
    mult = cat
    star = rep
  }
```

```
(* Beispiele *)
let ε = Eps
let a = Sym 'a'
let b = Sym 'b'
let many-as : Matrix⟨Reg⟨Char⟩⟩ =            // a*
  Block (block (Empty, ε, Empty, a),
         block (Empty, Empty, ε, Empty),
         block (Empty, Empty, Empty, Empty),
         block (Empty, Empty, Empty, Empty))
let even-odd : Matrix⟨Reg⟨Char⟩⟩ =           // gerade Anzahl von as und eine
  let A = block (Empty, a, a, Empty)         // ungerade Anzahl von bs
  let B = block (b, Empty, Empty, b)
  Block (A, B, B, A)
```

Abbildung 6.11.: Die »Kleene Algebra« der regulären Ausdrücke.

um das gleiche Problem handelt. Die Berechnung von Weglängen und die Berechnung von regulären Sprachen folgen den gleichen Gesetzen, denen der Kleene Algebra. Mehr noch, auch Graphen selbst formen eine Kleene Algebra mit der reflexiven, transitiven Hülle als »Sternoperator«. Die folgende Tabelle stellt die Kleene Algebren der Sprachen und Matrizen↘Graphen gegenüber.

Kleene Algebra $(\mathbb{K}, \sqsubseteq)$	$\bot$	$a \sqcup b$	1	$a \cdot b$	a^*
Sprachen $(\mathscr{P}(\mathbb{A}^*), \subseteq)$	$\varnothing$ leere Sprache	$R \cup S$ Vereinigung von Sprachen	$\{\varepsilon\}$ »leeres Wort«	$R \cdot S$ Konkatenation von Sprachen	R^* Wiederholung
quadratische Matrizen $(V \times V \to \mathbb{K}, \sqsubseteq)$	$\mathbf{0}$ Null-matrix	$A \sqcup B$ Matrix-vereinigung	$\mathbf{1}$ Diagonal-matrix	$A \cdot B$ Matrix-multiplikation	A^* reflexive, transitive Hülle

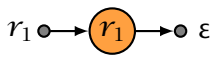
Übungen.

1. Setzen Sie die Begriffe »Syntaxdiagramm«, »Eisenbahndiagramm«, »gerichteter, gewichteter Graph« und »Matrix« zueinander in Beziehung.

6.3.2. Konstruktion von Syntaxdiagrammen⋆

Im letzten Abschnitt haben wir gesehen, dass ein Syntaxdiagramm in einen regulären Ausdruck überführt werden kann. In diesem Abschnitt zeigen wir, wie umgekehrt aus einem regulären Ausdruck ein Syntaxdiagramm entsteht. Wir haben die grundlegende Idee bereits in Abschnitt 6.1.1 kennengelernt — im Folgenden präzisieren wir das Verfahren und kümmern uns insbesondere um seine Korrektheit. (Das gibt uns ein gutes Gefühl, wenn wir im nächsten Abschnitt, aus einem Syntaxdiagramm systematisch Akzeptoren ableiten.)

Lassen wir noch einmal die in Abbildung 6.2 dargestellte Konstruktion von Syntaxdiagrammen Revue passieren. Nehmen wir an, wir wollen den regulären Ausdruck r_1 visualisieren. Ausgangspunkt der Konstruktion ist das Syntaxdiagramm, dessen einzige Kante mit r_1 markiert ist; r_1 ist ebenfalls der Startknoten; der Zielknoten ist ε.



Ausgehend von diesem Diagramm werden die Transformationen solange angewendet, bis nur noch mit Grundsymbolen markierte Kanten übrig sind. Dabei wird in jedem Schritt eine Kante durch ein kleines Diagramm ersetzt. In Abbildung 6.2 fehlen noch die Verbindungspunkte — diese sind in Abbildung 6.12 ergänzt. Sowohl die Knoten als auch die Markierungen der Graphen sind reguläre Ausdrücke. Die Knoten spezifizieren, welche Sprache ab der jeweiligen Position bis zum designierten Zielknoten ε generiert wird. Führen wir die Konstruktion für den regulären Ausdruck $(\mathtt{a} \mid \mathtt{b})^* \cdot \mathtt{b} \cdot (\mathtt{a} \mid \mathtt{b})$ durch, erhalten wir das Diagramm für die advPieb-Sprache (6.9). Das Konstruktionsverfahren ist übrigens nach dem »Erfinder«, dem israelischen Informatiker Zohar Manna (1939–2018), benannt [Man74].

Analyse Abbildung 6.12 beschreibt einen Algorithmus — nicht wie gewohnt mittels Prosa, Pseudocode oder einem Programm, sondern mit Hilfe von Grafiken, die Graphtransformationen illustrieren. Dessen ungeachtet wollen wir kurz die Eigenschaften des Verfahrens beleuchten. Zunächst einmal ist der Algorithmus *kompositional*; er folgt der Struktur regulärer Ausdrücke. Entsprechend gibt es drei Basisfälle (für Grundsymbole ist nichts zu tun; eine mit der leeren Sprache

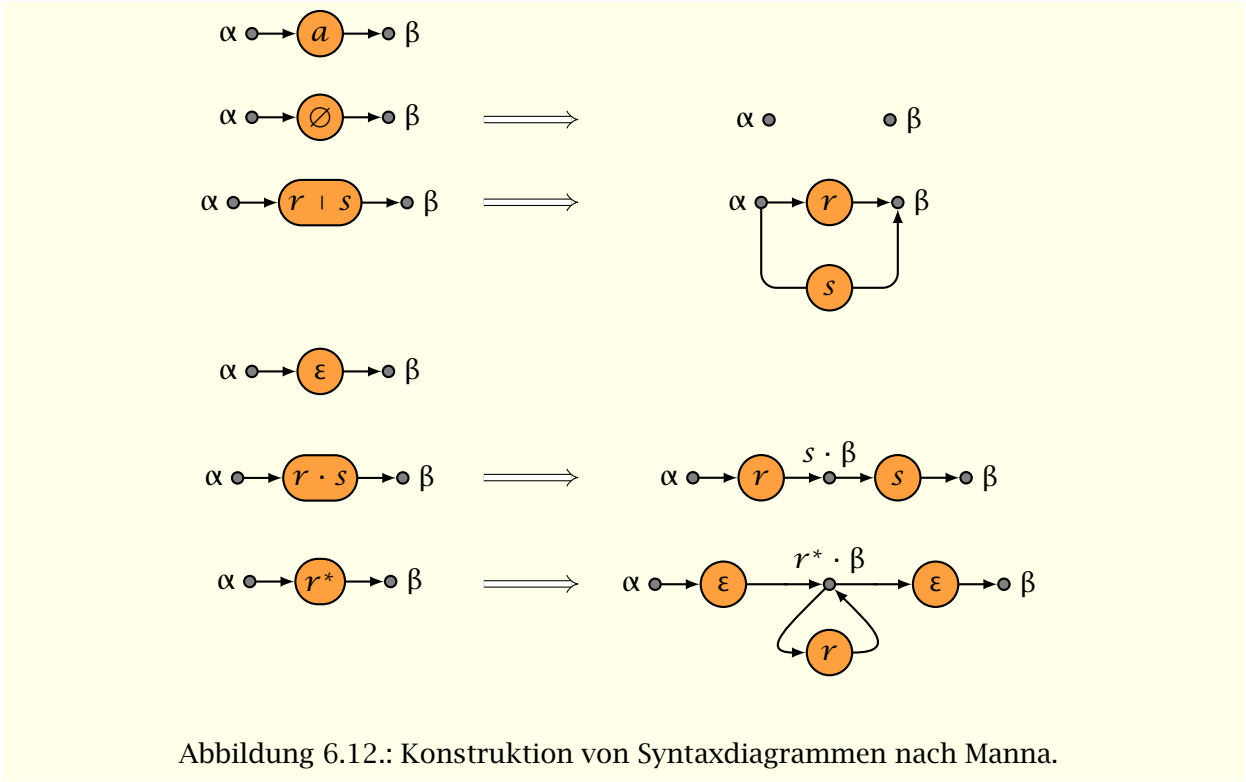
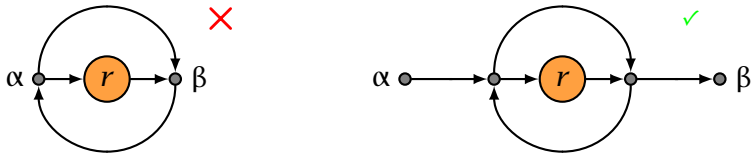


Abbildung 6.12.: Konstruktion von Syntaxdiagrammen nach Manna.

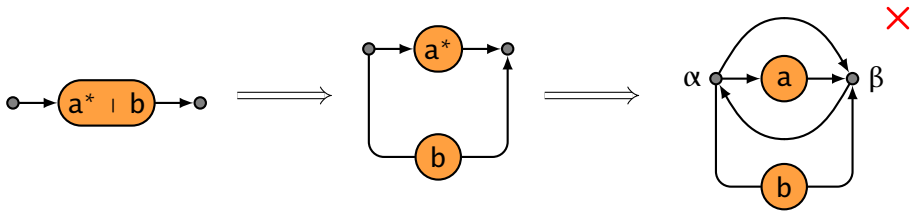
markierte Kante wird entfernt) und drei Rekursionsfälle: Die Diagramme auf der rechten Seite enthalten jeweils die Teilausdrücke der zusammengesetzten regulären Ausdrücke der entsprechenden linken Seite, für Alternative, Konkatenation und Wiederholung. Damit ist klar, dass die Laufzeit linear in der Größe des regulären Ausdrucks ist.

Was lässt sich über das resultierende Syntaxdiagramm aussagen? Sowohl die Anzahl der Knoten als auch die Anzahl der Kanten ist linear in der Größe des regulären Ausdrucks. Genauer: Jedes Grundsymbol resultiert in einer Kante; jede Wiederholung führt zwei zusätzliche Kanten ein. Ausgangspunkt ist ein Diagramm mit zwei Knoten; jede Konkatenation und jede Wiederholung führt einen zusätzlichen Knoten ein. Hier lässt sich eine interessante Beobachtung machen, deren Signifikanz allerdings erst später deutlich wird: Alle Knoten sind *Konkatenationen von Teilausdrücken* des gegebenen regulären Ausdrucks r_1: Wir starten mit r_1 als Startknoten und mit ε als Zielknoten; die Konkatenation führt den Knoten $s \cdot \beta$ ein; die Wiederholung den Knoten $r^* \cdot \beta$ — sowohl s als auch r^* sind Teilausdrücke von r_1. Diese regulären Ausdrücke nennen wir ***Teilfaktoren*** von r_1. In Abschnitt 6.3.5 zeigen wir, dass sich alle ***Rechtsfaktoren*** von r_1 als Vereinigungen von Teilfaktoren schreiben lassen — daher der Name.

Korrektheit Ist der Algorithmus korrekt? Generiert das Syntaxdiagramm für den regulären Ausdruck r_1 die Sprache $[\![r_1]\!]$? Oder kann etwas schieflaufen, wenn man beim Zeichnen von der künstlerischen Freiheit Gebrauch macht? Zunächst einmal ist intuitiv klar, dass die Transformationen die generierten Sprachen nicht verkleinern: Die Sprache, die auf der jeweils linken Seite durch eine einzelne Kante erzeugt wird, wird auf der korrespondierenden rechten Seite durch Pfade erzeugt. Zum Beispiel können wir in dem Diagramm für die Wiederholung beliebig große Potenzen von r erzeugen, indem wir entsprechend oft im Kreis fahren. Diese Eigenschaft erfüllt allerdings auch das Diagramm unten auf der linken Seite (eine unbeschriftete Kante ist implizit mit ε markiert).

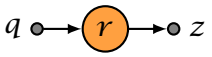


Das Diagramm hat den vermeintlichen »Vorteil«, dass kein zusätzlicher Knoten benötigt wird — allerdings ist das Diagramm nicht korrekt. Wenn wir zum Beispiel den Ausdruck `a* | b` unter Verwendung dieser Regel transformieren,



erhalten wir ein Syntaxdiagramm, das die Sprache $(\mathtt{a} \mid \mathtt{b})^*$ erzeugt. Autsch. Das heißt natürlich nicht, dass wir uns keine künstlerische Freiheit erlauben können. Das Diagramm weiter oben auf der rechten Seite ist ähnlich gestaltet, bereitet aber keine Probleme, da es zwei zusätzliche Knoten verwendet — wie sind diese zu beschriften? (Man kann zeigen, dass für die Wiederholung mindestens ein zusätzlicher Knoten benötigt wird.)

Um auszuschließen, dass wir über das Ziel hinausschießen und wie im Beispiel oben eine größere Sprache generieren, $[\![(\mathtt{a} \mid \mathtt{b})^*]\!] \supseteq [\![\mathtt{a}^* \mid \mathtt{b}]\!]$, müssen alle Kanten die folgende ***Invariante*** erfüllen.



$$[\![q]\!] \supseteq [\![r]\!] \cdot [\![z]\!]$$

Die Sprache, die über diese Kante generiert wird, ist eine Teilmenge von q. Eine Kante, die diese Eigenschaft erfüllt, nennen wir ***zulässig***. Beachte, dass wir keine Gleichheit fordern, da die Kante nach z in der Regel nicht die einzige von q ausgehende Kante ist. In dem Syntaxdiagramm für $(\mathtt{a} \mid \mathtt{b})^* \cdot \mathtt{b} \cdot (\mathtt{a} \mid \mathtt{b})$ werden die Knoten r_4 und r_5 zum Beispiel durch zwei Kanten verbunden. (Die Invariante kann auch mit Hilfe der Reduktionssemantik ausgedrückt werden: Aus q muss sich in mehreren Schritten $r \cdot z$ ableiten lassen, $q \to \cdots \to r \cdot z$.)

Man kann zeigen, dass jede in Abbildung 6.12 aufgeführte Transformation die Invariante erhält: Wenn die Kante auf der linken Seite zulässig ist, dann sind auch die Kanten auf der korrespondierenden rechten Seite zulässig. Der folgende Paragraph erklärt den Beweis »en détail« — für den Fall, dass Sie den Dingen auf den Grund gehen wollen.

Korrektheitsbeweis⋆⋆ Der Korrektheitsbeweis bewegt sich in einem typischen Spannungsfeld: Der Algorithmus arbeitet mit *lokalen* Transformationen; wir wollen aber eine *globale* Eigenschaft etablieren: Das Syntaxdiagramm erzeugt die gewünschte Sprache. Die Herausforderung besteht darin, Eigenschaften eines Graphen auf einzelne Knoten und Kanten herunterzubrechen — das macht den Beweis interessant, so dass wir ihm etwas Raum geben.

Das erste Problem, mit dem wir uns konfrontiert sehen, ist eher technischer Natur: Die Transformationen für Konkatenation und Wiederholung erzeugen *neue* Knoten; Graphen bzw. Matrizen mit unterschiedlichen Knotenmengen lassen sich aber nur schwer zueinander in Beziehung setzen (der punktweise Vergleich $A \sqsubseteq B$ setzt voraus, dass die Matrizen A und B die gleiche Dimension besitzen). Wir behelfen uns mit einem Trick und nehmen an, dass alle Knoten bereits im Ausgangsgraphen als isolierte Knoten enthalten sind. (Wenn man möchte, führen wir den Algorithmus gedanklich zweimal aus: einmal, um die Knotenmenge zu bestimmen, und ein zweites

Mal, um das Syntaxdiagramm zu konstruieren.) Seien $r_1, \ldots, r_n$ die Knoten des finalen Syntaxdiagramms (die Teilfaktoren) mit dem Startknoten r_1 und dem Zielknoten $r_n = \varepsilon$. Alle im Folgenden verwendeten Matrizen besitzen entsprechend die Dimension $n \times n$.

Die Semantik aus Abschnitt 6.3.1 gibt das Korrektheitskriterium vor; der für r_1 konstruierte Graph G muss die Sprache $[\![r_1]\!]$ generieren:

$$\text{(Korrektheit)} \qquad S \cdot G^* \cdot F = [\![r_1]\!] \quad \text{mit } S := \begin{pmatrix} \varepsilon & \varnothing & \ldots & \varnothing \end{pmatrix} \text{ und } F := \begin{pmatrix} \varnothing \\ \vdots \\ \varnothing \\ \varepsilon \end{pmatrix} \tag{6.15}$$

Die Vektoren selektieren den Eintrag in der rechten oberen Ecke von G^*.

Bei der Besprechung der Transformationen ist bereits angeklungen, dass sich der Korrektheitsbeweis in zwei Aspekte aufteilt. Wenn wir eine Kante durch einen Minigraphen ersetzen, müssen wir garantieren, dass die von der Kante beigesteuerte Sprache durch Pfade in dem Minigraphen erzeugt wird, sprich der »neue« Graph generiert *mindestens* die Sprache des »alten« Graphen. Darüber hinaus müssen wir sicherstellen, dass wir nicht über das Ziel hinausschießen, sprich der »neue« Graph generiert *höchstens* die Sprache des »alten« Graphen. Beweistechnisch entspricht dieses Argument einem ***Ping-Pong Beweis***: Um $A = B$ zu beweisen, zeigen wir $A \subseteq B$ und $A \supseteq B$. Wir werden sehen, dass im vorliegenden Fall beide Teilbeweise ganz unterschiedlich geführt werden.

Fangen wir mit dem anspruchsvolleren Teil an, dem »Ping«: $S \cdot G^* \cdot F \subseteq [\![r_1]\!]$. Wie können wir die Anforderung an G auf einzelne Knoten und Kanten herunterbrechen? Zu diesem Zweck verallgemeinern wir die Aussage, indem wir nicht nur den Startknoten r_1 und den Zielknoten ε, sondern alle Knoten ins Kalkül ziehen. Zur Erinnerung: Die Teilfaktoren $r_1, \ldots, r_n$ beschreiben — so zumindest die Behauptung — die Sprachen, die *von* dem jeweiligen Knoten r_i bis zum Zielknoten ε generiert werden. Dazu definieren wir den Vektor der generierten Sprachen:

$$\boldsymbol{L} := \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} \qquad \text{mit } L_i := [\![r_i]\!]$$

Jetzt können wir mit dem ersten Teilbeweis loslegen. Wir abstrahieren zunächst vom Startvektor S, um anschließend das Prinzip der Fixpunkt-Induktion anwenden zu können.

$$\begin{aligned}
& S \cdot G^* \cdot F \subseteq [\![r_1]\!] \\
\iff & \quad \{\ [\![r_1]\!] = S \cdot \boldsymbol{L}\ \} \\
& S \cdot G^* \cdot F \subseteq S \cdot \boldsymbol{L} \\
\impliedby & \quad \{\ \text{Monotonie der Konkatenation (6.3b)}\ \} \\
& G^* \cdot F \sqsubseteq \boldsymbol{L} \\
\impliedby & \quad \{\ \text{Fixpunkt-Induktion (6.2c)}\ \} \\
& G \cdot \boldsymbol{L} \sqcup F \sqsubseteq \boldsymbol{L} \\
\iff & \quad \{\ \text{Eigenschaft der Vereinigung — Supremum (B.22)}\ \} \\
& G \cdot \boldsymbol{L} \sqsubseteq \boldsymbol{L} \ \wedge\ F \sqsubseteq \boldsymbol{L} \\
\iff & \quad \{\ F \sqsubseteq \boldsymbol{L}\ \} \\
& G \cdot \boldsymbol{L} \sqsubseteq \boldsymbol{L}
\end{aligned}$$

Wir erhalten eine hinreichende Bedingung, die sicherstellt, dass wir »nicht über das Ziel hinausschießen«. Die Bedingung lässt sich als ***Invariante*** deuten: Die generierten Sprachen werden nicht

vergrößert, wenn wir die Pfade um eine Kante in G verlängern. Wir nennen den Graphen G ***zulässig***, wenn $\boldsymbol{L} \sqsupseteq G \cdot \boldsymbol{L}$ — dies ist ein *globales* Kriterium. Nun kann man zeigen, dass der Graph G genau dann zulässig ist, wenn jede einzelne seiner Kanten zulässig ist — damit erhalten wir das gewünschte *lokale* Kriterium. Der Zusammenhang lässt sich sehr schön mit Hilfe unseres laufenden Beispiels, der advPieb-Sprache, illustrieren. Dazu überführen wir die Matrixungleichung in ein System von Ungleichungen, eine für jede der sieben Kanten in (6.9).

$$\boldsymbol{L} \sqsupseteq M \cdot \boldsymbol{L} \iff \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{pmatrix} \sqsupseteq \begin{pmatrix} \varnothing & \varepsilon & \varnothing & \varnothing & \varnothing \\ \varnothing & \{a,b\} & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing & \{b\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \{a,b\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{pmatrix}$$

$$\iff \left\{ \begin{array}{l} L_1 \sqsupseteq \varepsilon \cdot L_2 \\ L_2 \sqsupseteq \{a,b\} \cdot L_2 \cup \varepsilon \cdot L_3 \\ L_3 \sqsupseteq \{b\} \cdot L_4 \\ L_4 \sqsupseteq \{a,b\} \cdot L_5 \\ L_5 \sqsupseteq \varnothing \end{array} \right\} \iff \left\{ \begin{array}{l} L_1 \sqsupseteq \varepsilon \cdot L_2 \\ L_2 \sqsupseteq \{a\} \cdot L_2 \\ L_2 \sqsupseteq \{b\} \cdot L_2 \\ L_2 \sqsupseteq \varepsilon \cdot L_3 \\ L_3 \sqsupseteq \{b\} \cdot L_4 \\ L_4 \sqsupseteq \{a\} \cdot L_5 \\ L_4 \sqsupseteq \{b\} \cdot L_5 \end{array} \right\}$$

Der gesamte Graph ist genau dann zulässig, wenn jede einzelne der sieben Kanten zulässig ist.

Erinnern Sie sich noch an die drei Phasen im Leben einer Invariante?

1. *Die Invariante wird etabliert:* Dazu müssen zeigen, dass die einzige Kante des Ausgangsgraphen zulässig ist.
2. *Die Invariante wird erhalten:* Wir müssen zeigen, dass die durch die Graphtransformationen hinzugekommenen Kanten zulässig sind — dabei dürfen wir ausnutzen, dass die jeweils entfernte Kante zulässig ist.
3. *Aus der Invariante folgt das gewünschte Ergebnis:* Die Invariante stellt sicher, dass wir »nicht über das Ziel hinausschießen«, siehe obige Rechnung.

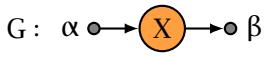
Nach diesen Vorarbeiten ist der eigentliche Beweis reine Fleißarbeit, Abbildungen 6.13 und 6.14 schwelgen in den Details.

Kommen wir zum zweiten Teil des Beweises, dem »Pong«, und nehmen an, dass der Graph H durch eine der in Abbildung 6.12 aufgeführten Graphtransformationen aus G hervorgegangen ist. Die Graphtransformationen basieren auf der Idee, eine *Kante* in G durch *Pfade* in H zu simulieren: $G \sqsubseteq H^*$ — die folgende Rechnung zeigt, dass wir genau das beweisen müssen.

$$\begin{array}{ll} & [\![r_1]\!] \subseteq S \cdot H^* \cdot F \\ \Longleftarrow & \quad \{ \text{ Annahme: G ist korrekt (6.15) und Transitivität } \} \\ & S \cdot G^* \cdot F \subseteq S \cdot H^* \cdot F \\ \Longleftarrow & \quad \{ \text{ Monotonie der Konkatenation (6.3b) } \} \\ & G^* \sqsubseteq H^* \\ \iff & \quad \{ \text{ Eigenschaft des Hüllenoperators } \} \\ & G \sqsubseteq H^* \end{array}$$

Wie gestaltet sich hier der Übergang von dem *globalen* Kriterium zu einem *lokalen* Kriterium? Zunächst einmal können wir $G \sqsubseteq H^*$ »kantenweise« zeigen: $G(i,j) \subseteq H^*(i,j)$ für alle Knoten i

und j.[11] Aufgrund der Monotonie des Sternoperators (6.3c) sind hinzugefügte Kanten unkritisch, für diese gilt: $G(i,j) \subseteq H(i,j) \subseteq H^*(i,j)$. Wir können uns also auf die *eine* Kante von α nach β konzentrieren, die entfernt wird. Allgemein gilt:



$$G(\alpha,\beta) \subseteq X \cup H(\alpha,\beta) \tag{6.16}$$

Wenn wir die entfernte Kantenmarkierung zu H hinzunehmen, erhalten wir mindestens G. Die folgende Rechnung zeigt, dass es somit genügt, $X \subseteq H^*(\alpha,\beta)$ zu zeigen.

$$\begin{aligned}
& G(\alpha,\beta) \subseteq H^*(\alpha,\beta) \\
\Longleftarrow \quad & \{\ (6.16) \text{ und Transitivität } \} \\
& X \cup H(\alpha,\beta) \subseteq H^*(\alpha,\beta) \\
\Longleftrightarrow \quad & \{\ \text{Eigenschaft der Vereinigung — Supremum (B.22)} \ \} \\
& X \subseteq H^*(\alpha,\beta) \ \wedge \ H(\alpha,\beta) \subseteq H^*(\alpha,\beta) \\
\Longrightarrow \quad & \{\ \text{eine Kante ist ein Pfad, siehe unten (6.17b)} \ \} \\
& X \subseteq H^*(\alpha,\beta)
\end{aligned}$$

Für den Nachweis der finalen Inklusion greifen wir auf die folgenden Eigenschaften zurück, die sich unmittelbar aus den Hülleneigenschaften (6.11) ableiten.

$$\varepsilon \subseteq M^*(i,i) \tag{6.17a}$$
$$M(i,j) \subseteq M^*(i,j) \tag{6.17b}$$
$$M^*(i,j) \cdot M^*(j,k) \subseteq M^*(i,k) \tag{6.17c}$$
$$\big(M^*(i,i)\big)^* \subseteq M^*(i,i) \tag{6.17d}$$

Vielleicht sind Sie beim Studium der Transformationen oder der Beispieldiagramme mit den Fingern an den Kanten entlang gelaufen. Die obigen Eigenschaften fangen die Sprachgenerierung »von Hand« ein. Die letzte Formel (6.17d) formalisiert zum Beispiel das »sich im Kreise drehen«: Eine Rundreise von i nach i kann beliebig oft wiederholt werden. Die Hülleneigenschaften beziehen sich auf einen Graphen als Ganzes (global), die obigen Ungleichungen beziehen sich auf einzelne Knoten und Kantenmarkierungen (lokal).

Abbildungen 6.13 und 6.14 führen wiederum die Details des Beweises aus.

6.3.3. Nichtdeterministische Automaten mit ε-Übergängen⋆

module Automata

Bislang haben wir Syntaxdiagramme durch die »Generatorbrille« betrachtet und die Frage beantwortet, welche Sprache durch ein Syntaxdiagramm generiert wird. Jetzt wechseln wir die Perspektive und studieren Syntaxdiagramme durch die »Akzeptorbrille«. Wir zeigen, dass sich das Wortproblem[12] mit Hilfe von Syntaxdiagrammen lösen lässt. Dazu reduzieren wir das Wortproblem auf ein Suchproblem: Finden wir zu einem gegebenen Wort einen entsprechend beschrifteten Pfad von einem Start- zu einem Zielknoten? (In Abschnitt 6.2.1 haben wir das Wortproblem bereits diskutiert; hier nähern wir uns dem Problem von einer anderen Seite — am Ende von Abschnitt 6.3 schließt sich der Kreis.)

Der Perspektivwechsel ist schnell vollzogen. Erinnern wir uns: Bei der schrittweisen Konstruktion von Syntaxdiagrammen haben wir jeden Knoten mit der Sprache beschriftet, die *von* ebendiesem Knoten bis zu einem Zielknoten generiert wird (einem Teilfaktor). Jede dieser Sprachen

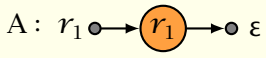
[11] Wir verzichten aus Gründen der Lesbarkeit auf die kompakte Matrixnotation G_{ij} und schreiben die Funktionsanwendung wie gewohnt $G(i,j)$.

[12] Zur Erinnerung: Das Wortproblem fragt, ob das Wort w in der Sprache L enthalten ist: $w \in L$?

Wir führen den Beweis induktiv über die Anzahl der Graphtransformationen.

.....

Induktionsbasis: Die Ausgangsmatrix A enthält nur einen einzigen Eintrag:



$$S := \begin{pmatrix} \varepsilon & \varnothing & \dots & \varnothing \end{pmatrix} \quad A := \begin{pmatrix} \varnothing & \cdots & \varnothing & [\![r_1]\!] \\ \varnothing & \cdots & \varnothing & \varnothing \\ \vdots & \ddots & \vdots & \vdots \\ \varnothing & \cdots & \varnothing & \varnothing \end{pmatrix} \quad F := \begin{pmatrix} \varnothing \\ \vdots \\ \varnothing \\ \varepsilon \end{pmatrix}$$

Wir müssen zeigen, dass die einzige Kante in A zulässig ist — das ist nicht schwer:

$$\begin{aligned} & [\![r_1]\!] \supseteq [\![r_1]\!] \cdot [\![\varepsilon]\!] \\ \iff & \quad \{ \text{ Semantik } \} \\ & [\![r_1]\!] \supseteq [\![r_1]\!] \cdot \varepsilon \\ \iff & \quad \{ \text{ neutrales Element } \} \\ & [\![r_1]\!] \supseteq [\![r_1]\!] \end{aligned}$$

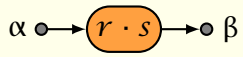
(Falls Sie sich wundern: Eine »nicht-existente« Kante von r_i nach r_j, die in der Matrix durch einen ∅-Eintrag repräsentiert wird, ist stets zulässig: $[\![r_i]\!] \supseteq \varnothing \cdot [\![r_j]\!] = \varnothing$.)
Weiterhin müssen wir nachweisen, dass der Ausgangsgraph die Sprache $[\![r_1]\!]$ generiert. Da der Graph nur eine, nicht-zyklische Kante enthält, gilt $A^2 = \mathbf{0}$ und somit $A^* = \mathbf{1} \cup A$.

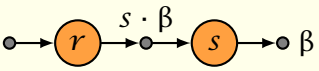
$$S \cdot A^* \cdot F = S \cdot (\mathbf{1} \cup A) \cdot F = S \cdot \mathbf{1} \cdot F \cup S \cdot A \cdot F = \varnothing \cup [\![r_1]\!] = [\![r_1]\!]$$

Da der Startknoten kein Zielknoten ist, gilt $S \cdot F = \varnothing$.

.....

Induktionsschritt: Wir nehmen an, dass der Graph H aus G durch Anwendung einer der Transformationen aus Abbildung 6.12 hervorgeht. Für die ersten vier Fälle ist nichts zu zeigen. (Warum?)

Fall: G : 

$\Longrightarrow$ H : 

Wir müssen nachweisen, dass die zwei zusätzlichen Kanten in H zulässig sind.

$$\begin{aligned} & [\![\alpha]\!] \supseteq [\![r]\!] \cdot [\![s \cdot \beta]\!] \\ \iff & \quad \{ \text{ Semantik } \} \\ & [\![\alpha]\!] \supseteq [\![r]\!] \cdot ([\![s]\!] \cdot [\![\beta]\!]) \\ \iff & \quad \{ \text{ Assoziativgesetz } \} \\ & [\![\alpha]\!] \supseteq ([\![r]\!] \cdot [\![s]\!]) \cdot [\![\beta]\!] \\ \iff & \quad \{ \text{ Semantik } \} \\ & [\![\alpha]\!] \supseteq [\![r \cdot s]\!] \cdot [\![\beta]\!] \end{aligned}$$

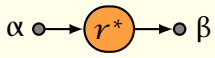
$$\begin{aligned} & [\![s \cdot \beta]\!] \supseteq [\![s]\!] \cdot [\![\beta]\!] \\ \iff & \quad \{ \text{ Semantik } \} \\ & [\![s]\!] \cdot [\![\beta]\!] \supseteq [\![s]\!] \cdot [\![\beta]\!] \\ \iff & \quad \{ \text{ Reflexivität } \} \\ & \mathit{true} \end{aligned}$$

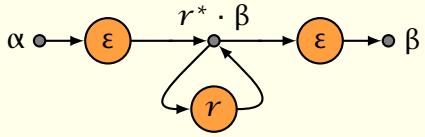
Die finale Ungleichung $[\![\alpha]\!] \supseteq [\![r \cdot s]\!] \cdot [\![\beta]\!]$ ist erfüllt, da die Kante in G zulässig ist.

Abbildung 6.13.: Korrektheit von Mannas Verfahren (Teil 1).

Weiterhin muss $[\![r \cdot s]\!]$ durch H generiert werden.

$$
\begin{array}{ll}
 & [\![r \cdot s]\!] \\
= & \quad \{ \text{ Semantik } \} \\
 & [\![r]\!] \cdot [\![s]\!] \\
\subseteq & \quad \{ \text{ Definition H } \} \\
 & H(\alpha, s \cdot \beta) \cdot H(s \cdot \beta, \beta) \\
\subseteq & \quad \{ \text{ eine Kante ist ein Pfad (6.17b) } \} \\
 & H^*(\alpha, s \cdot \beta) \cdot H^*(s \cdot \beta, \beta) \\
\subseteq & \quad \{ \text{ Konkatenation (6.17c) } \} \\
 & H^*(\alpha, \beta)
\end{array}
$$

Fall: G : 

$\Longrightarrow$ H : 

Wir müssen zeigen, dass die drei zusätzlichen Kanten in H zulässig sind.

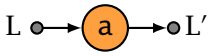
$$
\begin{array}{lll}
 & & [\![r^* \cdot \beta]\!] \supseteq [\![\varepsilon]\!] \cdot [\![\beta]\!] \ \wedge \ [\![r^* \cdot \beta]\!] \supseteq [\![r]\!] \cdot [\![r^* \cdot \beta]\!] \\
 & & \Longleftrightarrow \quad \{ \text{ Semantik } \} \\
 & [\![\alpha]\!] \supseteq [\![\varepsilon]\!] \cdot [\![r^* \cdot \beta]\!] & [\![r^*]\!] \cdot [\![\beta]\!] \supseteq \varepsilon \cdot [\![\beta]\!] \ \wedge \ [\![r^*]\!] \cdot [\![\beta]\!] \supseteq [\![r]\!] \cdot [\![r^*]\!] \cdot [\![\beta]\!] \\
\Longleftrightarrow & \quad \{ \text{ Semantik } \} & \Longleftarrow \quad \{ \text{ Monotonie (6.3b) } \} \\
 & [\![\alpha]\!] \supseteq \varepsilon \cdot [\![r^*]\!] \cdot [\![\beta]\!] & [\![r^*]\!] \supseteq \varepsilon \ \wedge \ [\![r^*]\!] \supseteq [\![r]\!] \cdot [\![r^*]\!] \\
\Longleftrightarrow & \quad \{ \text{ neutrales Element } \} & \Longleftrightarrow \quad \{ \text{ Supremum (B.22) } \} \\
 & [\![\alpha]\!] \supseteq [\![r^*]\!] \cdot [\![\beta]\!] & [\![r^*]\!] \supseteq \varepsilon \cup [\![r]\!] \cdot [\![r^*]\!] \\
 & & \Longleftrightarrow \quad \{ \text{ Fixpunkt (B.107a) } \} \\
 & & \mathit{true}
\end{array}
$$

Die finale Ungleichung $[\![\alpha]\!] \supseteq [\![r^*]\!] \cdot [\![\beta]\!]$ ist erfüllt, da die Kante in G zulässig ist.
Schließlich muss $[\![r^*]\!]$ durch H generiert werden.

$$
\begin{array}{ll}
 & [\![r^*]\!] \\
\subseteq & \quad \{ \text{ Semantik und neutrales Element } \} \\
 & \varepsilon \cdot [\![r]\!]^* \cdot \varepsilon \\
\subseteq & \quad \{ \text{ Definition H } \} \\
 & H(\alpha, i) \cdot \big(H(i, i)\big)^* \cdot H(i, \beta) \\
\subseteq & \quad \{ \text{ eine Kante ist ein Pfad (6.17b) } \} \\
 & H^*(\alpha, i) \cdot \big(H^*(i, i)\big)^* \cdot H^*(i, \beta) \\
\subseteq & \quad \{ \text{ Wiederholung (6.17d) } \} \\
 & H^*(\alpha, i) \cdot H^*(i, i) \cdot H^*(i, \beta) \\
\subseteq & \quad \{ \text{ Konkatenation (6.17c) } \} \\
 & H^*(\alpha, \beta)
\end{array}
$$

Abbildung 6.14.: Korrektheit von Mannas Verfahren (Teil 2).

überführen wir in einen ***Akzeptor***. Die Akzeptoren orchestrieren zusammen die Graphsuche: Befinden wir uns zum Beispiel in dem Knoten L,



dann bewegen wir uns nach L′, wenn das nächste Zeichen der Eingabe ein a ist. In der Matrixnotation entspricht die Folge der generierten Sprachen dem Spaltenvektor $M^* \cdot F$.[13] Dieser Vektor erfüllt die Gleichung $\boldsymbol{L} = M \cdot \boldsymbol{L} \cup F$ in der Unbekannten $\boldsymbol{L}$ — eine allgemeine Eigenschaft des Sternoperators (siehe Aufgabe 6.1.5).

$$\boldsymbol{L} = M^* \cdot F \quad \Longrightarrow \quad \boldsymbol{L} = M \cdot \boldsymbol{L} \cup F$$

Für unser laufendes Beispiel, die advPieb-Sprache, erhalten wir das folgende Gleichungssystem — um die Struktur hervorzuheben, haben wir wir die rechten Seiten der Gleichungen mit Hilfe der Gesetze $\varepsilon \cdot L = L$ und $(R \cup S) \cdot L = (R \cdot L) \cup (S \cdot L)$ geringfügig umgeformt.

$$\begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{pmatrix} = \begin{pmatrix} \varnothing & \varepsilon & \varnothing & \varnothing & \varnothing \\ \varnothing & \{a,b\} & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing & \{b\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \{a,b\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix} \cdot \begin{pmatrix} L_1 \\ L_2 \\ L_3 \\ L_4 \\ L_5 \end{pmatrix} \cup \begin{pmatrix} \varnothing \\ \varnothing \\ \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix} \qquad \begin{aligned} L_1 &= L_2 \\ L_2 &= a \cdot L_2 \cup b \cdot L_2 \cup L_3 \\ L_3 &= b \cdot L_4 \\ L_4 &= a \cdot L_5 \cup b \cdot L_5 \\ L_5 &= \varepsilon \end{aligned}$$

Da die Einträge der Matrix sehr einfache Sprachen sind, Mengen von Grundsymbolen, besitzen die Gleichungen ebenfalls eine sehr einfache Form. So einfach, dass wir für jede Sprache mehr oder weniger direkt einen Akzeptor angeben können. Um die Gleichungen buchstabengetreu umsetzen zu können, führen wir zunächst etwas Vokabular ein und implementieren eine ***Kombinatorbibliothek*** oder ***domänenspezifische Sprache*** (engl. domain-specific language, kurz DSL) für Akzeptoren.

```
type Alphabet = | A | B
type Acceptor = List⟨Alphabet⟩ → Bool
```

Eine Sprache ist eine Menge von Worten; Akzeptor ist ein anderer Name für die sogenannte *charakteristische Funktion* dieser Menge.

```
let end-of-input : Acceptor = function                  // ε
    | [ ]     → true
    | x :: xs → false
let seq (a : Alphabet, acc : Acceptor) : Acceptor = function   // a · L
    | [ ]     → false
    | x :: xs → a = x && acc xs
let empty : Acceptor =                                  // ∅ — Fehlschlag
    fun inp → false
let alt (acc1 : Acceptor, acc2 : Acceptor) =            // L1 ∪ L2 — Backtracking
    fun inp → acc1 inp || acc2 inp
```

Der Akzeptor für die Sprache ε ist *end-of-input*; wenn *acc* der Akzeptor für die Sprache L ist, dann erkennt *seq* (a, *acc*) die Sprache $a \cdot L$; *empty* ist der Akzeptor für ∅; ist acc_i der Akzeptor für L_i, dann erkennt *alt* (acc_1, acc_2) die Sprache $L_1 \cup L_2$.

[13] Die Matrixdarstellung $S \cdot M^* \cdot F$ ist symmetrisch bezüglich Start- und Zielknoten. Wollten wir die Eingabe von *rechts nach links* abarbeiten, würden wir den Zeilenvektor $S \cdot M^*$ der Sprachen betrachten, die ausgehend von einem Startknoten *bis* zu dem jeweiligen Knoten generiert werden.

Beispiele Mit Hilfe des Vokabulars lässt sich das Gleichungssystem für die advPieb-Sprache ziemlich direkt in ein System verschränkt rekursiver *Funktions*definitionen überführen (noch direkter wären verschränkt rekursive *Werte*definitionen; diese sind aber leider nicht zulässig).

```
module PenultimateSymbolIsB =          // (a | b)* · b · (a | b)
  let rec acc1 inp = acc2                                          inp
  and     acc2 inp = alt (alt (seq (A, acc2), seq (B, acc2)), acc3) inp
  and     acc3 inp = seq (B, acc4)                                 inp
  and     acc4 inp = alt (seq (A, acc5), seq (B, acc5))            inp
  and     acc5 inp = end-of-input                                  inp
  let accept = acc1
```

Der Akzeptor für die Sprache ist durch $S \cdot \boldsymbol{L}$ gegeben, in unserem Fall ist $S \cdot \boldsymbol{L} = L_1$.

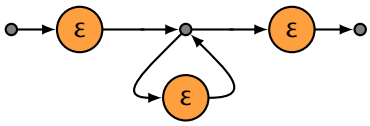
Der Akzeptor implementiert wie bereits angesprochen eine Graphsuche. Das gegebene Wort gibt den Suchpfad vor; wir hangeln uns im Syntaxdiagramm von Knoten zu Knoten, bis wir an einem Zielknoten angelangt sind; das nächste Zeichen der Eingabe weist uns jeweils den Weg. Allerdings ist nicht jeder Schritt zwangsläufig: Im zweiten Knoten können wir zum Beispiel entweder ein Zeichen konsumieren und im Knoten bleiben *oder* zum nächsten Knoten gehen, ohne die Eingabe zu verändern. Diese konkurrierenden Suchpfade explorieren wir mit Hilfe des Kombinators *alt*, der auf die Disjunktion Boolescher Werte zurückgeführt wird. Aus diesem Grund spricht man auch von einem ***nichtdeterministischen Automaten***. Die Akzeptoren aus Abschnitt 6.2 sind im Gegensatz dazu ***deterministisch***: In jedem Schritt gibt es in Abhängigkeit vom nächsten Eingabezeichen genau einen Folgeakzeptor.

Die Tests verlaufen zwar zufriedenstellend,

```
⋙ PenultimateSymbolIsB.accept [A; B; B; A]
true
⋙ PenultimateSymbolIsB.accept [B; A; B]
false
```

aber es ist nicht alles Gold, was glänzt:

Zunächst einmal stellen wir fest, dass die Akzeptoren *nicht* nach dem Struktur Entwurfsmuster für Listen gestrickt sind. Ganz im Gegenteil: Manchmal erfolgt der Aufruf einer verschränkt rekursiven Funktion, ohne dass die Eingabeliste verkleinert wird — im Syntaxdiagramm korrespondieren diese Übergänge zu ε-Kanten. Im obigen Beispiel stellt das allerdings kein Problem dar (warum?), im folgenden Beispiel schon.



$$S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \quad M := \begin{pmatrix} \varnothing & \varepsilon & \varnothing \\ \varnothing & \varepsilon & \varepsilon \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \quad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix}$$

Dieses Syntaxdiagramm erhalten wir, wenn wir die in Abbildung 6.12 aufgeführten Transformationen auf den regulären Ausdruck ε^* anwenden. Man sieht das Unheil nahen: Wir können uns wortwörtlich im Kreise drehen, ohne dass ein Fortschritt bei der Verarbeitung der Eingabe erzielt wird.

```
module Loop =          // ε*
  let rec acc1 inp = acc2                inp
  and     acc2 inp = alt (acc2, acc3)    inp      // acc2 inp = acc2 inp || acc3 inp
  and     acc3 inp = end-of-input        inp
  let accept inp = acc1 inp
```

Da die Hilfsfunktion acc_2 sich selbst bei unveränderter Eingabe aufruft, terminiert die Funktion *accept* für keine Eingabe. Dabei ist die Sprache trivial, $\varepsilon^* = \varepsilon$; der gesuchte Akzeptor für diese Sprache ist schlicht und einfach *end-of-input*.

Was ist zu tun? Wir müssen die ε-Kanten eliminieren!

6.3.4. Nichtdeterministische Automaten ohne ε-Übergänge⋆

Um ε-Übergänge zu eliminieren, teilen wir die Adjazenzmatrix auf: in eine Matrix, die nur ε-Einträge enthält, und eine Matrix ohne ε-Übergänge.

$$M = (M \sqcap E) \sqcup (M - E) \tag{6.18}$$

Dabei ist E eine Matrix, die überall das leere Wort ε enthält.[14] Der Durchschnitt und die Differenz von Matrizen sind genau wie die Vereinigung komponentenweise definiert.

$$\begin{aligned} E_{ij} &:= \varepsilon \\ (A \sqcap B)_{ij} &:= A_{ij} \cap B_{ij} \\ (A - B)_{ij} &:= A_{ij} - B_{ij} \end{aligned}$$

Die reflexive, transitive Hülle von M formen wir mit Hilfe der Dekompositionsregel (6.5) um.

$$\begin{aligned} & M^* \\ = \quad & \{ \text{ Partitionierung von M (6.18) } \} \\ & ((M \sqcap E) \sqcup (M - E))^* \\ = \quad & \{ \text{ Dekompositionsregel (6.5): } (A \sqcup B)^* = (A^* \cdot B)^* \cdot A^* \ \} \\ & ((M \sqcap E)^* \cdot (M - E))^* \cdot (M \sqcap E)^* \end{aligned}$$

Die Matrix $C := (M \sqcap E)^*$ nennt man auch den ε-***Abschluss*** (engl. ε-closure) von M. Die Umformung formalisiert, dass ein *Pfad* in M als alternierende Folge von ε-*Pfaden* und $\mathbb{A}$-*Kanten* gedeutet werden kann. Insgesamt erhalten wir:

$$M^* \cdot F = N^* \cdot F' \quad \text{mit} \quad \begin{cases} C := (M \sqcap E)^* \\ N := C \cdot (M - E) \\ F' := C \cdot F \end{cases}$$

Das gesuchte Syntaxdiagramm ohne ε-Übergänge ist somit $S \cdot N^* \cdot F'$ — der Startvektor bleibt unverändert.

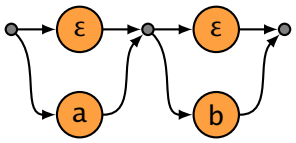
Ein Vektor bzw. eine Matrix A heißt ε-***frei***, wenn alle Einträge ε-frei sind: $A \sqcap E = \mathbf{0}$. Ähnlich wie ε-freien Sprachen kommt ε-freien Adjazenzmatrizen eine besondere Rolle zu. Zum Beispiel lässt sich die Gleichung $\boldsymbol{L} = N \cdot \boldsymbol{L} \cup F$ in der Unbekannten $\boldsymbol{L}$ *eindeutig* lösen,

$$\boldsymbol{L} = N^* \cdot F \quad \Longleftrightarrow \quad \boldsymbol{L} = N \cdot \boldsymbol{L} \cup F$$

wenn die Adjazenzmatrix N ε-frei ist (siehe auch Anhang B.6.7).

[14] Die Matrix E ist nicht mit der Einheitsmatrix $\mathbf{1}$ zu verwechseln. Letztere enthält das leere Wort bzw. die Sprache $\{\varepsilon\}$ nur auf der Hauptdiagonalen, erstere überall.

Beispiele Gehen wir die Transformation an einem überschaubaren Beispiel durch, der Potenzsprache aus Abschnitt 6.3.1.



$$S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \quad M := \begin{pmatrix} \varnothing & \{\varepsilon, a\} & \varnothing \\ \varnothing & \varnothing & \{\varepsilon, b\} \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \quad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix}$$

Da es keine Pfade der Länge > 2 gibt, ist die ε-Hülle von M schnell ausgerechnet.

$$C = (M \sqcap E)^0 \sqcup (M \sqcap E)^1 \sqcup (M \sqcap E)^2 = \begin{pmatrix} \varepsilon & \varnothing & \varnothing \\ \varnothing & \varepsilon & \varnothing \\ \varnothing & \varnothing & \varepsilon \end{pmatrix} \sqcup \begin{pmatrix} \varnothing & \varepsilon & \varnothing \\ \varnothing & \varnothing & \varepsilon \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \sqcup \begin{pmatrix} \varnothing & \varnothing & \varepsilon \\ \varnothing & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing \end{pmatrix}$$

Die Diagonale von εs breitet sich wie eine Welle nach rechts oben aus, bis das obere Dreieck der Matrix gefüllt ist.

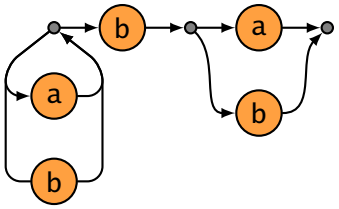
$$C := \begin{pmatrix} \varepsilon & \varepsilon & \varepsilon \\ \varnothing & \varepsilon & \varepsilon \\ \varnothing & \varnothing & \varepsilon \end{pmatrix} \qquad N := \begin{pmatrix} \varnothing & a & b \\ \varnothing & \varnothing & b \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \qquad F' := \begin{pmatrix} \varepsilon \\ \varepsilon \\ \varepsilon \end{pmatrix}$$

Die Multiplikation mit der ε-Hülle bewirkt, dass Übergänge vervielfacht werden. Im obigen Beispiel wird b verdoppelt; weiterhin wird jeder Knoten zu einem Zielknoten.

Die Vervielfachung von Einträgen illustriert auch unser laufendes Beispiel, die advPieb-Sprache.

$$C := \begin{pmatrix} \varepsilon & \varepsilon & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varepsilon & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing & \varepsilon & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \varepsilon \end{pmatrix} \qquad N := \begin{pmatrix} \varnothing & \{a,b\} & \varnothing & \{b\} & \varnothing \\ \varnothing & \{a,b\} & \varnothing & \{b\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \{b\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \{a,b\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix} \qquad F' := \begin{pmatrix} \varnothing \\ \varnothing \\ \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix}$$

Gelegentlich werden durch die Transformation Knoten überflüssig, angezeigt durch eine »leere« Spalte. In unserem Beispiel zeigt die dritte Spalte an, dass der entsprechende Knoten nicht mehr erreichbar ist. Nicht erreichbare Zustände korrespondieren im Akzeptor zu »totem Code« und können ohne Verlust eliminiert werden. Auch die erste Spalte ist leer; der erste Knoten ist aber ein Startknoten und wird somit prinzipiell benötigt. Allerdings gilt $L_1 = L_2$ (die ersten beiden Zeilen sind identisch), so dass wir L_2 als Startknoten verwenden und L_1 ebenfalls eliminieren können. Wir erhalten ein Syntaxdiagramm für $(a \mid b)^* \cdot b \cdot (a \mid b)$, das man vielleicht direkt von Hand entworfen hätte — statt dem Algorithmus in Abbildung 6.12 zu folgen.

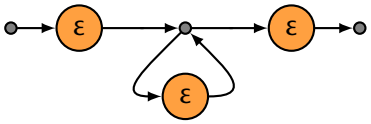


$$\begin{aligned} L_2 &= a \cdot L_2 \cup b \cdot L_2 \cup b \cdot L_4 \\ L_4 &= a \cdot L_5 \cup b \cdot L_5 \\ L_5 &= \varepsilon \end{aligned} \tag{6.19}$$

Dank der Kombinatorbibliothek lässt sich das Gleichungssystem direkt in ein Programm überführen.

```
module PenultimateSymbolIsB =          // (a | b)* · b · (a | b)
  let rec acc2 inp = alt (alt (seq (A, acc2), seq (B, acc2)), seq (B, acc4)) inp
  and     acc4 inp = alt (seq (A, acc5), seq (B, acc5))                      inp
  and     acc5 inp = end-of-input                                            inp
  let accept = acc2
```

Das Syntaxdiagramm für ε*, unserem Problemfall aus Abschnitt 6.3.3, illustriert ein Extrem: Die Adjazenzmatrix M enthält nur ∅- und ε-Einträge.



$$S := \begin{pmatrix} \varepsilon & \emptyset & \emptyset \end{pmatrix} \quad M := \begin{pmatrix} \emptyset & \varepsilon & \emptyset \\ \emptyset & \varepsilon & \varepsilon \\ \emptyset & \emptyset & \emptyset \end{pmatrix} \quad F := \begin{pmatrix} \emptyset \\ \emptyset \\ \varepsilon \end{pmatrix}$$

Entsprechend enthält die Adjazenzmatrix N ausschließlich ∅-Einträge.

$$C := \begin{pmatrix} \varepsilon & \varepsilon & \varepsilon \\ \emptyset & \varepsilon & \varepsilon \\ \emptyset & \emptyset & \varepsilon \end{pmatrix} \qquad N := \begin{pmatrix} \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset \end{pmatrix} \qquad F' := \begin{pmatrix} \varepsilon \\ \varepsilon \\ \varepsilon \end{pmatrix}$$

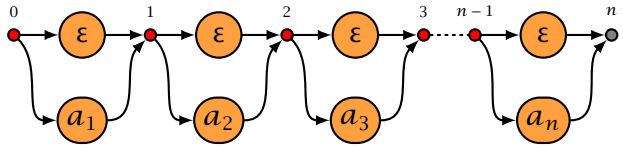
Vom ursprünglichen Programm bleibt nicht viel übrig.

```
module Loop =                 // ε*
  let rec acc1 inp = end-of-input inp
  let accept = acc1
```

Wenn wir zusätzlich die Definition von acc_1 einsetzen, erhalten wir den kürzesten aller Akzeptoren: *accept = end-of-input* — wie gewünscht.

Programmgröße und Laufzeit Durch die Elimination von ε-Kanten verändert sich die Anzahl der Knoten und Kanten. *Positiv:* Die Anzahl der Knoten bleibt gleich oder verringert sich sogar, wenn man nicht erreichbare Knoten (und damit toten Code) entfernt. *Negativ:* Die Anzahl der Kanten ist nicht länger linear in der Größe des regulären Ausdrucks, sondern möglicherweise quadratisch, da die ε-Hülle eine quadratische Zahl an ε-Einträgen haben kann. Die Multiplikation mit der ε-Hülle bewirkt, dass Übergänge vervielfacht werden. Die resultierenden Mini–F#-Programme können also recht groß werden — so groß, dass sich der Übersetzer verschluckt und den Übersetzungsvorgang mit einem Stack Overflow abbricht!

Es ist nicht allzu schwer, ein pathologisches Beispiel zu konstruieren. Dazu verallgemeinern wir die Potenzsprache aus Abschnitt 6.3.1: Der reguläre Ausdruck $(\varepsilon \mid a_1) \cdot (\varepsilon \mid a_2) \cdot \ldots \cdot (\varepsilon \mid a_n)$ bezüglich des Alphabets $\mathbb{A} = \{a_1, \ldots, a_n\}$ generiert die »Potenzmenge« von $\mathbb{A}$. Jedes Wort enthält jeden Buchstaben höchstens einmal; die Buchstaben sind weiterhin von links nach rechts angeordnet: Ist ua_iva_jw ein Wort der Sprache, dann gilt $i < j$. Jedes Wort der Potenzsprache korrespondiert zu einer Teilmenge von $\mathbb{A}$, daher der Name. Somit enthält die Sprache insgesamt 2^n verschiedene Worte. Zu dem regulären Ausdruck korrespondiert das folgende Syntaxdiagramm.

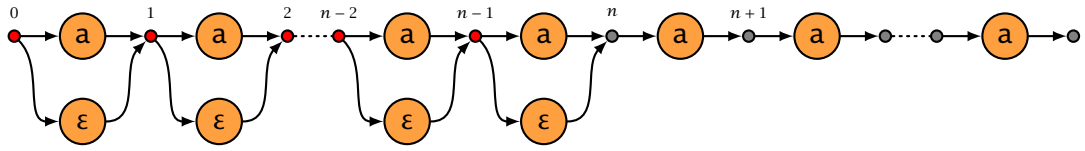


Die rot eingefärbten Knoten signalisieren Wahlmöglichkeiten. Der obere Pfad von εs bringt uns zum Beispiel vom i-ten zum j-ten Knoten (sofern $i \leqslant j$), ohne dass Eingaben konsumiert werden. Die ε-Hülle ist eine entsprechend gefüllte Dreiecksmatrix, unten aufgeführt für $n = 4$.

$$C := \begin{pmatrix} \emptyset & \varepsilon & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \varepsilon & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \varepsilon & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset & \varepsilon \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \end{pmatrix}^* = \begin{pmatrix} \varepsilon & \varepsilon & \varepsilon & \varepsilon & \varepsilon \\ \emptyset & \varepsilon & \varepsilon & \varepsilon & \varepsilon \\ \emptyset & \emptyset & \varepsilon & \varepsilon & \varepsilon \\ \emptyset & \emptyset & \emptyset & \varepsilon & \varepsilon \\ \emptyset & \emptyset & \emptyset & \emptyset & \varepsilon \end{pmatrix} \quad N := C \cdot \begin{pmatrix} \emptyset & a & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & b & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & c & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset & d \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \end{pmatrix} = \begin{pmatrix} \emptyset & a & b & c & d \\ \emptyset & \emptyset & b & c & d \\ \emptyset & \emptyset & \emptyset & c & d \\ \emptyset & \emptyset & \emptyset & \emptyset & d \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \end{pmatrix}$$

Berechnet man die ε-Hülle schrittweise, sieht man sehr schön, wie sich die Diagonale von εs wie eine Welle nach rechts oben ausbreitet, bis das obere Dreieck der Matrix C gefüllt ist.

Das war die nicht so gute Nachricht; die wirklich schlechte Nachricht betrifft die Laufzeit der Akzeptoren. Betrachten wir eine Variante des obigen Beispiels: $(\mathsf{a} \mid \varepsilon)^n \cdot \mathsf{a}^n$ beschreibt die Sprache aller Wörter der Form a^k mit $n \leqslant k \leqslant 2n$. (Da der reguläre Ausdruck keine Wiederholung verwendet, gibt es kein Terminierungsproblem, so dass wir aus Gründen der Übersichtlichkeit auf die Berechnung der ε-Hülle verzichten. Die Laufzeit ist unabhängig davon, welche Akzeptorvariante wir verwenden.)



An den rot markierten Knoten im Syntaxdiagramm werden wir vor eine Alternative gestellt: entweder ein a zu konsumieren oder ohne Änderung der Eingabe zum nächsten Knoten zu gehen. Der Kombinator *alt* geht an dieser Stelle nach dem ***Versuch-und-Irrtums Prinzip*** vor (engl. trial and error).

```
let alt (acc1, acc2) = fun inp → acc1 inp || acc2 inp
```

Zunächst wird die erste Alternative ausprobiert — die aktuelle Eingabe *inp* und die zweite Alternative acc_2 werden auf dem Laufzeitstack hinterlegt (siehe Abschnitt 4.5). Wenn die erste Alternative fehlschlägt, werden die hinterlegten Daten vom Stack heruntergenommen und die zweite Alternative exploriert. Zum Zeitpunkt des Fehlschlags ist die Verarbeitung der Eingabe in der Regel weiter fortgeschritten. Aus diesem Grund müssen wir uns die Liste *inp* merken, so dass die Suche an der ursprünglichen Eingabeposition wieder aufgenommen werden kann. Da Schritte zurückgenommen und alternative Wege exploriert werden, heißt die zugrundeliegende algorithmische Methode auch ***Backtracking*** oder auf Deutsch Rückverfolgung.

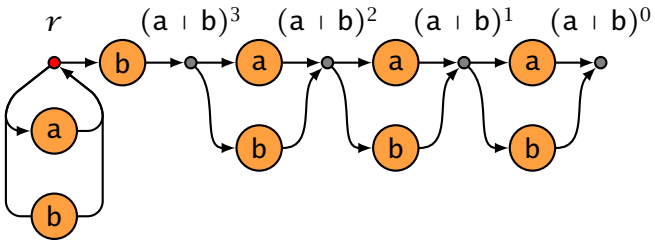
In unserem Beispiel ergibt sich für die Eingabe a^n, das kürzeste akzeptierte Wort, das folgende Bild. An jedem ***Entscheidungspunkt*** (engl. choice point) wird die erste Alternative verfolgt, so dass wir bis zum Knoten n gelangen. Hier löst der Kombinator *seq* einen Fehlschlag aus — das Zeichen a wird erwartet, aber die Eingabe ist leer. Wir »backtracken« und gehen nach links bis zum letzten Entscheidungspunkt, dem Knoten $n-1$. Dann geht es wieder nach rechts bis zum Knoten $n+1$. Wieder erfolgt ein Fehlschlag, wir »backtracken« bis zum Knoten $n-2$, dann geht es wieder nach rechts. Allerdings wird auf dem Weg nach rechts wieder ein Entscheidungspunkt an Position $n-1$ aufgebaut! So werden auf diese Weise insgesamt 2^n alternative Wege ausprobiert. Autsch.

Sequenzen von Alternativen wie $(\varepsilon \mid a_1) \cdot (\varepsilon \mid a_2) \cdot \ldots \cdot (\varepsilon \mid a_n)$ sind potentiell katastrophal. Wenn alle Buchstaben unterschiedlich sind, erzeugt der reguläre Ausdruck 2^n verschiedene Worte; sind alle Buchstaben gleich, sind es nur n Worte. *Aber:* Mittels Backtracking werden alle Möglichkeiten durchprobiert. Treten Fehlschläge erst spät auf, dann resultiert möglicherweise eine exponentielle Laufzeit. Unser Beispiel $(\mathsf{a} \mid \varepsilon)^n \cdot \mathsf{a}^n$ ist so konstruiert, dass ein Fehlschlag erst zum spätmöglichsten Zeitpunkt auftritt, nämlich dann, wenn die vollständige Eingabe a^n konsumiert wurde. So stochert der Akzeptor, der nur eine sehr lokale Sicht auf die Eingabe hat, sozusagen im Dunkeln.

Was ist zu tun? Eine radikale Idee: Anstatt die Alternativen nacheinander\sequentiell durchzuprobieren, verfolgen wir sie gleichzeitig\parallel.

6.3.5. Simulation nichtdeterministischer Automaten ohne ε-Übergänge⋆

Die parallele Graphsuche lässt sich prima an einer Verallgemeinerung der advPieb-Sprache illustrieren. Wir betrachten die Sprache aller Wörter über dem Alphabet $\{a, b\}$, die an der n-ten Position von hinten das Symbol b enthalten: $r := (a \mid b)^* \cdot b \cdot (a \mid b)^{n-1}$. Das kompaktestes Syntaxdiagramm für diese Sprache enthält $n+1$ Knoten: r selbst und und $(a \mid b)^i$ für $0 \leqslant i < n$, unten dargestellt für $n = 4$.



•○○○○	||abbaba
•○○○○	|a|bbaba
••○○○	|ab|baba
••●○○	|abb|aba
•○●●○	|abba|ba
••○●●	a|bbab|a
•○●○●	ab|baba|

Setzen wir die »Akzeptorbrille« auf und halten fest, dass der Akzeptor nichtdeterministisch ist: Im ersten Knoten, dem Startknoten, besteht eine Wahlmöglichkeit, wenn ein b gelesen wird. Entweder wir machen eine Rundreise (wir vermuten, dass dieses b nicht an der n-ten Position von hinten steht) oder wir fahren weiter nach rechts (wir spekulieren, dass wir das n-letzte Zeichen vor uns haben).

Die Abfolge auf der rechten Seite illustriert, wie die Eingabe abbaba verarbeitet wird. Wie bereits angedeutet, werden die Alternativen nicht sequentiell, sondern parallel verfolgt. Entsprechend befinden wir uns während der Verarbeitung der Eingabe nicht nur an einem Knoten, sondern möglicherweise an mehreren gleichzeitig — oben angezeigt durch schwarz gefüllte Kreise. Zum Beispiel bleiben wir stets im Startzustand, da uns jedes Zeichen in den Startzustand zurückführt. Der rechte senkrechte Strich markiert die Trennlinie zwischen den bereits verarbeiteten und den noch zu verarbeitenden Eingabezeichen. Die beiden Striche illustrieren das *endliche* Gedächtnis des Akzeptors: Um zu entscheiden, ob die Eingabe ein Element der Sprache $[\![r]\!]$ ist, muss sich der Akzeptor die jeweils n letzten Zeichen merken. Wenn Sie genau hinschauen, sehen Sie, dass sich diese Zeichenfolge im wahrsten Sinne des Wortes im Zustand wider*spiegelt* (wenn wir den Startzustand ignorieren): Befindet sich zum Beispiel bbab im »Sichtfenster«, dann lautet der Zustand •○•• — das Zeichen a korrespondiert zu ○ und b zu •.

Der Akzeptor unterhält eine *Menge* von Knoten, den »aktiven« Knoten. In jedem Schritt werden parallel alle Folgeknoten aller aktiven Knoten betrachtet. Witzigerweise müssen wir uns nicht besonders anstrengen, um die skizzierte parallele Graphsuche umzusetzen. Wir haben bereits alle Zutaten beisammen: Die von einem Syntaxdiagramm generierte Sprache ist $S \cdot M^* \cdot F$, wobei S und F beides ∅-ε-Vektoren sind, also *Mengen* von Knoten repräsentieren. Wir haben bisher noch keinen Gebrauch davon gemacht, dass mehrere Startknoten erlaubt sind — das ändert sich jetzt. Die Menge der »aktiven« Knoten entspricht einem Startvektor; ein paralleler Suchschritt korrespondiert zu einem Wechsel des Startvektors, bei unverändertem M und F. Zum Beispiel entspricht •○••○ dem Vektor $\begin{pmatrix}\varepsilon & \emptyset & \varepsilon & \varepsilon & \emptyset\end{pmatrix}$ und die obige Graphsuche korrespondiert zu der folgenden Abfolge von Wortproblemen:

$$
\begin{aligned}
& \mathsf{abbaba} \in \begin{pmatrix}\varepsilon & \emptyset & \emptyset & \emptyset & \emptyset\end{pmatrix} \cdot M^* \cdot F \\
\iff\ & \mathsf{bbaba} \in \begin{pmatrix}\varepsilon & \emptyset & \emptyset & \emptyset & \emptyset\end{pmatrix} \cdot M^* \cdot F \\
\iff\ & \mathsf{baba} \in \begin{pmatrix}\varepsilon & \varepsilon & \emptyset & \emptyset & \emptyset\end{pmatrix} \cdot M^* \cdot F \\
& \vdots \\
\iff\ & \mathsf{a} \in \begin{pmatrix}\varepsilon & \varepsilon & \emptyset & \varepsilon & \varepsilon\end{pmatrix} \cdot M^* \cdot F \\
\iff\ & \varepsilon \in \begin{pmatrix}\varepsilon & \emptyset & \varepsilon & \emptyset & \varepsilon\end{pmatrix} \cdot M^* \cdot F \\
\iff\ & \varepsilon \in \begin{pmatrix}\varepsilon & \emptyset & \varepsilon & \emptyset & \varepsilon\end{pmatrix} \cdot F
\end{aligned}
$$

Die letzte Sprache ist ε-haltig, so dass das Wort abbaba in der von $(\mathsf{a} \mid \mathsf{b})^* \cdot \mathsf{b} \cdot (\mathsf{a} \mid \mathsf{b})^3$ bezeichneten Sprache $L := S \cdot M^* \cdot F$ enthalten ist — wie erwartet.

In Abschnitt 6.2.1 haben wir gezeigt, dass sich das Wortproblem auf zwei Teilaufgaben reduzieren lässt: das ε-Problem (*nullable*) und die Berechnung von Rechtsfaktoren ($x \setminus L$). Weiterhin haben wir gezeigt, dass sich die *semantischen* Operationen auf der *syntaktischen* Repräsentation regulärer Sprachen, den regulären Ausdrücken, umsetzen lassen. Jetzt können wir das gleiche Programm für Syntaxdiagramme abspulen, einer alternativen Darstellung regulärer Sprachen. Dazu setzen wir die Multiplikation mit einem Wort und die Division durch ein Wort komponentenweise auf Matrizen fort — die Operationen firmieren auch unter den Namen ***Skalarmultiplikation*** bzw. ***-division***.

$$(w \cdot M)_{ij} = w \cdot M_{ij} \qquad (w \setminus M)_{ij} = w \setminus M_{ij}$$

Wenn die Übergangsmatrix N ε-frei ist und S und F beliebige ∅-ε-Vektoren sind, dann lassen sich die Rechtsfaktoren eines Syntaxdiagramms folgendermaßen berechnen:

$$x \setminus (S \cdot N^* \cdot F) = S \cdot (x \setminus N) \cdot N^* \cdot F \tag{6.20a}$$

Auch die Eigenschaft, ob eine Sprache ε-haltig ist, lässt sich an der Matrixdarstellung einfach festmachen:

$$\varepsilon \in S \cdot N^* \cdot F \quad \Longleftrightarrow \quad \varepsilon \in S \cdot F \tag{6.20b}$$

Die Äquivalenz besagt, dass die generierte Sprache genau dann ε enthält, wenn mindestens ein Startknoten gleichzeitig ein Zielknoten ist: $S \cdot F$. Da kein Eintrag von N ε-haltig ist, können wir die Hülle N^* sozusagen ignorieren.

Für unser laufendes Beispiel, die advPieb-Sprache,

$$S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \qquad N := \begin{pmatrix} \{\mathsf{a},\mathsf{b}\} & \{\mathsf{b}\} & \varnothing \\ \varnothing & \varnothing & \{\mathsf{a},\mathsf{b}\} \\ \varnothing & \varnothing & \varnothing \end{pmatrix} \qquad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \end{pmatrix}$$

ergeben sich die folgenden Rechtsfaktoren:

$$\mathsf{a} \setminus N = \begin{pmatrix} \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varepsilon \\ \varnothing & \varnothing & \varnothing \end{pmatrix} =: A \qquad \mathsf{b} \setminus N = \begin{pmatrix} \varepsilon & \varepsilon & \varnothing \\ \varnothing & \varnothing & \varepsilon \\ \varnothing & \varnothing & \varnothing \end{pmatrix} =: B$$

Aus den beiden ∅-ε-Matrizen können wir die ursprüngliche Übergangsmatrix rekonstruieren: $N = \mathsf{a} \cdot (\mathsf{a} \setminus N) \sqcup \mathsf{b} \cdot (\mathsf{b} \setminus N)$ — wir nehmen also lediglich einen Repräsentationswechsel vor. Mit Hilfe von A und B lässt sich das Wortproblem leicht lösen: abba ist zum Beispiel genau dann in der Sprache $(\mathsf{a} \mid \mathsf{b})^* \cdot \mathsf{b} \cdot (\mathsf{a} \mid \mathsf{b})$ enthalten, wenn $S \cdot A \cdot B \cdot B \cdot A \cdot F = \begin{pmatrix} \varepsilon \end{pmatrix}$ gilt. Das ist der Fall, wie die folgende Rechnung zeigt:

$$\begin{aligned}
&\begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \cdot A \cdot B \cdot B \cdot A \cdot F \\
=&\begin{pmatrix} \varepsilon & \varnothing & \varnothing \end{pmatrix} \cdot B \cdot B \cdot A \cdot F \\
=&\begin{pmatrix} \varepsilon & \varepsilon & \varnothing \end{pmatrix} \cdot B \cdot A \cdot F \\
=&\begin{pmatrix} \varepsilon & \varepsilon & \varepsilon \end{pmatrix} \cdot A \cdot F \\
=&\begin{pmatrix} \varepsilon & \varnothing & \varepsilon \end{pmatrix} \cdot F \\
=&\begin{pmatrix} \varepsilon \end{pmatrix}
\end{aligned}$$

Halten wir die Erkenntnis fest, dass sich das Wortproblem auf die Multiplikation von ∅-ε-Matrizen zurückführen lässt.

$$a_1 \dots a_n \in \mathrm{S} \cdot \mathrm{N}^* \cdot \mathrm{F} \quad \Longleftrightarrow \quad \varepsilon \in \mathrm{S} \cdot (a_1 \setminus \mathrm{N}) \cdot \dots \cdot (a_n \setminus \mathrm{N}) \cdot \mathrm{F} \tag{6.21}$$

Da die Matrizenmultiplikation assoziativ ist, kann das Matrixprodukt auf der rechten Seite ganz verschieden ausgerechnet werden: »streng von links nach rechts« — wenn wir die Eingabe von links nach rechts abarbeiten, »streng von rechts nach links« — wenn wir die Eingabe entsprechend von rechts nach links durchlaufen, »mittig« — wenn wir die Eingabe aufteilen, gegebenenfalls wiederholt, um sie parallel zu verarbeiten.

Implementierung Wenden wir uns der Implementierung des »Simulators« zu; dabei konzentrieren wir uns auf die Beschreibung der Automaten — der gesamte Quellcode inklusive einiger Beispiele ist in Abbildung 6.15 aufgeführt.

Ein ∅-ε-Vektor wird sehr direkt durch ein Array von Wahrheitswerten repräsentiert; dabei wird ∅ durch *false* und ε durch *true* dargestellt.[15] Um das Vektor-Matrix-Produkt einfach realisieren zu können, repräsentieren wir eine ∅-ε-Matrix durch ein Array von Spaltenvektoren. Dabei implementiert die Operation <*> das Skalarprodukt zweier Boolescher Vektoren, einem Zeilenvektor und einem Spaltenvektor:

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = (x_1 \wedge y_1) \vee (x_2 \wedge y_2) \vee \dots \vee (x_n \wedge y_n)$$

Ein Automat wird durch ein Record mit drei Komponenten beschrieben: dem Startvektor, einer Funktion, die jedem Zeichen x die Übergangsmatrix $x \setminus \mathrm{N}$ zuordnet, und dem Zielvektor.

```
type Automaton<'a> =                    // S · N* · F
  {
    start : bool array                  // Zeilenvektor S
    move : 'a → bool array array        // Zeichen auf Rechtsfaktor x ↦ x \ N
    final : bool array                  // Spaltenvektor F
  }
```

Der Typ ist mit dem Alphabet *'a* parametrisiert. (Falls Sie sich wundern, die Knoten des Syntaxdiagramms treten nicht in Erscheinung — ein attraktives Feature der Matrixdarstellung.)

Der generische Akzeptor ist nach dem Entwurfsmuster für Listen gestrickt — damit stellt sich ein warmes, wohliges Gefühl ein.

```
let generic-accept (automaton : Automaton<'a>) : 'a list → bool =
  let rec accept X = function
    | [ ]     → X <*> automaton.final
    | c :: cs → accept ⟦for col in automaton.move c → X <*> col⟧ cs
  in accept automaton.start
```

Das Argument X der Arbeitsfunktion *accept* repräsentiert die Menge der aktiven Knoten. Ist die Eingabe leer, so geben wir das Produkt aus X und dem Zielvektor zurück (6.20b). Anderenfalls

[15] *Math Fun Fact:* Die Kleene Algebra der Sprachen über dem leeren Alphabet $\mathcal{P}(\emptyset^*)$ ist isomorph zur Kleene Algebra der Wahrheitswerte, der sogenannten Erreichbarkeitsalgebra, siehe Abschnitt 5.5.1. Der Repräsentationswechsel entspricht dem Homomorphism $\mathrm{L} \mapsto \varepsilon \in \mathrm{L}$.

```
// Skalarprodukt: Ergebnis ist ein Skalar
let (<*>) row col = Array.fold2 (fun s x y → s || x && y) false row col
// Generischer, nichtdeterministischer Akzeptor.
type Automaton<'a> =                    // S · N* · F
  {
    start : bool array                  // Zeilenvektor S
    move : 'a → bool array array        // Zeichen auf Rechtsfaktor x ↦ x \ N
    final : bool array                  // Spaltenvektor F
  }
let generic-accept (automaton : Automaton<'a>) : 'a list → bool =
  let rec accept X = function
    | [ ]    → X <*> automaton.final
    | c :: cs → accept [[for col in automaton.move c → X <*> col]] cs
  in accept automaton.start
```

```
(* Beispiele *)
type Alphabet = | A | B
let PenultimateIsB : Automaton<Alphabet> = {          // r = (a | b)* · b · (a | b)
  start = [[true; false; false]]
  move = let aN = [[[true; false; false]]; [[false; false; false]]; [[false; true; false]]]
         let bN = [[[true; false; false]]; [[true; false; false]]; [[false; true; false]]]
         function | A → aN | B → bN
  final = [[false; false; true]] }
let Between30and60As : Automaton<Alphabet> = {        // (a | ε)^30 a^30
  start = [[for i in 1..61 → i = 1]]
  move = let aN = [[for j in 1..61 →
                     [[for i in 1..61 →
                       if    i ⩽ 30 then i + 1 ⩽ j && j ⩽ 32
                       elif  i ⩽ 60 then i + 1 = j
                       else              false]]]
         let bN = [[for j in 1..61 →
                     [[for i in 1..61 → false]]]]
         function | A → aN | B → bN
  final = [[for i in 1..61 → i = 61]] }
```

Abbildung 6.15.: Simulation nichtdeterministischer Automaten.

berechnen wir das Vektor-Matrix-Produkt von X und $c \setminus \mathrm{N}$ (6.20a). Da die Matrix durch eine Folge von Spaltenvektoren gegeben ist, geht das leicht von der Hand: Ist R ein Zeilenvektor und A eine Matrix in Spaltenform, dann berechnet $[\![\textit{for } C \textit{ in } A \to R \mathbin{<\!\!*\!\!>} C]\!]$ das Produkt $\mathrm{R} \cdot \mathrm{A}$, siehe auch Abbildung 4.1.

Da die Laufzeit des Skalarprodukts $<\!\!*\!\!>$ linear in der Größe der beteiligten Vektoren ist, benötigt das Vektor-Matrix-Produkt insgesamt eine quadratische Laufzeit. Die Operation bestimmt wesentlich die Laufzeit des Akzeptors: $n \cdot |r|^2$, wobei n die Länge der Eingabe und $|r|$ die Größe des regulären Ausdrucks r ist.

Um ein einzelnes Zeichen zu verarbeiten, werden also quadratisch viele Schritte benötigt. Der Aufwand lässt sich drücken, wenn wir die Zustände nicht zur ***Laufzeit*** bestimmen, sondern die Berechnung in die ***Übersetzungszeit*** verschieben. Der nächste Abschnitt greift diese Idee auf und erzählt die Geschichte der deterministischen Automaten ein zweites Mal. Am Ende schließt sich der Kreis und wir kehren zu den Akzeptoren aus Abschnitt 6.2.1 zurück.

6.3.6. Deterministische Automaten⋆

Wenden wir uns wieder der Kombinatorbibliothek aus Abschnitt 6.3.3 zu. Die auf Backtracking basierten Akzeptoren lassen sich etwas verbessern, indem wir mit Hilfe des Distributivgesetzes $a \cdot \mathrm{L}_i \cup a \cdot \mathrm{L}_j = a \cdot (\mathrm{L}_i \cup \mathrm{L}_j)$ gemeinsame Faktoren herausziehen. Für unser laufendes Beispiel, der advPieb-Sprache (6.19), erhalten wir das folgende Gleichungssystem:

$$\begin{aligned} \mathrm{L}_2 &= \mathsf{a} \cdot \mathrm{L}_2 \cup \mathsf{b} \cdot \mathrm{L}_2 \cup \mathsf{b} \cdot \mathrm{L}_4 \\ \mathrm{L}_4 &= \mathsf{a} \cdot \mathrm{L}_5 \cup \mathsf{b} \cdot \mathrm{L}_5 \\ \mathrm{L}_5 &= \varepsilon \end{aligned} \quad\Longrightarrow\quad \begin{aligned} \mathrm{L}_2 &= \mathsf{a} \cdot \mathrm{L}_2 \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4) \\ \mathrm{L}_4 &= \mathsf{a} \cdot \mathrm{L}_5 \cup \mathsf{b} \cdot \mathrm{L}_5 \\ \mathrm{L}_5 &= \varepsilon \end{aligned} \tag{6.22}$$

Auf diese Weise wird in L_2 das Zeichen b nur einmal mit der Eingabe abgeglichen, im Programm: $\mathit{seq}\ (B, \mathit{alt}\ (\mathit{acc}_2, \mathit{acc}_4))$, und nicht wie in Abschnitt 6.3.4 zweimal hintereinander, $\mathit{alt}\ (\mathit{seq}\ (B, \mathit{acc}_2), \mathit{seq}\ (B, \mathit{acc}_4))$. Da der gemeinsame Faktor, das Zeichen b, nach links herausgezogen wird, spricht man auch von ***Linksfaktorisierung***, einer allgemeinen Optimierung im Kontext von Sprachen und Sprachbeschreibungssprachen.

Wir machen eine interessante Beobachtung: Aus der Gleichung für L_2 lassen sich unmittelbar die ***Rechtsfaktoren*** ablesen und man sieht direkt, ob L_2 ε-haltig ist: $\mathsf{a} \setminus \mathrm{L}_2 = \mathrm{L}_2$, $\mathsf{b} \setminus \mathrm{L}_2 = \mathrm{L}_2 \cup \mathrm{L}_4$ und $\mathit{nullable}(\mathrm{L}_2) = \mathit{false}$. Auch die Rechtsfaktoren von $\mathrm{L}_2 \cup \mathrm{L}_4$ sind schnell ermittelt: Wir vereinigen die rechten Seiten der entsprechenden Gleichungen und *gruppieren* anschließend nach den Symbolen.

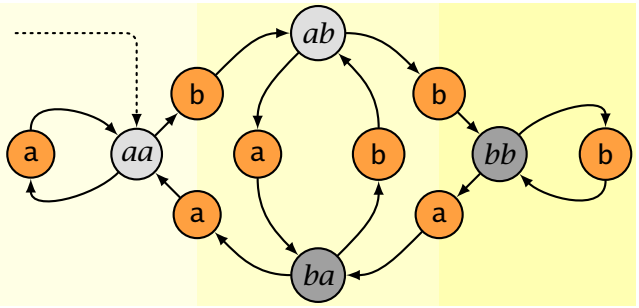
$$\mathrm{L}_2 \cup \mathrm{L}_4 = (\mathsf{a} \cdot \mathrm{L}_2 \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4)) \cup (\mathsf{a} \cdot \mathrm{L}_5 \cup \mathsf{b} \cdot \mathrm{L}_5) = \mathsf{a} \cdot (\mathrm{L}_2 \cup \mathrm{L}_5) \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4 \cup \mathrm{L}_5)$$

Zwei weitere Rechtsfaktoren treten auf: $\mathrm{L}_2 \cup \mathrm{L}_5$ und $\mathrm{L}_2 \cup \mathrm{L}_4 \cup \mathrm{L}_5$. Da $\mathrm{L}_5 = \varepsilon$ ist, kommen aber keine weiteren hinzu und wir erhalten das folgende Gleichungssystem.

$$\begin{aligned} \mathrm{L}_2 &= \mathsf{a} \cdot \mathrm{L}_2 \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4) \\ \mathrm{L}_2 \cup \mathrm{L}_4 &= \mathsf{a} \cdot (\mathrm{L}_2 \cup \mathrm{L}_5) \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4 \cup \mathrm{L}_5) \\ \mathrm{L}_2 \cup \mathrm{L}_5 &= \mathsf{a} \cdot \mathrm{L}_2 \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4) \cup \varepsilon \\ \mathrm{L}_2 \cup \mathrm{L}_4 \cup \mathrm{L}_5 &= \mathsf{a} \cdot (\mathrm{L}_2 \cup \mathrm{L}_5) \cup \mathsf{b} \cdot (\mathrm{L}_2 \cup \mathrm{L}_4 \cup \mathrm{L}_5) \cup \varepsilon \end{aligned} \tag{6.23}$$

Das Gleichungssystem lässt sich etwas lesbarer aufschreiben, wenn wir den Vereinigungen jeweils einen Namen geben. (Erkennen Sie die Systematik?)

$$
\begin{aligned}
L_{aa} &= a \cdot L_{aa} \cup b \cdot L_{ab} \\
L_{ab} &= a \cdot L_{ba} \cup b \cdot L_{bb} \\
L_{ba} &= a \cdot L_{aa} \cup b \cdot L_{ab} \cup \varepsilon \\
L_{bb} &= a \cdot L_{ba} \cup b \cdot L_{bb} \cup \varepsilon
\end{aligned}
$$



Voilà. Betrachten wir die Gleichungen auf der linken Seite bzw. das dazugehörige Syntaxdiagramm auf der rechten Seite durch die »Akzeptorbrille«, erkennen wir einen *deterministischen* Automaten: In jedem Knoten (Zustand) gibt es in Abhängigkeit vom nächsten Eingabezeichen genau einen Folgeknoten (Folgezustand). Überführen wir die Gleichungen in ein Programm, erhalten wir den gleichen Akzeptor für $(a \mid b)^* \cdot b \cdot (a \mid b)$ wie in Abschnitt 6.2.1 — das obige Syntaxdiagramm entspricht dem in Abbildung 6.4 dargestellten Aufrufgraphen!

```
module PenultimateSymbolIsB =          // (a | b)* · b · (a | b)
  let rec acc_aa inp = alt (seq (A, acc_aa), seq (B, acc_ab))                    inp
  and     acc_ab inp = alt (seq (A, acc_ba), seq (B, acc_bb))                    inp
  and     acc_ba inp = alt (alt (seq (A, acc_aa), seq (B, acc_ab)), end-of-input) inp
  and     acc_bb inp = alt (alt (seq (A, acc_ba), seq (B, acc_bb)), end-of-input) inp
  let accept = acc_aa
```

Im Vergleich zu Abschnitt 6.2.1 ist der Programmcode etwas kompakter, da an die Stelle der länglichen ***match***-Ausdrücke die Kombinatoren *alt* und *seq* getreten sind.

Halten wir fest: Das Gleichungssystem $\boldsymbol{L} = N \cdot \boldsymbol{L} \cup F$ enthält alle Informationen über die Rechtsfaktoren der Sprache $S \cdot \boldsymbol{L}$; jeder Rechtsfaktor ergibt sich als Vereinigung von ***Teilfaktoren***, den Einträgen des Sprachvektors $\boldsymbol{L}$. Damit ist klar, dass ein regulärer Ausdruck r nur endlich viele semantisch verschiedene Rechtsfaktoren besitzen kann! Die Rechtsfaktoren von r besitzen darüber hinaus eine einfache syntaktische Form: Wir haben in Abschnitt 6.3.2 gesehen, dass die Teilfaktoren Konkatenationen von Teilausdrücken von r sind; somit lässt sich jeder Rechtsfaktor als *Vereinigung von Konkatenationen von Teilausdrücken* von r schreiben. Damit haben wir den schwierigen Teil der merkenswerten

Charakterisierung regulärer Sprachen

Eine Sprache ist genau dann regulär, wenn sie endlich viele Rechtsfaktoren besitzt.

nachgewiesen. Um umgekehrt zu zeigen, dass eine Sprache mit endlich vielen Rechtsfaktoren regulär ist, erstellen wir ein Syntaxdiagramm, dargestellt als Gleichungssystem. Zunächst einmal wird jede Sprache durch zwei Angaben eindeutig charakterisiert: durch ihre direkten Rechtsfaktoren und durch die Angabe, ob sie ε-haltig ist.

$$L = (L \cap \varepsilon) \cup \bigcup_{a \in \mathbb{A}} a \cdot (a \setminus L) \tag{6.24}$$

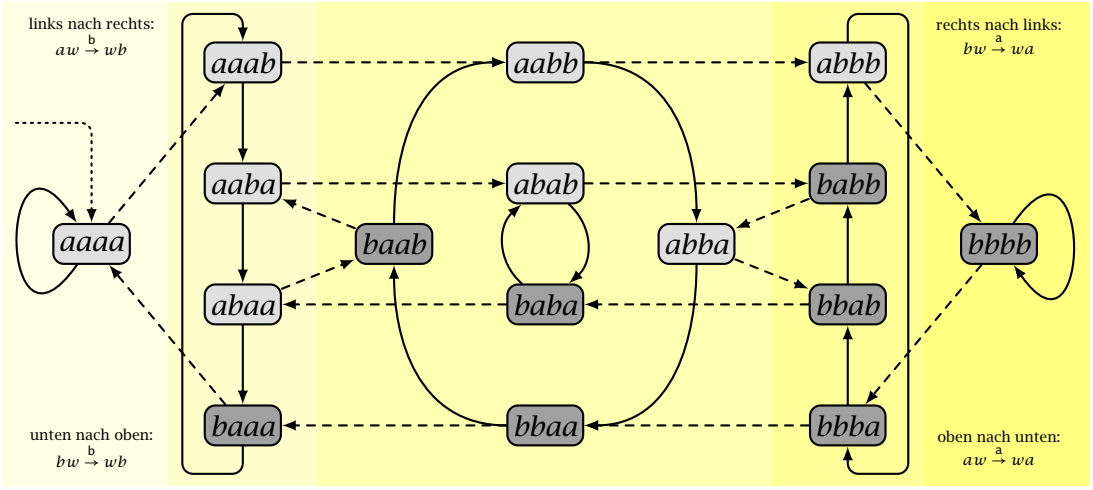
Besitzt eine Sprache L nur endlich viele verschiedene Rechtsfaktoren, so können wir ein endliches Gleichungssystem aufstellen, indem wir (6.24) auf die Sprache und ihre Rechtsfaktoren anwenden: $L = S \cdot \boldsymbol{L}$ mit $\boldsymbol{L} = N \cdot \boldsymbol{L} \cup F$. Da die Adjazenzmatrix N ε-frei ist, hat das Gleichungssystem eine eindeutige Lösung. Anders ausgedrückt: Das Syntaxdiagramm generiert die Sprache L, die

folglich regulär ist. Für die advPieb-Sprache L_{aa} erhalten wir zum Beispiel:

$$\begin{aligned} L_{aa} &= \mathsf{a} \cdot L_{aa} \cup \mathsf{b} \cdot L_{ab} \\ L_{ab} &= \mathsf{a} \cdot L_{ba} \cup \mathsf{b} \cdot L_{bb} \\ L_{ba} &= \mathsf{a} \cdot L_{aa} \cup \mathsf{b} \cdot L_{ab} \cup \varepsilon \\ L_{bb} &= \mathsf{a} \cdot L_{ba} \cup \mathsf{b} \cdot L_{bb} \cup \varepsilon \end{aligned} \qquad S := \begin{pmatrix} \varepsilon & \varnothing & \varnothing & \varnothing \end{pmatrix} \quad N := \begin{array}{c} \\ L_{aa} \\ L_{ab} \\ L_{ba} \\ L_{bb} \end{array} \begin{array}{c} \begin{array}{cccc} L_{aa} & L_{ab} & L_{ba} & L_{bb} \end{array} \\ \begin{pmatrix} \{\mathsf{a}\} & \{\mathsf{b}\} & \varnothing & \varnothing \\ \varnothing & \varnothing & \{\mathsf{a}\} & \{\mathsf{b}\} \\ \{\mathsf{a}\} & \{\mathsf{b}\} & \varnothing & \varnothing \\ \varnothing & \varnothing & \{\mathsf{a}\} & \{\mathsf{b}\} \end{pmatrix} \end{array} \quad F := \begin{pmatrix} \varnothing \\ \varnothing \\ \varepsilon \\ \varepsilon \end{pmatrix}$$

Programmgröße und Laufzeit Abbildung 6.16 fasst die verschiedenen Transformationen noch einmal zusammen und setzt sie zu den verschiedenen Akzeptortypen in Beziehung. Die Überführung des Gleichungssystems (6.22) in das Gleichungssystem (6.23) — die Transformation eines nichtdeterministischen Akzeptors in einen deterministischen — illustriert die sogenannte ***Potenzmengenkonstruktion***. Warum Potenzmenge? Auf der linken Seite einer Gleichung steht nicht länger eine einzelne Sprache, $L \in \{L_1, \ldots, L_n\}$, sondern eine endliche Vereinigung von Sprachen: $\bigcup \mathcal{L}$ mit $\mathcal{L} \subseteq \{L_1, \ldots, L_n\}$ oder als Mengenmitgliedschaft ausgedrückt, $\mathcal{L} \in \mathcal{P}(\{L_1, \ldots, L_n\})$. Besteht das ursprüngliche Gleichungssystem aus n Gleichungen, dann kann das neue System maximal 2^n Gleichungen umfassen. Statt exponentieller Laufzeit droht jetzt exponentieller Platzbedarf! Aber kann der schlechteste Fall überhaupt auftreten? Leider ja:

Die Verallgemeinerung der advPieb-Sprache, mit der wir die parallele Graphsuche veranschaulicht haben, $(\mathsf{a} \mid \mathsf{b})^* \cdot \mathsf{b} \cdot (\mathsf{a} \mid \mathsf{b})^{n-1}$, illustriert den »worst case«. Erinnern wir uns: Der Menge der aktiven Knoten codiert die letzten n Zeichen der Eingabe; somit gibt es insgesamt 2^n verschiedene Konstellationen. Überführen wir den nichtdeterministischen in einen äquivalenten deterministischen Akzeptor, dann umfasst dieser entsprechend 2^n verschiedene Zustände. Das unten aufgeführte Diagramm zeigt den Automaten für $n = 4$.



Aus Gründen der Lesbarkeit haben wir die Kantenmarkierungen weggelassen; sie lassen sich jeweils aus den Knoten rekonstruieren: Die Kante von xw nach wy ist mit y beschriftet. Jeder Zustand ist entsprechend der Anzahl seiner bs einem farblich hervorgehobenen Bereich zugeordnet. Der mittlere Bereich enthält zum Beispiel $\binom{4}{2} = 6$ Zustände. Insgesamt gibt es

$$\binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 1 + 4 + 6 + 4 + 1 = 16 = 2^4$$

verschiedene Zustände. Zur Verdeutlichung sind die Kanten zwischen den Bereichen gestrichelt: Die Anzahl der bs ändert sich. Die Kanten innerhalb eines Bereichs sind durchgezogen: Da die

Nichtdeterministischer Akzeptor mit ε-Übergängen

Gleichungssystem: $\boldsymbol{L} = \mathrm{M} \cdot \boldsymbol{L} \cup \mathrm{F}$ mit $\mathrm{M} : \mathrm{V} \times \mathrm{V} \to \mathscr{P}(\mathbb{A}_\varepsilon)$ und $\mathrm{F} : \mathrm{V} \to \mathscr{P}(\{\varepsilon\})$. Insgesamt n Gleichungen der Form:

$$\mathrm{L} \quad = \quad a_1 \cdot \mathrm{L}_1 \cup \cdots \cup a_i \cdot \mathrm{L}_i \quad \cup \quad \mathrm{L}'_1 \cup \cdots \cup \mathrm{L}'_j \quad \cup \quad (\mathrm{L} \cap \varepsilon)$$

wobei a_1, ..., a_i *nicht* notwendigerweise verschiedene Symbole sind.

⇓ ε-Hülle

Nichtdeterministischer Akzeptor ohne ε-Übergänge

Gleichungssystem: $\boldsymbol{L} = \mathrm{N} \cdot \boldsymbol{L} \cup \mathrm{F}$ mit $\mathrm{N} : \mathrm{V} \times \mathrm{V} \to \mathscr{P}(\mathbb{A})$ und $\mathrm{F} : \mathrm{V} \to \mathscr{P}(\{\varepsilon\})$. Maximal n Gleichungen der Form:

$$\mathrm{L} \quad = \quad a_1 \cdot \mathrm{L}_1 \cup \cdots \cup a_i \cdot \mathrm{L}_i \quad \cup \quad (\mathrm{L} \cap \varepsilon)$$

wobei a_1, ..., a_i *nicht* notwendigerweise verschiedene Symbole sind.

⇓ Linksfaktorisierung

Nichtdeterministischer Akzeptor ohne ε-Übergänge

Maximal n Gleichungen der Form:

$$\mathrm{L} \quad = \quad a_1 \cdot (\bigcup \mathcal{L}_1) \cup \cdots \cup a_k \cdot (\bigcup \mathcal{L}_k) \quad \cup \quad (\mathrm{L} \cap \varepsilon)$$

wobei a_1, ..., a_k *verschiedene* Symbole sind und $\mathcal{L}_1, \ldots, \mathcal{L}_k \subseteq \{\mathrm{L}_1, \ldots, \mathrm{L}_n\}$.

⇓ Potenzmengenkonstruktion

Deterministischer Akzeptor

Maximal 2^n Gleichungen der Form:

$$\bigcup \mathcal{L} \quad = \quad a_1 \cdot (\bigcup \mathcal{L}_1) \cup \cdots \cup a_k \cdot (\bigcup \mathcal{L}_k) \quad \cup \quad (\mathrm{L} \cap \varepsilon)$$

wobei a_1, ..., a_k *verschiedene* Symbole sind und $\mathcal{L}, \mathcal{L}_1, \ldots, \mathcal{L}_k \subseteq \{\mathrm{L}_1, \ldots, \mathrm{L}_n\}$.

⇓ Ergänzung von Fehlerzuständen ($\mathbb{A}$ endlich)

Deterministischer Akzeptor

Maximal 2^n Gleichungen der Form:

$$\bigcup \mathcal{L} \quad = \quad a_1 \cdot (\bigcup \mathcal{L}_1) \cup \cdots \cup a_k \cdot (\bigcup \mathcal{L}_k) \quad \cup \quad b_1 \cdot \varnothing \cup \cdots \cup b_l \cdot \varnothing \quad \cup \quad (\mathrm{L} \cap \varepsilon)$$

wobei $\{a_1, \ldots, a_k, b_1, \ldots, b_l\} = \mathbb{A}$ *alle* Symbole sind (und alle verschieden sind).

Abbildung 6.16.: Nichtdeterministische und deterministische Akzeptoren.

Anzahl der bs gleich bleibt, bilden sie disjunkte Zyklen. Der mittlere Bereich enthält zum Beispiel zwei verschiedene Zyklen:

$$aabb \xrightarrow{a} abba \xrightarrow{a} bbaa \xrightarrow{b} baab \xrightarrow{b} aabb \qquad \text{und} \qquad abab \xrightarrow{a} baba \xrightarrow{b} abab$$

Es ist erhellend den deterministischen Akzeptor mit seinem nichtdeterministischen Gegenstück zu vergleichen (siehe Abschnitt 6.3.5). Der nichtdeterministische Akzeptor enthält nur $n+1$ Knoten. Einer der Knoten ist ein Entscheidungspunkt; sehen wir ein b in der Eingabe, müssen wir raten: Haben wir das n-letzte Zeichen vor uns oder nicht? (Der Akzeptor verfügt nur über eine lokale Sicht, insbesondere kennt er nicht die Länge der Eingabe.) Im Gegensatz dazu hat der deterministische Akzeptor alles unter Kontrolle. Dazu merkt er sich die letzten n Zeichen; ist die Eingabe abgearbeitet, muss er für die Antwort nur sein Gedächtnis bemühen. Dafür zahlen wir allerdings einen Preis: Für das Gedächtnis werden 2^n Knoten benötigt. Wir haben ein typisches Beispiel für einen sogenannten ***Zeit-Speicher-Kompromiss*** (engl. time-space tradeoff) vor uns — wir verbessern die Laufzeit (von exponentiell auf linear) auf Kosten des Speicherplatzes (von linear bzw. quadratisch auf exponentiell).

Apropos Laufzeit. Die deterministischen Akzeptoren aus Abschnitt 6.2.1 legen eine lineare Laufzeit an den Tag. Verwenden wir die Kombinatorbibliothek aus Abschnitt 6.3.3, verschlechtert sich diese etwas. Das liegt daran, dass wir anstelle von ***match***-Ausdrücken geschachtelte *alt*-Aufrufe verwenden, um den Folgeakzeptor zu bestimmen. Da die Fälle sequentiell durchprobiert werden, verursacht dieser Schritt Kosten proportional zur Anzahl der Symbole wohingegen ein ***match***-Ausdruck in konstanter Zeit abgearbeitet wird. Insgesamt ergibt sich somit eine Laufzeit von $n \cdot k$, wobei k die Anzahl der verschiedenen Symbole in dem gegebenen regulären Ausdruck ist.

Zusammenfassung Eine reguläre Sprache lässt sich unterschiedlich beschreiben:

- durch einen regulären Ausdruck: r;
- durch ein Syntaxdiagramm:
  - dargestellt als Vektor-Matrix-Produkt: $S \cdot M^* \cdot F$;
  - dargestellt als Gleichungssystem: $\boldsymbol{L} = M \cdot \boldsymbol{L} \cup F$.

Ein Syntaxdiagramm lässt sich als Generator oder als Akzeptor deuten. Durch die Generatorbrille sehen wir ein Diagramm als Abbildung, die zwei Knoten $v \in V$ und $w \in V$ die Sprache zuordnet, die auf dem Weg von v nach w generiert wird. Durch die Akzeptorbrille sehen wir ein Diagramm als ***nichtdeterministischen Automaten***, beschrieben durch eine ***Transitionsfunktion***, die jedem Zustand $v \in V$ in Abhängigkeit vom Eingabesymbol $a \in \mathbb{A}$ eine Menge von Folgezuständen zuordnet. Zwei Sichtweisen auf das gleiche mathematische Objekt, formal eingefangen durch die folgende Isomorphie.[16]

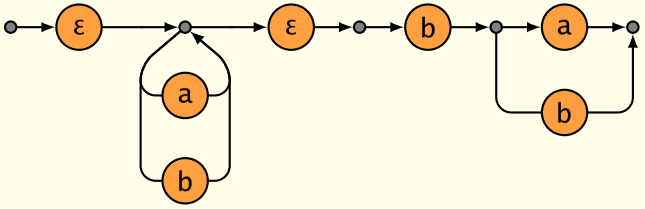
Generatorbrille		Akzeptorbrille
$V \times V \to \mathcal{P}(\mathbb{A})$	$\cong$	$\mathbb{A} \times V \to \mathcal{P}(V)$

Ein nichtdeterministischer Automat kann »sequentiell« mittels *Backtracking* simuliert werden oder »parallel«, indem Alternativen gleichzeitig verfolgt werden. Berechnet man die Zustandsmengen nicht dynamisch zur Laufzeit, sondern statisch zur Übersetzungszeit (Potenzmengenkonstruktion), so erhält man einen ***deterministischen Automaten***.

Abbildung 6.17 stellt die verschiedenen Darstellungen und die unterschiedlichen Automatentypen für unser laufendes Beispiel, die advPieb-Sprache, noch einmal gegenüber.

[16] Die Isomorphie basiert auf der Eins-zu-eins-Korrespondenz zwischen Relationen und mengenwertigen Funktionen, $\mathcal{P}(A \times B) \cong A \to \mathcal{P}(B)$.

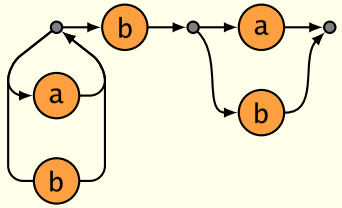
nichtdeterministischer Akzeptor mit ε-Übergängen



$$\begin{pmatrix} \varnothing & \varepsilon & \varnothing & \varnothing & \varnothing \\ \varnothing & \{a,b\} & \varepsilon & \varnothing & \varnothing \\ \varnothing & \varnothing & \varnothing & \{b\} & \varnothing \\ \varnothing & \varnothing & \varnothing & \varnothing & \{a,b\} \\ \varnothing & \varnothing & \varnothing & \varnothing & \varnothing \end{pmatrix}$$

$$\begin{aligned} L_1 &= L_2 \\ L_2 &= a \cdot L_2 \cup b \cdot L_2 \cup L_3 \\ L_3 &= b \cdot L_4 \\ L_4 &= a \cdot L_5 \cup b \cdot L_5 \\ L_5 &= \varepsilon \end{aligned}$$

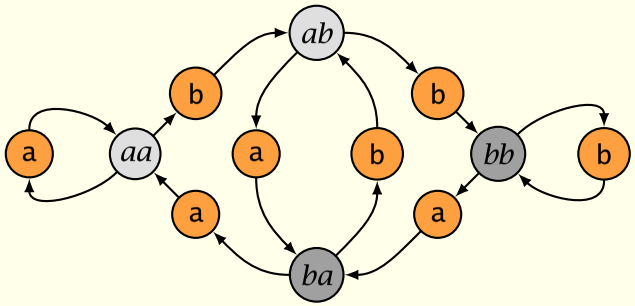
nichtdeterministischer Akzeptor ohne ε-Übergänge



$$\begin{pmatrix} \{a,b\} & \{b\} & \varnothing \\ \varnothing & \varnothing & \{a,b\} \\ \varnothing & \varnothing & \varnothing \end{pmatrix}$$

$$\begin{aligned} L_1 &= a \cdot L_1 \cup b \cdot L_1 \cup b \cdot L_2 \\ L_2 &= a \cdot L_3 \cup b \cdot L_3 \\ L_3 &= \varepsilon \end{aligned}$$

deterministischer Akzeptor



$$\begin{pmatrix} \{a\} & \varnothing & \{b\} & \varnothing \\ \{a\} & \varnothing & \{b\} & \varnothing \\ \varnothing & \{a\} & \varnothing & \{b\} \\ \varnothing & \{a\} & \varnothing & \{b\} \end{pmatrix}$$

$$\begin{aligned} L_{aa} &= a \cdot L_{aa} \cup b \cdot L_{ab} \\ L_{ab} &= a \cdot L_{ba} \cup b \cdot L_{bb} \\ L_{ba} &= a \cdot L_{aa} \cup b \cdot L_{ab} \cup \varepsilon \\ L_{bb} &= a \cdot L_{ba} \cup b \cdot L_{bb} \cup \varepsilon \end{aligned}$$

Abbildung 6.17.: Akzeptoren für die advPieb-Sprache: $(a \mid b)^* \cdot b \cdot (a \mid b)$.

6.4. Kontextfreie Grammatiken\kontextfreie Syntax

Wir haben in Abschnitt 6.1 gesehen, dass reguläre Ausdrücke nicht besonders ausdrucksstark sind. Syntaktische Hygienevorschriften wie »zu jeder offenen Klammer muss es eine korrespondierende schließende Klammer geben« lassen sich nicht formulieren.

$$\{\mathtt{a}^n\,\mathtt{b}^n \mid n \in \mathbb{N}\}$$

Die Sprache der wohlgeformten Klammerausdrücke lässt sich aber schrittweise (im Fachjargon: induktiv) definieren: ε ist wohlgeformt; wenn *w* wohlgeformt ist, dann auch a *w* b. Bei der Definition der Klammerausdrücke wird auf die definierte Sprache selbst zurückgegriffen. Mit einem Wort, wir benötigen ***Rekursion***. (Zur Erinnerung: Mini–F# erlaubt rekursiv definierte Funktionen und rekursiv definierte Varianten- und Recordtypen.) Hier erweitern wir reguläre Ausdrücke um rekursiv definierte Sprachen. Zum Beispiel wird die Sprache der wohlgeformten Klammerausdrücke durch den Ausdruck

rec $x \to \varepsilon \mid \mathtt{a}\ x\ \mathtt{b}$

beschrieben, der ziemlich direkt die obige Bildungsvorschrift einfängt. Wenn man möchte, kann man den Pfeil »→« als Implikation (»wenn …, dann …«) lesen: Wenn *x* ein Element der Sprache ist, dann auch ε und a *x* b.

Die Erweiterung von regulären Ausdrücken um Rekursion bekommt einen neuen Namen: Wir sprechen von ***kontextfreien Ausdrücken*** oder ***kontextfreien Grammatiken***.[17] Kontextfrei, weil der Bezeichner *x* in ***rec*** $x \to e$ ohne Einschränkungen, insbesondere ohne Berücksichtigung des jeweiligen Kontextes, verwendet werden kann. Neben regulären und kontextfreien Sprachen — das sind Sprachen, die durch reguläre bzw. kontextfreie Ausdrücke bezeichnet werden — gibt es auch ***kontextsensitive Sprachen***. Die Sprachfamilien formen eine strikte Hierarchie: Jede reguläre Sprache ist auch kontextfrei, jede kontextfreie Sprache auch kontextsensitiv, aber nicht umgekehrt. Mehr zu diesem Thema erfahren Sie später aus der Abteilung der Theoretischen Informatik.

Wir werden sehen, dass wir mit kontextfreien Ausdrücken die Syntax von Mini–F# hinreichend gut beschreiben können. Aber auch dieser Formalismus hat seine Grenzen: Kontextfreie Ausdrücke können eben keine kontextsensitiven Einschränkungen ausdrücken. Schauen wir uns ein kleines Beispiel an. Der folgende kontextfreie Ausdruck modelliert eine winzige Teilmenge von Mini–F#.

rec *expr* → `0` | `false` | *expr* + *expr*

Der Bezeichner *expr*, der stellvertretend für einen beliebigen Mini–F# Ausdruck steht, kann ohne Einschränkungen rechts verwendet werden. Wir erinnern uns: Mini–F# Ausdrücke sind beliebig kombinierbar. Insbesondere erlaubt die Grammatik, einen Booleschen Ausdruck, etwa `false`, in einem Kontext zu verwenden, in dem ein arithmetischer Ausdruck erwartet wird: `false + 0`. Diese Einschränkungen können wir nicht mit der kontextfreien Syntax ausdrücken. Müssen wir aber auch nicht; um diese Dinge kümmert sich ja gerade die statische Semantik. Durch die klare Trennung von Zuständigkeiten wird die Sprachdefinition von Mini–F# ungemein erleichtert.

6.4.1. Abstrakte Syntax

Kontextfreie Ausdrücke umfassen neben den Konstrukten regulärer Ausdrücke zusätzlich Bezeichner (auch ***Nichtterminalsymbole*** genannt) und Rekursion.

[17] Der Terminus »Grammatik« wird eigentlich für einen *anderen*, aber äquivalenten Formalismus verwendet. Wir missbrauchen den Fachbegriff im Folgenden, um nicht immer von einem »kontextfreien Ausdruck« sprechen zu müssen.

$x \in \mathsf{Ident}$

$c \in \mathsf{CF} ::=$		***kontextfreie Ausdrücke:***
	$\mid a$	einzelnes Zeichen\Terminalsymbol
	$\mid x$	Bezeichner\Nichtterminalsymbol
	$\mid \varepsilon$	das leere Wort
	$\mid c_1 \cdot c_2$	Konkatenation\Sequenz
	$\mid \emptyset$	die leere Sprache
	$\mid c_1 \mid c_2$	Alternative
	$\mid$ ***rec*** $x \to c$	Rekursion

Die Wiederholung ist kein primitives Konzept mehr; sie kann mit Hilfe der Rekursion ausgedrückt werden: c^* durch ***rec*** $x \to \varepsilon \mid c\ x$ oder ***rec*** $x \to \varepsilon \mid x\ c$. (Streng genommen ist auch $\emptyset$, das Symbol für die leere Sprache, redundant. Es kann — wie wir in Kürze sehen werden — mit ***rec*** $x \to x$ ausgedrückt werden.)

6.4.2. Reduktionssemantik

Kommen wir zur Semantik kontextfreier Ausdrücke. Wir haben motiviert, dass der Ausdruck ***rec*** $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$ die Sprache $\{\mathsf{a}^n\ \mathsf{b}^n \mid n \in \mathbb{N}\}$ bezeichnet. Dass dem so ist, leuchtet vielleicht unmittelbar ein. Aber ist auch die Bedeutung von ***rec*** $x \to x$, ***rec*** $x \to \mathsf{a}\ x\ \mathsf{b}$ oder ***rec*** $x \to x^*$ unmittelbar klar? Vielleicht, vielleicht aber auch nicht. Legen wir also die Semantik präzise fest, um die Bedeutung dieser »extremen« Beispiele ermitteln zu können. Semantik ist immer auch dazu da, Randfälle oder Extremfälle zu klären.

Diesmal fangen wir mit der ***Reduktionssemantik*** an, die — wir erinnern uns — eine lokale Sicht der Dinge vermittelt. Die Reduktionsregel für ***rec*** $x \to c$ formalisiert die Intuition. Ein rekursiver Ausdruck wird einmal »aufgefaltet«: Die Vorkommen von x in c werden durch den Ausdruck ***rec*** $x \to c$ selbst ersetzt, als Formel $c\{x \mapsto (\textbf{\textit{rec}}\ x \to c)\}$. Zu dem Beweissystem aus Abschnitt 6.1.2 kommt nur eine einzige Regel hinzu:

$$\frac{}{(\textbf{\textit{rec}}\ x \to c) \longrightarrow c\{x \mapsto (\textbf{\textit{rec}}\ x \to c)\}}$$

(Warum benötigen wir keine Regel für Bezeichner?)

Mit Hilfe dieser Regel können wir zum Beispiel aabb aus dem Ausdruck ***rec*** $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$ ableiten.

$$\begin{aligned}
& \textbf{\textit{rec}}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b} \\
\longrightarrow\ & \varepsilon \mid \mathsf{a}\ (\textbf{\textit{rec}}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b})\ \mathsf{b} \\
\longrightarrow\ & \mathsf{a}\ (\textbf{\textit{rec}}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b})\ \mathsf{b} \\
\longrightarrow\ & \mathsf{a}\ (\varepsilon \mid \mathsf{a}\ (\textbf{\textit{rec}}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b})\ \mathsf{b})\ \mathsf{b} \\
\longrightarrow\ & \mathsf{a}\ (\mathsf{a}\ (\textbf{\textit{rec}}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b})\ \mathsf{b})\ \mathsf{b} \\
\longrightarrow\ & \mathsf{a}\ (\mathsf{a}\ (\varepsilon \mid \mathsf{a}\ (\textbf{\textit{rec}}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b})\ \mathsf{b})\ \mathsf{b})\ \mathsf{b} \\
\longrightarrow\ & \mathsf{a}\ (\mathsf{a}\ \varepsilon\ \mathsf{b})\ \mathsf{b} \\
\longrightarrow\ & \mathsf{a}\ \mathsf{a}\ \mathsf{b}\ \mathsf{b}
\end{aligned}$$

Wie sieht es mit dem Ausdruck ***rec*** $x \to x$ aus? Nun, wir erhalten:

$$\begin{aligned}
& \textbf{\textit{rec}}\ x \to x \\
\longrightarrow\ & \textbf{\textit{rec}}\ x \to x \\
& \vdots
\end{aligned}$$

Man kann nicht behaupten, dass wir große Fortschritte erzielt haben: Der Rumpf x wird durch ***rec*** $x \to x$ ersetzt und wir erhalten wieder ***rec*** $x \to x$. Mit anderen Worten, wir können kein Wort ableiten; ***rec*** $x \to x$ bezeichnet demnach die leere Sprache. Das Gleiche gilt für den Ausdruck ***rec*** $x \to \mathsf{a}\ x\ \mathsf{b}$. Im Fall von ***rec*** $x \to x^*$ sieht es ein kleines bisschen »besser« aus.

$$
\begin{aligned}
& \textbf{\textit{rec}}\ x \to x^* \\
\longrightarrow\ & (\textbf{\textit{rec}}\ x \to x^*)^* \\
\longrightarrow\ & \varepsilon
\end{aligned}
$$

Ein anderes Wort lässt sich nicht ableiten. Also steht ***rec*** $x \to x^*$ für die Sprache $\{\varepsilon\}$.

Die Ersetzung von Bezeichnern durch kontextfreie Ausdrücke nennt man übrigens ***Substitution***: Ist c ein kontextfreier Ausdruck und $\theta \in \mathsf{Ident} \to_{\text{fin}} \mathsf{CF}$ eine endliche Abbildung von Bezeichnern auf Ausdrücke, dann bezeichnet $c\theta$ den Ausdruck, in dem die *frei* auftretenden Bezeichner aus $dom\ \theta$ durch die zugeordneten Ausdrücke ersetzt werden.

$$
\begin{aligned}
a\theta &= a \\
x\theta &= \begin{cases} \theta(x) & \text{falls } x \in dom\ \theta \\ x & \text{sonst} \end{cases} \\
\varepsilon\theta &= \varepsilon \\
(c_1 \cdot c_2)\theta &= (c_1\theta) \cdot (c_2\theta) \\
\varnothing\theta &= \varnothing \\
(c_1 \mid c_2)\theta &= (c_1\theta) \mid (c_2\theta) \\
(\textbf{\textit{rec}}\ x \to c)\theta &= \textbf{\textit{rec}}\ x \to c(\theta - \{x\})
\end{aligned}
$$

Ersetzen wir Bezeichner in dem Ausdruck ***rec*** $x \to c$, müssen wir sicherstellen, dass der *gebundene* Bezeichner x *nicht* ersetzt wird. Zum Beispiel ist $(\textbf{\textit{rec}}\ x \to x)\{x \mapsto \varepsilon\} =$ ***rec*** $x \to x$ und nicht etwa ***rec*** $x \to \varepsilon$. Zur Erinnerung: $\theta - \{x\}$ bezeichnet die ***Einschränkung*** von θ auf $dom\ \theta - \{x\}$. Oder positiv ausgedrückt: Eine Substitution ersetzt aus Hygienegründen nur *freie* Bezeichner.

6.4.3. Denotationelle Semantik

Kommen wir zur denotationellen Semantik, der Semantik, die eine globale Sicht vermittelt. Bei der Motivation von ***rec*** $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$ haben wir überlegt, wie sich zum Beispiel $\mathsf{a}^n\ \mathsf{b}^n$ schrittweise bilden lässt: aus ε wird ab, daraus wird aabb usw. Dieser Bildungsprozess lässt sich auch auf die *Sprache als Ganzes* übertragen. Aus dem Ausdruck ***rec*** $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$ leiten wir zunächst eine Funktion auf Sprachen ab.

$$F(L) = \{\varepsilon\} \cup \{\mathsf{a}\} \cdot L \cdot \{\mathsf{b}\}$$

Jetzt können wir uns der Semantik von ***rec*** $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$ durch wiederholte Anwendung von F ausgehend von der leeren Menge nähern.

$$
\begin{array}{lll}
\varnothing & & \\
F(\varnothing) & = \{\varepsilon\} \cup \{\mathsf{a}\} \cdot \varnothing \cdot \{\mathsf{b}\} & = \{\varepsilon\} \\
F(F(\varnothing)) & = \{\varepsilon\} \cup \{\mathsf{a}\} \cdot \{\varepsilon\} \cdot \{\mathsf{b}\} & = \{\varepsilon, \mathsf{ab}\} \\
F(F(F(\varnothing))) & = \{\varepsilon\} \cup \{\mathsf{a}\} \cdot \{\varepsilon, \mathsf{ab}\} \cdot \{\mathsf{b}\} & = \{\varepsilon, \mathsf{ab}, \mathsf{aabb}\} \\
F(F(F(F(\varnothing)))) & = \{\varepsilon\} \cup \{\mathsf{a}\} \cdot \{\varepsilon, \mathsf{ab}, \mathsf{aabb}\} \cdot \{\mathsf{b}\} & = \{\varepsilon, \mathsf{ab}, \mathsf{aabb}, \mathsf{aaabbb}\}
\end{array}
$$

Wir haben bewusst davon gesprochen, dass wir uns der Semantik *nähern*, da wir in endlich vielen Schritten niemals die unendliche Menge $\{\mathsf{a}^n\ \mathsf{b}^n \mid n \in \mathbb{N}\}$ konstruieren können. Mathematisch

lässt sich die Menge aber sehr wohl definieren, sie ergibt sich als Vereinigung aller endlichen Approximationen.

$$\bigcup\{F^n(\varnothing) \mid n \in \mathbb{N}\}$$

Hier bezeichnet $F^n(\varnothing)$ die n-fache Anwendung der Funktion F auf die leere Menge: $F^0(X) = X$ und $F^{n+1}(X) = F(F^n(X))$. Die obige Sprache, nennen wir sie S, hat die Eigenschaft, dass F sie unverändert lässt: $F(S) = S$. Man sagt auch, S ist ein ***Fixpunkt*** von F. Darüber hinaus ist S die *kleinste* Menge mit dieser Eigenschaft: S ist der ***kleinste Fixpunkt***. Kurz: Alles Notwendige ist drin, mehr aber nicht. Für den mathematischen Nachweis dieser Tatsache müssten wir etwas ausholen, was wir an dieser Stelle nicht tun wollen, siehe aber Aufgabe 6.4.3 und, wenn Sie das Thema vertiefen wollen, Anhang B.6.

Jetzt haben wir fast alles zusammen, um die semantischen Gleichungen der denotationellen Semantik aufzustellen. Wir müssen uns nur noch um die Bezeichner kümmern. Deren Bedeutung halten wir in einer Umgebung fest, die Bezeichner auf Sprachen abbildet.

$$\varrho \in \mathsf{Ident} \to_{\text{fin}} \mathscr{P}(A^*)$$

Die Semantikfunktion bildet einen kontextfreien Ausdruck, der innerhalb der Oxfordklammern steht, und eine Umgebung auf eine Sprache ab.

$$\begin{array}{ll}
[\![a]\!]\varrho & = \{a\} \\
[\![x]\!]\varrho & = \varrho(x) \\
[\![\varepsilon]\!]\varrho & = \{\varepsilon\} \\
[\![c_1\ c_2]\!]\varrho & = [\![c_1]\!]\varrho \cdot [\![c_2]\!]\varrho \\
[\![\varnothing]\!]\varrho & = \varnothing \\
[\![c_1 \mid c_2]\!]\varrho & = [\![c_1]\!]\varrho \cup [\![c_2]\!]\varrho \\
[\![\textbf{\textit{rec}}\ x \to c]\!]\varrho & = \bigcup\{F^n(\varnothing) \mid n \in \mathbb{N}\} \ \text{ mit } \ F(X) = [\![c]\!](\varrho, \{x \mapsto X\})
\end{array}$$

Die letzte Gleichung formalisiert die oben beschriebene Fixpunktsemantik: Aus dem Ausdruck ***rec*** $x \to c$ wird eine Funktion F auf Sprachen abgeleitet (»,« ist der Kommaoperator); deren kleinster Fixpunkt ist die Bedeutung des Ausdrucks. Ist die Umgebung leer, $\varrho = \varnothing$, schreiben wir $[\![c]\!]\varrho$ auch kurz als $[\![c]\!]$.

Gehen wir die »extremen« Beispiele noch einmal mit der denotationellen Semantik durch. Die dem Ausdruck ***rec*** $x \to x$ zugeordnete Funktion ist $F(L) = L$. Die Funktion hat unendlich viele Fixpunkte — jede Sprache ist Fixpunkt dieser Funktion. Der kleinste Fixpunkt ist die leere Sprache, somit ist $[\![\textbf{\textit{rec}}\ x \to x]\!] = \varnothing$. Ähnlich verhält es sich mit dem Ausdruck ***rec*** $x \to \mathsf{a}\ x\ \mathsf{b}$. Die zugehörige Funktion ist $G(L) = \{\mathsf{a}\} \cdot L \cdot \{\mathsf{b}\}$. Da $G(\varnothing) = \varnothing$ gilt, ist die Bedeutung von ***rec*** $x \to \mathsf{a}\ x\ \mathsf{b}$ ebenfalls die leere Sprache. Für das dritte Beispiel, ***rec*** $x \to x^*$, erhalten wir $H(L) = L^*$ mit

$$\begin{array}{l}
\varnothing \\
H(\varnothing) \quad = \varnothing^* \quad = \{\varepsilon\} \\
H(H(\varnothing)) = \{\varepsilon\}^* = \{\varepsilon\}
\end{array}$$

Damit ist $[\![\textbf{\textit{rec}}\ x \to x^*]\!] = \{\varepsilon\}$. Auch für kontextfreie Ausdrücke stimmen Reduktionssemantik und denotationelle Semantik überein.

6.4.4. Vertiefung: Syntax von Mini-F#

Im Folgenden spezifizieren wir schrittweise die kontextfreie Syntax von Mini-F#, eingeschränkt auf die in Kapitel 3 eingeführten Konstrukte. Dabei werden wir einige Schwierigkeiten zu bewältigen haben. Um diesen zu begegnen, wenden wir einige Tricks an und gehen verschiedene

Kompromisse ein. Beides erinnert noch einmal daran, dass die konkrete Syntax erstens technischen Einschränkungen unterworfen ist und zweitens den Geschmack der Sprachdesigner/-innen widerspiegelt.

Das zugrundeliegende Alphabet ist die Menge aller Mini-F# Lexeme. Wir verwenden *num* als Bezeichner für die Sprache aller Numerale, *string* steht entsprechend für die Sprache aller Stringliterale und *id* bzw. *Id* für kleine bzw. große Bezeichner. Alle anderen Lexeme notieren wir, wie in Abbildung 6.3 aufgeführt.

Versuchen wir uns an der kontextfreien Syntax einfacher arithmetischer Ausdrücke.

rec *expr* → *num* | *expr* + *expr* | *expr* * *expr*

Der kontextfreie Ausdruck ist an die Baumsprache für Ausdrücke angelehnt: Ein arithmetischer Ausdruck ist entweder ein Numeral, oder ein Ausdruck gefolgt von dem Symbol + gefolgt von einem weiteren Ausdruck, oder ein Ausdruck gefolgt von dem Symbol * gefolgt von einem weiteren Ausdruck. Aus dem kontextfreien Ausdruck lässt sich zum Beispiel das Wort `4711 + 815 * 2765` ableiten — wir kürzen den kontextfreien Ausdruck mit *E* ab und führen der Übersichtlichkeit halber nicht alle Reduktionsschritte auf:

E ⟶ *E* + *E*
⟶ *num* + *E*
⟶ 4711 + *E*
⟶ 4711 + *E* * *E*
⟶ 4711 + *num* * *E*
⟶ 4711 + 815 * *E*
⟶ 4711 + 815 * *num*
⟶ 4711 + 815 * 2765

Es gibt aber noch eine zweite mögliche Reduktionsfolge:

E ⟶ *E* * *E*
⟶ *E* + *E* * *E*
⟶ *num* + *E* * *E*
⟶ 4711 + *E* * *E*
⟶ 4711 + *num* * *E*
⟶ 4711 + 815 * *E*
⟶ 4711 + 815 * *num*
⟶ 4711 + 815 * 2765

Damit stehen wir dem ersten Problem gegenüber: Der obige kontextfreie Ausdruck ist ***mehrdeutig***; ein Wort kann auf verschiedene Weisen abgeleitet werden.[18] Warum ist das ein Problem? Nun, die kontextfreie Syntax dient einzig und allein dem Zweck, aus der linearen Folge von Lexemen die hierarchische Struktur eines Programms zu rekonstruieren. (Im nächsten Abschnitt sehen wir uns an, wie man *automatisch* die konkrete Syntax in die abstrakte Syntax überführt.) Die beiden unterschiedlichen Reduktionsfolgen legen aber einen unterschiedlichen hierarchischen Aufbau nahe: Die erste Reduktionsfolge sieht den Operator + oben, die zweite den Operator *. Entsprechend haben wir zwei abstrakte Syntaxbäume zur Auswahl.

[18] Diese Tatsache ist übrigens mit der denotationellen Semantik nicht fassbar, da jedem kontextfreien Ausdruck eine *Menge* und keine *Multimenge* zugeordnet wird.

Die Semantik ordnet den beiden Syntaxbäumen eine unterschiedliche Bedeutung zu. Kurzum: Der obige kontextfreie Ausdruck ist ungeeignet zur Beschreibung arithmetischer Ausdrücke, da er nicht jedem Ausdruck einen *eindeutigen* abstrakten Syntaxbaum zuordnet.

Was ist zu tun? Nun, wir können die Syntax von Mini–F# Ausdrücken überdenken und zum Beispiel arithmetische Operatoren nicht zwischen die Operatoren schreiben, sondern davor oder dahinter. Entsprechend der Position spricht man von ***Präfix-***, ***Infix-*** oder ***Postfixnotation***. Präfix- und Postfixnotation lassen sich wie folgt einfangen:

rec *expr* → *num* | + *expr expr* | * *expr expr*

rec *expr* → *num* | *expr expr* + | *expr expr* *

Beide Syntaxen sind ***eindeutig***. Wir haben in Abschnitt 2.2 erwähnt, dass die Programmiersprache ***Scheme*** Präfixnotation und die Programmiersprache ***PostScript*** Postfixnotation verwendet. Die allermeisten Sprachen notieren aber — wie auch Mini–F# — Operatoren infix. Warum? Wahrscheinlich, weil sie der mathematischen Tradition folgen. Das ist natürlich nur eine halbwegs befriedigende Antwort, klärt sie doch nicht, warum die Notation tatsächlich sinnvoll ist. Um den Gründen auf die Spur zu kommen, betrachten wir eine Summe aus drei Zahlen:

```
4711 + 815 + 2765
```

Notieren wir die Operatoren präfix, dann gibt es zwei alternative Ausdrücke, `+ 4711 + 815 2765` und `+ + 4711 815 2765`. Für die Postfixnotation gilt das gleiche. Semantisch sind beide Ausdrücke aber gleich, da die Addition *assoziativ* ist. Präfix- und Postfixnotation machen also einen Unterschied, wo es keinen gibt! Allein die Infixnotation stellt uns nicht vor die Wahl.

Assoziative Operatoren und Funktionen sind zahlreich: Disjunktion (||), Konjunktion (&&), Addition (+), Multiplikation (∗), Konkatenation von Strings (^), Minimum (*min*), Maximum (*max*), Konkatenation von Listen (@), der Kommaoperator (»,«) sind Vertreter dieser Gattung. Wir sehen: Nicht alle assoziativen Funktionen notieren wir tatsächlich infix, bei allen würde es sich aber anbieten.

Wo Licht ist, ist auch Schatten. Es hat sich eingebürgert, auch nicht-assoziative Funktionen, wie zum Beispiel die Subtraktion infix zu notieren: `– 4711 – 815 2765` und `– – 4711 815 2765` sind sehr wohl unterschiedlich und die Infixschreibweise

```
4711 – 815 – 2765                                                    (6.25)
```

klärt nicht, welche Variante gemeint ist. Ähnliches gilt für die Potenzfunktion (wenn wir uns entschließen, *power* (x, n) infix zu notieren, etwa als x ** n). An dieser Stelle bedarf es einer Festlegung: Wir müssen vereinbaren, was mit (6.25) gemeint ist. Die Subtraktion wird allgemein als ***linksassoziierend***[19] festgelegt (a – b – c steht für – – a b c), die Potenzfunktion als ***rechtsassoziierend*** (a ** b ** c steht für ** a ** b c).[20] Was aber machen wir, wenn wir die andere Variante benötigen, die wir ja infix nicht ausdrücken können? In diesem Fall behilft man sich mit Klammern die die Gruppierung explizit machen:

```
4711 – (815 – 2765)
```

Wir erinnern uns: Klammern sind ein Hilfsmittel der konkreten Syntax. Mit ihrer Hilfe lassen sich die Begriffe links- und rechtsassoziierend noch einmal verdeutlichen: Ist ein Operator ⊕

[19] Diese syntaktische Konvention wird manchmal auch als »linksassoziativ« bezeichnet; wir vermeiden diesen Begriff, da er zu sehr nach der semantischen Eigenschaft »assoziativ« klingt.

[20] Eine solche Festlegung kann übrigens auch im Fall assoziativer Funktionen sinnvoll sein. Nämlich dann, wenn eine Variante effizienter ist als die andere. Ein Beispiel hierfür liefert die Konkatenation von Listen: $xs_1 @ (xs_2 @ xs_3)$ und $(xs_1 @ xs_2) @ xs_3$ sind zwar gleichwertig, aber der erste Ausdruck ist schneller ausgerechnet. (Warum?)

linksassoziierend, dann meint $a \oplus b \oplus c$ den Ausdruck $(a \oplus b) \oplus c$ — Klammern links — ist der Operator rechtsassoziierend, dann ist der Ausdruck $a \oplus (b \oplus c)$ gemeint — Klammern rechts.

Bislang haben wir nur einen Operator für sich betrachtet. Bietet eine Sprache mehrere Operatoren an, dann muss man weiterhin klären, was passiert, wenn zwei Operatoren aufeinandertreffen. Damit kommen wir zu unserem Ausgangsbeispiel zurück.

```
4711 + 815 * 2765
```

Ist damit `(4711 + 815) * 2765` oder `4711 + (815 * 2765)` gemeint? Gängige Konvention — Punkt- vor Strichrechnung — gibt der zweiten Alternative den Vorzug. Hat man zwei beliebige Operatoren vor sich, zum Beispiel $\oplus$ und $\otimes$, so lässt sich der Konflikt mit Hilfe der sogenannten ***Bindungsstärke*** lösen.

$$a \oplus b \otimes c$$

Man stellt sich vor, dass $\oplus$ und $\otimes$ um den Operanden b streiten; der Operator mit der höheren Bindungsstärke zieht ihn an sich: Hat $\oplus$ die höhere Bindungsstärke, dann ist der Ausdruck $(a \oplus b) \otimes c$ gemeint, hat $\otimes$ die höhere Bindungsstärke, dann der Ausdruck $a \oplus (b \otimes c)$.

Zurück zu unserer Aufgabe, der Aufstellung einer Syntax für arithmetische Ausdrücke. Wir können den kontextfreien Ausdruck E eindeutig machen, indem wir unser neu erworbenes Wissen über Operatoren in die Beschreibung »hineinprogrammieren«. Die grundlegende Idee ist, eine Hierarchie E_i von Sprachen zu definieren, so dass E_i nur Ausdrücke umfasst, deren oberster Operator eine Bindungsstärke von i oder mehr hat. Konkret: E_0 umfasst alle Ausdrücke, E_1 nur Produkte und E_2 nur atomare oder geklammerte Ausdrücke.

$$\begin{array}{ll} \textbf{\textit{rec}} & expr_0 \to expr_1 \mid expr_1 + expr_0 \\ \textbf{\textit{and}} & expr_1 \to expr_2 \mid expr_2 * expr_1 \\ \textbf{\textit{and}} & expr_2 \to num \mid \texttt{(}\ expr_0\ \texttt{)} \end{array}$$

Die Grammatik ist ***verschränkt rekursiv***: Alle Bezeichner sind in allen rechten Seiten sichtbar. Die Bedeutung der Grammatik ist durch die Bedeutung des ersten Bezeichners gegeben (oben $expr_0$). Die Grammatik ist jetzt eindeutig: Jeder arithmetische Ausdruck lässt sich auf genau eine Art und Weise ableiten. Zum Beispiel (E_i kürzt $expr_i$ ab):

$$\begin{aligned} E_0 &\longrightarrow E_1 + E_0 \\ &\longrightarrow E_2 + E_0 \\ &\longrightarrow num + E_0 \\ &\longrightarrow 4711 + E_0 \\ &\longrightarrow 4711 + E_1 \\ &\longrightarrow 4711 + E_2 * E_1 \\ &\longrightarrow 4711 + num * E_1 \\ &\longrightarrow 4711 + 815 * E_1 \\ &\longrightarrow 4711 + 815 * E_2 \\ &\longrightarrow 4711 + 815 * num \\ &\longrightarrow 4711 + 815 * 2765 \end{aligned}$$

Vorläufiges Fazit: Die naheliegende Syntax für arithmetische Ausdrücke ist mehrdeutig. Um die Syntax eindeutig zu machen, muss man Vereinbarungen über die Assoziierung (links- oder rechtsassoziierend) und die Bindungsstärke treffen. Lässt man die Vereinbarungen in die Sprachbeschreibung einfließen, nimmt diese an Umfang zu und an Leserlichkeit ab. In der Praxis belässt man es oft bei der mehrdeutigen Syntax und führt die zusätzlichen Vereinbarungen getrennt davon auf. So werden wir es auch halten.

Die Erweiterung von kontextfreien Ausdrücken um verschränkte Rekursion ist auch notwendig für die Beschreibung von ***in***-Ausdrücken. Diese involvieren eine zweite syntaktische Kategorie: Deklarationen.

rec *expr* → *ident* | *num* | *expr* + *expr* | *expr* * *expr* | *decl** `in` *expr*
and *decl* → `let` *ident* = *expr*

Ausdrücke und Deklarationen sind verschränkt rekursiv: Ausdrücke beinhalten Deklarationen und umgekehrt.

Das Problem der Mehrdeutigkeiten ist leider nicht auf Infix-Operatoren beschränkt. Der Ausdruck ***let*** $n = 4711$ ***in*** $n + n$ ist ebenfalls mehrdeutig: Ist damit (***let*** $n = 4711$ ***in*** n) + n oder ***let*** $n = 4711$ ***in*** $(n + n)$ gemeint? Der Unterschied ist groß, meint doch das zweite Vorkommen von n in beiden Ausdrücken etwas anderes! Wir treffen die Vereinbarung, dass sich ein ***in***-Ausdruck so weit nach rechts wie möglich erstreckt. Damit wird ***let*** $n = 4711$ ***in*** $(n + n)$ als Bedeutung des obigen Ausdrucks festgelegt. Genau wie die Vereinbarungen über Assoziierung und Bindungsstärke kann man auch diese Metaregel in die Syntax hineinprogrammieren oder als separate Bemerkung zur Sprachbeschreibung hinzufügen.

Alternativ könnte man das Ende von ***in***-Ausdrücken explizit markieren, zum Beispiel mit dem Schlüsselwort ***end***. Weder ***let*** $n = 4711$ ***in*** n ***end*** + n noch ***let*** $n = 4711$ ***in*** $n + n$ ***end*** lassen einen Interpretationsspielraum zu.

Die Vereinbarung »so weit nach rechts wie möglich« kommt in Mini–F# auch bei Alternativen (***if*** e_1 ***then*** e_2 ***else*** e_3) und Funktionsausdrücken bzw. anonymen Funktionen (***fun*** $x \to e$) zum Zuge. Der Ausdruck ***fun*** $x \to x + x$ ist mehrdeutig: (***fun*** $x \to x$) + x und ***fun*** $x \to (x + x)$ stehen als Interpretationen zur Wahl. Der erste Ausdruck ist nicht typkorrekt. Um Typkorrektheit kümmert sich zwar die kontextfreie Syntax nicht, trotzdem ist das ein guter Grund der zweiten Interpretation den Vorzug zu geben. Da die Metaregel »so weit nach rechts wie möglich« in der Regel die sinnvolle Variante auswählt, wird auch das Ende von Alternativen und Funktionsausdrücken nicht explizit markiert. Wir sagen bewusst »in der Regel«, denn auch die erste Interpretation kann durchaus Sinn ergeben.[21]

Verschiedene Programmiersprachen gehen mit dem Problem der Mehrdeutigkeit verschieden um. Einige setzen auf explizite »Terminierungssymbole« — mittels gespiegelter Schlüsselwörter, wie in ***if*** e_1 ***then*** e_2 ***else*** e_3 ***fi*** und ***while*** e_1 ***do*** e_2 ***od*** oder mit Hilfe von Klammern, wie in ***if*** (e_1) $\{e_2\}$ ***else*** $\{e_3\}$. Andere Programmiersprachen setzen auf die Metaregel »so weit nach rechts wie möglich«. Zunehmend wird auch die Formatierung des Programmtextes, das ***Layout***, benutzt, um Mehrdeutigkeiten aufzulösen. Nicht selten werden auch mehrere Ansätze gleichzeitig verfolgt: In F# kann man zum Beispiel zwischen Layout-sensitiver Syntax und expliziten Terminierungssymbolen wählen.

Abbildung 6.18 fasst die syntaktischen Konstrukte von Mini–F#, eingeschränkt auf die in Kapitel 3 eingeführten Konstrukte, zusammen. Die Beschreibung verwendet mehrere abkürzende Schreibweisen: c^+ steht für eine mindestens einmalige Wiederholung von c, c_s^+ (bzw. c_s^*) für eine mindestens einmalige (bzw. beliebige) Wiederholung, bei der die c Elemente durch s Elemente getrennt werden. Als Formeln:

$$c^+ := \textbf{\textit{rec}}\ x \to c \mid c\ x$$
$$c_s^+ := \textbf{\textit{rec}}\ x \to c \mid c\ s\ x$$
$$c_s^* := \varepsilon \mid c_s^+$$

[21] In Abschnitt 7.2 führen wir einen Operator ein, mit dem zwei effektvolle Ausdrücke verknüpft werden können: $e_1; e_2$. Im Fall dieses Operators versagt die Metaregel: Beide Interpretationen des Ausdrucks ***if*** e_1 ***then*** e_2 ***else*** $e_3; e_4$ sind sinnvoll, so dass empfohlen wird, stets explizit zu klammern: ***if*** e_1 ***then*** e_2 ***else*** $(e_3; e_4)$ oder (***if*** e_1 ***then*** e_2 ***else*** e_3)$; e_4$.

// Ausdrücke		
rec *expr*	→ *aexpr*	atomarer Ausdruck
	| `if` *expr* `then` *expr* `else` *expr*	Alternative
	| `let` $decl^*$ `in` *expr*	lokale Deklaration
	| *expr* `||` *expr*	Disjunktion
	| *expr* `&&` *expr*	Konjunktion
	| *expr* `+` *expr*	Addition
	| *expr* `-` *expr*	Subtraktion
	| *expr* `*` *expr*	Multiplikation
	| *expr* `/` *expr*	Division
	| *expr* `%` *expr*	Divisionsrest
	| *expr* `<` *expr*	kleiner
	| *expr* `<=` *expr*	kleiner gleich
	| *expr* `=` *expr*	gleich
	| *expr* `<>` *expr*	ungleich
	| *expr* `>=` *expr*	größer gleich
	| *expr* `>` *expr*	größer
	| *expr* `^` *expr*	Konkatenation von Strings
	| `fun` $apat^+$ `->` *expr*	Funktionsabstraktion
	| *aexpr* $aexpr^+$	Funktionsapplikation
	| *expr* `:` *type*	Typangabe
and *aexpr*	→ *num*	Numeral
	| *string*	Stringliteral
	| *ident*	Bezeichner
	| `(` *expr* `)`	Gruppierung
// Deklarationen		
and *decl*	→ *pat* `=` *expr*	Wertedefinition
	| *funcdecl*	Funktionsdefinition
	| `rec` $fundecl^+_{\text{and}}$	rekursive Funktionsdefinitionen
and *fundecl*	→ *ident* $apat^+$ `:` *type* `=` *expr*	Funktionsdefinition
// Muster		
and *pat*	→ *apat*	atomares Muster
	| *pat* `:` *type*	Typangabe
and *apat*	→ *ident*	Bezeichner
	| `(` $pat^*_{,}$ `)`	Tupelmuster oder Gruppierung
// Typausdrücke		
and *type*	→ *atype*	atomarer Typ
	| *type* `*` *type*	Tupeltyp
	| *type* `->` *type*	Funktionstyp
and *atype*	→ *Ident*	Typbezeichner
	| `(` *type* `)`	Gruppierung

Abbildung 6.18.: Kontextfreie Syntax von Mini-Mini-F#.

Operator	Assoziierung
Ausdrücke	
`;`	rechtsassoziierend
`:=`	rechtsassoziierend
`,`	nicht assoziierend
`||`	linksassoziierend
`&&`	linksassoziierend
`< <= = <> >= >`	linksassoziierend
`^`	rechtsassoziierend
`:: @`	rechtsassoziierend
`+ -`	linksassoziierend (infix)
`* / %`	linksassoziierend
`**`	rechtsassoziierend
Funktionsapplikation	linksassoziierend
`+ - !`	linksassoziierend (prefix)
`.`	linksassoziierend
Muster	
`|`	rechtsassoziierend
`&`	rechtsassoziierend
Typen	
`->`	rechtsassoziierend
`*`	nicht assoziierend

Abbildung 6.19.: Assoziierung der Mini–F# Operatoren (die Operatoren sind aufsteigend nach ihrer Bindungsstärke angeordnet).

Neben den syntaktischen Kategorien für Ausdrücke und Deklarationen gibt es noch weitere für Muster und Typausdrücke. Ausdrücke teilen sich noch einmal auf in atomare Ausdrücke, *aexpr*, und Ausdrücke, *expr*. Atomare Ausdrücke können als aktuelle Parameter verwendet werden, *ohne* in Klammern gesetzt werden zu müssen. Ein atomarer Ausdruck ist entweder tatsächlich unteilbar (zum Beispiel ein Numeral) oder ein Ausdruck, der bereits geklammert ist. Die Aufteilung in atomare Konstrukte und nicht-atomare Konstrukte findet sich auch bei Mustern und Typausdrücken wieder.

Die Syntax ist — wie wir bereits besprochen haben — hochgradig mehrdeutig. Die Mehrdeutigkeiten werden zum Ersten durch die Vereinbarung aufgelöst, dass sich eine lokale Deklaration, die Alternative und die Funktionsabstraktion so weit nach rechts wie möglich erstreckt. Zum Zweiten wird die Bindungsstärke und Assoziierung von Operatoren wie in Abbildung 6.19 angegeben festgelegt (die Tabelle umfasst fast alle Operatoren, nicht nur die von Mini-Mini–F#). Ist ein Operator linksassoziierend, dann muss der linke Operand die gleiche oder eine höhere Bindungsstärke besitzen und der rechte eine echt höhere Bindungsstärke. Für rechtsassoziierende Operatoren gilt Entsprechendes. Ein nicht assoziativer Operator darf nur Operanden mit höherer Bindungsstärke besitzen. Atomare Ausdrücke haben die höchste Bindungsstärke.

Übungen.

1. Geben Sie für jede der folgenden Sprachen einen kontextfreien Ausdruck an, der die jeweilige Sprache beschreibt. Das zugrundeliegende Alphabet ist $\{\mathsf{a}, \mathsf{b}\}$.

(a) Die Sprache aller Wörter, bei denen auf jedes a direkt ein b folgt.

(b) Die Sprache aller Wörter, die eine gleiche Anzahl von a's und b's enthalten.

(c) Die Sprache $\{\mathsf{a}^{n+3}\,\mathsf{b}^{n+2} \mid n \in \mathbb{N}\}$.

(d) Die Sprache aller Wörter, die nicht das Teilwort abb enthalten.

2. Leiten Sie die Worte aaaba und baaba aus dem folgenden kontextfreien Ausdruck ab:

rec $x \to \mathsf{a} \mid x\,x \mid y\,x$
and $y \to \mathsf{b} \mid x\,y$

3. Ziel dieser Aufgabe ist es, zu zeigen, dass die dem kontextfreien Ausdruck ***rec*** $x \to c$ zugeordnete Funktion stets einen kleinsten Fixpunkt besitzt. Dazu benötigen wir etwas mathematisches Rüstzeug. Die Vereinigung $\bigcup \mathcal{X}$ einer Menge von Mengen ist durch die folgende Eigenschaft charakterisiert:

$$\bigcup \mathcal{X} \subseteq A \quad\Longleftrightarrow\quad \forall\, X \in \mathcal{X} \,.\, X \subseteq A$$

Eine Funktion $F : \mathcal{P}(A^*) \to \mathcal{P}(A^*)$ heißt ***monoton*** genau dann, wenn

$$X \subseteq Y \quad\Longrightarrow\quad F(X) \subseteq F(Y)$$

Eine Funktion $F : \mathcal{P}(A^*) \to \mathcal{P}(A^*)$ heißt ***stetig*** genau dann, wenn

$$F(\bigcup \mathcal{X}) = \bigcup\{F(X) \mid X \in \mathcal{X}\}$$

(a) Sei F stetig. Zeigen Sie, dass $\bigcup\{F^n(\varnothing) \mid n \in \mathbb{N}\}$ *ein* Fixpunkt von F ist.

(b) Zeigen Sie, dass eine stetige Funktion stets monoton ist.

(c) Sei F stetig. Zeigen Sie, dass $\bigcup\{F^n(\varnothing) \mid n \in \mathbb{N}\}$ der *kleinste* Fixpunkt von F ist.

(d) Zeigen Sie, dass die dem kontextfreien Ausdruck ***rec*** $x \to c$ zugeordnete Funktion stetig ist (schwierig).

6.5. Parser⧹Akzeptoren⋆

Wie für reguläre Ausdrücke kann man auch für einen kontextfreien Ausdruck einen Akzeptor programmieren, der überprüft, ob ein gegebenes Wort in der Sprache enthalten ist. Konstruiert das Programm aus der Folge von Lexemen im Erfolgsfall zusätzlich einen abstrakten Syntaxbaum, so spricht man von einem ***Parser***. Ein Parser ist für kontextfreie Ausdrücke das, was ein Scanner für reguläre Ausdrücke ist. Wenden wir uns zunächst der Programmierung von Akzeptoren zu.

6.5.1. Akzeptoren⋆

Im Fall regulärer Ausdrücke haben wir einen Akzeptor generiert, indem wir systematisch alle Rechtsfaktoren konstruiert haben. Das Verfahren lässt sich leider nicht ohne Weiteres auf kontextfreie Ausdrücke übertragen, da diese im Allgemeinen unendlich viele Rechtsfaktoren besitzen. Erinnern wir uns an die »Klammersprache«, die durch den kontextfreien Ausdruck $E =$ ***rec*** $x \to \varepsilon \mid \mathsf{a}\,x\,\mathsf{b}$ gegeben ist. Wir erhalten als Rechtsfaktoren:

$$\mathsf{a} \setminus E = \mathsf{a} \setminus (\varepsilon \mid \mathsf{a}\,E\,\mathsf{b}) = E\,\mathsf{b}$$
$$\mathsf{b} \setminus E = \mathsf{b} \setminus (\varepsilon \mid \mathsf{a}\,E\,\mathsf{b}) = \varnothing$$

module Grammar.AcceptorDyck

Wenn wir bereits ein a gesehen haben, erwarten wir als Rest einen korrekten Klammerausdruck gefolgt von einem b.

$$\begin{aligned}
\mathsf{a} \setminus E\ \mathsf{b} &= \mathsf{a} \setminus (\varepsilon \mid \mathsf{a}\ E\ \mathsf{b})\ \mathsf{b} = E\ \mathsf{b}^2 \\
\mathsf{b} \setminus E\ \mathsf{b} &= \mathsf{b} \setminus (\varepsilon \mid \mathsf{a}\ E\ \mathsf{b})\ \mathsf{b} = \varepsilon
\end{aligned}$$

Sehen wir ein weiteres a, dann müssen nach dem Klammerausdruck zwei bs kommen. Allgemein gilt:

$$\begin{aligned}
\mathit{nullable}(E\ \mathsf{b}^k) &= k = 0 \\
\mathsf{a} \setminus E\ \mathsf{b}^k &= E\ \mathsf{b}^{k+1} \\
\mathsf{b} \setminus E\ \mathsf{b}^k &= \begin{cases} \varnothing & \text{falls } k = 0 \\ \mathsf{b}^{k-1} & \text{sonst} \end{cases} \\
\mathit{nullable}(\mathsf{b}^k) &= k = 0 \\
\mathsf{a} \setminus \mathsf{b}^k &= \varnothing \\
\mathsf{b} \setminus \mathsf{b}^k &= \begin{cases} \varnothing & \text{falls } k = 0 \\ \mathsf{b}^{k-1} & \text{sonst} \end{cases}
\end{aligned}$$

Im Prinzip müssen wir die as zählen und überprüfen, ob genauso viele bs folgen. Damit können wir einen Akzeptor von Hand stricken.

```
type Alphabet = | A | B
type Acceptor = List⟨Alphabet⟩ → Bool
let accept-expr : Acceptor =
  let rec accept-bs (k : Nat) : Acceptor = function
    | [ ]       → k = 0
    | A :: rest → false
    | B :: rest → k > 0 && accept-bs (k – 1) rest
  let rec accept-expr-bs (k : Nat) : Acceptor = function
    | [ ]       → k = 0
    | A :: rest → accept-expr-bs (k + 1) rest
    | B :: rest → k > 0 && accept-bs (k – 1) rest
  in accept-expr-bs 0
```

Die lokale Funktion *accept-bs k* implementiert den Akzeptor für b^k, die Funktion *accept-expr-bs k* entsprechend den Akzeptor für $E\ \mathsf{b}^k$. Beide Definitionen basieren auf der Charakterisierung von Sprachen mit Hilfe von Rechtsfaktoren (6.24): Jeder kontextfreie Ausdruck c über dem Alphabet $\{\mathsf{a}, \mathsf{b}\}$ lässt sich zu $\mathsf{a} \cdot (\mathsf{a} \setminus c) \mid \mathsf{b} \cdot (\mathsf{b} \setminus c)$ oder zu $\varepsilon \mid \mathsf{a} \cdot (\mathsf{a} \setminus c) \mid \mathsf{b} \cdot (\mathsf{b} \setminus c)$ umschreiben. Ein kontextfreier Ausdruck der Form $a_1 \cdot c_1 \mid \cdots \mid a_n \cdot c_n$ bzw. $\varepsilon \mid a_1 \cdot c_1 \mid \cdots \mid a_n \cdot c_n$ lässt sich unmittelbar in den Mini–F#-Ausdruck

```
fun input → match input with
  | [ ]       → false  bzw. true
  | A1 :: rest → accept1 rest
  | …
  | An :: rest → acceptn rest
```

überführen, wobei A_i der zu a_i korrespondierende Konstruktor des Variantentyps *Alphabet* ist und accept_i der Akzeptor für c_i. Diesen Sachverhalt haben wir auch schon bei der Generierung

von Scannern in Abschnitt 6.2 ausgenutzt. Dort wie hier werden rekursiv definierte Sprachen — Wiederholung ist eine sehr spezielle Form der Rekursion — auf rekursiv definierte Akzeptoren abgebildet.

Die Herleitung des obigen Akzeptors ist stark auf die Klammersprache zugeschnitten, so dass sich die Frage stellt, ob wir die Entwicklung auch systematischer betreiben können. Betrachten wir noch einmal die Rechtsfaktoren von $E = \mathbf{rec}\ x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$.

$$\mathsf{a} \setminus E = \mathsf{a} \setminus (\varepsilon \mid \mathsf{a}\ E\ \mathsf{b}) = E\ \mathsf{b}$$
$$\mathsf{b} \setminus E = \mathsf{b} \setminus (\varepsilon \mid \mathsf{a}\ E\ \mathsf{b}) = \varnothing$$

Der Ausdruck E tritt im Rechtsfaktor wieder auf, allerdings gefolgt von dem Symbol b. Wir können E selbst durch eine rekursiv definierte Funktion implementieren, wenn wir die Funktion mit dem Akzeptor für den *Folgeausdruck* parametrisieren. Mit anderen Worten, ein kontextfreier Ausdruck c wird durch eine Funktion implementiert, die einen Akzeptor für c' auf einen Akzeptor für die Sequenz $c \cdot c'$ abbildet, für beliebige kontextfreie Ausdrücke c'. Für unser Beispiel ergibt sich:

```
type Follow = List ⟨Alphabet⟩ → Bool
let accept-b (follow : Follow) : Follow = function
    | B :: rest → follow rest
    | _         → false
let rec accept-expr (follow : Follow) : Follow = function
    | A :: rest → accept-expr (accept-b follow) rest
    | input     → follow input
```

Der formale Parameter *follow* ist jeweils der Folgeakzeptor, der die verbleibende Eingabe verarbeitet. Für jedes gelesene a wird der Folgeakzeptor von *accept-expr* um *accept-b* erweitert; nach zwei as zum Beispiel ist der Folgeakzeptor gleich *accept-b* (*accept-b follow*). Nach dem ersten b wird der akkumulierte Zopf von *accept-b*s abgearbeitet. Man sieht, wir können zählen, ohne die natürlichen Zahlen bemühen zu müssen. Den gewünschten Akzeptor für E erhalten wir schließlich, indem wir *accept-expr* mit dem Akzeptor für ε aufrufen: *accept-expr end-of-input* wobei *end-of-input* wie folgt definiert ist.

```
let end-of-input = function
    | [ ]    → true
    | _ :: _ → false
```

Der Schritt von Funktionen des Typs *Acceptor* zu Funktionen des Typs *Follow* → *Follow* ist ein weiteres Beispiel für die Programmiertechnik der ***Verallgemeinerung***: Wir verallgemeinern Akzeptoren für »isolierte« kontextfreie Ausdrücke zu »Akzeptoren« für in einen Kontext eingebettete kontextfreie Ausdrücke[22]. Mit Hilfe dieses Ansatzes können wir jetzt systematisch zu jedem kontextfreien Ausdruck einen korrespondierenden Mini–F# Ausdruck konstruieren. Gehen wir die Konstrukte der Reihe nach durch:

Das Terminalsymbol *a* wird durch den Mini–F# Ausdruck

```
fun follow → function
    | A :: rest → follow rest
    | _         → false
```

implementiert, wobei *A* das zu *a* korrespondierende Element des Alphabets ist.

[22] Das hört sich merkwürdig an, löst sich aber wie folgt auf: »Kontextfreier Ausdruck« ist ein feststehender Fachbegriff; Kontext meint das Umfeld, in den der Ausdruck eingebettet ist.

Der Bezeichner x wird auf den Mini–F# Bezeichner *accept-x* abgebildet.
Das leere Wort ε wird durch ***fun*** *follow* → ***fun*** *input* → *follow input* bzw. kürzer durch

```
fun follow → follow
```

implementiert, also durch die ***Identitätsfunktion***: Die Arbeit wird unmittelbar an den Folgeakzeptor delegiert.
Ist $accept_i$ die Implementierung von c_i, dann wird die Sequenz $c_1 \cdot c_2$ durch

```
fun follow → accept1 (accept2 follow)
```

implementiert, also durch die ***Komposition von Funktionen***. Beachte, dass $accept_i$ ein *Ausdruck* ist, nicht notwendigerweise ein Bezeichner.
Die leere Sprache ∅ entspricht dem Mini–F# Ausdruck

```
fun follow → fun input → false
```

Kommen wir zur Alternative $c_1 \mid c_2$; diese lässt sich wie folgt implementieren.

```
fun follow →
  fun input → accept1 follow input || accept2 follow input
```

Hier nutzen wir aus, dass die Sequenz über die Alternative distribuiert: $(c_1 \mid c_2)\ c_3 = c_1\ c_3 \mid c_2\ c_3$. Die Alternative wird dann durch die logische Disjunktion realisiert.
Und schließlich die Rekursion: Ist *accept* die Implementierung von c, dann wird der rekursive Ausdruck ***rec*** $x \to c$ durch die rekursive Mini–F# Definition

```
let rec accept-x (follow) =
  accept follow
in accept-x
```

implementiert. (Tritt x in c auf, so kommt entsprechend *accept-x* in *accept* vor.) Verschränkte Rekursion ***rec*** $x_1 \to c_1$ ***and*** ⋯ ***and*** $x_n \to c_n$ wird entsprechend auf verschränkte Rekursion abgebildet.

```
let rec  accept-x1 (follow) → accept1 follow
    and …
    and accept-xn (follow) → acceptn follow
in  accept-x1
```

Voilà. Setzen wir die Bausteine entsprechend zusammen, ergibt sich zum Beispiel für die Klammersprache ***rec*** $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}$ die folgende kompakte Mini–F# Definition.

```
let rec accept-x (follow : Follow) : Follow =
  fun input →
    follow input || accept-a (accept-x (accept-b follow)) input
in accept-x
```

Zu jedem kontextfreien Ausdruck korrespondiert ein Mini–F# Ausdruck. Wir können diese Korrespondenz auch explizit machen, indem wir den einzelnen Bausteinen einen Namen geben und in einer Bibliothek zusammenfassen, siehe Abbildung 6.20. (Die Bibliothek ist übrigens etwas allgemeiner als im Text beschrieben, da von einem konkreten Alphabet abstrahiert wird.) Elementare Bausteine haben den Typ *Acceptor* (wir redefinieren den Typ *Acceptor* an dieser Stelle):

module Grammar.GenericAcceptor

```
type Follow ⟨'a⟩ = List ⟨'a⟩ → Bool
type Acceptor ⟨'a⟩ = Follow ⟨'a⟩ → Follow ⟨'a⟩
let eps : Acceptor ⟨'a⟩ =
  fun follow → follow
let symbol (a : 'a) : Acceptor ⟨'a⟩ =
  fun follow → function
    | [ ]       → false
    | b :: rest → a = b && follow rest
let seq (accept1 : Acceptor ⟨'a⟩, accept2 : Acceptor ⟨'a⟩) : Acceptor ⟨'a⟩ =
  fun follow → accept1 (accept2 follow)
let seq3 (accept1 : Acceptor ⟨'a⟩, accept2 : Acceptor ⟨'a⟩, accept3 : Acceptor ⟨'a⟩) =
  fun follow → accept1 (accept2 (accept3 follow))
let empty : Acceptor ⟨'a⟩ =
  fun follow → fun input →
    false
let alt (accept1 : Acceptor ⟨'a⟩, accept2 : Acceptor ⟨'a⟩) : Acceptor ⟨'a⟩ =
  fun follow → fun input →
    accept1 follow input || accept2 follow input
let end-of-input : Follow ⟨'a⟩ = function
    | [ ]    → true
    | _ :: _ → false
```

Abbildung 6.20.: Akzeptor-Kombinatoren für kontextfreie Ausdrücke.

```
type Acceptor = Follow → Follow
```

Dieser Typ ist sozusagen der Implementierungstyp für kontextfreie Ausdrücke. Die Bausteine für die Sequenz und die Alternative, *seq* und *alt*, besitzen entsprechend den Typ *Acceptor ∗ Acceptor → Acceptor*. Das einzige Konstrukt, das wir nicht wiederfinden, ist ***rec*** $x \rightarrow c$; rekursive kontextfreie Ausdrücke müssen wir weiterhin von Hand umsetzen.[23] Mit Hilfe dieser Bibliothek können wir den Akzeptor für die Klammersprache etwas kompakter definieren.

```
let rec accept-expr : Acceptor = fun follow →
  alt (eps, seq (seq (symbol A, accept-expr), symbol B)) follow
```

Die Struktur der Mini-F# Definition spiegelt exakt die Struktur des kontextfreien Ausdrucks wider.

Probieren wir die Technik an einem weiteren Beispiel aus, den einfachen arithmetischen Ausdrücken aus Abschnitt 6.4.

```
E0 = rec  expr0 → expr1 + expr0
     and  expr1 → expr2 * expr1
     and  expr2 → num   | ( expr0 )
```

Das diesem Ausdruck zugrundeliegende Alphabet ist *Token*, siehe Abschnitt 6.2.2.

module Grammar.AcceptorExpr

[23] Es ist zwar prinzipiell möglich, für ***rec*** $x \rightarrow c$ einen Baustein anzugeben; dieser taugt aber nicht für verschränkt rekursive Ausdrücke.

Die Umsetzung des kontextfreien Ausdrucks E_0 geht mechanisch vonstatten; die verschränkte Rekursion wird auf eine verschränkt rekursive Funktionsdefinition abgebildet.

```
let rec accept-expr0 : Acceptor ⟨Token⟩ = fun follow →
  alt (accept-expr1, seq3 (accept-expr1, symbol Plus, accept-expr0))        follow
and     accept-expr1 : Acceptor ⟨Token⟩ = fun follow →
  alt (accept-expr2, seq3 (accept-expr2, symbol Asterisk, accept-expr1))    follow
and     accept-expr2 : Acceptor ⟨Token⟩ = fun follow →
  alt (accept_num, seq3 (symbol LParen, accept-expr0, symbol RParen))       follow
```

Es bleibt noch, den Parser für Numerale, *accept-num*, nachzureichen.

```
let accept-num : Acceptor ⟨Token⟩ = fun follow → function
  | Num _ :: rest → follow rest
  | _             → false
```

Da der Konstruktor *Num* ein Argument besitzt, können wir *accept-num* nicht mit Hilfe von *symbol* definieren.

Vertiefung: Optimierung Genau wie andere Programme lassen sich auch Parser optimieren. Die Implementierung der Alternative ist nicht sehr zielgerichtet: *alt* $(accept_1, accept_2)$ probiert $accept_1$ und $accept_2$ nacheinander aus. Im Fall von E_0 wird dadurch Arbeit dupliziert: *alt* $(accept\text{-}expr_1, seq3\ (accept\text{-}expr_1, symbol\ Plus, accept\text{-}expr_0)$ probiert zunächst $accept\text{-}expr_1$ aus; ist die Eingabe eine Summe, scheitert dieser Aufruf; dann wird $accept\text{-}expr_1$ erneut ausprobiert, jetzt gefolgt von *symbol Plus* und $accept\text{-}expr_0$. Für jeden Teilausdruck werden also zwei Anläufe unternommen. Diese Verdopplung können wir vermeiden, indem wir den kontextfreien Ausdruck umschreiben: Mit Hilfe des Distributivgesetzes $c \cdot c_1 \mid c \cdot c_2 = c \cdot (c_1 \mid c_2)$ erhalten wir

```
rec  expr0 → expr1 (ε | + expr0)
and expr1 → expr2 (ε | * expr1)
and expr2 → num | ( expr0 )
```

Die gemeinsamen Faktoren werden jeweils nach links herausgezogen — man spricht daher auch von ***Linksfaktorisierung***. Die Mini–F# Definition wird entsprechend umgeformt.

```
let rec accept-expr0 : Acceptor ⟨Token⟩ = fun follow →
  seq (accept-expr1, alt (eps, seq (symbol Plus, accept-expr0)))            follow
and     accept-expr1 : Acceptor ⟨Token⟩ = fun follow →
  seq (accept-expr2, alt (eps, seq (symbol Asterisk, accept-expr1)))        follow
and     accept-expr2 : Acceptor ⟨Token⟩ = fun follow →
  alt (accept_num, seq3 (symbol LParen, accept-expr0, symbol RParen))       follow
```

Zusammenfassung Fassen wir zusammen: Jeder kontextfreie Ausdruck lässt sich systematisch in ein Mini–F# Programm überführen. Rekursion wird auf Rekursion abgebildet, die anderen Konstrukte auf entsprechende Mini–F# Funktionen.

Ist damit der Fall abgeschlossen? Leider nein, die Umsetzung rekursiver Sprachen ist nicht perfekt: Der kontextfreie Ausdruck *rec* $x \to x$ wird auf den Mini–F# Ausdruck

```
let rec accept-x (follow) → accept-x follow in accept-x
```

abgebildet, das einfachste *nichtterminierende* Programm. Die Bedeutung von *rec* $x \to x$ ist aber die leere Sprache. Deren korrekte Implementierung lautet:

fun *follow* → ***fun*** *input* → *false*

ein einfaches, stets *terminierendes* Programm. Das Problem ist schnell ausgemacht: Im ersten Programm erfolgt der rekursive Aufruf, ohne dass das unsichtbare Argument, die Liste von Tokens, verkleinert wurde. Das Problem der Nichtterminierung tritt immer dann auf, wenn der kontextfreie Ausdruck ***linksrekursiv*** ist, wie zum Beispiel bei der folgenden Erweiterung der Klammersprache.

rec $x \to \varepsilon \mid x\ \mathsf{a}\ x\ \mathsf{b}$

Der zugehörige Akzeptor terminiert nicht, sobald die Eingabe mehr als ein Klammergebirge umfasst, zum Beispiel abab. Die äquivalente, ***rechtsrekursive*** Formulierung bereitet hingegen keine Probleme.

rec $x \to \varepsilon \mid \mathsf{a}\ x\ \mathsf{b}\ x$

Beim rekursiven Aufruf des Akzeptors ist sichergestellt, dass die Eingabe verkleinert wurde: Der zu a korrespondierende Akzeptor hat vorher einen Buchstaben konsumiert. Linksrekursion kann auch versteckt auftreten, etwa wenn der Ausdruck links vom Bezeichner ε-haltig ist.

rec $x \to \mathsf{a} \mid y\ x\ \mathsf{b}$
and $y \to \varepsilon \mid \mathsf{a}$

In diesem Beispiel ist y ε-haltig.

Fazit: Bei handgeschriebenen Akzeptoren muss man Sorge tragen, dass die rekursiven Aufrufe auf kleineren Eingaben arbeiten. *Linksrekursion ist um jeden Preis zu vermeiden.* Bei Scannern stellt das Konstruktionsverfahren sicher, dass die Eingabe stets kleiner wird.

6.5.2. Semantik, da capo⋆

Waiting is a very funny activity:
you can't wait twice as fast.

— Edsger W. Dijkstra (1930–2002), *February 28, 1984*

Es lohnt sich, die Diskrepanz zwischen rekursiv definierten Sprachen und rekursiv definierten Akzeptoren etwas genauer unter die Lupe zu nehmen. Wenn wir die Auswertungsregel für ***let rec fun*** $f\ (x) \to e$ ***in*** f mit der Reduktionsregel für ***rec*** $x \to x$ vergleichen, stellen wir fest, dass die Semantik der Rekursion sehr ähnlich ist: In beiden Fällen wird das gesamte »Objekt« für den jeweiligen Bezeichner »eingesetzt«. Trotzdem besteht offenbar ein Unterschied. Der Unterschied ist zunächst einmal ein formaler:

Die Bedeutung des Mini–F# Programms e ist ν, wenn $\varnothing \vdash e \Downarrow \nu$ mit Hilfe der Auswertungsregeln ableitbar ist. Wenn wir zurückblicken und die Auswertungsregeln Revue passieren lassen, stellen wir fest, dass auf jede »Situation« genau eine Auswertungsregel passt. Für die Alternative zum Beispiel gibt es zwar zwei Regeln, aber beide Regeln verlangen, dass die Bedingung ausgewertet wird. Das Ergebnis dieser Auswertung bestimmt dann, welche Regel tatsächlich zur Anwendung kommt. Ähnliches gilt für die Disjunktion, die wir als Abkürzung für ***if*** e_1 ***then*** *true* ***else*** e_2 eingeführt haben. Aus den Regeln für die Alternative können wir die folgenden Regeln für die Disjunktion ableiten.

$$\frac{\delta \vdash e_1 \Downarrow \mathit{true}}{\delta \vdash (e_1 \mid\mid e_2) \Downarrow \mathit{true}} \qquad \frac{\delta \vdash e_1 \Downarrow \mathit{false} \qquad \delta \vdash e_2 \Downarrow \nu}{\delta \vdash (e_1 \mid\mid e_2) \Downarrow \nu}$$

Man sieht, e_1 wird auf jeden Fall ausgewertet, danach ist klar, welche Regel zum Zug kommt. Im Fachjargon sagt man, das Beweissystem ist ***deterministisch***, in jedem Schritt gibt es nur eine anwendbare Regel. Der Mangel an Wahlmöglichkeiten ist erwünscht, da wir ja den Rechner rechnen lassen wollen. So ist dem Rechenknecht in jedem Schritt klar, was zu tun ist. Die Regeln sind sehr sorgfältig in Hinblick auf diese Eigenschaft gewählt. Nur zum Vergleich: Anstelle des asymmetrischen Regelpaars für die Disjunktion (erst e_1, dann e_2) hätten wir auch ein symmetrisches Regeltrio formulieren können:

$$\frac{\delta \vdash e_1 \Downarrow \mathit{true}}{\delta \vdash (e_1 \mid\mid e_2) \Downarrow \mathit{true}} \qquad \frac{\delta \vdash e_1 \Downarrow \mathit{false} \qquad \delta \vdash e_2 \Downarrow \mathit{false}}{\delta \vdash (e_1 \mid\mid e_2) \Downarrow \mathit{false}} \qquad \frac{\delta \vdash e_2 \Downarrow \mathit{true}}{\delta \vdash (e_1 \mid\mid e_2) \Downarrow \mathit{true}}$$

Jetzt ist die Auswertung nicht mehr festgelegt: Wir können e_1 oder e_2 auswerten; ist ein Ergebnis *true*, dann wird das Ergebnis des anderen Ausdrucks nicht mehr benötigt. Mit den neuen Regeln kann die Abarbeitung der Disjunktion nicht länger ***sequentiell*** erfolgen, sondern muss ***parallel*** durchgeführt werden.

Kommen wir zur Semantik von kontextfreien Ausdrücken. Die Bedeutung von c ist *die Menge aller Wörter w*, so dass $c \longrightarrow \cdots \longrightarrow w$ ableitbar ist. Das Beweissystem der Reduktionssemantik ist ***nichtdeterministisch***. Im Fall der Alternative haben wir die freie Wahl.

$$\frac{}{c_1 \mid c_2 \longrightarrow c_1} \qquad \frac{}{c_1 \mid c_2 \longrightarrow c_2}$$

Wäre die Bedeutung eines kontextfreien Ausdrucks ein *einzelnes Wort*, würde sich an dieser Stelle ein mulmiges Gefühl einstellen: Die Bedeutung wäre nicht eindeutig oder im Fachjargon ***nicht determiniert***. Determiniertheit ist etwas anderes als Determinismus. Das obige Regeltrio für die Disjunktion ist nichtdeterministisch; das Ergebnis der Auswertung ist aber determiniert: Unterschiedliche Rechenwege führen stets zum gleichen Ergebnis.

Vorläufiges Fazit: Die Semantik rekursiver Mini–F# Ausdrücke und die rekursiver kontextfreier Ausdrücke ist ähnlich aber nicht deckungsgleich. Der Unterschied tritt noch deutlicher zutage, wenn wir statt der »lokalen Semantik« die »globale Semantik« betrachten.

Wir erinnern uns: Die Semantik von ***rec*** $x \to c$ ist der kleinste Fixpunkt der Funktion $F(X) = [\![c]\!](\varrho, \{x \mapsto X\})$. Dieser Fixpunkt kann beliebig approximiert werden, indem man F wiederholt auf die leere Sprache anwendet.

$\varnothing$
$F(\varnothing)$
$F(F(\varnothing))$
$\ldots$

Mit jedem Schritt wird das Wissen über die bezeichnete Sprache größer: $F^2\ (\varnothing)$ ist informativer als $F^1\ (\varnothing)$ und $F^1\ (\varnothing)$ ist informativer als $F^0\ (\varnothing)$.

Eine entsprechende denotationelle Semantik können wir auch für Mini–F# aufstellen. Wir deuten sie an dieser Stelle nur an; eine vollständige Ausführung würde den Rahmen der Vorlesung sprengen.

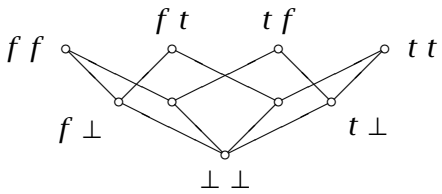
Die uninformativste Sprache ist die leere Sprache. Wenn wir die Idee der Approximation auf Programme übertragen wollen, müssen wir die Frage »Was ist das uninformativste Programm?« beantworten. Ein Ratespiel hilft uns dabei, die Frage zu durchdringen: Harry Hacker hat eine Funktion *unknown* : *Bool* → *Bool* programmiert; wir können die Definition nicht einsehen, dürfen sie aber im Mini–F# Interpreter mit verschiedenen Werten aufrufen. Zum Beispiel:

```
⋙ unknown false
true
⋙ unknown true
false
```

Das war sehr informativ, offenbar hat Harry die Negation programmiert. Zweite Runde mit einer anderen Definition von *unknown*:

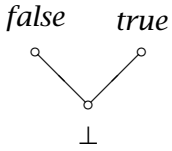
```
⋙ unknown false
true
⋙ unknown true
…
```

Der zweite Aufruf liefert kein Ergebnis, jedenfalls nicht in der Zeitspanne, die wir bereit waren zu warten. Zwei Möglichkeiten sind denkbar: Der Aufruf terminiert nicht oder der Aufruf terminiert, aber erst nach einer Weile. Wir sehen: Nichtterminierende Programme sind nicht sehr informativ, insbesondere, da wir uns der Nichtterminierung nicht sicher sein können — vielleicht ist das Programm ja nur extrem langsam. Der Informationsgehalt nimmt zu, je häufiger eine Funktion terminiert; die Funktion, die nie terminiert, ist das gesuchte Gegenstück zur leeren Sprache. Die Funktionen des Typs *Bool → Bool* lassen sich entsprechend ihres Informationsgehaltes in einer Hierarchie anordnen. Dazu ist es nützlich der Nichtterminierung einen Namen zu geben (ähnlich dem Symbol 0 für die Zahl Null oder dem Symbol ∅ für die leere Menge). Es hat sich eingebürgert, die Nichtterminierung mit dem Symbol ⊥ zu bezeichnen (engl. bottom). Mit ⊥ im Gepäck lassen sich neun verschiedenen Funktionen unterscheiden (wir führen lediglich die Funktionswerte von *false* und *true* auf).



In der obersten Reihe sind die informativsten Funktionen aufgeführt: Die konstante Funktion ***fun*** *b* → *false*, die Identität, die Negation und die konstante Funktion ***fun*** *b* → *true*. Darunter finden sich die Funktionen wieder, die für einen Wahrheitswert terminieren und für den anderen nicht. Das kleinste Element ist schließlich die Funktion, die nie terminiert.

Die Ordnung lässt sich systematisch konstruieren. Funktionen sind zunächst einmal ***punktweise*** geordnet: $f \preccurlyeq g$ gdw. $f(x) \preccurlyeq g(x)$ für alle x. Mini-F# Funktionen des Typs *Bool → Bool* entsprechen mathematischen Funktionen des Typs $\mathbb{B} \to \mathbb{B}_\perp$, wobei $\mathbb{B} = \{false, true\}$ der Bereich der Booleschen Werte ist — $\mathbb{B}$ verhält sich zu *Bool* wie $\mathbb{N}$ zu *Nat* — und $\mathbb{B}_\perp$ der um das Element ⊥ erweiterte Bereich. Der Bereich $\mathbb{B}_\perp$ selbst ist wie folgt geordnet.



Der Bereich der Funktionen $\mathbb{B} \to \mathbb{B}_\perp$ enthält insgesamt $3^2 = 9$ Elemente, die punktweise wie oben angeordnet sind.

Mit diesem Hintergrundwissen können wir die Idee der schrittweisen Approximation auf rekursiv definierte Funktionen übertragen (wir missbrauchen im Folgenden Mini-F# Syntax, um mathematische Funktionen zu notieren). Hier ist Harry Hackers zweites Programm:

```
let rec unknown (b : Bool) : Bool =
  if b then unknown (unknown true) else true
```

Zunächst ordnen wir dem Programm eine *nicht-rekursive* Funktion zu, die mit *unknown* parametrisiert ist (vergleiche mit der denotationellen Semantik von Sprachen).

```
let F(unknown : Bool → Bool) : Bool → Bool =
  fun (b : Bool) → if b then unknown (unknown true) else true
```

Der Fixpunkt von F ist die gesuchte Bedeutung von *unknown*; der Fixpunkt kann ausgehend von der nie terminierenden Funktion $\perp\!\!\!\perp$ = ***fun*** $b \to \bot$ beliebig approximiert werden:

$$
\begin{array}{ll}
 & \perp\!\!\!\perp \\
F(\perp\!\!\!\perp) & = \textbf{\textit{fun}}\ b \to \textbf{\textit{if}}\ b\ \textbf{\textit{then}}\ \perp\!\!\!\perp\ (\perp\!\!\!\perp\ \mathit{true})\ \textbf{\textit{else}}\ \mathit{true} \\
 & = \textbf{\textit{fun}}\ b \to \textbf{\textit{if}}\ b\ \textbf{\textit{then}}\ \bot\ \textbf{\textit{else}}\ \mathit{true} \\
F(F\ \perp\!\!\!\perp) & = \textbf{\textit{fun}}\ b \to \textbf{\textit{if}}\ b\ \textbf{\textit{then}}\ F(\perp\!\!\!\perp)\ (F(\perp\!\!\!\perp)\ \mathit{true})\ \textbf{\textit{else}}\ \mathit{true} \\
 & = \textbf{\textit{fun}}\ b \to \textbf{\textit{if}}\ b\ \textbf{\textit{then}}\ F(\perp\!\!\!\perp)\ (\bot)\ \textbf{\textit{else}}\ \mathit{true} \\
 & = \textbf{\textit{fun}}\ b \to \textbf{\textit{if}}\ b\ \textbf{\textit{then}}\ \bot\ \textbf{\textit{else}}\ \mathit{true}
\end{array}
$$

Nach der zweiten Iteration haben wir einen Fixpunkt gefunden: Die Bedeutung der Funktion *unknown* ist ***fun*** $b \to$ ***if*** b ***then*** $\bot$ ***else*** *true*. Bei der Vereinfachung haben wir übrigens ausgenutzt, dass $f(\bot) = \bot$ gilt: Wenn die Auswertung des Funktionsarguments nicht terminiert, dann terminiert auch der Funktionsaufruf nicht. Dies gilt für alle Programmiersprachen, die Parameter »call by value« übergeben.

Jetzt sind wir der Diskrepanz zwischen der Semantik von Sprachen und der Semantik von Mini–F# auf den Fersen. Die denotationelle Semantik ordnet Sprachen gemäß der Mengeninklusion, die Menge aller Sprachen ist der Potenzmengenverband $\mathcal{P}(\mathbb{A}^*)$. Die einfachsten Akzeptoren, die wir geschrieben haben, besitzen den Typ *List ⟨Alphabet⟩ → Bool* und können als ***charakteristische Funktion*** $\mathbb{A}^* \to \mathbb{B}$ aufgefasst werden. Wenn wir die Inklusionsordnung auf charakteristische Funktionen übertragen, erhalten wir: $f \preccurlyeq g$ gdw. $f(x) \Longrightarrow g(x)$ für alle $x \in \mathbb{B}$. Die Implikation $\Longrightarrow$ ist die zugrundeliegende Ordnung auf $\mathbb{B}$: *false* ist kleiner als *true*. Mit anderen Worten, eine getreue Umsetzung der Semantik kontextfreier Ausdrücke verlangt, dass $\mathbb{B}$ wie folgt geordnet ist.

Wir haben aber gesehen, dass der Wertebereich von Akzeptoren in Wirklichkeit $\mathbb{B}_\perp$ ist und diesem Bereich eine andere Ordnung zugrundeliegt. Somit hat die Sprache ***rec*** $x \to x$ die Bedeutung $\varnothing$, der Mini–F# Akzeptor

```
let rec fun accept-x (follow) → accept-x follow in accept-x
```

aber die Bedeutung $\perp\!\!\!\perp$; eine bedauerliche, aber leider unvermeidbare Diskrepanz.

6.5.3. Parser⋆

Die Akzeptoren aus Abschnitt 6.5.1 beantworten die Frage »Ist das gegebene Wort in der von dem kontextfreien Ausdruck bezeichneten Sprache enthalten?«. Ein Parser beantwortet die gleiche Frage, gibt aber im positiven Fall zusätzlich einen ***semantischen Wert*** zurück. Im Fall arithmetischer Ausdrücke kann der semantische Wert tatsächlich der Wert des Ausdrucks sein, es kann aber auch der abstrakte Syntaxbaum des Ausdrucks sein. Der letztere Ansatz ist allgemeiner — aus dem abstrakten Syntaxbaum können wir den Wert berechnen, aber nicht umgekehrt.

Die abstrakte Syntax arithmetischer Ausdrücke fangen wir mit einer rekursiven Variantentypdefinition ein.

module Grammar.Expr

```
type Expr =
  | Const of Nat
  | Add   of Expr * Expr
  | Mul   of Expr * Expr
```

Wir erinnern uns: Variantentypen sind das Mini–F# Pendant zu Baumsprachen, so dass wir die Baumsprache für arithmetische Ausdrücke im Wesentlichen übernehmen können (hier aus Platzgründen nur in Teilen). Ein Auswerter für arithmetische Ausdrücke ist fix geschrieben. Das Struktur Entwurfsmuster für *Expr* bringt uns schnell und sicher ans Ziel.

```
let rec evaluate (expr : Expr) : Nat =
  match expr with
  | Const nat              → nat
  | Add (expr1, expr2) → evaluate expr1 + evaluate expr2
  | Mul (expr1, expr2) → evaluate expr1 * evaluate expr2
```

Der Auswerter, ein echter Interpreter (!), implementiert die Semantik aus Abschnitt 3.1.

Kommen wir zur Implementierung von Parsern. Ein Akzeptor liefert einen Booleschen Wert als Ergebnis; jetzt müssen wir im Erfolgsfall einen Wert zurückgeben (im Fall eines Misserfolgs wäre eine aussagekräftige Fehlermeldung schön — diesen Aspekt ignorieren wir hier geflissentlich). Aus dem Typ *Bool* wird somit der Typ *Option ⟨'value⟩*.

```
type Follow ⟨'value⟩ = List ⟨Token⟩ → Option ⟨'value⟩
```

Der Typparameter spezifiziert den Typ des resultierenden Wertes, für unser laufendes Beispiel ist der Typ zum Beispiel *Nat* oder *Expr*. Welche Änderungen ergeben sich für die Programme? Modifizieren wir zunächst den »handgeschriebenen« Akzeptor aus Abbildung 6.21. Auf den ersten Blick sind es nicht allzu viele Änderungen: Nur *accept-RParen* und *end-of-input* enthalten konkrete Boolesche Werte. Die Änderung von *Bool* nach *Option ⟨'value⟩* gibt vor, dass *false* zu *None* wird und *true* zu *Some expr*, wobei *expr* der konstruierte abstrakte Syntaxbaum ist (siehe auch Abschnitt 5.3.3). Damit erhalten wir für *end-of-input*:

```
let end-of-input : Follow ⟨Expr⟩ = function
  | [ ]    → Some ??
  | _ :: _ → None
```

Aber woher nehmen wir das Argument für *Some*? Der Akzeptor *end-of-input* ist das letzte Glied in der Kette von Akzeptoren, er hat im Wesentlichen die Aufgabe abzunicken oder den Kopf zu schütteln. Es bleibt uns nichts anderes übrig, als *end-of-input* den semantischen Wert mit auf den Weg zu geben.

```
let end-of-input (e : Expr) : Follow ⟨Expr⟩ = function
  | [ ]    → Some e
  | _ :: _ → None
```

Aus einer Funktion des Typs *Follow* ist eine Funktion des Typs *Expr → Follow ⟨Expr⟩* geworden. Die Funktion *end-of-input* ist ein Folgeakzeptor (der initiale), damit drängt sich die folgende Idee auf: *Jeder Parser übergibt seinen semantischen Wert an den Folgeakzeptor.* Aus der Funktion $accept\text{-}expr_0 : Follow \to Follow$ wird mit dieser Idee die Funktion $parse\text{-}expr_0 : (Expr \to Follow\,\langle Expr\rangle) \to Follow\,\langle Expr\rangle$. In der Definition von $parse\text{-}expr_0$ wird der abstrakte Syntaxbaum für die Summe konstruiert und an den Folgeakzeptor weitergegeben: $follow\ (Add\ (expr_1, expr_2))$. Ein Aufruf von $parse\text{-}expr_0$ hat typischerweise die Form $parse\text{-}expr_0\ (\mathbf{fun}\ expr \to \ldots)$; der semantische Wert von $parse\text{-}expr_0$ wird dann im Rumpf der Funktionsabstraktion weiterverarbeitet. Der vollständige Programmcode ist in Abbildung 6.21 aufgeführt.

Es lohnt sich, ein konkretes Beispiel durchzurechnen: die Analyse von `4711+815*2765` bzw. als Liste von Tokens:

```
[Num 4711; Plus; Num 815; Asterisk; Num 2765]
```

```
type Token = | Num of Nat | LParen | RParen | Asterisk | Plus
type Follow ⟨'v⟩ = List ⟨Token⟩ → Option ⟨'v⟩
type Expr =
  | Const of Nat
  | Add   of Expr * Expr
  | Mul   of Expr * Expr
let parse-RParen (follow : Follow ⟨Expr⟩) : Follow ⟨Expr⟩ = function
  | RParen :: rest → follow rest
  | _              → None
let rec parse-expr0 (follow : Expr → Follow ⟨Expr⟩) : Follow ⟨Expr⟩ =
    parse-expr1 (fun e1 → function
      | Plus :: rest  → parse-expr0 (fun e2 → follow (Add (e1, e2))) rest
      | _             → follow e1 input)
  and parse-expr1 (follow : Expr → Follow ⟨Expr⟩) : Follow ⟨Expr⟩ =
    parse-expr2 (fun e1 → function
      | Asterisk :: rest → parse-expr1 (fun e2 → follow (Mul (e1, e2))) rest
      | _                → follow e1 input)
  and parse-expr2 (follow : Expr → Follow ⟨Expr⟩) : Follow ⟨Expr⟩ = function
    | Num n :: rest → follow (Const n) rest
    | LParen :: rest → parse-expr0 (fun e → parse-RParen (follow e)) rest
    | _             → None
let end-of-input (e : Expr) : Follow ⟨Expr⟩ = function
  | [ ]    → Some e
  | _ :: _ → None
let abstract-syntax-tree : String → Option ⟨Expr⟩ =
  explode ≫ lex ≫ parse-expr0 end-of-input
```

Abbildung 6.21.: Parser für einfache arithmetische Ausdrücke.

Da die Mini–F# Ausdrücke recht groß sind, führen wir nur die (rekursiven) Aufrufe auf und kürzen die Folgeakzeptoren jeweils ab (die Folgeakzeptoren können aus dem Programmtext, siehe Abbildung 6.21, rekonstruiert werden).

$\mathit{parse\text{-}expr}_0$	$\mathit{end\text{-}of\text{-}input}$	$[\mathit{Num}\ 4711, \ldots]$
$= \mathit{parse\text{-}expr}_1$	follow_0	$[\mathit{Num}\ 4711, \ldots]$
$= \mathit{parse\text{-}expr}_2$	follow_1	$[\mathit{Num}\ 4711, \ldots]$
$= \mathit{follow}_1$	$(\mathit{Const}\ 4711)$	$[\mathit{Plus}, \ldots]$
$= \mathit{follow}_0$	$(\mathit{Const}\ 4711)$	$[\mathit{Plus}, \ldots]$
$= \mathit{parse\text{-}expr}_0$	follow_2	$[\mathit{Num}\ 815, \ldots]$
$= \mathit{parse\text{-}expr}_1$	follow_3	$[\mathit{Num}\ 815, \ldots]$
$= \mathit{parse\text{-}expr}_2$	follow_4	$[\mathit{Num}\ 815, \ldots]$
$= \mathit{follow}_4$	$(\mathit{Const}\ 815)$	$[\mathit{Asterisk}, \ldots]$
$= \mathit{parse\text{-}expr}_1$	follow_5	$[\mathit{Num}\ 2765]$
$= \mathit{parse\text{-}expr}_2$	follow_6	$[\mathit{Num}\ 2765]$
$= \mathit{follow}_6$	$(\mathit{Const}\ 2765)$	$[\,]$
$= \mathit{follow}_5$	$(\mathit{Const}\ 2765)$	$[\,]$
$= \mathit{follow}_3$	$(\mathit{Mul}\ (\mathit{Num}\ 815, \mathit{Num}\ 2765))$	$[\,]$
$= \mathit{follow}_2$	$(\mathit{Add}\ (\mathit{Num}\ 4711, \mathit{Mul}\ (\mathit{Num}\ 815, \mathit{Num}\ 2765)))$	$[\,]$
$= \mathit{end\text{-}of\text{-}input}$	$(\mathit{Add}\ (\mathit{Num}\ 4711, \mathit{Mul}\ (\mathit{Num}\ 815, \mathit{Num}\ 2765)))$	$[\,]$
$= \mathit{Some}\ (\mathit{Add}\ (\mathit{Num}\ 4711, \mathit{Mul}\ (\mathit{Num}\ 815, \mathit{Num}\ 2765)))$		

Die Abfolge der Funktionsaufrufe entspricht im Wesentlichen der in Abschnitt 6.4 aufgeführten Reduktionsfolge von `4711+815*2765`. Der semantische Wert des bereits verarbeiteten Teils der Eingabe (in der Reduktionsfolge entspricht das dem Anfangsstück aus Terminalsymbolen) wird jeweils an den Folgeakzeptor weitergereicht; dieser ergänzt den semantischen Wert und reicht ihn an seinen Folgeakzeptor weiter. Insgesamt ergibt sich das Bild einer Kollekte: Um Geld für besondere Zwecke zu sammeln, wird ein Korb herumgereicht; jeder fügt ein paar Münzen hinzu und reicht den Korb an den Nachbarn (den Folgeakzeptor) weiter. Am Ende der Kette wird der Korb geleert (*end-of-input*). Beim Parsen, wie bei der Kollekte kann es passieren, dass der Korb unverändert weitergereicht wird oder dass sogar etwas entnommen wird. (Letzteres ist im Fall einer Kollekte unerwünscht.) Der Parser $\mathit{parse\text{-}expr}_0$ zum Beispiel reicht das Ergebnis von $\mathit{parse\text{-}expr}_1$ unverändert an *follow* weiter, wenn er kein *Plus* Symbol sieht.

Übungen.

1. Schreiben Sie einen Akzeptor für die Sprache der arithmetischen Ausdrücke in Präfixnotation.

rec *expr* → *num* | + *expr expr* | ∗ *expr expr*

Zusammenfassung und Anmerkungen

DIY: Zusammenfassung

7. Effekte\Effektvolles Rechnen

I amar prestar aen.
Die Welt ist im Wandel.

— John R. R. Tolkien (1892–1973), *Herr der Ringe*

Nach dem längeren Ausflug in die Welt der formalen Sprachen wenden wir uns wieder unserer Programmiersprache zu. Frischen wir unser Gedächtnis auf. In Kapitel 3 haben wir uns mit den grundlegenden Bestandteilen von Mini–F# vertraut gemacht: mit der Verarbeitung von Wahrheitswerten und natürlichen Zahlen, mit der Möglichkeit, Ausdrücken einen Namen zu geben und sich später auf die Werte dieser Ausdrücke zu beziehen und schließlich mit der Formulierung von Rechenregeln in Form von Funktionen und rekursiven Funktionen. Am Ende des Kapitels steht eine Sprache, mit der man die prinzipiellen Möglichkeiten eines Rechners ausschöpfen kann. In Kapitel 4 haben wir das bis dato bescheidene Repertoire an Typen erweitert: Wir haben gesehen, wie man mehrere Daten zu einer Einheit zusammenfasst und alternative Angaben als Einheit behandelt. Die Möglichkeiten zur Darstellung und Verwaltung von Daten sind vielfältig: Tupel, Records, Varianten, Listen, Bäume, Arrays usw. stehen zur Auswahl. Die verschiedenen Typen unterscheiden sich hinsichtlich Flexibilität, Bequemlichkeit und Schnelligkeit der sie manipulierenden Operationen.

Wir haben viele Funktionen kennengelernt und selbst programmiert. So unterschiedlich die Programme auch sein mögen, sie eint ein charakteristisches Merkmal: Funktionen verdienen ihren Namen! Das Ergebnis einer Funktion — die Ausgabe, wenn man so will — wird allein durch den aktuellen Parameter — die Eingabe, wenn man möchte — bestimmt. Das ist sowohl ein Segen als auch ein Fluch.

Es ist ein Segen, weil man Funktionen »lokal« lesen und verstehen kann. Um zu begreifen, was eine Funktion berechnet, muss ich nur ihre Definition studieren (und die Definitionen, von denen sie statisch abhängt). Rufe ich eine Funktion mit dem gleichen Argument auf, erhalte ich das gleiche Ergebnis.

Es ist ein Fluch, weil Funktionen in ihren Interaktionsmöglichkeiten stark eingeschränkt sind. Ich stelle eine Frage, indem ich die Funktion aufrufe, nach einer Periode der Stille und des Wartens erhalte ich die Antwort in Form des Funktionsergebnisses. Weiteren Einfluss auf den Verlauf der Rechnung habe ich nicht; weiteres Feedback erhalte ich nicht. Das gilt im übrigen für alle Ausdrücke, nicht nur für Funktionsaufrufe: Ein Ausdruck wird zu einem Wert ausgerechnet; die Rechnung selbst kann nicht beeinflusst oder beobachtet werden.

Halten wir fest: Die Kommunikation mit einem Programm ist stark eingeschränkt und passt sicherlich nicht in das Bild, das die meisten von einem Rechner und von dem Umgang mit diesem Medium haben. Persönliche Rechner interagieren mit der Benutzerin oder dem Benutzer über Bildschirm, Tastatur und Maus; Steuerungsrechner interagieren mit der Umwelt über Sensoren und Aktoren. Um auch diesen Einsatzgebieten gerecht zu werden, erweitern wir in diesem Kapitel die Idee des Rechnens: Ein Ausdruck kann neben einem Wert zusätzlich einen ***Effekt*** haben. Ein Effekt ist zum Beispiel eine Ausgabe auf dem Bildschirm, die Anforderung einer Eingabe, das Einlesen von Sensordaten oder die Steuerung eines Motors. Mit diesen ***externen Effekten*** beschäftigt sich Abschnitt 7.1. Wir beschränken uns dabei auf die Ein- und Ausgabe von Strings.

Neben externen gibt es auch ***interne Effekte***: Eine Rechnung kann von einem Gedächtnis abhängen oder das Gedächtnis verändern; eine Rechnung kann ergebnislos abgebrochen werden und an

anderer Stelle wiederaufgenommen werden. Das Kurzzeitgedächtnis eines Rechners ist der sogenannte Hauptspeicher; Abschnitt 7.2 macht uns mit dem Konzept des Speichers vertraut. (Die im Kurzzeitgedächtnis hinterlegten Daten verflüchtigen sich, wenn der Rechner ausgeschaltet wird. Im Langzeitgedächtnis, dem Hintergrundspeicher, abgelegte Daten bleiben hingegen erhalten.)

Abschnitt 7.3 führt Sprachkonstrukte ein, die es auf einfache Art und Weise ermöglichen, effektvolle Ausdrücke miteinander zu kombinieren: Effekte aneinanderzureihen (Sequenz), Effekte von Bedingungen abhängig zu machen (Alternative), Effekte zu wiederholen (Iteration).

Eine Rechnung führt nicht immer zu einem Ergebnis: Treffen wir im Laufe einer Rechnung zum Beispiel auf den Teilausdruck $1 \div 0$, müssen wir die Segel streichen. Abschnitt 7.4 zeigt, wie wir mit diesen und ähnlichen Ausnahmesituationen umgehen können, wie wir Rechnungen abbrechen und an anderer Stelle wiederaufnehmen.

Mit dem Einzug von Effekten verändert sich die Natur des Rechnens. Die Reihenfolge, in der Teilrechnungen bearbeitet werden, spielt plötzlich eine zentrale Rolle: Wenn e_1 und e_2 Effekte haben, ist es nicht mehr egal, wie zum Beispiel der Ausdruck $e_1 + e_2$ ausgerechnet wird. Ist eine Funktion effektvoll, weil sie Ein- oder Ausgaben tätigt oder weil sie vom Gedächtnis abhängt oder das Gedächtnis verändert, dann handelt es sich nicht mehr um eine Funktion im mathematischen Sinne. Eine effektvolle Funktion kann bei gleichen Argumenten unterschiedliche Resultate liefern! Vielleicht ahnt man die Gefahr. Setzt man die neuen Sprachkonstrukte nicht mit Bedacht ein, so wird aus dem Segen schnell ein Fluch: Klarheit und Lesbarkeit von Programmen leiden. Wenn eine Funktion auf vielfältigen Wegen mit ihrer Umwelt interagiert, dann kann die Funktion nicht mehr isoliert verstanden werden, sondern die vielfältigen Verflechtungen müssen zusätzlich berücksichtigt werden. Diese warnenden Worte sollte man beim Studium der folgenden Seiten stets im Gedächtnis behalten.

7.1. Ein- und Ausgabe

In Abschnitt 3.6 haben wir ein 2-Personenspiel programmiert, bei dem Spielerin B eine von Spieler A ausgedachte Zahl raten musste. Beide Parteien wurden bisher vom Rechner gestellt. Das wollen wir jetzt ändern: Die Benutzerin bzw. der Benutzer soll die Rolle von Spieler A übernehmen. Natürlich wird dieser weiterhin durch eine Mini–F# Funktion realisiert, etwa

let human-player (*guess* : *Nat*) : *Bool*

aber es soll eine Funktion sein, die über Ein- und Ausgaben mit dem/der Benutzer/-in interagiert und dessen/deren Antworten weiterleitet. Dazu benötigen wir grundlegende Funktionen zur Ein- und Ausgabe.

Ausgaben auf dem Bildschirm werden mit Hilfe der Funktion *putstring* getätigt. Der Aufruf

putstring `"hello, world"`

wertet zu dem leeren Tupel »()« aus und hat zusätzlich den Effekt, dass der String `"hello, world"` ausgegeben wird. Die Funktion *putstring* ist das erste Beispiel für eine nicht-mathematische Funktion. Der Funktionswert steht schon vor dem Aufruf fest; ignorieren wir die Effekte, dann entspricht *putstring* der Funktion ***fun*** (*s*:*String*) → (). Die Funktion *putstring* wird allein wegen ihres Effektes aufgerufen.

Man gewöhnt sich schnell an die Tatsache, dass ein Ausdruck neben einem Wert zusätzlich einen Effekt haben kann. Genauso schnell sollte man sich klarmachen, dass sich das Rechnen mit dem Einzug von Effekten verändert: Die Reihenfolge und die Multiplizität von Rechnungen spielen plötzlich eine Rolle. Bisher galt, dass zum Beispiel die Komponenten des Paarausdrucks

(*factorial* 9, *factorial* 10)

in beliebiger Reihenfolge ausgerechnet werden konnten. Die Auswertungsregel für Paarausdrücke

$$\frac{\delta \vdash e_1 \Downarrow \nu_1 \qquad \delta \vdash e_2 \Downarrow \nu_2}{\delta \vdash (e_1, e_2) \Downarrow (\nu_1, \nu_2)}$$

mag eine Auswertung von links nach rechts suggerieren, aber das ist eine Illusion. Auswertungsregeln wie die obige werden verwendet, um die Relation $\delta \vdash e \Downarrow \nu$ festzulegen. An dieser Relation ändert sich nichts, wenn wir die Voraussetzungen der Beweisregel umordnen.

$$\frac{\delta \vdash e_2 \Downarrow \nu_2 \qquad \delta \vdash e_1 \Downarrow \nu_1}{\delta \vdash (e_1, e_2) \Downarrow (\nu_1, \nu_2)}$$

Zurück zu unserem Beispiel: Wenn *factorial* zusätzlich einen Effekt hat, dann spielt die Reihenfolge der Teilrechnungen sehr wohl eine Rolle. Ebenso ist relevant, wie oft eine Rechnung durchgeführt wird. Der Ausdruck

```
let f = factorial 9 in (f, f * 10)
```

hat zwar den gleichen Wert, aber wahrscheinlich einen anderen Effekt. Hier ist eine effektvolle Version von *factorial*, bei der der Unterschied zwischen den obigen Ausdrücken zu Tage tritt.

```
let rec factorial (n : Nat) : Nat =
  let () = putstring (show n ^ "\n")
  in  if n = 0 then 1 else factorial (n - 1) * n
```

Die Ausgabeanweisung *putstring* (*show* n ^ "\n") ist ein Beispiel für einen Ausdruck, der nur seines Effektes willen, nicht aber seines Wertes wegen ausgerechnet wird. Ein wiederkehrendes Idiom in diesem Zusammenhang ist **let** () = e_1 **in** e_2. Die lokale Bindung dient dazu, die Auswertung von zwei Ausdrücken und damit das Auftreten von Effekten zu sequentialisieren. Zunächst wird e_1 ausgerechnet, das Ergebnis wird mit dem Muster »()« abgeglichen, anschließend wird e_2 ausgerechnet. Der Wert von e_1 spielt für die zweite Teilrechnung keine Rolle. Der Wert des gesamten Ausdrucks ist der Wert von e_2. Wir kürzen dieses Idiom mit $e_1; e_2$ ab (lies: e_1 gefolgt von e_2). Tatsächlich können wir das Semikolon auch weglassen, wenn wir e_1 und e_2 untereinander schreiben und durch das »Layout« unsere Intention ausdrücken. Weiterhin erlauben wir, die Deklaration **let** () = e mit **do** e abzukürzen (diese Abkürzung werden wir in Kapitel 8 häufiger verwenden). Mit Hilfe dieses »syntaktischen Zuckers« lässt sich die effektvolle Version von *factorial* etwas kompakter aufschreiben.

```
let rec factorial (n : Nat) : Nat =
  putstring (show n ^ "\n")
  if n = 0 then 1 else factorial (n - 1) * n
```

Der aktuelle Parameter n wird nach jedem Aufruf auf dem Bildschirm ausgegeben. Die Auswertung von (*factorial* 9, *factorial* 10) resultiert somit in 21 Ausgaben, wohingegen **let** f = *factorial* 9 **in** $(f, f * 10)$ nur 10 Ausgaben erzeugt.

Eingaben von der Tastatur können mit Hilfe der Funktion *getline* eingefangen werden. Der Aufruf

```
getline ()
```

liest eine einzelne Zeile ein, eine Folge von Zeichen, die von einem Zeilenvorschub abgeschlossen wird.[1] Der String *ohne* den Zeilenvorschub wird als Ergebnis zurückgegeben. Auch *getline*

[1] Die Benutzerin bzw. der Benutzer schließt die Eingabe einer Zeile mit der Eingabetaste (auch: Return- oder Enter-Taste) ab.

ist keine mathematische Funktion. Wäre sie eine, dann müsste sie stets den gleichen String zurückgeben. Wie auch bei Ausgaben spielt bei Eingaben die Reihenfolge und die Multiplizität von Rechnungen eine Rolle. Der Ausdruck

```
(getline (), getline ())
```

fordert zwei Eingaben an; der Aufruf

```
let s = getline () in (s, s)
```

hingegen nur eine.

Wir können *putstring* und *getline* kombinieren, um eine Funktion zu programmieren, die den/die Benutzer/-in zu einer Eingabe auffordert.

module Effects.Input

```
let query (prompt : String) : String =
  putstring prompt; getline ()
```

Mit Hilfe von *query* können wir *human-player* kurz und knapp definieren.

```
let human-player (guess : Nat) : Bool =
  query ("Ist die Zahl gleich oder kleiner als " ^ show guess ^ "? ") = "ja"
```

Der Ratekandidat *guess* wird ausgegeben; die Eingabe der Benutzerin oder des Benutzers wird in einen Booleschen Wert verwandelt. Hier sehen wir die Funktion in Aktion:

```
⋙ player-B (human-player, 0, 99)
Ist die Zahl gleich oder kleiner als 49 ? ja
Ist die Zahl gleich oder kleiner als 24 ? nein
Ist die Zahl gleich oder kleiner als 37 ? nein
Ist die Zahl gleich oder kleiner als 43 ? nein
Ist die Zahl gleich oder kleiner als 46 ? nein
Ist die Zahl gleich oder kleiner als 48 ? ja
Ist die Zahl gleich oder kleiner als 47 ? ja
47
```

Nach sieben Runden hat der Rechner die Zahl ermittelt.

Mit Hilfe des Tests *query* … = `"ja"` überprüfen wir, ob der/die Benutzer/-in `ja` eingegeben hat oder etwas anderes. Um verschiedenen Eingaben den Wahrheitswert *true* zuzuordnen, ist die Funktion *contains*:*String*→*List* ⟨*String*⟩→*Bool* nützlich. Zur Erinnerung: Die Funktion überprüft, ob das erste Argument in der angegebenen Liste enthalten ist. Der Aufruf *contains* (*query* …) $[s_1, \ldots, s_n]$ zum Beispiel testet, ob der/die Benutzer/-in einen der aufgeführten Strings eingegeben hat. Das nachfolgende Programm, das einen Wert vom Typ *Person* einliest, illustriert die Verwendung dieses Idioms.

```
let input-person () : Person =
  if contains (query "gender: ") ["f";"female"] then
    Female {name = query "name:    "}
  else
    Male   {name = query "name:    ";
            bald = contains (query "bald?:   ") ["y";"yes"]}
```

Zunächst wird das Geschlecht abgefragt; in Abhängigkeit von der Antwort werden ein oder zwei weitere Eingaben getätigt. Die folgende Interaktion illustriert die Verwendung von *input-person*.

```
⋙ input-person ()
gender : male
name   : Ralf
bald?  : yes
Male {name = "Ralf"; bald = true}
```

Es ist bemerkenswert, dass *input-person* eine Funktion des Typs $Unit \to Person$ ist und nicht ein Wert des Typs *Person*. Wäre *input-person* durch eine Wertebindung der Form ***let*** *input-person* = … gegeben, dann würde *ein* Datensatz unmittelbar bei Abarbeitung der Deklaration eingelesen. Der Bezeichner *input-person* stände nachfolgend für den eingegebenen Datensatz. Die obige Funktions*definition* ist hingegen effektfrei, da eine Funktion unmittelbar zu sich selbst auswertet! Die Eingaben werden erst angefordert, wenn die Funktion aufgerufen wird — mit »()« als Dummyargument. Und: Jeder weitere Aufruf führt zu einer erneuten Eingabe. Es besteht also ein großer Unterschied zwischen einem Ausdruck vom Typ *Person* und einem Ausdruck vom Typ $Unit \to Person$. Funktionen des Typs $Unit \to t$ bzw. $t \to Unit$ werden uns in diesem Kapitel häufig begegnen. Der Dummytyp *Unit* ist in der Regel ein Indiz dafür, dass eine Funktion effektvoll ist.

7.1.1. Abstrakte Syntax

Die Funktionen *putstring* und *getline* lassen sich auf Funktionen zurückführen, die ein einzelnes Zeichen ausgeben bzw. einlesen.

$e ::= \cdots$	***Ein- und Ausgabeoperationen:***
$\mid$ *getchar e*	Einlesen eines Zeichens
$\mid$ *putchar e*	Ausgabe eines Zeichens
$\mid$ *readFromFile e*	Einlesen von einer Datei
$\mid$ *writeToFile e*	Ausgabe in eine Datei

Zusätzlich gibt es Funktionen, die eine Textdatei einlesen bzw. einen String in eine Textdatei ausgeben. Eine Textdatei ist eine Folge von Zeichen, die auf einem Speichermedium abgelegt ist. Eine ***Datei*** kann die Laufzeit eines Programms überdauern und wird für die Verwaltung ***persistenter*** Daten verwendet (lat. anhaltend, beharrlich). In vielen Anwendungen sind Daten tatsächlich wichtiger als Programme. Mehr zu diesem Themenkreis erfahren Sie im weiteren Studium in der Vorlesung Informationssysteme.

7.1.2. Statische Semantik

Die Ein- und Ausgabeoperationen verarbeiten einzelne Zeichen.

$$\frac{\Sigma \vdash e : Unit}{\Sigma \vdash getchar\ e : Char} \qquad \frac{\Sigma \vdash e : Char}{\Sigma \vdash putchar\ e : Unit}$$

$$\frac{\Sigma \vdash e : String}{\Sigma \vdash readFromFile\ e : String} \qquad \frac{\Sigma \vdash e : String * String}{\Sigma \vdash writeToFile\ e : Unit}$$

Die Funktion *readFromFile* bzw. *writeToFile* erwartet als Argument bzw. als erstes Argument den Namen einer Datei.

7.1.3. Dynamische Semantik

Wir haben schon mehrfach angesprochen, dass sich die Auswertung mit dem Einzug von Effekten verändert. Diese Veränderung findet ihren Niederschlag bei der Aufstellung der dynamischen

Semantik. Zunächst einmal ist nicht unmittelbar klar, wie wir die Beweisregeln modifizieren müssen, damit wir Interaktionen mit der Umwelt modellieren können. Schließlich sind Beweisregeln genauso wenig interaktiv wie mathematische Funktionen. Überlegen wir: Ein Ausdruck hat neben einem Wert zusätzlich einen Effekt. Die dreistellige Relation $\delta \vdash e \Downarrow \nu$ taugt nicht mehr für dieses Szenario. Es liegt nahe, die Auswertungsrelation zu einer vierstelligen Relation zu erweitern, die eine Umgebung mit einem Ausdruck, einem Effekt und einem Wert in Beziehung setzt.

$$\delta \vdash e \Downarrow_t \nu$$

Den Effekt t notieren wir als Index an den Pfeil. Bleibt zu klären, was ein Effekt ist. Wir modellieren einen Effekt als Sequenz von externen Ereignissen, wobei ein einzelnes Ereignis zum Beispiel die Ein- oder Ausgabe eines einzelnen Unicode-Zeichens[2] ist.

$c \in \mathsf{Unicode}$

$t \in \mathsf{Event}^*$	Sequenz von Ereignissen
$\mathsf{Event} ::=$	Ereignis
$\mid \mathit{in}(c)$	Eingabe von c
$\mid \mathit{out}(c)$	Ausgabe von c

Wir beschränken uns auf die Definition von *getchar* und *putchar*; die dateiverarbeitenden Funktionen *readFromFile* und *writeToFile* werden analog behandelt.

$$\frac{\delta \vdash e \Downarrow_t ()}{\delta \vdash \mathit{getchar}\ e \Downarrow_{t \cdot \mathit{in}(c)} c} \qquad \frac{\delta \vdash e \Downarrow_t c}{\delta \vdash \mathit{putchar}\ e \Downarrow_{t \cdot \mathit{out}(c)} ()}$$

Wie üblich wird zunächst das Funktionsargument ausgerechnet. Dabei kann eine Folge von Ereignissen auftreten; *getchar* erweitert diese Folge um ein Eingabeereignis, *putchar* entsprechend um ein Ausgabeereignis. Schauen wir uns ein einfaches Beispiel an.

$$\frac{\dfrac{\varnothing \vdash () \Downarrow_\varepsilon ()}{\varnothing \vdash \mathit{getchar}\ () \Downarrow_{\mathit{in}(\mathtt{h})} \mathtt{'h'}}}{\varnothing \vdash \mathit{putchar}\ (\mathit{getchar}\ ()) \Downarrow_{\mathit{in}(\mathtt{h}) \cdot \mathit{out}(\mathtt{h})} ()}$$

Das leere Tupel »()« wertet zu sich selbst aus; die Auswertung hat keinen Effekt. Weiterhin sehen wir, dass *putchar* (*getchar* ()) insgesamt zu »()« auswertet und dabei die Ereignisfolge $\mathit{in}(\mathtt{h}) \cdot \mathit{out}(\mathtt{h})$ auftritt. Das ist nicht die einzige mögliche Ereignisfolge: Auch $\mathit{in}(\mathtt{a}) \cdot \mathit{out}(\mathtt{a})$ oder $\mathit{in}(\mathtt{l}) \cdot \mathit{out}(\mathtt{l})$ usw. sind denkbar, nicht aber $\mathit{in}(\mathtt{h}) \cdot \mathit{out}(\mathtt{a})$ oder $\mathit{in}(\mathtt{a}) \cdot \mathit{out}(\mathtt{h})$. Die Auswertungsrelation ist eine »echte« Relation — eine Umgebung, ein Ausdruck, eine Folge von Ereignissen und ein Wert werden zueinander in Beziehung gesetzt — und trägt damit der Tatsache Rechnung, dass viele unterschiedliche Interaktionen mit dem/der Benutzer/-in möglich sind.

Jetzt, da wir die Auswertungsrelation um ein Argument erweitert haben, müssen wir *alle* bisher aufgeführten Auswertungsregeln anpassen! Schließlich kann jeder Teilausdruck einen Effekt haben, auch zum Beispiel die Summanden einer Addition:

$$(\mathit{putstring}\ \mathtt{"hello,\ "}; 4700) + (\mathit{putstring}\ \mathtt{"world"}; 11)$$

[2] Unicode ist ein internationaler Standard, der die Kodierung und Darstellung von Schriftzeichen und Textelementen regelt. Insbesondere definiert Unicode verschiedene Zeichenkodierungen, Zuordnungen von Zeichen zu Zahlen. Zu den gängigsten Kodierungen zählen UTF-8, UTF-16 und UTF-32. In der aktuellen Version, Unicode 11.0, werden insgesamt 137.439 verschiedene Zeichen definiert, eine beeindruckende Zahl, die die immense Vielfalt von Sprachen und Schriften in Kultur und Wissenschaft widerspiegelt.

Nicht, dass dieser Programmierstil empfehlenswert ist — im Gegenteil — aber möglich sind solche Ausdrücke und somit müssen wir uns um deren Semantik kümmern. Glücklicherweise ist die Anpassung der Regeln recht einfach. Die Paarregel wird zum Beispiel wie folgt abgeändert.

$$\frac{\delta \vdash e_1 \Downarrow_{t_1} \nu_1 \qquad \delta \vdash e_2 \Downarrow_{t_2} \nu_2}{\delta \vdash (e_1, e_2) \Downarrow_{t_1 \cdot t_2} (\nu_1, \nu_2)}$$

Beide Teilausdrücke haben einen Effekt, t_1 bzw. t_2; der kumulierte Effekt des Paarausdrucks ist $t_1 \cdot t_2$. Somit treten die Effekte der ersten Komponente vor den Effekten der zweiten Komponente auf. Allgemein werden Ausdrücke von links nach rechts abgearbeitet und Effekte werden in dieser Reihenfolge sichtbar. Eine Auswertungsregel der Form

$$\frac{\delta_1 \vdash e_1 \Downarrow \nu_1 \qquad \cdots \qquad \delta_n \vdash e_n \Downarrow \nu_n}{\delta \vdash e \Downarrow \nu}$$

muss somit wie folgt erweitert werden:

$$\frac{\delta_1 \vdash e_1 \Downarrow_{t_1} \nu_1 \qquad \cdots \qquad \delta_n \vdash e_n \Downarrow_{t_n} \nu_n}{\delta \vdash e \Downarrow_{t_1 \cdot \ldots \cdot t_n} \nu}$$

Die Reihenfolge der Effekte wird durch die Konkatenation der Ereignissequenzen festgelegt.

Die Einführung von effektvollen Ausdrücken hat einen dramatischen Effekt auf die Semantik unserer Programmiersprache. Diese legt nunmehr pedantisch fest, in welcher Reihenfolge ein Programm abgearbeitet wird. Das ist in gewisser Weise ein Rückschritt. Bis dato konnten zum Beispiel die Teilausdrücke in $e_1 + e_2$ gleichzeitig oder im Fachjargon ***parallel*** ausgerechnet werden. Jetzt ist die sequentielle Auswertung die Norm. Wenn wir eine parallele Auswertung wegen des möglichen Geschwindigkeitsvorteils bevorzugen, dann müssen wir sicherstellen, dass e_1 keine Effekte hat, dass also stets $e_1 \Downarrow_\varepsilon \nu_1$ gilt. Diese Eigenschaft ist wie viele andere nicht formal entscheidbar, so dass man sich mit Näherungen an das tatsächliche Verhalten zufriedengeben muss. Tatsächlich ist die Parallelisierung von Programmen eine der großen Herausforderungen der Informatik. Trotz existierender Hardwareunterstützung (Stichwort: Multi-Core Prozessor), werden viele Programme weiterhin streng sequentiell ausgewertet.

7.1.4. Vertiefung

Eingabe mit Validierung Wir haben schon angesprochen, dass interaktive Programme wegen ihrer Interaktionen schwieriger zu lesen und zu verstehen sind als effektfreie Programme. Aus diesem Grund sollte man versuchen, Effekte auf einige wenige Funktionen zu beschränken und so viel wie möglich effektfrei zu rechnen. Wie dies auch für hochgradig interaktive Programme gelingen kann, wollen wir uns im Folgenden ansehen.

Die Programme aus der Einleitung zeigen, wie man systematisch Daten einliest; sie prüfen die Eingaben aber nicht auf Plausibilität.

```
⋙ query "age: "
age : hello, world
"hello, world"
```

Offenbar soll das Alter abgefragt werden, als Eingabe wird aber ein beliebiger String akzeptiert. Es wäre wünschenswert, wenn fehlerhafte Eingaben erkannt werden und die Eingabe entsprechend wiederholt wird. Was aber ist eine fehlerhafte Eingabe? Das hängt vom jeweiligen Anwendungsfall ab: Eine Altersangabe ist eine höchstens dreistellige natürliche Zahl; ein Vorname besteht aus Buchstaben und vielleicht einigen Sonderzeichen. Mit anderen Worten, die interaktive Funktion *query* kann nicht beurteilen, ob eine Eingabe gültig ist. Diese Erkenntnis legt nahe, *query*

mit einem ***Validator*** zu parametrisieren. Ein Validator bildet einen String auf ein Element des folgenden Datentyps ab.

```
type Result ⟨'value⟩ =
  | Okay of 'value
  | Error of String
```

Der Variantentyp ist eine Variante ;-) von *Option*: *Okay* entspricht *Some*, *Error* korrespondiert zu *None*. Der Konstruktor *Error* bietet im Unterschied zu *None* zusätzlich die Möglichkeit, anzugeben, warum eine Validierung gescheitert ist. Also: Ist der String zulässig, wird *Okay value* zurückgegeben, wobei *value* der semantische Wert des Strings ist, zum Beispiel eine natürliche Zahl; schlägt die Validierung fehl, wird *Error msg* zurückgegeben, wobei *msg* eine aussagekräftige Fehlermeldung ist. Nach diesen Vorarbeiten können wir eine validierende Version von *query* definieren:

```
let rec checked-query (prompt : String,
                       check : String → Result ⟨'value⟩) : 'value =
  match check (query (prompt ^ ":  ")) with
  | Okay v      → v
  | Error msg → putline ("***  " ^ msg);
                checked-query (prompt, check)
```

Es werden solange Eingaben angefordert, bis die Eingabe von *check* abgesegnet wird. Im Fehlerfall wird der/die Benutzer/-in auf den Fehler hingewiesen.

Validatoren sind einfache, effektfreie Funktionen: *is-nat* zum Beispiel überprüft, ob die Eingabe eine nicht-leere Folge von Ziffern ist.

```
let is-nat (s : String) : Result ⟨Nat⟩ =
  if s <> "" && String.forall Char.IsDigit s then
    Okay (Nat.Parse s)
  else
    Error "natural number expected"
```

Bei der Definition greifen wir auf die Funktion

```
forall : (Char → Bool) → String → Bool
```

zurück, die überprüft, ob alle Zeichen eines Strings das angegebene Prädikat erfüllen. Die Funktion *is-nat* ist im Prinzip ein einfacher Parser (!), der einen String in einen semantischen Wert überführt oder fehlschlägt. Sind die Eingabedaten komplizierter, so bietet es sich in der Tat an, eine Grammatik für die Menge aller zulässigen Eingaben aufzustellen und mit den Methoden aus Abschnitt 6.5.3 einen Parser zu konstruieren. Wenn der Parser die Eingabe nicht akzeptiert, muss man sich zusätzlich darum kümmern, eine aussagekräftige Fehlermeldung zu generieren.

Die folgende Interaktion zeigt *checked-query* in Aktion.

```
>>>  checked-query ("age", is-nat)
age : Hello, world !
*** natural number expected
age : 4711
4711
```

Als Ergebnis des Aufrufs wird eine Zahl zurückgegeben, kein String. Natürlich ist 4711 ein extrem hohes Alter. Wir sollten zusätzlich verlangen, dass die Angabe kleiner als 123 ist.[3]

[3] Warum 123? Als bis dato ältester Mensch der Welt gilt Jeanne Calment (1875–1997) mit 122 Jahren und 164 Tagen.

```
⋙ checked-query ("age", both (is-nat, is-less 123))
age : Ralf
* * * natural number expected
age : 4711
* * * number must be less than 123
age : 41
41
```

Die Funktion *both* kombiniert zwei Validatoren: *both* (*is-nat*, *is-less* 123) fordert, dass die Eingabe eine Folge von Ziffern ist *und* dass die korrespondierende Zahl kleiner als 123 ist. Um den String nicht wiederholt in eine Zahl umwandeln zu müssen, wird der semantische Wert des ersten Validators an den zweiten Validator weitergereicht: *is-nat* vom Typ *String* → *Result* ⟨*Nat*⟩ wird so mit *is-less* 123 vom Typ *Nat* → *Result* ⟨*Nat*⟩ kombiniert.

```
let both (first : 'a → Result ⟨'b⟩, second : 'b → Result ⟨'c⟩) : 'a → Result ⟨'c⟩ =
  fun x → match first x with
    | Okay y     → second y
    | Error msg → Error msg
```

Die Funktion ist »sehr polymorph«: *first* und *second* dürfen fast beliebige Argument- und Ergebnistypen haben; lediglich der Ergebnistyp des ersten Validators muss zum Argumenttyp des zweiten passen. Die Funktion *is-less* kleidet im Wesentlichen die Vergleichsoperation < in *Okay* bzw. *Error* ein.

```
let is-less (n : Nat) : Nat → Result ⟨Nat⟩ = fun m →
  if m < n then Okay m
           else Error ("number must be less than " ^ show n)
```

Mit Hilfe von *checked-query* können wir auch Eingaben auf eine vorgegebene Auswahl von Strings beschränken.

```
let choice (prompt : String, choices : List ⟨String⟩) : String =
  checked-query (prompt,
    fun s → if contains s choices
            then Okay s
            else Error ("choices: " ^ concat ", " choices))
```

Die Funktion

```
concat : String → List ⟨String⟩ → String
```

konkateniert eine Liste von Strings und fügt zwischen je zwei Elemente den angegebenen Separator, erstes Argument, ein. Die folgende Interaktion illustriert die Verwendung von *choice*.

```
⋙ choice ("gender", ["f";"m";"female";"male"])
gender : sehr maskulin
* * * choices : f, m, female, male
gender : m
"m"
```

Mit diesen Zutaten können wir die Funktion *input-person* neu definieren, diesmal inklusive Validierung der getätigten Eingaben.

```
let input-person () : Person =
  if contains (choice ("gender", ["f";"m";"female";"male"])) ["f";"female"]
  then
    Female {name = checked-query ("name    ", is-name)}
  else
    Male {name = checked-query ("name    ", is-name);
          bald = contains (choice ("bald?  ", ["y";"n";"yes";"no"])) ["y";"yes"]}
```

Die Funktion *is-name* überprüft, ob die Eingabe ein gültiger Name ist. Die Definition ist der Phantasie der Leserin oder des Lesers überlassen.

module Effects.Trace

Tracing Wechseln wir das Thema: Ausgaben können auch beim Testen von Programmen nützliche Dienste leisten. Etwa, wenn wir wissen wollen, mit welchen aktuellen Parametern eine Funktion aufgerufen wird oder welche Ergebnisse sie zurückliefert.

```
let rec factorial (n : Nat) : Nat =
  if n = 0 then
    Return 1
  else
    Return (Call factorial (n - 1) * n)
```

Mit Hilfe von *Return* wird der (Rückgabe-) Wert eines Ausdrucks protokolliert; mit Hilfe von *Call* der aktuelle Parameter einer Funktion. Wir stellen die Definition von *Return* und *Call* zurück und schauen uns zunächst einige Anwendungen an.

```
⋙  Call factorial 10
call   10
call   9
call   8
call   7
call   6
call   5
call   4
call   3
call   2
call   1
call   0
return 1
return 1
return 2
return 6
return 24
return 120
return 720
return 5040
return 40320
return 362880
return 3628800
3628800
```

Man sieht sehr schön, wie der aktuelle Parameter auf dem Hinweg zur Rekursionsbasis schrittweise verkleinert wird und wie auf dem Rückweg der Funktionswert anschwillt.

Die Rekursion muss nicht immer linear sein. Die ***Fibonacci-Funktion*** demonstriert ein lebhafteres Auf und Ab.

```
let rec fibonacci (n : Nat) : Nat =
  Return (if n ⩽ 1 then n
                   else Call fibonacci (n − 1) + Call fibonacci (n − 2))
```

Die Funktion ist nach dem italienischen Mathematiker Leonardo da Pisa, genannt Fibonacci, benannt, der mit dieser Funktion das Wachstum einer Kaninchenpopulation modellierte, siehe Abbildung 2.2. Die Funktion beantwortet die Frage »Wie viele Kaninchenpaare entstehen nach n Monaten aus einem einzigen Paar, wenn jedes Paar ab dem zweiten Lebensmonat ein weiteres Paar auf die Welt bringt?«. Nach dem ersten Monat gibt es ein Paar; danach erhöht sich die Zahl der Paare, *fibonacci* $(n-1)$, um die Zahl der geschlechtsreifen Paare, *fibonacci* $(n-2)$. Abbildung 7.1 zeigt das Auf und Ab der rekursiven Aufrufe von *fibonacci* 6 (und lässt reichlich Platz für Notizen). Man sieht sehr schön, dass wiederholt die gleichen Aufrufe getätigt werden (*call* 2 tritt fünfmal auf) und immer wieder neu berechnet werden. In Abschnitt 7.2 werden wir uns damit beschäftigen, wie man diese wiederholten Berechnungen vermeiden kann.

Es bleibt, die Definitionen von *Return* und *Call* nachzureichen.

```
let Return (x : 'a) : 'a =
  putline ("return " ^ show x); x
```

Wertmäßig ist *Return* die Identität: Das Argument wird als Ergebnis zurückgegeben. Damit *Return* für beliebige Werte verwendet werden kann, abstrahieren wir vom Typ des Arguments und verwenden *show*, um den beliebigen Wert in einen String zu überführen.

```
let Call (f : 'a → 'b) : 'a → 'b =
  fun x → putline ("call   " ^ show x); f x
```

Wertmäßig ist *Call* die Identität von Funktionen. Deswegen abstrahieren wir über zwei Typen: den Argument- und den Ergebnistyp der Funktion.

Übungen.

1. Schreiben Sie Funktionen, um eine Liste von natürlichen Zahlen auszugeben bzw. einzulesen. Wie lassen sich die Funktionen auf beliebige Listen verallgemeinern?

2. In Abschnitt 5.2.1 haben wir Funktionen für die Verwaltung von Personaldaten implementiert. Schreiben Sie ein interaktives Programm, um Personaldaten einzugeben und Personaldaten herauszusuchen. Verwenden Sie *readFromFile* und *writeToFile*, um die Stammdaten über eine interaktive Sitzung hinaus persistent zu speichern.

7.2. Zustand

Assignment is undoubtedly the most characteristic feature of programming a digital computer, and one that most clearly distinguishes it from other branches of mathematics.

— C.A.R. Hoare (1934), *CACM 12(10), 1969*

Wir haben im letzten Abschnitt gesehen, wie wir die Abarbeitung rekursiver Funktionen am Bildschirm protokollieren können. Versieht man verschiedene Funktionen mit Kontrollausgaben, so

```
⋙  Call fibonacci 6
call    6
call    5
call    4
call    3
call    2
call    1
return 1
call    0
return 1
return 2
call    1
return 1
return 3
call    2
call    1
return 1
call    0
return 1
return 2
return 5
call    3
call    2
call    1
return 1
call    0
return 1
return 2
call    1
return 1
return 3
return 8
call    4
call    3
call    2
call    1
return 1
call    0
return 1
return 2
call    1
return 1
return 3
call    2
call    1
return 1
call    0
return 1
return 2
return 5
return 13
```

Abbildung 7.1.: Trace von *fibonacci* 6.

werden die Protokolle schnell unübersichtlich, so dass der Wunsch aufkommt, die Ausgaben gezielt an- und ausschalten zu können. Eine solche ***Außensteuerung*** ist auch nützlich, wenn man die Protokollierung insgesamt ausschalten, die Protokollanweisungen *Return* und *Call* aber im Programm belassen möchte.

Funktionen können bis dato nur über das Funktionsargument von außen gesteuert werden. Diese Art der Steuerung ist für unser Szenario ungeeignet: Um das Protokoll an- oder auszuschalten, müssten wir das Programm an vielen verschiedenen Stellen ändern — überall dort, wo Protokollanweisungen stehen. Wir wünschen uns einen globalen Schalter, nicht viele lokale. Mit den bisherigen Mitteln lässt sich ein globaler Schalter nicht bewerkstelligen; wir benötigen ein neues Sprachkonstrukt. Die grundlegende Idee ist, ein Gedächtnis bzw. einen Speicher einzuführen, der abgefragt und manipuliert werden kann. Ein Schalter kann dann durch einen Speicher bzw. eine ***Speicherzelle*** realisiert werden, die einen Booleschen Wert enthält.

```
let trace = ref false
```

Der Ausdruck *ref false* legt eine neue Speicherzelle an. Im Fachjargon sagt man, die Speicherzelle wird ***allokiert***. Eine Speicherzelle ist wie ein Behälter oder eine Schublade. Der initiale ***Inhalt*** der allokierten Speicherzelle ist *false*. Als Ergebnis des Aufrufs gibt *ref* die ***Adresse*** der allokierten Speicherzelle zurück. Diese Adresse benötigen wir, um den Inhalt der Speicherzelle später abzufragen oder zu verändern. Aus diesem Grund binden wir die Adresse an den Bezeichner *trace*. Die Adresse hat den Typ *Ref ⟨Bool⟩*. Der Bezeichner *trace* ist also kein Boolescher Wert, sondern er verweist auf einen Booleschen Wert (*ref* bzw. *Ref* kürzt ***reference*** ab, engl. für ***Verweis*** oder Referenz).

Bezeichnet *e* die Adresse einer Speicherzelle, so ermittelt !*e* den Inhalt der Speicherzelle (lies: »bang e«, engl. für Knall nicht deutsch für ängstlich); *e* muss ein Ausdruck vom Typ *Ref ⟨t⟩* sein, !*e* ist dann entsprechend ein Ausdruck vom Typ *t*. Mit !*trace* lässt sich somit der Zustand des Schalters abfragen. Damit können wir eine Version von *Return* definieren, die sich von außen über den Schalter steuern lässt (*Call* wird analog behandelt).

```
let Return (x : 'value) : 'value =
  (if !trace then putline ("return " ^ show x) else ()); x
```

Nur wenn der Inhalt der Speicherzelle *true* ist, erfolgt die Kontrollausgabe. Die Alternative *if* e_1 *then* e_2 *else* () lässt sich übrigens zu *if* e_1 *then* e_2 abkürzen. (Die einarmige Alternative ergibt aber nur Sinn, wenn der *then*-Zweig den Typ *Unit* hat.)

Mit Hilfe der ***Zuweisung*** $e_1 := e_2$ können wir schließlich den Inhalt der von e_1 referenzierten Speicherzelle durch den Wert von e_2 ersetzen (lies: e_1 wird zu e_2); e_1 muss den Typ *Ref ⟨t⟩* besitzen und e_2 den Typ *t*. Der Wert der Zuweisung ist »()«, unser liebgewonnener Dummywert. Der Ausdruck *trace* := *true* schaltet somit die Protokollierung an und *trace* := *false* entsprechend aus.

```
⋙ factorial 1
1
⋙ trace := true
()
⋙ !trace
true
⋙ factorial 1
call   0
return 1
return 1
1
⋙ trace := false
()
⋙ !trace
false
⋙ factorial 1
1
```

Die Interaktion zeigt, dass auch »!« keine Funktion im mathematischen Sinne ist: Der gleiche Aufruf, !*trace*, führt zu zwei unterschiedlichen Ergebnissen.

Speicherzellen können beliebige Werte enthalten: Boolesche Werte, natürliche Zahlen, Funktionen, Adressen anderer Speicherzellen usw. Eine Speicherzelle vom Typ *Ref* ⟨*Nat*⟩ kann zum Beispiel verwendet werden, um ein Bankkonto zu modellieren.

module Effects.Bank

```
module Account =
  let private funds = ref 0
  let deposit (amount : Nat) =
    funds := !funds + amount
  let withdraw (amount : Nat) =
    let old = !funds
    funds := !funds – amount
    old – !funds
  let balance () = !funds
```

Mit **ref** 0 wird eine mit 0 initialisierte Speicherzelle allokiert, die Repräsentation des Kontostands. Die Funktion *deposit* modelliert eine Einzahlung, *withdraw* eine Auszahlung. Der Ausdruck *funds* := !*funds* + *amount* erhöht den Inhalt der Speicherzelle um den Betrag *amount* und ist ein typisches Idiom für Speicherzellen vom Typ *Ref* ⟨*Nat*⟩. Die Funktion *withdraw* gibt als Ergebnis den tatsächlich ausgezahlten Betrag zurück; (fast) wie im richtigen Leben kann der Kontostand nicht negativ werden. Mit *balance* kann der Kontostand abgefragt werden.

Die Deklaration der Speicherzelle ist lokal zu den Deklarationen der drei Funktionen. Der Zusatz **private** stellt sicher, dass der Bezeichner nur innerhalb des Moduls, nicht aber außerhalb sichtbar ist. Warum schränken wir die Sichtbarkeit ein? Nun, wir wollen sicherstellen, dass der Kontostand nur indirekt mit Hilfe von *deposit* und *withdraw* manipuliert wird und nicht etwa direkt über eine Zuweisung. Heimliche Kontomanipulationen sind ein in der Bankenwelt ungern gesehener Vorgang. Die Speicherzelle *funds* existiert zwar — Speicherzellen leben ewig — aber sie kann außerhalb des Moduls nicht direkt angesprochen werden. (Das ist ähnlich wie bei der Post: Um jemandem einen Brief zu schicken, benötigt man ihre oder seine Adresse; hat man die Adresse nicht, so folgt daraus nicht, dass die- oder derjenige nicht existiert.) Die folgende Interaktion demonstriert Ein- und Auszahlungen.

```
>>> Account.deposit 4711
()
>>> Account.withdraw 815
815
>>> Account.withdraw 2765
2765
>>> Account.withdraw 2765
1131
>>> Account.withdraw 2765
0
```

Auch hier wird deutlich, dass *withdraw* keine mathematische Funktion ist: drei Aufrufe der Form *withdraw* 2765, drei unterschiedliche Funktionsergebnisse. Diese Eigenschaft — nicht-mathematisch — ähnelt einer ansteckenden Krankheit: *withdraw* greift auf »!« zurück und steckt sich an.

7.2.1. Abstrakte Syntax

Wir erweitern Mini–F# um Sprachkonstrukte zur Speichermanipulation.

$e ::= \cdots$	***Speichermanipulation:***
$\mid$ ***ref*** e	Allokation
$\mid\ !e$	Dereferenzierung
$\mid\ e_1 := e_2$	Zuweisung

Der Ausdruck ***ref*** e allokiert eine Speicherzelle und gibt die Adresse der bzw. eine Referenz auf die Speicherzelle zurück. Aus diesem Grund heißt der Zugriff $!e$ auch Dereferenzierung. Die Zuweisung ist ein charakteristisches Merkmal der meisten Programmiersprachen (siehe auch das Zitat am Anfang des Abschnitts).

7.2.2. Statische Semantik

Adressen erhalten einen Referenztyp; dieser ist mit dem Typ des Inhaltes parametrisiert.

$t ::= \cdots$	***Typen:***
$\mid\ \mathit{Ref}\ \langle t \rangle$	Referenztyp

Bevor wir uns die Typregeln anschauen, lohnt es sich, noch einmal eine der Grundprinzipien von Mini–F# ins Gedächtnis zu rufen: Ausdrücke können beliebig miteinander kombiniert werden. Die Zuweisung $e_1 := e_2$ ist ein Ausdruck und kann überall dort verwendet werden, wo ein Ausdruck verlangt wird. Die linke Seite der Zuweisung ist ebenfalls ein Ausdruck. Als einzige Einschränkung verlangen wir, dass e_1 zu einer Adresse auswertet und dass die rechte Seite zur linken passt. Diese Einschränkungen formulieren wie immer die Typregeln.

$$\frac{\Sigma \vdash e : t}{\Sigma \vdash \textbf{\textit{ref}}\ e : \mathit{Ref}\ \langle t \rangle} \qquad \frac{\Sigma \vdash e : \mathit{Ref}\ \langle t \rangle}{\Sigma \vdash\ !e : t} \qquad \frac{\Sigma \vdash e_1 : \mathit{Ref}\ \langle t \rangle \qquad \Sigma \vdash e_2 : t}{\Sigma \vdash e_1 := e_2 : \mathit{Unit}}$$

Die Deklaration ***let*** p = (***ref*** *false*, ***ref*** 0) zum Beispiel bindet p an einen Wert vom Typ $\mathit{Ref}\ \langle \mathit{Bool} \rangle * \mathit{Ref}\ \langle \mathit{Nat} \rangle$. Bezüglich dieser Deklaration sind sowohl $!(\mathit{fst}\ p)$ als auch $\mathit{snd}\ p := 4711$ zulässige Ausdrücke. Die linke Seite der Zuweisung hat den Typ $\mathit{Ref}\ \langle \mathit{Nat} \rangle$, ist also eine Adresse, und die rechte Seite vom Typ Nat passt dazu.

7.2.3. Dynamische Semantik

Die drei neuen Konstrukte manipulieren einen sogenannten Hauptspeicher. Der Zusatz »Haupt« grenzt den Speicher vom Hintergrundspeicher ab, auf dem Daten persistent gespeichert werden. Daten im Hauptspeicher sind flüchtig: Sie überdauern eine Programmausführung bzw. eine interaktive Sitzung nicht.

Ein Speicher ist eine endliche Abbildung von Adressen auf Werte.

$a \in \mathsf{Addr}$	***Adressen***
$\sigma \in \mathsf{Addr} \to_{\mathrm{fin}} \mathsf{Val}$	***Speicher***

Den Bereich der Adressen lassen wir abstrakt; wir fordern nur, dass es unendlich viele Adressen gibt.

Die speichermanipulierenden Konstrukte haben wie die Ein- und Ausgabefunktionen neben einem Wert zusätzlich einen Effekt. Der Effekt besteht hier in der Veränderung des Speichers. Wie auch im letzten Abschnitt müssen wir die Auswertungsrelation erweitern, um den Effekt beschreiben zu können. Aus der dreistelligen Relation $\delta \vdash e \Downarrow \nu$ wird eine fünfstellige Relation

$$\delta \vdash \sigma \parallel e \Downarrow \nu \parallel \sigma'$$

Der Ausdruck e wertet zu ν aus und bewirkt zusätzlich eine Zustandsänderung: σ ist der Speicher vor der Auswertung von e und σ' ist der Speicher nach der Auswertung. Eigentlich müssten wir die vierstellige Relation $\delta \vdash e \Downarrow_t \nu$ des letzten Abschnitts zu einer sechsstelligen Relation

$$\delta \vdash \sigma \parallel e \Downarrow_t \nu \parallel \sigma'$$

erweitern, aber das wollen wir aus Gründen der Übersichtlichkeit nicht tun. In der Tat verändern die Ein- und Ausgabefunktionen nicht den Zustand und umgekehrt berühren die speichermanipulierenden Konstrukte nicht die Ereignisfolge. Ebenfalls im Interesse der Leserlichkeit lassen wir in diesem Abschnitt die Umgebung δ unter den Tisch fallen — keine der folgenden Regeln benötigt oder manipuliert die Umgebung.

Da der Ausdruck ***ref*** e eine Adresse zurückgibt, müssen wir noch den Bereich der Werte um Adressen erweitern.

$\nu ::= \cdots$	***Werte:***
$\mid a$	Adresse

Nach diesen Vorarbeiten können wir die dynamische Semantik der Konstrukte festlegen.

$$\frac{\sigma \parallel e \Downarrow \nu \parallel \sigma'}{\sigma \parallel \textbf{\textit{ref}}\ e \Downarrow a \parallel \sigma', \{a \mapsto \nu\}} \quad a \notin \mathit{dom}\ \sigma'$$

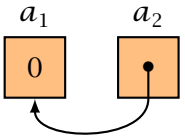
$$\frac{\sigma \parallel e \Downarrow a \parallel \sigma'}{\sigma \parallel\ !e \Downarrow \sigma'(a) \parallel \sigma'}$$

$$\frac{\sigma \parallel e_1 \Downarrow a \parallel \sigma_1 \qquad \sigma_1 \parallel e_2 \Downarrow \nu \parallel \sigma_2}{\sigma \parallel e_1 := e_2 \Downarrow () \parallel \sigma_2, \{a \mapsto \nu\}}$$

Generell gilt, dass zunächst die Teilausdrücke ausgerechnet werden. Im Fall von ***ref*** e wird zunächst e ausgewertet; diese Auswertung kann den Speicher verändern: σ wird zu σ'. Dann wird eine beliebige Adresse bestimmt, die nicht im Definitionsbereich von σ' enthalten ist: a ist diese

»frische« Adresse. Schließlich wird σ' um eine neue Speicherzelle, $\{a \mapsto v\}$, erweitert (»,« ist wie immer der Kommaoperator). Schauen wir uns die Auswertung von ***ref*** (***ref*** 0) an.

$$\dfrac{\dfrac{\varnothing \parallel 0 \Downarrow 0 \parallel \varnothing}{\varnothing \parallel \textbf{\textit{ref}}\ 0 \Downarrow a_1 \parallel \{a_1 \mapsto 0\}}}{\varnothing \parallel \textbf{\textit{ref}}\ (\textbf{\textit{ref}}\ 0) \Downarrow a_2 \parallel \{a_1 \mapsto 0, a_2 \mapsto a_1\}}$$



Zunächst wird die Auswertung von ***ref*** 0 und dann die Auswertung von 0 angestoßen; 0 wertet zu 0 aus, ohne den leeren Speicher zu verändern; dann wird eine Speicherzelle angelegt $\{a_1 \mapsto 0\}$ und schließlich eine zweite $\{a_2 \mapsto a_1\}$.

Die Dereferenzierung ist ein ***lesender Speicherzugriff***. Die Auswertung von e kann den Speicher verändern; der eigentliche Zugriff ist aber effektfrei: Der modifizierte Speicher σ' wird nicht mehr verändert.

Im Gegensatz dazu ist $e_1 := e_2$ ein ***schreibender Speicherzugriff***. Die Auswertung von e_1 kann den Speicher verändern: σ wird zu σ_1. Die Auswertung von e_2 »sieht« den modifizierten Speicher und ändert ihn zu σ_2. Die Zuweisung selbst schließlich modifiziert σ_2 zu $\sigma_2, \{a \mapsto v\}$: der Inhalt der durch a adressierten Speicherzelle wird mit v überschrieben.

Ähnlich wie im letzten Abschnitt müssen wir *alle* bisher aufgeführten Auswertungsregeln anpassen! Wie illustrieren die Änderungen zunächst an der Paarregel.

$$\dfrac{\sigma_0 \parallel e_1 \Downarrow v_1 \parallel \sigma_1 \qquad \sigma_1 \parallel e_2 \Downarrow v_2 \parallel \sigma_2}{\sigma_0 \parallel (e_1, e_2) \Downarrow (v_1, v_2) \parallel \sigma_2}$$

Beide Teilausdrücke verändern potentiell den Speicher: e_1 ändert σ_0 zu σ_1, wie bei der Zuweisung »sieht« e_2 den modifizierten Speicher und ändert ihn zu σ_2. Die kumulierte Änderung von σ_0 zu σ_2 ist der Effekt des Paarausdrucks. Allgemein gilt, wie auch im letzten Abschnitt, dass Ausdrücke von links nach rechts abgearbeitet werden und Effekte auch in dieser Reihenfolge sichtbar werden. Eine Auswertungsregel der Form

$$\dfrac{e_1 \Downarrow v_1 \qquad e_2 \Downarrow v_2 \qquad \cdots \qquad e_n \Downarrow v_n}{e \Downarrow v}$$

wird wie folgt angepasst:

$$\dfrac{\sigma_0 \parallel e_1 \Downarrow v_1 \parallel \sigma_1 \qquad \sigma_1 \parallel e_2 \Downarrow v_2 \parallel \sigma_2 \qquad \cdots \qquad \sigma_{n-1} \parallel e_n \Downarrow v_n \parallel \sigma_n}{\sigma_0 \parallel e \Downarrow v \parallel \sigma_n}$$

Der Zustand wird jeweils von Teilausdruck zu Teilausdruck weitergereicht. Man sagt auch, der Zustand wird durchgefädelt (engl. threading).

7.2.4. Vertiefung

Tracing Kommen wir noch einmal auf die Protokollierung von Funktionsargumenten und Funktionswerten zurück. Wir haben in der Einleitung eine Speicherzelle vom Typ *Ref ⟨Bool⟩* eingeführt, um die Protokollierung von außen an- und auszuschalten. Diese Speicherzelle war in allen nachfolgenden Definitionen und Ausdrücken sichtbar. Man sollte sich frühzeitig angewöhnen, die Sichtbarkeit von Speicherzellen mit lokalen ***let***-Bindungen oder mit Hilfe von Modulen und ***private***-Annotationen zu begrenzen, so wie wir das im Fall des Bankkontos gemacht haben. Eine entsprechend modifizierte Version könnte zum Beispiel wie folgt aussehen:

```
module Trace
  let private trace = ref false
  let trace-on () =
    trace := true
  let trace-off () =
    trace := false
  let traceline (s : String) =
    if !trace then putline s
```

Die Sichtbarkeit von *trace* wird auf drei Funktionen eingeschränkt: *traceline* ist eine »*trace*-sensitive« Version von *putline*, mit Hilfe von *trace-on* bzw. *trace-off* wird die Protokollierung an- bzw. abgeschaltet. Die Funktionen *Return* und *Call* können wir damit wie folgt definieren (der Aufruf von *putline* in der ursprünglichen Fassung ist einfach durch *traceline* ersetzt worden).

```
let Return (x : 'a) : 'a =
  Trace.traceline ("return " ^ show x); x
let Call (f : 'a -> 'b) : 'a -> 'b =
  fun x → Trace.traceline ("call   " ^ show x); f x
```

Der Zustand des Schalters kann nur mit Hilfe von *trace-on* und *trace-off* manipuliert werden. Man spricht in diesem Zusammenhang auch von ***Kapselung***. Die Tatsache, dass die Funktionen eine Speicherzelle vom Typ *Ref* ⟨*Bool*⟩ verwenden, ist nach außen nicht sichtbar. Was ist der Vorteil der gekapselten Version? Auf den ersten Blick macht es keinen großen Unterschied, ob die Protokollierung mit *trace* := *true* oder mit *trace-on* () eingeschaltet wird. Der Vorteil der gekapselten Version ist, dass sich die Implementierung leicht ändern und erweitern lässt. Zum Beispiel, wenn wir das An- und Ausschalten selbst protokollieren wollen. Bei der gekapselten Version ist die Änderung lokal: Wir müssen nur die Definition von *trace-on* und *trace-off* modifizieren.

```
let trace-on () =
  trace := true; putline "TRACE ON"
let trace-off () =
  trace := false; putline "TRACE OFF"
```

Bei der ursprünglichen Variante ist die Änderung global: Jedes Vorkommen von *trace* := *true* muss um *putline* "TRACE ON" erweitert werden.

module Effects.CountingFib

Memoisierung Wenden wir uns einem anderen Thema zu: Wenn wir ein Programm optimieren wollen, dann ist es nützlich zu wissen, wie oft eine bestimmte Funktion aufgerufen wird. (Wir erinnern uns: Man sollte nicht blindlings optimieren; es gilt, den oder die Laufzeitverbrecher zu finden. Dazu muss man, wie in jedem guten Krimi, zunächst Daten sammeln.) Zu diesem Zweck können wir einen Zähler, eine Speicherzelle vom Typ *Ref* ⟨*Nat*⟩, verwenden.

```
let counter = ref 0
let rec fibonacci (n : Nat) : Nat =
  counter := !counter + 1
  if n ⩽ 1 then
    n
  else
    fibonacci (n − 1) + fibonacci (n − 2)
```

Die Berechnung von *fibonacci n* ist aufwändig, wie die folgende Interaktion zeigt.

```
⋙ counter := 0; let f = fibonacci 10 in (f, !counter)
(55, 177)
⋙ counter := 0; let f = fibonacci 20 in (f, !counter)
(6765, 21891)
```

Die Anzahl der Aufrufe übersteigt den Wert der Fibonaccifunktion in beiden Fällen. Natürlich können wir auch *effektfrei* zählen, indem wir neben dem eigentlichen Wert zusätzlich die Anzahl der Aufrufe zurückgeben.

```
let rec counting-fibonacci (n : Nat) : Nat * Nat =
  if n ⩽ 1 then
    (n, 1)
  else
    let (f1, c1) = counting-fibonacci (n - 1)
    let (f2, c2) = counting-fibonacci (n - 2)
    (f1 + f2, c1 + c2 + 1)
```

Im Basisfall zählen wir nur den Aufruf selbst; im Rekursionsschritt kommt zu diesem Aufruf noch die Summe aus den beiden rekursiven Aufrufen hinzu. Man sieht, wir müssen uns bei der effektfreien Version mehr abstrampeln, aber der Einsatz wird auch belohnt: Aus der resultierenden Definition lässt sich ablesen, dass die Zahl c der Aufrufe für die Berechnung von *fibonacci n* fast doppelt so groß ist wie der Funktionswert von *fibonacci* $(n+1)$, es gilt: $c = 2 \cdot \mathit{fibonacci}\,(n+1) - 1$.

Das Problem bei der Berechnung von *fibonacci* ist, dass die gleichen Funktionswerte wiederholt berechnet werden. So wird beispielsweise *fibonacci* 8 bei der Berechnung von *fibonacci* 20 insgesamt 233 mal (= *fibonacci* 13) neu ausgerechnet. Da *fibonacci* eine mathematische Funktion ist, sind die wiederholten Berechnungen redundant, der Wert ist stets der gleiche. Eine naheliegende Idee ist, sich die Werte vorheriger Aufrufe zu merken und dann auf die memorierten Werte zurückzugreifen. Mit Hilfe eines Arrays lässt sich eine Funktion leicht tabellieren: `[| for i in 0 .. 99 → fibonacci i |]`. Abstrahieren wir von 99 und von *fibonacci*, erhalten wir

module Effects.Memoization

```
let memo (dom : Nat, f : Nat → 'value) : Nat → 'value =
  let
    memo-table = [| for i in 0 .. dom - 1 → f i |]
  in
    fun (n : Nat) → memo-table.[n]
let memo-fibonacci = memo (100, fibonacci)
```

Unglücklicherweise dauert die Auswertung von *memo-fibonacci* extrem (!) lange, da zunächst die Tabelle vollständig gefüllt wird. Die Werte von *fibonacci* 0 bis *fibonacci* 99 werden berechnet, ohne dass klar ist, ob diese später überhaupt benötigt werden. Eigentlich schwebt uns eine ***bedarfsgetriebene*** Füllung der Tabelle vor: Erst wenn ein Funktionswert angefordert wird, berechnet *memo* den entsprechenden Tabelleneintrag. Wenn wir Tabelleneinträge ändern wollen, müssen wir statt einem Array von Zahlen ein Array von Speicherzellen verwenden. Jede Speicherzelle nimmt dabei einen von zwei möglichen Zuständen an: »der Funktionswert wurde noch nicht berechnet« oder »der Wert wurde berechnet und er lautet …«. Die beiden Zustände können wir mit Elementen des Datentyps *Option* modellieren: *None* bzw. *Some value*, wobei *value* der berechnete Wert ist. Die Memotabelle hat somit insgesamt den furchteinflößenden Typ *Array* ⟨*Ref* ⟨*Option* ⟨'*a*⟩⟩⟩ statt *Array* ⟨'*a*⟩ wie bisher.

```
let memo (dom : Nat, f : Nat → 'value) : Nat → 'value =
  let
    memo-table = [| for i in 0 .. dom − 1 → ref None |]
  in
    fun (n : Nat) → match !memo-table.[n] with
                    | None   → let v = f n
                               memo-table.[n] := Some v
                               v
                    | Some v → v
let memo-fibonacci = memo (100, fibonacci)
```

Die Auswertung der beiden Deklarationen dauert nunmehr keinen Fingerschnips. Jetzt tritt eine lange (!) Stille ein, wenn wir zum Beispiel *memo-fibonacci* 99 aufrufen. Ist der Wert nach Hunderten von Jahren bestimmt, dann wird jeder weitere Aufruf sofort bedient. Aber, warum das lange Warten? Nun, die Memoisierung greift nicht beim Füllen der Tabelle: Die *rekursiven* Aufrufe der Fibonacci Funktion werden nicht memoisiert. Der Programmcode macht das deutlich: Die Definition von *memo-fibonacci* ist nicht rekursiv — *memo-fibonacci* ist durch eine Wertebindung gegeben — der zweite Parameter von *memo* ist die rekursive Funktion. Die rekursiven Aufrufe namens *fibonacci* beziehen sich auf diese Funktion, nicht auf die memoisierte Version namens *memo-fibonacci*.

Was ist zu tun? Wertedefinition dürfen nicht rekursiv sein; die Wertedefinition in eine Funktionsdefinition zu überführen, ist verführerisch, aber nicht sinnvoll. Dann wird für jeden rekursiven Aufruf eine *neue* Memotabelle angelegt. (Nachdenken!) Wir können die rekursiven Aufrufe memoisieren, indem wir *memo* nicht eine Funktion des Typs $Nat \to 'a$ übergeben, sondern eine Funktion des Typs $(Nat \to 'a) \to (Nat \to 'a)$, die über die rekursiven Aufrufe abstrahiert.

```
let rec-memo (dom : Nat,
              functional : (Nat → 'value) → (Nat → 'value)) : Nat → 'value =
  let memo-table = [| for i in 0 .. dom − 1 → ref None |]
  let rec memo-f (n : Nat) : 'value =
    match !memo-table.[n] with
    | None   → let v = functional memo-f n
               memo-table.[n] := Some v
               v
    | Some v → v
  in memo-f
let memo-fibonacci =
  rec-memo (100, fun fib → fun n →
                   if n ⩽ 1 then n
                            else fib (n − 1) + fib (n − 2))
```

Aus der rekursiven Funktion, zweites Argument von *memo*, ist eine nicht-rekursive Funktion geworden, zweites Argument von *rec-memo*, die die rekursiven Aufrufe zum Parameter macht. Dieser Parameter wird in der Definition von *rec-memo* mit der memoisierten Funktion belegt: *functional memo-f*. (Betrachten wir die Definition durch die semantische Brille, so bestimmt *rec-memo* den Fixpunkt des zweiten Arguments bei gleichzeitiger Memoisierung, siehe auch Abschnitt 6.5.2.) Der Lohn der Anstrengungen: Sowohl die Deklaration von *memo-fibonacci* als auch alle Aufrufe von *memo-fibonacci* sind in Windeseile ausgerechnet; auch die rekursiven Aufrufe füllen die Tabelle.

7.2.5. Über den Tellerrand

L- und R-Werte Zum Abschluss wollen wir noch einen Blick über den Tellerrand und auf andere Programmiersprachen werfen. In den historisch ersten Programmiersprachen und auch in den meisten aktuellen Sprachen spielen Speicherzellen eine weitaus größere Rolle als in Mini–F#. Es wird gerechnet, indem die Inhalte von Speicherzellen schrittweise verändert werden. Schauen wir uns die Unterschiede anhand zweier konkreter Beispiele an: der Programmiersprache ***Pascal*** und der Programmiersprache ***C***. Ein Bezeichner in diesen Sprachen oder in gängiger Terminologie eine ***Variable*** bezeichnet stets eine Speicherzelle. In Pascal führt die Deklaration `var i:integer` eine Speicherzelle ein, die eine ganze Zahl enthält; die C Deklaration `int i` unterscheidet sich syntaktisch etwas, bedeutet aber das Gleiche. Die korrespondierende Mini–F# Deklaration lautet ***let*** *i* = ***ref*** 0. Dereferenzierung ist in Pascal und C implizit: Statt wie in Mini–F# $i := !i + 4711$ programmiert man in Pascal `i := i + 4711` und in C `i = i + 4711` oder etwas kürzer `i += 4711`. Auf der rechten Seite der Zuweisung werden Speicherzellen automatisch dereferenziert — manchmal spricht man auch vom ***L-Wert*** und ***R-Wert*** einer Variablen; *l*inks ist die Adresse gemeint und *r*echts der Inhalt der Speicherzelle.

Automatische Dereferenzierung erscheint auf den ersten Blick bequem, hat aber wie alle Automatismen seine Nachteile: Was passiert, wenn auf der rechten Seite tatsächlich die Adresse gemeint ist und nicht der Inhalt? Schauen wir uns ein Beispiel an. Die folgende Version der Fakultät kommuniziert das Funktionsergebnis nicht über den Rückgabewert, sondern über das Argument! Das hört sich paradox an; werfen wir also einen Blick auf die Definition (in Mini–F#), um das Rätsel zu lösen.

module Effects.CallbyRef

```
let rec factorial (n : Nat, result : Ref ⟨Nat⟩) =
  if n = 0 then
    result := 1
  else
    factorial (n – 1, result)
    result := !result * n
```

Das zweite Argument ist vom Typ *Ref* ⟨*Nat*⟩. Der Funktion wird die Adresse übergeben, unter der sie das Ergebnis ablegen soll — ähnlich einem Postfach. Diese Technik (engl. destination passing style) wird in Pascal und C oft verwendet, um Funktionen mit mehreren Rückgabewerten zu simulieren — Funktionen dürfen in diesen Sprachen keine aggregierten Daten wie etwa ein Paar zurückgeben. Um diese Version der Fakultät zu verwenden, muss man ein Postfach anlegen und später dort nachschauen:

```
⋙ let post-office-box = ref 10
val post-office-box : Ref ⟨Nat⟩
⋙ factorial ( !post-office-box, post-office-box)
()
⋙ !post-office-box
3628800
```

Der zweite Ausdruck verwendet sowohl den L-Wert einer Variablen (*post-office-box*) als auch deren R-Wert (!*post-office-box*) einer Variablen. Sprachen, die automatisch dereferenzieren, sehen sich an dieser Stelle mit einem Problem konfrontiert. In Pascal wird das Problem gelöst, indem bei der Definition der Funktion der zweite Parameter besonders gekennzeichnet wird: `procedure factorial (n : integer, var result : integer)`. Man spricht von einem ***Variablen-*** oder ***Referenzparameter*** (engl. ***call by reference***). Die Deklaration bewirkt, dass der korrespondierende Aufruf in Pascal, `factorial (pob, pob)`, korrekt behandelt wird: Das erste Vorkommen von `pob` (kurz für post office box) wird dereferenziert, das zweite nicht.

In C wird ein Operator bereitgestellt, der sogenannte Adressoperator `&`, um die automatische Dereferenzierung zurückzunehmen: `factorial (pob, &pob)`. In der Deklaration der Funktion muss zusätzlich vermerkt werden, dass der zweite Parameter eine Adresse ist:
`int factorial (int n, int* result)`.

Fassen wir zusammen: Etwas vereinfachend kann man sagen, dass in Pascal L- und R-Werte syntaktisch durch die Grammatik unterschieden werden, in C hingegen ähnlich wie in Mini–F# anhand des Typs. Eine syntaktische Unterscheidung ist notgedrungen restriktiver als eine typmäßige Unterscheidung — Typregeln sind ausdrucksstärker als Grammatiken. Der konservative Ansatz in Pascal hat aber seinen Grund, der mit der ***Lebensdauer*** (engl. extent) von Variablen zusammenhängt. Speicherzellen in Mini–F# leben prinzipiell ewig (der Speicher σ wird stets größer, nie kleiner); in Pascal und C endet die Lebensdauer in der Regel mit dem Ende der Sichtbarkeit: Ist eine Variable nicht mehr sichtbar, wird sie deallokiert. Dahinter steht die Vorstellung oder vielmehr die Hoffnung, dass eine Speicherzelle nicht mehr benötigt wird, wenn ihre Adresse nicht mehr sichtbar ist. In Mini–F# gilt dies sicherlich nicht: In der Implementierung des Bankkontos ist die Speicherzelle *funds* nach Abarbeitung der Moduldefinition nicht mehr sichtbar, benötigt wird sie aber sehr wohl.

Die Adresse überlebt das Ende der Sichtbarkeit durch ihre Verwendung in den Funktionen *deposit*, *withdraw* und *balance*. Es lohnt sich, diesen Punkt mit Hilfe eines vereinfachten Beispiels noch einmal genauer zu beleuchten.

```
let inc =
  let counter = ref 0
  fun () : Nat →
    counter := !counter + 1
    !counter
```

Die lokale Definition wertet zu der Umgebung $\{counter \mapsto a\}$ aus, wobei a die Adresse der angelegten Speicherzelle ist. Bezüglich dieser Umgebung wird der Funktionsausdruck ausgewertet; das Ergebnis ist ein Funktionsabschluss. Die globale Definition wertet somit zu der Umgebung $\{inc \mapsto \langle\{counter \mapsto a\}, (), counter := !counter + 1; !counter\rangle\}$ aus. So entweicht die Adresse a aus ihrem Sichtbarkeitsbereich: a ist nicht mehr direkt via *counter* verfügbar, aber indirekt via *inc*.

Die Einschränkungen von Pascal garantieren, dass eine solche Situation nicht auftreten kann — das geht allerdings mit einem Verlust an Ausdruckskraft einher. In C ist die Situation verzwickter: Das obige Beispiel lässt sich wegen ähnlicher Einschränkungen nicht nachprogrammieren; eine Adresse kann also nicht auf diesem Wege entweichen. Aber C hat den Adressoperator im Repertoire: Dieser erlaubt es, die Adresse einer Variablen zu bestimmen. Merkt man sich diese Adresse, so kann es passieren, dass man später auf eine Speicherzelle zugreift, die längst nicht mehr existiert — mit unabsehbaren Folgen. (Die ungültige Adresse nennt man auch ***dangling pointer***.)

Die obige Diskussion wirft mindestens zwei weitere Fragen auf: Warum werden in Pascal und C Variablen am Ende ihrer Sichtbarkeit deallokiert. Wann und wie werden in Mini–F# Speicherzellen deallokiert? Die zweite Frage ist schnell beantwortet: In Mini–F# werden Speicherzellen deallokiert, wenn sie tatsächlich nicht mehr benötigt werden und wenn der Speicherplatz knapp wird. Diese Aufgabe übernimmt ein sogenannter ***Garbage collector*** (engl. für Müllmann), ein wichtiger Bestandteil des Mini–F# Interpreters. Ob ein Speicherplatz nicht mehr benötigt wird, ist eine globale Eigenschaft. Aus diesem Grund sollte sich jemand um die Müllentsorgung kümmern, der den Überblick hat — und das ist nicht notwendigerweise die Programmiererin oder der Programmierer. Pascal und C verfügen über keinen Garbage collector. Sie verwenden daher eine einfachere, aber durchaus bewährte Form der Speicherorganisation: Variablen am Anfang der Sichtbarkeit allokieren, am Ende deallokieren (Stichwort: stackartige Speicherorganisation).

Listen, da capo Da in Pascal und C das Konzept des Speichers dominierend ist, gehen diese Sprachen auch die Implementierung von Datenstrukturen wie Listen oder Bäumen anders an. Um die Unterschiede zu diskutieren, programmieren wir eine typische Listenimplementierung in Mini–F# nach. Der grundlegende Unterschied zu der Definition von Listen aus Abschnitt 4.2.2 ist, dass eine Liste selbst sowie sämtliche Restlisten Speicherzellen sind.

```
type List ⟨'elem⟩  = Ref ⟨Item ⟨'elem⟩⟩
and  Item ⟨'elem⟩ =
        | Nil
        | Cons of 'elem * List ⟨'elem⟩
```

Die Typen *List* und *Item* sind verschränkt rekursiv definiert: *List* verwendet *Item* und *Item* verwendet *List*. Analog zu verschränkt rekursiven Funktionen müssen auch verschränkt rekursive Typen mit ***and*** verknüpft werden. Entfernen wir den Typkonstruktor *Ref*, so erhalten wir unsere ursprüngliche Definition von Listen. Ein »Item« ist entweder leer oder besteht aus einem Listenelement und der Adresse des nächsten Items.

Wenn wir »clevere« Konstruktoren definieren,

```
let nil () = ref Nil
let cons (x, xs) = ref (Cons (x, xs))
```

dann ändert sich die Konstruktion von Listen im Vergleich zur Listendefinition aus Abschnitt 4.2.2 nur marginal. (Abbildung 7.2 erklärt, warum *nil* eine Funktion sein muss.)

```
>>>  let primes = cons (2, cons (3, cons (5, nil ())))
val primes : Ref ⟨Item ⟨Nat⟩⟩
>>>  primes
{contents = Cons (2, {contents = Cons (3, {contents = Cons (5,
    {contents = Nil})})})}
```

Lediglich die Ausgabe zeigt an, dass Speicherzellen involviert sind.[4]

Auch die Definition von »beobachtenden« Funktionen wie der Listenlänge ändert sich nur unwesentlich. Vor jeder Fallunterscheidung muss zunächst die Adresse dereferenziert werden:

```
let length (list : List ⟨'elem⟩) =
  let rec worker n p =
    match !p with
      | Nil          → n
      | Cons (x, xs) → worker (n + 1) xs
  in worker 0 list
```

(Aus Gründen der Effizienz verwendet *length* eine »endrekursive« Arbeiterfunktion mit einem akkumulierenden Parameter; die gleiche Optimierung ist auch auf unsere Listen aus Abschnitt 4.2.2 anwendbar und tatsächlich sinnvoll. Wir wenden uns diesem Thema ausführlich in Abschnitt 7.3.3 zu.)

Anders verhält es sich mit »transformierenden« Funktionen: Listen werden manipuliert, indem die Inhalte der adressierten Speicherzellen verändert werden. Die Definition der Listenkonkatenation illustriert die Vorgehensweise.

[4] Die Ausgabe verrät, wie der Mini–F# Interpreter Speicherzellen implementiert: als Records mit genau einer Komponente, dem Inhalt (engl. contents) der Speicherzelle, siehe Seite 398.

Speicherzellen und Polymorphie stehen in einem gewissen Spannungsverhältnis. So ist es *nicht* erlaubt, eine polymorphe Speicherzelle zu definieren.

```
let nil = ref Nil          // nicht zulässig (value restriction), nil : List ⟨'elem⟩
```

Wäre die Definition zulässig, hätte *nil* den Typ *List* ⟨*'elem*⟩ und wir könnten mit ihrer Hilfe Listen verschiedensten Typs konstruieren.

```
let bools = ref (Cons (false, ref (Cons (true, nil))))
let nats  = ref (Cons (4711, ref (Cons (815, nil))))
```

Vielleicht sieht man schon das Unheil nahen. Da *nil* eine veränderbare Speicherzelle ist, können wir ihren Inhalt modifizieren. Da *nil* einen polymorphen Typ vorgibt, können wir mit dem Inhalt auch den Typ abändern.

```
nil := Cons ("oh je", ref Nil)
```

Aus der leeren Liste ist eine einelementige Liste geworden, als Nebeneffekt sind sowohl *bools* als auch *nats* um ebendieses Element verlängert worden. Die Listen sind nicht länger homogen! Aus diesem Grund ist die Definition polymorpher Werte verboten; versucht man es trotzdem, meldet die Typprüfung eine Verletzung der ***Wertebeschränkung*** (engl. ***value restriction***). Keine Regel ohne Ausnahme: polymorphe Funktionen und polymorphe Datenkonstruktoren sind erlaubt.

```
let nil () = ref Nil       // zulässig, nil : Unit → Ref ⟨Item ⟨'elem⟩⟩
let nil = Nil              // zulässig, nil : Item ⟨'elem⟩
```

Abbildung 7.2.: Wertebeschränkung (engl. value restriction).

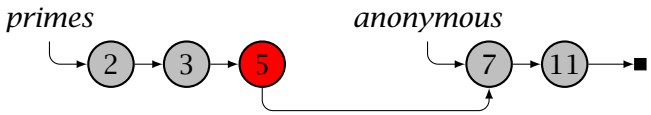
```
let rec append (list1 : List ⟨'elem⟩, list2 : List ⟨'elem⟩) : Unit =
  match !list1 with
    | Nil          → list1 := !list2
    | Cons (x, xs) → append (xs, list2)
```

Ist die erste Liste leer, so wird ihr der Inhalt der zweiten Liste zugewiesen. Anderenfalls wird die zweite Liste an die Restliste angehängt. Vergleichen wir diese Definition mit der Definition aus Abschnitt 4.2.2, so ist auffällig, dass *append* keine neue Liste konstruiert; *append* arbeitet »in situ« (lat. am Platz) mit den bestehenden Strukturen.

Probieren wir *append* aus:

```
⋙ append (primes, cons (7, cons (11, nil ())))
()
⋙ primes
{contents = Cons (2, {contents = Cons (3, {contents = Cons (5,
    {contents = Cons (7, {contents = Cons (11, {contents = Nil})})})})})}
```

Wir sehen: *append* hängt das zweite Argument an das erste an und modifiziert dieses dabei. Die ursprüngliche Liste hat sich nach diesem Aufruf verflüchtigt. Aus diesem Grund spricht man auch von einer ***ephemeren Datenstruktur*** (griech. nur einen Tag dauernd, vorübergehend). Die folgende Grafik visualisiert das resultierende Speichergeflecht (der rote Knoten ist überschrieben worden).



Vergleichen wir das Verhalten mit der Listenimplementierung aus Abschnitt 4.2.2:

```
⋙ let primes = Cons (2, Cons (3, Cons (5, Nil)))
val primes : List ⟨Nat⟩
⋙ primes
Cons (2, Cons (3, Cons (5, Nil)))
⋙ append (primes, Cons (7, Cons (11, Nil)))
Cons (2, Cons (3, Cons (5, Cons (7, Cons (11, Nil)))))
⋙ primes
Cons (2, Cons (3, Cons (5, Nil)))
⋙ append (primes, primes)
Cons (2, Cons (3, Cons (5, Cons (2, Cons (3, Cons (5, Nil))))))
```

Diese Version ist nicht destruktiv: *append* (*list1*, *list2*) konkateniert die Listen *list1* und *list2*; die Argumentlisten sind nach dem Aufruf unverändert, sie überdauern den Aufruf (klar, das Konzept des Speichers haben wir ja erst in diesem Abschnitt eingeführt). Aus diesem Grund spricht man auch von einer ***persistenten Datenstruktur*** (lat. anhaltend, beharrlich).[5] Persistente Datenstrukturen sind in der Regel ephemeren Datenstrukturen vorzuziehen. Da sie, zumindest nach außen, effektfrei sind, sind sie leichter zu verstehen, zu verwenden und darüber hinaus auch flexibler.

Die Gefahr von Effekten illustriert die folgende interaktive Sitzung.

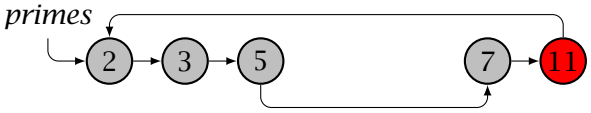
[5] Diese Verwendung des Begriffes Persistenz sollte nicht mit der für Daten auf einem Hintergrundspeicher verwechselt werden, siehe vorheriger Abschnitt. Hier ist gemeint, dass die für die Datenstruktur bereitgestellten Funktionen ihre Argumente nicht verändern.

```
⋙ append (primes, primes)
()
⋙ primes
{contents = Cons (2, {contents = Cons (3, {contents = Cons (5, {contents =
    Cons (7, {contents = Cons (11, {contents = ...})})})})})})}
```

Wir hängen die Liste der ersten fünf Primzahlen an die Liste der ersten fünf Primzahlen und erhalten — ja, was eigentlich? Um die Ausgabe überschaubar zu halten, gibt der Interpreter nur die ersten Elemente aus. Dass die Liste tatsächlich länger ist, wird durch die Ellipse »…« angedeutet. Aber wie lang?

```
⋙ length primes
…
```

Dem Aufruf von *length primes* folgt Stille, die Auswertung terminiert nicht! Der Funktionsaufruf *append* (*primes*, *primes*) hat nicht etwa eine 10-elementige Liste konstruiert, sondern eine ***zyklische Liste***: Das ursprüngliche Ende der Liste verweist nunmehr auf den Anfang der Liste selbst.



Das Beispiel zeigt, dass nicht alle Effekte erwartet oder gar erwünscht sind. Und noch etwas wird deutlich: Das Struktur Entwurfsmuster garantiert nicht länger, dass die nach dem Muster gestrickten Funktionen auch terminieren! Wir können — gewollt oder ungewollt — zyklische Speichergeflechte konstruieren, so dass die listenverarbeitenden Funktionen keinem Basisfall mehr zustreben.

```
⋙ let nihil : List ⟨Nat⟩ = nil ()
val nihil : Ref ⟨Item ⟨Nat⟩⟩
⋙ let cycle = cons (0, nihil)
val cycle : Ref ⟨Item ⟨Nat⟩⟩
⋙ nihil := !cycle
()
⋙ append (cycle, cons (1, nil ()))
…
```

Natürlich kann man solche Speichergeflechte in einem Programm auch bewusst einsetzen. In diesem Fall muss man die Terminierung mit anderen Mitteln gewährleisten, etwa indem man sich merkt, welche Speicherzellen schon verarbeitet wurden. Auf zyklische Geflechte kommen wir am Ende des Abschnitts noch einmal zu sprechen.

Speicherzellen verändern also die Natur des Rechnens — es gibt nicht länger eine Terminierungsgarantie für strukturell rekursive Funktionen. Aber es kommt noch schlimmer: Selbst die Terminierung von nicht-rekursiven Funktionen ist nicht mehr gewährleistet! Die folgenden beiden Wertebindungen implementieren die Fakultät — ersetzen wir die gesamte Alternative durch den ***else***-Zweig, so erhalten wir eine nicht-terminierende Funktion!

```
let fac = ref (fun (n : Nat) → 0)
let factorial =
  fac := (fun (n : Nat) → if n = 0 then 1
                          else n * (!fac) (n − 1))
  !fac
```

Die erste Wertebindung allokiert eine Speicherzelle, die eine Funktion enthält: *fac* hat den Typ *Ref* ⟨*Nat* → *Nat*⟩. Die zweite Wertebindung weist dieser Speicherzelle eine Funktion zu, die die in dieser Speicherzelle enthaltene Funktion aufruft, also dank der Zuweisung sich selbst: ein zyklisches Speichergeflecht, das Rekursion simuliert. Damit sollen nicht etwa »funktionale« Speicherzellen diffamiert werden — ähnlich wie Funktionen höherer Ordnung sind auch Speicherzellen, die Funktionen enthalten, nützlich (Stichwort: hooks).

Veränderliche\Variablen Neben Speicherzellen bietet F# noch ein weiteres Konstrukt an, um Programme mit einem Gedächtnis auszustatten: ***Veränderliche*** bzw. ***Variablen***.

```
let mutable funds = 0
```

Mit ***mutable*** wird ein Bezeichner als veränderlich gekennzeichnet: Aus einem Namen für einen Wert wird eine Speicherzelle. Zuweisungen an ***mutable***s werden wie folgt notiert.

```
funds ← funds + amount
```

Lies: funds wird zu *funds*+*amount* (engl. *funds* becomes *funds*+*amount*). Wie in C oder Pascal wird ein veränderlicher Bezeichner automatisch dereferenziert. Der Bezeichner *funds* hat tatsächlich den Typ *Nat* und kann wie gewohnt in jedem Kontext verwendet werden, in dem eine natürliche Zahl erwartet wird. Zusätzlich darf *funds* auf der linken Seite einer Zuweisung der Form $e_1 \leftarrow e_2$ stehen. Die Vor- und Nachteile der automatischen Dereferenzierung haben wir bereits am Anfang des Abschnitts diskutiert; sie gelten in gleicher Weise für ***mutable***s.

Was wir bisher verschwiegen haben: Auch Arrays sind veränderlich; die Elemente eines Arrays können mittels einer Zuweisung der Form $a.[e_1] \leftarrow e_2$ verändert werden. (Ein Array ist sozusagen eine große Speicherzelle mit nummerierten Fächern.) Mit diesem Wissen lässt sich die Implementierung der Memotabellen aus Abschnitt 7.2.4 verbessern: Der furchteinflößende Typ *Array* ⟨*Ref* ⟨*Option* ⟨'*a*⟩⟩⟩ kann zu *Array* ⟨*Option* ⟨'*a*⟩⟩ vereinfacht werden.

```
let memo (dom : Nat, func : Nat → 'value) : Nat → 'value =
  let
    memo-table = [| for i in 0 .. dom − 1 → None |]
  in
    fun (n : Nat) → match memo-table.[n] with
                    | None   → let v = func n
                               memo-table.[n] ← Some v
                               v
                    | Some v → v
```

Der Code ist fast identisch: Die Allokation von Speicherzellen mit ***ref*** entfällt, ebenso wie die Dereferenzierung mit »!«; die Zuweisung $e_1 := e_2$ wird in $e_1 \leftarrow e_2$ abgeändert.

Nicht nur Bezeichner können als veränderlich gekennzeichnet werden, auch Komponenten von Records. Wie bereits angedeutet, sind Speicherzellen tatsächlich Records mit einer veränderlichen Komponente, dem Inhalt (engl. contents) der Speicherzelle. Der Typ *Ref* ⟨'*value*⟩ und die Operationen auf Speicherzellen sind wie folgt definiert.

module Effects.Cell

```
type Ref ⟨'value⟩ =
  {mutable contents : 'value}
let ref value =
  {contents = value}
let (!) cell =
  cell.contents
let (:=) cell value =
  cell.contents ← value
```

Um symbolische Bezeichner wie »!« oder »:=« zu definieren, müssen diese in Klammern eingeschlossen werden. Der Unterschied zwischen einer Speicherzelle, sprich einer Adresse, und ihrem Inhalt wird hier noch einmal sehr deutlich: *cell* ist jeweils die Speicherzelle und *cell.contents* ihr Inhalt. (Harry Hacker würde übrigens die Zuweisung so modifizieren, dass der R-Wert zusätzlich als Ergebnis zurückgegeben wird.

```
let (:=) cell value =
  cell.contents ← value
  value
```

Damit lassen sich Zuweisungen aneinanderreihen, $x := y := 4711$, oder mit anderen Operationen kombinieren $(x := !x + 1) \leqslant 99$. Wenn Sie bereits das Vergnügen hatten in C zu programmieren, wird Ihnen dieses Idiom bekannt vorkommen.)

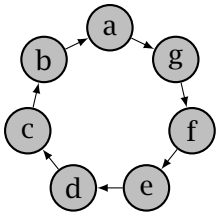
module Effects.Necklace

Perlenketten\Zyklische Listen

> *The following anecdote is told of William James. […] After a lecture on cosmology and the structure of the solar system, James was accosted by a little old lady.*
>
> *«Your theory that the sun is the centre of the solar system, and the earth is a ball which rotates around it has a very convincing ring to it, Mr. James, but it's wrong. I've got a better theory,« said the little old lady.*
>
> *»And what is that, madam?« inquired James politely.*
>
> *«That we live on a crust of earth which is on the back of a giant turtle.«*
>
> *Not wishing to demolish this absurd little theory by bringing to bear the masses of scientific evidence he had at his command, James decided to gently dissuade his opponent by making her see some of the inadequacies of her position.*
>
> *»If your theory is correct, madam," he asked, "what does this turtle stand on?«*
>
> *«You're a very clever man, Mr. James, and that's a very good question,« replied the little old lady, »but I have an answer to it. And it's this: The first turtle stands on the back of a second, far larger, turtle, who stands directly under him.«*
>
> *»But what does this second turtle stand on?« persisted James patiently.*
>
> *To this, the little old lady crowed triumphantly,*
>
> *»It's no use, Mr. James — it's turtles all the way down.«*
>
> — J. R. Ross, *Constraints on Variables in Syntax*

Besteht ein Record aus mehreren Komponenten, kann man selektiv für jede Komponente entscheiden, ob sie veränderlich sein soll oder eben nicht. Zum Beispiel:

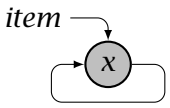
```
type Necklace ⟨'elem⟩ =
  {bead           : 'elem
   mutable next : Necklace ⟨'elem⟩}
```



Elemente dieses Typs sind ***Perlenketten*** (engl. necklaces) oder, etwas prosaischer, nicht-leere zyklisch verkettete Listen, siehe Abbildung zur Rechten. Die nicht veränderliche Komponente enthält eine Perle (engl. bead), ein Listenelement; die veränderliche Komponente verweist auf das nächste Kettenglied (engl. next). Der Typ ist bemerkenswert, da er zum Ersten rekursiv definiert ist, aber zum Zweiten keinen Basisfall anbietet. Eine Kette besteht aus einer Perle und einer Kette, die wiederum aus einer Perle besteht und einer Kette, die … — it's turtles all the way down. Der einzige Ausweg aus der Zwickmühle: Eine Kette muss notwendigerweise ein zyklisches, wenn auch nicht unbedingt ein zirkuläres Geflecht sein. (Über diese Geflechte sind wir schon gestolpert, als wir uns mit ephemeralen Listen beschäftigt haben. Hier setzen wir sie bewusst ein — a bug turned into a feature.)

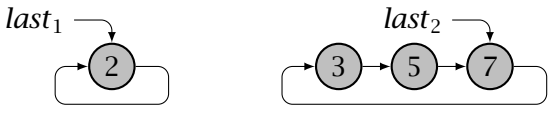
Wie konstruieren wir ein zyklisches Geflecht? Die Antwort ist so zwingend, wie vielleicht überraschend: durch eine rekursive *Werte*definition.

```
let single x =
  let rec item =
    {bead = x
     next = item}
  in item
```



Bis dato haben wir nur rekursive *Funktions*definitionen kennengelernt (es sei denn, Sie haben Abschnitt 4.5.5 gelesen). Aus gutem Grund. Rekursive Wertedefinition ergeben im Allgemeinen keinen Sinn: ***let rec*** $n = n + 1$ ist zum Beispiel nicht zulässig, da der Bezeichner n als Teil seiner eigenen Definition ausgewertet würde. (Auch als mathematische Gleichung hat $n = n + 1$ keine Lösung.) Funktionsdefinitionen sind hingegen unproblematisch, da sie unmittelbar zu Funktionsabschlüssen auswerten, im Fall einer rekursiven Definition zu einem zyklischen Geflecht, siehe Abschnitt 3.6. Die obige rekursive Wertedefinition ist ebenfalls unproblematisch, wenn auch ihre Auswertung etwas trickreich vonstatten geht. Hinter den Kulissen wird item in zwei Schritten konstruiert: Zunächst wird ***let*** *item* = {*bead* = *x*; *next* = ⊥} angelegt, wobei ⊥ ein Dummywert ist; dann wird mittels *item*.*next* ← *item* der Dummywert durch den zyklischen Verweis ersetzt. Wiederum wird aus einer rekursiven Definition ein zyklisches Geflecht.

Wir können Perlenketten verwenden, um nicht-leere, *endliche* Folgen von Elementen darzustellen — wir erhalten eine weitere Variation von ephemeralen Listen. Die grundlegende Idee ist, eine Folge von Elementen durch eine Kette mit entsprechenden Perlen zu repräsentieren und dabei auf das *letzte* Element der zu repräsentierenden Folge zu verweisen. Die einelementige Folge 2 und die dreielementige Folge 3 5 7 werden zum Beispiel durch



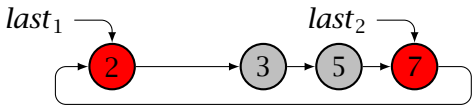
repräsentiert. (Wenn man möchte, kann man $last_1$ bzw. $last_2$ als Verschluss der jeweiligen Perlenkette ansehen.) Die Darstellung macht es *sehr* einfach, Folgen zu rotieren: $last_2$.*next* repräsentiert 5 7 3, $last_2$.*next*.*next* repräsentiert 7 3 5 und $last_2$.*next*.*next*.*next* ergibt die ursprüngliche Folge — der Ausdruck ist identisch zu $last_2$.

Das Kopfelement der Folge *last* ist *last*.*next*.*bead*; die Restfolge erhalten wird, indem wir das erste Element überspringen: *last*.*next* ← *last*.*next*.*next*.

```
let head (last : Necklace ⟨'elem⟩) : 'elem =
  last.next.bead
let tail (last : Necklace ⟨'elem⟩) : Necklace ⟨'elem⟩ =
  last.next ← last.next.next
  last
```

Perlenketten sind ephemeral: Die Funktion *tail* verändert ihr Argument, das lediglich aus Gründen der Bequemlichkeit zusätzlich als Funktionsergebnis zurückgegeben wird (so dass wir zum Beispiel *tail* (*tail xs*) schreiben können).

Wir haben noch nicht verraten, warum wir ausgerechnet auf das letzte und nicht etwa auf das erste Element verweisen. Diese Darstellung erlaubt es, zwei Folgen in *konstanter* Zeit zu konkatenieren. Wir müssen lediglich $last_1.next$ und $last_2.next$ vertauschen (die roten Knoten sind überschrieben worden).



Die Funktion *append* implementiert die Vertauschung; das Ergebnis der Konkatenation ist die zweite Folge. (Nachdenken!)

```
let append (last₁ : Necklace ⟨'elem⟩, last₂ : Necklace ⟨'elem⟩) : Necklace ⟨'elem⟩ =
  // swap last₁.next and last₂.next
  let tmp = last₁.next
  last₁.next ← last₂.next
  last₂.next ← tmp
  last₂
let cons (x, xs) = append (single x, xs)
```

Auch *append* verändert ihre Argumente: repräsentiert $last_i$ die Folge xs_i, dann repräsentiert $last_2$ *nach* dem Aufruf von *append* die Folge xs_1 @ xs_2, während $last_1$ die Folge xs_2 @ xs_1 darstellt — eine perfekte Symmetrie. Tatsächlich implementiert *append* so etwas wie die »symmetrische Konkatenation« zweier Folgen. Hier sind die verschiedenen Operationen in Aktion:

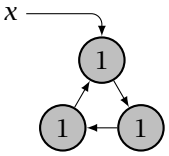
```
⋙ let mutable primes = single 2
⋙ primes
{bead = 2; next = ...}
⋙ primes ← append (primes, cons (3, cons (5, single 7)))
⋙ primes
{bead = 7; next = {bead = 2; next = {bead = 3; next = {bead = 5; next = ...}}}}
⋙ tail primes
{bead = 7; next = {bead = 3; next = {bead = 5; next = ...}}}
⋙ tail primes
{bead = 7; next = {bead = 5; next = ...}}
⋙ tail primes
{bead = 7; next = ...}
⋙ tail primes
{bead = 7; next = ...}
```

Man sieht jeweils sehr schön, dass auf das letzte Element der Folge verwiesen wird. Die letzten Aufrufe zeigen, dass sich eine einelementige Folge nicht weiter verkleinern lässt: *tail* (*single x*) ist und bleibt *single x*.

Übungen.

1. In Abschnitt 7.2.5 haben wir Sequenzen, endliche Folgen von Elementen, mit Hilfe von Perlenketten implementiert. Definieren Sie eine Funktion, die die Länge einer Perlenkette bestimmt. Die unten abgebildete Perlenkette x hat zum Beispiel die Länge 3. Für die Lösung dieser Aufgabe benötigen Sie noch zusätzliches Hintergrundwissen. Perlenketten werden tatsächlich durch die folgende Typdefinition eingeführt.

```
[<ReferenceEquality>]
type Necklace⟨'elem⟩ =
  {bead          : 'elem
   mutable next : Necklace⟨'elem⟩}
```



Das sogenannte ***Attribut*** (engl. attribute) [<*ReferenceEquality*>] instruiert den F# Übersetzer den Test auf Gleichheit nicht durch ***Wertegleichheit*** (engl. ***value equality***), sondern durch ***Verweisgleichheit*** (engl. ***reference equality***) zu implementieren. Die folgende Interaktion illustriert die Unterschiede.

```
⋙ let x = single 4711
⋙ let y = single 4711
⋙ x = y
false
⋙ x = x
true
```

Die Bezeichner x und y haben zwar den gleichen Wert, sie sind aber nicht identisch — im Hauptspeicher werden sie unter zwei unterschiedlichen Adressen geführt. In der obigen Grafik sind alle drei Perlen wertegleich, aber nicht verweisgleich, nicht identisch. Verweisgleichheit ist die diskriminierenste Gleichheit: Sind zwei Ausdrücke verweisgleich, dann sind sie auch wertegleich; die Umkehrung gilt nicht, wie die Interaktion demonstriert. Um die Länge einer Perlenkette zu bestimmen, muss die Möglichkeit bestehen, Perlen auf Identität zu testen. (Nachdenken!) Entfernen wir übrigens das Attribut [<*ReferenceEquality*>], dann folgt dem Aufruf $x = y$ eine lange Stille, die Auswertung terminiert nicht. (Warum?)

7.3. Kontrollstrukturen

Mit der Einführung von Operationen zur Ein- und Ausgabe und zur Speichermanipulation wird es notwendig, Effekte präzise zu kontrollieren: Welche Effekte treten auf, in welcher Reihenfolge treten sie auf und wie oft werden sie gegebenenfalls wiederholt. Mit dem Einzug von Effekten verändert sich nicht nur die Natur des Rechnens, auch der Programmierstil wird potentiell ein anderer. Der *problemnahe*, *deskriptive* Charakter — Was soll berechnet werden? — weicht einem *maschinennahen*, *präskriptiven* Stil — Wie genau wird die Rechnung durchgeführt? Das »Wie«, der Kontrollfluss, kann mit speziellen Sprachmitteln, den Kontrollstrukturen, präzisiert werden und ist wesentlicher Inhalt dieses Abschnitts. Im Einzelnen haben wir Folgendes vor:

In Abschnitt 7.3.1 führen wir Sprachmittel ein, um auf einfache Art und Weise Listen und Arrays zu bilden. Ironischerweise sind die Konstrukte deskriptiver Natur — sie *beschreiben* Listen und Arrays, anstatt *vorzuschreiben*, wie diese im Detail zu konstruieren sind. Abschnitt 7.3.1 bereitet den Boden für Abschnitt 7.3.2, in dem Kontrollstrukturen, inbesondere Konstrukte zur ***Iteration***, diskutiert werden: ***for***- und ***while***-Schleifen. Abschnitt 7.3.3 beleuchtet das Verhältnis zwischen Rekursion und Iteration. Daran anknüpfend zeigt Abschnitt 7.3.4, wie der Kontrollfluss mit den bisherigen Bordmitteln gesteuert werden kann.

7.3.1. Listen- und Arraybeschreibungen

In Abschnitt 4.4 haben wir zwei Möglichkeiten kennengelernt, Arrays zu konstruieren: explizit durch Aufzählung der Elemente bzw. implizit durch Angabe einer Bildungsvorschrift. So konstruiert $[\![2;3;5;7;11]\!]$ das Array der ersten fünf Primzahlen und $[\![\textbf{for } i \textbf{ in } 0..99 \to i*i]\!]$ das Array der

ersten hundert Quadratzahlen. Beide linguistischen Konstrukte sind auch für Listen verfügbar: [2;3;5;7;11] ist entsprechend die Liste der ersten fünf Primzahlen und [*for* i *in* $0..99 \to i*i$] die Liste der ersten hundert Quadratzahlen. Die Konstruktion mittels Angabe einer Bildungsvorschrift ist tatsächlich sehr viel allgemeiner als bisher vorgestellt: Generatoren dürfen aneinandergereiht und geschachtelt werden; zusätzlich können Filter oder Alternativen eingebaut werden. Die folgenden Beispiele illustrieren einige der Möglichkeiten:

```
⋙ [yield 4711; for i in 0..5 do yield i*i]
[4711;0;1;4;9;16;25]
⋙ [for i in 0..9 do if i%2 = 1 then yield i*i]
[1;9;25;49;81]
```

Zunächst einmal ist [*for* i *in* $e_1 \to e_2$] eine Abkürzung für [*for* i *in* e_1 *do yield* e_2]. Der Ausdruck *yield* e erzeugt bzw. generiert ein einzelnes Listenelement. Die Listenbeschreibung [*yield* 4711; *for* i *in* $0..5$ *do yield* $i*i$] generiert somit zunächst 4711 und dann für alle Elemente i im Intervall $(0,5)$ den Wert $i*i$. Mit einer einarmigen Alternative können Elemente herausgefiltert werden: *if* $i\%2 = 1$ lässt nur ungerade Werte für i zu.

Wenn die Beschreibungen komplizierter werden, deutet man die hierarchische Struktur am besten durch Einrückung an. Das folgende Beispiel generiert die Positionen aller schwarzen Felder auf einem 8×8-Schachbrett.

```
⋙ [for i in 1..8 do
     for j in 1..8 do
       if (i+j)%2 = 0 then
         yield (i,j)]
[(1,1);(1,3);(1,5);(1,7);(2,2);(2,4);(2,6);(2,8);(3,1);(3,3);(3,5);
 (3,7);(4,2);(4,4);(4,6);(4,8);(5,1);(5,3);(5,5);(5,7);(6,2);(6,4);
 (6,6);(6,8);(7,1);(7,3);(7,5);(7,7);(8,2);(8,4);(8,6);(8,8)]
```

(Die Verwendung von Layout ist auch hilfreich, um Mehrdeutigkeiten zu vermeiden, die bei einer linearen, einzeiligen Notierung zuweilen auftreten.

```
[yield 815                    [yield 815
 for i in 0..9 do              for i in 0..9 do
   yield i                       yield i
 yield 4711]                   yield 4711]
```

Links wird das Element 4711 genau einmal generiert; auf der rechten Seite 10-mal. Der einzeilige Ausdruck [*yield* 815; *for* i *in* $0..9$ *do yield* i; *yield* 4711] ist hingegen mehrdeutig.)

Mit Hilfe von *for* können wir auch über die Elemente einer Liste bzw. eines Arrays iterieren.

```
⋙ let js = [yield 4711; for i in 0..5 do yield i*i]
⋙ [for j in js do yield 2*j+1]
[9423;1;3;9;19;33;51]
```

Der Bezeichner j wird nacheinander an die Elemente der Liste *js* gebunden. Für jede Bindung wird mit *yield* $2*j+1$ ein Element der resultierenden Liste generiert. Der Generator *for* i *in* $l..u$ ist übrigens eine Abkürzung für *for* i *in* $[l..u]$. Listenbeschreibungen eignen sich insbesondere, um aus bestehenden Listen neue Listen zu generieren. »Aus Alt mach Neu.«

Abstrakte Syntax Wir erweitern Ausdrücke um Listen- bzw. Arraybeschreibungen.

$e \in \text{Expr} ::=$	***Listen- und Arraybeschreibungen:***
$\mid [\ se\ ]$	Listenbeschreibung
$\mid [\![se]\!]$	Arraybeschreibung

Innerhalb der Klammern steht ein sogenannter ***Sequenzausdruck***, eine neue syntaktische Kategorie, deren Elemente Sequenzen von Werten bezeichnen. Wir verwenden hier Sequenz als semantischen Oberbegriff für Liste und Array.

$se \in \text{SExpr} ::=$	***Sequenzausdrücke:***
$\mid$ ***yield*** e	Element\einelementige Sequenz
$\mid$ ***yield!*** e	mehrere Elemente\Sequenz
$\mid d$ ***in*** se	lokale Definition
$\mid se_1; se_2$	Konkatenation
$\mid$ ***if*** e ***then*** se	Filter
$\mid$ ***if*** e ***then*** se_1 ***else*** se_2	Alternative
$\mid$ ***for*** x ***in*** e ***do*** se	Generator\beschränkte Iteration

Der Sequenzausdruck ***yield*** e steht für eine einelementige Sequenz, dessen einziges Element e ist; ***yield!*** e ist eine Abkürzung für ***for*** x ***in*** e ***do yield*** x und überführt die Liste e in eine Sequenz. Diese beiden Sequenzausdrücke sind *keine* Ausdrücke; sie haben keinerlei Bedeutung außerhalb der $[\ldots]$ bzw. $[\![\ldots]\!]$ Klammern. Lokale Definitionen, Konkatenation, Filter und Alternativen sind hingegen Zwitterwesen: Sie dienen sowohl als Ausdrücke als auch als Sequenzausdrücke mit (fast) identischer Bedeutung.

Der ***Generator*** heißt auch ***for-Schleife***, der Teilausdruck se ***Rumpf*** der Schleife. Schleife, da die Auswertung des Rumpfs se für alle Elemente von e wiederholt wird. Der Bezeichner x, die sogenannte ***Schleifenvariable***, wird dabei neu eingeführt; seine bzw. ihre Sichtbarkeit erstreckt sich auf den Rumpf der Schleife. (Im nächsten Abschnitt werden wir sehen, dass eine ***for***-Schleife ebenfalls als Ausdruck verwendet werden kann.)

Listen- und Arraybeschreibungen unterscheiden sich nur im Hinblick auf den Ergebnistyp — einmal interpretieren wir eine Sequenz als Liste, einmal als Array. Aus diesem Grund beschränken wir uns im Folgenden auf die präzise Definition von Listenbeschreibungen.

Statische Semantik Die eckigen Klammern überführen eine Sequenz in eine Liste.

$$\frac{\Sigma \vdash se : t^*}{\Sigma \vdash [\ se\ ] : List\,\langle t \rangle}$$

Der »Sequenztyp« t^* steht für Sequenzen von Elementen des Typs t.

$$\frac{\Sigma \vdash e : t}{\Sigma \vdash \textbf{yield}\ e : t^*} \qquad \frac{\Sigma \vdash e : List\,\langle t \rangle}{\Sigma \vdash \textbf{yield!}\ e : t^*}$$

$$\frac{\Sigma \vdash d : \Sigma' \qquad \Sigma, \Sigma' \vdash se : t^*}{\Sigma \vdash (d\ \textbf{in}\ se) : t^*} \qquad \frac{\Sigma \vdash se_1 : t^* \qquad \Sigma \vdash se_2 : t^*}{\Sigma \vdash (se_1; se_2) : t^*}$$

$$\frac{\Sigma \vdash e : Bool \qquad \Sigma \vdash se : t^*}{\Sigma \vdash \textbf{if}\ e\ \textbf{then}\ se : t^*}$$

$$\frac{\Sigma \vdash e : Bool \qquad \Sigma \vdash se_1 : t^* \qquad \Sigma \vdash se_2 : t^*}{\Sigma \vdash \textbf{if}\ e\ \textbf{then}\ se_1\ \textbf{else}\ se_2 : t^*}$$

$$\frac{\Sigma \vdash e_1 : List\,\langle t_1 \rangle \qquad \Sigma, \{x_1 \mapsto t_1\} \vdash se : t^*}{\Sigma \vdash \textbf{for}\ x_1\ \textbf{in}\ e_1\ \textbf{do}\ se : t^*}$$

Die Typregel für die ***for***-Schleife macht noch einmal deutlich, dass die Schleifenvariable neu eingeführt wird und sich ihre Sichtbarkeit auf den Rumpf der Schleife erstreckt.

Dynamische Semantik Listenbeschreibungen sind »syntaktischer Zucker« im besten Sinne des Wortes: Sie versüßen das Leben beim Programmieren, sind aber nicht lebensnotwendig. Alle Konstrukte lassen sich mit den bisherigen Bordmitteln formulieren: Zum Beispiel ist der Ausdruck $[\,\textit{for}\ i\ \textit{in}\ 0\,..\,9\ \textit{do yield}\ i*i\,]$ gleichwertig zu $\mathit{map}\ (\textit{fun}\ i \to i*i)\ [\,0\,..\,9\,]$; $[\,\textit{if}\ i\%2 = 1\ \textit{then yield}\ i*i\,]$ kürzt $\textit{if}\ i\%2 = 1\ \textit{then}\ [\,i*i\,]\ \textit{else}\ [\,]$ ab. Die Bedeutung der Konstrukte können wir erklären, indem wir sie entzuckern, in uns bekannte Ausdrücke *übersetzen*: Die Listenbeschreibung $[\,se\,]$ wird in den listenwertigen Ausdruck $[\![se]\!]$ übersetzt, wobei $[\![se]\!]$ wie folgt definiert ist.

$$
\begin{array}{ll}
[\![\textit{yield}\ e]\!] & = [\,e\,] \\
[\![\textit{yield!}\ e]\!] & = e \\
[\![d\ \textit{in}\ se]\!] & = d\ \textit{in}\ [\![se]\!] \\
[\![se_1; se_2]\!] & = [\![se_1]\!]\ @\ [\![se_2]\!] \\
[\![\ \textit{if}\ e\ \textit{then}\ se]\!] & = \textit{if}\ e\ \textit{then}\ [\![se]\!]\ \textit{else}\ [\,] \\
[\![\ \textit{if}\ e\ \textit{then}\ se_1\ \textit{else}\ se_2]\!] & = \textit{if}\ e\ \textit{then}\ [\![se_1]\!]\ \textit{else}\ [\![se_2]\!] \\
[\![\textit{for}\ x\ \textit{in}\ e\ \textit{do}\ se]\!] & = \mathit{collect}\ (\textit{fun}\ x \to [\![se]\!])\ e
\end{array}
$$

Die einarmige Alternative, ein Filter, ist eine Abkürzung für eine zweiarmige Alternative, deren *else*-Zweig die leere Liste $[\,]$ zurückgibt. Ein Generator wird mit Hilfe der vordefinierten Funktion $\mathit{collect} : (\mathit{'a} \to \mathit{'b\ list}) \to (\mathit{'a\ list} \to \mathit{'b\ list})$ implementiert: $\mathit{collect}\ f\ \mathit{list}$ wendet die listenwertige Funktion f auf jedes Element von list an und konkateniert die resultierenden Listen — das Rekursionsmuster kennen wir von *sum-by*.

```
let rec collect f = function
    | [ ]     → [ ]
    | x :: xs → f x @ collect f xs
```

Das folgende Beispiel illustriert die Übersetzung und anschließende Auswertung einer Listenbeschreibung.

$$
\begin{array}{ll}
 & [\,\textit{for}\ i\ \textit{in}\ [\,0\,..\,9\,]\ \textit{do if}\ i\%2 = 1\ \textit{then yield}\ i*i\,] \\
= & \quad \{\ \text{Übersetzung Listenbeschreibung}\ \} \\
 & [\![\textit{for}\ i\ \textit{in}\ [\,0\,..\,9\,]\ \textit{do if}\ i\%2 = 1\ \textit{then yield}\ i*i]\!] \\
= & \quad \{\ \text{Übersetzung Generator}\ \} \\
 & \mathit{collect}\ (\textit{fun}\ i \to [\![\ \textit{if}\ i\%2 = 1\ \textit{then yield}\ i*i]\!])\ [\,0\,..\,9\,] \\
= & \quad \{\ \text{Übersetzung Filter}\ \} \\
 & \mathit{collect}\ (\textit{fun}\ i \to \textit{if}\ i\%2 = 1\ \textit{then}\ [\![\textit{yield}\ i*i]\!]\ \textit{else}\ [\,])\ [\,0\,..\,9\,] \\
= & \quad \{\ \text{Übersetzung}\ \textit{yield}\ \} \\
 & \mathit{collect}\ (\textit{fun}\ i \to \textit{if}\ i\%2 = 1\ \textit{then}\ [\,i*i\,]\ \textit{else}\ [\,])\ [\,0\,..\,9\,] \\
= & \quad \{\ \text{Definition von}\ [\,l\,..\,u\,]\ \} \\
 & \mathit{collect}\ (\textit{fun}\ i \to \textit{if}\ i\%2 = 1\ \textit{then}\ [\,i*i\,]\ \textit{else}\ [\,])\ [0;1;2;3;4;5;6;7;8;9] \\
= & \quad \{\ \text{Definition von}\ \mathit{collect}\ \} \\
 & [\,]\ @\ [\,1\,]\ @\ [\,]\ @\ [\,9\,]\ @\ [\,]\ @\ [\,25\,]\ @\ [\,]\ @\ [\,47\,]\ @\ [\,]\ @\ [\,81\,] \\
= & \quad \{\ \text{Definition von »@«}\ \} \\
 & [1;9;25;47;81]
\end{array}
$$

Der Funktionsausdruck $\textit{fun}\ i \to \ldots$ überführt eine ungerade Zahl in eine einelementige Liste und eine gerade Zahl in die leere Liste. Die Konkatenation der resultierenden Listen ist das Ergebnis der Listenbeschreibung.

Vertiefung: Hauptspeicherdatenbank Das Motto von Listenbeschreibungen »Aus Alt mach Neu« lässt sich prima mit Datenbanktabellen und Datenbankanfragen illustrieren. Die folgenden selbsterklärenden Typdefinitionen modellieren Studierende, Module und Prüfungsergebnisse.

module Effects.Database

```
type Name    = String          // student name
type GUID    = Int             // student id (Globally Unique Identifier)
type Course  = | ALG | FPR | IPR | OOP
type Mark    = | Insufficient | Sufficient | Good | VeryGood | Excellent
type Student = {name : Name; guid : GUID}
type Result  = {course : Course; guid : GUID; mark : Mark}
```

Eine ***Datenbanktabelle*** ist eine Liste von Records; eine ***Datenbankanfrage*** selektiert oder extrahiert Informationen aus einer Tabelle oder kombiniert Daten aus mehreren Tabellen, siehe Abbildung 7.3. Die Abarbeitung der Anfragen folgt dem oben beschriebenen Übersetzungsschema und taugt durchaus für kleine Tabellen mit mehreren hundert Einträgen. Für die Verarbeitung größerer Datenmengen müssen Tabellen geschickter dargestellt und Anfragen entsprechend optimiert werden. Mehr zum diesem Thema erfahren Sie im weiteren Studium in der Vorlesung Informationssysteme.

Vertiefung: »Dateisystem-Crawler« Die in Abbildung 7.3 aufgeführten Listenbeschreibungen sind frei von Effekten — passen also thematisch eher ins Kapitel 4. Listenbeschreibungen können aber auch gewinnbringend mit effektvollen Ausdrücken kombiniert werden. Die Standardbibliothek von F# bietet verschiedene Funktionen an, um auf das Dateisystem zuzugreifen. Kurz zum Hintergrund: Das ***Dateisystem*** (engl. file system) ist Bestandteil des Betriebssystems und organisiert die persistente Speicherung von Daten in sogenannten Dateien (engl. files). Moderne Dateisysteme sind hierarchisch organisiert: Dateien werden in Verzeichnissen (engl. folder) abgelegt; Verzeichnisse dürfen neben Dateien Unterverzeichnisse enthalten, die auf die gleiche Art und Weise organisiert sind. Die Grafik in Abbildung 7.4 zeigt einen *Auszug* aus der Verzeichnisstruktur eines Linux-Dateisystems.

module Effects.Files

Die F# Bibliothek *System.IO* enthält unter anderem die Funktionen

```
Directory.GetFiles       : String → Array ⟨String⟩
Directory.GetDirectories : String → Array ⟨String⟩
```

die die in einem Verzeichnis abgelegten Dateien bzw. Unterverzeichnisse ermitteln.

```
>>> open System.IO
>>> Directory.GetFiles "."
[|"./Mini.fs";"./README"|]
>>> Directory.GetDirectories "."
[|"./Algorithmics";"./Basics";"./Datatypes";"./Effects";"./Grammar";
 "./Introduction";"./Objects";"./Values"|]
```

Das Verzeichnis ».« ist eine Abkürzung für das aktuelle Verzeichnis, im obigen Beispiel für `/home/ralf/Mini-F#/`. Die folgende Funktion bestimmt alle Dateien, die in *und* unterhalb eines Verzeichnisses abgelegt sind.

```
open System.IO

let rec list-files dir =
  [|yield! Directory.GetFiles dir
    for d in Directory.GetDirectories dir do
      yield! list-files d|]
```

```
let students : Student list =
  [{name = "Ralf"; guid = 4711};
   {name = "Lisa"; guid = 815  };...]
let results : Result list =
  [{course = ALG; guid = 4711; mark = Good      };
   {course = FPR; guid = 815;  mark = Excellent };
   {course = FPR; guid = 4711; mark = Sufficient};...]
```

Wie heißt der Student mit der Matrikelnummer 4711?

```
let query1 : Name =
  List.head [for student in students do
                if student.guid = 4711 then
                  yield student.name]
```

Liste die Ergebnisse der Vorlesung *ALG*.

```
let query2 : Mark list =
  [for result in results do
     if result.course = ALG then
       yield result.mark]
```

Wer hat das beste Ergebnis in der Vorlesung *FPR* erzielt?

```
let query3 : GUID =
  snd (List.max [for result in results do
                   if result.course = FPR then
                     yield (result.mark, result.guid)])
```

Welche Ergebnisse hat der Student namens `"Ralf"` erzielt?

```
let query4 : Mark list =
  [for student in students do
     if student.name = "Ralf" then
       for result in results do
         if student.guid = result.guid then
           yield result.mark]
```

Wer hat mindestens ein exzellentes Ergebnis in einem der Kurse?

```
let query5 : Name list =
  [for result in results do
     if result.mark = Excellent then
       for student in students do
         if result.guid = student.guid then
           yield student.name]
```

Abbildung 7.3.: Eine Prüfungsdatenbank und verschiedene Datenbankanfragen.

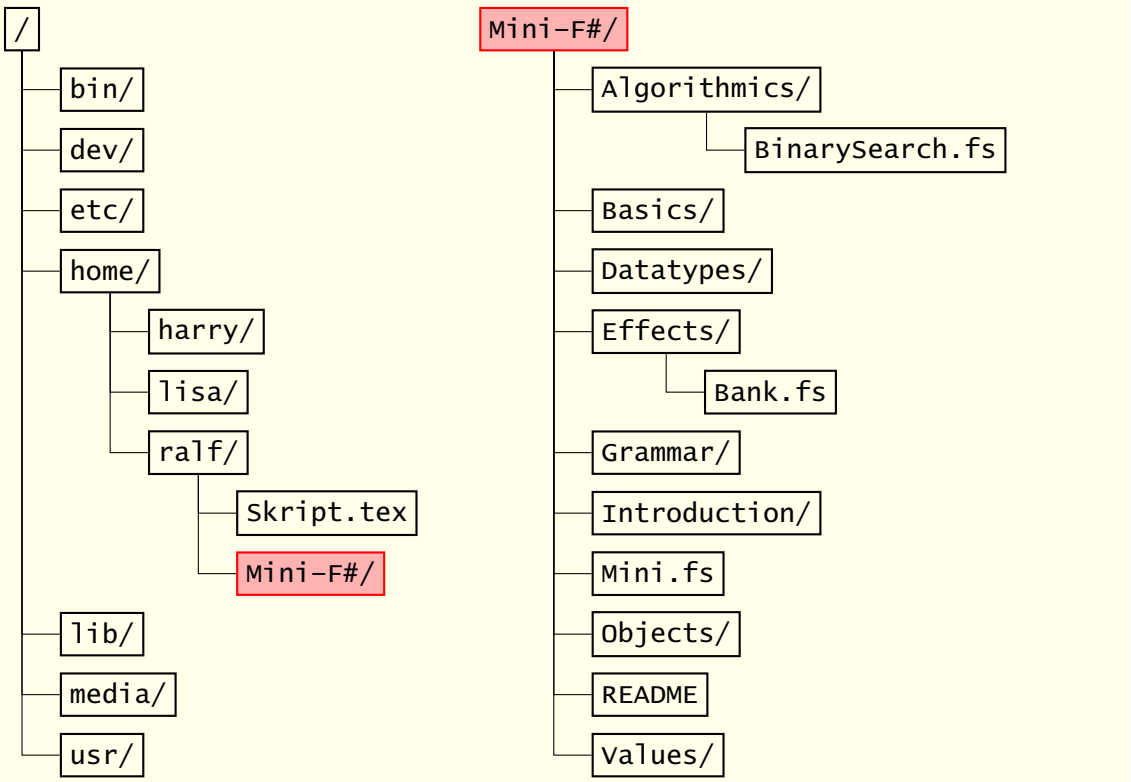


Abbildung 7.4.: Verzeichnisstruktur eines Linux-Dateisystems.

Zunächst werden mit ***yield***! alle Dateien im aktuellen Verzeichnis aufgezählt; für jedes Unterverzeichnis erfolgt ein rekursiver Aufruf, der entsprechend abgearbeitet wird. Die Rekursion terminiert, wenn ein Verzeichnis keine weiteren Unterverzeichnisse enthält, der Aufruf *Directory.GetDirectories dir* das leere Array zurückgibt. Die Funktion *list-files* in Aktion:

```
>>> list-files "."
[|"./Mini.fs";"./README";"./Algorithmics/BinarySearch.fs";
 "./Algorithmics/Neighbours.fs";...;"./Datatypes/Person.fs";...;
 "./Effects/Bank.fs";"./Effects/Files.fs";...|]
```

7.3.2. Schleifen

Eine ***for***-Schleife kann auch verwendet werden, um effektvolle Ausdrücke aneinanderzureihen. Die folgenden Beispiele illustrieren einige der Möglichkeiten:

```
>>> print 4711; for i in 0 .. 5 do print (i * i)
4711
0
1
4
9
16
25
```

```
⋙ for i in 0..9 do if i%2 = 1 then print (i * i)
1
9
25
49
81

⋙ for i in 1..8 do
    for j in 1..8 do
      if (i+j)%2 = 0 then
        print (i,j)
(1,1)
(1,3)
…
(8,6)
(8,8)
```

Die Ausdrücke sind fast identisch zu denen aus Abschnitt 7.3.1. Wir haben lediglich ***yield*** durch *print* ersetzt und die Listenklammern entfernt. Anstatt Elemente mit ***yield*** in einer Liste zu sammeln, wird jetzt jedes Element mit *print* ausgegeben. Anstatt Elemente aneinanderzureihen, werden Effekte aneinandergereiht. Die Funktion *print* gibt übrigens einen beliebigen Wert aus: ***let*** *print a* = *putline* (*show a*).

Es ist natürlich nicht zwingend, die Elemente auszugeben. Das folgende Beispiel illustriert einen anderen Effekt.

```
let sum (xs : List ⟨Int⟩) : Int =
  let mutable acc = 0
  for x in xs do
    acc ← acc + x
  acc
```

Die Funktion *sum* addiert die Elemente der angegebenen Liste auf. Wir verwenden eine Veränderliche namens *acc* (kurz für accumulator, engl. für Akkumulator), um uns die jeweilige Zwischensumme zu merken. Für jedes Listenelement wird die Zwischensumme um ebendieses Element erhöht — diese Zuweisung ist der effektvolle Ausdruck, der für jedes Listenelement ausgeführt wird. Ist das Listenende erreicht, wird die Zwischensumme zur Gesamtsumme.

Ganz entsprechend lassen sich Arrays aufaddieren.

```
let sum (a : Array ⟨Int⟩) : Int =
  let mutable acc = 0
  for x in a do
    acc ← acc + x
  acc
```

```
let sum (a : Array ⟨Int⟩) : Int =
  let mutable acc = 0
  for i in 0..a.Length - 1 do
    acc ← acc + a.[i]
  acc
```

Wir können entweder direkt über die Arrayelemente selbst iterieren oder über ihre Hausnummern. Bezüglich der Laufzeit ergeben sich keine Unterschiede, da die Subskription, der Zugriff über die Hausnummer, in konstanter Zeit erfolgt.

Eine ***for***-Schleife wiederholt einen Effekt für *alle* Elemente einer Liste oder eines Arrays. Diese Kontrollstruktur ist nicht für alle Aufgabenstellungen adäquat. Erinnern wir uns an die lineare Suche: Ist ein Element mit der gewünschten Eigenschaft gefunden, wird die Suche unmittelbar beendet. In Abschnitt 3.6 haben wir die lineare Suche *rekursiv* formuliert. Das folgende Programm zeigt, wie man die lineare Suche *iterativ* mit Hilfe einer ***while***-Schleife implementiert.

module Effects.Sort

```
let linear-search (key : 'elem) (a : Array ⟨'elem⟩) : Option ⟨Int⟩ =
  let mutable i = 0
  while i < a.Length && a.[i] < key do
    i ← i + 1
  if i < a.Length && a.[i] = key then Some i
                                 else None
```

Die Funktion verlangt ein sortiertes Feld und bestimmt die kleinste Hausnummer i, so dass $a.[i] = key$. Der Rumpf der ***while***-Schleife wird wiederholt, solange die Schleifenbedingung wahr ist. Solange das Ende des Arrays noch nicht erreicht ist, $i < a.Length$, und das aktuelle Arrayelement kleiner ist als der Suchschlüssel, $a.[i] < key$, wird der Index erhöht, $i \leftarrow i + 1$. Eine ***while***-Schleife ist *nur* im Zusammenspiel mit Effekten sinnvoll. Die Schleifenbedingung wird wiederholt ausgerechnet; damit sich der Wahrheitswert ändert, *muss* der Ausdruck von Benutzereingaben oder vom Speicher abhängen. Das ist hier der Fall: Beide Bestandteile der Konjunktion enthalten die Veränderliche i, deren Wert im Rumpf auch verändert wird.

Auch die binäre Suche lässt sich iterativ formulieren — die Funktion *binary-search* aus Abschnitt 3.6 ist ebenso wie die lineare Suche *endrekursiv*; endrekursive Funktionen können relativ einfach in iterative Programme übersetzt werden, siehe Abschnitt 7.3.3. Das folgende Programm löst das gleiche Problem wie *linear-search*, basiert aber auf der Idee der binären Suche, der Intervallschachtelung. (Da die Funktion einen 3-Wege Vergleich verwendet, haben wir sie auf den Namen *ternary-search* getauft.)

```
let ternary-search (key : 'elem) (a : Array ⟨'elem⟩) : Option ⟨Int⟩ =
  let mutable l = 0
  let mutable u = a.Length − 1
  let mutable found = None
  while l ⩽ u && found = None do
    let m = (l + u) ÷ 2
    if    key < a.[m]   then u ← m − 1
    elif  key = a.[m]   then found ← Some m
    (* key > a.[m] *)  else  l ← m + 1
  found
```

Wir definieren drei Veränderliche: die beiden Intervallgrenzen und den Suchstatus. Die Schleifenbedingung involviert alle drei Veränderliche; im Schleifenrumpf wird genau eine von ihnen modifiziert. Nach endlich vielen Schritten ist entweder das Suchintervall $l\,..\,u$ leer oder der Suchschlüssel *key* gefunden.

Abstrakte Syntax Ausdrücke vom Typ *Unit*, die *nur* ihres Effektes wegen ausgerechnet werden, heißen auch ***Anweisungen***. Eine Funktion des Typs $t \to Unit$, die *nur* ihres Effektes wegen aufgerufen wird, wird auch ***Prozedur*** genannt.

Die folgende Tabelle fasst die wichtigsten Kontrollstrukturen zusammen, mit deren Hilfe elementare Anweisungen wie zum Beispiel Ausgabeoperationen oder Zuweisungen zu komplexen Anweisungen zusammengebaut werden.

$e ::= \cdots$	***Kontrollstrukturen:***
$\mid e_1; e_2$	Sequenz
$\mid$ ***if*** e_1 ***then*** e_2	einarmige Alternative
$\mid$ ***if*** e_1 ***then*** e_2 ***else*** e_3	zweiarmige Alternative
$\mid$ ***for*** x ***in*** e_1 ***do*** e_2	beschränkte Wiederholung\Iteration
$\mid$ ***while*** e_1 ***do*** e_2	unbeschränkte Wiederholung\Iteration

Zur Erinnerung: Die Sequenz $e_1; e_2$ entspricht dem ***in***-Ausdruck ***let*** $\_ = e_1$ ***in*** e_2, der die Auswertung von e_1 und e_2 sequentialisiert. Die einarmige Alternative ***if*** e_1 ***then*** e_2 ist eine Abkürzung für ***if*** e_1 ***then*** e_2 ***else*** $()$. Der Dummywert »()« zeigt an, dass der ***else***-Zweig keinen Effekt hat. Der Teilausdruck e_1 in ***while*** e_1 ***do*** e_2 heißt ***Schleifenbedingung*** oder ***Laufbedingung***; e_2 heißt ***Schleifenrumpf***. (Laufbedingung, weil die Schleife »läuft«, solange die Bedingung wahr ist; es gibt in anderen Programmiersprachen auch Schleifenkonstrukte mit inverser Logik, die eine ***Abbruchbedingung*** verwenden.)

Statische Semantik Wir beschränken uns auf die Formalisierung von ***for***-Schleifen, die über Listen iterieren. Analoge Überlegungen gelten für Iterationen über Arrays. Die ***for***-Schleife ist ein »Binder«: Die Schleifenvariable ist im Rumpf der Schleife sichtbar.

$$\frac{\Sigma \vdash e_1 : \mathit{List}\,\langle t_1 \rangle \qquad \Sigma, \{x_1 \mapsto t_1\} \vdash e : \mathit{Unit}}{\Sigma \vdash \textbf{\textit{for}}\ x_1\ \textbf{\textit{in}}\ e_1\ \textbf{\textit{do}}\ e : \mathit{Unit}}$$

$$\frac{\Sigma \vdash e_1 : \mathit{Bool} \qquad \Sigma \vdash e_2 : \mathit{Unit}}{\Sigma \vdash \textbf{\textit{while}}\ e_1\ \textbf{\textit{do}}\ e_2 : \mathit{Unit}}$$

Der Schleifenrumpf ist jeweils eine Anweisung, ein Ausdruck vom Typ *Unit*. Beide Schleifen werden nur des Effektes willen ausgeführt.

module Effects.Control

Dynamische Semantik Aus Gründen des Lesbarkeit beschränken wir uns wie in Abschnitt 7.2 auf die Modellierung von Speichereffekten und ignorieren externe Effekte.

$$\frac{\sigma \parallel \delta \vdash e_1 \Downarrow [\nu_0; \ldots; \nu_{n-1}] \parallel \sigma_0 \qquad \sigma_i \parallel \delta, \{x_1 \mapsto \nu_i\} \vdash e \Downarrow () \parallel \sigma_{i+1} \mid i \in \mathbb{N}_n}{\sigma \parallel \delta \vdash \textbf{\textit{for}}\ x_1\ \textbf{\textit{in}}\ e_1\ \textbf{\textit{do}}\ e \Downarrow () \parallel \sigma_n}$$

Zunächst wird die Liste e_1 ausgewertet; die Schleifenvariable x_1 wird nacheinander an die Listenelemente gebunden; bezüglich jeder Bindung wird der Schleifenrumpf e ausgerechnet. Zur Erinnerung: $\phi_i \mid i \in \mathbb{N}_n$ ist eine kompakte Schreibweise für die n Voraussetzungen ϕ_0, …, ϕ_{n-1}. Jede Auswertung verändert potentiell den Speicher, der von Auswertung zu Auswertung weitergereicht wird. Die ***for***-Schleife »kommuniziert« mit ihrer Umwelt mittels des Speichers — ihr Wert, das einzige Element vom Typ *Unit*, steht ja bereits vor der Auswertung fest.

Für die ***while***-Schleife gelten ähnliche Überlegungen.

$$\frac{\sigma \parallel \delta \vdash e_1 \Downarrow \mathit{false} \parallel \sigma_1}{\sigma \parallel \delta \vdash \textbf{\textit{while}}\ e_1\ \textbf{\textit{do}}\ e_2 \Downarrow () \parallel \sigma_1}$$

$$\frac{\sigma \parallel \delta \vdash e_1 \Downarrow \mathit{true} \parallel \sigma_1 \qquad \sigma_1 \parallel \delta \vdash e_2 \Downarrow \nu \parallel \sigma_2 \qquad \sigma_2 \parallel \delta \vdash \textbf{\textit{while}}\ e_1\ \textbf{\textit{do}}\ e_2 \Downarrow () \parallel \sigma_3}{\sigma \parallel \delta \vdash \textbf{\textit{while}}\ e_1\ \textbf{\textit{do}}\ e_2 \Downarrow () \parallel \sigma_3}$$

Zunächst wird die Schleifenbedingung e_1 ausgewertet. Ist das Ergebnis *false*, ist die Auswertung damit abgeschlossen; anderenfalls wird der Schleifenrumpf e_2 ausgewertet und *die Schleife wird erneut ausgewertet*. Ein wichtiges Detail: Die wiederholte Auswertung »sieht« den modifizierten Speicher σ_2. Die letzte Auswertungsregel zählt zu den ungewöhnlichsten, die uns bisher begegnet sind. Normalerweise wird die Bedeutung eines Ausdrucks auf die Bedeutung seiner *Teil*ausdrücke zurückgeführt. Die ***while***-Regel folgt nicht dieser kompositionalen Herangehensweise: Eine der Voraussetzung enthält den zu definierenden Ausdruck selbst.

Der Dämon der Nichtterminierung lugt um die Ecke. Verändern weder e_1 noch e_2 den Speicher, ***while*** *true* ***do*** $i \leftarrow i + 1$, dann tritt die Schlussfolgerung unverändert als Voraussetzung auf, ein unendlicher Regress. Mit anderen Worten: Es lässt sich kein Beweisbaum für die Auswertung konstruieren. Es ist zwingend notwendig, dass der Speicher modifiziert wird. Notwendig, aber nicht hinreichend: $i \leftarrow 1$; ***while*** $i > 0$ ***do*** $i \leftarrow i + 1$ terminiert ebenfalls nicht. Wie die ungebändigte

Rekursion — Rekursion, die nicht den Vorgaben eines Entwurfsmusters folgt — birgt die ***while***-Schleife die Gefahr der Nichtterminierung und sollte daher mit Bedacht verwendet werden.

Schleifen sind wie Listen- und Arraybeschreibungen syntaktischer Zucker. Wir können ihre Bedeutung auch klären, indem wir sie in uns bereits bekannte Konstrukte übersetzen, sprich, indem wir die Schleifen programmieren. Die Schleife ***for*** *x* ***in*** *l*..*u* ***do*** *e* lässt sich zum Beispiel in den Aufruf *foreach* (*l*, *u*) (***fun*** *x* → *e*) übersetzen, wobei *foreach* wie folgt definiert ist. (Umgekehrt kann *foreach* (*l*, *u*) *body* durch ***for*** *x* ***in*** *l*..*u* ***do*** *body x* implementiert werden.)

```
let rec foreach (lower : Nat, upper : Nat) (body : Nat → Unit) : Unit =
  if lower ⩽ upper then
    body lower
    foreach (lower + 1, upper) body
```

Die ***for***-Schleife ist ein Binder; in der Übersetzung wird die Bindung auf einen Funktionsausdruck abgebildet, die Mutter aller variablenbindenden Konstrukte. Die Definition von *foreach* folgt dem Entwurfsmuster für Intervalle: Die Terminierung ist garantiert, sofern der Rumpf stets terminiert. Zur Übung: Programmieren sie entsprechende Funktionen, um über alle Elemente einer Liste bzw. eines Arrays zu iterieren, siehe Aufgabe 7.3.3.

In die Übersetzung der ***while***-Schleife müssen wir mehr Grips stecken. Die Typregel suggeriert, eine Funktion der Form ***let rec*** *whiledo* (*test* : *Bool*) (*body* : *Unit*) : *Unit* zu definieren. Das ist allerdings zu kurz gedacht. Da Parameter in Mini–F# vor dem Aufruf ausgewertet werden (Stichwort: call by value), würde der Test und der Rumpf genau einmal beim Aufruf von *whiledo* ausgewertet. (Mit den entsprechenden Konsequenzen: Die Schleife wird entweder gar nicht ausgeführt oder endlos.) Die Schleifenbedingung ist kein Boolescher Wert, sondern eine *Rechnung*, die einen Wahrheitswert zum Ergebnis hat. Wir müssen den Test durch eine *Funktion* des Typs *Unit* → *Bool* modellieren und den Rumpf entsprechend durch eine Funktion des Typs *Unit* → *Unit*. Die Schleife ***while*** e_1 ***do*** e_2 wird dann in *whiledo* (***fun*** () → e_1) (***fun*** () → e_2) übersetzt. Wir erinnern uns: »Funktionsausdrücke werten zu sich selbst aus«; ihre Auswertung wird eingefroren. Beim Aufruf von *whiledo* wird auf diese Weise weder e_1 noch e_2 ausgewertet. (Umgekehrt kann *whiledo test body* durch ***while*** *test* () ***do*** *body* () implementiert werden.)

```
let rec whiledo (test : Unit → Bool) (body : Unit → Unit) : Unit =
  if test () then
    body ()
    whiledo test body
```

Die Funktionsabschlüsse werden zum Leben erweckt, sie werden aufgetaut, indem sie auf das Dummyargument »()« angewendet werden. Die Definition von *whiledo* führt uns die Gefahr der Nichtterminierung noch einmal plastisch vor Augen: Der rekursive Aufruf ist identisch zu dem ursprünglichen Aufruf, kein Parameter wird verändert.

Die Definitionen von *foreach* und *whiledo* sind übrigens *endrekursiv*: Der rekursive Aufruf ist die letzte Aktion im Funktionsrumpf. Endrekursive Programme lassen sich in iterative Programme übersetzen, siehe Abschnitt 7.3.3 — der Kreis schließt sich.

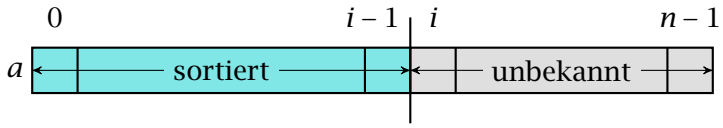
Vertiefung: Sortieren In Abschnitt 5.1.1 haben wir zwei einfache Algorithmen kennengelernt, um Folgen von Elementen zu sortieren: Sortieren durch Einfügen und Sortieren durch Auswählen. Die Implementierungen der Sortierverfahren arbeiten auf Listen: Sie nehmen eine unsortierte Liste als Eingabe und geben eine sortierte Permutation als Ausgabe zurück. Im Folgenden schauen wir uns an, wie man Arrays sortieren kann. Genauer: Wir überlegen, wie man die Elemente an »Ort und Stelle« (engl. in place, lat. in situ) sortieren kann, *ohne* zusätzlichen Speicher zu allokieren. Die folgende Interaktion zeigt die Vorgehensweise.

module Effects.Sort

```
⋙ let revenues = ⟦815; 4; 7; 1; 1⟧
⋙ selection-sort revenues
()
⋙ revenues
⟦1; 1; 4; 7; 815⟧
```

Die Sortierfunktion hat kein interessantes Ergebnis — sie hat den Ergebnistyp *Unit* — aber einen bemerkenswerten Effekt: Nach dem Aufruf ist das Eingabearray sortiert. Wir werden sehen, dass die Reimplementierung der Sortierverfahren sich stark von den Programmen aus Abschnitt 5.1.1 unterscheidet — obwohl sie jeweils die gleiche algorithmische Idee umsetzen.

Wenden wir uns zunächst dem Sortieren durch Auswählen zu. Da wir mit dem zur Verfügung stehenden Platz in Form des Eingabearrays auskommen müssen, organisieren wir die Sortierung durch wiederholtes Vertauschen von Arrayelementen. Dazu teilen wir das gegebene Array a gedanklich in zwei Zonen auf:



wobei $n = a.Length$. Die linke, grüne Zone ist sortiert; über die rechte, graue Zone wissen wir nichts. Die grüne Zone wird schrittweise nach rechts ausgedehnt, bis sie sich über das gesamte Areal erstreckt. Ein Schritt besteht darin, das Minimum der grauen Zone zu bestimmen und mit dem ersten Element der grauen Zone auszutauschen.

```
let selection-sort (a : Array ⟨'elem⟩) =
  let n = a.Length
  for i in 0 .. n – 2 do
    // determine minimum of a.[i], . . . , a.[n – 1]
    let mutable m = i
    for j in i + 1 .. n – 1 do
      if a.[j] < a.[m] then
        m ← j;
    // swap a.[i] and a.[m]
    let tmp = a.[i]
    a.[i]   ← a.[m]
    a.[m] ← tmp
```

Um die Vertauschung einfach durchführen zu können, wird die *Position* des Minimums bestimmt: m ist die Position und $a.[m]$ das eigentliche Minimum.

Ist das Programm korrekt? Ähnlich wie wir die Korrektheit eines rekursiven Programms mit Hilfe einer Rekursionsinvariante nachweisen können (siehe Abschnitt 5.2.4), können wir die Korrektheit eines iterativen Programms mit Hilfe einer ***Schleifeninvariante*** zeigen. Die Invariante fängt typischerweise die algorithmische Idee ein, in unserem Beispiel die Unterteilung des Arrays in zwei Zonen.

Invariante (i): $\quad a.[0] \leqslant a.[1] \leqslant \cdots \leqslant a.[i-1]$
$\forall\, j, k \;.\; 0 \leqslant j < i \;\wedge\; i \leqslant k < n \;\Rightarrow\; a.[j] \leqslant a.[k]$

Die Invariante ist mit der Zonengrenze i parametrisiert. Die Invariante fordert, dass die grüne Zone sortiert ist und dass die Elemente der grünen Zone höchstens so groß sind, wie die Elemente der grauen Zone.

Auch Schleifeninvarianten durchlaufen in ihrem Leben drei Phasen:

1. die Invariante wird etabliert (vor der Schleife);
2. die Invariante wird erhalten (bei einem Schleifendurchlauf);
3. aus der Invariante folgt das gewünschte Ergebnis (nach der Schleife).

Für unser Beispiel ergeben sich die folgenden Überlegungen:
1. Phase: Wenn $i = 0$ gilt, dann ist die grüne Zone leer und die Anforderungen gelten trivialerweise.
2. Phase: Wir müssen zeigen, dass nach einem Schleifendurchlauf die Invariante für $i+1$ gilt, unter der Annahme, dass sie vor dem Durchlauf für i gilt. Da der grüne Bereich um das Element $a.[i]$ erweitert wird, reicht es zu zeigen, dass dieses Element größer ($\geqslant$) ist als alle Elemente zur Linken und kleiner ($\leqslant$) als alle Elemente zur Rechten. Ersteres gilt aufgrund der Invariante für i und der Tatsache, dass $a.[i]$ aus der grauen Zone stammt. Letzteres gilt, da $a.[i]$ das Minimum der grauen Zone ist.
3. Phase: Wenn $i = n-1$ ist, dann besteht die graue Zone aus genau einem Element, das zudem größer ist als alle Elemente der grünen Zone. Somit ist das gesamte Array sortiert. Was zu beweisen war.

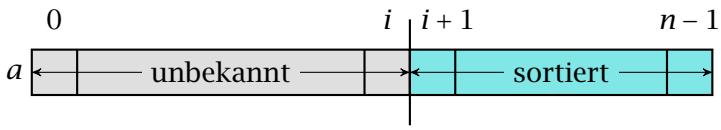
Terminiert das Programm? Klare Antwort: Ja! Eine ***for***-Schleife gibt ein Terminierungsversprechen. Da nur über endliche viele Elemente eines Intervalls, einer Liste oder eines Arrays iteriert wird, ist die Terminierung sichergestellt, sofern der Schleifenrumpf stets terminiert. Das obige Programm besteht aus zwei ineinandergeschachtelten ***for***-Schleifen und einigen elementaren Ausdrücken, so dass nichts anbrennen kann.

Welche Laufzeit hat das Programm? Laufzeit ist die kleine Schwester der Terminierung. Eine ***for***-Schleife gibt nicht nur ein Terminierungsversprechen, sondern sie erlaubt auch klare Aussagen über die Laufzeit. Ein Schleife der Form ***for*** x ***in*** $l\,..\,u-1$ ***do*** e wiederholt den Schleifenrumpf e insgesamt $u-l$ mal; die Kosten für die Abarbeitung des Rumpfes müssen entsprechend aufsummiert werden. Hängt die Laufzeit nicht von der Schleifenvariablen x ab, dann ergibt sich die Laufzeit als Produkt von $u-l$ und der Anzahl der benötigten Schritte für e. Besteht eine Abhängigkeit, müssen wir mittels einer Summenformel die Kosten aufaddieren. Unser Beispiel illustriert beide Fälle. (Wir zählen der Einfachheit halber nur die Anzahl der Vergleiche $a.[j] < a.[m]$). Die innere Schleife wiederholt die einarmige Alternative $n-(i+1)$ mal; die äußere Schleife wiederholt die innere Schleife $n-1$ mal, allerdings mit unterschiedlichen Werten für die Schleifenvariable i. Mit einer Summenformel ausgedrückt:

$$\sum_{i=0}^{n-2} n-(i+1) = \sum_{i=1}^{n-1} i = (n-1)\cdot n/2$$

Das Ergebnis stimmt exakt mit der Laufzeit der listenbasierten Implementierung aus Abschnitt 5.1.1 überein. Sortieren durch Auswählen ist und bleibt ein quadratisches Sortierverfahren.

Kommen wir zum Sortieren durch Einfügen. Wir teilen das zu sortierende Array wiederum gedanklich in zwei Zonen auf.



Dual zum Sortieren durch Einfügen befindet sich die sortierte, grüne Zone jetzt rechts. Wir lassen sie schrittweise wachsen, indem wir jeweils ein graues Element in die grüne Zone einfügen. (Aufgabe 7.3.1 klärt, warum wir von rechts nach links vorgehen.)

```
let insertion-sort (a : Array ⟨'elem⟩) =
  let n = a.Length
  for i in n − 2 .. −1 .. 0 do
    let key = a.[i]
    // insert key into the sorted sub-array a.[i + 1], . . , a.[n − 1]
    let mutable j = i + 1
    while j < n && key > a.[j] do
      a.[j − 1] ← a.[j]
      j ← j + 1
    a.[j − 1] ← key
```

Die ***for***-Schleife verwendet ein Konstrukt, das uns bisher noch nicht untergekommen ist, ein ***Intervall mit Schrittweite***: $l\,..\,d\,..\,r$ generiert die Elemente l, $l+d$, $l+2\cdot d$, ..., r. Mit $0\,..\,1\,..\,n-1$ oder kurz $0\,..\,n-1$ werden die Hausnummern des Arrays a aufsteigend, von links nach rechts aufgezählt; mit $n-1\,..\,-1\,..\,0$ absteigend, von rechts nach links; kurz: spiegelverkehrt.

Um das Element $a.[i]$ in die grüne Zone einzufügen, verwenden wir eine ***while***-Schleife: Solange wir noch nicht den rechten Rand der grünen Zone erreicht haben und die richtige Position nicht ermittelt ist, gehen wir nach rechts. »Einfügen« hört sich etwas einfacher an, als es tatsächlich ist. Um ein Element in ein Array einzufügen, müssen wir Platz schaffen. Auf dem Weg durch die grüne Zone werden die Arraylemente um eine Position nach links verschoben. Das erste Arrayelement, das *überschrieben* wird, ist das einzufügende Element selbst. Aus diesem Grund merken wir uns das Element, indem wir $a.[i]$ an den Bezeichner *key* binden. Summa summarum werden die Arrayelemente $a.[i]$, ..., $a.[j-1]$ zyklisch nach links vertauscht, wobei $a.[j-1]$ das größte Element der grünen Zone ist, das echt kleiner als $a.[i]$ ist.

Terminiert das Programm? Vorsicht ist geboten: Im Unterschied zu einer ***for***-Schleife gibt eine ***while***-Schleife kein Terminierungsversprechen: Zum Beispiel terminiert der Ausdruck ***while*** *true* ***do*** *print* `"busy"` nicht. Im Fall von *insertion-sort* können wir allerdings Entwarnung geben: Das erste Glied der Konjunktion, $j < n$, im Zusammenspiel mit der letzten Zuweisung im Schleifenrumpf, $j \leftarrow j+1$, stellt die Terminierung sicher.

Welche Laufzeit hat das Programm? Die ***while***-Schleife wird im schlechtesten Fall $n-(i+1)$ mal durchlaufen. Die ***for***-Schleife wiederholt die ***while***-Schleife $n-1$ mal, allerdings mit unterschiedlichen Werten für die Schleifenvariable i. Insgesamt werden $(n-1)\cdot n/2$ Schritte benötigt.

Die ***while***-Schleife implementiert eine lineare Suche. Können wir die Suche beschleunigen, indem wir binär suchen? Ja, aber das zahlt sich leider nicht aus, da für das einzufügende Element Platz geschaffen werden muss. Der konstante Zugriff auf Arrayelemente lässt sich in diesem Fall nicht zu unserem Vorteil nutzen.

Auch Sortieren durch Einfügen ist und bleibt ein quadratisches Sortierverfahren. Unterschiede ergeben sich allerdings, wie bereits besprochen, im besten Fall: Ist die Eingabe bereits sortiert, benötigt Sortieren durch Einfügen nur $n-1$ Vergleiche, während Sortieren durch Auswählen weiterhin eine quadratische Laufzeit hat. Diese Unterschiede lassen sich an Äußerlichkeiten festmachen. Sortieren durch Auswählen verwendet zwei ineinandergeschachtelte ***for***-Schleifen, die stets über die gleichen Intervalle iterieren; die Anzahl der Schritte ist somit unabhängig von den Eingabeelementen. Sortieren durch Auswählen ist »vergesslich« (engl. oblivious). Sortieren durch Einfügen ersetzt die innere Schleife durch eine ***while***-Schleife, die *maximal* $n-(i+1)$ mal durchlaufen wird, aber unter Umständen auch gar nicht. Sortieren durch Einfügen zeigt ein *adaptives* Verhalten.

Wir haben in Abschnitt 5.1.3 besprochen, dass jedes Sortierverfahren, das auf dem Vergleichen von Elementen basiert, im schlechtesten Fall mindestens $n \lg n$ Vergleiche benötigt. Nun ist es nicht immer zwingend zu vergleichen; um zum Beispiel ein Array zu sortieren, das nur Zahlen aus einem gegebenen Intervall, $0\,..\,m$, enthält, bietet es sich an, zu zählen, wie häufig jedes Element

aus dem Intervall vorkommt.

```
let counting-sort (m : Int, array : Array ⟨Int⟩) : Array ⟨Int⟩ =
  let counts = ⟦for i in 0 .. m → 0⟧
  for j in array do
    counts.[j] ← counts.[j] + 1
  ⟦for i in 0 .. m do
     for c in 1 .. counts.[i] do
       yield i⟧
```

In dem Array *counts* halten wir die Häufigkeit der einzelnen Elemente fest. Im Ausgabearray wird jedes Element entsprechend seiner Häufigkeit im Eingabearray wiederholt. Die Laufzeit des Verfahrens, ***Sortieren durch Zählen***, ist proportional zu $\max\{m, n\}$, wobei n die Größe des Eingabearrays ist. Ein Laufzeitgewinn — es sei denn, m ist sehr viel größer als n.

Die Funktion *counting-sort* kombiniert geschickt ***for***-Schleifen mit Arraybeschreibungen, um ein sortiertes Ausgabearray zu erstellen. *Zur Übung:* wie muss das Programm modifiziert werden, um das Eingabearray in situ zu sortieren?

7.3.3. Endrekursion

To iterate is human;
to recurse, divine.
— L Peter Deutsch (1946)

Rekursion ist wie ein Einkaufsbummel von der Wohnung in die Fußgängerzone: Sowohl auf dem Hin- als auch auf dem Rückweg gibt es interessante Aktivitäten. Auf dem Hinweg werden Probleme in immer kleinere Teilprobleme zerteilt; auf dem Rückweg werden Teillösungen zu immer größeren Lösungen kombiniert, siehe Abbildung 5.1. *Iteration* ist in gewissem Sinne Einwegrekursion: Aktivitäten finden nur auf dem Hinweg statt; ist man am Ziel angelangt, wird man zurück ins Heim gebeamt. (Oder umgekehrt: der Hinweg führt ereignislos ans Ziel; nur auf dem Rückweg werden die Besorgungen erledigt.) Die Idee der »Einwegrekursion« wollen wir im Folgenden genauer unter die Lupe nehmen.

In Abschnitt 4.5 haben wir uns mit ähnlichen Themen beschäftigt (Stichworte: Endrekursion, Fortsetzungen, Stack und Heap), dort aus Implementierungssicht, auf der Ebene einer abstrakten Maschine. In diesem und im nächsten Abschnitt machen wir gewissermaßen einen zweiten Durchlauf durch den Themenkomplex, diesmal aus Programmiersicht, auf der Ebene der Programmiersprache. Trotz einer gewissen, durchaus gewollten Redundanz ergänzen sich die Abschnitte: Hier liegt der Fokus auf Programmiertechniken, dort auf Implementierungsdetails, die diese Techniken unterstützen.

Tail Recursion Elimination Betrachten wir noch einmal die Funktion *product*, die die Elemente einer Liste miteinander multipliziert.

```
let rec product = function
  | [ ]      → 1
  | x :: xs → x * product xs
```

Die Definition ist exakt nach dem Struktur Entwurfsmuster für Listen gestrickt: Der Basisfall wird ad hoc gelöst; im Rekursionsschritt wird *product* auf die Restliste angewendet; die erhaltene Teillösung, das Produkt der Restliste, wird durch Multiplikation mit dem Kopfelement zur Gesamtlösung erweitert. Das Rekursionsmuster wird greifbar, wenn man sich eine konkrete Auswertung

anschaut:

$$
\begin{aligned}
& \mathit{product}\ (4 :: 7 :: 11 :: [\,]) \\
= \quad & \{ \text{ Definition von } \mathit{product} \ \} \\
& 4 * \mathit{product}\ (7 :: 11 :: [\,]) \\
= \quad & \{ \text{ Definition von } \mathit{product} \ \} \\
& 4 * (7 * \mathit{product}\ (11 : [\,])) \\
= \quad & \{ \text{ Definition von } \mathit{product} \ \} \\
& 4 * (7 * (11 * \mathit{product}\ [\,])) \\
= \quad & \{ \text{ Definition von } »*« \ \} \\
& 4 * (7 * (11 * 1)) \\
= \quad & \{ \text{ Definition von } »*« \ \} \\
& 4 * (7 * 11) \\
= \quad & \{ \text{ Definition von } »*« \ \} \\
& 4 * 77 \\
= \quad & \{ \text{ Definition von } »*« \ \} \\
& 308
\end{aligned}
$$

Beim rekursiven Abstieg wird ein Turm von Multiplikationen aufgebaut; beim rekursiven Aufstieg wird dieser Turm Schritt für Schritt abgebaut. Die Laufzeit, die »Höhe« der Rechnung, ist linear zur Länge der Liste — was zu erwarten ist. Allerdings ist auch der Speicherbedarf, die »Breite« der Rechnung, linear zur Listenlänge. Sind wir im Basisfall angelangt, hat sich für eine n-elementige Liste ein Turm von n Multiplikationen aufgebaut. Um sich diesen Ausdruck zu merken, wird Speicherplatz benötigt, *zusätzlich* zu dem Platz, den die Liste selbst verschlingt. Das ist ein Problem, wenn der Speicherplatz knapp oder die Liste *sehr* lang ist. Das Ergebnis ist in beiden Fällen das Gleiche: Die Rechnung wird mit einem »Stack Overflow« abgebrochen. (Auf dem Rechner des Dozenten führt der Aufruf $\mathit{product}\ [0\,..\,999999]$ zum besagten Fehlerabbruch.) Kurz zum Hintergrund: Die Buchhaltung von Funktionsaufrufen wird in der Regel stack-artig organisiert. Beim Funktionsaufruf werden die Parameter auf dem ***Rekursionsstack*** abgelegt und nach Abarbeitung des Funktionsrumpfes wieder entfernt. Leider kann der Rekursionsstack nicht in den Himmel wachsen; seine Größe ist beschränkt. Ist die maximale Größe erreicht, wird die Rechnung unvermittelt mit der obigen Fehlermeldung abgebrochen.

Der iterativen Variante von *product* ist dieses Problem nicht zu eigen.

```
let product list =
  let mutable acc = 1
  for x in list do
    acc ← acc * x
  acc
```

Der zusätzlich benötigte Speicherplatz ist konstant: Wir verwenden eine Speicherzelle, *acc*, um uns jeweils das aktuelle Zwischenergebnis zu merken. Die gesamte Arbeit wird sozusagen auf dem Hinweg durch die Liste erledigt; ist das Listenende erreicht, wird das Zwischenergebnis unmittelbar zum Endergebnis.

Um das Verhältnis von Rekursion zu Iteration genauer zu beleuchten, lassen Sie uns die rekursive Definition von *product* so umschreiben, dass ebenfalls die gesamte Arbeit auf dem Hinweg erledigt wird. Zu diesem Zweck spezifizieren wir eine Arbeiterfunktion:

$$\mathit{worker}\ \mathit{acc}\ \mathit{list} = \mathit{acc} * \mathit{product}\ \mathit{list} \tag{7.1}$$

Die Funktion *worker* erledigt zwei Aufgaben auf einmal: Sie bildet das Produkt einer Liste *und* multipliziert zusätzlich das Ergebnis mit ihrem ersten Argument. Die rechte Seite der Spezifikation ähnelt stark dem Rekursionsschritt von *product* — das ist kein Zufall; die zusätzliche Multiplikation ist ja gerade der Speicherplatzverbrecher, den wir eliminieren wollen. Die Spezifikation ist übrigens ein Beispiel für die Programmiertechnik der Verallgemeinerung, des Rekursionsparadoxons. Die noch zu definierende Funktion *worker* verallgemeinert *product*; haben wir eine effiziente Implementierung von *worker* gefunden, programmieren wir:

```
let product list = worker 1 list
```

Um sicherzustellen, dass wir keine Programmierfehler machen, *leiten* wir die Definition von *worker* aus der Spezifikation *her*.

Fall $list = [\,]$**:**

$$
\begin{aligned}
& worker\ a\ [\,] \\
= \quad & \{ \text{ Spezifikation von } worker\ (7.1) \ \} \\
& a * product\ [\,] \\
= \quad & \{ \text{ Definition von } product \ \} \\
& a * 1 \\
= \quad & \{ \text{ 1 ist das neutrale Element von »}*\text{« } \} \\
& a
\end{aligned}
$$

Fall $list = x :: xs$**:**

$$
\begin{aligned}
& worker\ a\ (x :: xs) \\
= \quad & \{ \text{ Spezifikation von } worker\ (7.1) \ \} \\
& a * product\ (x :: xs) \\
= \quad & \{ \text{ Definition von } product \ \} \\
& a * (x * product\ xs) \\
= \quad & \{ \text{ »}*\text{« ist assoziativ } \} \\
& (a * x) * product\ xs \\
= \quad & \{ \text{ Spezifikation von } worker\ (7.1) \ \} \\
& worker\ (a * x)\ xs
\end{aligned}
$$

Fassen wir den ersten und den letzten Ausdruck jeweils zu einer Rechenregel zusammen, erhalten wir das folgende Programm (a haben wir zu *acc* umbenannt).

```
let rec worker acc = function
  | [ ]     → acc
  | x :: xs → worker (acc * x) xs
```

Es ist wichtig festzuhalten, dass die Herleitung algebraische Eigenschaften der Multiplikation verwendet: »∗« ist assoziativ und 1 ist das neutrale Element von »∗«. Die gleiche Herleitung funktioniert somit auch für die Addition, »+« und 0; *nicht* aber für die Subtraktion, »−« und 0. Insbesondere wird deutlich, dass *product* und *worker* nicht die identischen Operationen ausführen:

$$
\begin{aligned}
product\ [a;b;c;d] &= a * (b * (c * (d * 1))) \\
worker\ 1\ [a;b;c;d] &= ((((1 * a) * b) * c) * d)
\end{aligned}
$$

Die Funktion *product* klammert rechtsassoziierend; *worker* 1 hingegen linksassoziierend. Da die Multiplikation assoziativ mit 1 als neutralem Element ist, unterscheiden sich die jeweiligen Ergebnisse trotz der unterschiedlichen Klammerung nicht.

Zurück zur Definition von *worker*: Der Parameter *acc* ist ein sogenannter ***akkumulierender Parameter*** oder kurz ***Akkumulator***; die Funktion *worker* selbst ist ***endrekursiv***. Nach dem rekursiven Aufruf, auf dem Rückweg, ist nichts mehr zu tun, wie die folgende Rechnung zeigt.

```
    worker 1 (4 :: 7 :: 11 :: [ ])
=     { Definition von worker }
    worker 4 (7 :: 11 :: [ ])
=     { Definition von worker }
    worker 28 (11 :: [ ])
=     { Definition von worker }
    worker 308 [ ]
=     { Definition von worker }
    308
```

Die Auswertung illustriert, warum *acc* Akkumulator heißt. Im Gegensatz zum Listenargument wird der erste Parameter nicht kleiner, sondern schwillt mit jedem rekursiven Aufruf an. Das Beispiel macht zudem die Vorteile der endrekursiven Variante deutlich. Ist das Listenende erreicht, wird der Akkumulator unmittelbar als Ergebnis zurückgegeben. Wie bei der iterativen Variante ist der zusätzliche Speicherbedarf konstant; die Rechnung geht nicht in die Breite. Da der rekursive Aufruf die letzte »Aktion« im Funktionsrumpf von *worker* ist, wird der Parameter *acc* nach dem rekursiven Aufruf nicht mehr benötigt; der Speicherplatz kann entsprechend wiederverwendet werden. Ein guter Übersetzer führt die sogenannte ***Tail Recursion Elimination***[6] (TRE) durch: Aus der Rekursion wird eine Schleife; aus dem Parameter wird eine Veränderliche; aus der Änderung des Parameter wird die Zuweisung $acc \leftarrow acc * x$. Kurzum: Das endrekursive Programm wird in das (maschinennähere) iterative Programm umgeschrieben.

```
let product list =
  let rec worker acc = function
    | [ ]     → acc
    | x :: xs → worker (acc * x) xs
  worker 1 list
```

```
let product list =
  let mutable acc = 1
  for x in list do
    acc ← acc * x
  acc
```

Der Effekt ist nachprüfbar: *product* [0 . . 999999] wertet jeweils problemlos zu 0 aus.

Tail Call Optimization Allgemein lassen sich Funktionsaufrufe in ***Endpositionen***, sogenannte ***tail calls***, bezüglich des Speicherverbrauchs optimieren. Dabei wird der Speicherplatz, der von den Funktionsparametern der aufrufenden Funktion belegt wird, bereits *vor* dem Aufruf freigegeben bzw. für den Aufruf wiederverwendet. Der Aufruf von g (bzw. g_1 und g_2) befindet sich in den folgenden Beispielen jeweils an einer Endposition; der Wert des Parameters x wird nach dem Aufruf von g nicht mehr benötigt und somit kann der von x belegte Speicherplatz für den »tail call« wiederverwendet werden.

```
let f x = g e
let f x = if e then g1 e1 else g2 e2
let f x = let p1 = e1 in g e
```

[6] Leider unterstützen nicht alle Programmiersprachen bzw. deren Implementierungen diese wichtige Optimierung.

Im Unterschied dazu befindet sich der Aufruf von g in ***let*** $f\ x = x * g\ e$ *nicht* an einer Endposition; der Parameter x wird nach dem Aufruf von g für die Berechnung des Produkts benötigt.

Die Unterschiede lassen sich an den Auswertungsregeln festmachen.

$$\frac{\delta \vdash e_1 \Downarrow \mathit{true} \qquad \delta \vdash e_2 \Downarrow \nu}{\delta \vdash \mathbf{if}\ e_1\ \mathbf{then}\ e_2\ \mathbf{else}\ e_3 \Downarrow \nu} \qquad \frac{\delta \vdash e_1 \Downarrow \mathit{false} \qquad \delta \vdash e_3 \Downarrow \nu}{\delta \vdash \mathbf{if}\ e_1\ \mathbf{then}\ e_2\ \mathbf{else}\ e_3 \Downarrow \nu}$$

Man sieht, dass das Ergebnis des ***then***- bzw. des ***else***-Zweigs *unverändert* als Ergebnis der gesamten Alternative übernommen wird. Bei der Multiplikation ist das nicht der Fall:

$$\frac{\delta \vdash e_1 \Downarrow n_1 \qquad \delta \vdash e_2 \Downarrow n_2}{\delta \vdash e_1 * e_2 \Downarrow n_1 \cdot n_2}$$

Das Zwischenergebnis n_2 muss noch mit n_1 multipliziert werden (oder umgekehrt).

Tail Calls und nicht-lineare Strukturen Die Umschreibung von *product* in eine endrekursive Form gelingt deshalb so problemlos, weil die zugrundeliegende Datenstruktur linear ist. Betrachten wir statt Listen zum Beispiel Binärbäume, sehen wir uns vor neue Herausforderungen gestellt.

module Effects.Tree

```
let rec product tree =
  match tree with
  | Leaf           → 1
  | Node (l, x, r) → product l * x * product r
```

Die Definition ist exakt nach dem Struktur Entwurfsmuster für Binärbäume gestrickt: Der Basisfall wird ad hoc gelöst; Im Rekursionsschritt wird *product* auf den linken und auf den rechten Teilbaum angewendet; die erhaltenen Teillösungen werden durch Multiplikation mit dem Wurzelelement zur Gesamtlösung erweitert.

Um zu testen, wie robust *product* ist — wann tritt ein Stack Overflow auf? — definieren wir zwei Baumgeneratoren, einen, der linksschiefe, und einen, der rechtsschiefe Binärbäume erzeugt.

```
let left-skewed size (x : 'elem) =
  let rec bottom-up n (tree : Tree ⟨'elem⟩) =
    if n = 0 then tree else bottom-up (n − 1) (Node (tree, x, Leaf))
  bottom-up size Leaf
let right-skewed size (x : 'elem) =
  let rec bottom-up n (tree : Tree ⟨'elem⟩) =
    if n = 0 then tree else bottom-up (n − 1) (Node (Leaf, x, tree))
  bottom-up size Leaf
```

Im Unterschied zu den Definitionen aus Abschnitt 5.3.5 sind die obigen Varianten *endrekursiv*. Die Bäume werden nicht von oben nach unten (»top down«) konstruiert, sondern von unten nach oben (»bottom up«). Warum? Nun, wir müssen vermeiden, dass bereits bei der Generierung eines Testbaums selbst ein Stack Overflow auftritt! Zur Übung: Formulieren Sie die Funktionen iterativ mit Hilfe einer ***for***- oder einer ***while***-Schleife.

Wie zu erwarten, verursacht sowohl der Aufruf *product* (*left-skewed* 1000000 1) als auch *product* (*right-skewed* 1000000 1) einen Stack Overflow. Versuchen wir, die Funktion robuster zu machen. Die Idee des akkumulierenden Parameters führt zu der folgenden Definition.

```
let rec product-acc acc tree =
  match tree with
  | Leaf           → acc
  | Node (l, x, r) → product-acc (product-acc acc l * x) r
```

Leider ist das nur die halbe Miete. Da ein Binärknoten zwei Teilbäume besitzt, benötigen wir zwei rekursive Aufrufe. Da diese irgendwie geschachtelt werden müssen, kann nur ein Aufruf in einer Endposition stehen. Da die Abarbeitung des linken Teilbaums, *product-acc acc l*, kein »tail call« ist, verursacht *product-acc* 1 (*left-skewed* 1000000 1) weiterhin einen Stack Overflow. Immerhin wertet *product-acc* 1 (*right-skewed* 1000000 1) problemlos zu 1 aus.

Wollen wir sämtliche »non-tail calls« eliminieren, müssen wir radikaler ans Werk gehen. Eine vielleicht revolutionäre Idee ist, den impliziten Rekursionsstack (die Ursache der Überläufe) durch einen expliziten Stack, der unter unserer Kontrolle steht, zu ersetzen. Wir repräsentieren den Stack durch eine Liste und spezifizieren:

$$\mathit{product\text{-}acc\text{-}many}\ \mathit{acc}\ \mathit{trees} = \mathit{worker}\ \mathit{acc}\ [\,\textbf{\textit{for}}\ t\ \textbf{\textit{in}}\ \mathit{trees} \rightarrow \mathit{product}\ t\,] \tag{7.2}$$

Die Funktion *product-acc-many* bildet das Produkt einer Liste von Bäumen und multipliziert das Ergebnis zusätzlich mit dem Akkumulator. Aus dieser Spezifikation lässt sich die folgende Implementierung herleiten:

```
let rec product-acc-many acc = function
  | [ ]                 → acc
  | Leaf :: ts          → product-acc-many acc ts
  | Node (l, x, r) :: ts → product-acc-many (acc * x) (l :: r :: ts)
let product tree = product-acc-many 1 [tree]
```

Wenn man möchte, kann man das zweite Argument als *Todo-Liste* lesen. Auf ihr merken wir uns, welche Teilbäume noch bearbeitet werden müssen. Ist die Todo-Liste leer, wird der Akkumulator zurückgegeben. Anderenfalls betrachten wir den ersten Baum. Im Falle eines Blatts arbeiten wir die Restliste ab; im Fall eines Knotens wird der Akkumulator mit dem Wurzelelement multipliziert und die beiden Teilbäume werden zur Todo-Liste hinzugefügt. Dabei wird allerdings die Reihenfolge der Faktoren vertauscht — die Programmtransformation basiert auf der Tatsache, dass die Multiplikation ***kommutativ*** ist, und ist somit für nicht-kommutative Operationen nicht anwendbar, siehe aber Aufgabe 7.3.2. Der Lohn der Mühen: Sowohl der Aufruf *product-acc-many* 1 [*left-skewed* 1000000 1] als auch *product-acc-many* 1 [*right-skewed* 1000000 1] werten klaglos zu 1 aus. Zur Übung: Überführen Sie *product-acc-many* in ein iteratives Programm, das heißt, führen Sie die »tail recursion optimization« von Hand durch.

7.3.4. Fortsetzungen ⋆

Mit Hilfe von akkumulierenden Parametern lassen sich Funktionen wie *length*, *sum*, *product* usw. in eine endrekursive Form bringen. Endrekursive Programme sind vorteilhaft, da sie mit dem Stackspeicher sparsam umgehen und so unerwünschte Stack Overflows verhindern. (Zur Klarstellung: Diese treten nur auf, wenn *sehr* große Datenmengen verarbeitet werden.) Wir haben im letzten Abschnitt gesehen, dass die Transformation in eine endrekursive Form von Eigenschaften der beteiligten Operationen abhängt (z.B. Assoziativität oder Kommutativität) und somit nicht immer angewendet werden kann. In diesem Abschnitt lernen wir eine allgemeine Technik kennen, mit der die Transformation immer gelingt, *ohne* zusätzliche Annahmen machen zu müssen.

Kommen wir noch einmal zu dem Ausgangspunkt unserer Überlegungen zurück.

```
let rec product = function
  | [ ]     → 1
  | x :: xs → x * product xs
```

Das Ziel ist klar: Wir wollen die zusätzliche Arbeit nach dem rekursiven Aufruf vermeiden, die Multiplikation mit *x*. Dazu haben wir im letzten Abschnitt eine Funktion *worker* definiert, die *x*

als zusätzlichen Parameter mit auf den Weg nimmt, siehe (7.1). Aber warum nur *x*? Die Restarbeit ist ja »*x* ∗ «, eine *Multiplikation* mit *x*. Allgemeiner formuliert: *product* wird in einem bestimmten Kontext aufgerufen, *cont* (*product list*), der die Berechnung *fortsetzt* und die Rückgabe von *product* verarbeitet. Die Idee ist nun, diese restliche Arbeit, die sogenannte ***Fortsetzung*** (engl. ***continuation***), der Funktion *worker* mit auf den Weg geben. Wir spezifizieren (*cont* kürzt continuation ab):

$$worker\ list\ cont = cont\ (product\ list) \tag{7.3}$$

Im Normalfall wird *worker* sein Ergebnis *nicht* zurückgeben, sondern als letzte Aktion an die Fortsetzung *cont* weiterreichen. Die Spezifikation ist ein weiteres Beispiel für die Programmiertechnik der Verallgemeinerung, des Rekursionsparadoxons. Wie gewohnt verallgemeinert die noch zu definierende Funktion *worker* die ursprüngliche Funktion *product*; haben wir eine effiziente Implementierung von *worker* gefunden, definieren wir:

$$\textbf{\textit{let}}\ product\ list = worker\ list\ (\textbf{\textit{fun}}\ r \to r)$$

Als initiale Fortsetzung wählen wir die identische Abbildung $\textbf{\textit{fun}}\ r \to r$, auch bekannt unter dem Namen *id*.

Um Programmierfehler zu vermeiden, leiten wir die Definition von *worker* wiederum aus der Spezifikation her.

Fall $list = [\,]$**:**

$$\begin{aligned}
&worker\ [\,]\ c\\
=\quad &\{\ \text{Spezifikation von } worker\ (7.3)\ \}\\
&c\ (product\ [\,])\\
=\quad &\{\ \text{Definition von } product\ \}\\
&c\ 1
\end{aligned}$$

Fall $list = x :: xs$**:**

$$\begin{aligned}
&worker\ (x :: xs)\ c\\
=\quad &\{\ \text{Spezifikation von } worker\ (7.3)\ \}\\
&c\ (product\ (x :: xs))\\
=\quad &\{\ \text{Definition von } product\ \}\\
&c\ (x * product\ xs)\\
=\quad &\{\ \text{Funktionsaufruf}\ \}\\
&(\textbf{\textit{fun}}\ r \to c\ (x * r))\ (product\ xs)\\
=\quad &\{\ \text{Spezifikation von } worker\ (7.3)\ \}\\
&worker\ xs\ (\textbf{\textit{fun}}\ r \to c\ (x * r))
\end{aligned}$$

Im vorletzten Schritt wird der Kontext von *product xs* in eine Funktion überführt. Also, aus $c\ (x * product\ xs)$ wird $c\ (x * \bullet)$, ein Ausdruck mit einem Platzhalter oder einem Loch; aus diesem wird die Funktion $\textbf{\textit{fun}}\ r \to c\ (x * r)$.

Fassen wir den ersten und den letzten Ausdruck jeweils zu einer Rechenregel zusammen, erhalten wir das folgende Programm (*c* haben wir zu *cont* umbenannt).

```
let rec worker xs cont =
  match xs with
  | [ ]     → cont 1
  | x :: xs → worker xs (fun r → cont (x * r))
```

Die Funktion *worker* ist wie gewünscht endrekursiv. Bei der Herleitung haben wir keinerlei Annahmen gemacht, keine Eigenschaften der beteiligten Operationen ausgenutzt.

Schauen wir uns ein Beispiel für eine Auswertung an.

$$
\begin{aligned}
& \mathit{worker}\ (4 :: 7 :: 11 :: [\,])\ (\textbf{\textit{fun}}\ r_1 \to r_1) \\
= \quad & \{\ \text{Definition von } \mathit{worker}\ \} \\
& \mathit{worker}\ (7 :: 11 :: [\,])\ (\textbf{\textit{fun}}\ r_2 \to (\textbf{\textit{fun}}\ r_1 \to r_1)\ (4 * r_2)) \\
= \quad & \{\ \text{Definition von } \mathit{worker}\ \} \\
& \mathit{worker}\ (11 :: [\,])\ (\textbf{\textit{fun}}\ r_3 \to (\textbf{\textit{fun}}\ r_2 \to (\textbf{\textit{fun}}\ r_1 \to r_1)\ (4 * r_2))\ (7 * r_3)) \\
= \quad & \{\ \text{Definition von } \mathit{worker}\ \} \\
& \mathit{worker}\ [\,]\ (\textbf{\textit{fun}}\ r_4 \to (\textbf{\textit{fun}}\ r_3 \to (\textbf{\textit{fun}}\ r_2 \to (\textbf{\textit{fun}}\ r_1 \to r_1)\ (4 * r_2))\ (7 * r_3))\ (11 * r_4)) \\
= \quad & \{\ \text{Definition von } \mathit{worker}\ \} \\
& (\textbf{\textit{fun}}\ r_4 \to (\textbf{\textit{fun}}\ r_3 \to (\textbf{\textit{fun}}\ r_2 \to (\textbf{\textit{fun}}\ r_1 \to r_1)\ (4 * r_2))\ (7 * r_3))\ (11 * r_4))\ 1 \\
= \quad & \{\ \text{Funktionsaufruf}\ \} \\
& (\textbf{\textit{fun}}\ r_3 \to (\textbf{\textit{fun}}\ r_2 \to (\textbf{\textit{fun}}\ r_1 \to r_1)\ (4 * r_2))\ (7 * r_3))\ 11 \\
= \quad & \{\ \text{Funktionsaufruf}\ \} \\
& (\textbf{\textit{fun}}\ r_2 \to (\textbf{\textit{fun}}\ r_1 \to r_1)\ (4 * r_2))\ 77 \\
= \quad & \{\ \text{Funktionsaufruf}\ \} \\
& (\textbf{\textit{fun}}\ r_1 \to r_1)\ 308 \\
= \quad & \{\ \text{Funktionsaufruf}\ \} \\
& 308
\end{aligned}
$$

Man sieht sehr schön die endrekursive Natur von *worker*: Ein Aufruf wird durch den nächsten ersetzt. Ebenso deutlich wird, dass die Rechnung in die Breite geht: Die jeweiligen Fortsetzungen, Multiplikation mit 4, Multiplikation mit 7, Multiplikation mit 11, werden im zweiten Parameter protokolliert. Es entsteht ein Turm von Fortsetzungen, ineinandergeschachtelte Funktionsausdrücke. Trotzdem werden auch größere Listen klaglos ausmultipliziert: Der Aufruf $\mathit{worker}\ [0\,..\,999999]\ (\textbf{\textit{fun}}\ r \to r)$ ergibt wie gewünscht 0.

Warum tritt kein Stack Overflow auf? Wie bereits angedeutet, wird eine stack-artige Organisation für die Verwaltung von Parametern bei (geschachtelten) Funktionsaufrufen eingesetzt. Die tatsächlichen Daten, auf die die Parameter verweisen, also natürliche Zahlen (!), Paare, Records, Listen, Bäume und eben auch Funktionsabschlüsse, müssen in der Regel Funktionsaufrufe überleben. Sie werden dauerhaft gespeichert, solange bis sie tatsächlich nicht mehr benötigt werden. Der zu diesem Zweck verwendete Speicherbereich heißt im Fachjargon ***Heap*** (engl. für Haufen) und enthält recht wörtlich einen ungeordneten Haufen von Daten. Die Größe des Heaps ist in der Regel nur durch die tatsächliche Speicherkapazität des Rechners begrenzt. Wird der Speicherplatz auf dem Heap knapp, identifiziert der ***Garbage collector*** nicht mehr benötigte Daten und »recycelt« den belegten Speicherplatz.

Jetzt da wir zwei endrekursive Varianten von *product* implementiert haben, eine, die einen akkumulierenden Parameter verwendet, und eine, die auf Fortsetzungen basiert, stellt sich natürlich die Frage, wie sich die beiden Varianten im Vergleich schlagen? Das Anlegen von Funktionsabschlüssen ist mit Aufwand verbunden, Aufwand, den man spüren bzw. hören kann: Der Aufruf $\mathit{worker}\ [0\,..\,999999]\ (\textbf{\textit{fun}}\ r \to r)$ ist ungleich langsamer als der korrespondierende Aufruf $\mathit{worker}\ 1\ [0\,..\,999999]$ aus Abschnitt 7.3.3. Die akkumulierende Variante verarbeitet jedes Listenelement in einem Zug: Der Akkumulator wird mit dem Element multipliziert. Die fortsetzungsbasierte Variante arbeitet zweischrittig: Eine Fortsetzung wird angelegt, die dann zu einem

späteren Zeitpunkt abgearbeitet wird. Die Ausnutzung algebraischer Eigenschaften ist also segensreich.

Die Stärke des fortsetzungsbasierten Ansatzes liegt in seiner Allgemeinheit: Mit dem gleichen Ansatz können wir auch einen Binärbaum endrekursiv ausmultiplizieren. Im Fall von Listen legen wir eine Fortsetzung an; im Fall von Binärbäumen haben wir entsprechend zwei Fortsetzungen.


```
let rec product-cont tree cont =
  match tree with
  | Leaf          → cont 1
  | Node (l, x, r) → product-cont l (fun pl →
                     product-cont r (fun pr →
                     cont (pl ∗ x ∗ pr)))
```

Der linke Teilbaum wird ausmultipliziert; das Ergebnis wird an die erste Fortsetzung weitergereicht (*fun pl* → …); dann wird der rechte Teilbaum ausmultipliziert; das Ergebnis wird an die zweite Fortsetzung weitergereicht (*fun pr* → …); die Ergebnisse werden multipliziert und an die ursprüngliche Fortsetzung (*cont*) übergeben. Insgesamt ergibt sich das Bild einer Kollekte: Um Geld zu sammeln, wird ein Korb herumgereicht; jeder fügt ein paar Münzen hinzu und reicht den Korb an den Nachbarn (die Fortsetzung) weiter. Der Lohn der Mühen: Weder das Produkt linksschiefer Bäume *product-cont* (*left-skewed* 1000000 1) (*fun n* → *n*) noch das rechtsschiefer Bäume *product-cont* (*right-skewed* 1000000 1) (*fun n* → *n*) bereiten Probleme.

Beide Programmiertechniken, Akkumulatoren und Fortsetzungen, lassen sich auch mit Gewinn kombinieren:

```
let rec product-acc-cont acc tree cont =
  match tree with
  | Leaf          → cont acc
  | Node (l, x, r) → product-acc-cont acc l (fun pl →
                     product-acc-cont (pl ∗ x) r cont)
```

Die Zahlen in den linken Teilbäumen werden akkumuliert; für die rechten Teilbäume werden Fortsetzungen angelegt. Zur Übung: Wenn Sie mögen, überführen Sie die endrekursive Funktion *product-acc-cont* in eine iterative Form.

Die Technik der Fortsetzungen (engl. ***continuation passing style***, kurz CPS) haben wir übrigens bereits bei der Implementierung von Parsern in Abschnitt 6.5.3 eingesetzt: Der Folgeakzeptor entspricht gerade einer Fortsetzung, die die syntaktische Analyse fortsetzt.

Übungen.

1. Ein Sortierverfahren heißt ***stabil***, wenn es die relative Reihenfolge von äquivalenten Elementen nicht verändert, siehe Aufgabe 5.1.2. Zeigen Sie, dass die imperativen Varianten von Sortieren durch Einfügen und Sortieren durch Auswählen aus Abschnitt 7.3.2 stabil sind.

2. Die Funktion *product* berechnet das »Produkt« der Elemente eines Binärbaums.

```
let rec product = function
  | Leaf          → e
  | Node (l, x, r) → product l ⊗ x ⊗ product r
```

Von der Operation ⊗ wissen wir lediglich, dass sie assoziativ mit *e* als neutralem Element ist. (Insbesondere dürfen wir nicht annehmen, dass ⊗ kommutativ ist.) Programmieren Sie eine endrekursive Variante von *product*. *Hinweis:* Eine Idee ist, die in Abschnitt 7.3.3 eingeführte Metapher der Todo-Liste konsequent weiterzuverfolgen, indem man erlaubt, verschiedene »Items« auf die Todo-Liste zu setzen.

```
type Item =
  | Mul of Nat
  | Sub of Tree⟨Nat⟩
type Todo =
  Item list
```

Orientieren Sie sich bei der Lösung der Aufgabe an der Funktion *product-acc-many*.

3. Definieren Sie die Funktionen,

```
foreach-list  (list  : List ⟨'elem⟩  ) (body : 'elem → Unit) : Unit
foreach-array (array : Array ⟨'elem⟩) (body : 'elem → Unit) : Unit
```

die über eine Liste bzw. ein Array iterieren, mit den Mitteln aus Kapitel 3 und 4. Übersetzen Sie die Schleifen *for x in list do e* und *for x in array do e* in Aufrufe dieser Funktionen.

7.4. Ausnahmen

Nicht jede Rechnung lässt sich einem erfolgreichen Ende zuführen: Treffen wir im Laufe einer Rechnung auf den Teilausdruck $2 \div 0$, dann bleibt uns nichts anderes übrig, als mit den Schultern zu zucken und aufzugeben. Die dynamische Semantik äußert sich bis dato nicht zu dieser Situation — wie wir in Abschnitt 3.1 angemerkt haben, ist die Auswertungsregel für »÷« schlicht und einfach nicht anwendbar. Es ist klar, dass wir die Teilrechnung an dieser Stelle nicht weiterführen können, daraus folgt aber nicht notwendigerweise, dass wir damit auch die Gesamtrechnung abbrechen müssen. Ganz im Gegenteil: Der Divisor könnte aus einer interaktiven Eingabe resultieren; das Programm sollte dann den/die Benutzer/-in auf den Fehler hinweisen und sich nicht klang- und sanglos verabschieden. Nun ist Division durch Null nicht die einzige Ausnahmesituation: Eine Fallunterscheidung kann unvollständig sein, ein Arrayzugriff kann außerhalb der Arraygrenzen liegen usw. Da viele Dinge während einer Rechnung schieflaufen können, liegt es nahe, einen allgemeinen Mechanismus einzuführen, um Ausnahmesituationen zu signalisieren, Rechnungen abzubrechen und an anderer Stelle wieder aufzunehmen.

Eine Rechnung wird abgebrochen, indem eine sogenannte ***Ausnahme*** (engl. exception) ausgelöst wird. Die ausgelöste Ausnahme kann an einer anderen Stelle behandelt werden; an dieser anderen Stelle wird die Rechnung dann fortgesetzt. Etwas bildlicher spricht man auch davon, dass eine Ausnahme *geworfen* und *gefangen* wird. Die Divisionsoperation wirft zum Beispiel die Ausnahme *Div*, wenn der Divisor Null ist.

```
⋙ 815 ÷ (4711 - 7 * 673) + 1
uncaught exception: Div
```

Da die Ausnahme nicht gefangen wird, trifft der Wurf auf die Benutzungsoberfläche und führt zu einer Fehlermeldung. Eine Ausnahme kann auch explizit mit ***raise*** geworfen werden. Der nachfolgende Ausdruck hat somit den gleichen Effekt wie der obige.

```
⋙ raise Div + 1
uncaught exception: Div
```

Da die Rechnung abgebrochen wird, besitzt der Ausdruck *raise Div* + 1 *keinen* Wert, sondern hat nur einen Effekt.

Eine geworfene Ausnahme kann mit dem ***try***-Konstrukt gefangen werden.

```
⋙ try show (815 ÷ (4711 - 7 * 673) + 1) with | Div → "oops"
"oops"
⋙ try show (815 ÷ (4711 - 6 * 773) + 1) with | Div → "oops"
"12"
```

Zwischen den Schlüsselwörtern ***try*** und ***with*** steht der auszurechnende Ausdruck. Gelingt dessen Auswertung, so ist der berechnete Wert auch der Wert des gesamten Ausdrucks. Wird hingegen während der Auswertung eine Ausnahme geworfen, dann kommt der Teil nach dem Schlüsselwort ***with*** zum Einsatz. Dieser entspricht dem Rumpf einer erweiterten Fallunterscheidung mit ***match***. Passt die Ausnahme auf die linke Seite einer Regel, so wird mit der Auswertung der rechten Seite fortgefahren. Passt kein Muster, so wird die Ausnahme weitergeworfen.

```
⋙ try show (815 ÷ (4711 − 7 ∗ 673) + 1) with | Match → "oops"
uncaught exception : Div
```

Die Ausnahme *Div* passt nicht auf das Muster *Match*, so dass *Div* weitergeworfen wird. Ausnahmen sind normale Werte, Elemente des Typs *Exception* (Kurzform: *exn*), und können wie Elemente eines Variantentyps verwendet werden.

```
⋙ let exns = (Div, Match)
val exns : Exception ∗ Exception
⋙ match snd exns with | Div → "div" | Match → "match"
"match"
```

Zunächst wird ein Paar von Ausnahmen konstruiert; anschließend wird die zweite Komponente mit einer Fallunterscheidung analysiert.

Die Ausnahme *Match* signalisiert übrigens, dass eine Fallunterscheidung fehlgeschlagen ist, dass keines der angegebenen Muster auf den analysierten Wert gepasst hat. Unvollständige Fallunterscheidungen sollten zwar so weit wie möglich vermieden werden, aber manchmal lässt sich nicht jeder Fall behandeln — zumindest auf den ersten Blick.

```
let head (list : List ⟨'elem⟩) : 'elem =
  match list with
  | x :: _ → x
```

Die Funktion *head* bestimmt das erste Element einer Liste; *head* ist somit eine ***partielle Funktion***: Der Aufruf *head e* wirft die Ausnahme *Match*, wenn *e* zur leeren Liste auswertet.

```
⋙ head (head ([ ] :: [4711] :: [ ]))
uncaught exception : Match
⋙ try head (head ([ ] :: [4711] :: [ ])) with | Match → 0
0
```

Eine *Match* Ausnahme ist nicht sehr spezifisch; sie drückt aus, dass irgendwo im Programm eine Fallunterscheidung fehlgeschlagen ist. Nun kann ein Programm viele Fallunterscheidungen verwenden. Dass eine Fallunterscheidung nicht alle Fälle abdeckt, kann gewollt sein, kann aber auch auf einen ***Programmierfehler*** (engl. ***bug***) hindeuten. Aus diesem Grund sollte man Fallunterscheidungen vervollständigen und eventuelle Fehlerfälle explizit machen, zum Beispiel, mit einer maßgeschneiderten Ausnahme.

```
exception Head
let head (list : List ⟨'elem⟩) : 'elem =
  match list with
  | [ ]    → raise Head
  | x :: _ → x
```

Die Deklaration ***exception*** führt eine neue Ausnahme ein; der Datentyp *Exception* wird auf diese Weise um ein Element erweitert. Die neue Ausnahme wird geworfen, wenn *head* mit der leeren

Liste aufgerufen wird; der Programmtext dokumentiert auf diese Weise, dass *head* diesen Fall nicht behandeln kann (oder will).

Ausnahmen wie *Div* und *Head* können wie Konstruktoren verwendet werden. Wie Konstruktoren können Ausnahmen auch ein Argument haben, zum Beispiel um Informationen vom Ort des Abbruchs zum Ort der Wiederaufnahme zu transportieren. Die folgende Reimplementierung des Bankkontos illustriert diese Möglichkeit.

module Effects.Bank

```
exception Insufficient of Nat
module Junior-Account =
  let private min-funds = 10
  let private funds     = ref 0
  let deposit (amount : Nat) =
      funds := !funds + amount
  let withdraw (amount : Nat) =
    if !funds – amount ⩾ min-funds then
      funds := !funds – amount
    else
      raise (Insufficient (!funds – min-funds))
  let balance () =
      !funds
```

Die Funktion *withdraw* ist abgeändert worden: Der gewünschte Betrag wird nur abgebucht, wenn das Konto gedeckt ist — ein Betrag von 10 € muss auf dem Konto verbleiben. Anderenfalls wird die Ausnahme *Insufficient n* geworfen, wobei *n* der Betrag ist, der höchstens abgehoben werden kann. Das ursprüngliche Verhalten von *withdraw* — soviel abheben wie möglich — lässt sich nachprogrammieren, indem man die geworfene Ausnahme fängt und dann das Konto leerräumt.

```
let maximal-withdraw (amount : Nat) : Nat =
  try
    Junior-Account.withdraw amount; amount
  with
  | Insufficient rest → Junior-Account.withdraw rest; rest
```

7.4.1. Abstrakte Syntax

Wir erweitern Deklarationen um Ausnahmedeklarationen und Ausdrücke um Konstrukte zum Werfen und Fangen von Ausnahmen.

$d ::= \cdots$	***Deklarationen:***
$\mid$ ***exception*** C ***of*** t	Deklaration einer Ausnahme

Wird bei einer ***exception*** Deklaration kein Typargument angegeben, dann fassen wir das, wie bei »normalen« Konstruktoren, als Abkürzung für C ***of*** *Unit* auf.

$e ::= \cdots$	***Ausnahmebehandlung:***
$\mid$ ***raise*** e	Werfen einer Ausnahme
$\mid$ ***try*** e ***with*** m	Fangen einer Ausnahme

Syntaktisch entspricht ***try*** e ***with*** m einer erweiterten Fallunterscheidung mit ***match***: e ist ein Ausdruck und m eine Folge von Regeln der Form $p \to e$, siehe Abschnitt 4.2.3.

7.4.2. Statische Semantik

Ausnahmen haben den Typ *Exception*.

$t ::= \cdots$	***Typen:***
$\mid$ *Exception*	Typ der Ausnahmen

Der Typ entspricht im Wesentlichen einem Variantentyp mit dem Unterschied, dass die Konstruktoren nicht auf einen Schlag, sondern peu à peu mit Hilfe von ***exception*** Deklarationen eingeführt werden.

Die Ausnahmedeklaration ***exception*** C ***of*** t wird ähnlich wie eine Variantentypdeklaration gehandhabt: Der Ausnahmekonstruktor korrespondiert zu einer Funktion des Typs $t \to$ *Exception*. Wir erlauben es *nicht*, Ausnahmekonstruktoren zu redefinieren oder lokal zu definieren — aus den gleichen Gründen, die die Redefinition von Record- und Variantentypen verbieten, siehe Abschnitt 4.1.

$$\frac{\Sigma \vdash e : \textit{Exception}}{\Sigma \vdash \textbf{\textit{raise}}\ e : t}$$

Das Argument von ***raise*** muss ein Ausdruck sein, der zu einer Ausnahme auswertet; ***raise*** e selbst hat einen beliebigen Typ! Mit anderen Worten, ***raise*** e kann überall verwendet werden, als Boolescher Wert (***raise*** *Div* && e), als natürliche Zahl (***raise*** *Div* + 4711), als Funktion ((***raise*** *Div*) 4711), als Paar (*snd* (***raise*** *Div*)) usw. Warum? Nun, ***raise*** e bricht die aktuelle Rechnung ab, deswegen kann der Ausdruck in jedem beliebigen Kontext stehen; der Kontext bekommt den Wert von ***raise*** e ja niemals zu Gesicht.

$$\frac{\Sigma \vdash e : t \qquad \Sigma \vdash \textit{Exception}\ \textbf{\textit{with}}\ m : t}{\Sigma \vdash \textbf{\textit{try}}\ e\ \textbf{\textit{with}}\ m : t}$$

Der Rumpf des ***try***-Ausdrucks muss, angewendet auf eine Ausnahme, zu einem Element des Typs t auswerten, wobei t der Typ des Ausdrucks ist, der »ausprobiert« wird.

7.4.3. Dynamische Semantik

Wie auch in den letzten beiden Abschnitten müssen wir die Auswertungsregeln abändern. Dies führt uns zunächst zu der Frage, zu welchem Wert zum Beispiel der Ausdruck ***raise*** *Div* auswertet. Der Ausdruck hat sicherlich keinen »normalen« Wert; er wirft ja die Ausnahme *Div*. Diese Ausnahme können wir als »außergewöhnlichen« Wert des Ausdrucks ansehen. Mit der Einführung von Ausnahmen kann die Auswertung eines Ausdrucks zwei mögliche Resultate produzieren: normale Werte und Ausnahmen. Um im Bilde zu bleiben, nennt man die geworfenen Ausnahmen auch ***Pakete***.

$r \in \mathsf{Result} ::=$	***Resultate***
$\mid \nu$	Wert
$\mid \boxed{\nu}$	Paket

Das Kästchen $\boxed{\nu}$ soll verdeutlichen, dass es sich um ein Paket handelt. Der Inhalt des Pakets, zum Beispiel *Div* oder *Insufficient* 4711, ist ein normaler Wert — statisch gesehen ein Element des Typs *Exception*. Die Auswertungsrelation $\delta \vdash e \Downarrow \nu$ wird nun abgeändert zu

$$\delta \vdash e \Downarrow r$$

um der Tatsache Rechnung zu tragen, dass eine Auswertung zwei mögliche Resultate haben kann. Das ist die dritte und letzte Änderung der Auswertungsrelation. Wenn wir es genau nehmen, müssten wir natürlich die geänderte Relation ändern: Aus der Formel $\delta \vdash e \Downarrow_t \nu$ wird

$$\delta \vdash e \Downarrow_t r$$

bzw. eigentlich müssten wir die geänderte geänderte Relation ändern: Aus $\delta \vdash \sigma \parallel e \Downarrow_t \nu \parallel \sigma'$ wird die sechsstellige Relation

$$\delta \vdash \sigma \parallel e \Downarrow_t r \parallel \sigma'$$

Glücklicherweise kommen sich die jeweiligen Erweiterungen, Ein- und Ausgabe, Zustand und Ausnahmen, nicht allzu sehr ins Gehege, so dass wir jede Erweiterung separat betrachten können und dies aus Gründen der Lesbarkeit auch tun.

Kommen wir zu den Auswertungsregeln: Für das Werfen einer Ausnahme mit ***raise*** gibt — vielleicht überraschend — zwei Regeln.

$$\frac{\delta \vdash e \Downarrow \nu}{\delta \vdash \textbf{\textit{raise}}\ e \Downarrow \boxed{\nu}} \qquad \frac{\delta \vdash e \Downarrow \boxed{\nu}}{\delta \vdash \textbf{\textit{raise}}\ e \Downarrow \boxed{\nu}}$$

Wie immer wird zunächst das Argument ausgewertet. Die Auswertung von e kann zwei mögliche Ergebnisse haben: einen Wert oder ein Paket. Wenn e zu dem Wert ν auswertet, schnürt ***raise*** daraus ein Paket $\boxed{\nu}$ und wirft es. Wenn bei der Auswertung von e aber bereits ein Paket geworfen wird, so wirft ***raise*** dieses Paket weiter. (Werte werden niemals doppelt verpackt: Ein Ergebnis der Form $\boxed{\nu}$ gibt es *nicht*.) Zwei künstlich konstruierte Beispiele für den letzten Fall sind ***raise*** (***raise*** *Div*) oder ***raise*** (***raise*** *Div*; *Match*). Beide Ausdrücke sind äquivalent zu ***raise*** *Div*.

$$\frac{\dfrac{\varnothing \vdash \mathit{Div} \Downarrow \mathit{Div}}{\varnothing \vdash \textbf{\textit{raise}}\ \mathit{Div} \Downarrow \boxed{\mathit{Div}}}}{\varnothing \vdash \textbf{\textit{raise}}\ (\textbf{\textit{raise}}\ \mathit{Div}) \Downarrow \boxed{\mathit{Div}}}$$

Sie sind äquivalent, weil beide bzw. alle drei Ausdrücke das gleiche Ergebnis liefern.

Kommen wir zum Fangen von Paketen.

$$\frac{\delta \vdash e \Downarrow \nu}{\delta \vdash \textbf{\textit{try}}\ e\ \textbf{\textit{with}}\ m \Downarrow \nu}$$

$$\frac{\delta \vdash e \Downarrow \boxed{\nu} \qquad \delta \vdash \nu\ \textbf{\textit{with}}\ m \Downarrow r}{\delta \vdash \textbf{\textit{try}}\ e\ \textbf{\textit{with}}\ m \Downarrow r} \qquad \frac{\delta \vdash e \Downarrow \boxed{\nu} \qquad \delta \vdash \nu\ \textbf{\textit{with}}\ m \Downarrow \lightning}{\delta \vdash \textbf{\textit{try}}\ e\ \textbf{\textit{with}}\ m \Downarrow \boxed{\nu}}$$

Zunächst wird e ausgewertet (»die Auswertung wird versucht«); resultiert die Auswertung in einem Wert, so ist dieser auch der Wert des gesamten Ausdrucks (»der Versuch ist erfolgreich«). Wird bei der Auswertung das Paket $\boxed{\nu}$ geworfen (»die Auswertung im bisherigen Sinne misslingt«), so fängt ***try*** das Paket auf und packt es aus. Jetzt sind zwei bzw. eigentlich sogar drei Fälle denkbar: ν passt auf die linke Seite einer der in m aufgeführten Regeln, dann wird die entsprechende rechte Seite ausgerechnet. Das Ergebnis dieser Rechnung ist auch das Ergebnis des gesamten Ausdrucks — das schließt ausdrücklich Ausnahmen ein, die bei der Abarbeitung geworfen werden. Passt ν hingegen nicht auf eine der aufgeführten Regeln, ν ***with*** $m \Downarrow \lightning$, dann wird das Paket weitergeworfen. Es gibt also insgesamt vier unterschiedliche Konstellationen:

try 4711	***with*** | *Div*	→ 815	⇓ 4711
try 4711 ÷ 0	***with*** | *Div*	→ 815	⇓ 815
try 4711 ÷ 0	***with*** | *Div*	→ ***raise*** *Match*	⇓ $\boxed{\mathit{Match}}$
try 4711 ÷ 0	***with*** | *Match*	→ 815	⇓ $\boxed{\mathit{Div}}$

Im ersten Beispiel wertet der von ***try*** und ***with*** eingeschlossene Ausdruck zu einem Wert aus; in den anderen drei Beispielen wird eine Ausnahme geworfen. Diese Ausnahme wird im zweiten

und dritten Beispiel abgefangen, im vierten nicht. Die Behandlung der Ausnahme führt im zweiten Beispiel zu einem Wert, im dritten Beispiel wird eine Ausnahme geworfen.

Wie in den Abschnitten 7.1 und 7.2 müssen wir auch in diesem Abschnitt die bisher aufgestellten Auswertungsregeln anpassen. Aber nicht nur das, jetzt haben wir endlich die Mittel in der Hand, um die fehlenden Auswertungsregeln nachzutragen. Erinnern wir uns: Wir haben Ausnahmen insbesondere eingeführt, um die Semantik von Ausdrücken wie $1 \div 0$, ***match*** [ ] ***with*** $x :: xs \to 4711$ oder $[\![1;2]\!].[4711]$ festlegen zu können. Fangen wir mit den arithmetischen Operationen an.

$$\frac{\delta \vdash e_2 \Downarrow 0}{\delta \vdash e_1 \div e_2 \Downarrow \boxed{\mathit{Div}}} \qquad \frac{\delta \vdash e_2 \Downarrow 0}{\delta \vdash e_1 \,\%\, e_2 \Downarrow \boxed{\mathit{Mod}}}$$

Wertet der Divisor zu 0 aus, wird eine entsprechende Ausnahme geworfen.

$$\frac{\delta \vdash e \Downarrow \nu \qquad \delta \vdash \nu \;\mathbf{with}\; m \Downarrow \lightning}{\delta \vdash \mathbf{match}\; e \;\mathbf{with}\; m \Downarrow \boxed{\mathit{Match}}}$$

Passt keine der Regeln auf den Wert des Diskriminatorausdrucks, wird eine *Match* Ausnahme geworfen.

$$\frac{\delta \vdash e_1 \Downarrow s \qquad \delta \vdash e_2 \Downarrow i}{\delta \vdash e_1.[e_2] \Downarrow \boxed{\mathit{Subscript}}} \quad i \notin \mathit{dom}\; s$$

Ist der Index i nicht im Definitionsbereich des Arrays, dann wird eine *Subscript* Ausnahme geworfen. Die folgenden Ausnahmen sind vordefiniert:[7]

exception *Div*
exception *Mod*
exception *Match*
exception *Subscript*

Kommen wir auf die Änderungen an den bestehenden Regeln zu sprechen, zunächst exemplarisch an der Paarbildung. Die folgenden beiden Regeln kommen zu der ursprünglichen *hinzu*:

$$\frac{\delta \vdash e_1 \Downarrow \boxed{\nu}}{\delta \vdash (e_1, e_2) \Downarrow \boxed{\nu}} \qquad \frac{\delta \vdash e_1 \Downarrow \nu_1 \qquad \delta \vdash e_2 \Downarrow \boxed{\nu}}{\delta \vdash (e_1, e_2) \Downarrow \boxed{\nu}}$$

Die Rechnung wird abgebrochen, wenn eine der beiden Komponenten eine Ausnahme wirft. Diese Ausnahme ist auch das Ergebnis des Paarausdrucks. Im Allgemeinen müssen wir für eine Regel mit n Voraussetzungen n zusätzliche Regeln angeben. Die Regel

$$\frac{\delta_1 \vdash e_1 \Downarrow \nu_1 \qquad \delta_2 \vdash e_2 \Downarrow \nu_2 \qquad \cdots \qquad \delta_n \vdash e_n \Downarrow \nu_n}{\delta \vdash e \Downarrow \nu}$$

wird um die folgenden n Regeln *ergänzt*:

$$\frac{\delta_1 \vdash e_1 \Downarrow \boxed{\nu}}{\delta \vdash e \Downarrow \boxed{\nu}}$$

[7] Dichtung und Wahrheit: In F# wird bei einem ungültigen Arrayzugriff tatsächlich die Ausnahme *IndexOutOfRangeException* geworfen. Diese Ausnahme ist ein sogenanntes Objekt, eine Instanz der gleichnamigen Klasse *IndexOutOfRangeException*, einem Untertyp von *Exception*, siehe Kapitel 8. Möchte man diese Ausnahme behandeln, schreibt man tatsächlich statt … ***with*** | *Subscript* → *e* etwas länglicher … ***with*** | :? *System.IndexOutOfRangeException* → *e*. Auch *Match* hat einen etwas längeren Namen, *Microsoft.FSharp.Core.MatchFailureException*, und erwartet in Wirklichkeit drei Argumente.

$$\frac{\delta_1 \vdash e_1 \Downarrow \nu_1 \qquad \delta_2 \vdash e_2 \Downarrow \boxed{\nu}}{\delta \vdash e \Downarrow \boxed{\nu}}$$

$$\vdots$$

$$\frac{\delta_1 \vdash e_1 \Downarrow \nu_1 \qquad \delta_2 \vdash e_2 \Downarrow \nu_2 \qquad \cdots \qquad \delta_n \vdash e_n \Downarrow \boxed{\nu}}{\delta \vdash e \Downarrow \boxed{\nu}}$$

Jeder Teilausdruck kann eine Ausnahme werfen, die dann auch das Ergebnis der Rechnung darstellt. Auf diese Weise wird eine Ausnahme bis zum nächsten umgebenden ***try***-Ausdruck propagiert. Dabei können beliebig viele Teilrechnungen abgebrochen werden, etwa wenn der Wurf einer Ausnahme in einer rekursiven Funktion erfolgt.

7.4.4. Vertiefung

Panik Nicht immer lässt sich eine abgebrochene Rechnung sinnvoll weiterführen; manchmal ist sie schlicht und einfach Symptom eines Programmierfehlers. Unter anderem für die Dokumentation dieser »unmöglichen Fälle« ist die in Mini-F# vordefinierte Ausnahme *Panic* gedacht.

```
exception Panic of String
let panic (message : String) : 'a =
  raise (Panic message)
```

Die Funktion *panic* hat den Ergebnistyp *'a* und zeigt damit an, dass sie keinen Wert zurückgibt. (Ein Ausdruck vom Typ *'a* kann in jedem Kontext verwendet werden, etwa als natürliche Zahl oder als Wahrheitswert.)

Wenn man möchte, kann man *Panic* Ausnahmen abfangen — am besten mit einem ***try***-Ausdruck um das Hauptprogramm — und dem/der Benutzer/-in mit der Bitte um einen Fehlerbericht präsentieren.

```
try
  ...
with
| Panic msg →
  putline ("panic! (the 'impossible' happened)\n" ^ msg ^
           "\nPlease report it as a bug to support@harry-hacker.org.")
```

module Effects.Product

Ausnahmen als Kontrollstruktur Der Begriff Ausnahme suggeriert, dass die Konstrukte ***raise*** und ***try*** nur in Ausnahmesituationen verwendet werden sollten. Das ist zwar prinzipiell nicht ganz falsch, schöpft aber das Potential der Konstrukte nicht aus. Wir können ***raise*** und ***try*** auch gezielt einsetzen, um die Auswertung zu steuern. Nehmen wir an, wir wollen das Produkt einer Liste von Zahlen bestimmen. Mit dem Struktur Entwurfsmuster erhalten wir die folgende, uns wohlbekannte Definition.

```
let rec product (list : List ⟨Nat⟩) : Nat =
  match list with
    | [ ]      → 1
    | n :: ns → n * product ns
```

Hat die Eingabeliste die Länge n, so werden n Produkte berechnet, unabhängig vom Wert der Listenelemente. Enthält die Liste irgendwo eine Null, dann wird viel unnötige Arbeit verrichtet. Die folgende Implementierung vermeidet diese Arbeit: Die Funktion *product* terminiert unmittelbar mit dem Ergebnis 0, sobald sie auf eine 0 trifft.

```
exception Zero
let product (list : List ⟨Nat⟩) : Nat =
  try
    let rec worker = function
      | [ ]      → 1
      | n :: ns → if n = 0 then raise Zero else n * worker ns
    in worker list
  with
  | Zero → 0
```

Wenn im Rumpf der Hilfsfunktion *worker* die Ausnahme *Zero* geworfen wird, werden sämtliche rekursiven Aufrufe abgebrochen und es wird mit der rechten Seite der Regel *Zero* → 0 weitergerechnet. Wir springen sozusagen aus der Rekursion heraus.

Eingabe mit Validierung, da capo Themenwechsel: Mit Hilfe von Ausnahmen können wir *einfache* Parser programmieren, hier vorgeführt an der Funktion *read-nat*, die einen String in eine natürliche Zahl überführt.

module Effects.Input2

```
exception Read
let read-nat (s : String) : Nat =
  let rec nat = function
    | [ ]      → 0
    | c :: cs → if Char.IsDigit c then
                  Nat.ord c – Nat.ord '0' + 10 * nat cs
                else
                  raise Read
  if s = "" then raise Read
            else  nat (List.rev (explode s))
```

Ist die Syntaxanalyse erfolgreich, wird der semantische Wert direkt zurückgegeben; im Fall eines Syntaxfehlers wird eine Ausnahme geworfen: *read-nat* beklagt sich, wenn der String leer ist oder wenn andere Zeichen als Ziffern vorkommen. (Mit Hilfe der Funktion *explode* wird eine Zeichenkette in eine Liste von Zeichen überführt; diese wird mit *rev* gespiegelt, so dass die niedrigstwertige Ziffer an den Anfang kommt; *Nat.ord* bildet ein Zeichen auf seinen Zeichencode ab.) Die Funktion *read-nat* können wir zum Beispiel verwenden, um den Validator *is-nat* aus Abschnitt 7.1 etwas kürzer zu definieren.

```
let is-nat (s : String) : Result ⟨Nat⟩ =
  try
    Okay (read-nat s)
  with
  | Read → Error "natural number expected"
```

Die eventuell von *read-nat* geworfene Ausnahme wird gefangen und in ein Element des Datentyps *Result* überführt.

Der Datentyp *Result* mit seinen Konstruktoren *Okay* und *Error* ist unserer Modellierung von Ausnahmen mit den möglichen Resultaten ν und $\boxed{\nu}$ sehr ähnlich: *Okay value* und ν stehen für Ergebnisse geglückter Rechnungen, *Error msg* und $\boxed{\nu}$ signalisieren Fehler. In der Tat sind ***try*** und ***raise*** in gewisser Hinsicht überflüssig: Alle Effekte lassen sich unter Verwendung des Datentyps *Result* nachprogrammieren! Umgekehrt lässt sich der Datentyp *Result* durch Ausnahmen ersetzen. Welchen Ansatz man wählt, ist zum Teil eine Frage des guten Geschmacks und zum Teil eine

Frage der Bequemlichkeit. Machen wir die Unterschiede explizit, indem wir die Validatoren aus Abschnitt 7.1 noch einmal mit Ausnahmen nachprogrammieren. Erinnern wir uns: Ein Validator hat den Typ $t_1 \to \mathit{Result}\,\langle t_2\rangle$. Wenn wir statt *Result* Ausnahmen verwenden, können wir den Typ zu $t_1 \to t_2$ vereinfachen. Eine fehlerhafte Eingabe wird jetzt durch das Werfen einer Ausnahme signalisiert.[8] Wir missbrauchen die oben eingeführte *Panic* Ausnahme zu diesem Zweck. Damit sieht die Definition von *checked-query* wie folgt aus:

```
let rec checked-query (prompt : String, check : String → 'a) : 'a =
  try
    check (query (prompt ^ ": "))
  with
  | Panic msg → putline ("*** " ^ msg); checked-query (prompt, check)
```

Die Fallunterscheidung mit ***match*** ist einem ***try***-Ausdruck gewichen.

Die Validatoren haben, wie gesagt, einen einfacheren Typ: Sie geben entweder den semantischen Wert zurück oder werfen eine *Panic* Ausnahme.

```
let is-nat (s : String) : Nat =
  try readnat s with
  | Read → panic "natural number expected"
let is-less (n : Nat) : Nat → Nat =
  fun m → if m < n
          then m
          else panic ("number must be less than " ^ show n)
```

Die Funktion *both* ist jetzt schlicht und einfach die Vorwärtskomposition von Funktionen. (Die übliche Komposition $f \cdot g$ mit $(f \cdot g)(x) = f(g(x))$ komponiert Funktionen rückwärts: Erst wird g auf x angewendet, dann f auf das Ergebnis.)

```
let both (first : 'a → 'b, second : 'b → 'c) : 'a → 'c =
  fun x → second (first x)
```

Zur Erinnerung: Die Vorwärtskomposition ist auch als Infixoperator vordefiniert: $f \gg g$. *Lies:* f dann g — der »Pfeil« $\gg$ zeigt an, dass das Ergebnis von f in die Funktion g eingespeist wird.

Für den Anwender von *checked-query* ändert sich nichts; die Aufrufe funktionieren unverändert:

```
⋙ checked-query ("age", both (is-nat, is-less 123))
age : 41
41
```

Kommen wir zu den Vor- und Nachteilen. Verwendet man den Datentyp *Result*, dann macht der Typ von Ausdrücken und Funktionen explizit, wer »Ausnahmen wirft« und wer nicht. Das ist zunächst ein Vorteil: Man kann nicht vergessen, Ausnahmen zu behandeln, und man kommt nicht in Versuchung, Ausnahmen zu fangen, die gar nicht geworfen werden. Die Tatsache, dass alles explizit gemacht wird, ist gleichzeitig aber auch ein Nachteil: Im Prinzip müssen die Auswertungsregeln für Ausnahmen nachprogrammiert werden. Um zum Beispiel ein Paar vom Typ

[8] Interessanterweise spiegelt sich die Tatsache, dass ein Validator eine Ausnahme werfen kann, *nicht im* Typ der Funktionen wider. Man könnte sich durchaus vorstellen, diesen Effekt dort zu vermerken, zum Beispiel in der Form $t_1 \to t_2$ **throws** *Panic*. Einen solchen Ansatz verwendet die Sprache ***Java*** — das sogenannte »Catch or Specify Requirement« verlangt, dass eine Ausnahme entweder behandelt wird oder dass im Typ vermerkt wird, dass sie *möglicherweise* geworfen wird.

Result $\langle t_1 * t_2 \rangle$ aus zwei Ausdrücken e_i vom Typ *Result* $\langle t_i \rangle$ zu konstruieren — beide Ausdrücke können Ausnahmen werfen — muss man die drei Paarregeln in Programmcode überführen.

```
match e1 with
| Okay v1 →
    match e2 with
    | Okay v2    → Okay (v1, v2)
    | Error msg → Error msg
| Error msg → Error msg
```

Jeder der drei Zweige korrespondiert zu einer Auswertungsregel. Zum Vergleich: Verwendet man Ausnahmen, programmiert man einfach (e_1, e_2).

Fassen wir zusammen: Variantentypen wie *Result* oder *Option* dienen dem gleichen Zweck wie Ausnahmen. Ausnahmen sind fest in Mini–F# verdrahtet, aber nicht unbedingt notwendig: Mit Fleiß und Ausdauer können wir Ausnahmen mit Hilfe von Variantentypen nachprogrammieren. Kurzum: Einmal formalisieren wir Ausnahmen in der Objektsprache (mit den Mitteln von Mini–F#), einmal in der Metasprache (in der dynamischen Semantik mit Hilfe von Auswertungsregeln).

Projekt: interaktiver Taschenrechner Lösen wir zum Schluss des Kapitels noch eine letzte Aufgabe, die Programmierung eines interaktiven Taschenrechners. Wir stellen zwei verschiedene Varianten vor: einen UPN-Rechner und einen Mini^2-F# Rechner. Fangen wir mit dem altmodischen Gerät an: ***UPN*** steht für *U*mgekehrte *P*olnische *N*otation, ein Synonym für Postfixnotation, siehe Abschnitt 6.4. Schauen wir uns eine kurze Interaktion an:

module Effects.UPNCalculator

```
UPN⟩ 4711
UPN⟩ 815
UPN⟩ 2765
UPN⟩ *
UPN⟩ +
UPN⟩ .
2258186
```

Der Postfix-Ausdruck wird Zeile für Zeile eingegeben: 4711 815 2765 * + entspricht dem Infix-Ausdruck 4711 + 815 * 2765. Ausdrücke in Postfixnotation lassen sich besonders leicht ausrechnen: Wir merken uns die eingegebenen Zahlen; jede Operation ersetzt die letzten beiden Zahlen durch das Ergebnis. Die obigen Eingaben lassen sich wie folgt abarbeiten:

```
4711                4711
815                 4711 815
2765                4711 815 2765
*                   4711 2253475
+                   2258186
```

Die Liste der Zahlen nennt man auch ***Stapel*** (engl. ***stack***): Optisch muss man die Listen um 90° nach links drehen. Jede eingegebene Zahl wird oben auf dem Stapel abgelegt; eine Operation nimmt die beiden obersten Elemente vom Stapel und legt das Ergebnis dort wieder ab.

Einen Stapel, das Gedächtnis des UPN-Rechners, können wir durch eine Speicherzelle repräsentieren, die eine Liste von Zahlen enthält.

```
exception Pop
exception Top

module Stack =
  let private stack = ref [ ]
  let push (x : Nat) =
    stack := x :: !stack
  let pop () : Nat =
    match !stack with
    | [ ]     → raise Pop
    | x :: xs → stack := xs; x
  let top () : Nat =
    match !stack with
    | [ ]     → raise Top
    | x :: xs → x
```

Die Funktion *push* legt ein Element auf dem Stapel ab, *pop* entfernt ein Element und *top* inspiziert das oberste Element. Die letzten beiden Funktionen werfen gleichnamige Ausnahmen, wenn der Stapel leer ist. Die Speicherzelle, auf der die Funktionen arbeiten, ist wie immer gekapselt, also nur lokal sichtbar.

Der UPN-Taschenrechner implementiert ähnlich wie der Mini–F# Interpreter eine einfache Kommandozeile: Ein Prompt wird ausgegeben, ein Kommando eingelesen und anschließend ausgeführt.

```
let rec upn-calculator () =
  try
    match query "UPN > " with
    | ""  → ()
    | "+" → Stack.push (Stack.pop () + Stack.pop ())
    | "*" → Stack.push (Stack.pop () * Stack.pop ())
    | "." → print (Stack.top ())
    | s   → Stack.push (read-nat s)
  with
  | Pop | Top → putline "stack is empty"
  | Read      → putline "enter a number or an operator"
  upn-calculator ()
```

Typisch für einen Kommandozeileninterpreter ist der ***endrekursive*** Aufruf am Ende: Der Interpreter terminiert nicht, zumindest nicht auf den ersten Blick. Das Verhalten einschließlich der Terminierung wird von dem/der Benutzer/-in gesteuert. Signalisiert er/sie das Ende der Eingabe[9], dann wirft *query* eine *EOF* Ausnahme. Diese Ausnahme wird im Gegensatz zu *Pop*, *Top* und *Read* nicht abgefangen und führt damit zum Programmabbruch. Die Erweiterung des Taschenrechners in Abbildung 7.5 fängt auch diese Ausnahme und verabschiedet sich von dem/der Benutzer/-in. Auch die Eingabe von `quit` oder Synonymen terminiert den Taschenrechner.

Kommen wir zum Mini²-F# Rechner, einem Taschenrechner, der Infixnotation unterstützt. Wie man sieht, simuliert der Taschenrechner den Mini–F# Interpreter.

module Effects.Mini2

[9] Unter Linux und UNIX wird das Ende der Eingabe vermittels der Tastenkombination Control-D, respektive Strg-D auf einer deutschen Tastatur, signalisiert; unter Microsofts DOS verwendet man Control-Z respektive Strg-Z.

```
let upn-calculator () =
  let rec read-eval-print-loop () =
    try
      match query "UPN > " with
       | ""   → ()
       | "+" → Stack.push (Stack.pop () + Stack.pop ())
       | "*" → Stack.push (Stack.pop () * Stack.pop ())
       | "." → print (Stack.top ())
       | "exit" | "halt" | "q" | "quit" | "stop"
             → raise EOF
       | s    → Stack.push (read-nat s)
    with
     | Pop | Top → putline "stack is empty"
     | Read      → putline "enter a number or an operator"
    read-eval-print-loop ()
  in
    try
      read-eval-print-loop ()
    with
     | EOF → putline "bye bye"
```

Abbildung 7.5.: Ein UPN-Taschenrechner.

```
Mini-Mini⟩ 4711 + 815 * 2765
2258186
Mini-Mini⟩ 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10
55
Mini-Mini⟩ 1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10
3628800
Mini-Mini⟩ Hello, world !
lexical error : illegal character
Mini-Mini⟩ 4711 815 2765 * +
syntax error
```

Die Implementierung, siehe Abbildung 7.6, ist etwas kürzer als die des UPN-Taschenrechners, da wir auf die Vorarbeiten aus Kapitel 6 zurückgreifen können. So verwenden wir die Funktion *abstract-syntax-tree*, um den eingegebenen String in einen abstrakten Syntaxbaum zu überführen und *evaluate* um den Baum auszuwerten. Zwei Arten von Fehlern werden erkannt: lexikalische Fehler und Syntaxfehler. Der Scanner aus Abschnitt 6.2.2 wirft eine *Panic* Ausnahme, wenn ein unzulässiges Zeichen auftritt. Dieser Fehler wird mit einem ***try***-Ausdruck abgefangen. Ein Syntaxfehler liegt vor, wenn der Parser den Wert *None* zurückgibt. Dieser Fehler wird mit einem ***match***-Ausdruck abgefangen. Der Mini^2-F# Interpreter realisiert eine echte »read-eval-print loop«: Ein Ausdruck wird eingelesen, der Ausdruck wird ausgewertet und das Ergebnis wird ausgegeben. Der Mini–F# Interpreter selbst folgt dem gleichen Schema, nur dass die einzelnen Phasen etwas aufwändiger sind, zum Beispiel wird der abstrakte Syntaxbaum erst typgeprüft, dann wird der Ausdruck in eine einfachere Sprache übersetzt und erst dann erfolgt die eigentliche Auswertung.

```
let rec read-eval-print-loop () =
  try
    let s = query "Mini-Mini > "
    if s = "" then
      ()
    elif contains s ["exit";"halt";"q";"quit";"stop"] then
      raise EOF
    else
      match abstract-syntax-tree s with
      | None   → putline "syntax error"
      | Some e → print (evaluate e)
  with
  | Panic s → putline ("lexical error: " ^ s)
  read-eval-print-loop ()
let mini2 () =
  try
    read-eval-print-loop ()
  with
  | EOF → putline "bye bye"
```

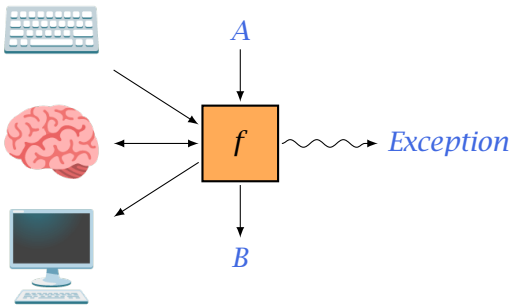
Abbildung 7.6.: Ein Taschenrechner (Mini^2-F# in Mini-F#).

Übungen.

1. Ein Array lässt sich in linearer Zeit in eine Liste überführen. Die Konvertierung einer Liste in ein Array ist schwieriger: Mit den Mitteln von Kapitel 3 oder 4 lässt sich dies nur in quadratischer Zeit bewerkstelligen. Welche in diesem Kapitel eingeführten Konzepte benötigt man, um die Konvertierung in linearer Zeit zu schaffen? Geben Sie eine Implementierung an.

2. Erweitern Sie den UPN-Taschenrechner um weitere arithmetische Funktionen wie Subtraktion und Division. Fangen Sie die Division durch Null ab und machen Sie die Benutzer*in auf den Fehler aufmerksam.

Zusammenfassung und Anmerkungen



DIY: Zusammenfassung

8. Objekte\Rechnen im Großen

I made up the term 'object-oriented', and
I can tell you I didn't have C++ in mind.
— Alan Kay, *OOPSLA '97*

Object oriented programming is, in some sense, just a programming trick using indirection. It's a trick good programmers have been using for years.
— Bjarne Stroustrup

There are only two things wrong with C++.
The initial concept and the implementation.
— Bertrand Meyer

In den vorangegangenen Kapiteln haben wir uns mit der ***Programmierung im Kleinen*** beschäftigt, mit Algorithmen und Datenstrukturen. Wie werden Rechenregeln aufgestellt? Wie lassen sich Daten und Informationen repräsentieren? Wie kann ein Programm mit der Umwelt interagieren? Wie kann man Rechenregeln mit einem Gedächtnis ausstatten? Wie kann man mit Ausnahmesituationen umgehen?

In diesem, dem letzten und damit abschließenden Kapitel wenden wir uns der ***Programmierung im Großen*** zu und diskutieren, wie sich Rechenregeln zu größeren konzeptionellen Einheiten zusammenfassen lassen, wie diese Einheiten ihrerseits organisiert und komponiert werden können.

Es gibt im Wesentlichen zwei Mechanismen, um größere Programme oder Softwaresysteme zu strukturieren:

- ***Modulsysteme*** und
- ***Objektsysteme***.

Grob gesprochen ist ein Objekt eine homogene Sammlung von Operationen, während ein Modul eine inhomogene Sammlung von Werten, Typen und anderen Modulen ist. Die beiden Mechanismen stehen in einer gewissen Konkurrenzsituation. Die meisten Programmiersprachen bieten entweder ein ausgefeiltes Modulsystem oder ein ausgefeiltes Objektsystem an. Mini–F# gehört zur letzten Kategorie: Ihr Modulsystem ist bewusst einfach gestrickt und dient im Wesentlichen der Verwaltung von Namensräumen (der Namenshygiene). Das zentrale Thema dieses Kapitels ist somit ihr Objektsystem.

Objektsysteme können auf Prototypen oder auf Klassen basieren. Sie werden schnell merken, dass es neben den eigentlichen Sprachkonzepten, einiges an technischem Jargon zu lernen gibt. Objekte werden gerne in eine biologische Metapher eingekleidet: »Ein Objekt sendet eine Nachricht an ein anderes Objekt«; »ein Objekt erbt Verhalten von einem anderen Objekt.« Prototypenbasierte Systeme sind im gewissen Sinne näher an der biologische Metapher: Ein neues Objekt wird erzeugt, indem ein bereits bestehendes Objekt geklont wird. In klassenbasierten Systemen werden neue Objekte erzeugt, indem Lücken von vorgefertigten Schablonen, den sogenannten Klassen, mit Leben erfüllt werden. Wir betrachten beide Varianten, den prototypenbasierten Ansatz vorwiegend in den Abschnitten 8.1 und 8.2 und den klassenbasierten Ansatz in den Abschnitten 8.3 und 8.5.

Die Zitate am Anfang dieses Kapitels deuten an, dass es durchaus sehr konträre Meinungen gibt, was eine objektorientierte Sprache ausmacht. Fragt man 10 Experten, so erhält man 20 Meinungen. Relativ unstrittig sind die folgenden Charakteristika:

- ***Dynamische Bindung*** (engl. dynamic dispatch): Wird eine Operation auf einem Objekt durchgeführt, bestimmt das Objekt selbst, welcher Code ausgeführt wird. Objekte mit derselben Schnittstelle können unterschiedlich implementiert sein. Die Implementierungen der Operationen heißen ***Methoden***; der Anwendung einer Operation entsprechend ***Methodenaufruf*** (engl. method invocation). Man sagt auch, dem Objekt wird eine Nachricht geschickt.

- ***Kapselung*** (engl. encapsulation): Die interne Repräsentation eines Objekts ist außen nicht sichtbar und kann somit lokal geändert werden.

- ***Untertypen*** (engl. interface inheritance): Auf Schnittstellen lässt sich eine natürliche Untertypbeziehung definieren: Ein Objekt lässt sich in einem Kontext verwenden, in dem nur eine Teilmenge der Methoden benötigt wird. Auf diese Weise lassen sich polymorphe Funktionen definieren, die unterschiedliche Objekte uniform behandeln.

- ***Vererbung*** (engl. implementation inheritance): Vererbung erlaubt es, die Implementierung verschiedener Objekte zu faktorisieren, so dass gemeinsames Verhalten nur einmal implementiert werden muss. Prototypenbasierte Sprachen verwenden ***Delegation***, klassenbasierte Sprachen bieten Klassen und ***Unterklassen*** an.

Mit all diesen Konzepten werden wir uns intensiv auseinandersetzen. Das folgende Konzept fällt dabei unter den Tisch, obwohl es von vielen Proponenten der Objektorientierung als ebenso zentral angesehen wird (siehe aber Übung 8.5.3).

- ***Objektidentität*** (engl. object identity): Jedes Objekt hat eine eigene Identität (»all objects are born unequal«).

Im Einzelnen haben wir Folgendes vor.

Abschnitt 8.1 führt den Markenkern von Objektsystemen ein, Schnittstellen und Objekte, und zeigt, wie Objekte mittels Delegation komponiert werden können. Das Objektsystem von Mini–F# basiert streng genommen nicht auf Prototypen; die leichtgewichtigen Objekte aus Abschnitt 8.1 kommen der Idee aber sehr nahe. Wir kontrastieren Objekte mit uns bereits bekannten und vertrauten Konzepten: Modulen, Records, Varianten und abstrakten Datentypen.

Abschnitt 8.2 beschäftigt sich mit einer zweiten Spielart der Polymorphie, der Inklusionspolymorphie, die es erlaubt, überqualifizierte Objekte in Kontexten zu verwenden, die eine geringere Funktionalität erfordern.

Abschnitt 8.3 wendet sich dem klassenbasierten Ansatz zu und zeigt, dass Klassen im Prinzip Sprachkonzepte von Modulen mit denen von Objekten kombinieren.

Abschnitt 8.4 unternimmt einen kurzen Ausflug in die Welt der Modellierung und diskutiert den Entwurf von Schnittstellen am Beispiel von Sequenzen. Folgen von Elementen lassen sich nicht nur explizit durch Daten (»Was sind die Elemente der Sequenz?«), sondern auch implizit durch Programme darstellen (»Wie zähle ich die Elemente der Sequenz auf?«).

Abschnitt 8.5 zeigt schließlich, wie im klassenbasierten Ansatz Objekte mittels Unterklassen kompositional definiert werden können. Das Konzept der Vererbung wird anhand von zwei objektorientierten Entwurfsmustern, dem Beobachter- und dem Schablonen-Entwurfsmuster, illustriert und dem Konzept der Delegation aus Abschnitt 8.1 gegenübergestellt.

8.1. Schnittstellen und Objekte

Rufen wir uns noch einmal die Implementierung eines Bankkontos aus Kapitel 7 ins Gedächtnis (*Account* aus Abschnitt 7.2 bzw. *JuniorAccount* aus Abschnitt 7.4).

module Objects.Bank

```
exception Insufficient of Nat
let monus (n1 : Nat, n2 : Nat) : Nat =
  if n1 ⩾ n2 then n1 ∸ n2
             else raise (Insufficient n1)
module Account =
  let mutable private funds = 0
  let deposit (amount : Nat) =
    funds ← funds + amount
  let withdraw (amount : Nat) =
    funds ← monus (funds, amount)
  let balance () = funds
```

Wir haben mehrere kleinere Änderungen vorgenommen: An die Stelle einer Speicherzelle (*let funds = ref 0*) ist ein veränderlicher Bezeichner getreten (*let mutable funds = 0*); aus Gründen der Übersichtlichkeit haben wir die »Subtraktion mit Ausnahme« aus dem Rumpf der Funktion *withdraw* herausgenommen und als getrennte Funktion implementiert; und schließlich verzichten wir darauf, auf dem Konto einen Minimalbetrag *minFunds* zu belassen.

Erinnern wir uns: Die Funktionen *deposit*, *withdraw* und *balance* verwenden die Veränderliche *funds*, die den jeweils aktuellen Kontostand repräsentiert. Nach außen ist dieses Implementierungsdetail nicht sichtbar: Der Zustand ist gekapselt. Mit Hilfe des Modulsystems werden die drei Operationen weiterhin zu einer konzeptionellen Einheit zusammengefasst: Das lokale Modul *Account* modelliert ein Bankkonto.

Trotz dieser wünschenswerten Eigenschaften scheint die Verwendung des Modulsystems nicht adäquat: Auf diese Weise wird genau *ein* Bankkonto realisiert — es ist unklar, ob und wie man ein Bankinstitut mit einer Vielzahl von Konten modellieren kann. Um dieser Anforderung Rechnung zu tragen, führen wir einen sogenannten ***Schnittstellentyp*** ein.

```
type IAccount =
  interface
    abstract member Deposit  : Nat → Unit
    abstract member Withdraw : Nat → Unit
    abstract member Balance  : Nat with get
  end
```

Die Schnittstelle (engl. interface) legt fest, was mit einem Konto, einem Element des Typs *IAccount*, gemacht werden kann:

- Mit Hilfe von *Deposit* kann ein Betrag in ein Konto eingezahlt werden.
- Die sogenannte *Methode Withdraw* erlaubt es, einen Betrag abzuheben.
- Der Kontostand kann mit Hilfe der *Eigenschaft Balance* eingesehen werden.

Die interne Repräsentation eines Kontos ist im Typ *nicht* festgelegt und kann, wie wir sehen werden, sehr unterschiedlich sein. Eine Schnittstelle basiert auf der Idee des ***abstrakten Datentyps*** — wie das Schlüsselwort *abstract* andeutet. Später mehr zu diesem Thema.

Etwas Fachjargon: Eine Schnittstelle heißt auch Objekttyp; Elemente eines Objekttyps heißen entsprechend ***Objekte***. In der Schnittstelle aufgeführte Funktionen nennt man ***Methoden*** (engl. methods), andere Werte ***Eigenschaften*** (engl. properties). Im obigen Beispiel sind *Deposit* und *Withdraw* Methoden, während *Balance* eine Eigenschaft ist. Der Ergebnistyp der beiden Methoden, *Unit*, deutet an, dass diese um ihres Effektes und nicht um ihres Wertes willen verwendet werden. Die Eigenschaft *Balance* ist lesbar (*get* ist nach dem Schlüsselwort ***with*** aufgeführt), aber nicht schreibbar (*set* fehlt).

Ist der Schnittstellentyp *IAccount* gegeben, dann kann ein einzelnes Bankkonto mit einem sogenannten ***Objektausdruck*** der Form {***new*** *IAccount* ***with*** …} angelegt werden. Nach dem Schlüsselwort ***with*** wird konkretisiert, wie die verschiedenen Mitglieder der Schnittstelle, Methoden und Eigenschaften, implementiert werden.

```
let lisas : IAccount =
  let mutable funds = 0
  {
    new IAccount with
      member self.Deposit (amount : Nat) =
        funds ← funds + amount
      member self.Withdraw (amount : Nat) =
        funds ← monus (funds, amount)
      member self.Balance
        with get () = funds
  }
```

Allgemein erzeugt {***new*** T ***with*** …} ein Element des Typs T, ein ***Objekt***. Ein Objekt selbst ist ein Wert und kann somit mittels einer Wertedefinition an einen Bezeichner gebunden werden. Wie in der modulbasierten Variante hat das Objekt *lisas* einen internen Zustand, die Speicherzelle *funds*, um den aktuellen Kontostand zu repräsentieren. Durch die lokale Bindung mit ***let*** ist dieses Implementierungsdetail nicht nach außen sichtbar — der Zustand ist *gekapselt*.

Auf die Mitglieder eines Objekts wird mit Hilfe der Punktnotation zugegriffen, die wir schon von Modulen und Records kennen.

```
>>> lisas.Deposit 4711
()
>>> lisas.Withdraw 815
()
>>> lisas.Withdraw 2765
()
>>> lisas.Balance
1131
```

Man sagt auch dem Objekt *lisas* wird die ***Nachricht*** *Deposit* geschickt. In der Definition von *lisas* steht der frei wählbare Bezeichner *self* jeweils für das Objekt selbst, dem Empfänger der Nachricht. (Methoden können verschränkt rekursiv definiert werden; mit Hilfe von *self* kann das Objekt im Rumpf einer Methode oder einer Eigenschaft Nachrichten an sich selbst schicken. Wenn man möchte, kann man ein Objekt in erster Näherung als ein rekursiv definiertes Record auffassen, siehe Abschnitt 8.1.4.)

Ein Objekt definiert sich einzig und allein durch sein Verhalten (engl. behaviour). Das gleiche Verhalten kann auf sehr unterschiedliche Art und Weise realisiert werden. Die folgende Implementierung eines Bankkontos merkt sich die letzten *n* Kontostände in einer Art »Ringpuffer«.

```
let ludwigs : IAccount =
  let size        = 10
  let history     = [| for k in 0 .. size - 1 → 0 |]
  let mutable i = 0
  let next ()     = (i + 1) % size
  {
    new IAccount with
      member self.Deposit (amount : Nat) =
        history.[next ()] ← history.[i] + amount
        i ← next ()
      member self.Withdraw (amount : Nat) =
        history.[next ()] ← monus (history.[i], amount)
        i ← next ()
      member self.Balance
        with get () = history.[i]
  }
```

Jetzt da wir zwei verschiedene Bankkonten zur Verfügung haben, können wir eine Überweisung tätigen.

```
⋙ lisas.Balance
1131
⋙ ludwigs.Deposit 4711
()
⋙ let n = 1000 in lisas.Withdraw n; ludwigs.Deposit n
()
⋙ lisas.Balance
131
⋙ ludwigs.Balance
5711
```

Da die beiden Objekte die gleiche Schnittstelle implementieren, verstehen sie die gleichen Nachrichten. Die interne Umsetzung ist aber ganz unterschiedlich. Jedes Objekt entscheidet selbst, wie es auf eine Nachricht reagiert, sprich welcher Programmcode ausgeführt wird (engl. ***dynamic dispatch***).

Objekte sind wie gesagt normale Werte; sie können insbesondere Argument oder Ergebnis von Funktionen sein. Die Funktion *transfer*, die eine Überweisung realisiert, illustriert die Verwendung von Objekten als Funktionsargumente.

```
let transfer (sender : IAccount, amount : Nat, receiver : IAccount) =
  sender.Withdraw amount
  receiver.Deposit  amount
```

Die Funktion *transfer* kann lediglich die in der Schnittstelle zur Verfügung gestellten Operationen nutzen. Wie potentielle Argumente gestrickt sind, ist für ihre Funktionsweise uninteressant und unerheblich. Tatsächlich können wir *transfer* programmieren, ohne dass Implementierungen der Schnittstelle überhaupt existieren — nur testen könnten wir *transfer* in einem solchen Fall nicht.

```
>>> (lisas.Balance, ludwigs.Balance)
(131, 5711)
>>> transfer (ludwigs, 815, lisas)
()
>>> (lisas.Balance, ludwigs.Balance)
(946, 4896)
```

Kommen wir von einem Bankkonto zu vielen Bankkonten, sprich einer Bank. Ein einzelnes Bankinstitut kann durch eine Funktion implementiert werden, die ein Bankkonto als Ergebnis hat und auf diese Weise die Eröffnung eines Kontos modelliert.

```
let account (seed : Nat) : IAccount =
  let mutable funds = seed
  {
    new IAccount with
      member self.Deposit (amount : Nat) =
        funds ← funds + amount
      member self.Withdraw (amount : Nat) =
        funds ← monus (funds, amount)
      member self.Balance
        with get () = funds
  }
```

Die Funktion *account* illustriert die Verwendung von Objekten als Funktionsergebnis. Die Funktion heißt auch ***Objektkonstruktor*** oder kurz ***Konstruktor***, da sie Objekte konstruiert.

module Objects.Person

»Getter« und »Setter« Hinter der öffentlichen Eigenschaft *Balance* steht die interne Veränderliche *funds* (im Englischen wird *funds* auch als »backing store« von *Balance* bezeichnet). Ihr Wert wird von *Balance* unverändert bekannt gemacht. Das muss nicht zwangsläufig so sein: Eine Eigenschaft kann sich auch aus einem Datum oder aus mehreren Daten ableiten; sie kann eine ***Sicht*** (engl. view) auf die Daten anbieten.

```
type Person =
  interface
    abstract member Name : String with get
    abstract member Age  : Nat    with get, set
  end
let doctor name alias age =
  let mutable age = age
  {
    new Person with
      member self.Name
        with get () = "Doctor " ^ name ^
                      if alias = "" then "" else " (aka " ^ alias ^ ")"
      member self.Age
        with get ()  = age
        and  set inc = age ← age + inc
  }
```

Die Eigenschaft *Name* definiert eine spezielle ***Sicht*** (engl. view) auf die zugrundeliegenden »Rohdaten«. Die Schnittstelle *Person* bietet neben dieser nur lesbaren Eigenschaft auch eine Eigenschaft an, die sowohl les- als auch schreibbar ist. Schreibbare Eigenschaften können auf der linken Seite einer Zuweisung der Form $e_1 \leftarrow e_2$ stehen.

```
⋙ let dolittle = doctor "Dolittle" "King Jong Thinkalot" 42
⋙ dolittle.Name
"Doctor Dolittle (aka King Jong Thinkalot)"
⋙ dolittle.Age ← 2
()
⋙ dolittle.Age
44
```

Es ist bemerkenswert, dass die Zuweisung nicht das Alter auf den angegebenen Wert setzt, sondern um diesen Wert erhöht. (Die Zuweisung *dolittle.Age* ← 2 entspricht somit der C Zuweisung `dolittle.Age += 2`.) Anders als im Fall von Veränderlichen können beim Lesen und beim Schreiben von Eigenschaften beliebige Berechnungen durchgeführt werden!

8.1.1. Abstrakte Syntax

Eine ***Eigenschaft*** ist tatsächlich syntaktischer Zucker für zwei Methoden, die sogenannten »Setter« und »Getter« der Eigenschaft. Mit anderen Worten, die Semantik von Eigenschaften können wir erklären, indem wir die Sprachkonstrukte übersetzen und so auf die Semantik von Methoden zurückführen. Die Deklaration der Eigenschaft

abstract member $\ell : t$ ***with*** *get*, *set*

ist eine Abkürzung für die Methodendeklarationen

abstract member *get-*$\ell : \mathit{Unit} \to t$
abstract member *set-*$\ell : t \to \mathit{Unit}$

Fehlt bei der Deklaration der Eigenschaft der Zusatz *get* oder *set*, dann ist entsprechend nur eine der beiden Methoden verfügbar. Ist t ein nicht-funktionaler Typ, dann ist die Deklaration ***abstract member*** $\ell : t$ eine Abkürzung für ***abstract member*** $\ell : t$ ***with*** *get*.

Somit können wir uns auf die formale Definition von Methoden konzentrieren. Wie üblich beschränken wir uns auf den binären Fall und formalisieren nur Objekte mit exakt zwei Methoden. Alle Sprachkonstrukte verallgemeinern sich in naheliegender Weise auf n Methoden.

Ein Schnittstellentyp (engl. interface type) wird durch eine Definition eingeführt.

$d ::= \cdots$	***Deklarationen:***
type T =	Schnittstellentypdefinition ($\ell_1 \neq \ell_2$)
interface	
abstract member $\ell_1 : t_1$	
abstract member $\ell_2 : t_2$	
end	

Der Bezeichner T wird durch die Definition neu eingeführt, ebenso die Bezeichner für die ***Methoden***, ℓ_1 und ℓ_2, die verschieden sein müssen: $\ell_1 \neq \ell_2$. (Das Schlüsselwort ***member*** kann übrigens weggelassen werden, ebenso wie die ***interface*** … ***end*** Klammer.)

Wir erweitern Ausdrücke um Sprachkonstrukte, die Objekte konstruieren und analysieren, um Objektausdrücke (engl. object expressions) und Methodenaufrufe (engl. method invocations).

$e ::= \cdots$	***Ausdrücke:***
$\mid \{\,\textit{new}\ \mathrm{T}\ \textit{with}$	Objektausdruck\anonymes Objekt ($\ell_1 \neq \ell_2$)
$\quad\ \textit{member}\ s_1.\ell_1 = e_1$	
$\quad\ \textit{member}\ s_2.\ell_2 = e_2$	
$\quad\}$	
$\mid e.\ell$	Methodenaufruf

So wie ein Funktionsausdruck eine anonyme Funktion konstruiert, so erzeugt ein Objektausdruck ein anonymes Objekt. Nach dem Schlüsselwort ***member*** wird jeweils ein beliebiger Bezeichner aufgeführt, der den Empfänger der Nachricht repräsentiert, das heißt, der für das durch den Objektausdruck erzeugte Objekt selbst steht. Aufgrund dieser Selbstbezüglichkeit wird als Name oft *me*, *self* oder *this* gewählt (wir verwenden durchgehend *self*). Benötigt man keine Referenz auf das Objekt selbst, kann eine anonyme Variable angegeben werden. Ähnlich wie bei Funktionsdefinitionen wird nach dem Gleichheitszeichen der ***Methodenrumpf*** aufgeführt. Mit $e.\ell$ wird die Methode ℓ aufgerufen; man sagt auch, dem Objekt e wird die Nachricht ℓ geschickt.

In der konkreten Syntax wird zwischen Methoden und Eigenschaften unterschieden. Für Methoden *muss* die Syntax $\textit{member}\ s.\ell\ x = e$ benutzt werden, das heißt nach dem Methodennamen wird der Parametername aufgeführt; für Eigenschaften wird die Syntax

$$\textit{member}\ s.\ell\ \textit{with}\ \textit{get}\ () = e_1\ \textit{and}\ \textit{set}\ v = e_2$$

verwendet. Die Definition ist syntaktischer Zucker für die entsprechenden »Setter« und »Getter« der Eigenschaft ℓ:

$$\begin{aligned}&\textit{member}\ s.\textit{get-}\ell\ () = e_1\\ &\textit{member}\ s.\textit{set-}\ell\ v\ = e_2\end{aligned}$$

Wir fassen im Folgenden die konkrete Syntax

$$\textit{member}\ s.\ell\ x = e \text{ als Abkürzung für } \textit{member}\ s.\ell = \textit{fun}\ x \to e$$

auf. Auf diese Weise wird vermieden, dass wir die Typ- und Auswertungsregeln für Funktionen für Methoden duplizieren. In der konkreten Syntax ist die obige Abkürzung leider nicht zulässig, da sie für die Definition von Eigenschaften reserviert ist: $\textit{member}\ s.\ell = e$ kürzt die Definition $\textit{member}\ s.\ell\ \textit{with}\ \textit{get}\ () = e$ ab.

Ist ℓ eine Eigenschaft, so wird mit $e.\ell$ die Eigenschaft des Objekts e abgefragt und mit $e.\ell \leftarrow e'$ gesetzt. Der Ausdruck $e.\ell$ ist syntaktischer Zucker für den Methodenaufruf $e.\textit{get-}\ell\ ()$, die Zuweisung $e.\ell \leftarrow e'$ entsprechend Zucker für $e.\textit{set-}\ell\ e'$.

8.1.2. Statische Semantik

Die folgenden Typregeln setzen voraus, dass die Typdefinition

$$\begin{aligned}&\textit{type}\ \mathrm{T} =\\ &\quad\textit{interface}\\ &\qquad\textit{abstract member}\ \ell_1 : t_1\\ &\qquad\textit{abstract member}\ \ell_2 : t_2\\ &\quad\textit{end}\end{aligned}$$

bekannt ist. Die Typregeln sind denen für Records nicht unähnlich.

$$\frac{\Sigma, \{s_1 \mapsto \mathrm{T}\} \vdash e_1 : t_1 \qquad \Sigma, \{s_2 \mapsto \mathrm{T}\} \vdash e_2 : t_2}{\begin{aligned}\Sigma \vdash \{&\textit{new}\ \mathrm{T}\ \textit{with member}\ s_1.\ell_1 = e_1\\ &\textit{member}\ s_2.\ell_2 = e_2\} : \mathrm{T}\end{aligned}}$$

$$\frac{\Sigma, \{s_1 \mapsto \mathrm{T}\} \vdash e_1 : t_1 \qquad \Sigma, \{s_2 \mapsto \mathrm{T}\} \vdash e_2 : t_2}{\Sigma \vdash \{\,\textit{new}\ \mathrm{T}\ \textit{with member}\ s_2.\ell_2 = e_2\ \textit{member}\ s_1.\ell_1 = e_1\,\} : \mathrm{T}}$$

$$\frac{\Sigma \vdash e : \mathrm{T}}{\Sigma \vdash e.\ell_i : t_i} \quad i \in \{1, 2\}$$

Bei der Konstruktion eines Objekts müssen stets alle in der Schnittstelle aufgeführten Mitglieder definiert werden; die Reihenfolge der Definitionen ist allerdings beliebig. Auf diese Weise wird sichergestellt, dass ein Objekt alle Nachrichten versteht. Der »*self*-Bezeichner« s_i ist im Methodenrumpf e_i sichtbar und besitzt den gleichen Typ wie das Objekt selbst.

8.1.3. Dynamische Semantik

Wir erweitern Werte um Methodentabellen, die Objekte repräsentieren, und Methodenabschlüsse, zu denen Methoden auswerten.

$\mu \in \mathsf{Lab} \to_{\mathrm{fin}} \mathsf{Val}$	***Methodenumgebungen\Methodentabellen***
$\nu ::= \cdots$	***Werte:***
$\mid\ \mu$	Objekt
$\mid\ \langle\!\langle \delta, s, e \rangle\!\rangle$	Methodenabschluss

Die Methodentabelle (engl. method table or dispatch table) bildet Methodennamen auf Werte ab. Der Methodenabschluss $\langle\!\langle \delta, s, e \rangle\!\rangle$ korrespondiert zu dem *rekursiven* Funktionsabschluss $\langle \delta, s, x, e \rangle$ mit dem Unterschied, dass der formale Parameter x fehlt.

Ein Objekt wertet im Wesentlichen zu sich selbst aus.

$$\frac{}{\delta \vdash \{\,\textit{new}\ \mathrm{T}\ \textit{with member}\ s_1.\ell_1 = e_1\ \textit{member}\ s_2.\ell_2 = e_2\,\} \Downarrow \{\ell_1 \mapsto \langle\!\langle \delta, s_1, e_1 \rangle\!\rangle, \ell_2 \mapsto \langle\!\langle \delta, s_2, e_2 \rangle\!\rangle\}}$$

$$\frac{}{\delta \vdash \{\,\textit{new}\ \mathrm{T}\ \textit{with member}\ s_2.\ell_2 = e_2\ \textit{member}\ s_1.\ell_1 = e_1\,\} \Downarrow \{\ell_1 \mapsto \langle\!\langle \delta, s_1, e_1 \rangle\!\rangle, \ell_2 \mapsto \langle\!\langle \delta, s_2, e_2 \rangle\!\rangle\}}$$

Dem Objekt wird eine Methodentabelle zugeordnet, in der die Methodennamen an die jeweiligen Methodenabschlüsse gebunden sind. Ähnlich wie bei Funktionsausdrücken wird der Methodenrumpf e_i *nicht* ausgewertet.

Erst wenn dem Objekt eine Nachricht geschickt wird, erfolgt die Auswertung des Methodenrumpfs.

$$\frac{\delta \vdash e \Downarrow \mu \qquad \delta', \{s_i \mapsto \mu\} \vdash e_i \Downarrow \nu_i}{\delta \vdash e.\ell_i \Downarrow \nu_i} \quad \text{mit } \mu(\ell_i) = \langle\!\langle \delta', s_i, e_i \rangle\!\rangle$$

Das Label ℓ_i wird zur Laufzeit in der zu dem Objekt e gehörigen Methodentabelle nachgeschlagen (engl. dynamic dispatch). Die statische Semantik stellt sicher, dass $\ell_i \in \mathit{dom}\ \mu$. Der »*self*-Bezeichner« s_i wird an das Objekt selbst (engl. self) gebunden; in der erweiterten Umgebung wird der Rumpf der Methode ausgewertet. Das Ergebnis ist auch das Ergebnis des Methodenaufrufs.

Die Auswertungsregel für Methodenaufrufe ist der Regel für die Applikation rekursiver Funktionen nicht unähnlich, siehe Abschnitt 3.6 — in beiden Fällen wird aus einer rekursiven Definition ein zyklisches Geflecht.

8.1.4. Vertiefung

Ein Record aggregiert Werte, ein Modul aggregiert Definitionen und ein Objekt aggregiert Methoden bzw. etwas weniger prosaisch Verhalten. Auf die Komponenten der Aggregation wird jeweils mit der Punktnotation zugegriffen. Drei ähnliche Sprachkonzepte, deren Verhältnis wir im Folgenden näher beleuchten wollen.

module Objects.Clock

Objekte versus Records Ein Record aggregiert Werte; da Funktionen Werte sind, können insbesondere Funktionen aggregiert werden. Wird ein Record mit funktionalen Komponenten rekursiv definiert, erhalten wir faktisch ein Objekt. Schauen wir uns ein Beispiel an: In der folgenden Gegenüberstellung wird das Konzept einer Uhr modelliert, einmal mit Hilfe einer Schnittstelle und eines Objektkonstruktors und ein zweites Mal unter Verwendung eines Recordtyps und eines rekursiv definierten Records.

```
type Clock =
  interface
    abstract Tick  : Nat → Nat
    abstract Time : Nat with get
  end
let clock () =
  let mutable hours = 0

  {new Clock with
     member self.Tick inc =
       hours ← hours + inc
       self.Time
     member self.Time
       with get () = hours % 24
  }
```

```
type Clock =
  {
    Tick  : Nat → Nat
    Time : Unit → Nat
  }
let clock () =
  let mutable hours = 0
  let rec self =
    {
      Tick  = fun inc →
                hours ← hours + inc
                self.Time ()
      Time = fun () →
                hours % 24
    }
  self
```

Die Eigenschaft *Time* gibt die »aktuelle« Uhrzeit in Stunden an. Die Methode *Tick* stellt die Uhr um die angegebene Stundenzahl vor und gibt die Uhrzeit nach der Zeitumstellung zurück. Zu diesem Zweck ruft *Tick* die Methode *Time* auf; das Objekt *self* schickt sich selbst eine Nachricht. Diese Selbstbenachrichtigung wird in der record-basierten Variante durch eine rekursive Wertedefinition realisiert (siehe auch Abschnitt 7.2.5) — mit *let rec self* wird das Record namens *self* rekursiv definiert und anschließend als Ergebnis von *clock* () zurückgegeben. In der objekt-basierten Version rückt der »*self*«-Bezeichner zu jeder einzelnen Methode und steht dort für den Empfänger der Nachricht, also für das Objekt selbst. Die übrigen Unterschiede sind kosmetischer Natur: Eine Methodendefinition entspricht syntaktisch einer Funktionsdefinition; für Recordkomponenten ist diese Syntax nicht verfügbar, so dass wir die Funktionsdefinitionen in Funktionsausdrücke überführen müssen.

In der praktischen Handhabung unterscheiden sich die beiden Varianten nicht, wie die folgenden Interaktionen demonstrieren.

```
>>> let now = clock ()
>>> now.Tick 4711
7
>>> now.Time
7
```

```
>>> let now = clock ()
>>> now.Tick 4711
7
>>> now.Time ()
7
```

In der record-basierten Variante muss bei der Abfrage der Zeit explizit das Dummyargument »()« angegeben werden; in der objekt-basierten Version erledigt das die »Entzuckerung«: *now.Time*

wird hinter den Kulissen in den Aufruf der »Getter«-Methode *now*.*get-Time* () übersetzt. Auch auf die Gefahr hin etwas Offensichtliches zu betonen: Die Komponente *Time* muss eine Funktion sein; ersetzen wir *Time*:*Unit*→*Nat* durch *Time*:*Nat* und entsprechend *Time* = ***fun*** () → *hours*%24 durch *Time* = *hours*%24, dann wird die Zeit ein unveränderlicher Wert, sie wird auf die Stundenzahl bei der Erzeugung des Records eingefroren, nämlich 0.

Vorläufiges Fazit: Bezüglich der bisher eingeführten Funktionalität sind Objekte und rekursive Records austauschbar. Das wird nicht so bleiben: Wir werden in Abschnitt 8.2 sehen, dass eine Schnittstelle um Funktionalität erweitert werden kann; dies ist bei einem Recordtyp nicht möglich. Aber wir greifen vor.

Objekte versus Module In Kapitel 7 haben wir ein Bankkonto durch ein Modul modelliert. An die Stelle eines einzelnen Moduls ist jetzt eine Sammlung von Objekten getreten. Mit der Einführung von Objekten verlieren Module aber nicht ihre Daseinsberechtigung. Es bietet sich zum Beispiel an, die verschiedenen Operationen einer Bank mit Hilfe eines Moduls zu einer konzeptionellen Einheit zusammenzufassen, siehe Abbildung 8.1. Das Bankinstitut »Trust Me« wird durch ein lokales Modul realisiert, das bankspezifische, kontoübergreifende Operationen zusammenfasst. Zum Beispiel lässt sich die Gesamtzahl der eröffneten Konten abfragen. (Zur Erinnerung: ***do*** *e* ist eine Abkürzung für ***let*** () = *e* und kennzeichnet Definitionen, die nur ihres Effektes willen eingeführt werden.) Kontospezifische Operationen werden weiterhin in der Schnittstelle *IAccount* gebündelt.

Fazit: Module und Objekte stehen in keiner wirklichen Konkurrenzsituation; die Sprachkonzepte ergänzen sich eher sinnvoll. Module sind in Mini–F# keine Konstrukte »erster Klasse«: Ein Modul kann zum Beispiel nicht an eine Funktion übergeben werden oder als Ergebnis eines Funktionsaufrufs erhalten werden. Module haben in Mini–F# einen eher statischen Charakter. (Aus diesem Grund haben wir Module für die Modellierung von Bankkonten verworfen. Ein Modul realisiert genau ein Bankkonto; eine Funktion, die ein Bankkonto, sprich ein Modul, generiert, lässt sich nicht programmieren.) Die Zweitklassigkeit von Modulen liegt in der Tatsache begründet, dass sie neben Wertedefinitionen auch Typdefinitionen (inbesondere Schnittstellendefinitionen) aggregieren.

Delegation Neben dem Standardkonto bietet die Bank »Trust Me« zusätzlich ein Konto für Studierende an, das mit einer kleinen Einschränkung daherkommt: Es dürfen bei einer einzelnen Transaktion maximal 1000 € abgehoben werden (siehe Abbildung 8.1). Der Konstruktor *student-account* illustriert die Programmiertechnik der ***Delegation***: Dem Studierendenkonto liegt ein Standardkonto zugrunde, an das die Nachrichten *Deposit* und *Balance* delegiert werden. Die besprochene Einschränkung beim Abheben wird durch eine Alternative realisiert:

```
member self.Withdraw amount =
  if amount > limit then raise Limit
                    else basic.Withdraw amount
```

Liegt der Betrag über dem Limit, wird eine Ausnahme ausgelöst; anderenfalls wird auch die Nachricht *Withdraw* an das Standardkonto *basic* delegiert.

Der interne Zustand des Bankkontos ist in diesem Fall durch ein anderes Objekt gegeben und nicht durch eine Speicherzelle. Die kompositionale Architektur der Konten bringt viele Vorteile mit sich. Der Implementierungsaufwand wird verringert — Delegation verhindert, dass wir das Rad stets aufs Neue erfinden. Das Studierendenkonto verhält sich in den meisten Aspekten wie ein Standardkonto — Delegation stellt die Konsistenz sicher. Wird das Objekt, an das die Arbeit delegiert wird, verbessert, so profitiert auch der Auftraggeber von der Verbesserung.

Die folgende Interaktion zeigt die Operationen des Bankinstituts in Aktion.

```
exception Limit
module TrustMe =
  do putline "TrustMe is founded."
  let BIC = 4711            // Bank Identifier Code
  let mutable private no = 0
  let total-no-of-accounts () = no

  // TrustMe standard account
  let account (seed : Nat) =
    do no ← no + 1
    let mutable funds = seed
    {
      new IAccount with
        member self.Deposit (amount : Nat) =
          funds ← funds + amount
        member self.Withdraw (amount : Nat) =
          funds ← monus (funds, amount)
        member self.Balance =
          funds
    }

  // TrustMe student account: maximum withdrawal given by limit
  let limit = 1000
  let student-account (seed : Nat) =
    let basic = account seed
    {
      new IAccount with
        member self.Deposit amount = basic.Deposit amount
        member self.Withdraw amount =
          if amount > limit then raise Limit
                            else basic.Withdraw amount
        member self.Balance = basic.Balance
    }
```

Abbildung 8.1.: Modellierung eines Bankinstituts (modulbasiert).

```
>>> TrustMe.BIC
4711
>>> let hermines = TrustMe.account 8150
>>> let harrys = TrustMe.student-account 0
>>> TrustMe.total-no-of-accounts ()
2
>>> transfer (hermines, 2000, harrys)
>>> transfer (harrys, 2000, hermines)
uncaught exception: Limit
```

Objekte versus Varianten Themenwechsel: Objekte müssen nicht zwangsläufig einen internen Zustand besitzen. Um zustandslose Objekte (engl. value objects oder immutable objects) zu illustrieren, versuchen wir uns an einer Reimplementierung arithmetischer Ausdrücke. In Abschnitt 6.5.3 haben wir Ausdrücke mit Hilfe des rekursiven Variantentyps

module Objects.Expr

```
type Expr =
  | Const of Nat
  | Add   of Expr * Expr
  | Mul   of Expr * Expr
```

modelliert (siehe auch Aufgaben 4.2.3 und 4.2.4). *Lies:* Ein arithmetischer Ausdruck ist entweder eine Konstante, sprich eine natürliche Zahl, oder eine Summe bestehend aus zwei Ausdrücken oder ein Produkt.

Kommen wir zur objektbasierten Implementierung. Ein Objekt ist die Summe seines Verhaltens, so dass wir uns als Erstes fragen müssen, was wir mit einem arithmetischen Ausdruck machen wollen. Die Antwort »auswerten und anzeigen« führt zu dem folgenden Schnittstellentyp.

```
type IExpr =
  interface
    abstract member Value : Nat
    abstract member Show : String
  end
```

Aus den drei Datenkonstruktoren des Variantentyps werden Objektkonstruktoren des Schnittstellentyps. Wir führen Funktionen ein, die Konstanten, Summen und Produkte konstruieren.

```
let constant (n : Nat) : IExpr =
  { new IExpr with
      member self.Value = n
      member self.Show = show n
  }
let add (expr1 : IExpr, expr2 : IExpr) : IExpr =
  { new IExpr with
      member self.Value = expr1.Value + expr2.Value
      member self.Show = "(" ^ expr1.Show ^ " + " ^ expr2.Show ^ ")"
  }
let mul (expr1 : IExpr, expr2 : IExpr) : IExpr =
  { new IExpr with
      member self.Value = expr1.Value * expr2.Value
      member self.Show = "(" ^ expr1.Show ^ " * " ^ expr2.Show ^ ")"
  }
```

Jeder Objektkonstruktor detailliert, wie er auf die beiden möglichen Nachrichten, *Value* und *Show*, reagiert.

Vergleichen wir die obige Implementierung mit den korrespondierenden Definitionen für den variantenbasierten Ansatz,

```
let rec Value = function
  | Const n              → n
  | Add (expr1, expr2)   → Value expr1 + Value expr2
  | Mul (expr1, expr2)   → Value expr1 * Value expr2
let rec Show = function
  | Const n              → show n
  | Add (expr1, expr2)   → "(" ^ Show expr1 ^ " + " ^ Show expr2 ^ ")"
  | Mul (expr1, expr2)   → "(" ^ Show expr1 ^ " * " ^ Show expr2 ^ ")"
```

sehen wir, dass der Programmcode jeweils sehr unterschiedlich organisiert ist. Im objektbasierten Ansatz wird der Code nach den Varianten gruppiert: *constant* fasst die konstantenspezifischen Anteile aller Operationen zusammen. Im variantenbasierten Ansatz ist der Code nach den Operationen gruppiert: *Value* fasst alle Fälle der Auswertungsoperation zusammen. Stellen wir Varianten und Operationen in einer Matrix

	Const	*Add*	*Mul*
Value			
Show			

dar, dann ist im objektbasierten Ansatz der Code spaltenweise organisiert und im variantenbasierten Ansatz zeilenweise.

In der Organisation spiegelt sich die unterschiedliche Philosophie von abstrakten und konkreten Datentypen wider. Objekte definieren sich durch ihr Verhalten (»Was kann mit dem Objekt gemacht werden?«) und verkörpern die Idee des abstrakten Datentyps. Im Gegensatz dazu ist ein Variantentyp konkret: Er definiert sich durch die Angabe seiner Elemente. In unserem Beispiel fragen wir entweder »Was möchte ich mit einem arithmetischen Ausdruck machen?« oder »Wie ist ein arithmetischer Ausdruck aufgebaut?«. Die jeweilige Antwort führt zu einem Schnittstellentyp bzw. einem rekursiven Variantentyp. Die jeweils andere Frage fällt natürlich nicht unter den Tisch, kann aber entspannter angegangen werden: Für den Schnittstellentyp werden peu à peu Objektkonstruktoren definiert bzw. für den Variantentyp werden peu à peu Funktionen bereitgestellt.

In der praktischen Handhabung unterscheiden sich der variantenbasierte und der objektbasierte Ansatz nur unwesentlich. Verwendet man Objekte, dann sieht eine mögliche Interaktion wie folgt aus.

```
⋙ let e = add (constant 4711, mul (constant 815, constant 2765))
⋙ e.Show
"(4711 + (815 * 2765))"
⋙ e.Value
2258186
⋙ (add (e, e)).Value
4516372
⋙ (add (e, e)).Show
"((4711 + (815 * 2765)) + (4711 + (815 * 2765)))"
```

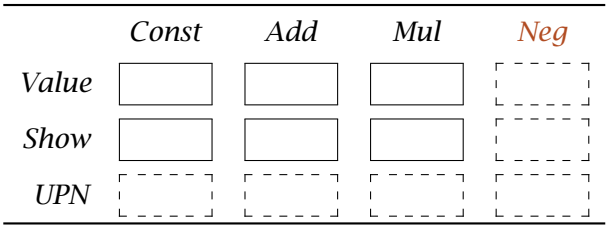
An die Stelle von Funktionsaufrufen tritt das Senden von Nachrichten mit der Punktnotation.

Unterschiede treten allerdings zutage, wenn man versucht, die jeweiligen Programme zu *erweitern*, entweder um neue Varianten (zum Beispiel Negation oder Kehrwert) oder um neue Funktionalität (zum Beispiel Übersetzung in UPN).

Im variantenbasierten Ansatz ist es einfach, neue Funktionalität hinzuzufügen: Es wird einfach eine neue Funktion definiert. In Gegensatz dazu ist es aufwändig, neue Varianten hinzuzufügen: Der Variantentyp muss um den neuen Fall erweitert werden und zusätzlich muss *jede* bestehende Funktion auf dem Variantentyp angepasst werden. Wir müssen uns jeweils überlegen, wie wir den neuen Fall behandeln.

Für den objektbasierten Ansatz kehren sich Vor- und Nachteile um. Es ist einfach, neue Varianten hinzuzufügen: Es wird einfach ein neuer Objektkonstruktor definiert. In Gegensatz dazu ist es aufwändig, neue Funktionalität hinzuzufügen: Der Schnittstellentyp muss erweitert werden und zusätzlich muss *jeder* bestehende Objektkonstruktor angepasst werden. Wir müssen uns jeweils überlegen, wie wir die neue Operation behandeln.

Eine der beiden Erweiterungen ist jeweils einfach, da lokal durchführbar; die andere ist aufwändig, da sie globale Änderungen nach sich zieht. Die zweidimensionale Darstellung



illustriert noch einmal Vor- und Nachteile. Ist die Matrix zeilenweise (spaltenweise) organisiert, dann ist es einfach eine neue Zeile (Spalte) hinzuzufügen, aber schwierig eine neue Spalte (Zeile) zu ergänzen.

Objekte versus abstrakte Datentypen Die Zusammenfassung von Operationen zu einer einheitlichen Schnittstelle kennen wir bereits von den abstrakten Datentypen. In Abschnitt 5.3 haben wir die Schnittstelle[1] eines abstrakten Datentyps mit Hilfe des *Modulsystems* realisiert. Konkret haben wir drei Implementierungen von »endlichen Abbildungen« besprochen: Listen, Suchlisten und Suchbäume.

In diesem Abschnitt haben wir gesehen, wie man Schnittstellen mit Hilfe des *Objektsystems* realisiert. Objekte basieren ebenfalls auf der Idee des abstrakten Datentyps und entwickeln diese in gewisser Weise weiter:

- Verschiedene Implementierungen eines abstrakten Datentyps zeigen exakt das gleiche Verhalten; sie sind austauschbar: Für den Benutzer macht es bezüglich des Ein- und Ausgabeverhaltens keinen Unterschied, ob endliche Abbildungen durch Listen, Suchlisten oder Suchbäume implementiert werden.
- Charakteristik des Modulsystems: Eine Schnittstelle wird zu einem Zeitpunkt durch *eine* Implementierung realisiert.
- Objekte, die die gleiche Schnittstelle unterstützen, zeigen ein verwandtes, nicht aber notwendigerweise ein identisches Verhalten: Ein Studierendenkonto verhält sich beim Abheben eines größeren Betrags anders als ein Standardkonto.

[1] F# kennt neben ***Implementierungsmodulen*** (Endung `.fs`, engl. implementation files) auch ***Schnittstellenmodule*** (Endung `.fsi`, engl. signature files). Ein Schnittstellenmodul ist gewissermaßen der »Typ« eines Implementierungsmoduls und enthält alle für die statische Semantik notwendigen Informationen, insbesondere Kopien der Typdefinitionen und die Signaturen von Wertedefinitionen.

- Charakteristik des Objektsystems: Eine Schnittstelle kann zu einem Zeitpunkt durch *mehrere* Objekte realisiert werden.

Dass ein abstrakter Datentyp mit Hilfe des Modulsystems implementiert wird, ist natürlich nicht zwingend; auch das Objektsystem kann für die Realisierung herangezogen werden. Die Tatsache, dass eine Schnittstelle zu einem Zeitpunkt durch mehrere Objekte realisiert werden kann, erweist sich, wie wir im Folgenden sehen werden, dabei oft als vorteilhaft.

module Objects.UPNCalculator

Parametrisierte Schnittstellen\generische Schnittstellen Wie Record- und Variantentypen können auch Schnittstellentypen mit einem oder mehreren Typen parametrisiert werden.

```
type IStack⟨'elem⟩ =
  interface
    abstract member IsEmpty : Bool
    abstract member Push    : 'elem → Unit
    abstract member Pop     : Unit → 'elem
    abstract member Top     : 'elem
  end
```

Auf einen Stapel (engl. stack) kann mit *Push* ein Element abgelegt werden, mit *Pop* wird das oberste Element entfernt und mit *Top* wird es inspiziert, ohne den Stapel zu verändern. Wie Listen und Arrays sind auch Stacks homogene Container: Der Typ der Elemente ist beliebig; alle Elemente eines Containers müssen aber den gleichen Typ besitzen.

In gleicher Weise wie der Objektkonstruktor *account* das Modul *Account* aus Abschnitt 7.2 verallgemeinert, so verallgemeinert der nachfolgend definierte Objektkonstruktor *stack* das Modul *Stack* aus Abschnitt 7.4.4.

```
exception Pop
exception Top
let stack⟨'elem⟩ () =
  let mutable stack = [ ]
  {
    new IStack⟨'elem⟩ with
      member self.IsEmpty =
        List.isEmpty stack
      member self.Push x =
        stack ← x :: stack
      member self.Pop () =
        match stack with
        | [ ]    → raise Pop
        | x :: xs → stack ← xs; x
      member self.Top =
        match stack with
        | [ ]    → raise Top
        | x :: xs → x
  }
```

Der Objektkonstruktor generiert einen leeren Stack eines beliebigen Elementtyps. Mit anderen Worten, *stack* ist eine *polymorphe Funktion* des Typs *Unit → IStack⟨'elem⟩*.

```
let upn-calculator-deluxe () =
  let stacks : IStack ⟨IStack ⟨Nat⟩⟩ = stack ()
  try
    stacks.Push (stack ())
    while true do
      try
        match Input.query "UPN > " with
        | ""  → ()
        | "+" → stacks.Top.Push (stacks.Top.Pop + stacks.Top.Pop)
        | "*" → stacks.Top.Push (stacks.Top.Pop * stacks.Top.Pop)
        | "." → putline (show stacks.Top.Top)
        | "exit" | "halt" | "q" | "quit" | "stop" → raise EOF
        | "(" → stacks.Push (stack ())
        | ")" → stacks.Pop |> ignore
        | s   → stacks.Top.Push (read-nat s)
      with
        | Pop | Top → putline "stack is empty"
        | Read      → putline "enter a number or an operator"
    with
    | EOF → putline "bye bye"
```

Abbildung 8.2.: Ein UPN-Taschenrechner, der Hilfsrechnungen unterstützt.

Abbildung 8.2 zeigt den Objektkonstruktor in Aktion. Der UPN-Rechner Deluxe ermöglicht Hilfsrechnungen, die mit »(« begonnen und mit »)« beendet werden. Der interne Zustand des Rechners ist ein Stack von Stacks von natürlichen Zahlen. Die Operationen +, * usw. arbeiten auf dem obersten Stack, »(« legt einen leeren Stack ab und »)« entfernt den obersten Stack — mit Hilfe von *ignore* wird das Ergebnis von *Pop* ignoriert: *let ignore _ = ()*. Zur Laufzeit existiert somit ein Stack vom Typ *IStack ⟨IStack ⟨Nat⟩⟩* und beliebig viele Stacks des Typs *IStack ⟨Nat⟩*. Polymorphie macht's möglich.

Übungen.

1. Implementieren Sie die Schnittstelle *IStack* aus Abschnitt 8.1.4 mit Hilfe von Arrays. Verwenden Sie einen »Wasserstandsanzeiger«, der auf die erste freie Position verweist; *Push* erhöht den Wasserstand; *Pop* verringert ihn. Ein array-basierter Stack hat eine Kapazitätsgrenze, die durch die Größe des Arrays gegeben ist. Wird diese überschritten, wird eine Ausnahme geworfen (der bekannte und gefürchtete »Stack Overflow«). *Tipp:* Das Interface ist generisch; wenn Sie Probleme haben, ein leeres Array zu erzeugen, verwenden Sie optionale Elemente: *Array ⟨Option ⟨'elem⟩⟩*.

2. Reimplementieren Sie Aufgaben 4.2.3 und 4.2.4 mit Hilfe von Objekten. Lassen Sie sich von der in Abschnitt 8.1.4 vorgestellten Darstellung (*IExpr*) inspirieren.

8.2. Untertypen

Informatikerinnen und Informatiker bilden Modelle der Wirklichkeit. Ein Modell wird in der Regel auf Grundlage von Anforderungen entwickelt, die präzisieren, was die Software leisten soll. Im Laufe der Zeit können sich diese Anforderungen ändern, etwa weil die Wirklichkeit vorangeschritten ist und die Modelle an die neuen Gegebenheiten angepasst werden müssen. Oder der

Einsatz der Software war so erfolgreich, dass neue Begehrlichkeiten geweckt wurden. In diesem und in den nächsten Abschnitten werden wir uns schrittweise dem Thema »Software-Evolution« annähern. Wie kann die Änderung und insbesondere die Erweiterung von Programmen linguistisch unterstützt werden, so dass die notwendigen Eingriffe »minimal invasiv« sind? Wir sagen bewusst »annähern«, da das Ideal in voller Schönheit nicht erreicht wird und wohl auch nie erreicht werden wird.

Nehmen wir an, wir wollen einige Bankkonten um die Möglichkeit erweitern, einen Kontoauszug abzurufen. Zu diesem Zweck könnten wir ein entsprechendes Mitglied zur Schnittstelle *IAccount* hinzufügen. Nun haben wir im letzten Abschnitt diskutiert, dass eine solche Änderung aufwändig ist, da jeder bestehende Objektkonstruktor geändert werden muss. Eine kostengünstigere Alternative besteht darin, eine zweite Schnittstelle als *Erweiterung* von *IAccount* zu definieren.

```
type IAccountPlus =
  interface
    inherit IAccount
    abstract member Statement : Array ⟨Nat⟩
  end
```

Die Schnittstelle *IAccountPlus* bietet die Funktionalität von *IAccount*, deren Mitglieder »vererbt« werden, und offeriert darüber hinaus die Eigenschaft *Statement*. (Ein Kontoauszug ist der Einfachheit halber die Folge der letzten Kontostände — es geht uns an dieser Stelle nicht darum, das Bankenwesen möglichst wirklichkeitsgetreu zu erfassen.)

Das Objekt *ludwigs*, das wir in Abschnitt 8.1 definiert haben, lässt sich ohne großen Aufwand zu einem Plus-Konto erweitern. Wir ordnen lediglich die vorhandene Historie um, so dass der aktuelle Kontostand als Erstes aufgeführt wird.

```
let ludwigs : IAccountPlus =
  let size         = 10
  let history      = [| for k in 0 .. size − 1 → 0 |]
  let mutable i = 0
  let next ()      = (i + 1) % size
  {
    new IAccountPlus with
      member self.Deposit (amount : Nat) =
        history.[next ()] ← history.[i] + amount; i ← next ()
      member self.Withdraw (amount : Nat) =
        history.[next ()] ← monus (history.[i], amount); i ← next ()
      member self.Balance =
        history.[i]
      member self.Statement =
        [| for k in 0 .. size − 1 → history.[(size + i − k) % size] |]
  }
```

Wenn wir das erweiterte Konto verwenden, machen wir allerdings eine unliebsame Entdeckung. Der Aufruf

```
transfer (lisas, 1000, ludwigs)
```

wird von der statischen Semantik abgewiesen, da der Typ des formalen Parameters nicht mit dem Typ des aktuellen Parameters übereinstimmt, siehe Typregel für die Applikation (3.4) in Abschnitt 3.5.

$transfer : IAccount * Nat * IAccount \to Unit$

$ludwigs : IAccountPlus$

Der Typ von *IAccountPlus* ist nicht *gleich* dem Typ *IAccount*. Die dynamische Semantik ist weniger wählerisch: Der Ausdruck kann problemlos ausgerechnet werden, da *ludwigs* mehr Funktionalität als gefordert anbietet — *ludwigs* ist sozusagen überqualifiziert.

Mit anderen Worten, *IAccountPlus* und *IAccount* sind nicht zwei beliebige Typen, sondern sie stehen in einer engen Beziehung: Alle Elemente von *IAccountPlus* können als Elemente *IAccount* verwendet werden. In Anlehnung an die mathematische Teilmengenbeziehung nennen wir *IAccountPlus* einen ***Untertyp*** von *IAccount* und umgekehrt *IAccount* einen ***Obertyp*** von *IAccountPlus*. In eine Formel gegossen:

$IAccountPlus \preccurlyeq IAccount$

Das Typsystem von Mini–F# kann mit Hilfe von ***Untertypen*** flexibler gemacht werden. Die grundlegende Idee ist, dass ein Element eines Untertyps überall da verwendet werden kann, wo ein Element eines Obertyps verlangt wird. Mit Hilfe einer sogenannten ***Typanpassung*** (engl. type cast) lässt sich ein Element eines Untertyps in ein Element eines Obertyps überführen.

$transfer\ (lisas, 1000, ludwigs :> IAccount)$

Das Symbol »:>« deutet an, dass die »breitere« Schnittstelle von *ludwigs* auf die »schmalere« Schnittstelle *IAccount* verengt wird.

8.2.1. Abstrakte Syntax

Wir erweitern Schnittstellentypen um ***inherit*** Klauseln.

$d ::= \cdots$	***Deklarationen:***
$\mid$ ***type*** U =	erweiterte Definition eines Schnittstellentyps
interface	
inherit T_1	
inherit T_2	
abstract member $\ell : t$	
end	

Wie immer vereinfachen wir etwas: Tatsächlich dürfen beliebig viele ***inherit*** Klauseln aufgeführt werden und beliebig viele neue Mitglieder hinzukommen.

Wir erweitern Ausdrücke um Typanpassungen.

$e ::= \cdots$	***Ausdrücke:***
$\mid e :> t$	Typanpassung\Typeinschränkung

8.2.2. Statische Semantik

Gemäß dem Motto »Vertrauen ist gut, Kontrolle ist besser« überprüfen wir bei der Typanpassung $e :> t$, ob der Typ von e ein Untertyp von t ist, als Formel $t' \preccurlyeq t$.

$$\frac{\Sigma \vdash e : t' \qquad t' \preccurlyeq t}{\Sigma \vdash (e :> t) : t} \tag{8.1}$$

Eine Typanpassung geht in der Regel mit einem Informationsverlust einher. Wird die Schnittstelle eines Objekts verengt, so ist die Interaktion mit dem Objekt fürderhin eingeschränkt. (Ein Objekt ist die Summe seines Verhaltens.)

Die gute Nachricht ist, dass Typanpassungen auch automatisch vorgenommen werden (engl. automatic upcast).

$$\frac{\Sigma \vdash e : t \qquad t \preccurlyeq t'}{\Sigma \vdash e : t'} \tag{8.2}$$

Die sogenannte ***Subsumptionsregel*** fängt die Idee von Untertypen ein: ein Element eines Untertyps kann überall da verwendet werden, wo ein Element eines Obertyps verlangt wird. Die Subsumptionsregel wird zum Beispiel angewendet bei Funktionsaufrufen — wenn der Typ des aktuellen Parameters ein Untertyp des Typs des formalen Parameters ist — und bei der Zuweisung — wenn der Typ der rechten Seite ein Untertyp des Typs der linken Seite ist. Die schlechte Nachricht ist, dass die automatische Typanpassung nicht in voller Schönheit gelingt. Sie ist gewissen technischen Einschränkungen unterworfen, die der Tatsache geschuldet sind, dass F# die Typen von Ausdrücken *inferiert*. Einschränkungen, die wir im Folgenden aber ignorieren wollen. (Die Zweige einer Alternative stellen zum Beispiel eine Problemzone dar, insbesondere wenn die Ausdrücke unterschiedliche Typen besitzen.)

Wir müssen die Relation »$\preccurlyeq$« natürlich noch mit Leben füllen. Welche prinzipiellen Eigenschaften hat die Untertypbeziehung? Wie interagieren die Typkonstrukte, die wir bisher kennengelernt haben, mit Untertypen?

Quasiordnung Zunächst einmal ist die Untertypbeziehung eine ***Quasiordnung*** (siehe auch Abschnitt 5.1 und Anhang B.4): Sie ist ***reflexiv*** und ***transitiv***.

$$\frac{}{t \preccurlyeq t} \qquad \frac{t_1 \preccurlyeq t_2 \qquad t_2 \preccurlyeq t_3}{t_1 \preccurlyeq t_3}$$

Die Eigenschaften lassen sich im Zusammenspiel mit der Regel für die Typanpassung (8.1) motivieren. Reflexivität erlaubt eine triviale Typanpassung: Hat e den Typ t, dann ist $e :> t$ zulässig. Transitivität hilft, geschachtelte Typanpassungen zu vereinfachen: $(e :> t_2) :> t_3$ kann zu $e :> t_3$ verkürzt werden.

Schnittstellen Beziehungen zwischen Schnittstellentypen leiten sich direkt aus dem Programm ab; sie werden von dem/der Programmierer/-in *explizit* festgelegt. Aus der Typdefinition

```
type U =
  interface
    inherit T1
    inherit T2
    abstract member ℓ : t
  end
```

werden die folgenden Axiome abgeleitet:

$$\frac{}{\mathrm{U} \preccurlyeq \mathrm{T}_1} \qquad \frac{}{\mathrm{U} \preccurlyeq \mathrm{T}_2}$$

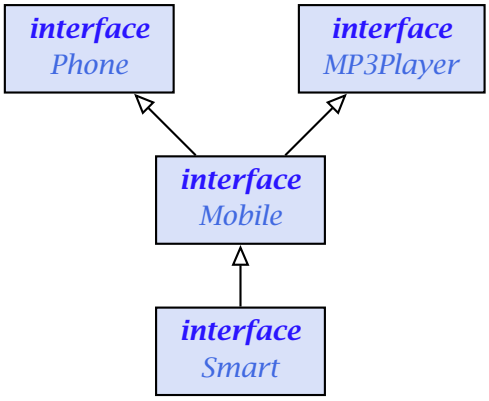
Die Schnittstelle U *vereinigt die Operationen* von T_1 und T_2 und fügt eine weitere hinzu. Damit liegen die Objekte von U im *Durchschnitt der Objekte* von T_1 und T_2. (Nachdenken!) Allgemein gilt: Je mehr Operationen eine Schnittstelle umfasst, desto weniger Objekte unterstützen die

```
type Phone =
  interface
    abstract member Dial : Nat → Unit              // Nummer wählen
  end
type MP3Player =
  interface
    abstract member Play : String → Unit           // MP3 abspielen
  end
type Mobile =
  interface
    inherit Phone
    inherit MP3Player
    abstract member Lookup : String → Nat          // Suche im Telefonbuch
    abstract member Call   : String → Unit         // Person anrufen
  end
type Smart =
  interface
    inherit Mobile
    abstract member Browse : String → Unit         // URL anzeigen
  end
let aPhone : Phone = …
let aMobile : Mobile = …
let aSmart : Smart = …
```

Abbildung 8.3.: Schnittstellenhierarchie: Geräte im Wandel der Zeit.

Schnittstelle. Diese Beobachtung ist übrigens nicht spezifisch für Mini–F# im Besonderen oder Programmiersprachen im Allgemeinen, sondern lässt sich auch im täglichen Leben machen:

Abbildung 8.3 zeigt einen Programmausschnitt, der elektrische und elektronische Geräte modelliert: Telefone mit Wählscheibe, MP3-Spieler, Mobiltelefone und Smartphones. Bezüglich ihrer Funktionalität sind die Geräte hierarchisch organisiert.



Ein Mobiltelefon vereinigt die Eigenschaften eines gusseisernen Telefons und eines MP3-Spielers; ein Smartphone fügt dem weitere Funktionalität hinzu. (Nehmen Sie den Programmcode nicht zu ernst — er dient lediglich dem Zweck, die Phänomene an einem weiteren Beispiel zu verdeutlichen.) Mit fast jedem Gerät lässt sich telefonieren: Möchte ich einen Anruf tätigen, kann ich das mit einem altmodischen Telefon tun oder mit einem modernen Smartphone. Bezüglich dieser Funktionalität unterscheiden sich die Geräte nicht (Sichtweise des abstrakten Datentyps). Natürlich sehen die Geräte anders aus und funktionieren ganz unterschiedlich (Sichtweise des konkreten Datentyps). Die Schnittstelle mit der geringsten Funktionalität enthält also die meisten Objekte. Je mehr Funktionalität ich einfordere, desto weniger Geräte stehen zur Auswahl: Möchte ich im Internet surfen, muss ich zum Smartphone greifen.

Paare Als Nächstes machen wir uns daran, »$\preccurlyeq$« auf strukturierten Typen wie zum Beispiel dem Paartyp $t_1 * t_2$ zu definieren. Die Regel für Paare legt fest, dass ein Paartyp Untertyp eines anderen Paartyps ist, wenn die jeweiligen Komponententypen in einer Untertypbeziehung stehen.

$$\frac{t_1 \preccurlyeq t_1' \qquad t_2 \preccurlyeq t_2'}{t_1 * t_2 \preccurlyeq t_1' * t_2'} \tag{8.3}$$

Warum ist das eine sinnvolle Festlegung? Um diese Frage zu beantworten ist es hilfreich, sich noch einmal ins Gedächtnis zu rufen, welche Operationen auf Paare angewendet werden können. Erhalte ich ein Paar, kann ich die Komponenten mit Hilfe der Projektionsfunktionen *fst* und *snd* extrahieren. Nach der Extraktion kann eine Typanpassung vorgenommen werden.

$$\frac{\dfrac{\vdots}{\Sigma \vdash e : t_1 * t_2}}{\dfrac{\Sigma \vdash fst\ e : t_1 \qquad \dfrac{\vdots}{t_1 \preccurlyeq t_1'}}{\Sigma \vdash fst\ e : t_1'}} \qquad \frac{\dfrac{\vdots}{\Sigma \vdash e : t_1 * t_2}}{\dfrac{\Sigma \vdash snd\ e : t_2 \qquad \dfrac{\vdots}{t_2 \preccurlyeq t_2'}}{\Sigma \vdash snd\ e : t_2'}}$$

Mit Hilfe der Paarregel (8.3) kann die Typanpassung alternativ zu dem Paar selbst verschoben werden. (Die Typanpassung und der Zugriff auf die Komponenten können im Programmtext ja tatsächlich weit auseinanderliegen.)

$$\frac{\dfrac{\vdots}{\Sigma \vdash e : t_1 * t_2} \qquad \dfrac{\dfrac{\vdots}{t_1 \preccurlyeq t_1'} \qquad \dfrac{\vdots}{t_2 \preccurlyeq t_2'}}{t_1 * t_2 \preccurlyeq t_1' * t_2'}}{\dfrac{\Sigma \vdash e : t_1' * t_2'}{\Sigma \vdash fst\ e : t_1'}} \qquad \frac{\dfrac{\vdots}{\Sigma \vdash e : t_1 * t_2} \qquad \dfrac{\dfrac{\vdots}{t_1 \preccurlyeq t_1'} \qquad \dfrac{\vdots}{t_2 \preccurlyeq t_2'}}{t_1 * t_2 \preccurlyeq t_1' * t_2'}}{\dfrac{\Sigma \vdash e : t_1' * t_2'}{\Sigma \vdash snd\ e : t_2'}}$$

Die obige Argumentation bewegt sich innerhalb der statischen Semantik. Nun soll die statische Semantik sicherstellen, dass die Auswertung fehlerfrei verläuft. Validieren wir die Paarregel also noch einmal aus dem Blickwinkel der dynamischen Semantik. In dem folgenden Programmfragment fehlt ein Teilausdruck vom Typ *Mobile* $*$ *Mobile*.

let (*mobile1*, *mobile2*) = ☐ *in* *mobile1*.*Call* ("Hannah"); *mobile2*.*Call* ("Lee")

Welcher Ausdruck kann in die Lücke eingesetzt werden, so dass die Nachricht *Call* jeweils verstanden wird? Da *Call* eine Methode der Schnittstelle *Mobile* ist, lässt sich problemlos ein Paar von Mobiltelefonen einsetzen. Wird ein Mobiltelefon durch ein Telefon ersetzt, schlägt die Auswertung fehl: Ein Telefon versteht die Nachricht *Call* nicht. Unproblematisch ist der »Upgrade« zu einem Smartphone: Dieses bietet zusätzliche Funktionalität an, versteht aber weiterhin die Nachricht *Call*. Kurzum: beide Komponenten des Paares müssen Elemente eines Untertyps von *Mobile* sein, so wie es die Subsumptionsregel (8.2) im Zusammenspiel mit der Paarregel (8.3) vorschreibt.

Funktionen Wenden wir uns Funktionen zu. In dem folgenden Programmfragment fehlt ein Teilausdruck vom Typ *Mobile* $\to$ *Mobile* (*aMobile* ist in Abbildung 8.3 definiert).

(☐ *aMobile*).*Call* ("Holly")

Wiederum die Frage: Welcher Ausdruck kann in die Lücke eingesetzt werden, ohne dass bei der Auswertung Probleme auftreten? Mit einem Ausdruck vom Typ *Mobile* $\to$ *Mobile* (»das Mobiltelefon wird repariert«) sind wir auf der sicheren Seite — die Anforderung wird präzise erfüllt. Die Funktion kann aber an Stelle eines Mobiltelefons auch ein Smartphone zurückgeben; ein Ausdruck vom Typ *Mobile* $\to$ *Smart* (»Upgrade«) ist zulässig. Diese Änderung betrifft den Ergebnistyp, wie sieht es mit dem Argumenttyp aus? Können wir eine Funktion des Typs *Smart* $\to$ *Mobile* einsetzen? Nein, das wird nicht gutgehen: Die Funktion fordert ein Smartphone, erhält aber nur ein Mobiltelefon — die Erwartung wird enttäuscht. Die Funktion kann aber weniger einfordern; ein Ausdruck vom Typ *Phone* $\to$ *Mobile* ist unproblematisch: Die Funktion erwartet nur ein altmodisches Telefon, erhält aber ein Mobiltelefon — die Erwartung wird übertroffen. Halten wir fest: Wird eine Funktion vom Typ $t_1' \to t_2'$ erwartet, dann können wir auch eine Funktion einsetzen, die weniger fordert (Obertyp von t_1') und mehr verspricht (Untertyp von t_2').[2]

$$\frac{t_1' \preccurlyeq t_1 \qquad t_2 \preccurlyeq t_2'}{t_1 \to t_2 \preccurlyeq t_1' \to t_2'} \tag{8.4}$$

Im Fachjargon sagt man: Der Funktionstyp ist

- ***kontravariant*** im Argumenttyp ($t_1' \preccurlyeq t_1$) und
- ***kovariant*** im Ergebnistyp ($t_2 \preccurlyeq t_2'$).

Die Vorsilbe »kontra« deutet an, dass sich die Richtung der Quasiordnung umkehrt. Im Gegensatz zum Funktionstyp ist der Paartyp kovariant in beiden Komponententypen.

Die Varianz des Funktionstyps lässt sich auch »herleiten«, wenn man sich anschaut, wie die Typregel für die Funktionsapplikation mit der Subsumptionsregel interagiert.

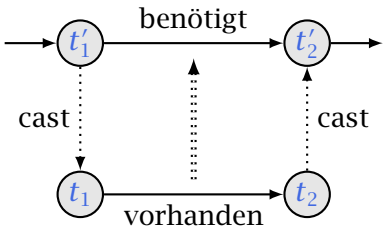
$$\dfrac{\dfrac{\dfrac{\vdots}{\Sigma \vdash e : t_1 \to t_2} \qquad \dfrac{\dfrac{\vdots}{\Sigma \vdash e_1 : t_1'} \qquad \dfrac{\vdots}{t_1' \preccurlyeq t_1}}{\Sigma \vdash e_1 : t_1}}{\Sigma \vdash e\ e_1 : t_2} \qquad \dfrac{\vdots}{t_2 \preccurlyeq t_2'}}{\Sigma \vdash e\ e_1 : t_2'}$$

[2] Das Phänomen ist uns bereits untergekommen, als wir Anforderungen und Garantien in Verträgen diskutiert haben (design by contract), siehe Abschnitt 5.2.4.

Anstatt erst das Funktionsargument und dann das Funktionsergebnis anzupassen, kann mit Hilfe der Funktionsregel (8.4) direkt die Funktion angepasst werden.

$$\dfrac{\dfrac{\dfrac{\vdots}{\Sigma \vdash e : t_1 \to t_2} \qquad \dfrac{\dfrac{\vdots}{t_1' \preccurlyeq t_1} \quad \dfrac{\vdots}{t_2 \preccurlyeq t_2'}}{t_1 \to t_2 \preccurlyeq t_1' \to t_2'}}{\Sigma \vdash e : t_1' \to t_2'} \qquad \dfrac{\vdots}{\Sigma \vdash e_1 : t_1'}}{\Sigma \vdash e\ e_1 : t_2'}$$

Das folgende Diagramm illustriert die Typanpassungen: Eine Funktion des Typs $t_1' \to t_2'$ kann über den Umweg $t_1 \to t_2$ konstruiert werden.



Die Richtung der Typanpassungen kehrt sich für Argument und Ergebnis um.

Wenn wir Funktionstypen schachteln, also Funktionen höherer Ordnung bilden, ergibt sich ein interessantes Bild:

$$\begin{gathered}
\mathit{Smart} \to \mathit{Smart} \preccurlyeq \mathit{Smart} \to \mathit{Phone} \\
\mathit{Phone} \to \mathit{Smart} \preccurlyeq \mathit{Smart} \to \mathit{Smart} \\
\mathit{Phone} \to \mathit{Smart} \preccurlyeq \mathit{Smart} \to \mathit{Phone} \\
(\mathit{Smart} \to \mathit{Phone}) \to \mathit{Smart} \preccurlyeq (\mathit{Phone} \to \mathit{Smart}) \to \mathit{Phone} \\
((\mathit{Phone} \to \mathit{Smart}) \to \mathit{Phone}) \to \mathit{Smart} \preccurlyeq ((\mathit{Smart} \to \mathit{Phone}) \to \mathit{Smart}) \to \mathit{Phone}
\end{gathered}$$

In dem Typ $((t_1 \to t_2) \to t_3) \to t_4$ stehen t_1 und t_3 an kontravarianten Positionen und t_2 und t_4 an kovarianten Positionen. Die Richtung der Quasiordnung wechselt mit jeder Schachtelung im Argumenttyp.

Speicherzellen Wenden wir uns dem nächsten Typ zu: den Speicherzellen. Zur Erinnerung: Eine Speicherzelle kann mit »!« gelesen und mit »:=« geschrieben werden. Starten wir die Diskussion mit einem kleinen Quiz: Gelingt die Auswertung des folgenden Ausdrucks?

```
let mobile-case : Ref ⟨Mobile⟩ = ref aMobile
let phone-box   : Ref ⟨Phone⟩  = mobile-case
phone-box := aPhone
(!mobile-case).Play ("Siberian Khatru")
```

Wir allokieren eine Speicherzelle vom Typ *Ref ⟨Mobile⟩* und geben diese in der zweiten Zeile als Speicherzelle vom Typ *Ref ⟨Phone⟩* aus. Beachten Sie, dass keine zweite Speicherzelle angelegt wird: *phone-box* ist lediglich ein ***Alias***, ein anderer Name, für *mobile-case*. In der Speicherzelle *phone-box* wird sodann ein Telefon abgelegt. Schließlich nimmt das Unglück seinen Lauf: Dem Inhalt von *mobile-case* alias *phone-box* wird die Nachricht *Call* geschickt. Was läuft schief?

In den Zeilen 1, 3 und 4 wird jeweils »typkonform« gearbeitet, nur in der 2. Zeile kommen Untertypen ins Spiel. Das Programm zeigt, dass *Ref ⟨Mobile⟩* *kein* Untertyp von *Ref ⟨Phone⟩* ist, obwohl *Mobile* ein Untertyp von *Phone* ist! Gehen wir der Ursache auf den Grund. In dem folgenden Programmfragment fehlt ein Teilausdruck vom Typ *Ref ⟨Mobile⟩*.

(!□).*Call* ("Hannah")

Die Lücke können wir mit ***ref*** *aMobile*, aber auch mit ***ref*** *aSmart* füllen. Mit anderen Worten, der lesende Speicherzugriff ist kovariant. Wie sieht es mit dem schreibenden Speicherzugriff aus?

□ := *aMobile*

Jetzt können wir einen Ausdruck vom Typ $Ref\ \langle Mobile \rangle$, aber auch einen vom Typ $Ref\ \langle Phone \rangle$ in die Lücke setzen. Der schreibende Speicherzugriff ist also kontravariant.

Der Lesezugriff ist kovariant; der Schreibzugriff ist kontravariant; da Speicherzellen beide Zugriffsarten unterstützen, sind sie summa summarum ***invariant***.

$$\frac{t \preccurlyeq t' \qquad t' \preccurlyeq t}{Ref\ \langle t \rangle \preccurlyeq Ref\ \langle t' \rangle}$$

Der Typ $Ref\ \langle t \rangle$ ist ein Untertyp von $Ref\ \langle t' \rangle$, wenn t und t' äquivalent sind, die Typen wechselseitig austauschbar sind. In Mini–F# bedeutet dies, dass t und t' tatsächlich *identisch* sein müssen. Entsprechendes gilt für alle modifizierbaren Datenstrukturen (engl. mutable data structures) wie zum Beispiel Arrays. Zur Erinnerung: Die Elemente eines Arrays können mit $a.[i] \leftarrow e$ überschrieben werden.

Die Varianz des lesenden und des schreibenden Speicherzugriffs lässt sich auch aus dem Zusammenspiel der Subsumptionsregel mit den Typregeln für die Dereferenzierung »!« und die Zuweisung »:=« ablesen.

$$\frac{\dfrac{\dfrac{\vdots}{\Sigma \vdash e : Ref\ \langle t \rangle}}{\Sigma \vdash\ !e : t} \qquad \dfrac{\vdots}{t \preccurlyeq t'}}{\Sigma \vdash\ !e : t'} \qquad\qquad \frac{\dfrac{\vdots}{\Sigma \vdash e_1 : Ref\ \langle t \rangle} \qquad \dfrac{\dfrac{\vdots}{\Sigma \vdash e_2 : t'} \qquad \dfrac{\vdots}{t' \preccurlyeq t}}{\Sigma \vdash e_2 : t}}{\Sigma \vdash (e_1 := e_2) : Unit}$$

Beim lesenden Zugriff müssen wir $t \preccurlyeq t'$ voraussetzen, beim schreibenden Zugriff die gespiegelte Inklusion $t' \preccurlyeq t$.

Ein Gedankenexperiment: Unterschiede man mit Hilfe des Typsystems zwischen lesendem und schreibendem Zugriff — was weder Mini–F# noch F# machen — ergäbe sich ein verfeinertes Bild.

$$\frac{\Sigma \vdash e : t}{\Sigma \vdash \textbf{\textit{ref}}\ e : Ref\ \langle t \rangle}$$

$$\frac{\Sigma \vdash e : Read\text{-}Ref\ \langle t \rangle}{\Sigma \vdash\ !e : t} \qquad\qquad \frac{\Sigma \vdash e_1 : Write\text{-}Ref\ \langle t \rangle \qquad \Sigma \vdash e_2 : t}{\Sigma \vdash e_1 := e_2 : Unit}$$

Wir verwenden drei (!) verschiedene Typen für Speicherzellen: $Read\text{-}Ref\ \langle t \rangle$ ist der Typ einer »read-only« Speicherzelle; $Write\text{-}Ref\ \langle t \rangle$ ist der Typ einer »write-only« Speicherzelle; und $Ref\ \langle t \rangle$ ist unverändert der Typ einer Speicherzelle, die sowohl les- als auch schreibbar ist. Da wir beide Aspekte getrennt modellieren, können wir festlegen:

$$\frac{t' \preccurlyeq t}{Read\text{-}Ref\ \langle t' \rangle \preccurlyeq Read\text{-}Ref\ \langle t \rangle} \qquad\qquad \frac{t \preccurlyeq t'}{Write\text{-}Ref\ \langle t' \rangle \preccurlyeq Write\text{-}Ref\ \langle t \rangle}$$

Der Typ $Read\text{-}Ref\ \langle t \rangle$ ist kovariant; $Write\text{-}Ref\ \langle t \rangle$ hingegen kontravariant; $Ref\ \langle t \rangle$ ist der Durchschnitt von $Read\text{-}Ref\ \langle t \rangle$ und $Write\text{-}Ref\ \langle t \rangle$.

$$\frac{}{Ref\ \langle t \rangle \preccurlyeq Read\text{-}Ref\ \langle t \rangle} \qquad\qquad \frac{}{Ref\ \langle t \rangle \preccurlyeq Write\text{-}Ref\ \langle t \rangle}$$

Eine les- und schreibbare Speicherzelle lässt sich zu einer read-only oder einer write-only Speicherzelle herabstufen. Einem Ausdruck kann auf diese Weise ein genauerer Typ zugeordnet werden, genauer und flexibler. Die Sinnhaftigkeit von read-only Speicherzellen erschließt sich einem

unmittelbar; unsere Bankkonten realisieren im Prinzip nichts anderes: Der Kontostand kann direkt mit *Balance* gelesen, aber nicht überschrieben werden. Aber wozu sind write-only Speicherzellen gut? Denken Sie an die Implementierung der Fakultät aus Abschnitt 7.2, die ihr Ergebnis über eine Speicherzelle kommuniziert (engl. destination passing style). *Ende des Gedankenexperiments.*

8.2.3. Dynamische Semantik

Die Auswertung von Programmen ändert sich nicht.

$$\frac{\delta \vdash e \Downarrow \nu}{\delta \vdash (e :> t) \Downarrow \nu}$$

Typanpassungen spielen für die Abarbeitung keine Rolle.

8.2.4. Vertiefung

Untertypen sind eine Spielart der ***Polymorphie***. Erinnern wir uns: Der Name Polymorphie kommt aus dem Griechischen (πολυμορφια) und bedeutet Vielgestaltigkeit. Im Kontext von Programmiersprachen meint Polymorphie, dass ein Wert in unterschiedlichen Typkontexten verwendet werden kann. *Kurz:* ein Wert hat mehrere Typen.

Die polymorphe Funktion $length : List\ \langle 'a \rangle \to Nat$ kann zum Beispiel die Länge einer Liste eines beliebigen Elementtyps bestimmen; sie besitzt im Prinzip unendlich viele Typen.

$length : List\ \langle Nat \rangle \to Nat$
$length : List\ \langle Bool \rangle \to Nat$
$length : List\ \langle List\ \langle Nat \rangle \rangle \to Nat$
$length : List\ \langle List\ \langle Bool \rangle \rangle \to Nat$
…

Da *length* einen heimlichen Typparameter hat, spricht man auch genauer von einer ***parametrisch polymorphen Funktion*** oder etwas weniger sperrig von einer ***generischen Funktion*** (engl. generic function).

Die Funktion *transfer* ist ebenfalls polymorph; sie kann auf Elemente eines beliebigen Untertyps von *IAccount* angewendet werden.

$transfer : IAccount * Nat * IAccount \to Unit$
$transfer : IAccount * Nat * IAccountPlus \to Unit$
$transfer : IAccountPlus * Nat * IAccount \to Unit$
$transfer : IAccountPlus * Nat * IAccountPlus \to Unit$
…

Die Zahl der Untertypen von *IAccount* ist zwar endlich, aber unbegrenzt, da die Schnittstellenhierarchie zu jedem Zeitpunkt beliebig erweitert werden kann. Statt von Untertyppolymorphie spricht man aus diesem Grund auch von Schnittstellenvererbung (engl. interface inheritance).

Insgesamt unterscheidet man zwischen vier verschiedenen Arten von Polymorphie, siehe Abbildung 8.4. Zu den beiden prinzipiellen oder universellen Spielarten gesellen sich noch zwei weniger prinzipielle Formen, Überladung und Konversion, die wir im Folgenden kurz unter die Lupe nehmen wollen.

	universelle Polymorphie	ad-hoc Polymorphie
konjunktive Polymorphie	parametrische Polymorphie ($\forall$) (engl. generics) *length*	Überladung ($\wedge$) (engl. overloading) =, +
Inklusionspolymorphie	Untertypen ($\preccurlyeq$) (engl. subtyping) *transfer*	Konversion (engl. coercion) —

Abbildung 8.4.: Spielarten der Polymorphie.

Überladung Von ***Überladung*** (engl. overloading) spricht man, wenn der *gleiche* Bezeichner für *unterschiedliche* Funktionen bzw. allgemeiner für unterschiedliche Werte verwendet wird. In Mini–F# wird zum Beispiel »+« sowohl für die Addition von natürlichen Zahlen (4711 + 815), die Addition von Fließkommazahlen (8.15 + 0.4711e2), als auch für die Konkatenation von Strings (`"Hello, "` + `"world!"`) verwendet.

$(+) : \mathit{Nat} \to \mathit{Nat} \to \mathit{Nat}$
$(+) : \mathit{float} \to \mathit{float} \to \mathit{float}$
$(+) : \mathit{String} \to \mathit{String} \to \mathit{String}$

Überladung ist die kleine Schwester der parametrischen Polymorphie. Ähnlich wie *length*, kann »+« auf Argumente unterschiedlichen Typs angewendet werden. Im Unterschied zu *length* wird die Operation aber jeweils ganz unterschiedlich implementiert; hinter den Kulissen ist jeweils eine andere Funktion am Werk. Im Gegensatz dazu wird im Fall von *length* unabhängig vom Typ immer der gleiche Programmcode ausgeführt (»one size fits all«).

Erinnern wir uns: Wir haben in Abschnitt 4.2.2 die natürlichen Zahlen auf zwei verschiedene Art und Weisen implementiert, einmal auf Grundlage des unären Zahlensystems (*Peano*) und ein zweites Mal auf Grundlage des binären Zahlensystems (*Leibniz*). Je nach konkreter Zahlenrepräsentation wird die Addition unterschiedlich umgesetzt. Dies gilt in gleicher Weise auch für andere Zahlentypen: Zahlen mit beschränkter Genauigkeit (Maschinenzahlen mit ihrer modularen Arithmetik), Fließkommazahlen, rationale Zahlen, komplexe Zahlen usw. Natürlich ist es naheliegend, sogar wünschenswert, jeweils das Symbol »+« zu verwenden, da allen Operationen ja gemeinsam ist, dass sie das mathematische Konzept der Addition umsetzen.

Ebenso wünschenswert wäre es natürlich, auch für numerische Konstanten, etwa die Zahl Null, jeweils das gleiche Symbol verwenden zu können. Das ist leider nicht erlaubt. Je nach Typ unterscheidet sich die lexikalische Syntax von Numeralen: 0 ist eine natürliche Zahl (*Nat*), 0.0 ist eine 64-Bit Fließkommazahl (*float*, doppelte Genauigkeit, engl. double precision). Für »ähnliche« Zahlentypen wird der Typ durch einen Suffix angezeigt: $0y$ ist eine vorzeichenbehaftete 8-Bit Zahl (*sbyte*), $0.0f$ ist eine 32-Bit Fließkommazahl (*float32*, einfache Genauigkeit, engl. single precision).[3]

Wie bereits angesprochen, kann »+« auch für die Konkatenation von Strings verwendet werden. Eine Verwendung, die aus dem Rahmen fällt und den ad-hoc Charakter der Überladung unterstreicht. Die Addition von Zahlen und die Konkatenation von Strings haben wenig gemeinsam — beide Operationen sind assoziativ und haben ein neutrales Element (sie formen einen Monoid), aber das gilt auch für die Multiplikation von Zahlen, die Komposition von Funktionen usw.

[3] Da F# von Haus aus keine natürlichen Zahlen kennt, bezeichnet 0 in Wirklichkeit eine ganze Zahl (*Int*); natürliche Zahlen werden mit dem Suffix N gekennzeichnet: 0N.

(Übrigens verwendet man in der Mathematik für die Konkatenation in der Regel kein additives, sondern ein multiplikatives Symbol: $s_1 \cdot s_2$. Auch in der Mathematik ist Überladung beliebt: Wir haben »·« sowohl für die Konkatenation von Wörtern als auch für die Konkatenation von Sprachen verwendet.)

Die ad-hoc Natur der Überladung wird ebenfalls deutlich, wenn wir überladene Funktionen komponieren: ***fun*** $x \rightarrow x + x$. Wird hier eine Zahl verdoppelt oder ein String mit sich selbst konkateniert? Unterschiedliche Programmiersprachen reagieren unterschiedlich auf diese *Mehrdeutigkeit*. In F# wird willkürlich angenommen, dass eine ganze Zahl verdoppelt wird: $Int \rightarrow Int$. Alternativ könnte der Ausdruck durch die statische Semantik zurückgewiesen werden, da die Mehrdeutigkeit nicht aufgelöst werden kann. Die Funktion ***fun*** $x \rightarrow x$ + "?" hingegen ist unproblematisch, da das zweite Argument die Mehrdeutigkeit behebt. Diese Problematik ist parametrisch polymorphen Funktionen nicht zu eigen: ***fun*** *xs* → *length xs* > 0 hat den Typ $List\ \langle 'a \rangle \rightarrow Bool$ und erbt sozusagen die Flexibilität in der Anwendung von *length*. Parametrische Polymorphie ist universeller, weniger ad hoc.

Die bisherige Diskussion rankt sich um die *vordefinierte* Operation »+«; können überladene Funktionen auch selbst definiert werden? Die Antwort ist ein entschiedenes »Jein«. Bezeichner als überladen zu kennzeichnen ist nicht möglich, allerdings dürfen Methodennamen überladen werden. In der folgenden Schnittstelle ist die Methode *Push* überladen.

```
type IStack⟨'elem⟩ =
  interface
    abstract member IsEmpty : Bool
    abstract member Push    : 'elem → Unit
    abstract member Push    : List⟨'elem⟩ → Unit
    abstract member Pop     : Unit → 'elem
    abstract member Top     : 'elem
  end
```

Mit *Push* kann sowohl ein einzelnes Element als auch alle Elemente einer Liste auf einen Stack abgelegt werden. Wie schon angesprochen, führen überladenene Bezeichner unter Umständen zu Mehrdeutigkeiten. Aus diesem Grund müssen sich die *Argumenttypen* der überladenen Methoden unterscheiden. Zwei gleichnamige Methoden mit gleichen Argumenttypen, aber unterschiedlichen Ergebnistypen sind nicht erlaubt.

Wir werden von diesem Feature allerdings keinen Gebrauch machen. Bei der Verwendung von Überladung sollte man stets bedenken, dass nicht nur der Übersetzer Mehrdeutigkeiten auflösen muss, sondern auch menschliche Leser/-innen eines Programms. Statt *Push* zu überladen, kann man im obigen Beispiel auch ohne allzu großen Komfortverlust *Push* und *PushMany* verwenden. Pointierter formuliert: Wer überladene Bezeichner einführt, ist nur zu faul, sich unterschiedliche Namen auszudenken. (Das trifft insbesondere auf den Autor des Skripts zu, der »·« sowohl für die Konkatenation von Wörtern als auch für die Konkatenation von Sprachen verwendet.)

Konversion Von ***Konversion*** (engl. coercion) spricht man, wenn ein Element eines Typs automatisch in ein Element eines anderen Typs umgewandelt wird. In vielen Programmiersprachen wird diese Bequemlichkeit für numerische Typen angeboten: *int*s werden zum Beispiel automatisch in *float*s überführt. Der Repräsentationswechsel kann unter Umständen mit einem Informationsverlust einhergehen. Aus diesem Grund wird Konversion in Mini-F# *nicht* unterstützt. Um eine ganze Zahl in eine Fließkommazahl zu konvertieren oder umgekehrt eine Fließkommazahl in eine ganze Zahl, muss eine Funktion aufgerufen werden — die Funktion heißt wie der Zieltyp der Umwandlung.

```
>>> float32 123456789
val it : float32 = 123456792.0f
>>> int it
val it : int = 123456792
```

Da eine 32-Bit Fließkommazahl nur 24+1 Bits für die Mantisse (und 8 Bits für den Exponenten) zur Verfügung hat, kann ein 32-Bit Integer in der Regel nicht ohne Genauigkeitsverlust repräsentiert werden. Auch in der umgekehrten Richtung kann man böse Überraschungen erleben,

```
>>> int 1e10f
val it : int = -2147483648
>>> float32 it
val it : float32 = -2147483650f
```

etwa wenn eine sehr große positive Zahl plötzlich negativ wird.

Konversion ist die kleine Schwester des Untertyppolymorphismus. Eine Typumwandlung ließe sich durch eine Untertypregel einfangen.

```
int ≤ float
```

Da diese »Inklusion« tatsächlich mit einem Wandel der Repräsentation einhergeht, müssten in der Folge sämtliche Auswertungsregeln für arithmetische Operationen angepasst werden! Aber, wie gesagt, Konversion wird in Mini–F# *nicht* unterstützt.

8.3. Klassen

Ein Bankinstitut, eine Sammlung von Bankkonten, kann alternativ durch eine sogenannte ***Klasse*** (engl. class) modelliert werden.

module Objects.Bank

```
type TrustMe (seed : Nat) =
  class
    let mutable funds = seed
    member self.Deposit (amount : Nat) =
      funds ← funds + amount
    member self.Withdraw (amount : Nat) =
      funds ← monus (funds, amount)
    member self.Balance =
      funds
  end
```

Die Definition sieht einem Objektkonstruktor sehr ähnlich: der interne Zustand, die Veränderliche *funds* wird mit Hilfe einer ***let***-Bindung eingeführt; daneben sind die uns mittlerweile schon vertrauten Methoden *Deposit*, *Withdraw* und *Balance* aufgeführt, die den internen Zustand manipulieren.

Ein Unterschied fällt allerdings ins Auge: *TrustMe* wird durch eine *Typ*definition eingeführt, nicht durch eine *Werte*definition. Klassendefinitionen sind die fünfte und letzte Spielart von Typen, die wir einführen, so dass an dieser Stelle ein kurzer Rück- bzw. Überblick angezeigt ist:

- ***type*** T = { $\ell_1 : t_1, \ldots$ }
  führt einen Recordtyp ein;

- ***type*** T = | C_1 ***of*** t_1 | ⋯
  führt einen Variantentyp ein;

- ***type*** T = ***interface abstract member*** ℓ_1 : t_1 … ***end***
  führt eine Schnittstelle ein;

- ***type*** T = ***class let*** … ***member*** … ***end***
  führt eine Klasse ein;

- ***type*** T = t
  führt ein Typsynonym ein, einen anderen Namen für t.

Kommen wir auf die Definition von *TrustMe* zurück. Etwas ungewöhnlich für eine Typdefinition hat *TrustMe* einen Werteparameter ähnlich wie eine Funktion — einen *Werte*parameter, nicht einen *Typ*parameter. Wie wir sehen werden, ist eine Klasse tatsächlich ein Zwitterwesen: *TrustMe* ist sowohl ein Typ, genauer: eine Schnittstelle, als auch ein Wert, der die Schnittstelle implementiert, ein Objektkonstruktor, der sogenannte ***primäre Konstruktor*** (engl. ***primary constructor***). Damit ist vielleicht klar, dass die Typdefinition nicht unmittelbar ausgewertet wird. Selbst wenn wir die Definition als Funktion lesen, fehlt ja die Angabe des Startkapitals *seed*.

Objekterzeugung Ein Bankkonto wird eröffnet, indem wir *TrustMe* mit einem Parameter versorgen: Mit *TrustMe* 4711 wird ein neues Konto eröffnet, in das ein initialer Betrag von 4711 € eingezahlt wird. Wenn man betonen möchte, dass ein *neues* Objekt erschaffen wird, kann man auch ***new*** *TrustMe* 4711 schreiben.

```
⋙ let lisas = TrustMe 4711
val lisas : TrustMe
⋙ lisas.Deposit 815
()
⋙ lisas.Balance
5526
⋙ let ludwigs = new TrustMe 815
val ludwigs : TrustMe
```

Etwas Fachjargon: Statt »*TrustMe* 4711 ist ein Element des Typs *TrustMe*« sagt man im Jargon »*TrustMe* 4711 ist eine Instanz der Klasse *TrustMe*«. Klassen sind wie gesagt Zwitterwesen: *TrustMe* 4711 ist ein normaler Ausdruck und kann überall dort verwendet werden, wo Ausdrücke gefragt sind (der Ausdruck muss nicht notwendigerweise an einen Bezeichner gebunden werden); wird der Ausdruck abgearbeitet, entsteht ein Objekt des angegebenen Typs. Allgemein lässt sich eine Klassendefinition ***type*** T (*x*) = ***class*** … ***end*** als Schablone (engl. template) auffassen; mit ***new*** T *e* oder kurz T *e* wird die Schablone instantiiert; das Ergebnis ist ein Objekt vom Typ T.

Felder, Methoden und Eigenschaften Es ist hilfreich, die Klassendefinition dem entsprechenden Objektkonstruktor aus Abschnitt 8.1 gegenüberzustellen.

```
let account seed =

  let mutable funds = seed
  {new IAccount with
    member self.Deposit amount =
      funds ← funds + amount
    member self.Withdraw amount =
      funds ← monus (funds, amount)
    member self.Balance =
      funds
  }
let lisas = account 4711
lisas.Deposit 815
```

```
type TrustMe seed =
  class
    let mutable funds = seed

    member self.Deposit amount =
      funds ← funds + amount
    member self.Withdraw amount =
      funds ← monus (funds, amount)
    member self.Balance =
      funds
  end
let lisas = TrustMe 4711
lisas.Deposit 815
```

In der praktischen Handhabung unterscheiden sich die Ansätze zunächst einmal nicht. (Wir werden in Abschnitt 8.3.1 sehen, dass sich tatsächlich Unterschiede ergeben, was die Interaktion mit anderen Objekten anbelangt.) Der wesentliche Unterschied ist ein syntaktischer oder wenn man möchte ein organisatorischer: Der interne Zustand und die nach außen sichtbare Schnittstelle rücken in der Klassendefinition enger zusammen; sie werden unter dem Dach der ***class*** … ***end*** Klammer zusammengefasst.

Neben Definitionen von (veränderlichen) Werten, Methoden und Eigenschaften lassen sich in eine Klassendefinition weitere Aspekte integrieren, für die wir in Abschnitt 8.1 ein Modul verwendet haben. (Wir haben schon angedeutet, dass Modul- und Klassensysteme in einer gewissen Konkurrenz stehen, so dass es vielleicht nicht verwundert, dass es eine nicht unerhebliche Überschneidung von Sprachfeatures gibt.) Das sind Aspekte, die das Bankinstitut als Ganzes betreffen, nicht nur ein einzelnes Bankkonto: Wie lautet der BIC? Wieviele Konten sind insgesamt eröffnet worden? Abbildung 8.5 zeigt, wie der modulbasierte Programmcode aus Abbildung 8.1 für Klassen umgeschrieben wird. (Für das Verständnis der folgenden Diskussion ist es ratsam, noch einmal zurückzublättern und Abbildung 8.1 zu studieren.) Im Vergleich zum modulbasierten Code wird kein Studierendenkonto (*student-account*) angeboten — darauf kommen wir in Abschnitt 8.5 noch einmal zurück.

Im modulbasierten Programm werden zwei Veränderliche eingeführt: Die Gesamtzahl der Konten wird in *no* abgelegt, der Kontostand bzw. die Kontostände in *funds*. Die Speicherzelle *no* wird bei der Abarbeitung des Moduls angelegt und ist (fast) im gesamten Modul sichtbar. Anders verhält es sich mit *funds*: Bei jedem Aufruf von *account* wird eine neue Speicherzelle allokiert; der Bezeichner *funds* ist nur lokal in der Funktion sichtbar. Die Position der Bezeichner im Programmtext macht deutlich, dass *no* genau einmal existiert, wohingegen *funds* einmal pro erzeugtem Objekt existiert. In der klassenbasierten Variante werden die Definitionen der Speicherzellen zusammengeführt; sowohl *no* als auch *funds* werden lokal innerhalb der Klasse definiert. Der unterschiedliche Charakter der Speicherzellen muss aus diesem Grund mit anderen linguistischen Mitteln ausgedrückt werden: Das Schlüsselwort ***static***[4] zeigt an, dass *no* nur einmal pro Klasse existiert. Im Fachjargon sagt man auch, *no* ist eine ***Klassenvariable***. Bei der Definition von *funds* fehlt hingegen das Schlüsselwort: Somit existiert *funds* einmal pro mit ***new*** erzeugtem Objekt. Im Unterschied zu *no* ist *funds* eine sogenannte ***Instanzvariable***.

[4] Der Name ist historisch bedingt: Mit ***static*** werden in der Programmiersprache C Variablen gekennzeichnet, die statisch vor der Programmausführung und nicht dynamisch während der Programmausführung (auf dem Stack oder mit `malloc()` auf dem Heap) allokiert werden.

```
type TrustMe (seed : Nat) =
  class
    static do putline "TrustMe is founded."
    static let mutable no = 0
    do no ← no + 1
    let mutable funds = seed
    static member BIC = 4711
    static member total-no-of-accounts = no
    member self.Deposit (amount : Nat) =
      funds ← funds + amount
    member self.Withdraw (amount : Nat) =
      funds ← monus (funds, amount)
    member self.Balance =
      funds
  end
```

Abbildung 8.5.: Modellierung eines Bankinstituts (klassenbasiert, siehe auch Abbildungen 8.1 und 8.8).

Ähnliche Überlegungen gelten für die Abarbeitung der mit ***do*** gekennzeichneten Ausdrücke. (Zur Erinnerung: ***do*** *e* ist eine Abkürzung für ***let*** () = *e* und kennzeichnet eine Definition, die nur um ihres Effektes willen eingeführt wird.) In der modulbasierten Variante bestimmt die Position, wie oft ein Ausdruck ausgewertet wird, in der klassenbasierten Variante das Schlüsselwort ***static***. Also, ein ***static do*** Block wird einmal bei der Abarbeitung der Klassendefinition (!) ausgeführt. Fehlt das Schlüsselwort, wird der Block einmal bei jeder Erzeugung eines Objekts ausgeführt.

Die bisherige Diskussion betrifft die interne Organisation einer Klasse bzw. von Objekten einer Klasse. Kommen wir zur externen »Präsentation«, der Schnittstelle. Diese umfasst zwei »Arten« von Methoden und Eigenschaften: solche, die spezifisch für die Klasse sind, und solche, die spezifisch für ein einzelnes Objekt sind. Zu den ersteren gehören der BIC und die Auskunft über die Gesamtzahl der Konten. In der modulbasierten Variante werden diese Bezeichner auf Modulebene definiert, also *nicht* lokal zum Objektkonstruktor *account*. Die klassenbasierte Variante kennzeichnet sie erwartungsgemäß mit dem Schlüsselwort ***static***. Man spricht auch von ***Klassenmethoden*** und ***Klasseneigenschaften***. Beide können unabhängig von der Existenz eines Objekts, sprich eines Bankkontos, verwendet werden — zum Zeitpunkt der Gründung einer Bank existieren noch keine Konten. Die jeweilige Nachricht wird an die Klasse in unserem Beispiel an die Bank geschickt.

```
>>> TrustMe.BIC
4711
>>> let lisas = TrustMe 4711
val lisas : TrustMe
>>> TrustMe.total-no-of-accounts
1
```

Kommen wir zur Sichtbarkeit von Bezeichnern: Welcher Bezeichner ist wo sichtbar? Die Regeln für die klassenbasierte Variante lassen sich aus der modulbasierten Variante ableiten: Zum

Beispiel ist *funds* in *Withdraw*, nicht aber in *total-no-of-accounts* sichtbar. Allgemein gilt, dass Instanzvariablen und -methoden nicht in den Definitionen von Klassenvariablen und -methoden sichtbar sind. Von außen betrachtet sind mit ***let*** eingeführte Konstanten, Funktionen und Veränderliche privat, das heißt *nicht* sichtbar und damit nicht zugreifbar; mit ***member*** eingeführte Methoden und Eigenschaften sind hingegen öffentlich, das heißt sichtbar und damit zugreifbar. Letzteres kann man verhindern, wenn man Mitglieder als ***private*** kennzeichnet. Dies ist nützlich, sogar angezeigt, um Implementierungsdetails zu verbergen. Zum Beispiel würde man eine Methode verbergen, die den Charakter einer Hilfsfunktion hat: Sie arbeitet anderen Methoden zu, soll aber nach außen nicht in Erscheinung treten.

Verschaffen wir uns einen Überblick über die Komponenten einer Klassendefinition.

- ***let*** *a* = *e*
  führt eine Konstante ein, einen Bezeichner für einen Wert (diese Konstante kann allerdings die Adresse einer Speicherzelle sein: ***let*** *funds* = ***ref*** *seed*). Die Bindung wird bei der Erzeugung eines Objekts mit ***new*** ausgewertet. Eine Konstante ist stets privat und kann nicht öffentlich gemacht werden.

- ***let*** *f x* = *e*
  führt eine Funktion ein. Eine Funktion ist stets privat.

- ***let mutable*** *s* = *e*
  führt eine Instanzvariable ein, auch ***Feld***[5] (engl. field) genannt. Auch eine Instanzvariable ist stets privat.

- ***do*** *e*
  kennzeichnet einen Ausdruck, der bei der Erzeugung eines Objekts mit ***new*** ausgeführt wird.

- ***member*** *self*.*p* ***with*** *get* () = e_1 ***and*** *set v* = e_2
  member *self*.*p* ***with private*** *get* () = e_1 ***and*** *set v* = e_2
  führt eine Eigenschaft ein; es kann auch nur der Getter bzw. nur der Setter angegeben werden. Eigenschaften sind öffentlich; die Sichtbarkeit kann aber mit ***private*** selektiv eingeschränkt werden.

- ***member*** *self*.*m x* = *e*
  member private *self*.*m x* = *e*
  führt eine Methode ein. Methoden sind ebenfalls öffentlich, es sei denn, die Sichtbarkeit wird mit ***private*** eingeschränkt.

- ***static let*** *a* = *e*
  führt eine »Klassenkonstante« ein. Die Bindung wird bei der Abarbeitung der Klassendefinition ausgewertet; in *e* sind nur mit ***static*** gekennzeichnete Bezeichner sichtbar. Eine Konstante ist stets privat.

- ***static let*** *f x* = *e*
  führt eine »Klassenfunktion« ein. Im Rumpf *e* sind nur mit ***static*** gekennzeichnete Bezeichner sichtbar. Eine Funktion ist stets privat.

- ***static let mutable*** *s* = *e*
  führt eine Klassenvariable ein. Auch eine Klassenvariable ist stets privat.

[5] Der Begriff »Feld« wird auch für Array verwendet. Das eine hat mit dem anderen nichts zu tun.

- ***static do*** *e*
  kennzeichnet einen Ausdruck, der bei der Abarbeitung der Klassendefinition ausgeführt wird. In *e* sind nur mit ***static*** gekennzeichnete Bezeichner sichtbar.

- ***static member*** *p* ***with*** *get* () = e_1 ***and*** *set* v = e_2
  static member *p* ***with private*** *get* () = e_1 ***and*** *set* v = e_2
  führt eine Klasseneigenschaft ein. Auf die Eigenschaft wird über den Klassennamen zugegriffen. Auch Klasseneigenschaften sind öffentlich; die Sichtbarkeit kann aber mit ***private*** eingeschränkt werden.

- ***static member*** *m x* = *e*
  static member private *m x* = *e*
  führt eine Klassenmethode ein. Eine Klassenmethode ist der Natur nach eine ordinäre Funktion; lediglich der Aufruf erfolgt über den Klassennamen.

8.3.1. Klassen und Schnittstellen

Eine Klasse besteht aus einer öffentlichen Schnittstelle, der Sammlung aller öffentlichen Methoden und Eigenschaften, und einer privaten Implementierung, der Sammlung aller privaten Konstanten, Funktionen, Veränderlichen, Methoden und Eigenschaften. Der interne Zustand eines Objekts, einer Instanz, ist gekapselt und damit nach außen nicht sichtbar. Wir haben schon wiederholt gesehen, dass die gleiche Schnittstelle auf sehr unterschiedliche Art und Weise implementiert werden kann. Die folgende Implementierung einer Bank merkt sich alle Kontostände.

```
type Cheap'N'Easy (seed : Nat) =
  class
    let mutable funds-log = [seed]
    member self.Deposit (amount : Nat) =
      funds-log ← (head funds-log + amount) :: funds-log
    member self.Withdraw (amount : Nat) =
      funds-log ← monus (head funds-log, amount) :: funds-log
    member self.Balance =
      head funds-log
    member self.Cancel =
      funds-log ← tail funds-log
  end
```

Die Klasse bietet zusätzlich eine aus Sicht der Finanzwelt sehr abenteuerliche Operation an, mit der die jeweils letzte Transaktion rückgängig gemacht werden kann.

In Abschnitt 8.1 haben wir die Funktion *transfer* eingeführt, die eine Banküberweisung modelliert. Wenn wir diese Funktion einsetzen wollen, erleben wir eine unliebsame Überraschung: Weder ein Objekt vom Typ *TrustMe* noch ein Objekt vom Typ *Cheap'N'Easy* kann an die Funktion *transfer* übergeben werden.

```
transfer : IAccount * Nat * IAccount → Unit

TrustMe       4711 : TrustMe
Cheap'N'Easy 815   : Cheap'N'Easy
```

Die drei Typen, *IAccount*, *TrustMe* und *Cheap'N'Easy*, sind nicht miteinander kompatibel. Diese Tatsache macht sich zunächst an den Namen fest: Alle drei Typbezeichner sind verschieden. In

Anlehnung an die Unabhängigkeitserklärung der Vereinigten Staaten sagt man auch »*all types are created unequal.*«[6] Hat sich der anfängliche Ärger über die Inkompatibilität gelegt, realisiert man, dass dies tatsächlich eine sinnvolle Festlegung ist: Die Gleichheit der Methodennamen könnte rein zufällig sein. Uns geht es aber nicht um Äußerlichkeiten (Wie heißt eine Methode?), sondern um innere Werte (Wie verhält sich eine Methode?). Die Instanzen der verschiedenen Klassen und die Elemente eines Schnittstellentyps sollten nicht nur die gleichen Nachrichten verstehen, sie sollten sich auch gleich oder zumindest ähnlich verhalten. Von der Eigenschaft *Balance* erwartet man, dass sie den aktuellen Kontostand zurückgibt und nicht etwa das Gepäck im Frachtraum eines Flugzeugs gleichmäßig verteilt. (Für den Rechner ist *Balance* ein Bezeichner bestehend aus sieben Buchstaben, der frei von jeglicher Bedeutung ist; Bedeutung, die für uns als menschliche Leserinnen und Leser immer mitschwingt.)

Möchten wir Instanzen der Klassen *TrustMe* und *Cheap'N'Easy* als Bankkonten verwenden, so müssen wir unsere Intention *explizit* machen; wir müssen bekanntgeben, dass eine Klasse eine Schnittstelle implementiert. Die Bekanntgabe lässt sich auf verschiedene Art und Weise organisieren. In der folgenden Überarbeitung der Klasse *Cheap'N'Easy* werden die Methoden der Schnittstelle *IAccount* *direkt* implementiert.

```
type Cheap'N'Easy (seed : Nat) =
  class
    let mutable funds-log = [seed]
    interface IAccount with
      member self.Deposit (amount : Nat) =
        funds-log ← (head funds-log + amount) :: funds-log
      member self.Withdraw (amount : Nat) =
        funds-log ← monus (head funds-log, amount) :: funds-log
      member self.Balance =
        head funds-log
    member self.Cancel =
      funds-log ← tail funds-log
  end
```

Aus den Klassenmethoden sind Methoden der Schnittstelle *IAccount* geworden. Nach der Ankündigung ***interface*** *IAccount* ***with*** wird konkretisiert, wie die Methoden *Deposit*, *Withdraw* und *Balance* implementiert werden. *Lies: Cheap'N'Easy* implementiert die Schnittstelle *IAccount*. Damit ist *Cheap'N'Easy* ein Untertyp von *IAccount*, als Formel

$$\mathit{Cheap'N'Easy} \preccurlyeq \mathit{IAccount}$$

Jetzt gelingt die Überweisung: Beim Aufruf der Funktion *transfer* wird der Typ automatisch mit Hilfe der Subsumptionsregel (8.2) angepasst.

[6] Von dieser Regel gibt es nur eine Ausnahme: Ein Typsynonym wie zum Beispiel ***type*** *Age* = *Int* führt einen Bezeichner für einen bestehenden Typ ein; *Age* und *Nat* sind per definitionem gleich und somit beliebig austauschbar.

```
>>> let hermines = Cheap'N'Easy 4711
>>> let harrys = Cheap'N'Easy 10
>>> transfer (hermines, 100, harrys)
()
>>> (harrys :> IAccount).Balance
110
>>> harrys.Cancel
()
>>> (harrys :> IAccount).Balance
10
```

Eine explizite Typanpassung ist notwendig, wenn auf die Methoden der Schnittstelle zugegriffen wird: Von Haus aus versteht *harrys* die Nachricht *Balance* nicht. Wir sehen in Kürze, warum der »Cast« sinnvoll ist. Im Gegensatz dazu wird die Nachricht *Cancel* direkt verstanden. Möchte man aus Gründen der Bequemlichkeit den direkten Zugriff auf die Schnittstellenmethoden ermöglichen, kann man diese *zusätzlich* als Methoden der Klasse »veröffentlichen«.

```
type Cheap'N'Easy (seed : Nat) =
  class
    ...
    // expose interface
    member self.Deposit  amount = (self :> IAccount).Deposit  amount
    member self.Withdraw amount = (self :> IAccount).Withdraw amount
    member self.Balance         = (self :> IAccount).Balance
  end
```

Die Gleichungen geben jeweils an, dass die Methode der Klasse (links: *self*.*Withdraw*) durch die Schnittstellenmethode (rechts: (*self* :> *IAccount*).*Withdraw*) definiert wird. Die Typanpassung muss zwingend vorgenommen werden; lässt man sie weg, erfolgt ein rekursiver Aufruf mit der Konsequenz der Nichtterminierung!

Man kann auch den umgekehrten Weg beschreiten und die Schnittstellenmethoden durch Methoden der Klasse definieren. Die folgende Klassendefinition illustriert diese *indirekte* Implementierung einer Schnittstelle.

```
type TrustMe (seed : Nat) =
  class
    let mutable funds = seed
    member self.Deposit (amount : Nat)  = funds ← funds + amount
    member self.Withdraw (amount : Nat) = funds ← monus (funds, amount)
    member self.Balance                 = funds
    interface IAccount with
      // these are not recursive definitions
      member self.Deposit  amount = self.Deposit  amount
      member self.Withdraw amount = self.Withdraw amount
      member self.Balance         = self.Balance
  end
```

Die Gleichungen geben jeweils an, dass die Schnittstellenmethode (links: *self*.*Withdraw*) durch die Methode der Klasse (rechts: *self*.*Withdraw*) definiert wird. Die Gleichungen sehen verdächtig nach rekursiven Definitionen aus, sind aber keine: die Nachricht *Deposit* wird an das Objekt der Klasse *TrustMe* geschickt; damit wird die weiter oben definierte Methode aufgerufen und abgearbeitet.

Nach diesen Vorarbeiten lassen sich sowohl Banküberweisungen tätigen als auch die Kontostände direkt ohne Umweg über die Schnittstelle abrufen.

```
>>> let hermines = TrustMe 4711
>>> let harrys = Cheap'N'Easy 0
transfer (hermines, 100, harrys)
()
>>> hermines.Balance
4611
>>> harrys.Balance
100
```

Der direkte Zugriff mit *Balance* ist möglich, weil entweder die Schnittstelle bekanntgegeben wurde oder die Schnittstelle mit den Methoden der Klasse implementiert wurde.

Eine Klasse kann auch mehrere Schnittstellen gleichzeitig implementieren.

```
type IPositive =
  abstract Answer : string
type INegative =
  abstract Answer : string
type Undecided () =     // don't forget »()«
  class
    member self.Answer = "maybe"
    interface IPositive with
      member self.Answer = "yup"
    interface INegative with
      member self.Answer = "nope"
  end
```

Die Methode *Answer* wird dreimal definiert: einmal als Methode der Klasse *Undecided*, ein zweites Mal als Methode der Schnittstelle *IPositive* und ein drittes Mal als Methode der Schnittstelle *INegative*. Die Schnittstellen repräsentieren unterschiedliche Stimmungen; je nach konkreter Stimmung fällt die »Antwort« unterschiedlich aus.

```
>>> let turncoat = Undecided ()
>>> turncoat.Answer
val it : string = "maybe"
>>> (turncoat :> IPositive).Answer
val it : string = "yup"
(turncoat :> INegative).Answer
val it : string = "nope"
```

Damit wird klar, warum bei Methodenaufrufen *keine* automatischen Typanpassungen vorgenommen werden (*Undecided* $\preccurlyeq$ *IPositive* oder *Undecided* $\preccurlyeq$ *INegative*): Kein Automatismus kann die vorhandene *Mehrdeutigkeit* auflösen.

Nun ist das Beispiel etwas künstlich; ein ähnliches Szenario tritt aber durchaus auf, etwa wenn ein Objekt in verschiedene *Rollen* schlüpft: Eine Person kann in der Rolle einer Studentin/eines Studenten oder in der Rolle einer Tutorin/eines Tutors auf die gleichen Nachricht unterschiedlich reagieren. (Die Methodenamen könnten auch nur zufällig übereinstimmen — neue Namen zu erfinden ist, wie schon gesagt, schwer.) Erst die Angabe der Rolle, sprich der Schnittstelle, macht unzweideutig klar, was mit der Nachricht gemeint ist.

8.3.2. Parametrisierte Klassen\Generische Klassen

module Objects.Dictionary

Wie Record-, Varianten- und Schnittstellentypen können auch Klassentypen mit einem oder mehreren Typen parametrisiert werden. Kurzum: Typdefinitionen jeglicher Couleur können mit Typparametern versehen werden.

In Abschnitt 5.3 haben wir endliche Abbildungen mit Hilfe von Listen, Suchlisten und Suchbäumen implementiert. Zur Erinnerung ein Auszug aus der Schnittstelle:

```
type Map⟨'key, 'value when 'key : comparison⟩
val empty : Map⟨'key, 'value⟩
val add    : 'key * 'value → Map⟨'key, 'value⟩ → Map⟨'key, 'value⟩
val lookup : 'key → Map⟨'key, 'value⟩ → 'value option
```

Die genannten Implementierungen sind ***persistent***: Wird eine endliche Abbildung um ein Schlüssel-Wert Paar erweitert, so wird als Ergebnis die erweiterte Abbildung zurückgegeben — die ursprüngliche Abbildung und die neue Umgebung koexistieren friedlich und können unabhängig voneinander verwendet und weiterentwickelt werden.

Im Folgenden implementieren wir eine ephemerale Variante von endlichen Abbildungen: Beim Erweitern wird die ursprüngliche Abbildung überschrieben; sie ist nach der Operation *nicht* mehr verfügbar. Genauer: Um die ephemerale Variante zu realisieren, verwenden wir die persistente Implementierung von endlichen Abbildungen auf Basis von Suchbäumen (Abschnitt 5.3.3).

Die folgende Interaktion zeigt die Implementierung in Aktion.

```
>>> let perfume = SearchTree⟨Nat, String⟩ ()
>>> perfume.Add (4711, "Kölnisch Wasser")
()
>>> perfume.Add (5, "Chanel")
()
>>> perfume.Lookup 5
"Chanel"
>>> perfume.[5]
"Chanel"
>>> perfume.[0] ← "Eau"
()
>>> perfume.[0]
"Eau"
>>> perfume.[0] ← "Wasser"
()
>>> perfume.[0]
"Wasser"
```

Das Wörterbuch *perfume* ordnet natürlichen Zahlen Strings zu. Mit der Methode *Add* wird das Wörterbuch um einen Eintrag erweitert; *Lookup* schlägt im Wörterbuch nach. Die ephemerale Natur wird deutlich: *Add* hat den Ergebnistyp *Unit*; zu jedem Zeitpunkt existiert nur eine Version der endlichen Abbildung *perfume*.

Für beide Operationen bieten wir syntaktischen Zucker an: $perfume.[k] \leftarrow v$ fügt ein neues Schlüssel-Wert Paar hinzu (bzw. aktualisiert einen bestehenden Eintrag für den Schlüssel k); $perfume.[k]$ schlägt den angegebenen Schlüssel nach.

```
type SearchTree⟨'key, 'value when 'key : comparison⟩ () =
  class
    let mutable mapping : Map⟨'key, 'value⟩ = empty
    member self.Add (key, value) =
      mapping ← add (key, value) mapping
    member self.Lookup key =
      match lookup key mapping with
      | None       → raise (KeyNotFoundException ())
      | Some value → value
    member self.Item
      with get key       = self.Lookup key
      and  set  key value = self.Add (key, value)
  end
```

Ähnlich wie eine polymorphe Funktion (siehe Abschnitt 4.3.2) ist die Klasse *SearchTree* sowohl mit Typen, *'key* und *'value*, als auch mit einem Wert, dem Dummy »()«, parametrisiert: *SearchTree* ist ein ***polymorpher Objektkonstruktor***. Der interne Zustand ist durch die Veränderliche *mapping* gegeben, die von *Add* modifiziert und von *Lookup* gelesen wird. Zusätzlich führt *Lookup* eine Umkodierung durch: An die Stelle eines optionalen Rückgabewerts tritt eine Ausnahme.

Der syntaktische Zucker für Erweiterung und Zugriff wird mittels der Eigenschaft *Item* realisiert. Es handelt sich um eine sogenannte ***indizierte Eigenschaft*** (engl. indexed property). Sowohl der Getter als auch der Setter sind (zusätzlich) mit dem Schlüssel parametrisiert. So wie die Eigenschaft ℓ die Abkürzungen $e.\ell$ und $e.\ell \leftarrow e'$ ermöglicht, so erlaubt eine indizierte Eigenschaft den syntaktischen Zucker $e.\ell\,[\,i\,]$ und $e.\ell\,[\,i\,] \leftarrow e'$. Ist weiterhin ℓ = *Item*, dann kann man ℓ auch auslassen und kurz $e.[\,i\,]$ und $e.[\,i\,] \leftarrow e'$ schreiben.

Übungen.

1. Definieren Sie eine Schnittstelle für ephemerale Wörterbücher, siehe Abschnitt 8.3.2, und ändern Sie die Definition der Klasse *SearchTree*, so dass die Schnittstelle implementiert wird.

8.4. Aufzähler und aufzählbare Objekte

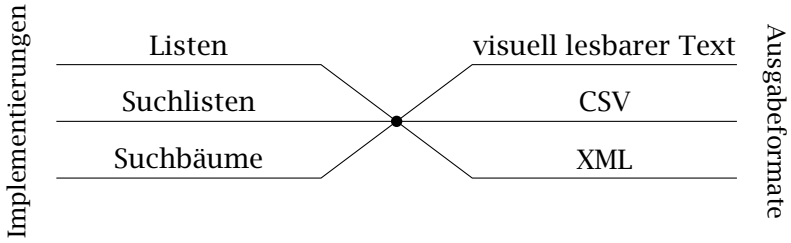
module Objects.Enumerator

Nehmen wir an, wir wollen das Wörterbuch aus Abschnitt 8.3.2 um die Möglichkeit erweitern, die verwalteten Schlüssel-Wert Paare auszugeben — entweder flüchtig auf dem Bildschirm oder dauerhaft in eine Datei. Eine unscheinbare Aufgabe, die aber ganz unterschiedlich angegangen werden kann. Tatsächlich eine lehrreiche Aufgabe, so dass wir uns verschiedene Designs für die Schnittstelle anschauen und ihre jeweiligen Vor- und Nachteile diskutieren wollen.

Möglichkeit A: Wir erweitern die Klasse um eine maßgeschneiderte Methode.

```
member Print : Unit → Unit
```

Die Erweiterung erfüllt sicherlich ihren Zweck, ist aber zu kurz gedacht. Zum Einen sind viele verschiedene Ausgabeformate denkbar: visuell lesbarer Text (engl. human readable text); durch Komma getrennte Werte (Comma-Separated Values, kurz CSV); Formate zur Darstellung hierarchisch strukturierter Daten (engl. Extensible Markup Language, abgekürzt XML). Zum Anderen kann ein Wörterbuch auf verschiedene Art und Weise implementiert werden: durch Listen, Suchlisten oder Suchbäume, siehe Abschnitt 5.3.



Der obige Ansatz führt zu einer kombinatorischen Explosion von Programmieraufgaben. Gibt es m verschiedene Implementierungen und n verschiedene Ausgabeformate, dann müssen $m \cdot n$ Methodenrümpfe mit Leben gefüllt werden, unweigerlich mit sich wiederholenden Programmfragmenten.

Möglichkeit B: Wir überführen die Daten des Wörterbuchs in ein einheitliches Zwischenformat (einen Mediator), zum Beispiel eine Liste oder ein Array von Schlüsseln, das dann von den verschiedenen Ausgabefunktionen weiterverarbeitet wird.

```
member Keys : Unit → List ⟨'key⟩
```

Ein Gewinn an Modularität: Konzeptionell wird die Verwaltung des Wörterbuchs von Funktionen zur Ein- und Ausgabe getrennt (engl. separation of concerns); praktisch reduziert sich der Implementierungsaufwand auf $m + n$ Methoden- bzw. Funktionsrümpfe. Jede Implementierung muss die Methode *Keys* umsetzen; für jedes Ausgabeformat wird eine entsprechende listenverarbeitende Funktion programmiert. Allerdings gibt es einen Nachteil: Der Ansatz benötigt zusätzlichen Speicherplatz. Die Daten, die bereits im Wörterbuch abgelegt sind, werden faktisch dupliziert, indem sie zusätzlich in einer Liste bereitgestellt werden.

Möglichkeit C: Wir ersetzen Listen durch eine alternative Darstellung von Sequenzen, die es uns erlaubt, schrittweise und *bedarfsgetrieben* ein Element nach dem anderen zu generieren.

```
member Keys : Unit → IEnumerator ⟨'key⟩
```

Der Sequenztyp *IEnumerator* firmiert unter vielen verschiedenen Namen — »Aufzähler« (engl. enumerator), »Wiederholer« (engl. iterator), »Cursor« (engl. cursor), »faule Liste« (engl. lazy list) und Generator — und wird vielfältig genutzt, so dass es sich lohnt, das Konzept genauer unter die Lupe zu nehmen.

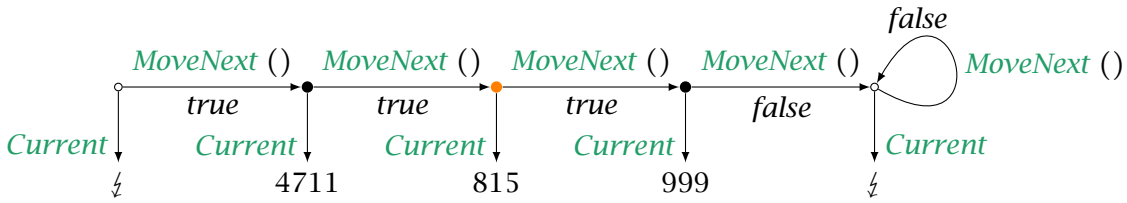
Aufzähler Abstrakt gesprochen ersetzen wir eine *Datenstruktur* (eine Liste oder ein Array) durch eine *Kontrollstruktur* (einen Aufzähler). Aus einem *Datum*, das alle Elemente der repräsentierten Sequenz umfasst, wird ein *Programm*, das es erlaubt, alle Elemente nacheinander aufzuzählen. Konkret ist ein Aufzähler ein Objekt, das zwei Nachrichten versteht.

```
type IEnumerator ⟨'elem⟩ =
  interface
    abstract member Current  : 'elem
    abstract member MoveNext : Unit → Bool
  end
```

Die Methode *Current* gibt das aktuelle Element der Aufzählung zurück; *MoveNext* () rückt zum nächsten Element vor und signalisiert über den Rückgabewert, ob ein Folgeelement tatsächlich existiert. Wird *Current* wiederholt aufgerufen, ohne zwischenzeitlich *MoveNext* aufzurufen, wird stets das identische Element zurückgegeben.

Bei der Verwendung der Schnittstelle muss man sich an ein striktes ***Protokoll*** halten: *vor* dem ersten Zugriff mit *Current* muss zunächst mit *MoveNext* () sichergestellt werden, dass überhaupt

ein Element existiert; der Zugriff auf das erste sowie die folgenden Elemente ist nur zulässig, wenn *MoveNext* () grünes Licht gibt, also *true* zurückgibt. Ein Aufzähler der dreielementigen Sequenz 4711 815 999 durchlebt somit insgesamt 5 (!) verschiedene Zustände.



Der »Cursor« der Aufzählung kann entweder auf ein Element zeigen oder vor dem ersten bzw. nach dem letzten Element stehen. Der Wert von *Current* ist vor dem ersten Aufruf von *MoveNext* und nach einem Aufruf von *MoveNext*, der *false* zurückgibt, undefiniert, angezeigt durch den Wurf einer Ausnahme.

```
let not-started () =
  invalidOp "Enumeration has not started. Call MoveNext."
let already-finished () =
  invalidOp "Enumeration already finished."
```

Die Funktion *invalidOp*, eine Variante von ***raise***, zeigt an, dass eine Operation ungültig ist, in unserem Fall, dass die Operation nicht gemäß des vereinbarten Protokolls verwendet wird.

Auch auf die Gefahr hin, das Offensichtliche zu benennen: Aufzähler sind zustandsbehaftet; je nach Zustand wird *Current* in der Regel verschiedene Elemente zurückgeben. Der Cursor kann nur von links nach rechts bewegt werden, aber nicht zurück; ist der Cursor ans Ende gelangt, ist die Aufzählung beendet und damit der Aufzähler praktisch nutzlos (*Current* wirft eine Ausnahme; *MoveNext* gibt *false* zurück) oder etwas drastischer formuliert: Objektmüll.

Kommen wir zur Implementierung von Aufzählern. Der folgende Objektkonstruktor repräsentiert das Intervall *lower* . . *upper*.

```
let range (lower, upper) =
  let mutable started  = false
  let mutable current = lower
  { new IEnumerator⟨Int⟩ with
    member self.Current =
      if started then
        if current ⩽ upper then current
                           else  already-finished ()
      else
        not-started ()
    member self.MoveNext () =
      if started then
        current ← current + 1
      else
        started ← true
      current ⩽ upper
  }
```

Die Position des Cursors wird durch zwei Zustandsvariablen repräsentiert: *started* gibt an, ob *MoveNext* bereits aufgerufen wurde; *current* ist der aktuelle Zahlenwert im oder rechts vom

```
let non-empty = function
  | [ ] → false
  | _  → true
let from-list (list : List ⟨'elem⟩) : IEnumerator ⟨'elem⟩ =
  let mutable started = false
  let mutable suffix  = list
  { new IEnumerator ⟨'elem⟩ with
      member self.Current =
        if started then
          match suffix with
          | [ ]      → already-finished ()
          | hd :: tl → hd
        else
          not-started ()
      member self.MoveNext () =
        if started then
          match suffix with
          | [ ]      → false
          | hd :: tl → suffix ← tl
                       non-empty suffix
        else
          started ← true
          non-empty suffix
  }
```

Abbildung 8.6.: Aufzählung einer Liste.

Intervall. Die Implementierung ist ***robust***: Falls der/die Benutzer/-in sich nicht an das Protokoll hält, wird er/sie mehr oder weniger dezent darauf hingewiesen. Man sagt auch, die Funktion *range* ist ***defensiv programmiert***: Annahmen und Voraussetzungen werden explizit überprüft. Der Nachteil der defensiven Herangehensweise liegt in einer gewissen Redundanz: Der Test $current \leqslant upper$ wird zum Beispiel sowohl in *Current* als auch in *MoveNext* durchgeführt. Vertraut man hingegen darauf, dass der/die Klient/-in sich an den Vertrag hält (Stichwort: ***design by contract***), programmiert man sehr viel kürzer:

```
let mutable current = lower − 1          // »undo« first call to MoveNext
…
member self.Current      = current
member self.MoveNext () = current ← current + 1; current ⩽ upper
```

Die Funktion *from-list* : $List\ \langle'elem\rangle \to IEnumerator\ \langle'elem\rangle$ zählt die Elemente einer Liste auf, siehe Abbildung 8.6. Sie implementiert somit einen ***Repräsentationswechsel***: Eine Darstellung von Sequenzen, Listen, wird in eine andere überführt, Aufzählungen. Die Implementierungsdetails sind ähnlich wie im Fall von *range*: Die Veränderliche *started* gibt an, ob *MoveNext* bereits aufgerufen wurde; *suffix* enthält einen Suffix, ein Endstück, der aufzuzählenden Liste.

Die implizite Darstellung einer Sequenz durch ein Programm hat gegenüber der expliziten Darstellung durch ein Datum den Vorteil, dass sich auch *unendliche* Sequenzen repräsentieren las-

sen. Der folgende Objektkonstruktor zählt zum Beispiel *alle* natürlichen Quadratzahlen auf (vergleiche mit dem Modell der Quadratwürmer aus Abschnitt 2.4).

```
let squares () =
  let mutable started = false
  let mutable current = 0
  let mutable odd     = 1
  { new IEnumerator⟨Nat⟩ with
    member self.Current =
      if started then
        current
      else
        not-started ()
    member self.MoveNext () =
      if started then
        current ← current + odd
        odd ← odd + 2
      else
        started ← true
      true
  }
```

Die Methode *MoveNext* gibt immer *true* zurück; die Aufzählung terminiert nie.

Aufzählbare Objekte Kommen wir noch einmal auf den Ausgangspunkt unserer Überlegungen zurück. Möglichkeit C sieht vor, eine Methode *Keys* : *Unit* → *IEnumerator* ⟨*'key*⟩ zum Wörterbuch hinzuzufügen. Nun sind viele »Dinge« aufzählbar, die Elemente einer Zahlenfolge (die Primzahlen, die Catalanzahlen usw.), die Elemente eines Containers (eines Arrays, einer Liste, eines Stacks usw.), so dass es sich anbietet, die Abstraktionsleiter noch eine Stufe hinaufzusteigen und eine allgemeine Schnittstelle für ***aufzählbare Objekte*** zu definieren.

```
type IEnumerable⟨'elem⟩ =
  interface
    abstract member GetEnumerator : Unit → IEnumerator ⟨'elem⟩
  end
```

An die Stelle des anwendungsspezifischen Bezeichners *Keys* ist in der Schnittstelle der neutrale Bezeichner *GetEnumerator* getreten.

Wir haben noch nicht thematisiert, warum *Keys* bzw. *GetEnumerator* eine Funktion ist, die einen Aufzähler zurückgibt, und nicht direkt ein Aufzähler ist. Aufzählungen sind wie schon erwähnt zustandsbehaftet und damit »flüchtig« (ephemeral): Sobald der Cursor mit *MoveNext* vorangewegt wird, kann auf das vorherige Element nicht mehr zugegriffen werden; ist der Cursor ans Ende gelangt, ist die Aufzählung beendet. Die Methode *GetEnumerator* erwartet ein Dummyargument, um bei jedem Aufruf einen »frischen« Aufzähler zurückgeben zu können — sie generiert sozusagen Generatoren. Das ist nützlich, ja unabdingbar, wenn zum Beispiel ein Wörterbuch in verschiedenen Formaten ausgegeben werden soll — für jedes Format muss die Liste aller Schlüssel einmal durchlaufen werden. Oder wenn sich das Wörterbuch im Laufe der Zeit ändert; *GetEnumerator* erstellt jeweils einen *Schnappschuss* der aktuell verfügbaren Schlüssel. Das ist übrigens leichter gesagt als getan. (Nachdenken!) In Kürze mehr dazu.

Die einheitliche Schnittstelle erlaubt es, die Verarbeitung von aufzählbaren Objekten mit etwas syntaktischem Zucker zu versüßen: mit Hilfe einer ***for***-Schleife können wir über alle Elemente einer Aufzählung iterieren.

```
for x in xs do
  body
```

```
let enumerator = xs.GetEnumerator ()
while enumerator.MoveNext () do
  let x = enumerator.Current
  body
```

Die ***for***-Schleife zur Linken ist eine Abkürzung für die ***while***-Schleife zur Rechten; die Aufrufe der Methoden *GetEnumerator*, *MoveNext* und *Current* werden so geschickt verborgen. Einen Wermutstropfen gibt es allerdings: ***for***-Schleifen, die über allgemeine Aufzählungen iterieren, geben nicht länger ein Terminierungsversprechen `:-(` — die Aufzählung muss ja nicht endlich sein (siehe *squares*). Eine ***for***-Schleife iteriert immer bis zum Ende einer Aufzählung; möchte man diese vorzeitig abbrechen, etwa weil ein gesuchtes Element gefunden wurde, muss an die Stelle einer ***for***-Schleife eine ***while***-Schleife mit entsprechender Abbruchbedingung treten.

Die beiden Schnittstellen in Verbindung mit dem syntaktischem Zucker erlauben es, eine ***generische Funktion*** zu schreiben, die die Elemente einer Aufzählung addiert.

```
let sum (xs : IEnumerable⟨Nat⟩) : Nat =
  let mutable acc = 0
  for x in xs do
    acc ← acc + x
  acc
```

Das Attribut »generisch« ist angebracht, da *sum* für beliebige aufzählbare Objekte funktioniert, insbesondere für Listen und Arrays.

Implementiert das Wörterbuch die obige Schnittstelle, so können wir die Schlüssel-Wert Paare mit Hilfe einer ***for***-Schleife ausgeben.

```
>>> let phone-book = SearchTree⟨String, Nat⟩ ()
>>> phone-book.Add ("Lisa", 815)
()
>>> phone-book.Add ("Harry", 4711)
()
>>> for key in phone-book do
      putline (key ^ "'s phone number is " ^ show phone-book.[key])
Harry's phone number is 4711
Lisa's phone number is 815
```

Der noch zu definierende Aufzähler generiert die Schlüssel in lexikographischer Reihenfolge, so dass die Einträge sortiert ausgegeben werden.

module Objects.Sequence

Sequenzausdrücke, da capo Wir haben gesehen, dass die Definition von Aufzählern des Typs *IEnumerator⟨'elem⟩* recht mühsam ist. Die Programme der letzten Seiten haben einen dediziert ***präskriptiven*** Charakter: Es wird jeweils genau detailliert, *wie* das nächste Element in Abhängigkeit vom aktuellen Zustand generiert und der Zustand aktualisiert wird. Alternativ können Sequenzen ***deskriptiv*** programmiert werden, indem man beschreibt, *was* die Elemente der Sequenz sind. Zu diesem Zweck können wir ***Sequenzbeschreibungen*** verwenden. Die Syntax kennen wir schon von Listen- und Arraybeschreibungen, siehe Abschnitt 7.3.1. Der einzige syntaktische Unterschied besteht in der umschließenden Klammer: An die Stelle von […] bzw. ⟦…⟧ tritt *seq* {…}. Zum Beispiel korrespondiert *seq* {*lower* .. *upper*} zu dem Aufzähler *range* (*lower*, *upper*) bzw. genauer zu dem aufzählbaren Objekt *Range* (*lower*, *upper*).

```
let Range (lower : Int, upper : Int) =
  { new IEnumerable<Int> with
      member self.GetEnumerator () = range (lower, upper)
  }
```

Intervalle eignen sich prima, um die Unterschiede zwischen Sequenzen als Daten (*List* ⟨*'a*⟩ oder *Array* ⟨*'a*⟩) und Sequenzen als Programme (*IEnumerable* ⟨*'a*⟩) zu illustrieren. Stellt man dem Mini-F# Interpreter die Anfrage [1 .. 100000000], tritt eine längere Stille ein, da hinter den Kulissen eine Liste mit einhundert Millionen Elementen aufgebaut wird. Die korrespondierende Anfrage *seq* {1 .. 100000000} wird hingegen in Windeseile ausgerechnet: Das Ergebnis ist ein Programm, das die einhundert Millionen Elemente bedarfsgetrieben peu à peu generiert.

Die Folge aller Quadratzahlen lässt sich mit Hilfe von Sequenzbeschreibungen wie folgt definieren.

```
let squares =
  let rec generate (current, odd) =
    seq {yield current; yield! generate (current + odd, odd + 2)}
  generate (0, 1)
```

Aus dem internen Zustand eines Objekts (siehe Seite 481) sind Parameter einer Hilfsfunktion geworden. Der Sequenzausdruck ***yield*** *x*; ***yield***! *xs* entspricht der Listenkonstruktion *x* :: *xs*. Zur Erinnerung: ***yield***! *e* ist eine Abkürzung für ***for*** *x* ***in*** *e* ***do yield*** *x* und zählt die Elemente der Sequenz *e* auf.

Tatsächlich lässt sich *squares* noch direkter und eleganter formulieren:

```
let squares = seq {for n in nats do yield n * n}
```

wobei *nats* die Folge aller natürlichen Zahlen ist. Die Folge der natürlichen Zahlen selbst lässt sich entweder präskriptiv mit einem Objektausdruck (siehe Aufgabe 8.4.1) oder deskriptiv mit Hilfe einer rekursiven *Werte*definition programmieren.

```
let rec nats =
  seq {yield 0
       for n in nats do
         yield n + 1}
```

Die Definition fängt Giuseppe Peanos Beschreibung der natürlichen Zahlen ein: Eine natürliche Zahl ist entweder 0 oder der Nachfolger $n+1$ einer natürlichen Zahl n (siehe Abbildung 3.6).

Kommen wir zur Implementierung der Klasse *SearchTree*; die Definition des Aufzählers für die Schlüssel des Wörterbuchs steht noch aus. Da das Wörterbuch durch einen binären Suchbaum gegeben ist, müssen wir im Wesentlichen den Inorder-Durchlauf aus Abschnitt 5.3.5 adaptieren.

```
let rec inorder = function
  | Leaf           -> Seq.empty
  | Node (l, x, r) -> seq {yield! inorder l; yield x; yield! inorder r}
```

Im Fall eines Blatts geben wir die leere Sequenz zurück. (Leider ist *seq* { } *nicht* zulässig, so dass wir auf die Bibliotheksfunktion *Seq.empty* zurückgreifen.) Anderenfalls zählen wir die Elemente des linken Teilbaums, das Wurzelelement und die Elemente des rechten Teilbaums auf.

Die vollständige Implementierung des Wörterbuchs ist in Abbildung 8.7 aufgeführt. Die Hilfsfunktion *enumerate-keys* entspricht im Wesentlichen *inorder*, zählt aber die Schlüssel eines Suchbaums auf, nicht die Elemente. (Aus historischen Gründen müssen zwei Schnittstellen implementiert werden: die getypte Schnittstelle *IEnumerable* ⟨*'key*⟩ und die ungetypte Schnittstelle *IEnumerable*. Letztere wird auf Erstere zurückgeführt.)

```
let enumerate-keys (Rep tree) =
  let rec inorder = function
    | Leaf           → Seq.empty
    | Node (l, x, r) → seq { yield! inorder l; yield x.key; yield! inorder r }
  inorder tree
type SearchTree⟨'key, 'value when 'key : comparison⟩ () =
  class
    let mutable mapping : Map⟨'key, 'value⟩ = empty
    member self.Add (key, value) =
      mapping ← add (key, value) mapping
    member self.Lookup key =
      match lookup key mapping with
      | None       → raise (KeyNotFoundException ())
      | Some value → value
    member self.Item
      with get key       = self.Lookup key
      and set key value = self.Add (key, value)
    interface IEnumerable⟨'key⟩ with
      member self.GetEnumerator () =
                  (enumerate-keys mapping).GetEnumerator ()
    interface IEnumerable with       // needed for historical reasons
      member self.GetEnumerator () =
                  (self :> IEnumerable⟨'key⟩).GetEnumerator () :> IEnumerator
  end
```

Abbildung 8.7.: Implementierung eines Wörterbuchs.

Wir haben schon angesprochen, dass *GetEnumerator* einen *Schnappschuss* der Schlüsselfolge zum Zeitpunkt des Aufrufs erstellt. In unserem Fall ist dies einfach zu bewerkstelligen, da die zugrundeliegende Implementierung von Binärbäumen *persistent* ist. Die Knoten eines Binärbaums werden niemals überschrieben, so dass der Aufzähler ohne Probleme über den jeweils aktuellen Binärbaum iterieren kann — zwar wird die Veränderliche *mapping* durch *Add* modifiziert, nicht aber der unterliegende Binärbaum.

Würden wir die persistente Implementierung von Binärbäumen durch eine ephemerale ersetzen (analog zu den ephemeralen Listen aus Abschnitt 7.2.5), dann ließe sich die »Schnappschuss-Semantik« nicht länger mit vertretbarem Aufwand realisieren. (Nachdenken!) Aus diesem Grund greift man zu einer drastischen Alternative: Wird während der Aufzählung der Schlüssel das zugrundeliegende Wörterbuch verändert, wird die Rechnung unmittelbar abgebrochen und eine Ausnahme geworfen (engl. fail-fast behaviour)!

8.4.1. Abstrakte Syntax

Wir erweitern Ausdrücke um Sequenzbeschreibungen.

$e \in \mathsf{Expr} ::=$	***Ausdrücke:***
$\quad \mid \mathit{seq}\,\{\mathit{se}\}$	Sequenzbeschreibungen

Innerhalb der Klammern steht ein ***Sequenzausdruck***, dessen Syntax wir in Abschnitt 7.3.1 definiert haben.

8.4.2. Statische Semantik

Sequenzbeschreibungen besitzen den Typ $\mathit{seq}\,\langle t\rangle$, ein Alias für den Schnittstellentyp $\mathit{IEnumerable}\,\langle t\rangle$ bzw. genauer $\mathit{System.Collections.Generic.IEnumerable}\,\langle t\rangle$.

$t \in \mathsf{Type} ::=$	***Typen:***
$\quad \mid \mathit{seq}\,\langle t\rangle$	Sequenztyp

Listen und Arrays implementieren die Schnittstelle $\mathit{IEnumerable}\,\langle t\rangle$ alias $\mathit{seq}\,\langle t\rangle$ und sind damit Untertypen von $\mathit{seq}\,\langle t\rangle$.

$$\overline{\mathit{List}\,\langle t\rangle \preccurlyeq \mathit{seq}\,\langle t\rangle} \qquad \overline{\mathit{Array}\,\langle t\rangle \preccurlyeq \mathit{seq}\,\langle t\rangle}$$

Die Klammer $\mathit{seq}\,\{\ldots\}$ überführt einen Sequenzausdruck in einen Aufzähler.

$$\frac{\Sigma \vdash \mathit{se} : t^*}{\Sigma \vdash \mathit{seq}\,\{\mathit{se}\} : \mathit{seq}\,\langle t\rangle}$$

Die Typregeln für Sequenzausdrücke, $\Sigma \vdash \mathit{se} : t^*$, sind in Abschnitt 7.3.1 aufgeführt.

8.4.3. Dynamische Semantik

Bei der Festlegung der dynamischen Semantik beschreiten wir im Allgemeinen zwei unterschiedliche Wege. Die Bedeutung von Sprachkonstrukten der »Kernsprache«, wie zum Beispiel der Alternative ***if*** e_1 ***then*** e_2 ***else*** e_3, wird durch Beweisregeln festgelegt. Die Bedeutung von »syntaktischem Zucker«, also Sprachkonstrukten, die zwar bequem aber nicht lebensnotwendig sind, wird mittels Übersetzung in die Kernsprache festgelegt. Die bequeme Formulierung wird erklärt, indem sie auf die unbequeme Variante der Kernsprache zurückgeführt wird.

Sequenzbeschreibungen sind ein gutes Beispiel für den zweiten Ansatz. Sequenzbeschreibungen verwenden die gleiche Syntax wie Listenbeschreibungen. Letztere haben wir in Abschnitt 7.3.1 auf vordefinierte Listenfunktionen abgebildet. Listen repräsentieren Sequenzen; da aufzählbare Objekte eine andere Repräsentation von Sequenzen sind, müssen wir in den semantischen Gleichungen lediglich die Listenfunktionen durch korrespondierende Funktionen auf dem Typ *seq* ersetzen:

Die Sequenzbeschreibung *seq* {*se*} wird in den Ausdruck ⟦*se*⟧ übersetzt, wobei ⟦*se*⟧ wie folgt definiert ist.

$$
\begin{array}{ll}
[\![\textbf{yield}\ e]\!] & = Seq.singleton\ e \\
[\![\textbf{yield!}\ e]\!] & = e \\
[\![d\ \textbf{in}\ se]\!] & = d\ \textbf{in}\ [\![se]\!] \\
[\![se_1; se_2]\!] & = Seq.append\ ([\![se_1]\!])\ ([\![se_2]\!]) \\
[\![\ \textbf{if}\ e\ \textbf{then}\ se]\!] & = \textbf{if}\ e\ \textbf{then}\ [\![se]\!]\ \textbf{else}\ Seq.empty \\
[\![\ \textbf{if}\ e\ \textbf{then}\ se_1\ \textbf{else}\ se_2]\!] & = \textbf{if}\ e\ \textbf{then}\ [\![se_1]\!]\ \textbf{else}\ [\![se_2]\!] \\
[\![\textbf{for}\ x\ \textbf{in}\ e\ \textbf{do}\ se]\!] & = Seq.collect\ (\textbf{fun}\ x \rightarrow [\![se]\!])\ e
\end{array}
$$

Die Implementierung der Bibliotheksfunktionen *Seq.empty* usw. ist zwar kein Hexenwerk, aber mühsam — der syntaktische Zucker steht ja nicht zur Verfügung, die aufzählbaren Objekte müssen präskriptiv mit zustandsbehafteten Objektausdrücken realisiert werden — so dass wir uns auf ein illustratives Beispiel beschränken wollen: die Konkatenation *Seq.append*.

Wir sind in diesem Abschnitt die Abstraktionsleiter zwei Stufen hinaufgestiegen und haben zwei Schnittstellentypen definiert: einen für Aufzähler, *IEnumerator* und einen für aufzählbare Objekte, *IEnumerable*. Entsprechend müssen wir für *append* zwei Objekte definieren. Entweder durch geschachtelte Objektausdrücke oder etwas modularer mit Hilfe zweier Objektkonstruktoren wie unten (siehe auch die Definition von *range* und *Range*).

```
let append-enumerators (first : IEnumerator ⟨'elem⟩) (second : IEnumerator ⟨'elem⟩) =
  let mutable first-active = true
  {new IEnumerator ⟨'elem⟩ with
    member self.Current =
      if first-active then
        first.Current
      else
        second.Current
    member self.MoveNext () =
      if first-active then
        first-active ← first.MoveNext ()
        first-active || second.MoveNext ()
      else
        second.MoveNext ()
  }
```

Wir merken uns in einer Veränderlichen, ob der erste Aufzähler aktiv ist. Wenn er inaktiv ist, werden die Nachrichten an den zweiten Aufzähler delegiert.

```
let append (first : IEnumerable ⟨'elem⟩) (second : IEnumerable ⟨'elem⟩) =
  {new IEnumerable ⟨'elem⟩ with
    member self.GetEnumerator () =
      append-enumerators (first.GetEnumerator ()) (second.GetEnumerator ())
  }
```

Noch ein abschließendes Wort zur Laufzeit. Aufzählbare Objekte können in konstanter Zeit konkateniert werden: *Seq.append* (*seq* {1 .. 1000000}) (*seq* {***yield*** 0}) wird in wenigen Schritten ausgerechnet. Die Laufzeit hängt insbesondere *nicht* von der Länge der beteiligten Sequenzen ab, sondern von der Schachtelungstiefe der Generatoren! Tief geschachtelte Aufzähler führen zu langen Nachrichtenketten: Die Nachricht *Current* wird von übergeordneten Aufzählern nach »unten« weitergereicht, so dass einige Zeit vergehen kann, bis das erste Element tatsächlich generiert wird: Der Aufruf *inorder* (*left-skewed* (1.000.000, `"hello, world"`)) zeigt das gleiche quadratische Verhalten, wie die listenbasierte Variante aus Abschnitt 5.3.5 (siehe auch Aufgabe 8.4.2).

8.4.4. Vertiefung

Testen Harry Hacker hat einen neuen Sortieralgorithmus entwickelt: *lightning-sort*. Lisa Lista, die mit einer gesunden Skepsis ausgestattet ist, schlägt vor, das Programm vor dem produktiven Einsatz systematisch zu testen. Sequenzbeschreibungen eignen sich wunderbar für die Generierung geeigneter Testdaten.

module Objects.Permutations

```
for n in 0 .. 10 do
  for xs in permutations [1 .. n] do
    if lightning-sort xs <> List.sort xs then
      raise (Panic "Harry!")
```

Die Funktion *permutations* : $List\,\langle'a\rangle \to seq\,\langle List\,\langle'a\rangle\rangle$ generiert systematisch alle Permutationen der angegebenen Liste. Zur Erinnerung: Zu einer Liste der Länge n existieren n Fakultät verschiedene Permutationen. Um nicht gigantische Mengen an Speicherplatz zu verbrauchen, ist es essentiell, dass eine *Sequenz* von Listen und nicht etwa eine *Liste* von Listen zurückgegeben wird. Auf diese Weise wird Harrys Programm erschöpfend für alle Eingabelisten der Länge $\leqslant 10$ getestet. Summa summarum werden 4.037.914 Tests durchgeführt. Aber wie lassen sich die Permutationen systematisch generieren?

Wenden wir das verallgemeinerte Peano Entwurfsmuster auf das Permutationsproblem an. Um die Problemgröße zu reduzieren, müssen wir ein Element der zu permutierenden Folge zur Seite legen. *Zwei* kanonische Ansätze drängen sich auf: Wir entfernen das erste Element der Eingabe *oder* wir wählen das erste Element der Ausgabe. Zwei Möglichkeiten, zwei Permutationsverfahren:

Permutieren durch Einfügen:

- Lege das erste Element zur Seite,
- bilde alle Permutationen der restlichen Elemente,
- *füge* das erste Element in jede Permutation nacheinander an allen möglichen Positionen *ein*.

Permutieren durch Auswählen:

- *Wähle* nacheinander alle Elemente *aus*,
- bilde jeweils alle Permutationen der restlichen Elemente,
- setze das entfernte Element vor jede korrespondierende Permutation.

Die beiden Verfahren sind im gewissen Sinne »dual« zueinander. Beim Permutieren durch Einfügen ist der erste Schritt einfach und der letzte Schritt aufwändig; beim Permutieren durch Auswählen ist es genau umgekehrt.

Nehmen wir an, wir wollen alle Ziffern der Zahl 1234 permutieren. Permutieren durch Einfügen entfernt die erste Ziffer, die ①, und berechnet die 3! = 6 Permutationen der restlichen Ziffern: 234, 324, 342, 243, 423, 432. In jede dieser Permutationen müssen wir ① an allen 4 Positionen einfügen. Insgesamt erhalten wir 3!·4 = 4! = 24 Permutationen, die auf der linken Seite aufgeführt sind.

①234	2①34	23①4	234①
①324	3①24	32①4	324①
①342	3①42	34①2	342①
①243	2①43	24①3	243①
①423	4①23	42①3	423①
①432	4①32	43①2	432①

①234	①243	①324	①342	①423	①432
②134	②143	②314	②341	②413	②431
③124	③142	③214	③241	③412	③421
④123	④132	④213	④231	④312	④321

Beim Permutieren durch Auswählen wird nacheinander die erste Ziffer der Ausgabe ausgewählt: zuerst ①, dann ②, dann ③ und schließlich ④. Für jede Auswahl werden die 3! = 6 Permutationen der restlichen Ziffern bestimmt und jeweils an die erste Ziffer angehängt. Wiederum erhalten wir insgesamt $4 \cdot 3! = 4! = 24$ Permutationen, die auf der rechten Seite aufgeführt sind.

Das Einfügen an allen Positionen und die Generierung aller Permutationen selbst lassen sich bequem mit Sequenzbeschreibungen formulieren.

```
let rec insertions x = function
  | [ ]            → seq {yield [x]}
  | xs & (y :: ys) → seq {yield (x :: xs); for zs in insertions x ys do yield y :: zs}
let rec ipermutations = function
  | [ ]    → seq {yield [ ]}
  | x :: xs → seq {for ys in ipermutations xs do
                     for zs in insertions x ys do yield zs}
```

Wie *ipermutations* ist auch die Hilfsfunktion *insertions* streng nach dem Struktur Entwurfsmuster für Listen gestrickt. Ist die Liste, in die x einzufügen ist, leer, dann gibt es nur ein Ergebnis: die einelementige Liste $[x]$. Anderenfalls setzen wir x entweder an die erste Position, $x :: xs$, oder wir fügen x rekursiv in die Restliste ein.

```
>>> ipermutations [1..4]
seq {[1;2;3;4];[2;1;3;4];[2;3;1;4];[2;3;4;1];
     [1;3;2;4];[3;1;2;4];[3;2;1;4];[3;2;4;1];
     [1;3;4;2];[3;1;4;2];[3;4;1;2];[3;4;2;1];
     [1;2;4;3];[2;1;4;3];[2;4;1;3];[2;4;3;1];
     [1;4;2;3];[4;1;2;3];[4;2;1;3];[4;2;3;1];
     [1;4;3;2];[4;1;3;2];[4;3;1;2];[4;3;2;1]}
```

Kommen wir zum Permutieren durch Auswählen. Die Hilfsfunktion *deletions* gibt neben dem ausgewählten Element zusätzlich die Liste der restlichen Elemente zurück.

```
let rec deletions = function
  | [ ]    → Seq.empty
  | x :: xs → seq {yield (x, xs); for (y, ys) in deletions xs do yield (y, x :: ys)}
let rec dpermutations = function
  | [ ] → seq {yield [ ]}
  | xs → seq {for (y, ys) in deletions xs do
                for zs in dpermutations ys do yield y :: zs}
```

Die Dualität der beiden Verfahren lässt sich auch am Programmcode festmachen. Im Rekursionsfall wird hier *erst* ein Element ausgewählt, *deletions xs*, *dann* erfolgt der rekursive Aufruf *dpermutations ys*. Beim Permutieren durch Einfügen vertauscht sich die Reihenfolge: *Erst* erfolgt der rekursive Aufruf, *ipermutations xs*, *dann* wird das Kopfelement eingefügt, *insertions x ys*.

```
>>> dpermutations [1..4]
seq {[1;2;3;4];[1;2;4;3];[1;3;2;4];[1;3;4;2];[1;4;2;3];[1;4;3;2];
     [2;1;3;4];[2;1;4;3];[2;3;1;4];[2;3;4;1];[2;4;1;3];[2;4;3;1];
     [3;1;2;4];[3;1;4;2];[3;2;1;4];[3;2;4;1];[3;4;1;2];[3;4;2;1];
     [4;1;2;3];[4;1;3;2];[4;2;1;3];[4;2;3;1];[4;3;1;2];[4;3;2;1]}
```

Ein Problem, zwei algorithmische Lösungen. Welches Verfahren ist vorzuziehen? Bezüglich der Laufzeit gibt es keine Unterschiede. Trotzdem lässt sich ein klarer Gewinner ausmachen: Permutieren durch Auswählen, weil es die Permutationen in *lexikographischer Reihenfolge* generiert.

Übungen.

1. Definieren Sie einen Aufzähler für natürliche Zahlen, präskriptiv mit Objektausdrücken, das heißt, ohne Sequenzbeschreibungen zu verwenden.

2. Wir haben in Abschnitt 8.4.3 bemerkt, dass die Laufzeit von *Seq.append* nicht von der Länge der zu konkatenierenden Sequenzen abhängt, sondern von der Schachtelungstiefe: Je tiefer *Seq.append* Aufrufe geschachtelt werden, desto länger werden die Nachrichtenketten. Explorieren wir die Konsequenzen:

(a) Testen Sie die naive Definition von *inorder* mit links- und rechtsschiefen Binärbäumen. Wie lassen sich die Ergebnisse erklären?

(b) Übertragen Sie die Definition von *inorder-append* aus Abschnitt 5.3.5 auf aufzählbare Objekte vom Typ *seq* ⟨'*a*⟩. Wiederholen Sie die Laufzeittests.

(c) Implementieren Sie *inorder* ohne syntaktischen Zucker präskriptiv mit Objektausdrücken. *Hinweis:* Orientieren Sie sich an der Definition von *from-list* aus Abschnitt 8.4; merken Sie sich in einer Liste die noch zu traversierenden Bäume. Führen Sie die Laufzeittests ein drittes Mal durch.

3. Aufzählbare Objekte vom Typ *IEnumerator* ⟨'*a*⟩ werden auch als ***externere Iteratoren*** bezeichnet. Extern, weil aus Sicht des Objekts die Benutzer*in die Kontrolle ausübt. Alternativ kann das Objekt selbst die Iteration durchführen.

```
type Iterator ⟨'a⟩ =
  interface
    member Foreach : ('a → Unit) → Unit
  end
```

Eine Instanz des Typs *Iterator* ⟨'*a*⟩ ist ein sogenannter ***interner Iterator***: Die übergebene Funktion wird über alle Elemente der repräsentierten Sequenz iteriert. Definieren sie elementare Iteratoren: für die leere Sequenz, für eine einelementige Sequenz, für Intervalle, Listen und Arrays. Zeigen Sie, wie Iteratoren hintereinander geschaltet (*append*) und geschachtelt (*collect*) werden können. In Abschnitt 8.4 haben wir gesehen, dass ein interner Iterator (eine ***for***-Schleife) mit Hilfe eines externen Iterators (*IEnumerator* ⟨'*a*⟩) definiert werden kann. Gilt auch die Umkehrung?

8.5. Vererbung

I fear the new object-oriented systems may suffer the fate of LISP, in that they can do many things, but the complexity of the class hierarchies may cause them to collapse under their own weight.

— Bill Joy

In ähnlicher Weise wie Schnittstellen durch »Vererbung« verbreitert werden können, so lassen sich auch Klassen um zusätzliche Funktionalität erweitern. Die folgende Klassendefinition erweitert die uns wohlbekannte Klasse *TrustMe* um eine Methode, mit der sich ein Konto »leerräumen« lässt.

```
type TrustMeGold (seed : Nat) =
  class
    inherit TrustMe (seed)
    member self.Clear () : Nat =
      let amount = self.Balance
      self.Withdraw amount
      amount
  end
```

Die ***inherit*** Klausel muss als erste Deklaration im Rumpf der Klassendefinition aufgeführt werden. Sie macht *TrustMeGold* zu einer ***Unterklasse*** (engl. subclass) der Klasse *TrustMe*; umgekehrt wird *TrustMe* zu einer ***Oberklasse*** (engl. superclass) der Klasse *TrustMeGold* bzw. zu deren ***Basisklasse*** (engl. base class). Die neu definierte Klasse erbt die *Implementierung* der Methoden der Oberklasse und fügt diesen eine weitere hinzu: *Clear*. Aus diesem Grund spricht man auch von ***Implementierungsvererbung*** (engl. implementation inheritance), im Gegensatz zur reinen ***Schnittstellenvererbung*** (engl. interface inheritance). Während eine Schnittstelle *mehrere* andere Schnittstellen beerben kann — die Schnittstelle *Mobile* erweitert sowohl *Phone* als auch *MP3Player* — darf eine Klasse nur von *einer* Oberklasse erben. Im Fachjargon: Schnittstellen unterstützen ***Mehrfachvererbung***, wohingegen Klassen lediglich ***Einfachvererbung*** zulassen. Eine Klasse kann allerdings mehrere, auch voneinander unabhängige Schnittstellen implementieren. Auf diesen Aspekt kommen wir später noch einmal zurück.

Klassen sind wie schon mehrfach angesprochen Zwitterwesen, sowohl Schnittstelle als auch Implementierung. Lesen wir die Klassendefinition mit der »Schnittstellenbrille«, dann etabliert die ***inherit***-Klausel eine Untertypbeziehung:

$$\mathit{TrustMeGold} \preccurlyeq \mathit{TrustMe}$$

Setzen wir die »Implementierungsbrille« auf, erkennen wir eine Aufrufstruktur: Wird mit ***new*** ein Objekt der Klasse *TrustMeGold* erzeugt, so wird zunächst der Objektkonstruktor *TrustMe* aufgerufen. Der Parameter *seed* des Konstruktors wird unverändert an den Objektkonstruktor *TrustMeGold* weitergereicht — dies ist aber nicht zwingend.

8.5.1. Redefinition\Overriding

Das Bankinstitut »Trust Me« bietet neben dem Standardkonto zusätzlich ein Konto für Studierende an, das wir bisher noch nicht realisiert haben. In der objektbasierten Implementierung, siehe Abbildung 8.1, haben wir das Studierendenkonto mit Hilfe von *Delegation* umgesetzt. In der klassenbasierten Implementierung ist dies in gleicher Weise möglich (siehe Aufgabe 8.5.1). Alternativ können wir die zweite Kontoart mit Hilfe einer Unterklasse realisieren.

```
type TrustMeStudent (seed : Nat, limit : Nat) =
  class
    inherit TrustMe (seed)
    let limit = min limit 1000
    override self.Withdraw (amount : Nat) =
      if amount > limit then raise Limit
                        else base.Withdraw amount
  end
```

Streng genommen ist die abgeleitete Klasse *TrustMeStudent* keine Erweiterung von *TrustMe*, da keine neue Funktionalität hinzukommt. Stattdessen wird die in der Basisklasse eingeführte Me-

thode *Withdraw* ***redefiniert***. Das Schlüsselwort ***override*** zeigt an, dass sich über die bereits bestehende Definition hinweggesetzt wird (engl. override). In der Redefinition von *Withdraw* wird allerdings auf die ursprüngliche Definition mit ***base***.*Withdraw* zugegriffen. Der Zusatz ***base*** ist notwendig, da nunmehr zwei unterschiedliche Definitionen der Methode existieren: Mit *self*.*Withdraw* erfolgt ein *rekursiver* Aufruf der Methode der abgeleiteten Klasse; ***base***.*Withdraw* ruft hingegen die Methode der Basisklasse auf. (Der formale Parameter *limit* des Objektkonstruktors wird übrigens auch redefiniert: Die Bindung ***let*** *limit* = *min limit* 1000 verwendet den Parameter und verschattet ihn dann — so wird das Transaktionslimit auf 1000 € oder einen kleineren Betrag gesetzt.)

Die Basisklasse muss allerdings Reimplementierungen zulassen — die bisherige Klassendefinition verbietet diese, so dass eine Änderungen notwendig wird (die vollständige Implementierung des Bankinstitut »Trust Me« ist in Abbildung 8.8 aufgeführt):

```
type TrustMe (seed : Nat) =
  class
    …
    abstract member Withdraw : Nat → Unit
    default self.Withdraw (amount : Nat) =
      funds ← monus (funds, amount)
    …
  end
```

Wie in einer Schnittstellendefinition spezifizieren wir die Signatur von *Withdraw*. Zusätzlich wird eine ***Standarddefinition*** (engl. default definition) angegeben. Wie wir später sehen werden, ist die mit dem Schlüsselwort ***default*** gekennzeichnete Definition optional. Eine abstrakte Methode mit einer Standarddefinition heißt auch ***virtuelle Methode*** (engl. virtual method).

8.5.2. Klassen und Schnittstellen

Eine Klasse kann eine oder mehrere, auch voneinander unabhängige Schnittstellen implementieren. Die Klassenhierarchie kann dabei unabhängig von der Schnittstellenhierarchie entwickelt werden. Die Organisation der Implementierung kann die Schnittstellenhierarchie widerspiegeln, siehe Abbildung 8.9. Dies ist aber nicht zwingend: Eine Klasse kann zum Beispiel eine Unterschnittstelle implementieren, ohne eine Unterklasse zu sein, siehe Abbildung 8.10. Die Definition der Klasse *OnlineBank* in Abbildung 8.10 illustriert übrigens ein weiteres Sprachfeature. Die Ersteinzahlung wird mittels eines ***do***-Blocks vorgenommen, in dem die Methode *Deposit* aufgerufen wird. Der für die Selbstnachricht benötigte Bezeichner *self* wird mit Hilfe einer ***as***-Klausel auf der linken Seite der Typdefinition eingeführt. Wie immer ist der Bezeichner frei wählbar und steht für das erzeugte Objekt selbst.

Für den Fall, dass Sie den Überblick verloren haben: Die folgende Grafik fasst die bisher eingeführten Schnittstellen und Klassen in einem sogenannten ***Klassendiagramm*** zusammen.

```
type TrustMe (seed : Nat) =
  class
    static do putline "TrustMe is founded."
    static let mutable no = 0
    do no ← no + 1
    let mutable funds = seed
    static member BIC = 4711
    static member total-no-of-accounts = no
    member self.Deposit (amount : Nat) =
      funds ← funds + amount
    abstract member Withdraw : Nat → Unit
    default self.Withdraw (amount : Nat) =
      funds ← monus (funds, amount)
    member self.Balance =
      funds
    interface IAccount with
      // these are not recursive definitions
      member self.Deposit  amount = self.Deposit  amount
      member self.Withdraw amount = self.Withdraw amount
      member self.Balance         = self.Balance
  end
type TrustMeStudent (seed : Nat) =
  class
    inherit TrustMe (seed)
    let limit = 1000
    override self.Withdraw (amount : Nat) =
      if amount > limit then raise Limit
                        else base.Withdraw amount
  end
```

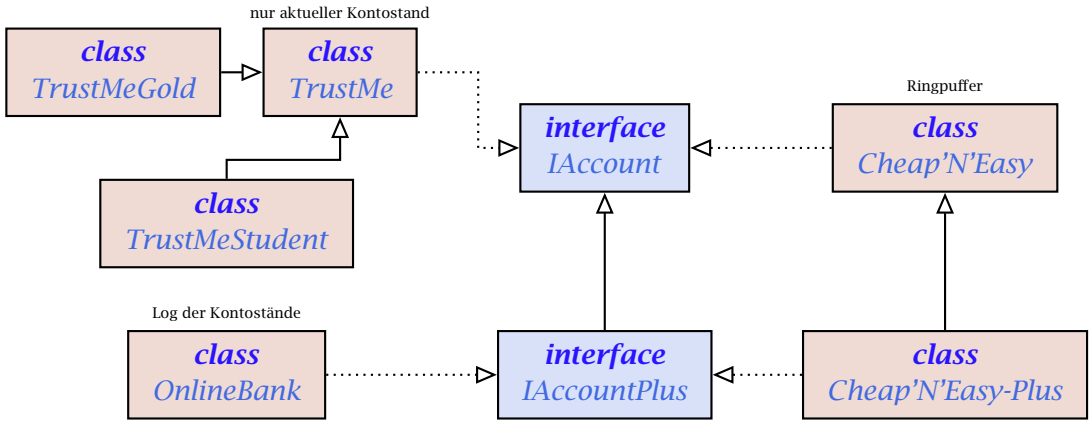
Abbildung 8.8.: Modellierung eines Bankinstituts (klassenbasiert, mit Vererbung).

```
type Cheap'N'Easy (seed : Nat) =
  class
    let mutable funds-log = [seed]
    static member BIC = 1234
    member internal self.Log = funds-log
    interface IAccount with
      member self.Deposit (amount : Nat) =
        funds-log ← (head funds-log + amount) :: funds-log
      member self.Withdraw (amount : Nat) =
        funds-log ← monus (head funds-log, amount) :: funds-log
      member self.Balance =
        List.head funds-log
    member self.Cancel =
      funds-log ← List.tail funds-log
    // expose interface
    member self.Deposit  amount = (self :> IAccount).Deposit  amount
    member self.Withdraw amount = (self :> IAccount).Withdraw amount
    member self.Balance         = (self :> IAccount).Balance
  end
type Cheap'N'Easy-Plus (seed : Nat) =
  class
    inherit Cheap'N'Easy (seed)
    interface IAccountPlus with
      member self.Statement =
        [| for x in take 10 self.Log → x |]
    // expose interface
    member self.Statement = (self :> IAccountPlus).Statement
  end
```

Abbildung 8.9.: Parallele Schnittstellen- und Klassenhierarchie.

```
type OnlineBank (seed : Nat, size : Int) as self =        // introduce name for object
  class
    let size         = min size 365
    let history      = [| for k in 0 .. size - 1 → 0 |]
    let mutable i = 0
    let next ()      = (i + 1) % size
    do (self :> IAccount).Deposit seed                    // initial deposit
    static member BIC = 0815
    interface IAccount with
      member self.Deposit (amount : Nat) =
        history.[next ()] ← history.[i] + amount; i ← next ()
      member self.Withdraw (amount : Nat) =
        history.[next ()] ← monus (history.[i], amount); i ← next ()
      member self.Balance =
        history.[i]
    interface IAccountPlus with
      member self.Statement =
        [| for k in 0 .. size - 1 → history.[(size + i - k) % size] |]
  end
```

Abbildung 8.10.: Eine Klasse implementiert eine Schnittstellenhierarchie.



Durchgezogene Pfeile zeigen an, dass eine Schnittstelle (Klasse) von einer anderen Schnittstelle (Klasse) abgeleitet wird bzw. erbt. Gepunktete Pfeile halten fest, dass eine Klasse eine Schnittstelle implementiert. Klassendiagramme sind Bestandteil der »Unified Modeling Language« (kurz UML), einer Modellierungssprache für Software. Zu diesem Thema erfahren Sie im weiteren Verlauf des Studiums mehr aus der Abteilung »Software Engineering«.

8.5.3. Abstrakte Klassen

Bei der Definition einer Klasse können eine oder mehrere Methoden als abstrakt markiert werden (siehe zum Beispiel Abbildung 8.8). Gibt man keine ***default***-Implementierung für eine dieser Methoden an, so wird die Klasse selbst ***abstrakt*** (engl. abstract class): Es können keine Instanzen der Klasse erzeugt werden. Ein solches Objekt wäre ja nicht in der Lage, auf eine entsprechen-

de Nachricht zu reagieren, da nur die Absicht erklärt wurde, eine Methode bereitzustellen. Erst wenn man dieser Absicht nachkommt und in einer Unterklasse der abstrakten Klasse die Methode(n) realisiert, dann können Objekte mit ***new*** erzeugt werden. In diesem Abschnitt schauen wir uns zwei Beispiele für abstrakte Klassen an, die allgemeine objektorientierte Programmiertechniken illustrieren: das sogenannte Beobachter-Entwurfsmuster (engl. observer design pattern, auch listener design pattern) und das Schablonen-Entwurfsmuster (engl. template design pattern).

module Objects.Observer

Beobachter-Entwurfsmuster In Abschnitt 7.2.4 haben wir mit Hilfe einer Speicherzelle einen einfachen Schrittzähler realisiert, um den Aufwand für die Berechnung der Fibonacci-Funktion abzuschätzen. Im Folgenden reimplementieren wir den Zähler, allerdings mit einem zusätzlichen Pfiff: Veränderungen des Zählers sollen beobachtbar sein, so dass wir auf Änderungen frühzeitig reagieren können. Das folgende Beispiel illustriert die Idee.

```
let steps = counter ()
do steps.Attach (fun n → if n % 1000 = 1 then putchar '*')
let rec fibonacci (n : Nat) : Nat =
  steps.State ← steps.State + 1
  if n ⩽ 1 then n
           else fibonacci (n - 1) + fibonacci (n - 2)
```

Mit *counter* () erzeugen wir einen neuen Zähler, an den ein Beobachter angeheftet wird, der eine einfache »Fortschrittsanzeige« (auch Fortschrittsbalken) realisiert: Nach jeweils 1000 Schritten wird ein Asteriskus '*' ausgegeben.

```
⋙ steps.State ← 0
val it : Unit = ()
⋙ fibonacci 20
**********************val it = 987
⋙ steps.State
val it = 21891
```

Ein ***Beobachter*** ist eine Prozedur, die einen Zustand verarbeitet. Aus Gründen der Allgemeinheit parametrisieren wir Beobachter mit dem Typ des Zustands.

```
type Observer ⟨'state⟩ = 'state → Unit
```

Das Subjekt, das wir beobachten wollen, wird durch eine abstrakte Klasse realisiert. Diese kümmert sich um die Verwaltung von Beobachtern und deren Benachrichtigung — wir erlauben, dass sich mehrere Beobachter registrieren. Die Verwaltung des eigentlichen Zustands bleibt hingegen abstrakt.

```
[<AbstractClass>]
type Subject<'state>() =
  class
    let mutable observers = []
    abstract member State : 'state with get, set
    member self.Attach(observer : Observer<'state>) =
      observers <- observer :: observers
      observer self.State              // notify observer
    member internal self.Notify() =
      for observer in observers do
        observer self.State            // notify observer
  end
```

Der/die Programmierer/-in muss ihre Absicht, eine abstrakte Klasse zu definieren, *explizit* machen: Das sogenannte ***Attribut*** (engl. attribute) [<*AbstractClass*>] kennzeichnet *Subject* als abstrakt. Auf diese Weise wird sichergestellt, dass nicht aus Versehen die Bereitstellung einer ***default***-Methode versäumt wird. Die interne Methode *Notify*, mit der Nachrichten an die Beobachter versendet werden, ist nicht für den Endbenutzer gedacht, sondern wird lediglich Unterklassen zur Verfügung gestellt. (Grob gesprochen schränkt ***internal*** die Sichtbarkeit der Methode auf das gleiche Modul bzw. die gleiche Bibliothek ein. Andere Programmiersprachen bieten den Zugriffsmodifizierer ***protected*** an, der die Sichtbarkeit gezielt auf die Klasse und deren Unterklassen einschränkt. Dieser würde an dieser Stelle benötigt, ist in F# aber leider nicht verfügbar.)

Kommen wir zur Implementierung des eigentlichen Zählers. Eine abstrakte Klasse kann entweder durch eine Unterklasse konkretisiert werden oder »on the fly« durch einen Objektausdruck. Letztere verwendet man typischerweise, wenn die notwendigen Ergänzungen wie in unserem Fall nicht allzu umfangreich sind und/oder wenn viele verschiedene Konkretisierungen vorgenommen werden sollen (für jede Unterklasse müsste man sich ja einen Namen ausdenken — neue Namen zu erfinden ist, wie schon mehrfach erwähnt, schwer).

```
let counter() =
  let mutable n = 0
  { new Subject<Nat>() with
      member self.State
        with set k = n <- k
                     self.Notify()
        and get() = n
  }
```

Der Zähler ist ein Subjekt vom Typ *Nat*, der die Eigenschaft *State* mit entsprechenden Getter und Setter-Methoden konkretisiert. Wir haben uns mehr oder weniger willkürlich dafür entschieden, nur schreibende Zugriffe zu beobachten (via *Notify*), nicht aber lesende.

module Objects.Template

Schablonen-Entwurfsmuster Beim Beobachter-Entwurfsmuster wird der zu beobachtende Zustand zu einer abstrakten Eigenschaft; alle anderen Mitglieder der Klasse *Subject* sind konkret. Im nächsten Beispiel verkehrt sich die Situation: Alle Methoden sind abstrakt, mit einer Ausnahme, die das Skelett eines Algorithmus definiert.

```
[<AbstractClass>]
type TwoPlayerGame () =
  class
    abstract member Finished : Bool
    abstract member Position : Unit → Unit
    abstract member Move     : Bool → Unit
    abstract member Winner   : Bool → Unit
    member self.Play () =
      try
        let mutable turn = false
        while not self.Finished do
          self.Position ()
          turn ← not turn
          self.Move turn
        self.Winner turn
      with
      | EOF → putline "\nbye bye"
  end
```

Die Klasse modelliert ein sogenanntes ***neutrales Zwei-Personen-Spiel*** (engl. impartial two-player game). Neutral meint, dass die Zugmöglichkeiten in einer Position unabhängig davon sind, welcher Spieler zieht. (Schach ist nicht neutral, da ein Spieler die weißen und der andere Spieler die schwarzen Figuren kontrolliert.) Der Spielablauf lässt sich in eine ***Schablone*** pressen: Die Spieler sind abwechselnd am Zug; ein Spieler verliert, wenn keine Zugmöglichkeiten mehr existieren. Im Schablonen-Entwurfsmuster werden die variablen Bestandteile des Algorithmus (Ist die Endposition erreicht? Gib die aktuelle Position am Bildschirm aus. Mache einen Zug. Präsentiere den Gewinner.) mit Hilfe abstrakter Methoden modelliert. Der Algorithmus selbst ist eine konkrete Methode, die aber von den abstrakten Bestandteilen abhängt.

Das wohl bekannteste neutrale Zwei-Personen-Spiel ist ***Nim***: Von einem Haufen Streichhölzer werden in einem Spielzug 1–3 Hölzer entfernt. Die folgende Interaktion zeigt einen typischen Spielverlauf (Mensch versus Rechner).

```
⋙ (Nim 10).Play ()
||||| |||||
number of matches: 1
||||| ||||
I take 1
||||| |||
number of matches: 3
|||||
I take 1
||||
number of matches: 2
||
I take 2
I win
```

Der menschliche Spieler eröffnet den Reigen und entfernt 1 Streichholz. Nach drei Runden gewinnt, wie zu erwarten (?), der Rechner (»`I win`«).

Kommen wir zur Implementierung von Nim. Wir definieren zunächst zwei Hilfsfunktionen, um Streichholzhaufen übersichtlich in Fünferpäckchen ausgeben zu können.

```
let bars (i : Nat)    = String.replicate (int i) "|"
let (^^) x (i : Nat) = List.replicate (int i) x
```

Der Aufruf *bars* 5 wertet zu einem Fünferpäckchen aus: "|||||"; *bars* 5 ^^ 3 erzeugt eine Liste mit 3 Fünferpäckchen: ["|||||";"|||||";"|||||"]. Zur Erinnerung: Um einen Infixoperator zu definieren, muss dieser in runde Klammern eingeschlossen werden: **let** (^^) *x i* = ….

Das Spiel selbst spezialisiert die Klasse *TwoPlayerGame*.

```
type Nim (n : Nat) =
  class
    inherit TwoPlayerGame ()
    let mutable matches = n
    let announce i = putline ("I take " ^ show i); i
    override self.Finished =
      matches = 0
    override self.Position () =
      putline (String.concat "  " (((bars 5) ^^ (matches ÷ 5)) @ [bars (matches % 5)]))
    override self.Move (human : Bool) : Unit =
      let i =
        if human then
          checked-query ("number of matches",
                         both (is-nat, both (isGreater 0, is-less 4)))
        else
          announce (max 1 (matches % 4))
      matches ← matches ÷ i
    override self.Winner human =
      putline ((if human then "you" else "I") ^ " win")
  end
```

Die abstrakten Methoden, die Schritte des Algorithmus, werden jeweils mit Leben gefüllt. Die Methode *Move* verwendet die validierende Eingabefunktion *checked-query* aus Abschnitt 7.1.4, wenn der menschliche Spieler am Zug ist. Anderenfalls werden *max* 1 (*matches* % 4) Hölzer entfernt. Wie beurteilen Sie die Spiellogik des Rechners?

Kritik Von den unzähligen Sprachfeatures, die wir im Laufe der Vorlesung eingeführt haben, ist Vererbung das wohl kontroverseste. Wir werden im folgenden und letzten Abschnitt sehen, dass Vererbung in einem sehr angespannten Verhältnis zur Kapselung, einem der Grundpfeiler der Objektorientierung, steht. In vielen Fällen lässt sich Vererbung durch einfachere und bewährte Sprachfeatures ersetzen. Nehmen wir das Schablonen-Entwurfsmuster. Eine Schablone ist im Prinzip nichts anderes als eine parametrisierte Funktion — eine ***Funktion höherer Ordnung***, da die Parameter, die Schritte des Algorithmus, selbst Funktionen sind. (Erinnern Sie sich an das Ratespiel aus Abschnitt 3.6.)

Bündeln wir die abstrakten Schritte in einer Schnittstelle,

```
type ITwoPlayerGame =
  interface
    abstract member Finished : Bool
    abstract member Position : Unit → Unit
    abstract member Move     : Bool → Unit
    abstract member Winner   : Bool → Unit
  end
```

dann lässt sich das Schablonen-Entwurfsmuster alternativ mit Hilfe einer Funktion umsetzen, die mit einem Spielobjekt parametrisiert ist.

```
let play (game : ITwoPlayerGame) =
  try
    let mutable turn = false
    while not game.Finished do
      game.Position ()
      turn ← not turn
      game.Move turn
    game.Winner turn
  with
  | EOF → putline "\nbye bye"
```

Die Unterschiede sind marginal: Die Nachrichten *Finished*, *Position* etc. werden nicht länger an *self* geschickt, sondern an den Parameter *game*. Konkrete Spiele, Instanzen der Schnittstelle *ITwoPlayerGame*, können dann entweder mit Objektausdrücken oder mit Hilfe von Klassen definiert werden (siehe Aufgabe 8.5.2).

Lässt sich Vererbung auch im Fall des Beobachter-Entwurfsmusters umgehen? Die Verflechtung zwischen der abstrakten Klasse und dem sie konkretisierenden Objekt sind hier enger: Das Objekt ruft *Notify* auf; im Rumpf von *Notify* wird wieder auf das Objekt selbst zurückgegriffen.

Als ersten Schritt definieren wir zunächst eine Schnittstelle für »Zustände«.

```
type IState⟨'state⟩ =
  interface
    abstract member State : 'state with get, set
  end
```

Eine »low cost« Version des beobachtbaren Zählers lässt sich sehr einfach umsetzen. Wenn es nur einen Beobachter gibt, können wir diesen dem Objektkonstruktor unmittelbar mit auf den Weg geben.

```
let counter (observer : Nat → Unit) =
  let mutable n = 0
  { new IState⟨Nat⟩ with
      member self.State
        with set  k  = n ← k
                       observer n
        and  get () = n
  }
let steps = counter (fun n → if n % 1000 = 1 then putchar '*')
```

Der Objektkonstruktor *counter* ist jetzt eine ***Funktion höherer Ordnung***: Er nimmt eine Funktion als Argument und gibt ein Objekt, eine Sammlung von Methoden, als Ergebnis zurück.

Diese Umsetzung des Entwurfsmuster ist natürlich sehr speziell. Im Allgemeinen möchten wir Beobachter auch verwalten können: neue Beobachter hinzufügen, alte Beobachter entfernen. Denken Sie etwa an ein Zeitschriftenabonnement oder einen Newsletter, einen elektronischen Informationsbrief — das Entwurfsmuster wird auch unter dem Namen »publish-subscribe pattern« geführt. In diesem Fall müssen wir die Parametrisierung weiter vorantreiben! Der Zähler wird jetzt mit der Benachrichtigungsfunktion parametrisiert (der vollständige Programmcode ist in Abbildung 8.11 aufgeführt).

```
let counter (notify : Unit → Unit) = …
```

Die Verwaltung von Beobachtern wird von der Klasse *Observable* übernommen, die wiederum mit dem Subjekt der Beobachtungen parametrisiert ist — *counter* hat den passenden Typ (*Unit* → *Unit*) → *IState* ⟨*Nat*⟩.

```
type Observable ⟨'state⟩ (subject : (Unit → Unit) → IState ⟨'state⟩) as self =
  class
    let state = subject self.Notify       // delegatee
    …
    member private self.Notify () = …
    …
  end
```

Der Objektkonstruktor ist sozusagen ein ***Objektkonstruktor höherer Ordnung***: Er nimmt einen Objektkonstruktor als Argument und gibt ein Objekt als Ergebnis zurück. Im Rumpf der Klasse wird der Parameter, das Subjekt, mit der Benachrichtigungsfunktion versorgt (die jetzt privat ist); an das resultierende Zustandsobjekt *state* werden dann die Get- und Set-Nachrichten ***delegiert*** (siehe Abbildung 8.11). Einen beobachtbaren Zähler erhalten wir schließlich mit

```
let steps = Observable ⟨Nat⟩ counter
do steps.Attach (fun n → if n % 1000 = 1 then putchar '*')
```

Im Vergleich zur ursprünglichen Version des Beobachter-Entwurfsmusters sind jetzt die Abhängigkeiten zwischen den einzelnen Komponenten ***manifest*** (lat. offenbar, offenkundig). Das ist ein Segen und ein Fluch. Ein Fluch, weil die Versorgung mit Parametern von Hand vorgenommen werden muss. Diese Klempnerarbeiten (engl. plumbing) werden in der ursprünglichen Version hinter den Kulissen vom Mechanismus der Vererbung erledigt. Ein Segen, weil die Versorgung mit Parametern von Hand vorgenommen werden kann. Die Komponenten (*counter* und *Observable*) sind entkoppelt und lassen sich getrennt programmieren und testen und können auch einfach ausgetauscht werden. Wie so oft haben Automatismen sowohl Vor- als auch Nachteile.

8.5.4. Delegation versus Vererbung

module Objects.StepCounter

Um Objekte kompositional zu definieren, haben wir zwei grundlegende Techniken kennengelernt: *Delegation* in Abschnitt 8.1 und *Unterklassen* (Implementierungsvererbung) in diesem Abschnitt, Abschnitt 8.5. Wir haben schon anklingen lassen, dass im Allgemeinen Delegation die bessere Wahl ist. Im Folgenden wollen wir den Gründen für diese Präferenz nachgehen.

Zunächst einmal ist es wichtig, den Mechanismus des Nachrichtensendens im Zusammenspiel von Klassen und Unterklassen genau zu verstehen. Zu diesem Zweck haben wir eine Variante des Schrittzählers mit Kontrollausgaben versehen (ignorieren Sie zunächst den Code auf der rechten Seite).

```
type IState⟨'state⟩ =
  interface
    abstract member State : 'state with get, set
  end
let counter (notify : Unit → Unit) =
  let mutable n = 0
  {
    new IState⟨Nat⟩ with
      member self.State
        with set k = n ← k
                    notify ()
        and get () = n
  }
type Observable⟨'state⟩ (subject : (Unit → Unit) → IState⟨'state⟩) as self =
  class
    let state = subject self.Notify       // delegatee
    let mutable observers = [ ]
    member self.Attach (observer : Observer⟨'state⟩) =
      observers ← observer :: observers
      observer state.State                // notify observer
    member private self.Notify () =
      for observer in observers do
        observer state.State
    member self.State                     // delegate calls
      with get () = state.State
      and set v = state.State ← v
    interface IState⟨'state⟩ with         // implement interface
      member self.State
        with get () = self.State
        and set v = self.State ← v
  end
let steps = Observable⟨Nat⟩ counter
do steps.Attach (fun n → if n%1000 = 1 then putchar '*')
let rec fibonacci (n : Nat) : Nat =
  steps.State ← steps.State + 1
  if n ⩽ 1 then n
           else fibonacci (n - 1) + fibonacci (n - 2)
```

Abbildung 8.11.: Beoachter-Entwurfsmuster mit Delegation.

```
type StepCounter () =
  class
    let mutable n = 0
    abstract Inc : Unit → Unit
    default self.Inc () =
      putline "Inc: base class"
      n ← n + 1
    abstract Step : Int → Unit
    default self.Step k =
      putline "Step: base class"
      for i in 1 .. k do
        self.Inc ()
  end
```

```
type StepCounter () =
  class
    let mutable n = 0
    abstract Inc : Unit → Unit
    default self.Inc () =
      putline "Inc: base class"
      n ← n + 1
    abstract Step : Int → Unit
    default self.Step k =
      putline "Step: base class"
      n ← n + k

  end
```

Die Nachrichten *Inc* und *Step* sind ***virtuell*** — sie sind abstrakt, aber mit einer Standarddefinition versehen. Insbesondere lassen wir zu, dass eine Unterklasse die Methoden redefiniert, so geschehen im folgenden Programmstück (ignorieren Sie wiederum den Code rechts).

```
type ParityCounter () =
  class
    inherit StepCounter ()
    let mutable even = true
    override self.Inc () =
      putline "Inc: subclass"
      base.Inc ()
      even ← not even
    override self.Step k =
      putline "Step: subclass"
      base.Step k
      even ← even = (k % 2 = 0)
    member self.Parity = even
  end
```

```
type ParityCounter () =
  class
    inherit StepCounter ()
    let mutable even = true
    override self.Inc () =
      putline "Inc: subclass"
      base.Inc ()
      even ← not even

    member self.Parity = even
  end
```

Der Paritätszähler hält nach, ob die Gesamtzahl der Schritte gerade oder ungerade ist.[7] Zu diesem Zweck wird die Veränderliche *even* verwendet; die Methoden *Inc* und *Step* werden entsprechend redefiniert, um Änderungen nachhalten zu können. Dazu wird ausgenutzt, dass die Parität der Summe $i+j$ sich aus der Parität der Summanden ableiten lässt: gerade + gerade = gerade, gerade + ungerade = ungerade, ungerade + gerade = ungerade und ungerade + ungerade = gerade, oder als Formel,

$$((i+j)\,\%\,2 = 0) \quad = \quad (i\,\%\,2 = 0) = (j\,\%\,2 = 0)$$

[7] Das Beispiel ist bewusst einfach gehalten, steht aber stellvertretend für Anwendungen, in denen aufwändig zu berechnende Eigenschaften mittels eines Caches in konstanter Zeit bereitgestellt werden. Zum Beispiel: Um die Größe einer Liste oder eines Stacks zu bestimmen, benötigt man lineare Laufzeit. Merkt man sich die Länge und trägt bei Modifikationen des Stacks, *Push* oder *Pop*, jeweils die Längenänderung nach, +1 oder −1, steht die Eigenschaft in konstanter Zeit zur Verfügung.

Bevor die Parität nachgehalten wird, werden jeweils die Methoden der Basisklasse aufgerufen, die die eigentliche Arbeit verrichten.

Senden wir einem Paritätszähler die Nachricht *Step* 3, ergibt sich eine interessante Nachrichtenkaskade.

```
⋙ let counter = ParityCounter ()
⋙ counter.Step 3
Step: subclass
Step: baseclass
Inc: subclass
Inc: baseclass
Inc: subclass
Inc: baseclass
Inc: subclass
Inc: baseclass
⋙ counter.Parity
true
```

Die Nachricht *Step* 3 wird an einen Paritätszähler gesendet; die *Step*-Methode der Unterklasse ruft dann die gleichnamige Methode der Basisklasse auf (***base***.*Step k*); in der Basisklasse sendet das Objekt sich selbst eine Nachricht: *self*.*Inc* (). Da das Objekt ein Paritätszähler ist (!), ist die redefinierte *Inc*-Methode der Unterklasse gemeint, die ihrerseits die gleichnamige Methode der Basisklasse aufruft (***base***.*Inc* ()). Mit anderen Worten, virtuelle Methoden werden stets zur Laufzeit in der zu dem Objekt gehörigen Methodentabelle nachgeschlagen (dynamic dispatch), auch und inbesondere für Selbstnachrichten.

Für unsere Anwendung hat die Nachrichtenkaskade einen unerwünschten Effekt: Jede Erhöhung wird doppelt gezählt, so dass 3 als gerade klassifiziert wird (*counter*.*Parity* ergibt *true*). Autsch! Was ist zu tun? Wir dürfen *Step* nicht redefinieren, so wie im Code oben auf der rechten Seite. Problem gelöst? Nicht ganz … Einige Zeit später im Zuge einer Coderevision optimiert Harry Hacker die Klasse *StepCounter*: Er ersetzt die Schleife ***for*** *i* ***in*** 1 . . *k* ***do*** *self*.*Inc* () im Rumpf der Methode *Step* durch die Zuweisung $n \leftarrow n + k$, siehe Code ganz oben auf der rechten Seite. Wiederholen wir jetzt die obige Interaktion, ergibt sich das folgende Bild.

```
⋙ let counter = ParityCounter ()
⋙ counter.Step 3
Step: baseclass
⋙ counter.Parity
true
```

Da *Step* nicht redefiniert wurde, wird die Nachricht direkt von der Basisklasse behandelt mit dem Ergebnis, dass keine Aktualisierung der Parität erfolgt (*counter*.*Parity* ergibt den ursprünglichen Wert, nämlich *true*).

Wie man's macht, macht man's falsch.
Und macht man's falsch, ist's auch nicht richtig.
— Klaus Klages (1938)

Die Änderung der Basisklasse *StepCounter* zieht eine Änderung der Unterklasse *ParityCounter* nach sich. Im Zuge der Coderevision hätte die Unterklasse ebenfalls revidiert werden müssen: Die Methode *Step* muss redefiniert werden, so wie im Code oben links. (Das Zusammenspiel der Klassen funktioniert nur »über Kreuz«.) Das ist kein großes Problem, wenn die Unterklasse im gleichen Modul definiert wird und von dem/der gleichen Programmierer/-in gepflegt wird. Nun

kann eine Klasse aber viele Unterklassen besitzen und diese können über verschiedene Module und Anwendungen verstreut sein. Problematisch ist, dass die Änderung der Basisklasse nicht lokal ist; sie zieht nicht-lokale Folgeänderungen nach sich (das Programm ist fragil). Umgekehrt betrachtet, lässt sich die Unterklasse *ParityCounter* nicht ohne intime Kenntnis der Oberklasse *StepCounter* korrekt implementieren. Die Kapselung, die eine Klasse vornimmt, wird durch virtuelle Methoden und Vererbung aufgeweicht: *inheritance breaks abstraction*.

Komponieren wir die beiden Zählertypen mit Hilfe von Delegation, tritt, wie wir gleich sehen werden, das Problem nicht auf. Delegation kann mit Klassen realisiert werden (siehe Abbildung 8.11) oder mit Schnittstellen und Objektausdrücken. Wir ziehen die zweite Option und definieren zunächst eine Schnittstelle für Schrittzähler.

```
type IStepCounter =
  interface
    abstract member Inc  : Unit → Unit
    abstract member Step : Int  → Unit
  end
```

Ähnlich wie in der Variante mit Klassen und Unterklassen realisieren wir den Objektkonstruktor *step-counter* auf zwei Weisen: Links ruft *Step* die Methode *Inc* auf, die Zustandsänderung erfolgt also indirekt; rechts wird der Zustand direkt mit einer Zuweisung aktualisiert.

```
let step-counter () =
  let mutable n = 0
  { new IStepCounter with
      member self.Inc () =
        putline "Inc: delegatee"
        n ← n + 1
      member self.Step k =
        putline "Step: delegatee"
        for i in 1 .. k do
          self.Inc ()
  }
```

```
let step-counter () =
  let mutable n = 0
  { new IStepCounter with
      member self.Inc () =
        putline "Inc: delegatee"
        n ← n + 1
      member self.Step k =
        putline "Step: delegatee"
        n ← n + k

  }
```

Die Implementierung des Paritätszählers erfolgt *unabhängig* davon, wie der Schrittzähler implementiert ist. Wir müssen nur wissen, *was* der Schrittzähler macht, aber nicht *wie* das Verhalten detailliert umgesetzt wird. Wie üblich definieren wir zunächst einen Untertyp von *IStepCounter*.

```
type IParityCounter =
  interface
    inherit IStepCounter
    abstract member Parity : Bool
  end
```

Der Paritätszähler delegiert die Hauptarbeit an einen Schrittzähler; zusätzlich werden wie vorher die Änderungen der Priorität nachgehalten.[8]

[8] Im Englischen ist der »delegator« die- oder derjenige, die/der Arbeit delegiert, und »delegatee« die- oder derjenige, an die/den Arbeit delegiert wird. Die Endungen »-or« und »-ee« finden sich auch in anderen Wortpaaren wieder: Ein »advisor« erteilt Ratschläge, die ein »advisee« entgegennimmt.

```
let parity-counter () =
  let basic           = step-counter ()      // delegatee
  let mutable even = true
  {new IParityCounter with
      member self.Inc () =
        putline "Inc: delegator"
        basic.Inc ()
        even ← not even
      member self.Step k =
        putline "Step: delegator"
        basic.Step k
        even ← even = (k % 2 = 0)
      member self.Parity = even
  }
```

Technisch gesehen ergeben sich im Vergleich zur Realisierung mit Klassen und Unterklassen zwei Änderungen: Die ***inherit***-Klausel der Unterklasse ist einer ***let***-Bindung gewichen, die einen Namen für den zugrundeliegenden Schrittzähler vergibt. (Warum ist *basic* kein ***mutable***?) Entsprechend sind die Aufrufe der Basisklasse, ***base***.*Inc* (), durch Aufrufe des »Basisobjekts« , *basic*.*Inc* (), ersetzt worden.

Je nachdem, welche Implementierung des Schrittzählers zugrundeliegt, ergeben sich unterschiedliche Kontrollausgaben. Die Parität wird aber unabhängig von der Umsetzung des Schrittzählers korrekt berechnet.

```
⋙ let counter = parity-counter ()
⋙ counter.Step 3
Step: delegator
Step: delegatee
Inc: delegatee
Inc: delegatee
Inc: delegatee
⋙ counter.Parity
false
```

```
⋙ let counter = parity-counter ()
⋙ counter.Step 3
Step: delegator
Step: delegatee
⋙ counter.Parity
false
```

Der Paritätszähler delegiert die Arbeit an den Schrittzähler, dann arbeitet dieser: links durch wiederholte Aufrufe von *Inc*; rechts direkt mit einer Zuweisung.

Wie erklären sich die Unterschiede zwischen den beiden Ansätzen? In der ursprünglichen Realisierung existiert genau *ein* Objekt, der Paritätszähler, der aber Verhalten von der Basisklasse erbt. Mit dem Akt der Vererbung werden die Methoden kompliziert miteinander verflochten, via Nachrichten an die Basisklasse und via Selbstnachrichten. Im Gegensatz dazu existieren hier *zwei* Objekte, der Paritätszähler und der Schrittzähler, die in nachvollziehbarer Weise miteinander interagieren: Einer delegiert Arbeit an den anderen.

Damit soll das Konzept von Unterklassen nicht prinzipiell verteufelt werden, aber als Fazit können wir festhalten, dass virtuelle Methoden und Unterklassen mit Bedacht eingesetzt werden sollten.

Übungen.

1. In Abschnitt 8.5.1 haben wir Studierendenkonten mittels Vererbung von Standardkonten abgeleitet. Reimplementieren Sie die Klasse *TrustMeStudent* mit Hilfe von *Delegation*. Bietet Delegation in diesem Fall konkrete Vorteile?

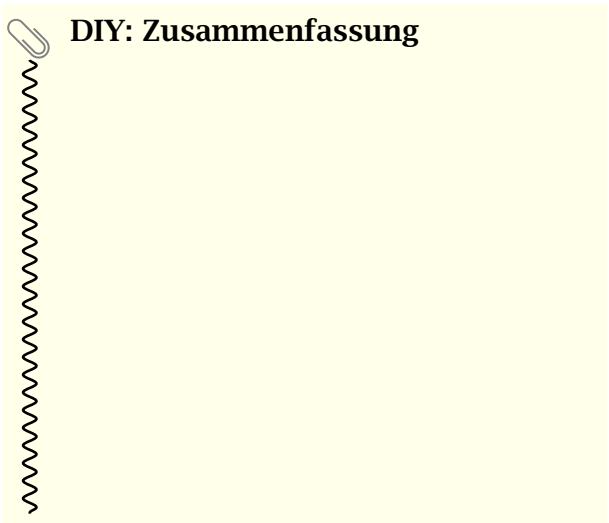
2. Komplettieren Sie die alternative Implementierung des Schablonen-Entwurfsmusters, indem Sie die Schnittstelle *ITwoPlayerGame* mit Leben füllen: Definieren Sie konkrete Spiele (zum Beispiel Nim oder Hackenbush) mit Objektausdrücken oder mit Hilfe von Klassen.

3. Die Klasse *Subject* erlaubt es, neue Beobachter hinzuzufügen (etwa wenn ein Zeitschriftenabonnement abgeschlossen wird), aber nicht einen Beobachter zu entfernen (etwa wenn das Abonnement ausläuft oder gekündigt wird). Tatsächlich kann aus prinzipiellen Gründen keine *Remove* Methode definiert werden, da die Gleichheit von Funktionen nicht formal entscheidbar ist. (Zwei Funktionen f und g sind gleich, wenn sie für gleiche Argumente gleiche Ergebnisse liefern: $f\ x = g\ x$, für alle x. Wäre die Gleichheit von Funktionen entscheidbar, dann könnte man Übungsblätter korrigieren, indem man die Abgaben mit den Musterlösungen vergleicht, zum Beispiel, *student-sort* = *trusted-sort*. Leider gelingt das nicht in voller Schönheit — wäre auch zu schön gewesen.) Was ist zu tun? Eine Möglichkeit besteht darin, die Beobachterfunktion als Objekt einzukleiden.

```
type Observer ⟨'state⟩ =
  interface
    abstract Update : 'state → Unit
  end
```

Warum löst dieser Kniff das Problem der unentscheidbaren Gleichheit? Bei Objekten wird nicht die ***Wertegleichheit***, sondern die ***Verweisgleichheit*** zugrundegelegt, siehe auch Aufgabe 7.2.1. Genau wie Speicherzellen haben Objekte eine eindeutige Identität (»*all objects are created unequal*«). Führen Sie die notwendigen Änderungen durch und fügen Sie eine Methode *Remove* hinzu, die es ermöglicht, einen Beobachter zu entfernen.

Zusammenfassung und Anmerkungen



A. Wunsch und Wirklichkeit: Mini–F# versus F#

Unterschiede in der lexikalischen Syntax Die Lehrsprache Mini–F# ist eng angelehnt an die Programmiersprache F#. Idealerweise ist jedes Mini–F# Programm ein gültiges F# Programm. Aus didaktischen Gründen sowie aus Gründen der Lesbarkeit und Bequemlichkeit weicht allerdings die *lexikalische Syntax* von Mini–F# in einigen Details von F# ab. Einige wenige Punkte sind zu beachten, wenn Ausdrücke oder Programme aus dem Skript oder den Vorlesungsfolien übernommen werden. Die folgende Gegenüberstellung illustriert zwei wichtige Unterschiede.

```
let rec ggt (m : Nat, n : Nat) : Nat =
  if   m = 0 then n
  elif n = 0 then m
  elif m ⩾ n then ggt (m % n, n)
  else            ggt (m, n % m)
```

```
let rec ggt(m: Nat, n: Nat): Nat =
    if   m =  0N then n
    elif n =  0N then m
    elif m >= n  then ggt(m % n, n)
    else              ggt(m, n % m)
```

Der wichtigste Unterschied: Natürliche Zahlen müssen in F# mit dem Suffix `N` gekennzeichnet werden, also `0N` statt 0 und `4711N` statt 4711. Das liegt daran, dass F# im Unterschied zu Mini–F# viele verschiedene Zahlentypen kennt (`47uy` ist zum Beispiel ein vorzeichenloses »Byte«, eine natürliche Zahl aus dem Bereich von 0 bis $2^8 - 1 = 255$).

Operatoren und Bezeichner werden in Mini–F# aufgehübscht. Die Vergleichsoperation ⩾ (in Mini–F# ein Zeichen) muss in F# mit `>=` (zwei Zeichen) notiert werden.

Mini–F#	F#	Mini–F#	F#
$a < b$	`a < b`	$a + b$	`a + b`
$a \leqslant b$	`a =< b`	$a \dot{-} b$	`a - b`
$a = b$	`a = b`	$a * b$	`a * b`
$a <> b$	`a <> b`	$a \div b$	`a / b`
$a \geqslant b$	`a >= b`	$a \,\%\, b$	`a % b`
$a > b$	`a > b`		

Die konkrete Syntax für die natürliche Subtraktion $\dot{-}$ ist `-`. Die Subtraktion auf den natürlichen Zahlen »$\dot{-}$« und die Subtraktion auf den reellen Zahlen »–« haben sehr unterschiedliche Eigenschaften. Aus diesem Grund ist es hilfreich, sie einfach im Text unterscheiden zu können. Die natürliche Division $\div$ wird in F# mit `/` notiert. Auch hier ist der Grund für die Diskrepanz ein didaktischer: Die Notation »$\div$« erinnert stets daran, dass die Division auf den natürlichen Zahlen (und auch auf den ganzen Zahlen) sich stark von der Division auf den reellen Zahlen »/« unterscheidet.

In Mini–F# dürfen Bezeichner Bindestriche enthalten; in F# ist das nicht erlaubt: Aus *total-area* wird in F# zum Beispiel `totalArea`. In Mini–F# nehmen wir uns weiterhin die Freiheit, Bezeichner mit einem Index zu versehen; in F# ist das nicht erlaubt: Aus s_1 wird in F# `s1`. (Hier spiegeln sich meine persönlichen Vorlieben wider, für die Sie mich gerne kritisieren können — sehen Sie es als Herausforderung, geistig flexibel zu bleiben.)

Interpreter \Read-Eval-Print-Loop Programme können mit dem Interpreter, der sogenannten Read-Eval-Print-Loop (REPL), einfach ausgeführt, ausprobiert und getestet werden. Der *virtuelle* Mini–F# Interpreter und der *reale* F# Interpreter unterscheiden sich ebenfalls in einigen Details.

```
⋙ 47 * 11
517
⋙ it * it
267289
⋙ reduce (*) [1..10]
3628800
⋙ ggt (2*2*3*7, 2*5*7)
14
```

```
> 47N * 11N ;;
val it : Nat = 517N
> it * it ;;
val it : Nat = 267289N
> List.reduce (*) [1..10] ;;
val it : int = 3628800
> let rec ggt(m: Nat, n: Nat): Nat =
-     if   m =  0N then n
-     elif n =  0N then m
-     elif m >= n  then ggt(m % n, n)
-     else              ggt(m, n % m) ;;
val ggt : m:Nat * n:Nat -> Nat
> ggt (2N*2N*3N*7N, 2N*5N*7N) ;;
val it : Nat = 14N
```

Das sogenannte ***Prompt***, die Eingabeaufforderung, ist jeweils unterschiedlich. Mini-F# verwendet »⋙ «; F# unterscheidet zwei Aufforderungszeichen: »> « kennzeichnet den Start einer Eingabe; eine noch unvollständige Eingabe wird durch »- « angezeigt. Da sich Eingaben in F# über mehrere Zeilen erstrecken können, muss das Eingabeende explizit durch `;;` angezeigt werden. Die Antwort auf eine Eingabe fällt in F# etwas ausführlicher aus: Mit ***val*** $it : t = v$ wird neben dem Wert v auch sein Typ t ausgegeben. Der Wert wird an den Bezeichner *it* gebunden und steht für weitere Rechnungen zur Verfügung.

Das Modulsystem von F# F# verfügt über ein einfaches ***Modulsystem***, mit dessen Hilfe Ausdrücke und Deklarationen zu größeren konzeptionellen Einheiten zusammengefasst werden können. In der Vorlesung selbst wird das Modulsystem nicht thematisiert (siehe aber Kapitel 8); für die praktischen Übungen sind Module zwar nicht unverzichtbar, jedoch sehr bequem. In der Regel werden Sie für jede Programmieraufgabe entweder ein »Modulskelett mit Leben füllen« oder ein eigenes Modul erstellen müssen. Bei der Softwareentwicklung hilft das Modulsystem größere oder große Softwaresysteme zu organisieren; in ähnlicher Weise wird die Organisation der Übungen und deren Lösung unterstützt: Es wird sichergestellt, dass sich Lösungen für verschiedene Aufgaben »nicht ins Gehege kommen« und Sie können, wenn die Aufgaben aufeinander aufbauen, Lösungen wieder- und weiterverwenden.

Schauen wir uns ein überschaubares Beispiel an.

module Introduction.Arithmetic

```
module Introduction.Arithmetic
let rec ggt (m : Nat, n : Nat) : Nat =
  if   m = 0 then n
  elif n = 0 then m
  elif m ≥ n then ggt (m % n, n)
  else            ggt (m, n % m)
let kgv (m : Nat, n : Nat) : Nat =
  (m * n) / ggt (m, n)
```

```
module Introduction.Arithmetic
let rec ggt(m: Nat, n: Nat): Nat =
    if   m =  0N then n
    elif n =  0N then m
    elif m >= n  then ggt(m % n, n)
    else              ggt(m, n % m)
let kgv(m: Nat, n: Nat): Nat =
    (m * n) / ggt (m, n)
```

Nach dem Schlüsselwort ***module*** wird der Name des Moduls angegeben —für jedes Modul müssen Sie sich einen Namen ausdenken bzw. geben wir in der Übung einen Namen vor. Die Beispielprogramme aus der Vorlesung sind der Übersichtlichkeit halber auf mehrere Ordner verteilt: Der Ordner `Introduction` enthält zum Beispiel die Programme aus Kapitel 1; das obige Programm befindet sich in diesem Ordner in der Datei `Arithmetic`. (Hinweise der Form

module *Introduction.Arithmetic* im Seitenrand weisen den Weg.) Das Modul kann man entweder im Interpreter mit dem Befehl `#load` »laden«

```
$ fsi Mini.fs
Microsoft (R) F# Interactive version 10.7.0.0 for F# 4.7
...
> #load "Introduction/Arithmetic.fs" ;;
> Introduction.Arithmetic.ggt(84N, 70N) ;;
val it : Nat = 14N
```

oder dem Interpreter beim Aufruf mit auf den Weg geben.

```
$ fsi Mini.fs Introduction/Arithmetic.fs
Microsoft (R) F# Interactive version 10.7.0.0 for F# 4.7
...
> Introduction.Arithmetic.ggt(84N, 70N) ;;
val it : Nat = 14N
```

F# kennt von Haus aus keine natürlichen Zahlen; das Modul `Mini.fs` bringt F# die natürlichen Zahlen und einige andere Dinge bei. Das von uns zur Verfügung gestellte Modul sollte beim Aufruf des Interpreters stets als erstes Argument angegeben werden.

Jedes Modul spannt einen eigenen Namensraum auf. In unterschiedlichen Modulen können die gleichen Bezeichner definiert werden, ohne dass sich diese ins Gehege kommen. Innerhalb eines Moduls gelten die üblichen Sichtbarkeitsregeln: *kgv* sieht zum Beispiel *ggt* und kann sich auf diese Funktion abstützen. Möchte man eine Funktion außerhalb eines Moduls verwenden, so muss man dem Bezeichner den Modulnamen voranstellen: Aus *ggt* wird der sogenannte ***qualifizierte*** Bezeichner *Introduction.Arithmetic.ggt* (siehe obige Interaktion). Alternativ lässt sich ein Modul »öffnen«.

```
> open Introduction.Arithmetic ;;
> ggt(84N, 70N) ;;
val it : Nat = 14N
```

Jetzt wird der Modulpräfix automatisch ergänzt. (Das Modul *Mini* wird übrigens immer automatisch geöffnet, so dass keine qualifizierten Bezeichner verwendet werden müssen.)

B. Kompendium Mathematik

Zwei Seelen wohnen, ach! in meiner Brust,
Die eine will sich von der andern trennen;
Die eine hält, in derber Liebeslust,
Sich an die Welt mit klammernden Organen;
Die andre hebt gewaltsam sich vom Dust
Zu den Gefilden hoher Ahnen.

— Johann Wolfgang von Goethe (1749–1832), *Faust I*

Das Kompendium gliedert sich in zwei Teile:

Der erste, kürzere Teil (Abschnitte B.1–B.3) fasst die wichtigsten mathematischen Begriffe und Notationen zusammen, die im Skript als bekannt vorausgesetzt werden. Die Übersicht ist als »Nachschlagewerk« konzipiert. — Vielleicht sind die Abschnitte hilfreich, verschüttetes mathematisches Grundwissen aufzufrischen; aufgrund der Kürze der Darstellung wird der Text allerdings weniger geeignet sein, in die Themengebiete einzuführen. Für eine Einführung in die Mathematik sei auf die einschlägigen Lehrbücher verwiesen und auf den Online Mathematik Brückenkurs (insbesondere das Zusatzmodul »Überblick: Logik und Mengenlehre«):

https://www.mathematik.uni-kl.de/studium/brueckenkurse/omb/

Im Einzelnen. Abschnitt B.1 taucht in die Welt der ***mathematischen Logik*** ein — wie kann ich Aussagen exakt formulieren und wie beweise ich sie? Abschnitt B.2 betreibt etwas ***Mengenlehre*** — wir sortieren Grundbegriffe wie Menge, Relation, Abbildung und werfen einen Blick auf die Unendlichkeit. Abschnitt B.3 greift noch einmal das Beweisen auf und erklärt das Dominoprinzip, vulgo das Prinzip der ***Induktion***.

Der zweite, längere Teil (Abschnitte B.4–B.6) vertieft den Lehrstoff des Hauptteils, vornehmlich der Kapitel 3, 5 und 6, und bespricht insbesondere Themen, die in anderen Vorlesungen nicht oder nur am Rande behandelt werden. Im Einzelnen. Ordnung ist das halbe Leben« wie man so schön sagt — Abschnitt B.4 führt in die Welt der ***Ordnungs***- und ***Verbandstheorie*** ein. Im Hauptteil haben wir das Rechnen mit Zahlen als hausbackenen Sonderfall diffamiert — Abschnitt B.5 leistet Abbitte und erklärt die ***Arithmetik***,die Mathematik hinter dem Rechnen. Was haben Optimierungsprobleme und Grammatiken gemeinsam? Abschnitt B.6 erklimmt einige Sprossen auf der Abstraktionsleiter und führt ein Juwel der Mathematik ein: ***Galoisverbindungen***.

Mit einem oder zwei Sternen ⋆ markierte Abschnitte enthalten weiterführenden oder anspruchsvolleren Stoff und/oder richten sich in erster Linie an mathematisch interessierte Leser/-innen. Aber lassen Sie sich dadurch nicht abschrecken …

B.1. Logik und Algebra

B.1.1. Aussagenlogik

Eine ***Aussage*** ist ein Satz, für den es sinnvoll ist zu fragen, ob er falsch oder wahr ist. Je nach Teilgebiet der Mathematik oder Informatik werden die ***Wahrheitswerte*** unterschiedlich notiert:

- »falsch« unter anderem als 0, $\bot$, f, F oder *false*;

- »wahr« als 1, $\top$, w, t, T oder *true*.

Aussagen werden mit Hilfe von »nicht«, »und«, »oder«, »wenn, dann«, »genau dann, wenn« usw. zu komplexen Aussagen verknüpft. Auch die Bezeichnungen für diese ***aussagenlogischen Verknüpfungen*** sind nicht einheitlich und variieren von Lehrbuch zu Lehrbuch:

- die ***Negation*** von a wird unter anderem durch $\neg a$, $\bar{a}$, a' oder *not a* bezeichnet;
- die ***Konjunktion*** von a und b durch $a \wedge b$, $a \cdot b$, ab oder a && b;
- die ***Disjunktion***[1] (Adjunktion) von a und b durch $a \vee b$, $a + b$ oder a || b;
- die ***Implikation*** (Subjunktion) von a und b durch $a \Rightarrow b$, $a \to b$ oder $a \leqslant b$;
- die ***Äquivalenz*** (Bijunktion) von a und b durch $a \Leftrightarrow b$, $a \leftrightarrow b$, $a \equiv b$ oder $a = b$.

Die Bedeutung der Verknüpfungen wird mit Hilfe von ***Wahrheitstabellen*** festgelegt.

a	$\neg a$
0	1
1	0

a	b	$a \wedge b$	$a \vee b$	$a \Rightarrow b$	$a \Leftarrow b$	$a \Leftrightarrow b$
0	0	0	0	1	1	1
0	1	0	1	1	0	0
1	0	0	1	0	1	0
1	1	1	1	1	1	1

Zwischen den Verknüpfungen gelten die folgenden Beziehungen, die sich mit Hilfe der Wahrheitstabellen nachprüfen lassen (siehe Aufgabe B.1.1).

$$\begin{aligned} \neg a &= a \Rightarrow 0 \\ a \wedge b &= \neg(a \Rightarrow \neg b) \\ a \vee b &= \neg a \Rightarrow b \\ a \Rightarrow b &= \neg a \vee b \\ a \Leftarrow b &= a \vee \neg b \\ a \Leftrightarrow b &= (a \Rightarrow b) \wedge (a \Leftarrow b) \end{aligned} \tag{B.1}$$

Man sagt auch, die Aussagen $\neg a$ und $a \Rightarrow 0$ sind äquivalent, und schreibt die Gleichheit mit dem Doppelpfeil der Äquivalenz: $(\neg a) \Longleftrightarrow (a \Rightarrow 0)$. Wir verwenden für die Gleichheit von Wahrheitswerten sowohl das normale Gleichheitszeichen als auch das Äquivalenzsymbol.

Beweise und Beweistechniken Viele mathematische Sätze, Lemmata und Theoreme, haben die Form einer Implikation $a \Longrightarrow b$. Die Aussage a heißt ***Voraussetzung*** oder ***Annahme*** und b ***Behauptung*** oder ***Folgerung***. Hat die Annahme die Form einer Konjunktion $a_1 \wedge \cdots \wedge a_n$, so spricht man auch von Annahmen (Plural). Um $a \Longrightarrow b$ zu beweisen, müssen wir unter der Annahme, dass a wahr ist, die Behauptung b zeigen.

Ein ***Beweis durch Kontraposition*** (engl. proof by contrapositive) zeigt die Implikation $a \Longrightarrow b$ *indirekt*: Unter der Annahme, dass $\neg b$ wahr ist, wird die Aussage $\neg a$ gezeigt.

$$(a \Rightarrow b) = (\neg a \Leftarrow \neg b) \qquad\qquad (a \Leftrightarrow b) = (\neg a \Leftrightarrow \neg b)$$

Beachte, dass sich die Richtung der Implikation umkehrt.

[1] Der Begriff »Disjunktion« ist etwas unglücklich gewählt, da er die falsche Assoziation weckt, dass sich die beiden Teilaussagen ausschließen müssen (»entweder … oder«). Das ist nicht der Fall.

Jede natürliche Zahl ist entweder ***gerade***, von der Form $2 \cdot n$, oder ***ungerade***, von der Form $2 \cdot n + 1$. Um die Aussage

$$a^2 \text{ gerade} \quad \Longrightarrow \quad a \text{ gerade}$$

zu etablieren, zeigen wir deren Kontraposition:

$$a^2 \text{ ungerade} \quad \Longleftarrow \quad a \text{ ungerade}$$

Wir nehmen an, dass a ungerade ist, also von der Form $2 \cdot n + 1$, und berechnen a^2.

$$(2 \cdot n + 1)^2 = 4 \cdot n^2 + 4 \cdot n + 1 = 2 \cdot (2 \cdot n^2 + 2 \cdot n) + 1$$

Damit ist auch a^2 ungerade.

.....

Euklids Beweis, dass $\sqrt{2}$ ***irrational*** ist, etabliert eine negative Aussage: $\sqrt{2}$ lässt sich *nicht* als Bruch darstellen ($\sqrt{2} \in \mathbb{R} - \mathbb{Q}$). Zum Beweis nehmen wir die positive Aussage an: Es gibt natürliche Zahlen a und b, so dass $a/b = \sqrt{2}$. Wir nehmen weiterhin an, dass a/b in gekürzter Form vorliegt: a und b sind teilerfremd, a ***gcd*** $b = 1$, siehe auch Abschnitt B.5.4.

$$a/b = \sqrt{2} \quad \Longrightarrow \quad a^2 = 2 \cdot b^2$$

Also ist a^2 gerade und damit auch a. Setzen wir $a := 2 \cdot n$ in die Gleichung $a^2 = 2 \cdot b^2$ ein, erhalten wir

$$(2 \cdot n)^2 = 2 \cdot b^2 \quad \Longrightarrow \quad 2 \cdot n^2 = b^2$$

Damit ist auch b^2 gerade und folglich b. Wir haben einen Widerspruch zur Annahme hergeleitet, dass a/b in gekürzter Form vorliegt.

.....

Als Beispiel für einen Beweis durch Widerspruch zeigen wir: Es gibt irrationale Zahlen, deren Potenzwert rational ist. Wir nehmen das Gegenteil der Aussage an: Für alle irrationalen Zahlen a und b ist auch a^b irrational. Nach Euklid ist $x := \sqrt{2}$ irrational und damit gemäß der Annahme auch x^x. Wir wenden die Annahme ein zweites Mal an und schlussfolgern, dass auch $(x^x)^x$ irrational sein muss. Aber

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2} \cdot \sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$

ist tatsächlich rational — ein Widerspruch. (Ein Widerspruchsbeweis ist *nicht* konstruktiv. Wir haben keine irrationale Zahlen gefunden, deren Potenzwert rational ist. Die Potenz $\sqrt{2}^{\sqrt{2}}$ ist tatsächlich irrational, sogar transzendent, aber das zeigt der Beweis nicht. Um diese konkrete Aussage nachzuweisen, muss man sich erheblich mehr abstrampeln.)

Abbildung B.1.: Kontrapositionsbeweis, Beweis einer Negation, Widerspruchsbeweis.

Gilt die Implikation $a \Longleftarrow b$, so ist b eine ***hinreichende Bedingung*** für a. Gilt umgekehrt $a \Longrightarrow b$, so ist b eine ***notwendige Bedingung*** für a. Die Logik des Begriffs erschließt sich, wenn man die Kontraposition bildet: $\neg a \Longleftarrow \neg b$. Also: Wenn b nicht gilt, dann gilt auch a nicht — insofern ist b notwendig für die Gültigkeit von a.

Ein ***Beweis durch Widerspruch*** (engl. proof by contradiction, lat. reductio ad absurdum) zeigt die Aussage a, indem unter der Annahme, dass a falsch ist, ein Widerspruch hergeleitet wird.

$$a = (\neg a \Rightarrow \mathit{false})$$

Nicht ganz zutreffend werden manchmal auch Beweise negativer Aussagen (engl. proof of negation) als Widerspruchsbeweise klassifiziert.

$$\neg a = (a \Rightarrow \mathit{false})$$

Eine negative Aussage $\neg a$ wird gezeigt, indem aus a ein Widerspruch abgeleitet wird. Abbildung B.1 illustriert die verschiedenen Beweistechniken mit Beispielen.

Übungen.

1. Zeigen Sie die Beziehungen zwischen den aussagenlogischen Verknüpfungen (B.1) mit Hilfe der Wahrheitstabellen. Finden Sie weitere Beziehungen.

2. Inwiefern kann ein Beweis durch Widerspruch als Spezialfall der Kontraposition angesehen werden?

3. Eine Zahl ist genau dann gerade, wenn sie durch 2 teilbar ist. Zeigen Sie

$$a \cdot b \text{ gerade} \quad \Longrightarrow \quad a \text{ gerade} \ \vee \ b \text{ gerade}$$

mittels Kontraposition. Gilt eine entsprechende Aussage auch für Teilbarkeit durch 3? Und Teilbarkeit durch 4?

B.1.2. Boolesche Algebra

Die beiden Wahrheitswerte bilden zusammen mit den Verknüpfungen »nicht«, »und« und »oder« eine sogenannte ***Boolesche Algebra***, eine mathematische Struktur, die die Gesetze in Abbildung B.2 erfüllt. Es lohnt sich, die Gesetze und deren Namen einzuprägen. Drei Gesetze verdienen besondere Beachtung:

Das ***Assoziativgesetz*** $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ erlaubt es, drei oder mehr Aussagen mit »und« zu verknüpfen, ohne Klammern setzen zu müssen: $a \wedge b \wedge c$ — eine wichtige Schreiberleichterung.

Das ***Kommutativgesetz*** $a \wedge b = b \wedge a$ besagt, dass weiterhin die Reihenfolge der Einzelaussagen keine Rolle spielt. Die Konjunktion von drei Aussagen kann zum Beispiel auf sechs Weisen formuliert werden (warum sechs?):

$$a \wedge b \wedge c = a \wedge c \wedge b = b \wedge a \wedge c = b \wedge c \wedge a = c \wedge a \wedge b = c \wedge b \wedge a$$

Das ***Distributivgesetz*** $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ regelt schließlich das Zusammenspiel von Konjunktion und Disjunktion. Von links nach rechts gelesen wird die Formel »ausmultipliziert«; von rechts nach links gelesen wird ein gemeinsamer »Faktor« herausgezogen. (Auch die ganzen Zahlen mit Addition und Multiplikation erfüllen ein Distributivgesetz: $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$.)

Die Anordnung der Gesetze in zwei Spalten veranschaulicht das ***Dualitätsprinzip***: Ersetze ich in einer Formel systematisch 0 durch 1, 1 durch 0, $\wedge$ durch $\vee$ und $\vee$ durch $\wedge$, erhalte ich die *duale* Formel aus der anderen Spalte — die Involution $\neg(\neg a) = a$ ist zu sich selbst dual. Allgemein gilt, dass ein Gesetz genau dann wahr ist, wenn das duale Gesetz wahr ist (»Buy one get one free!«). Die obigen Ausführungen zur Assoziativität, Kommutativität und Distributivität treffen somit in gleicher Weise auf die Disjunktion zu. (Das Dualitätsprinzip gilt *nicht* für die ganzen Zahlen mit Addition und Multiplikation: Die Multiplikation distribuiert über die Addition, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, aber *nicht* umgekehrt, $a + (b \cdot c) = (a + b) \cdot (a + c)$.)

Axiome der Booleschen Algebra:

	konjunktive Axiome	disjunktive Axiome
(Assoziativität)	$(a \wedge b) \wedge c = a \wedge (b \wedge c)$	$(a \vee b) \vee c = a \vee (b \vee c)$
(Kommutativität)	$a \wedge b = b \wedge a$	$a \vee b = b \vee a$
(Idempotenz)	$a \wedge a = a$	$a \vee a = a$
(Adjunktivität)	$a \wedge (a \vee b) = a$	$a \vee (a \wedge b) = a$
(Distributivität)	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
(Neutralität)	$a \wedge 1 = a$	$a \vee 0 = a$
(Extreme)	$a \wedge 0 = 0$	$a \vee 1 = 1$
(Komplementarität)	$a \wedge \neg a = 0$	$a \vee \neg a = 1$

Die Gesetze sind nicht voneinander unabhängig: So folgen etwa (Assoziativität), (Idempotenz), (Adjunktivität) und (Extreme) aus den vier sogenannten ***Huntington-Axiomen***: (Kommutativität), (Distributivität), (Neutralität) und (Komplementarität).

Folgerungen aus den Axiomen:

(Dualität)	$\neg 1 = 0$	$\neg 0 = 1$
(Involution)	$\neg(\neg a) = a$	$\neg(\neg a) = a$
(De Morgansche Gesetze)	$\neg(a \wedge b) = \neg a \vee \neg b$	$\neg(a \vee b) = \neg a \wedge \neg b$
	konjunktive Axiome	disjunktive Axiome

Abbildung B.2.: Axiome der Booleschen Algebra und Folgerungen aus den Axiomen.

Übungen.

4. Zeigen Sie, dass aus der Adjunktivität von $\wedge$ und $\vee$ deren Idempotenz folgt.

5. Versuchen Sie, die Dualitätsgesetze, das Involutionsgesetz und die De Morganschen Gesetze aus den Axiomen der Booleschen Algebra zu folgern, siehe Abbildung B.2.

6. Möchte man nachweisen, dass eine Struktur eine Boolesche Algebra ist, muss man weniger Aufwand betreiben, als die Definition es vermuten lässt: Zeigen Sie, dass die in Abbildung B.2 aufgeführten Axiome der Booleschen Algebra bereits aus den vier Huntington-Axiomen folgen.

(Kommutativität)	$a \wedge b = b \wedge a$	$a \vee b = b \vee a$
(Distributivität)	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
(Neutralität)	$a \wedge 1 = a$	$a \vee 0 = a$
(Komplementarität)	$a \wedge \neg a = 0$	$a \vee \neg a = 1$

Zeigen Sie, dass die Huntington-Axiome voneinander unabhängig sind, indem Sie Beispiele, sogenannte Modelle, konstruieren, für die jeweils drei der vier Axiome gelten, aber das vierte nicht.

B.1.3. Prädikatenlogik

Mit den bisherigen Sprachmitteln lassen sich nur endlich viele Aussagen miteinander verknüpfen. Oft trifft man aber Aussagen über alle Elemente einer Menge. Die starke Goldbachsche Vermutung besagt zum Beispiel, dass »jede gerade Zahl, die größer als 2 ist, sich als Summe zweier Primzahlen schreiben lässt.« Wenn wir die Menge der natürlichen Zahlen mit $\mathbb{N}$ und die Menge der Primzahlen mit $\mathbb{P}$ bezeichnen, dann lässt sich die Aussage mit Hilfe sogenannter ***Quantoren*** wie folgt formalisieren:

$$\forall\, n \in \mathbb{N} \;.\; \exists\, p_1 \in \mathbb{P} \;.\; \exists\, p_2 \in \mathbb{P} \;.\; n = p_1 + p_2$$

Hier bedeutet $n \in \mathbb{N}$, dass n ein Element der Menge $\mathbb{N}$ ist, also eine natürliche Zahl. Das gespiegelte »A« und das gespiegelte »E« sind Quantoren:

- ***Existenzquantor***: es existiert ein $x \in \mathrm{X}$, so dass die Aussage $\mathrm{P}(x)$ gilt;

  $$\exists\, x \in \mathrm{X} \;.\; \mathrm{P}(x)$$

- ***Allquantor***: für alle $x \in \mathrm{X}$ gilt die Aussage $\mathrm{P}(x)$.

  $$\forall\, x \in \mathrm{X} \;.\; \mathrm{P}(x)$$

Dabei ist $\mathrm{P}(x)$ eine sogenannte ***Aussagenfunktion***, eine Aussage, die eine oder mehrere Variablen enthält und zu einer Aussage wird, wenn die Variablen durch Elemente der Menge X ersetzt werden.

Der Existenzquantor verallgemeinert die Disjunktion und wird aus diesem Grund manchmal auch mit $\bigvee x \in \mathrm{X}$ notiert; entsprechend verallgemeinert der Allquantor die Konjunktion und wird mit $\bigwedge x \in \mathrm{X}$ notiert. Besteht die Menge X nur aus endlich vielen Elementen, zum Beispiel $x_1, \ldots, x_n$, dann gilt:

$$\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \;=\; \mathrm{P}(x_1) \vee \cdots \vee \mathrm{P}(x_n) \qquad \exists\, x \in \varnothing \,.\, \mathrm{P}(x) \;=\; \mathit{false}$$
$$\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \;=\; \mathrm{P}(x_1) \wedge \cdots \wedge \mathrm{P}(x_n) \qquad \forall\, x \in \varnothing \,.\, \mathrm{P}(x) \;=\; \mathit{true}$$

Ist die Menge leer, $\mathrm{X} = \varnothing$, dann ist die Existenzaussage falsch und die Allaussage wahr!

Für das Arbeiten mit Quantoren sind die folgenden Gesetze nützlich — die Auflistung erhebt aber keinen Anspruch auf Vollständigkeit. Sei $a \in \mathrm{X}$, dann

$$\mathrm{P}(a) \implies \exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \tag{B.2a}$$
$$\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \implies \mathrm{P}(a) \tag{B.2b}$$
$$p \wedge (\exists\, x \in \mathrm{X} \,.\, \mathrm{Q}(x)) \iff \exists\, x \in \mathrm{X} \,.\, p \wedge \mathrm{Q}(x) \tag{B.2c}$$
$$p \vee (\forall\, x \in \mathrm{X} \,.\, \mathrm{Q}(x)) \iff \forall\, x \in \mathrm{X} \,.\, p \vee \mathrm{Q}(x) \tag{B.2d}$$
$$p \Rightarrow (\forall\, x \in \mathrm{X} \,.\, \mathrm{Q}(x)) \iff \forall\, x \in \mathrm{X} \,.\, p \Rightarrow \mathrm{Q}(x) \tag{B.2e}$$
$$(\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \Rightarrow q \iff \forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \Rightarrow q \tag{B.2f}$$
$$\exists\, x \in \mathrm{X} \,.\, \mathit{false} \iff \mathit{false} \tag{B.2g}$$
$$\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \vee \mathrm{Q}(x) \iff (\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \;\vee\; (\exists\, x \in \mathrm{X} \,.\, \mathrm{Q}(x)) \tag{B.2h}$$
$$\forall\, x \in \mathrm{X} \,.\, \mathit{true} \iff \mathit{true} \tag{B.2i}$$
$$\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \wedge \mathrm{Q}(x) \iff (\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \;\wedge\; (\forall\, x \in \mathrm{X} \,.\, \mathrm{Q}(x)) \tag{B.2j}$$
$$\neg(\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \iff \forall\, x \in \mathrm{X} \,.\, \neg\mathrm{P}(x) \tag{B.2k}$$
$$\neg(\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \iff \exists\, x \in \mathrm{X} \,.\, \neg\mathrm{P}(x) \tag{B.2l}$$

B.1.4. Rund um's Formalisieren und Beweisen

»Aber es sind Gleichungen!« sagte sie. »Und das ist nicht gerade das, worauf die Leute sich stürzen. …«

— Ulrich Woelk (1960), *Joana Mandelbrot und ich*

Im Anhang, wie auch im gesamten Skript, vermeiden wir den beliebten mathematischen Dreisprung von Definition, Satz und Beweis. Neue Konzepte werden in der Regel ohne viel Brimborium eingeführt. Um trotzdem das Auffinden von Definitionen zu erleichtern, heben wir neu eingeführte Fachbegriffe ***typographisch*** hervor und machen neu eingeführte Bezeichner und Symbole mit Hilfe eines Doppelpunkts kenntlich. Mittels der Gleichung $u := k$ oder $k =: u$ wird u durch k definiert; der Doppelpunkt steht jeweils auf der Seite der definierten Größe. Für die Lateiner/-innen unter Ihnen:

Definiendum := Definiens Definiens =: Definiendum

Zum Beispiel hätten wir uns bei den aussagenlogischen Verknüpfungen darauf beschränken können, Negation, Konjunktion und Disjunktion mit Wahrheitstabellen einzuführen, um sodann die restlichen Konnektoren auf diese zurückzuführen: $a \Rightarrow b :\iff \neg a \vee b$, $a \Leftarrow b :\iff a \vee \neg b$ und $a \Leftrightarrow b :\iff (a \Rightarrow b) \wedge (a \Leftarrow b)$, wobei die Gleichheit von Wahrheitswerten mit dem Äquivalenzsymbol gekennzeichnet wird.

Gleichheitsbeweise Den meisten von Ihnen werden Gleichheitsbeweise geläufig sein: Wir reihen Gleichungen aneinander, $\tan 45^\circ = \sin 45^\circ / \cos 45^\circ = \big(1/\sqrt{2}\big)\big/\big(1/\sqrt{2}\big) = 1$, um daraus den gewünschten Sachverhalt, $\tan 45^\circ = 1$, zu folgern. Dabei nutzen wir wesentlich aus, dass die Gleichheitsrelation ***transitiv*** ist: Aus $a = b$ und $b = c$ folgt $a = c$. Beim Lesen und Verstehen von Gleichheitsbeweisen gilt es zu erkennen, welches Gesetz, welche Eigenschaft in welchem Schritt zur Anwendung kommt. Um diesen kognitiven Prozess zu unterstützen, favorisieren und verwenden

wir ein Beweisformat, das Kommentaren und Rechtfertigungen großzügigen Platz einräumt.

$$
\begin{aligned}
& \tan 45^\circ \\
= \quad & \{ \text{ Definition Tangens } \} \\
& \sin 45^\circ / \cos 45^\circ \\
= \quad & \{ \sin 45^\circ = 1/\sqrt{2} = \cos 45^\circ \} \\
& \left(1/\sqrt{2}\right)/\left(1/\sqrt{2}\right) \\
= \quad & \{ \text{ Arithmetik } \} \\
& 1
\end{aligned}
$$

Innerhalb der geschweiften Klammern geben wir jeweils an, warum eine Umformung gültig ist: $\tan 45^\circ$ ist gleich $\sin 45^\circ / \cos 45^\circ$ auf Grund der Definition der Tangensfunktion.

Ein Beweis ist ein Dialog, wenn auch ein stiller zwischen den Beweisführenden und den Beweisnachvollziehenden. Wie in jeder guten Konversation gilt es, sich auf die Gesprächspartner einzustellen — schließlich möchte man sie von der Korrektheit des Beweises und damit der Behauptung überzeugen. An zwei »Stellschrauben« kann man drehen: der Granularität der Schritte und dem Detaillierungsgrad der Rechtfertigungen. Die richtigen »Einstellungen« zu finden ist kein leichtes Unterfangen. Sehen Sie selbst — können Sie die folgende Rechnung problemlos nachvollziehen?

$$
\begin{aligned}
& \sin 112.5^\circ / \sin 22.5^\circ \\
= \quad & \{ \text{ Halbwinkelidentität: } \sin(\alpha/2) = \pm\sqrt{(1-\cos\alpha)/2} \} \\
& \sqrt{(1-\cos 225^\circ)/2}\Big/\sqrt{(1-\cos 45^\circ)/2} \\
= \quad & \{ \text{ Periodizität: } \cos(\alpha + 180^\circ) = -\cos\alpha \} \\
& \sqrt{(1+\cos 45^\circ)/2}\Big/\sqrt{(1-\cos 45^\circ)/2} \\
= \quad & \{ \text{ Arithmetik } \} \\
& (1+\cos 45^\circ)\Big/\sqrt{(1-\cos^2 45^\circ)} \\
= \quad & \{ \text{ Pythagoras: } \sin^2\alpha + \cos^2\alpha = 1 \} \\
& (1+\cos 45^\circ)/\sin 45^\circ \\
= \quad & \{ \sin 45^\circ = 1/\sqrt{2} = \cos 45^\circ \} \\
& \left(1+1/\sqrt{2}\right)/\left(1/\sqrt{2}\right) \\
= \quad & \{ \text{ Arithmetik } \} \\
& 1+\sqrt{2}
\end{aligned}
$$

Ist insbesondere der dritte mit »Arithmetik« begründete Schritt nachvollziehbar? Führt man je-

den einzelnen Zwischenschritt aus (mit der Abkürzung $x := \cos 45°$),

$$
\begin{aligned}
& \sqrt{(1+x)/2}\big/\sqrt{(1-x)/2} \\
= \quad & \{ \text{ Potenzgesetze: } \sqrt{a}\big/\sqrt{b} = \sqrt{a/b} \ \} \\
& \sqrt{((1+x)/2)\big/((1-x)/2)} \\
= \quad & \{ \text{ Bruchrechnen: } (a/2)\big/(b/2) = a/b \ \} \\
& \sqrt{(1+x)/(1-x)} \\
= \quad & \{ \text{ Bruchrechnen: mit } 1+x \text{ erweitern } \} \\
& \sqrt{(1+x)^2/((1-x)\cdot(1+x))} \\
= \quad & \{ \text{ binomische Formel: } (a+b)\cdot(a-b) = a^2 - b^2 \ \} \\
& \sqrt{(1+x)^2/(1-x^2)} \\
= \quad & \{ \text{ Potenzgesetze: } \sqrt{a}\big/\sqrt{b} = \sqrt{a/b} \text{ und } \sqrt{a^2} = a \ \} \\
& (1+x)\big/\sqrt{(1-x^2)}
\end{aligned}
$$

wird der Beweis um einiges länger, wahrscheinlich zu lang — Ermüdung ist auch ein nicht zu vernachlässigender Faktor. (Lassen Sie es mich wissen, wenn Sie einen eleganteren, kürzeren oder direkteren Beweis für $\sin 112.5°/\sin 22.5° = 1+\sqrt{2}$ finden.)

Bezeichner und Binder\Variablen und Quantoren Gleichheitsbeweise sind nicht zuletzt so attraktiv, weil sie eng mit dem Rechnen verwandt sind, einer Tätigkeit, mit der wir seit Kindesbeinen vertraut sind. Wenn wir einen Ausdruck ausrechnen — und damit beschäftigt sich der Hauptteil des Skripts — führen wir im Prinzip einen Gleichheitsbeweis; wir zeigen, dass der zu berechnende Ausdruck gleich dem berechneten Wert ist. Gleichheitsbeweise kommen etwas allgemeiner daher, da an die Stelle konkreter Werte wie $\cos 45°$ auch Bezeichner wie x treten können, wie bereits im letzten Beweis geschehen. Es lohnt sich, das Konzept von Bezeichnern, Platzhaltern und Variablen etwas genauer unter die Lupe zu nehmen (siehe auch Abschnitt 3.3).

Wir haben bereits regen Gebrauch von Variablen gemacht, etwa bei der Formulierung von Gesetzen und Axiomen, siehe Abbildung B.2. Variablen werden in der Regel durch sogenannte ***Binder*** eingeführt: in der Programmierung zum Beispiel durch Funktionsausdrücke (***fun*** $x \to x * x$) oder durch ***let***-Ausdrücke (***let*** $pi = 3.141592654$ ***in*** $pi * pi$), in der Analysis zum Beispiel mittels der Differentialnotation ($\int x^2 \,\mathrm{d}x$), in der Prädikatenlogik zum Beispiel durch All- oder Existenzquantoren ($\forall\, x \;.\; x + 0 = x$). Für Gleichungen gilt die oft stillschweigend getroffene Vereinbarung, dass alle in einer Gleichung auftretenden Variablen implizit *allquantifiziert* sind und der Geltungsbereich auf die jeweilige Gleichung beschränkt ist. Macht man die Quantoren explizit, zum Beispiel,

$$\text{(Adjunktivität)} \qquad (\forall\, a \;.\; \forall\, b \;.\; a \vee (a \wedge b) = a) \qquad (\forall\, a \;.\; \forall\, b \;.\; a \wedge (a \vee b) = a)$$

erkennt man, warum die Vereinbarung getroffen wird — die Lesbarkeit leidet doch arg. Gleiches gilt für Beweise, die Variablen involvieren: Diese sind implizit allquantifiziert, ihr Geltungsbereich erstreckt sich allerdings auf die gesamte Gleichungskette, nicht nur eine einzelne Gleichung. Die folgenden Beweise zeigen zum Beispiel, dass aus der Adjunktivität von $\wedge$ und $\vee$ deren Idempotenz folgt (damit lösen wir Aufgabe B.1.4).

$$
\begin{aligned}
& a \\
= & \quad \{ \text{ Adjunktivität Disjunktion } \} \\
& a \vee (a \wedge (a \vee b)) \\
= & \quad \{ \text{ Adjunktivität Konjunktion } \} \\
& a \vee a
\end{aligned}
\qquad\qquad
\begin{aligned}
& a \\
= & \quad \{ \text{ Adjunktivität Konjunktion } \} \\
& a \wedge (a \vee (a \wedge b)) \\
= & \quad \{ \text{ Adjunktivität Disjunktion } \} \\
& a \wedge a
\end{aligned}
$$

Da wir aus zwei Gesetzen zwei weitere folgern, haben wir es im Prinzip mit vier verschiedenen as zu tun, vier verschiedenen Vorkommen der gleichen Variable, die jeweils allquantifiziert ist. Zur Erinnerung: Aus der allquantifizierten Aussage $\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)$ können wir mittels ***Spezialisierung*** (B.2b) die Aussage $\mathrm{P}(a)$ ableiten, sofern $a \in \mathrm{X}$. Gelegentlich ist es hilfreich, die Ersetzung $x := a$ im Beweis explizit zu benennen. Die folgende Überarbeitung des Beweises von $a = a \vee a$ erhellt den ersten Beweisschritt.

$$
\begin{aligned}
& a \\
= & \quad \{ \text{ Adjunktivität Disjunktion mit } a := a \text{ und } b := a \vee b \ \} \\
& a \vee (a \wedge (a \vee b)) \\
= & \quad \{ \text{ Adjunktivität Konjunktion mit } a := a \text{ und } b := b \ \} \\
& a \vee a
\end{aligned}
$$

Im ersten Schritt wird die allquantifizierte Variable b in $a \vee (a \wedge b) = a$ durch den Ausdruck $a \vee b$ ersetzt. Im zweiten Schritt wenden wir das Gesetz $a \wedge (a \vee b) = a$ sozusagen »wortwörtlich« an. Der Beweis wird noch klarer und transparenter, wenn wir tatsächlich unterschiedliche Bezeichner verwenden.

$$
\begin{aligned}
& x \\
= & \quad \{ \text{ Adjunktivität Disjunktion mit } a := x \text{ und } b := x \vee y \ \} \\
& x \vee (x \wedge (x \vee y)) \\
= & \quad \{ \text{ Adjunktivität Konjunktion mit } a := x \text{ und } b := y \ \} \\
& x \vee x
\end{aligned}
$$

Aber: Sich Namen auszudenken ist mühsam, so dass oft die Klarheit der Bequemlichkeit zum Opfer fällt.

Iverson Klammer Manchmal sind es die kleinen Dinge, die einem das Leben erleichtern. Die folgende Konvention fällt in diese Kategorie — nicht notwendig, aber nützlich. Eine Aussage, die in eckige Klammern eingeschlossen wird, steht für 0, wenn sie falsch ist, und für 1, wenn sie wahr ist.

$$[\mathit{false}] = 0 \qquad\qquad [\mathit{true}] = 1$$

Vorsicht: Verwechseln Sie $[b]$ nicht mit einer einelementigen Liste. Die Notation geht auf Kenneth E. Iverson zurück und wird aus diesem Grund auch ***Iverson Klammer*** (engl. Iverson bracket) genannt.[2]

[2] Eine Bemerkung zur Syntax: Iverson benutzte runde statt eckiger Klammern. Das ist keine brillante Idee, da runde Klammern auch für Gruppierung von Ausdrücken und in der Mathematik auch für Funktionsaufrufe verwendet werden: $f(x)$ ist doppeldeutig — wird f auf a oder auf (a) angewendet?

Mit Hilfer der Iverson Klammer können unschöne Fallunterscheidungen in arithmetischen Formeln vermieden werden. Die Vorteile lassen sich am besten an einem konkreten Beispiel illustrieren: Traditionell werden die ***Vorzeichenfunktion*** $\operatorname{sign} x$ (lat. signum) und der ***Absolutwert*** $\operatorname{abs} x$ mittels einer expliziten Fallunterscheidung eingeführt.

$$\operatorname{sign} x := \begin{cases} -1 & \text{falls } x < 0 \\ 0 & \text{falls } x = 0 \\ 1 & \text{falls } x > 0 \end{cases} \qquad \operatorname{abs} x := \begin{cases} -x & \text{falls } x < 0 \\ 0 & \text{falls } x = 0 \\ x & \text{falls } x > 0 \end{cases}$$

Die Notation kommt etwas sperrig daher. Das merkt man schnell, wenn man die so definierten Funktionen in Rechnungen oder Beweisen verwenden möchte. Der erste Schritt in einem Beweis besteht in der Regel darin, eine Variable oder eine Funktion durch ihre Definition zu ersetzen — aber, wie falten wir zum Beispiel $\operatorname{sign} x \cdot \operatorname{sign} y$ auf?[3] Mit Hilfe der Inverson Klammer formulieren wir eleganter:

$$\operatorname{sign} x := [x > 0] - [x < 0] \qquad \operatorname{abs} x := [x > 0] \cdot x - [x < 0] \cdot x \tag{B.3}$$

Überzeugen Sie sich, dass die gleichen Funktionen definiert werden. Der Teilausdruck $[x > 0] \cdot x$ ergibt zum Beispiel x für positive x und 0 sonst.

Die Notation erfreut sich zunehmender Popularität, was nicht einer gewissen Ironie entbehrt. Aus Hygienegründen unterscheiden wir heutzutage streng zwischen Wahrheitswerten, *false* und *true*, und Zahlen, 0 und 1. Die Emanzipation der Wahrheitswerte von den Zahlen hat einige Zeit in Anspruch genommen — der Begründer der mathematischen Logik, George Boole, stellte die Wahrheitswerte noch durch die Zahlen 0 und 1 dar und drückte die aussagenlogischen Verknüpfungen durch entsprechende arithmetische Operationen aus, siehe Abbildung 3.2. Die Iverson Klammer dreht in gewissem Sinne die Geschichte zurück und hebt die Grenzen zwischen Wahrheitswerten und Zahlen fast wieder auf. Aber eben nur fast — die Notation $[\text{-}] : \mathbb{B} \to \mathbb{R}$ macht die vorgenommene *Typumwandlung* explizit. Booles Formeln aus Abbildung 3.2 korrespondieren zu Eigenschaften der Iverson Klammer (aussagenlogische Verknüpfungen à la Boole).

$$[\neg p] = 1 - [p] \qquad [p \wedge q] = [p] \cdot [q] \qquad [p \vee q] = [p] - [p] \cdot [q] + [q] \tag{B.4}$$

Bei der Disjunktion muss man etwas aufpassen: $[p \vee q]$ ist nur dann gleich $[p]+[q]$, wenn p und q sich ausschließen. Mit Hilfe der Iverson Klammer lassen sich beliebige Aussagen in Gleichungen überführen:

$$p \iff [p] = 1 \qquad \neg p \iff [p] = 0 \tag{B.5}$$

Um die Klammern in Aktion zu sehen, zeigen wir eine Eigenschaft der Vorzeichenfunktion: Das

[3] Wir könnten alternativ auf Notation aus der Programmierung zurückgreifen und die Vorzeichenfunktion mit Hilfe einer geschachtelten Alternative definieren: *sign x = **if** x < 0 **then** −1 **elif** x = 0 **then** 0 **else** 1*. Leider verschleiert diese Formulierung die vorhandene Symmetrie. Die Iverson Klammer spielt hier ihre Stärke aus, da einer der Zweige 0 ist.

Vorzeichen eines Produkts ist das Produkt der Vorzeichen.

$$
\begin{aligned}
& \operatorname{sign}(x \cdot y) \\
= & \quad \{ \text{ Definition sign (B.3) } \} \\
& [x \cdot y > 0] - [x \cdot y < 0] \\
= & \quad \{ \text{ Vorzeichenregeln } \} \\
& [(x > 0 \land y > 0) \ \lor \ (x < 0 \land y < 0)] - [(x < 0 \land y > 0) \ \lor \ (x > 0 \land y < 0)] \\
= & \quad \{ \text{ Durchschnitt und Vereinigung à la Boole (B.4) } \} \\
& ([x > 0] \cdot [y > 0] + [x < 0] \cdot [y < 0]) - ([x < 0] \cdot [y > 0] + [x > 0] \cdot [y < 0]) \\
= & \quad \{ \text{ Distributivgesetz } \} \\
& ([x > 0] - [x < 0]) \cdot ([y > 0] - [y < 0]) \\
= & \quad \{ \text{ Definition sign (B.3) } \} \\
& \operatorname{sign} x \cdot \operatorname{sign} y
\end{aligned}
$$

Zum Vergleich: Mit einer expliziten Fallunterscheidung müssten wir insgesamt $3 \cdot 3 = 9$ Fälle unterscheiden — jeder einzelne Fall ist trivial, aber würde der Beweis das auch reflektieren?

Iverson Klammer

Eine in eckige Klammern eingeschlossene Aussage steht für 0, wenn sie falsch ist, und für 1, wenn sie wahr ist.

Übungen.

7. Zeigen Sie die folgenden Gleichungen, *ohne* explizite Fallunterscheidungen zu verwenden. *Hinweis:* (B.5) erweist sich vielleicht als nützlich.

$$[x = 0] \cdot x = 0 \qquad\qquad [x \neq 0] \cdot x = x \tag{B.6}$$

8. Lisa verwendet alternative Definitionen für die Vorzeichenfunktion und den Absolutwert.

$$\operatorname{sign} x := [x \geqslant 0] - [x \leqslant 0] \qquad\qquad \operatorname{abs} x := [x \geqslant 0] \cdot x - [x \leqslant 0] \cdot x$$

Harry muss zweimal hinschauen, um den Unterschied zu den »offiziellen« Definitionen zu erkennen, und fragt sich, ob die Definitionen tatsächlich äquivalent sind.

9. Zeigen Sie die folgenden Beziehungen zwischen dem Absolutwert und der Vorzeichenfunktion. (Versuchen Sie wie in Aufgabe B.1.7, explizite Fallunterscheidungen zu vermeiden.)

$$\operatorname{abs} x = \operatorname{sign} x \cdot x \qquad\qquad x = \operatorname{sign} x \cdot \operatorname{abs} x$$

10. Zeigen Sie, dass sich das Maximum und das Minimum zweier Zahlen mit Hilfe der Iverson Klammer ausdrücken lassen.

$$a \uparrow b = [a \geqslant b] \cdot a + [a < b] \cdot b \tag{B.7a}$$
$$a \downarrow b = [a < b] \cdot a + [a \geqslant b] \cdot b \tag{B.7b}$$

Den Ausdrücken auf den rechten Seiten mangelt es an Symmetrie — lässt sich das »reparieren«? Verwenden Sie die Eigenschaften, um den folgenden Zusammenhang zu zeigen.

$$(a - b) \uparrow (b - a) = \operatorname{abs}(a - b) = \operatorname{abs}(b - a) = (a \uparrow b) - (a \downarrow b) \tag{B.7c}$$

B.2. Mengenlehre

Eine Menge ist eine Zusammenfassung von Elementen zu einer Einheit. Dabei spielt weder die Reihenfolge der Elemente noch deren Vielfachheit eine Rolle. Wir schreiben $x \in \mathrm{X}$, um auszudrücken, dass x ein Element der Menge X ist, und $x \notin \mathrm{X}$, wenn das nicht der Fall ist. Die leere

Menge wird mit $\varnothing$ bezeichnet. Da die leere Menge keine Elemente enthält, ist $x \in \varnothing$ stets falsch. Mit $|X|$ bezeichnen wir die ***Kardinalität*** oder ***Mächtigkeit*** der Menge X, also die Gesamtzahl ihrer Elemente, falls diese Anzahl endlich ist.

Die folgenden Bezeichnungen sind gebräuchlich:

- $\mathbb{B}$ ist die Menge der Wahrheitswerte (falsch und wahr);
- $\mathbb{N}$ ist die Menge der natürlichen Zahlen $(0, 1, 2, \ldots)$;
- $\mathbb{P}$ ist die Menge der Primzahlen $(2, 3, 5, 7, 11, 13, 17 \ldots)$;
- $\mathbb{Z}$ ist die Menge der ganzen Zahlen $(\ldots, -2, -1, 0, 1, 2, \ldots)$;
- $\mathbb{Q}$ ist die Menge der rationalen Zahlen (Bruchzahlen);
- $\mathbb{R}$ ist die Menge der reellen Zahlen.

Eine endliche Menge kann durch Aufzählung ihrer Elemente definiert werden:

$$\{2, 3, 5, 7\}$$

ist zum Beispiel die Menge der ersten vier Primzahlen. Da die Reihenfolge der Elemente irrelevant ist, kann die Menge alternativ durch $\{7, 5, 3, 2\}$ oder durch $\{3, 7, 5, 2\}$ angegeben werden. Auch $\{2, 2, 3, 3, 3, 5, 5, 5, 5, 5, 7, 7, 7, 7, 7, 7, 7\}$ bezeichnet die gleiche Menge, da irrelevant ist, wie häufig ein Element aufgeführt wird.

Eine endliche oder unendliche Menge kann durch eine sogenannte »Mengenbeschreibung« oder kurz »Beschreibung« (engl. set comprehension) definiert werden:

$$\{ x^2 \mid x \in \mathbb{N} \}$$

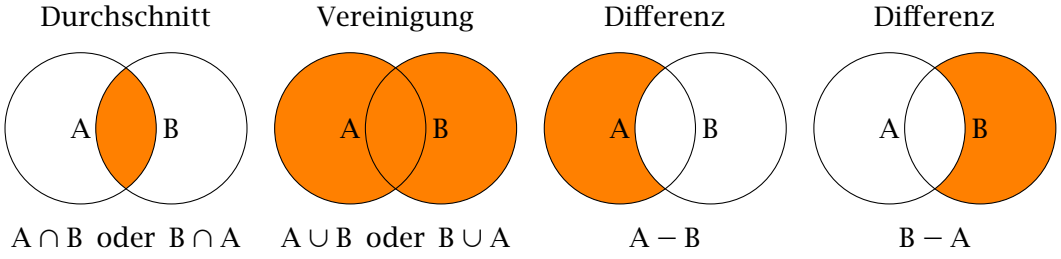
ist zum Beispiel die Menge der Quadratzahlen. *Lies:* »die Menge aller x^2, so dass x eine natürliche Zahl ist«.

B.2.1. Mengenoperationen

Aus zwei gegebenen Mengen lassen sich mit Hilfe der folgenden ***Mengenoperationen*** neue Mengen bilden.[4]

(Durchschnitt)	$A \cap B := \{ x \mid x \in A \wedge x \in B \}$
(Vereinigung)	$A \cup B := \{ x \mid x \in A \vee x \in B \}$
(Differenz)	$A - B := \{ x \mid x \in A \wedge x \notin B \}$

Die Operationen kann man sich durch sogenannte ***Venn-Diagramme*** veranschaulichen:



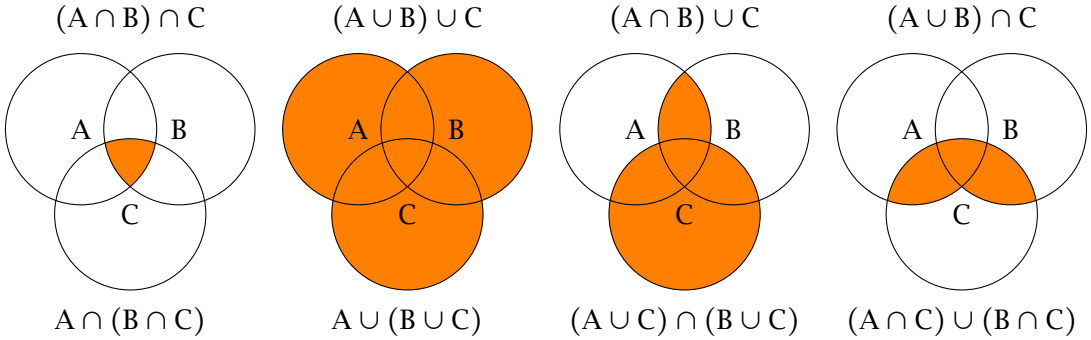
[4] Die Mengendifferenz wird üblicherweise mit $A \setminus B$ notiert, eine Notation, die eher einen Quotienten denn eine Differenz suggeriert. Wir reservieren Divisionssymbole für die Teilbarkeitsrelation, $a \setminus b$, siehe Abschnitte B.4.1 und B.5.4, und für Links- bzw. Rechtsfaktoren, a / b bzw. $a \setminus b$, siehe Abschnitt B.6.6.

Gemäß der Definition des Durchschnitts gilt $x \in A \cap B \iff x \in A \wedge x \in B$. Somit ziehen die Eigenschaften der Konjunktion entsprechende Eigenschaften des Mengendurchschnitts nach sich: Der Durchschnitt ist assoziativ, kommutativ und idempotent. Entsprechende Überlegungen gelten für die Mengenvereinigung: Auch sie ist assoziativ, kommutativ und idempotent. Die Menge der ersten vier Primzahlen kann zum Beispiel alternativ als Vereinigung einelementiger Mengen geschrieben werden:

$$\{2\} \cup \{3\} \cup \{5\} \cup \{7\} = \{3\} \cup \{7\} \cup \{5\} \cup \{2\} = \{2\} \cup \{3\} \cup \{2\} \cup \{7\} \cup \{5\} \cup \{3\}$$

Da die Mengenvereinigung assoziativ ist, müssen wir geschachtelte Vereinigungen nicht klammern; da sie kommutativ ist, spielt die Reihenfolge der Grundmengen keine Rolle; da sie idempotent ist, spielt keine Rolle, wie oft eine Grundmenge aufgeführt wird. Im Unterschied zum Durchschnitt und zur Vereinigung ist die Mengendifferenz weder assoziativ, noch kommutativ (siehe obige Venn-Diagramme), noch idempotent.

Auch das Zusammenspiel von Durchschnitt und Vereinigung lässt sich mit Hilfe von Venn-Diagrammen illustrieren.



Die ersten beiden Diagramme veranschaulichen die Assoziativität von Durchschnitt und Vereinigung. Die letzten beiden Diagramme »zeigen«, dass die Vereinigung über den Durchschnitt distribuiert und umgekehrt der Durchschnitt über die Vereinigung.

B.2.2. Konstruktionen auf Mengen

Die Menge A heißt ***Teilmenge*** oder ***Untermenge*** von B genau dann, wenn jedes Element aus A in B enthalten ist.

(Teilmenge/Untermenge)	$A \subseteq B \quad :\iff \quad \forall x \,.\, x \in A \Longrightarrow x \in B$
(Obermenge)	$A \supseteq B \quad :\iff \quad \forall x \,.\, x \in A \Longleftarrow x \in B$
(Mengengleichheit)	$A = B \quad :\iff \quad \forall x \,.\, x \in A \iff x \in B$

Die Teilmengenbeziehung ist reflexiv, transitiv und antisymmetrisch.

(Reflexivität)	$A \subseteq A$
(Transitivität)	$A \subseteq B \wedge B \subseteq C \Longrightarrow A \subseteq C$
(Antisymmetrie)	$A \subseteq B \wedge B \subseteq A \Longrightarrow A = B$

Sei U eine beliebige Grundmenge, ein sogenanntes ***Universum***. Die Gesamtheit aller Teilmengen von U heißt ***Potenzmenge*** $\mathcal{P}(U)$ von U.

(Potenzmenge)	$\mathcal{P}(U) := \{ X \mid X \subseteq U \}$

Ist das Universum U endlich, dann gilt für die Anzahl der Teilmengen: $|\mathcal{P}(U)| = 2^{|U|}$. Für jedes Element des Universums können wir entscheiden, ob es in einer bestimmten Teilmenge enthalten ist oder nicht. Die Potenzmenge $\mathcal{P}(U)$ bildet mit den Mengenoperationen eine Boolesche Algebra: $(\mathcal{P}(U), \varnothing, U, \neg, \cap, \cup)$, wobei $\neg A := U - A$ das ***relative Komplement*** bezüglich U ist. Mit anderen Worten, die in Abbildung B.2 aufgeführten Gesetze gelten in gleicher Weise für die Mengenoperationen. Durchschnitt und Vereinigung lassen sich auf Mengen von Mengen $\mathcal{A} \subseteq \mathcal{P}(U)$ verallgemeinern:

(Durchschnitt) $\bigcap \mathcal{A} := \{ x \mid \forall A \in \mathcal{A} \,.\, x \in A \}$

(Vereinigung) $\bigcup \mathcal{A} := \{ x \mid \exists A \in \mathcal{A} \,.\, x \in A \}$

Das ***kartesische Produkt*** $A \times B$ von A und B ist die Menge aller Paare, deren erste Komponente aus A und deren zweite Komponente aus B stammt.

(Kartesisches Produkt) $A \times B := \{ (a, b) \mid a \in A \wedge b \in B \}$

Entsprechend wird das kartesisches Produkt von endlich vielen Mengen als Menge aller n-Tupel definiert. Sind die Grundmengen A und B endlich, dann gilt: $|A \times B| = |A| \cdot |B|$.

B.2.3. Relationen und Abbildungen\Funktionen

Eine binäre ***Relation*** R zwischen zwei Mengen A und B ist eine Teilmenge des kartesischen Produkts: $R \subseteq A \times B$. Relationen lassen sich vielfältig darstellen, siehe Abbildung B.3. Eine Relation $f \subseteq A \times B$ mit der Eigenschaft, dass es zu jedem $x \in A$ genau ein $y \in B$ mit $(x, y) \in f$ gibt, heißt ***Abbildung*** oder ***Funktion***. Dabei ist A der ***Definitionsbereich*** und B der ***Bild-*** oder ***Wertebereich*** der Funktion, notiert $f : A \to B$. Das eindeutige Element y heißt ***Funktionswert*** von x, notiert $y = f(x)$.

Eine Funktion ordnet jedem Element aus dem Definitionsbereich *genau* ein Element aus dem Wertebereich zu. Möchte man diese Eigenschaft mit Formeln der Prädikatenlogik einfangen, dann teilt man die Phrase »genau ein« oft in zwei Teilaspekte auf: »höchstens ein« und »mindestens ein«.

(rechtseindeutig) $\forall x \in A \,.\, \forall y_1, y_2 \in B \,.\, (x, y_1) \in R \;\wedge\; (x, y_2) \in R \implies y_1 = y_2$

(linkstotal) $\forall x \in A \,.\, \exists y \in B \,.\, (x, y) \in R$

Eine rechtseindeutige Relation wird auch als ***partielle Funktion*** bezeichnet.

Die obigen Eigenschaften lassen sich umkehren — die Namen deuten das bereits an — indem man gedanklich Definitions- und Wertebereich vertauscht ($A \leftrightarrow B$ und $x \leftrightarrow y$).

(linkseindeutig) $\forall y \in B \,.\, \forall x_1, x_2 \in A \,.\, (x_1, y) \in R \;\wedge\; (x_2, y) \in R \implies x_1 = x_2$

(rechtstotal) $\forall y \in B \,.\, \exists x \in A \,.\, (x, y) \in R$

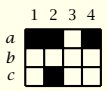
Eine linkseindeutige Funktion nennt man auch ***injektiv***, eine rechtstotale Funktion ***surjektiv***. Eine Funktion, die sowohl injektiv als auch surjektiv ist, heißt ***bijektiv*** (statt bijektiv sagt man auch »umkehrbar eindeutig« oder »eineindeutig«). Eine bijektive Abbildung $f : A \to B$ stellt eine Eins-zu-eins-Korrespondenz zwischen den Elementen des Definitionsbereichs A und den Elementen des Wertebereichs B her. Existiert eine Bijektion zwischen A und B, schreiben wir auch $A \cong B$.

Funktionen passenden Typs lassen sich ***komponieren***, $f \circ g : A \to C$, indem das Ergebnis der einen Funktion, $g : A \to B$, an die andere Funktion, $f : B \to C$, weitergereicht wird. Die ***Identitätsfunktion*** $id : A \to A$ ist das neutrale Element der Komposition.

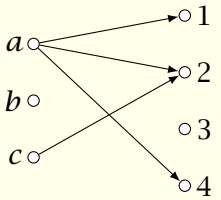
$id(x) = x$ $\qquad$ $(f \circ g)(x) = f(g(x))$

Relationen lassen sich vielfältig darstellen, als Tabellen, als 0-1-Matrizen oder durch Pfeildiagramme.

$$\{(a,1),(a,2),(a,4),(c,2)\}$$



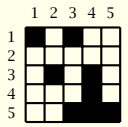
$$\begin{array}{c} \\ a \\ b \\ c \end{array}\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

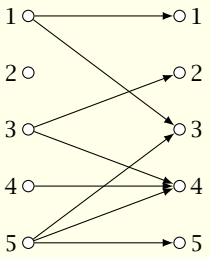


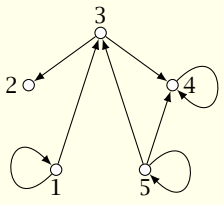
Die Tabellenform leitet sich direkt aus der Definition von Relationen ab: Ein Eintrag repräsentiert ein Paar; die Menge aller Paare entspricht der Relation. Dabei nutzt man implizit die Eins-zu-eins-Korrespondenz zwischen Potenzmengen und $\mathbb{B}$-wertigen Funktionen aus: $\mathcal{P}(A \times B) \cong A \times B \to \mathbb{B}$. Die Matrizendarstellung macht das explizit: Der Eintrag in Zeile x und Spalte y ist 1, wenn $(x,y) \in R$ gilt und 0 sonst. Die Tabellenform ist allerdings zu einem gewissen Grad willkürlich: Je nach Beschriftung der Zeilen und Spalten ergeben sich ganz unterschiedliche Tabellen.

Ansprechender lässt sich eine Relation $R \subseteq A \times B$ mit einem Pfeildiagramm darstellen. Die Elemente von A und B werden dabei als Punkte in der Ebene angeordnet; von x nach y wird genau dann ein Pfeil gezeichnet, wenn $(x,y) \in R$ gilt. In der Regel werden alle Elemente aus A und alle Elemente aus B untereinander oder nebeneinander angeordnet. Ist aus dem Kontext klar, welche Punkte welcher Menge zuzuordnen sind, erübrigt sich die Orientierung der Verbindungslinien.

Sind die Mengen A und B identisch, lässt sich die Darstellung übersichtlicher gestalten, indem nur eine Punktmenge gezeichnet wird. (Relationen dieses Typs werden manchmal etwas kryptisch ***Endorelationen*** genannt.)







Endorelationen korrespondieren zu *quadratischen* Tabellen und Matrizen.

Abbildung B.3.: Darstellung von Relationen und Endorelationen.

Ergibt die Funktionskomposition die identische Abbildung, $g \circ f = id$, so heißt f ***Linksinverse*** von g und umgekehrt g ***Rechtsinverse*** von f. Die Funktion f ist notwendigerweise injektiv und g notwendigerweise surjektiv. (Warum?)

$$
\begin{array}{rcll}
f : A \to B \text{ injektiv} & \iff & \exists\, g : B \to A \;.\; g \circ f = id & \text{falls } A = \emptyset \Longrightarrow B = \emptyset \\
f : A \to B \text{ surjektiv} & \iff & \exists\, g : B \to A \;.\; f \circ g = id & \\
f : A \to B \text{ bijektiv} & \iff & \exists\, g : B \to A \;.\; g \circ f = id \;\wedge\; f \circ g = id &
\end{array}
$$

Nur injektive Funktionen des Typs $\emptyset \to B$ mit $B \neq \emptyset$ haben keine Linksinverse, da es schlicht und einfach keine Funktionen des Typs $B \to \emptyset$ gibt.

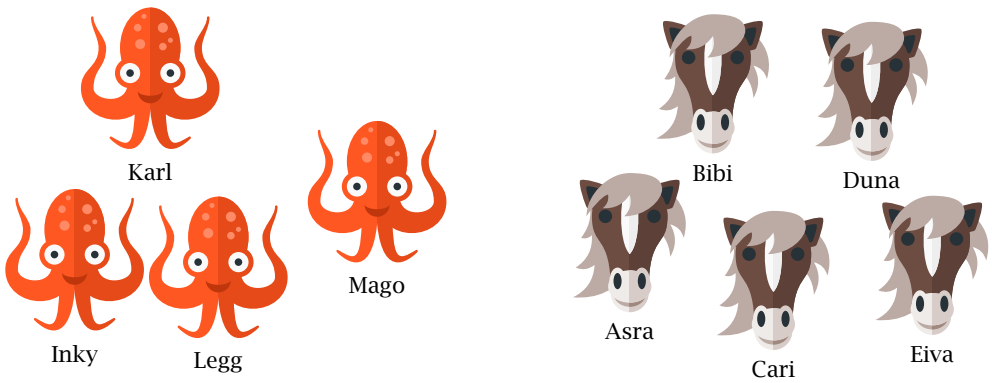
B.2.4. Mächtigkeit von Mengen

Fruchtbaren Begriffsbildungen und Schlußweisen wollen wir, wo immer nur die geringste Aussicht sich bietet, sorgfältig nachspüren und sie pflegen, stützen und gebrauchsfähig machen. Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können.

— David Hilbert (1862–1943), *Über das Unendliche*

In der Einleitung 1 haben wir angemerkt, dass es formal unentscheidbare Probleme gibt. Es genügt, sich auf Ja/Nein-Probleme zu konzentrieren, auf Funktionen des Typs $\mathbb{N} \to \mathbb{B}$. (Ist die Eingabe gerade? Ist sie eine Primzahl? Die Eingabe codiert eine aussagenlogische Formel; ist diese Formel allgemeingültig?) Ein Problem heißt formal entscheidbar, wenn es mit Hilfe eines Programms des Typs *Nat→Bool* mechanisch, durch stupides Rechnen gelöst werden kann. Die Existenz unentscheidbarer Probleme liegt salopp gesprochen an der auf den ersten Blick verwirrenden Tatsache, dass es mehr Probleme als Programme gibt: Die Menge der Programme ist weniger mächtig als die Menge der Ja/Nein-Probleme. Die Beschäftigung mit unendlichen Mengen ist faszinierend und führt uns zu einem der schönsten Beweise der Mathematik …

Endliche Mengen Nähern wir uns dem Konzept der Mächtigkeit schrittweise und wenden uns zunächst einem vertrauten Spezialfall zu, den endlichen Mengen. Auf der linken Seite sehen Sie eine Menge von Tintenfischen, auf der rechten Seite eine Menge von Pferden. Welche Menge ist mächtiger?



Wie sind Sie vorgegangen? Die Wahrscheinlichkeit ist groß, dass Sie die Elemente der beiden Mengen gezählt haben: Es gibt vier Tintenfische, aber fünf Pferde. Mit dem Zählen stellen wir eine Eins-zu-eins-Korrespondenz zwischen der betrachteten Menge und einem Anfangsabschnitt der natürlichen Zahlen her, zum Beispiel, $\{\text{Inky} \mapsto 1, \text{Karl} \mapsto 2, \text{Legg} \mapsto 3, \text{Mago} \mapsto 4\}$. Wir können den Umweg über die natürlichen Zahlen auch vermeiden und eine direkte Eins-zu-eins-Korrespondenz

etablieren, indem wir jedem Tintenfisch eineindeutig einen Partner unter den Pferden zuordnen. Leider klappt die Partnervermittlung nicht ganz, ein Pferd bleibt stets einsam zurück, zum Beispiel ist bei der Zuordnung $\{\text{Inky} \mapsto \text{Eiva}, \text{Karl} \mapsto \text{Cari}, \text{Legg} \mapsto \text{Bibi}, \text{Mago} \mapsto \text{Asra}\}$ Duna partnerlos. Die Menge der Tintenfische ist somit weniger mächtig als die Menge der Pferde.

Eine Menge A heißt ***gleichmächtig*** zu einer Menge B, notiert $|A| = |B|$, wenn eine Bijektion $A \to B$ existiert. Gibt es eine Bijektion $A \to B'$ auf eine Teilmenge $B' \subseteq B$, dann heißt A ***höchstens gleichmächtig*** zu B, notiert $|A| \leqslant |B|$. Gilt $|A| \leqslant |B|$, aber *nicht* $|A| = |B|$, dann heißt A ***weniger mächtig*** als B und wir schreiben $|A| < |B|$. (Auf diese Weise wird eine ***totale Ordnung*** auf Mengen definiert, siehe auch Abschnitt B.4.) Im obigen Beispiel gilt $|\{1, \dots, 4\}| = |\text{Tintenfische}| < |\text{Pferde}| = |\{1, \dots, 5\}|$.

Statt $|A| = |\{1, \dots, n\}|$ schreibt man auch kurz $|A| = n$. Mit dieser Vereinbarung lässt sich die ***Mächtigkeit*** bzw. die ***Kardinalität*** einer Menge für die verschiedenen, in den Abschnitten B.2.2 und B.2.3 eingeführten Mengenkonstruktionen ausrechnen.

$$|A \uplus B| = |A| + |B| \qquad |A \times B| = |A| \cdot |B| \qquad |A \to B| = |B|^{|A|} \qquad |\mathscr{P}(A)| = 2^{|A|}$$

Der Operator $\uplus$ bezeichnet dabei die ***disjunkte Vereinigung*** von Mengen: $A \uplus B := \{ (0, a) \mid a \in A \} \cup \{ (1, b) \mid b \in B \}$.[5] Ist die Vereinigung nicht disjunkt, müssen doppelt gezählte Elemente wieder abgezogen werden: $|A \cup B| = |A| - |A \cap B| + |B|$ — es kommt das ***Prinzip der Einschließung und Ausschließung*** zum Tragen, siehe Abbildung 4.3. Die beiden Komponenten eines Paares können unabhängig voneinander gewählt werden, deswegen multipliziert sich deren Anzahl. Gleiches gilt für Funktionen: Für jedes Argument können wir $|B|$ mögliche Funktionswerte wählen, dementsprechend gibt es insgesamt $|B|^{|A|}$ verschiedene Funktionen. Mit $|\mathbb{B}| = 2$ leitet sich daraus die Formel für Potenzmengen ab. (Potenzmengen $\mathscr{P}(A)$ stehen in Eins-zu-eins-Korrespondenz zu $\mathbb{B}$-wertigen Funktionen $A \to \mathbb{B}$.)

Abzählbar unendliche Mengen Wenden wir uns unendlichen Mengen zu und stellen uns die Frage, ob mehr natürliche als gerade Zahlen existieren? Der Bauch sagt »Ja klar!« — intuitiv gibt es ja nur halb so viele gerade Zahlen, da auf dem Zahlenstrahl jede zweite Position freibleibt:

0	1	2	3	4	5	6	7	8	9	⋯
0	—	2	—	4	—	6	—	8	—	⋯

Vielleicht sollten wir die Frage zunächst präzisieren: Ist die Menge der natürlichen Zahlen *mächtiger* als die Menge der geraden Zahlen? Die vielleicht überraschende Antwort ist »Nein, die Mengen sind gleichmächtig.« Zum Beweis stellen wir eine Eins-zu-eins-Korrespondenz zwischen den beiden Mengen her, zum Beispiel, wie folgt:

0	1	2	3	4	5	6	7	8	9	⋯
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	⋯
0	2	4	6	8	10	12	14	16	20	⋯

$$f(n) := n \cdot 2$$
$$g(n) := n/2$$

Die zueinander inversen Funktionen f und g bezeugen die Korrespondenz.

Auf ähnliche Weise können wir zum Beispiel auch zeigen, dass es (informell gesprochen) genauso viele Primzahlen wie natürliche Zahlen gibt: $|\mathbb{N}| = |\mathbb{P}|$.

0	1	2	3	4	5	6	7	8	9	⋯
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	⋯
2	3	5	7	11	13	17	19	23	29	⋯

[5] Variantentypen in Mini-F# entsprechen disjunkten Vereinigungen.

Die Zeugen der Eins-zu-eins-Korrespondenz, die zueinander inversen Funktionen, sind hier nicht mehr so leicht aufzuschreiben, aber das soll uns nicht stören. (Wenn Sie bereits etwas Programmiererfahrung mitbringen, können Sie versuchen, die Funktionen zu programmieren — das Konzept der ***Aufzähler*** aus Abschnitt 8.4 erweist sich als nützlich.)

Eine Menge M heißt ***endlich***, wenn eine natürliche Zahl $n \in \mathbb{N}$ existiert, so dass $|M| = n$. Gilt $|M| = |\mathbb{N}|$, so heißt die Menge ***abzählbar unendlich***. Die Kardinalität von $\mathbb{N}$ wird auch mit $\aleph_0$ (sprich »Aleph[6] Null«) bezeichnet, $|\mathbb{N}| = \aleph_0$, der kleinsten unendlichen ***Kardinalzahl***. Man kann zeigen, dass jede Teilmenge einer abzählbaren Menge entweder endlich oder selbst abzählbar unendlich ist.

Bislang haben wir Untermengen von $\mathbb{N}$ betrachtet; wie sieht es mit größeren Zahlenmengen aus, ist zum Beispiel die Menge der ganzen Zahlen mächtiger als die Menge der natürlichen Zahlen?

⋯	□	–	–	–	–	–	–	–	–	0	1	2	3	4	5	6	7	8	9	⋯
⋯	−9	−8	−7	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6	7	8	9	⋯

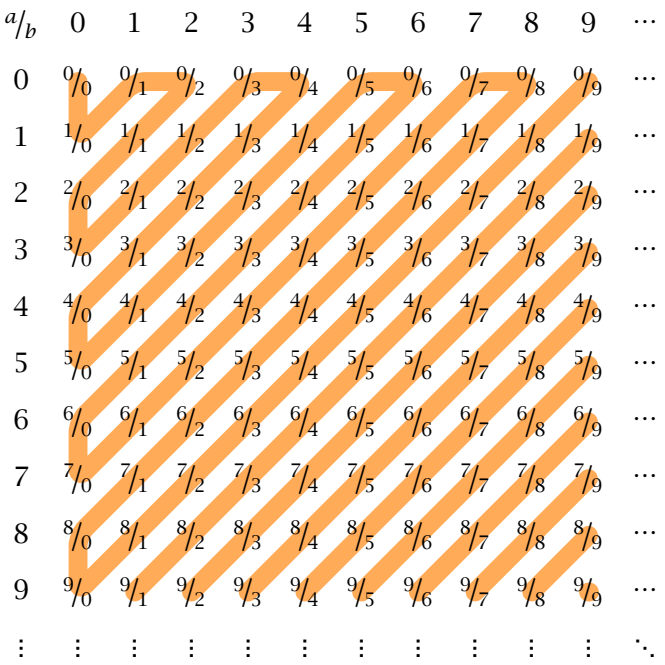
Die Situation ist vergleichbar mit unserem ersten Beispiel, $|\mathbb{N}| = |2 \cdot \mathbb{N}|$, und dort wie hier haben wir es mit gleichmächtigen Mengen zu tun: $|\mathbb{N}| = |\mathbb{Z}|$.

0	1	2	3	4	5	6	7	8	9	⋯
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	⋯
0	−1	1	−2	2	−3	3	−4	4	−5	⋯

Wir verbandeln die nichtnegativen Zahlen mit den geraden Zahlen und die negativen Zahlen mit den ungeraden.

Aber sicherlich gibt es mehr rationale Zahlen als natürliche Zahlen? Zwischen zwei rationale Zahlen können wir immer eine weitere quetschen, ihren Mittelwert: Wenn a kleiner ist als b, dann gilt $a < \frac{a+b}{2} < b$. Somit liegen zwischen zwei benachbarten natürlichen Zahlen unendlich viele rationale Zahlen. Allerdings: Die bis dato betrachteten Beispiele haben schon angedeutet, dass Veranschaulichungen mit Hilfe der Zahlengeraden nur bedingt hilfreich sind, wenn es um die Mächtigkeit von Zahlenmengen geht. Wenn wir $|\mathbb{N}| = |\mathbb{Q}|$ zeigen wollen, genügt es ja, irgendeine Bijektion zu finden; die Bijektion muss insbesondere nicht die Anordnung der Zahlen erhalten. Um die Abzählbarkeit der nichtnegativen, rationalen Zahlen nachzuweisen, ordnen wir sie in einer unendlichen Tabelle an, wobei jede Zeile die Brüche mit dem gleichen Zähler enthält und jede Spalte die mit dem gleichen Nenner.

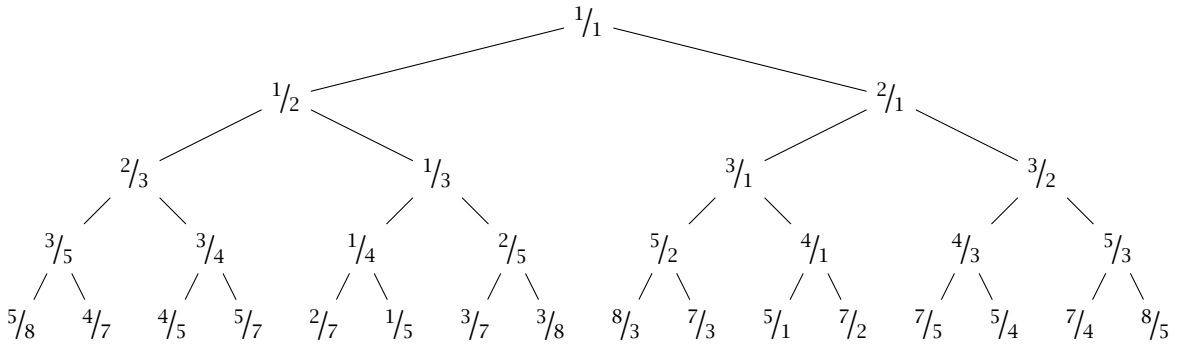
[6] Aleph (אלף) ist der erste Buchstabe im hebräischen Alphabet.



Wenn wir in der linken oberen Ecke starten und uns im Zick-Zack-Kurs entlang der Nebendiagonalen bewegen, können wir die rationalen Zahlen systematisch aufzählen.

Die Perfektionisten/Perfektionistinnen unter den Lesern/Leserinnen werden sich vielleicht an zwei Details stören: Die Einträge in der obersten Zeile stellen keine gültigen rationalen Zahlen dar und jede Zahl tritt mehrfach, sogar unendlich oft auf, zum Beispiel kürzen sich alle Einträge auf der Hauptdiagonalen mit Ausnahme von $^0/_0$ zu 1. Das erste Problem lässt sich einfach beheben, indem die erste Zeile weggelassen wird. Aber das zweite? Eigentlich zeigt der obige Beweis, dass Paare von natürlichen Zahlen abzählbar sind: $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Erstaunlicherweise lassen sich die positiven, rationalen Zahlen in *gekürzter Form* aufzählen, so dass jede Zahl genau einmal auftritt. Dazu ordnen wir die Brüche statt in einer unendlichen Tabelle in einem unendlichen Binärbaum an [Hin09]. Der folgende Ausschnitt zeigt die ersten fünf Ebenen des Baums.



Der Baum besitzt viele *wunder*volle Eigenschaften. Er ist ***selbstähnlich***: Inkrementieren wir alle Einträge und bilden anschließend den Kehrwert, $q \mapsto 1/(q+1)$, erhalten wir den linken Teilbaum; führen wir die beiden Operationen in umgekehrter Reihenfolge aus, $q \mapsto (1/q)+1$, erhalten wir den rechten Teilbaum. Zusammen mit der Festlegung, dass die Wurzel mit $^1/_1$ markiert ist, wird der Baum auf diese Weise eindeutig beschrieben. Mit Hilfe der beiden Transformationen lässt sich der Baum ebenenweise konstruieren, zum Beispiel leiten sich aus der dritten Ebene

$^2/_3, {}^1/_3, {}^3/_1, {}^3/_2$

die beiden Hälften der vierten Ebene ab $(1/(^2/_3 + 1) = {}^3/_5$ und $(1/^2/_3) + 1 = {}^5/_2$ usw.):

$$^3/_5, {}^3/_4, {}^1/_4, {}^2/_5 \qquad \text{und} \qquad {}^5/_2, {}^4/_1, {}^4/_3, {}^5/_3$$

Die rechte Hälfte ergibt sich aus der gespiegelten linken Hälfte, indem man jeweils den Kehrwert bildet. In dem unendlichen Baum befinden sich die positiven, natürlichen Zahlen auf einem zackigen rechts-links Pfad. Geht man ausgehend von der Wurzel ${}^1/_1$ stets nach rechts, begegnet man Brüchen, deren Zähler und Nenner aufeinanderfolgende Fibonacci-Zahlen sind: ${}^{F_{n+1}}/_{F_n}$. Die Folge dieser Brüche konvergiert somit gegen den ***goldenen Schnitt*** $\varphi = (1 + \sqrt{5})/2$. Soviel zu den wundervollen Eigenschaften der Konstruktion. (Um zu erklären, warum alle Brüche auftreten und das nur in gekürzter Form, müssten wir zu weit ausholen, siehe aber *loc. cit.*)

Wenn wir von Zahlen und Zahlenmengen abstrahieren, können wir als kurzes Zwischenfazit festhalten, dass die disjunkte Vereinigung und das kartesische Produkt von abzählbar unendlichen Mengen wieder eine abzählbar unendliche Menge hervorbringt.

$$|A| = \aleph_0 \;\wedge\; |B| = \aleph_0 \implies |A \uplus B| = \aleph_0$$
$$|A| = \aleph_0 \;\wedge\; |B| = \aleph_0 \implies |A \times B| = \aleph_0$$

Insbesondere können wir zu einer abzählbar unendlichen Menge abzählbar unendlich viele Elemente hinzufügen, ohne die Mächtigkeit zu verändern.

Nicht abzählbar unendliche Mengen Nachdem es uns bisher nicht gelungen ist, mächtigere Mengen als $\mathbb{N}$ zu konstruieren, liegt die Vermutung nahe, dass vielleicht gar keine existieren. Das ist aber nicht der Fall und damit kommen wir zu einem der wunderbarsten Beweise der Mathematik, ***Cantors Diagonalargument***. Der deutsche Mathematiker Georg Cantor (1845–1918) zeigte mit dieser Beweistechnik, dass es unterschiedliche Stufen der Unendlichkeit gibt, derer sogar unendlich viele! Das zu akzeptieren fällt noch heute vielen schwer, seine mathematischen Zeitgenossen aber schockte er regelrecht und, wie immer, wenn Weltbilder umgeworfen werden, reichten die Reaktionen von totaler Ablehnung bis zur Euphorie.

Der Quantensprung von einer Stufe der Unendlichkeit zur nächsten findet statt, wenn wir von einer unendlichen Menge M zu ihrer Potenzmenge $\mathcal{P}(M)$ übergehen: $|M| < |\mathcal{P}(M)|$. Insbesondere ist somit $\mathcal{P}(\mathbb{N})$ ***überabzählbar***. Den Beweis führen wir durch Widerspruch und nehmen dazu an, dass wir einen Weg gefunden haben, alle Teilmengen der natürlichen Zahlen aufzuzählen, X_0, X_1, X_2, … oder anschaulicher als Tabelle:

	0	1	2	3	4	5	6	7	8	9	⋯
X_0	yes	no	yes	no	yes	no	no	no	no	no	⋯
X_1	yes	no	no	no	yes	no	yes	no	yes	no	⋯
X_2	no	no	yes	yes	no	no	yes	yes	yes	yes	⋯
X_3	yes	no	yes	no	no	yes	yes	no	yes	no	⋯
X_4	yes	no	no	yes	yes	yes	yes	no	yes	yes	⋯
X_5	yes	no	yes	no	yes	yes	yes	no	no	no	⋯
X_6	no	yes	yes	no	no	yes	yes	yes	yes	yes	⋯
X_7	yes	yes	no	yes	no	no	yes	no	yes	yes	⋯
X_8	yes	yes	no	yes	yes	no	yes	yes	yes	no	⋯
X_9	yes	no	yes	no	yes	yes	yes	no	yes	no	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱
X	no	yes	no	yes	no	no	no	yes	no	yes	⋯

Jede Zeile repräsentiert eine Teilmenge, die erste oder besser nullte Zeile repräsentiert die Menge X_0, die die Elemente 0, 2 und 4 enthält, aber nicht 1, 3, 5, 6, 7, 8 und 9. Eine beeindruckende

Liste, aber leider unvollständig. Betrachten wir die rot eingefärbten Einträge auf der Hauptdiagonalen; aus ihnen bilden wir eine neue Zeile, die braun dargestellte Menge X, indem wir jeden Eintrag negieren: Aus »yes« wird »no« und umgekehrt. Wir behaupten, dass die Menge X in der Auflistung fehlt. Warum? Nun, X kann nicht X_0 sein, da 0 in X_0 enthalten ist, aber nicht in X. Auch X_1 kommt nicht in Frage, da $1 \notin X_1$, aber $1 \in X$. Da X das Komplement der Diagonale ist, gilt allgemein $i \notin X_i \iff i \in X$. Da somit die Menge X in der Aufzählung fehlt, haben wir die Annahme, dass sich alle Teilmengen aufzählen lassen, zum Widerspruch geführt.

Der Beweis zeigt für den Spezialfall $M = \mathbb{N}$, dass eine Funktion $f : M \to \mathcal{P}(M)$ *nicht* surjektiv und damit auch *nicht* bijektiv sein kann. Da sich aber M in $\mathcal{P}(M)$ einbetten lässt, $x \mapsto \{x\}$, und damit M höchstens so mächtig ist wie $\mathcal{P}(M)$, folgt insgesamt die Aussage $|M| < |\mathcal{P}(M)|$. Die i-te Zeile in der obigen Tabelle entspricht dabei dem Funktionswert $f(i)$. Die fehlende Menge X wird als Komplement der Diagonalen definiert.

$$X := \{\, x \in M \mid x \notin f(x) \,\} \tag{B.8}$$

Wäre f surjektiv, müsste es ein Element $i \in M$ geben mit $f(i) = X$. Aus der Frage, ob i selbst in $f(i)$ enthalten ist, leitet sich ein Widerspruch ab:

$$\begin{aligned}
& i \in f(i) \\
\iff & \quad \{\text{ Annahme: } f(i) = X \,\} \\
& i \in X \\
\iff & \quad \{\text{ Definition von X (B.8) } \} \\
& i \notin f(i)
\end{aligned}$$

Cantors Ergebnisse sendeten wie gesagt Schockwellen durch die Welt der Mathematik. Das Kapitel war damit aber noch nicht abgeschlossen: Wir wissen zwar, dass $\mathcal{P}(\mathbb{N})$ mächtiger ist als $\mathbb{N}$, aber nicht, ob $|\mathcal{P}(\mathbb{N})|$ auch die nächstgrößere Kardinalzahl ist, auf $\aleph_0$ folgt $\aleph_1$ — vielleicht gibt es ja eine Menge W mit $|\mathbb{N}| < |W| < |\mathcal{P}(\mathbb{N})|$? Auch die Antwort auf diese Frage war nicht ganz nach dem Geschmack der Mathematiker: Aus den Axiomen der Mengenlehre lässt sich die sogenannte ***Kontinuumshypothese*** — zwischen $|\mathbb{N}|$ und $|\mathcal{P}(\mathbb{N})|$ liegt *keine* weitere Kardinalzahl — *weder* beweisen *noch* widerlegen.

Kommen wir zum Ausgangspunkt unserer Überlegungen zurück, der Behauptung, dass es mehr Probleme als Programme gibt. Da wir Ja/Nein-Probleme mit Teilmengen von $\mathbb{N}$ identifizieren, zeigt Cantors Diagonalargument, dass es überabzählbar viele Ja/Nein-Probleme gibt. Dieser unvorstellbaren Vielfalt an Problemen stehen aber nur abzählbar unendlich viele Programme gegenüber. Ein Computerprogramm, in welcher Sprache auch immer geschrieben, ist ein endlicher Text, eine endliche Folge von Zeichen eines Alphabets. Wörter über einem endlichen Alphabet $\mathbb{A}$ lassen sich einfach aufzählen: erst alle Wörter der Länge 0, dann die Wörter der Länge 1 usw. Hier am Beispiel von $\mathbb{A} = \{0, 1\}$:

$$\varepsilon, \quad 0, 1, \quad 00, 01, 10, 11, \quad 000, 001, 010, 011, 100, 101, 110, 111, \quad \ldots$$

Selbst wenn wir ein abzählbar unendliches Alphabet verwenden, ändert sich an der Abzählbarkeit nichts (siehe Aufgabe B.2.6).

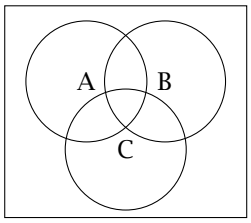
$$|\mathbb{A}| = \aleph_0 \quad \Longrightarrow \quad |\mathbb{A}^*| = \aleph_0 \tag{B.9}$$

Nun sind nicht alle Elemente von $\mathbb{A}^*$ legale Programme, aber, da jede unendliche Teilmenge einer abzählbaren Menge ebenfalls abzählbar ist, folgt: Die Menge aller Mini–F# Programme ist abzählbar unendlich.

Wir bekommen die Grenzen des Rechnens aufgezeigt: Nicht alle Probleme lassen sich mit Hilfe von Rechenvorschriften mechanisch lösen. Das wohl bekannteste formal unentscheidbare Problem ist das ***Halteproblem***: Terminiert ein Programm für eine bestimmte, gegebene Eingabe? Ebensowenig kann man formal entscheiden, ob zwei Programme das gleiche Ein- und Ausgabeverhalten an den Tag legen, etwa die Musterlösung einer Programmieraufgabe und die tatsächliche oder vermeintliche studentische Lösung. Schade, oder vielleicht auch nicht: Tutoren/Tutorinnen lassen sich nicht so leicht ersetzen — Unentscheidbarkeit als Arbeitsplatzgarantie. Mehr zu diesem Thema erfahren Sie in späteren Semestern aus der Abteilung der theoretischen Informatik.

Übungen.

1. Mit Hilfe von drei Kreisen lässt sich die Ebene in acht Teilflächen aufteilen.

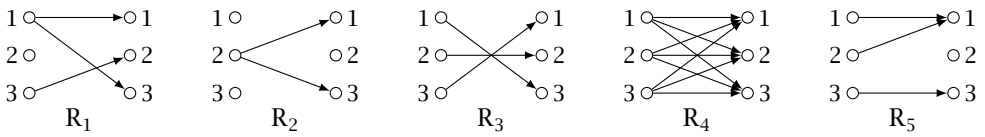


Geben Sie für jede der acht Flächen einen Mengenausdruck an.

2. Die Venn-Diagramme für Vereinigung, Durchschnitt und Differenz legen die folgende Beziehung zwischen den drei Mengenoperationen nahe. Beweisen Sie die Eigenschaft.

$$A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$$

3. Welche der folgenden Relationen sind rechtseindeutig? Welche linkstotal? Welche linkseindeutig? Welche rechtstotal?



Zum Knobeln: Es gibt insgesamt $2^{3 \cdot 3} = 512$ verschiedene Relationen in $\{a, b, c\}$. Jede Relation kann unterschiedliche Eigenschaften besitzen: rechtseindeutig, linkstotal, linkseindeutig, rechtstotal. Insgesamt lassen sich somit $2^4 = 16$ verschiedene Typen unterscheiden. Wieviele Relationen in $\{a, b, c\}$ gibt es jeweils von jedem Typ?

4. »Im *Grand Hotel Hilbert* ist immer ein Zimmer für sie frei — wir verfügen über unendlich viele Betten.« Hacker eilt an dem Plakat vorbei auf die Rezeption zu. »Ich hätte gerne ein Zimmer für eine Nacht.« Hacker schaut die junge Rezeptionistin erwartungsvoll an, »Lista« steht in dezenten Lettern auf ihrem Revers. »Oh, das tut mir leid. Wir sind leider ausgebucht.« Damit hatte er nicht gerechnet: »Wie kann das denn sein — Sie werben doch mit unendlich vielen Zimmern.« »Der Mathematikkongress — wir haben zur Zeit unendlich viele Gäste,« erklärt die Rezeptionistin. Hacker wendet sich bereits zum Gehen, als sie mit einem Lächeln hinzufügt: »Aber ich kann ein Zimmer für Sie freimachen!« Sie beugt sich über ein Mikrophon: »Sehr verehrte Gäste, darf Sie kurz um Ihre geschätzte Aufmerksamkeit bitten. Ich muss Sie leider bitten, das Zimmer zu wechseln. Bitte treten Sie in 15 Minuten auf den Flur und beziehen das Zimmer mit der nächsthöheren Nummer, sie finden es linker Hand.« Zu Hacker gewandt setzt sie erklärend hinzu: »Jedes Zimmer verfügt über eine Lautsprecheranlage. So kann ich die Gäste ansprechen. Sie haben es mitbekommen: In circa einer Viertelstunde können sie Zimmer 0 beziehen!«

- Ein Bus des Unternehmens *Infinity-Travel* fährt auf dem Parkplatz des Hotels vor, ein sehr spezieller Bus, der unendlich viele Passagiere befördert. Wie können die Gäste untergebracht werden, wenn bereits alle Zimmer belegt sind?
- Es fahren unendlich viele Busse mit jeweils unendlich vielen Gästen vor. Gibt es eine Möglichkeit, alle diese Gäste unterzubringen?

5. Zeigen Sie $|\mathbb{N}| = |\mathbb{Z}|$, indem Sie bijektive Funktionen $f : \mathbb{N} \to \mathbb{Z}$ und $g : \mathbb{Z} \to \mathbb{N}$ mit $g \circ f = id$ und $f \circ g = id$ konstruieren.

6. Zeigen Sie, dass die Menge aller Wörter $\mathbb{A}^*$ abzählbar unendlich ist, sofern das Alphabet $\mathbb{A}$ höchstens abzählbar unendlich ist (B.9).

7. Zeigen Sie, dass die Menge der reellen Zahlen $\mathbb{R}$ überabzählbar ist. *Hinweis:* Beschränken Sie sich auf das Einheitsintervall $[0,1] := \{x \mid 0 \leqslant x \leqslant 1\}$ und betrachten Sie die Darstellung dieser Zahlen als unendliche Binärbrüche, zum Beispiel $1/4 = 0.01\overline{0}$ und $1/3 = 0.\overline{01}$.

B.3. Induktion

B.3.1. Natürliche Induktion

Auf Giuseppe Peano (1858–1932) geht das folgende Axiomensystem zur Einführung der natürlichen Zahlen zurück, siehe auch Abbildungen 3.6 und B.10.

- 0 ist eine natürliche Zahl.

  $$0 \in \mathbb{N}$$

- Für alle n gilt, dass, wenn n eine natürliche Zahl ist, auch die auf n folgende Zahl eine natürliche Zahl ist.

  $$\forall\, n \in \mathbb{N} \;.\; n+1 \in \mathbb{N}$$

- Wenn auf zwei Zahlen dieselbe Zahl folgt, sind sie identisch.

  $$\forall\, m \in \mathbb{N} \;.\; \forall\, n \in \mathbb{N} \;.\; m+1 = n+1 \Longrightarrow m = n$$

- 0 kann nicht auf eine natürliche Zahl folgen.

  $$\neg(\exists\, n \in \mathbb{N} \;.\; 0 = n+1) \quad \text{oder} \quad \forall\, n \in \mathbb{N} \;.\; 0 \neq n+1$$

- Das *Induktionsaxiom:* Wenn 0 eine Eigenschaft hat und wenn jede auf eine natürliche Zahl folgende Zahl die Eigenschaft besitzt, sofern die Zahl selbst die Eigenschaft hat, dann haben alle natürlichen Zahlen die betreffende Eigenschaft.

  $$\mathrm{P}(0) \;\wedge\; (\forall\, n \in \mathbb{N} \;.\; \mathrm{P}(n) \Rightarrow \mathrm{P}(n+1)) \quad\Longrightarrow\quad \forall\, n \in \mathbb{N} \;.\; \mathrm{P}(n)$$

Das letzte Axiom ist die Grundlage der Beweismethode durch ***natürliche Induktion*** (auch: ***vollständige*** oder ***mathematische*** Induktion). Die Beweismethode hat somit ihre Wurzeln in den Eigenschaften der natürlichen Zahlen und ist nicht etwa formallogisch begründet, gottgegeben oder gar ein Naturgesetz. (Das Attribut »vollständig« oder »mathematisch« grenzt das Schlussverfahren von der *philosophischen* Induktion ab, die aus Spezialfällen eine allgemeine Gesetzmäßigkeit folgert und kein logisch korrektes Schlussverfahren darstellt.)

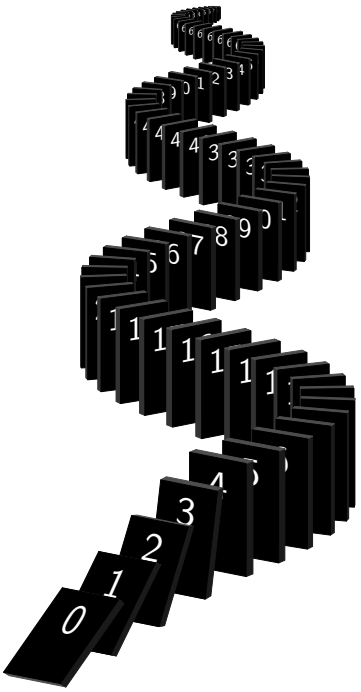
Die Beweismethode lässt sich etwas übersichtlicher mit Hilfe einer Deduktionsregel aufschreiben.

$$\frac{\mathrm{P}(0) \qquad \forall\, n \in \mathbb{N} \;.\; \mathrm{P}(n) \Longrightarrow \mathrm{P}(n+1)}{\forall\, n \in \mathbb{N} \;.\; \mathrm{P}(n)}$$

Um eine Aussage zu zeigen, die für alle natürlichen Zahlen gilt — die Schlussfolgerung unter dem Strich — müssen zwei Beweise geführt werden — die Voraussetzungen über dem Strich:

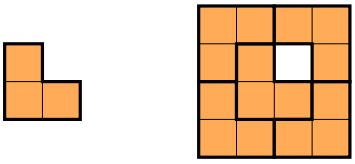
- ***Induktionsbasis*** oder ***-verankerung***: Man muss zeigen, dass die Aussage für 0 gilt.

- ***Induktionsschritt***: Für alle natürlichen Zahlen n muss man unter der Annahme, dass die Aussage für n gilt, zeigen, dass sie für $n+1$ gilt. Die Annahme nennt man ***Induktionsannahme*** oder ***-hypothese***.



Die Beweismethode der natürlichen Induktion wird auch manchmal als ***Dominoprinzip*** bezeichnet. Um eine lange Reihe hochkant aufgestellter Dominosteine umzuwerfen, muss man den ersten Stein antippen (Induktionsbasis) und man muss sicherstellen, dass der n-te Stein beim Fallen den $(n+1)$-ten Stein trifft und diesen zum Umfallen bringt (Induktionsschritt). Um die Domino-Kettenreaktion zu garantieren, muss letzteres für alle natürlichen Zahlen n gewährleistet sein.

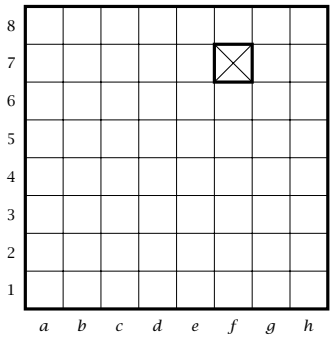
In der Schule und in den meisten mathematischen Lehrbüchern wird das Induktionsprinzip mit Beispielen aus der Arithmetik illustriert und eingeübt. Wir wollen uns an dieser Stelle ein geometrisches Problem vornehmen und dieses induktiv lösen. Es gilt ein Schachbrett mit sogenannten ***L-Trominos*** zu kacheln. Ähnlich wie ein Dominostein aus zwei gleichgroßen Quadraten zusammengesetzt wird, besteht ein Tromino aus drei Quadraten. Da die Steine beim Kacheln beliebig gedreht werden dürfen, gibt es lediglich zwei unterschiedliche Trominos: das I-Tromino und das L-Tromino  . Ziel ist es, ein $2^n \times 2^n$ großes Schachbrett möglichst vollständig zu kacheln, ohne dass sich Steine überlappen oder aus dem Brett herausragen.



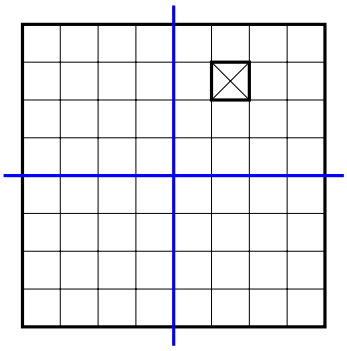
Da $2^n \times 2^n = 4^n$ kein Vielfaches von 3 ist, lässt sich das Brett nicht vollständig kacheln. Aber wir können alle Felder mit einer einzigen, *beliebigen* Ausnahme bedecken. Wenn man möchte, kann man das Problem als Spiel auffassen: Der Opponent wählt eine Brettgröße aus und markiert ein beliebiges Feld, das freibleiben soll. Wir müssen dann das restliche Spielfeld mit L-Trominos kacheln. Wir führen den Beweis, dass dies immer gelingt, durch natürliche Induktion über n.

Induktionsbasis: Ein $2^0 \times 2^0$ Schachbrett besteht nur aus einem einzigen Feld. Der Opponent hat keine andere Möglichkeit, als dieses Feld auszuwählen. Das restliche Feld ist leer und damit auch vollständig gekachelt.

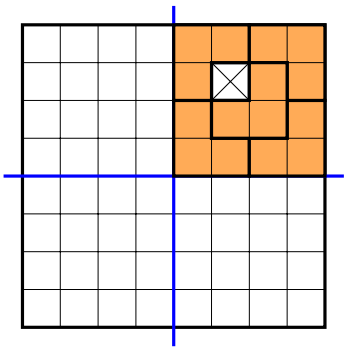
Induktionsschritt: Wir müssen ein $2^{n+1} \times 2^{n+1}$ Schachbrett kacheln und dürfen annehmen, dass wir Schachbretter der Größe $2^n \times 2^n$ bereits kacheln können (*Induktionsannahme*). Schauen wir uns ein konkretes Beispiel an, um eine Idee für den Lösungsansatz zu bekommen (n ist 3 und das ausgewählte Feld ist f7).



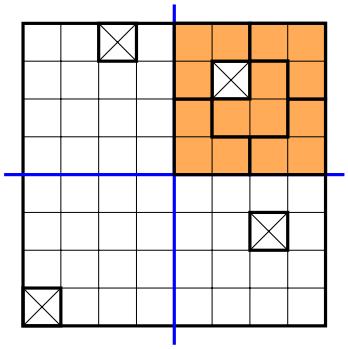
Wir müssen versuchen, die Induktionsannahme anzuwenden. Eine vielleicht naheliegende Idee ist, das Feld in vier Quadranten der Größe $2^n \times 2^n$ aufzuteilen. (Das ist *nicht* die einzige Möglichkeit — später mehr dazu.)



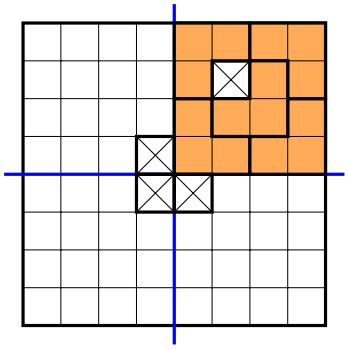
Damit lässt sich die Induktionsannahme auf den rechten, oberen Quadranten anwenden. (Da es in dem Beweis nur um die Existenz einer Kachelung geht, interessiert uns eigentlich nicht, wie diese konkret aussieht.)



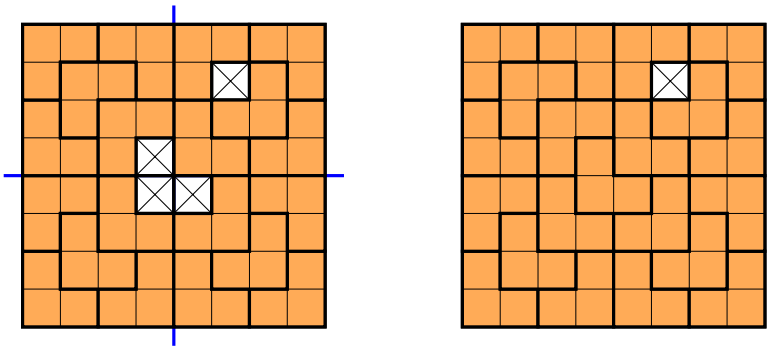
Auf die übrigen drei Quadranten ist die Induktionsannahme leider *nicht* anwendbar, da keine Felder markiert sind. Was ist zu tun? Es gibt mindestens zwei Auswege aus dem Dilemma. Wir haben im Prinzip ein neues Problem identifiziert, die Kachelung eines großen L-Trominos, das wir ebenfalls induktiv lösen könnten. Versuchen Sie es! (Abschnitt B.3.2 widmet sich dieser reizvollen Aufgabe.) Alternativ können wir einfach in jedem der Quadranten ein Feld markieren.



Jetzt lässt sich die Induktionsannahme auf die drei Quadranten anwenden. Leider ist nichts gewonnen, da wir insgesamt eine Kachelung mit vier freien Feldern erhalten. Gewonnen haben wir aber vielleicht die Einsicht, dass wir die freien Felder so wählen müssen, dass wir sie mit einem L-Tromino bedecken können. Da bleibt uns nur eine Wahl.



Jetzt lässt sich die Induktionsannahme auf alle vier Quadranten anwenden *und* wir können die drei Felder in der Mitte mit einem L-Tromino bedecken.



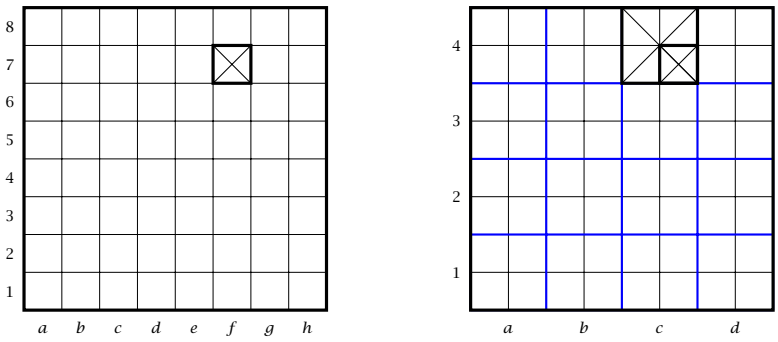
Da die Vorgehensweise unabhängig von der Größe des Schachbretts und der Position des freien Feldes ist, haben wir das Problem gelöst.

Was lassen sich für Erkenntnisse aus dem Beweis ziehen? Was haben wir gelernt? Fasst man Beweisen als eine zielgerichtete Tätigkeit auf, so gibt es im Induktionsschritt zwei klar identifizierbare Teilziele bzw. Teilprobleme (»divide et impera«):

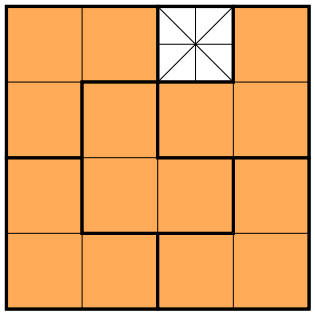
- Die Anwendbarkeit der Induktionsannahme ist nicht immer offensichtlich. Wir müssen *kreativ* sein und uns überlegen, wie wir das Problem für $n + 1$ auf ein oder mehrere Teilprobleme für n reduzieren können (»teile«).
- Wenn wir die Teillösungen für die Teilprobleme durch Anwendung der Induktionsannahme in der Hand halten, müssen wir überlegen, wie sich diese zu einer Gesamtlösung für das ursprüngliche Problem zusammenführen lassen (»herrsche«). Auch das ist Teil der *kreativen* Leistung beim induktiven Beweisen.

Um die beiden Punkte noch einmal zu betonen, lassen Sie uns das Kachelungsproblem bzw. den Induktionsschritt ein zweites Mal lösen.

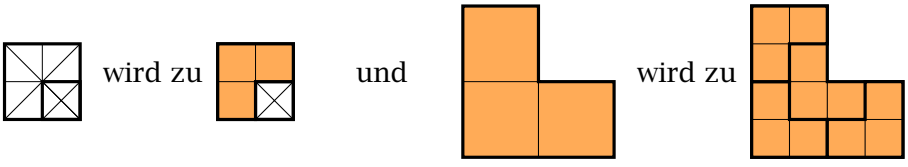
Wir können ein $2^{n+1} \times 2^{n+1}$ Schachbrett alternativ auf *ein* $2^n \times 2^n$ Schachbrett zurückführen, indem wir die Felder vergrößern.



Jedes Feld besteht jetzt aus 2×2 Feldern des ursprünglichen Schachbretts; aus dem markierten Feld f7 wird das 2×2 Feld c4. Haben wir vorher die Induktionsannahme viermal angewendet, so müssen wir das jetzt nur noch einmal tun.



Allerdings erhalten wir eine Teillösung mit großen L-Trominos und einem großen freien Feld. Um die Teillösung in eine Lösung für das ursprüngliche Problem zu überführen, müssen wir uns überlegen, wie wir das große »Loch« in das ursprüngliche kleine »Loch« verwandeln und wie sich ein großes L-Tromino mit kleinen L-Trominos kacheln lässt. (Eine geometrische Figur, die mit kleinen Kopien ihrer selbst gekachelt werden kann, nennt man im Englischen übrigens ***rep-tile***, siehe auch Abschnitt B.3.2.)



Führt man die entsprechenden Ersetzungen durch, erhält man überraschenderweise die gleiche Lösung wie beim ersten Ansatz. Beide Beweise sind ***konstruktiv***: Der induktive Beweis lässt sich jeweils in ein rekursives Programm überführen, das eine konkrete Kachelung berechnet. (Wenn Sie bereits über etwas Programmiererfahrung verfügen, ist das vielleicht eine reizvolle Aufgabe.)

Das Kachelungsproblem zeigt geometrisch, dass 4^n ***mod*** $3 = 1$ — wenn wir ein Schachbrett der Größe $2^n \times 2^n$ mit Steinen der Größe 3 kacheln, bleibt notwendigerweise ein Feld frei. (Die Operation ***mod*** berechnet den Rest der ganzzahligen Division, siehe auch Abschnitt B.5.1.) Lassen wir den Abschnitt mit einem induktiven Beweis von $4^n \equiv 1$ ausklingen, wobei $a \equiv b$ bedeutet, dass die Differenz $a - b$ durch 3 teilbar ist: $a \equiv b :\Longleftrightarrow a$ ***mod*** $3 = b$ ***mod*** 3.

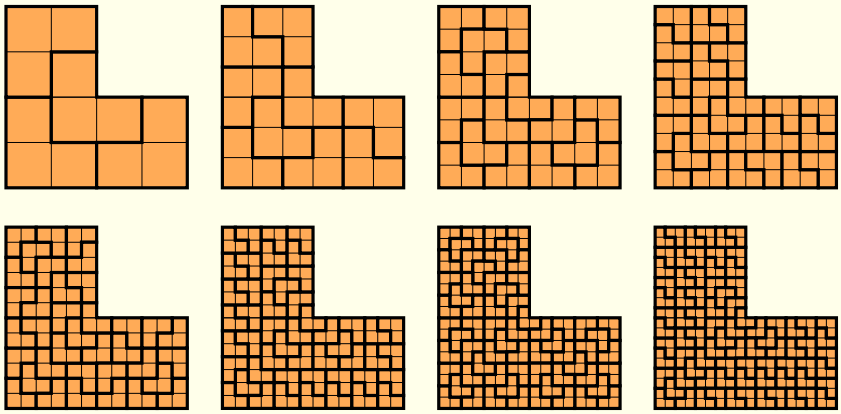


Abbildung B.4.: Selbstgekachelte L-Trominos der Größen 2 bis 9.

Induktionsbasis:

$$
\begin{aligned}
& 4^0 \\
\equiv \quad & \{ \text{ Potenzgesetze } \} \\
& 1
\end{aligned}
$$

Induktionsschritt:

$$
\begin{aligned}
& 4^{n+1} \\
\equiv \quad & \{ \text{ Potenzgesetze } \} \\
& 4 \cdot 4^n \\
\equiv \quad & \{ 4 \equiv 1 \text{ und Induktionsannahme } 4^n \equiv 1 \} \\
& 1 \cdot 1 \\
\equiv \quad & \{ \text{ Arithmetik } \} \\
& 1
\end{aligned}
$$

Im zweiten Schritt verwenden wir ein Gesetz der modularen Arithmetik (siehe auch Abschnitt B.5.5): Aus $a \equiv a'$ und $b \equiv b'$ folgt die Äquivalenz $a \cdot b \equiv a' \cdot b'$. Übrigens: Wie das obige Beispiel illustriert, lässt sich das Beweisformat für beliebige *transitive* Relationen verwenden. Als Äquivalenzrelation ist »≡« insbesondere transitiv.

B.3.2. Noethersche Induktion

Das L-Tromino ist ein sogenanntes ***rep-tile***[7]: Jede n-fache Vergrößerung der Figur lässt sich mit n^2 Kopien des Originalsteins vollständig kacheln. Abbildung B.4 illustriert die Selbstkachelung für verschiedene Vergrößerungsfaktoren. Wir haben im letzten Abschnitt bereits gezeigt, dass Selbstkachelungen für Zweierpotenzen möglich sind:

[7] Der Name ist ein Wortspiel: self-*rep*licating *tile*.

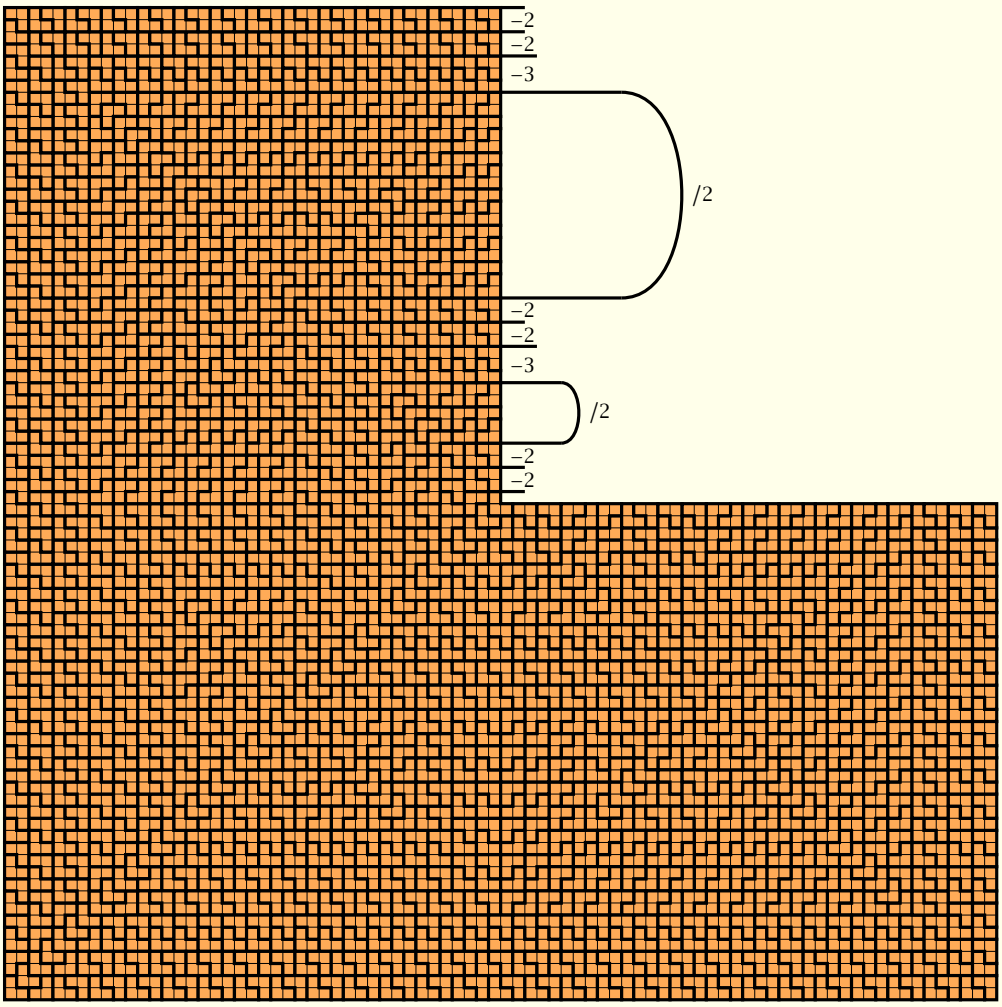
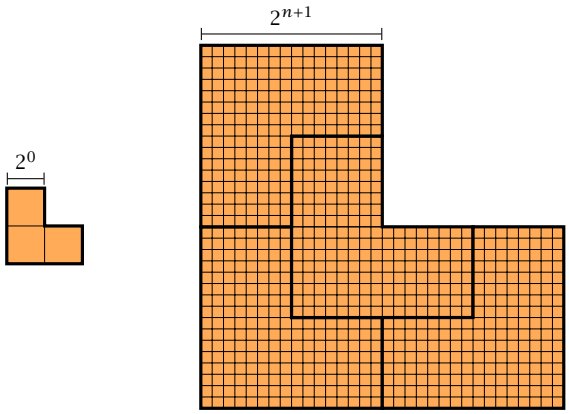
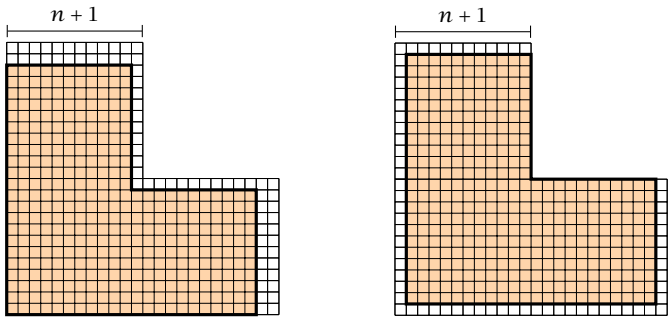


Abbildung B.5.: Selbstgekacheltes L-Tromino der Größe 41.

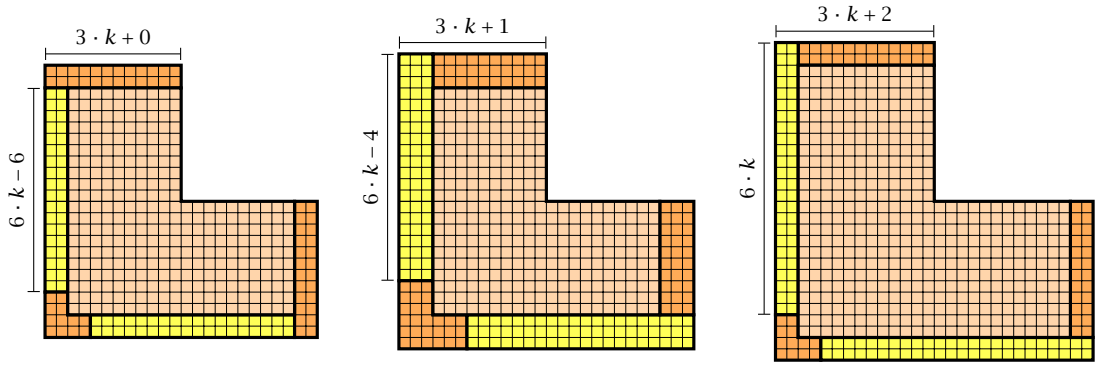


Aber wie gehen wir vor, wenn der Vergrößerungsfaktor keine exakte Zweierpotenz ist? Das Prinzip der natürlichen Induktion scheint an seine Grenzen zu stoßen. Im Induktionsschritt können wir zwar annehmen, dass es uns gelingt, ein n-fach vergrößertes L-Tromino zu kacheln:



Aber das nützt uns wenig, da sich die Teillösung nicht zu einer Gesamtlösung erweitern lässt — wo immer wir den n-fach vergrößerten L-Tromino auch platzieren, der verbleibende Streifen ist zu schmal, als dass er sich mit L-Trominos kacheln ließe. Allerdings lassen sich zwei L-Trominos zu einem 2×3 Rechteck zusammenfügen, so dass wir 2-er und 3-er Streifen bilden können.

Versuchen wir es mit einer 2-er Umrandung. Leider ergibt sich unmittelbar eine Einschränkung: Da die Länge des Streifens ein Vielfaches von 3 ist, muss der Vergrößerungsfaktor durch 3 teilbar sein … nicht ganz, je nachdem, wie der Streifen um die Ecken geführt wird, sind Längen der Form $3 \cdot k + 0$ und $3 \cdot k + 2$ machbar.



In der linken unteren Ecke platzieren wir jeweils einen 2-fach vergrößerten L-Tromino, so dass sich die Längen der Teilstreifen (in gelb und orange) jeweils durch 3 teilen lassen. Dabei nehmen

wir frech an, dass sich die restliche Fläche induktiv kacheln lässt. Der verbleibende Fall $3 \cdot k + 1$ gibt uns eine härtere Nuss zu knacken. Da sich ein 2-er Streifen nicht anbringen lässt, versuchen wir es mit einer 3-er Umrandung. Nun ist die Länge eines 3-er Streifens ein Vielfaches von 2, so dass $3 \cdot k - 2$ bzw. $6 \cdot k - 4$ durch 2 teilbar sein muss. Aber das ist nur der Fall, wenn k gerade ist. Was machen wir, wenn k ungerade ist? In diesem Fall ist die Gesamtlänge $3 \cdot k + 1$ gerade, so dass wir wie im Fall exakter Zweierpotenzen vorgehen können: Wir kacheln die Fläche mit vier Kopien halb so großer L-Trominos. (So können wir natürlich für alle geraden Vergrößerungsfaktoren vorgehen, insbesondere für $n = 2$.)

Lassen wir den Beweis noch einmal Revue passieren. Je nach Teilerrest unterscheiden wir vier verschiedene Fälle. In jedem der Fälle gehen wir davon aus, dass wir kleinere Flächen induktiv kacheln können. Starten wir zum Beispiel mit dem Vergrößerungsfaktor 41, ergibt sich die folgende Abfolge von Seitenlängen, siehe auch Abbildung B.5.

$$41 \xrightarrow{-2} 39 \xrightarrow{-2} 37 \xrightarrow{-3} 34 \xrightarrow{/2} 17 \xrightarrow{-2} 15 \xrightarrow{-2} 13 \xrightarrow{-3} 10 \xrightarrow{/2} 5 \xrightarrow{-2} 3 \xrightarrow{-2} 1$$

Nach zehn Schritten haben wir das ursprüngliche Problem auf den trivialen Vergrößerungsfaktor 1 zurückgeführt.

Unserem Beweis liegt das Prinzip der ***noetherschen Induktion*** zugrunde, benannt nach der deutschen Mathematikerin Amalie Emmy Noether (1882–1935). Verschiedentlich wird das Prinzip auch ***starke Induktion*** genannt, da im Induktionsschritt eine sehr viel stärkere Annahme getroffen werden darf:

$$\frac{\forall\, n \in \mathbb{N}\ .\ (\forall\, m < n\ .\ \mathrm{P}(m)) \Longrightarrow \mathrm{P}(n)}{\forall\, n \in \mathbb{N}\ .\ \mathrm{P}(n)}$$

Um eine Aussage zu zeigen, die für alle natürlichen Zahlen gilt, muss gemäß dieses Induktionsprinzips lediglich ein Beweis geführt werden:

- ***Induktionsschritt***: Für alle natürlichen Zahlen n muss man unter der Annahme, dass die Aussage für alle *echt kleineren* Zahlen gilt, zeigen, dass sie für n gilt.

Natürlich hat sich die Induktionsbasis, der Fall $n = 0$, nicht in Luft aufgelöst; sie ergibt sich jetzt als Spezialfall des Induktionsschritts: Für $n = 0$ ist die Induktionsannahme »leer« und man muss schlicht und einfach $\mathrm{P}(0)$ zeigen. Im obigen Kachelungsbeweis gibt es übrigens zwei Basisfälle, die beide trivial sind: $n = 0$ und $n = 1$.

Wir haben im letzten Abschnitt angemerkt, dass das Prinzip der natürlichen Induktion nicht gottgegeben ist, sondern aus den Eigenschaften der natürlichen Zahlen folgt — von Peano als Axiom postuliert. Muss auch das Prinzip der noetherschen Induktion zum Axiom erhoben werden? Hat gar Peano die bequeme Beweismethode bei der Axiomatisierung der natürlichen Zahlen vergessen? Die Antwort auf beide Fragen lautet »Nein!« Die noethersche Induktion ist stark, aber nicht stärker als die natürliche Induktion — sie folgt aus Peanos Axiomensystem. Um den Umgang mit Formeln der Prädikatenlogik etwas einzuüben, wagen wir uns an einen Nachweis dieser vielleicht überraschenden Tatsache. Dazu zeigen wir, dass sich jeder Beweis, der das Prinzip der noetherschen Induktion verwendet, in einen äquivalenten Beweis überführen lässt, der auf der natürlichen Induktion fußt. (Ein Beweis über Beweise — verwirrend?) Der »Trick« besteht darin, die stärkere Induktionsannahme als zu beweisende Aussage zu verwenden:

$$\mathrm{Q}(n) \quad :\Longleftrightarrow \quad \mathrm{P}(0) \ \wedge\ \cdots\ \wedge\ \mathrm{P}(n) \quad \Longleftrightarrow \quad \forall\, m \leqslant n\ .\ \mathrm{P}(m) \tag{B.10a}$$

Das Prädikat Q lässt sich alternativ auch induktiv definieren.

$$\mathrm{Q}(0) \quad :\Longleftrightarrow \quad \mathrm{P}(0) \tag{B.10b}$$

$$\mathrm{Q}(n+1) \quad :\Longleftrightarrow \quad \mathrm{Q}(n) \ \wedge\ \mathrm{P}(n+1) \tag{B.10c}$$

Intuitiv ist vielleicht klar, dass sich P genau dann mit Noethers Prinzip zeigen lässt, wenn sich Q mit Peanos Prinzip beweisen lässt. Zum Nachweis formen wir den noetherschen Induktionsschritt mittels einer Fallunterscheidung über die allquantifizierte Variable n um. **Fall $n := 0$:** Wir haben uns schon überlegt, dass wir in diesem Spezialfall »bedingungslos« $\mathrm{P}(0)$ zeigen müssen.

$$
\begin{aligned}
& (\forall\ m < 0\ .\ \mathrm{P}(m)) \Longrightarrow \mathrm{P}(0) \\
\Longleftrightarrow\quad & \quad \{\ \text{Logik — Quantifizierung über die leere Menge: } (\forall\ m < 0\ .\ \mathrm{P}(m)) \Longleftrightarrow \mathit{true}\ \} \\
& \mathrm{P}(0) \\
\Longleftrightarrow\quad & \quad \{\ \text{Eigenschaft (B.10b)}\ \} \\
& \mathrm{Q}(0)
\end{aligned}
$$

Wir erhalten die Induktionsbasis der natürlichen Induktion. **Fall $n := n + 1$:** In diesem Fall lässt sich der noethersche Induktionsschritt in den Schritt der natürlichen Induktion überführen.

$$
\begin{aligned}
& (\forall\ m < n+1\ .\ \mathrm{P}(m)) \Longrightarrow \mathrm{P}(n+1) \\
\Longleftrightarrow\quad & \quad \{\ \text{Definition Q (B.10a) und } m < n+1 \Longleftrightarrow m \leqslant n\ \} \\
& \mathrm{Q}(n) \Longrightarrow \mathrm{P}(n+1) \\
\Longleftrightarrow\quad & \quad \{\ \text{Logik: } (a \Rightarrow b) \Longleftrightarrow (a \Rightarrow a \wedge b)\ \} \\
& \mathrm{Q}(n) \ \Longrightarrow\ \mathrm{Q}(n) \wedge \mathrm{P}(n+1) \\
\Longleftrightarrow\quad & \quad \{\ \text{Eigenschaft (B.10c)}\ \} \\
& \mathrm{Q}(n) \Longrightarrow \mathrm{Q}(n+1)
\end{aligned}
$$

Mit dem Prinzip der noetherschen Induktion können wir $\forall\, n \in \mathbb{N}\,.\,\mathrm{P}(n)$ folgern, mit dem Prinzip der natürlichen Induktion $\forall\, n \in \mathbb{N}\,.\,\mathrm{Q}(n)$. Aber: Während $\mathrm{Q}(n)$ für jede einzelne natürliche Zahl n stärker ist als $\mathrm{P}(n)$, sind die korrespondierenden Allaussagen äquivalent.

$$
\begin{aligned}
(\forall\, n \in \mathbb{N}\,.\,(\forall\, m < n\,.\,\mathrm{P}(m)) \Longrightarrow \mathrm{P}(n)) \ &\Longleftrightarrow\ (\mathrm{Q}(0) \ \wedge\ \forall\, n \in \mathbb{N}\,.\,\mathrm{Q}(n) \Longrightarrow \mathrm{Q}(n+1)) \\
(\forall\, n \in \mathbb{N}\,.\,\mathrm{P}(n)) \ &\Longleftrightarrow\ (\forall\, n \in \mathbb{N}\,.\,\mathrm{Q}(n))
\end{aligned}
$$

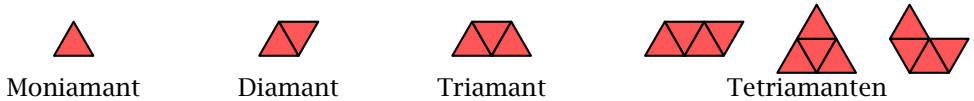
Die Voraussetzungen beider Beweisprinzipien sind äquivalent, die Folgerungen ebenfalls, somit sind auch die Beweisprinzipien selbst äquivalent. Wir halten fest, dass das noethersche Prinzip zwar praktisch bequemer ist, aber nicht theoretisch mächtiger als die natürliche Induktion.

Übungen.

1. Wir haben zwei Methoden kennengelernt, ein $2^n \times 2^n$ Schachbrett mit L-Trominos zu kacheln. Beide Ansätze produzieren die identische Kachelung, aber kann ein Schachbrett tatsächlich nur auf eine Art und Weise gekachelt werden?

2. Der Beweis, dass der L-Tromino ein rep-tile ist, verwendet eine Fallunterscheidung über den Divisionsrest des Vergrößerungsfaktors: n ***mod*** 3. Versuchen Sie einen alternativen, kürzeren (?) Beweis zu finden, der nur zwischen geraden und ungeraden Vergrößerungsfaktoren unterscheidet.

3. Ein ***Triamant*** setzt sich aus drei gleichseitigen Dreiecken zusammen (ein halbes Hexagon). Der Name ist eine Rückbildung des Wortes *Di*amant, so gewählt, da ein Diamant oft in der Form von zwei gleichseitigen Dreiecken gezeichnet wird. (Diamant geht tatsächlich auf das lateinische Wort *adamus* zurück; etymologisch ist somit *di* nicht der griechische Präfix für zwei.)

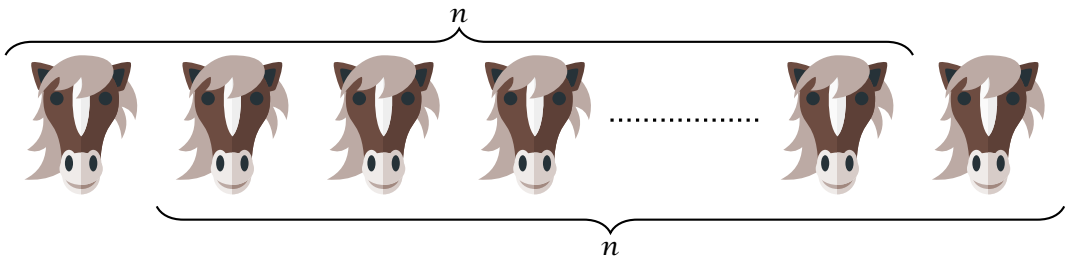


(a) Versuchen Sie, ein gleichseitiges Dreieck der Seitenlänge n mit n ***div*** 3 Triamanten zu kacheln. Ist n nicht durch drei teilbar, muss ein Feld frei bleiben. Kann dieses Feld wie im Fall der L-Trominos frei gewählt werden?

(b) Zeigen Sie, dass der Triamant ein rep-tile ist.

Ein ***Polyiamant*** besteht aus k gleichseitigen Dreiecken. Während für $k \leqslant 3$ jeweils nur eine Form existiert, gibt es drei unterschiedliche Tetriamanten: die Pfeile, das Dreieck und das Segelboot. Denken Sie sich Kachelungsaufgaben aus, lassen Sie ihrer Phantasie freien Lauf. (Lässt sich ein Dreieck mit Tetriamanten kacheln? Ein Pfeil? Ein Segelboot? Welche Figuren sind rep-tiles?)

4. Eine gewagte Aussage: »In einer Herde mit n Pferden ($n > 0$), besitzen alle Pferde die gleiche Farbe.« Was stimmt mit dem Beweis nicht? »Wir zeigen die Aussage durch natürliche Induktion über n. **Induktionsbasis:** Besteht die Herde nur aus einem Pferd, gilt offensichtlich die Aussage. **Induktionsschritt:** Wir stellen die $n + 1$ Pferde nebeneinander auf.



Gemäß der Induktionsannahme besitzen die ersten n Pferde die gleiche Farbe. Wir wenden die Induktionsannahme ein zweites Mal an, diesmal auf die letzten n Pferde. Da die ersten n Pferde *und* die letzten n Pferde die gleiche Farbe besitzen, können wir folgern, dass alle Pferde die gleiche Farbe besitzen müssen.«

B.4. Ordnungen und Verbände

Order! Order! Order!
— John Simon Bercow (1963)

Ordnung ist das halbe Leben — sie durchdringt unseren Alltag, die Mathematik und die Informatik. Wir ordnen an: ersten, zweitens, drittens, … Wir vergleichen: besser und schlechter, billiger und teurer, kleiner und größer, langsamer und schneller, … Wir gruppieren, reihen und sortieren. Dieser Abschnitt präzisiert die Begriffe, die sich um Ordnungen ranken, und führt Boolesche Algebren ein zweites Mal ein, diesmal durch die ordnungstheoretische Brille betrachtet als Boolesche Verbände.

B.4.1. Ordnungen

Eine Menge P mit einer Relation $R \subseteq P \times P$ heißt ***Quasiordnung***, wenn R ***reflexiv*** und ***transitiv*** ist. Ist die Ordnungsrelation ***total***, so spricht man entsprechend von einer ***totalen Quasiordnung***, anderenfalls von einer ***partiellen Quasiordnung***. Eine ***Ordnung*** liegt vor, wenn R zusätzlich ***antisymmetrisch*** ist. Eine ***totale Ordnung*** besitzt alle vier Eigenschaften. Eine Ordnungsrelation wird üblicherweise mit dem Vergleichszeichen $\leqslant$ notiert, das in vielen verschiedenen Variationen existiert: $\leq$, $\leqslant$, $\preceq$, $\preccurlyeq$, $\subseteq$.

(Reflexivität)	$a \leqslant a$
(Transitivität)	$a \leqslant b \;\wedge\; b \leqslant c \;\Longrightarrow\; a \leqslant c$
(Totalität)	$a \leqslant b \;\vee\; b \leqslant a$
(Antisymmetrie)	$a \leqslant b \;\wedge\; b \leqslant a \;\Longrightarrow\; a = b$

Ist a kleiner gleich b und b kleiner gleich c, so schreibt man oft abkürzend $a \leqslant b \leqslant c$.[8] Die umgangssprachliche Aussage »a ist kleiner als b« lässt in der Regel offen, ob $a \leqslant b$ oder $a < b$ gemeint ist. Ist Ersteres intendiert, so formuliert man präziser »a ist höchstens so groß wie b«. Um zu betonen, dass gleiche Werte nicht zulässig sind, kann man den Gradpartikel »echt« hinzufügen: »a ist *echt* kleiner als b.« Wenn wir die zugrundeliegende Menge P explizit benennen wollen, schreiben wir »$a \leqslant b$ in P«.

Aus einer gegebenen Quasiordnung lassen sich weitere Relationen ableiten: die ***duale*** Ordnung $\geqslant$, die die Quasiordnung »auf den Kopf stellt«; die ***Äquivalenzrelation*** $\sim$; die ***strikten*** Ordnungen $<$ und $>$; und die ***Unvergleichbarkeitsrelation*** $\parallel$.

$$
\begin{array}{rcl}
a \geqslant b & :\Longleftrightarrow & b \leqslant a \\
a \sim b & :\Longleftrightarrow & a \leqslant b \ \wedge \ b \leqslant a \\
a < b & :\Longleftrightarrow & a \leqslant b \ \wedge \ \neg(b \leqslant a) \iff b > a \\
a > b & :\Longleftrightarrow & \neg(a \leqslant b) \ \wedge \ b \leqslant a \iff b < a \\
a \parallel b & :\Longleftrightarrow & \neg(a \leqslant b) \ \wedge \ \neg(b \leqslant a)
\end{array}
$$

Eine strikte Ordnung ist ***irreflexiv*** und transitiv; eine Äquivalenzrelation ist reflexiv, ***symmetrisch*** und transitiv.

(Irreflexivität)	$\neg(a < a)$
(Symmetrie)	$a \sim b \implies b \sim a$

Ist $\leqslant$ eine *totale* Quasiordnung, dann ergeben sich die strikten als Negation der nicht-strikten Ordnungen: $\neg(a \leqslant b) \iff (a > b)$ und $\neg(a < b) \iff (a \geqslant b)$, siehe auch Aufgabe B.4.1. Diesen Zusammenhang nutzt man auch bei der Verbalisierung von Ordnungen aus: $a > 0$ wird »a ist positiv« ausgesprochen, $a \geqslant 0$ hingegen »a ist nichtnegativ.«

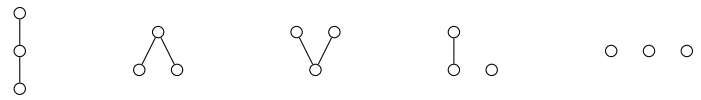
Die Wahrheitswerte $\mathbb{B}$ bilden mit der Implikation $\Rightarrow$ eine totale Ordnung, »falsch« ist kleiner als »wahr« : *false* $\Rightarrow$ *true* (oder mit George Booles arithmetischer Notation: $0 \leqslant 1$). Die Potenzmenge $\mathcal{P}(U)$ bildet mit der Mengeninklusion $\subseteq$ eine partielle Ordnung. Auf den natürlichen Zahlen $\mathbb{N}$ lassen sich verschiedene Ordnungen definieren:

$$a \leqslant b \quad :\Longleftrightarrow \quad \exists\, d \in \mathbb{N} \ .\ d + a = b \tag{B.11}$$

$$a \setminus b \quad :\Longleftrightarrow \quad \exists\, q \in \mathbb{N} \ .\ q \cdot a = b \tag{B.12}$$

Die »übliche« Ordnung auf den natürlichen Zahlen »$\leqslant$« ist total; die ***Teilbarkeitsrelation*** »$\setminus$« ist hingegen partiell.

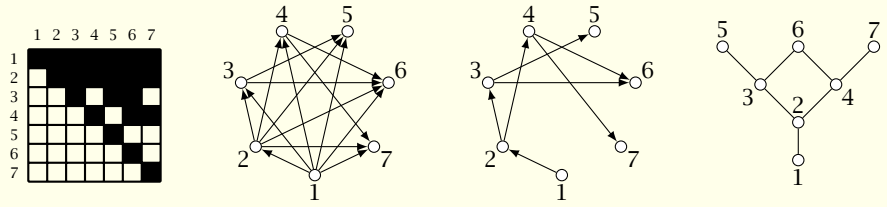
Ordnungen lassen sich wunderbar mit Hilfe sogenannter ***Hassediagramme*** veranschaulichen, siehe Abbildung B.6. Drei Elemente können zum Beispiel auf fünf unterschiedliche Weisen angeordnet werden:



Das Diagramm auf der linken Seite repräsentiert eine totale Ordnung (eine ***Kette***), das Diagramm ganz rechts eine ***diskrete Ordnung*** (eine ***Antikette***): Zwei Elemente sind genau dann angeordnet, wenn sie identisch sind. Das folgende Diagramm ordnet die Teiler der Zahl 60 an — einen umfassenderen Ausschnitt der Teilbarkeitsordnung findet man in Abbildung B.12.

[8] Geschachtelte Ausdrücke kennen wir von Summen und Produkten. Die Schachtelung meint hier aber etwas völlig anderes: $a + b + c$ ist *assoziativ* zu lesen, $(a + b) + c$ oder $a + (b + c)$, und wird üblicherweise bei assoziativen Operationen verwendet; $a \leqslant b \leqslant c$ ist hingegen *konjunktiv* zu lesen, $a \leqslant b \wedge b \leqslant c$, und wird üblicherweise bei transitiven Relationen verwendet.

Ordnungsrelationen lassen sich ganz unterschiedlich darstellen, als Tabellen⧵Matrizen, als gerichtete Graphen oder als Hassediagramme.



Die Darstellung als Tabelle spiegelt mehr oder weniger direkt die definierenden Eigenschaften einer Ordnungsrelation wider: Reflexivität (die Einträge in der Hauptdiagonalen sind gesetzt), Antisymmetrie (korrespondierende Felder über und unter der Hauptdiagonalen sind nicht gleichzeitig markiert), Transitivität (weniger offensichtlich: werden Zeilen und Spalten so permutiert, dass »aufeinanderfolgende« Elemente benachbart sind, füllen diese ein Dreieck).

Der ***Graph*** einer Relation visualisiert die Beziehungen: Zwei Elemente sind angeordnet, wenn die entsprechenden Knoten durch eine gerichtete Kante verbunden sind. Durch die Reflexivität bedingte »Schleifen« spart man dabei aus Gründen der Übersichtlichkeit aus. Noch übersichtlicher wird die Darstellung, wenn man zusätzlich »redundante«, transitive Kanten weglässt und vereinbart, dass zwei Elemente angeordnet sind, wenn sie durch einen *Pfad*, eine Abfolge von gerichteten Kanten verbunden sind. Statt der Ordnungsrelation $\leqslant$ zeichnet man lediglich die ***Bedeckungsrelation*** (engl. covering relation) $\prec$.

$$a \prec b \quad :\Longleftrightarrow \quad a < b \ \wedge \ \neg(\exists\, x \ .\ a < x < b)$$

Zwei verschiedene, angeordnetete Elemente folgen ***direkt*** aufeinander, wenn zwischen ihnen keine weiteren Elemente liegen. Die Bedeckungsrelation $\prec$ ist die kleinste Relation, aus der sich die ursprüngliche Ordnungsrelation rekonstruieren lässt.

Aufgrund der Antisymmetrie sind die Graphen ***azyklisch***: Es gibt keinen Pfad, der von einem Knoten zu dem Knoten selbst zurückführt. In einem ***Hassediagramm*** nutzt man diese Eigenschaft aus: Zwei direkt aufeinanderfolgende Elemente $a \prec b$ werden durch eine ungerichtete, *nichthorizontale* Kante verbunden; dabei wird das kleinere Element a weiter unten positioniert und das größere Element b weiter oben.

Die gleiche Ordnung kann durch verschiedene Hassediagramme visualisiert werden. Das Zeichnen dieser Diagramme ist tatsächlich eine Kunst; ihre »Lesbarkeit« hängt stark von der Platzierung der Knoten ab. Die folgenden Hassediagramme deuten die künstlerische Freiheit an — alle visualisieren die gleiche Ordnungsrelation. (Welche?)

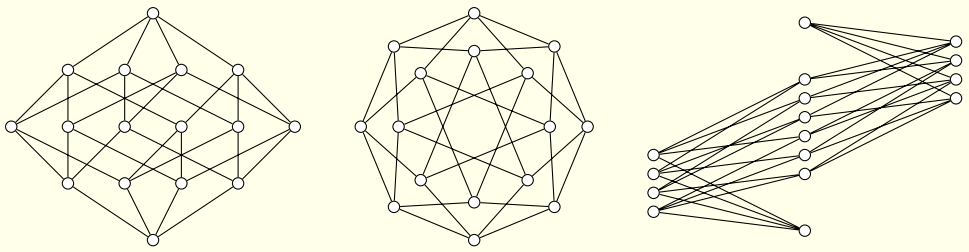
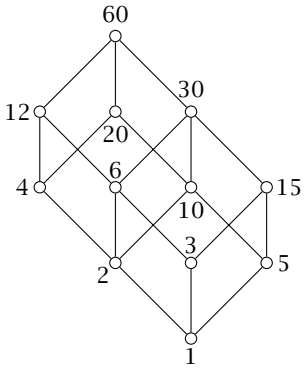


Abbildung B.6.: Tabellen, gerichtete Graphen und Hassediagramme.



Es gibt übrigens mehr als eine Billion verschiedene Möglichkeiten, zwölf Elemente anzuordnen — laut OEIS sind es exakt 1.104.891.746 Ordnungsrelationen, siehe A000112.

Ordnungshomomorphismen\Monotone Funktionen Seien $(P, \leqslant)$ und $(Q, \sqsubseteq)$ zwei Ordnungen. Funktionen zwischen P und Q können die Ordnungen ***erhalten*** oder ***reflektieren***.

$$a \leqslant b \implies f(a) \sqsubseteq f(b) \tag{B.13a}$$
$$a \leqslant b \impliedby g(a) \sqsubseteq g(b) \tag{B.13b}$$
$$a \leqslant b \iff h(a) \sqsubseteq h(b) \tag{B.13c}$$

Die Funktion $f : P \to Q$ erhält die Ordnung; eine ordnungserhaltende Funktion heißt auch ***Ordnungshomomorphismus***. Die Funktion $h : P \to Q$ erhält und reflektiert die Ordnung; h ist eine ***Ordnungseinbettung***. Die identische Abbildung ist eine Ordnungseinbettung; komponiert man monotone Funktionen, erhält man wieder eine monotone Funktion. Sind $\leqslant$ und $\sqsubseteq$ *totale* Ordnungen, dann folgt aus (B.13a)–(B.13c) mittels Kontraposition:

$$a > b \impliedby f(a) \sqsupset f(b)$$
$$a > b \implies g(a) \sqsupset g(b)$$
$$a > b \iff h(a) \sqsupset h(b)$$

Homomorphismus
Für jede mathematische Struktur führt man strukturerhaltende Abbildungen ein, die ***Homomorphismen*** (homo- griech. «gemeinsam, gleich, ähnlich«; Morphe griech. »Gestalt, Form, Aussehen«). Die Werte einer homomorphen Abbildung verhalten sich hinsichtlich der Struktur ebenso, wie sich die Argumente im Definitionsbereich verhalten.

Die Funktion f reflektiert die strikte Ordnung, während g sie erhält.

Sind beide Ordnungen identisch, so heißt $f : (P, \leqslant) \to (P, \leqslant)$ ***isoton***. Sind die beteiligten Ordnungen dual zueinander, so bezeichnet man $f : (P, \leqslant) \to (P, \geqslant)$ als ***antiton***.

In der Analysis sind folgende, alternative Bezeichnungen gebräuchlich.

f erhält die Ordnung	f monoton	$a \leqslant b \implies f(a) \sqsubseteq f(b)$
f erhält die strikte Ordnung	f streng monoton	$a < b \implies f(a) \sqsubset f(b)$
f isoton	f monoton steigend	$a \leqslant b \implies f(a) \leqslant f(b)$
f antiton	f monoton fallend	$a \leqslant b \implies f(a) \geqslant f(b)$

Beweistechniken Um die Gleichheit bzw. Ungleichheit von Elementen nachzuweisen, gibt es zwei populäre Beweistechniken: den Ping-Pong Beweis und den indirekten Beweis.

Der ***Ping-Pong Beweis*** leitet sich direkt aus Reflexivität und Antisymmetrie ab.

$$a = b \iff a \leqslant b \ \wedge \ b \leqslant a \tag{B.14}$$

Ich zeige, dass das eine Element von dem anderen dominiert wird und umgekehrt.

Der ***indirekte Beweis*** basiert auf der folgenden Einsicht: Zwei Elemente sind gleich, wenn sie sich zu allen Elementen gleich verhalten (»soziale Gleichheit«).

$$a = b \iff \forall\, x \in \mathrm{P} \,.\, a \leqslant x \iff b \leqslant x \tag{B.15a}$$
$$a = b \iff \forall\, x \in \mathrm{P} \,.\, x \leqslant a \iff x \leqslant b \tag{B.15b}$$
$$a \leqslant b \iff \forall\, x \in \mathrm{P} \,.\, a \leqslant x \impliedby b \leqslant x \tag{B.15c}$$
$$a \leqslant b \iff \forall\, x \in \mathrm{P} \,.\, x \leqslant a \implies x \leqslant b \tag{B.15d}$$

Die Technik der Indirektion kommt auch bei Definitionen zum Einsatz, etwa wenn ein Element durch seine Beziehungen zu anderen Elementen festgelegt wird. Die folgenden Konzepte illustrieren »indirekte Definitionen«.

Extrema und Schranken Die Ordnung P besitzt genau dann ein ***kleinstes Element*** $\bot$, wenn für alle $b \in \mathrm{P}$ gilt:

$$\text{(kleinstes Element)} \qquad \bot \leqslant b \tag{B.16}$$

Entsprechend besitzt P ein ***größtes Element*** $\top$, wenn für alle $a \in \mathrm{P}$ gilt:

$$\text{(größtes Element)} \qquad a \leqslant \top \tag{B.17}$$

In der »Standardordnung« $(\mathbb{N}, \leqslant)$ ist 0 das kleinste Element; ein größtes Element gibt es nicht. In der »Teilbarkeitsordnung« $(\mathbb{N}, \backslash)$ ist 1 das kleinste und 0 das größte Element!

Sei P eine Ordnung und $\mathrm{A}, \mathrm{B} \subseteq \mathrm{P}$. Die Menge A besitzt genau dann eine ***kleinste obere Schranke*** oder ein ***Supremum*** $\bigsqcup \mathrm{A}$, wenn für alle $b \in \mathrm{P}$ gilt:

$$\text{(kleinste obere Schranke}\backslash\text{Supremum)} \qquad \bigsqcup \mathrm{A} \leqslant b \iff (\forall\, a \in \mathrm{A} \,.\, a \leqslant b) \tag{B.18}$$

Ein Element b, das die Formel auf der rechten Seite erfüllt, heißt ***obere Schranke*** von A: b ist größer als alle Elemente in A. Von links nach rechts gelesen besagt die obige Äquivalenz, dass $\bigsqcup \mathrm{A}$ eine obere Schranke von A ist — ersetze b durch $\bigsqcup \mathrm{A}$. Von rechts nach links gelesen wird $\bigsqcup \mathrm{A}$ als kleinste aller oberen Schranken identifiziert.

Entsprechend existiert die ***größte untere Schranke*** oder das ***Infimum*** $\bigsqcap \mathrm{B}$ von B, wenn für alle $a \in \mathrm{P}$ gilt:

$$\text{(größte untere Schranke}\backslash\text{Infimum)} \qquad (\forall\, b \in \mathrm{B} \,.\, a \leqslant b) \iff a \leqslant \bigsqcap \mathrm{B} \tag{B.19}$$

Gilt $\bigsqcap \mathrm{B} \in \mathrm{B}$, so wird $\bigsqcap \mathrm{B}$ auch ***Minimum*** von B genannt (alternativ notiert: $\min \mathrm{B}$); entsprechend heißt $\bigsqcup \mathrm{A}$ mit $\bigsqcup \mathrm{A} \in \mathrm{A}$ ***Maximum*** von A (alternativ notiert: $\max \mathrm{A}$).

In der Standardordnung $(\mathbb{N}, \leqslant)$ besitzt jede *nicht-leere* Menge ein Infimum, das Minimum der Menge; jede *endliche* Menge ein Supremum, das Maximum der Menge. In der »Teilbarkeitsordnung« $(\mathbb{N}, \backslash)$ existieren Suprema und Infima beliebiger Mengen! Abschnitt B.5.4 beschäftigt sich ausführlich mit der Teilbarkeitsordnung.

Übungen.

1. Je mehr Eigenschaften eine Quasiordnung besitzt, desto enger sind die verschiedenen Relationen miteinander verbandelt.

(a) Sei $\leqslant$ eine totale Quasiordnung. Zeigen Sie:

$$\neg(a \leqslant b) \iff a > b \qquad \neg(a \geqslant b) \iff a < b \tag{B.20a}$$
$$\neg(a < b) \iff a \geqslant b \qquad \neg(a > b) \iff a \leqslant b \tag{B.20b}$$

(b) Sei $\leqslant$ eine totale Ordnung. Zeigen Sie:

$$a \leqslant b \iff a = b \vee a < b \qquad a \geqslant b \iff a = b \vee a > b \tag{B.20c}$$
$$a < b \iff a \neq b \wedge a \leqslant b \qquad a > b \iff a \neq b \wedge a \geqslant b \tag{B.20d}$$

2. Welche der folgenden Funktionen des Typs $\mathbb{R} \to \mathbb{R}$ sind isoton, welche der Funktionen sind antiton (jeweils für $c = 3$ und $c = -3$)?

$$f(x) := x + c \qquad g(x) := c - x \qquad h(x) := x \cdot c \qquad k(x) := c/x$$

3. »Aus Alt mach Neu.« Sei $f : \mathrm{P} \to \mathrm{Q}$ eine beliebige Funktion. Zeigen Sie, dass sich bestimmte auf Q definierte Strukturen mittels f auf P übertragen lassen.

(a) Wenn $\sqsubseteq$ eine Quasiordnung ist, dann wird durch

$$a \leqslant b \quad :\Longleftrightarrow \quad f(a) \sqsubseteq f(b)$$

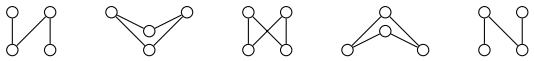
eine Quasiordnung auf P definiert. Ist zum Beispiel P eine Menge von Personen und f ein bestimmtes Merkmal (etwa Alter oder Körpergröße), dann ordnet $\leqslant$ Personen bezüglich dieses Merkmals an (etwa absteigend nach ihrem Alter oder aufsteigend nach der Körpergröße). Ist $\leqslant$ antisymmetrisch (total), wenn $\sqsubseteq$ antisymmetrisch (total) ist?

(b) Wenn $\equiv$ eine Äquivalenzrelation ist, dann wird durch

$$a \sim b \quad :\Longleftrightarrow \quad f(a) \equiv f(b)$$

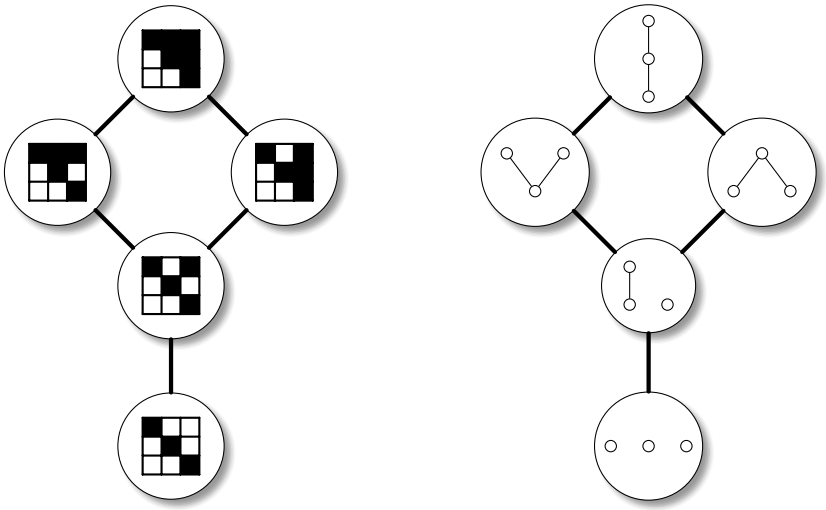
eine Äquivalenzrelation auf P definiert.

4. Welche Hassediagramme visualisieren die gleiche Ordnung?



5. Sei $\leqslant$ eine endliche Ordnung. Wie groß ist die Bedeckungsrelation $\prec$ im Vergleich zur Ordnungsrelation im besten und im schlechtesten Fall?

6. »Wir ordnen die Ordnungen.« Da eine Relation eine Menge von Paaren ist, lassen sich Relationen, insbesondere Ordnungsrelationen, mit der Teilmengenbeziehung anordnen. Die fünf Ordnungen auf einer 3-elementigen Menge sind wie folgt angeordnet.



Die kleinste Ordnung ist die Antikette, die größte die Kette. Die Ordnung auf der linken Seite ist dual zur Ordnung auf der rechten Seite; die Ordnungen in der Mitte sind selbstdual. Erstellen Sie analoge Diagramme für alle 16 Ordnungen auf 4 Elementen.

7. Zeigen Sie, dass die »indirekten Beweise« (B.15a)–(B.15d) korrekte Beweistechniken sind.

8. Lisa Lista ist sich unsicher, ob durch die »indirekten Definitionen« Extrema ($\bot$ und $\top$) und Schranken ($\bigsqcup$ und $\bigsqcap$) tatsächlich *eindeutig* definiert werden. Helfen Sie ihr. (Betrachtet man statt Ordnungen nur Quasiordnungen, dann ist die Eindeutigkeit nicht länger garantiert: Es kann zum Beispiel mehrere kleinste Elemente geben, diese sind aber notwendigerweise äquivalent. Allgemein werden im Fall von Quasiordnungen durch indirekte Definitionen Konzepte nur bis auf Äquivalenz eindeutig festgelegt.)

9. Harry Hacker fragt sich, ob es auch größte obere und kleinste untere Schranken gibt.

B.4.2. Verbände ⋆

Wenden wir uns den algebraischen Eigenschaften der kleinsten oberen und der größten unteren Schranke zu und nehmen die Gelegenheit wahr, einige Beweise zu führen. Dazu vereinbaren wir Abkürzungen für binäre Suprema und Infima:

$$a \sqcup b := \bigsqcup\{a, b\} \qquad\qquad a \sqcap b := \bigsqcap\{a, b\} \tag{B.21}$$

Das binäre Maximum notieren wir $a \uparrow b$, das Minimum mit $a \downarrow b$. (In Abschnitt 5.1.5 haben wir die alternative Notation $a \triangleright b$ und $a \triangleleft b$ verwendet.)

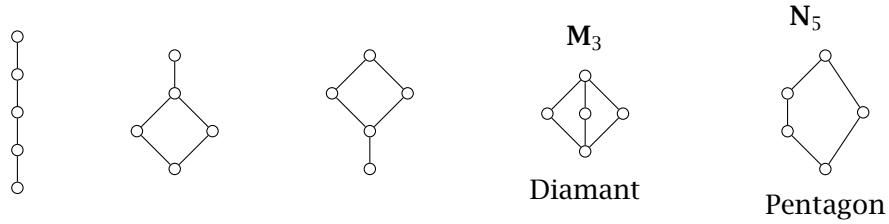
Abbildung B.7 fasst die Gesetze sogenannter ***Boolescher Verbände*** zusammen, die wir im Folgenden Schritt für Schritt einführen und diskutieren.

Eine Ordnung P heißt ***Verband*** (engl. lattice), wenn $a \sqcup b$ und $a \sqcap b$ für alle $a, b \in \mathrm{P}$ existieren. Der Verband ist darüber hinaus ***vollständig*** (engl. complete), wenn $\bigsqcup \mathrm{A}$ und $\bigsqcap \mathrm{B}$ für beliebige Teilmengen $\mathrm{A}, \mathrm{B} \subseteq \mathrm{P}$ existieren. Ein vollständiger Verband besitzt stets ein kleinstes und ein größtes Element:

$$\bigsqcup \varnothing = \bot = \bigsqcap \mathrm{P} \qquad\qquad \bigsqcap \varnothing = \top = \bigsqcup \mathrm{P}$$

Jede totale Ordnung ist ein Verband mit dem Maximum als Supremum und dem Minimum als Infimum. Jeder endliche Verband mit Extremelementen ist vollständig. Die Wahrheitswerte mittels *false* $\Rightarrow$ *true* angeordnet bilden somit einen vollständigen Verband: Das Supremum ist durch die Disjunktion $\vee$ gegeben, das Infimum durch die Konjunktion $\wedge$. Ein Potenzmengenverband ist das paradigmatische Beispiel für einen vollständigen Verband: die Mengenvereinigung $\bigcup$ dient als Supremum, der Mengendurchschnitt $\bigcap$ als Infimum. Die Teilbarkeitsordnung $(\mathbb{N}, \backslash)$ ist ebenfalls vollständig: Das Infimum ist der ***größte gemeinsame Teiler***, das Supremum das ***kleinste gemeinsame Vielfache***.

Von den insgesamt 63 Ordnungen mit fünf Elementen erfüllen nur 5 die Verbandseigenschaften — OEIS listet die Gesamtzahl aller Verbände mit n Elementen als A006966.



Das Scheitern kann zwei unterschiedliche Ursachen haben: (1) Elemente besitzen keine obere (untere) Schranke; (2) es existieren zwar obere (untere) Schranken, aber keine kleinste (größte). Die unten aufgeführten Diagramme zeigen Beispiele des Scheiterns.

Statt Supremum und Infimum von der kleinsten oberen bzw. der größten unteren Schranke abzuleiten, können wir sie alternativ mittels der folgenden Äquivalenzen definieren — (B.22) und (B.23) sind (B.18) und (B.19) spezialisiert auf 2-elementige Mengen.

$$\text{(binäres Supremum)} \qquad a_1 \sqcup a_2 \leqslant b \iff a_1 \leqslant b \ \wedge \ a_2 \leqslant b \tag{B.22}$$

$$\text{(binäres Infimum)} \qquad a \leqslant b_1 \ \wedge \ a \leqslant b_2 \iff a \leqslant b_1 \sqcap b_2 \tag{B.23}$$

Konzentrieren wir uns auf das Supremum — die folgenden Erörterungen gelten entsprechend für das Infimum. Überlegen wir, welche Folgerungen sich aus (B.22) ziehen lassen. Wir können zum Beispiel die linke Seite der Äquivalenz wahr machen, indem wir b durch $a_1 \sqcup a_2$ ersetzen. Somit gilt auch die rechte Seite und wir erhalten:

$$\text{(obere Schranke)} \qquad a_1 \leqslant a_1 \sqcup a_2 \ \wedge \ a_2 \leqslant a_1 \sqcup a_2 \tag{B.24a}$$

Die Formel besagt, dass das Supremum $a_1 \sqcup a_2$ tatsächlich eine obere Schranke von a_1 und a_2 ist. (Welche Formel erhalten wir, wenn wir umgekehrt die rechte Seite von (B.22) wahr machen?)

Das Supremum »verträgt« sich mit der zugrundeliegenden Ordnung: $\sqcup$ ist ***ordnungserhaltend*** oder ***monoton***.

$$\text{(Monotonie)} \qquad a_1 \leqslant b_1 \ \wedge \ a_2 \leqslant b_2 \implies a_1 \sqcup a_2 \leqslant b_1 \sqcup b_2 \tag{B.24b}$$

Der Beweis basiert im Wesentlichen auf der Transitivität der Ordnungsrelation.

$$\begin{aligned}
& a_1 \sqcup a_2 \leqslant b_1 \sqcup b_2 \\
\iff & \quad \{ \text{ Supremum (B.22) } \} \\
& a_1 \leqslant b_1 \sqcup b_2 \ \wedge \ a_2 \leqslant b_1 \sqcup b_2 \\
\impliedby & \quad \{ \text{ obere Schranken } b_1 \leqslant b_1 \sqcup b_2 \text{ und } b_2 \leqslant b_1 \sqcup b_2 \text{ (B.24a) und Transitivität } \} \\
& a_1 \leqslant b_1 \ \wedge \ a_2 \leqslant b_2
\end{aligned}$$

Das Supremum ist weiterhin assoziativ, kommutativ und idempotent. Da die Operation indirekt definiert worden ist, führt man die Beweise ebenfalls indirekt.

$$\begin{aligned}
& a \sqcup b \leqslant x \\
\iff & \quad \{ \text{ Supremum (B.22) } \} \\
& a \leqslant x \ \wedge \ b \leqslant x \\
\iff & \quad \{ \text{ Logik: } \wedge \text{ ist kommutativ } \} \\
& b \leqslant x \ \wedge \ a \leqslant x \\
\iff & \quad \{ \text{ Supremum (B.22) } \} \\
& b \sqcup a \leqslant x
\end{aligned}$$

Die Kommutativität von $\sqcup$ folgt somit aus der entsprechenden Eigenschaft der Konjunktion. Gleiches gilt für Assoziativität und Idempotenz.

Verbindungslemma Die folgenden Äquivalenzen, das sogenannte ***Verbindungslemma*** (engl. connection lemma), setzen Supremum $\sqcup$ und Infimum $\sqcap$ zueinander und mit der Ordnungsrelation $\leqslant$ in Beziehung.

$$a \sqcup b = b \iff a \leqslant b \iff a \sqcap b = a \tag{B.25}$$

Wir zeigen die erste Äquivalenz — ein analoger Beweis etabliert die zweite.

$$
\begin{aligned}
& a \sqcup b = b \\
\iff & \quad \{ \text{ Ping-Pong Beweis (B.14) } \} \\
& a \sqcup b \leqslant b \ \wedge \ b \leqslant a \sqcup b \\
\iff & \quad \{ \ a \sqcup b \text{ ist eine obere Schranke von } a \text{ und } b \text{ (B.24a) } \} \\
& a \sqcup b \leqslant b \\
\iff & \quad \{ \text{ Supremum (B.22) } \} \\
& a \leqslant b \ \wedge \ b \leqslant b \\
\iff & \quad \{ \text{ Reflexivität } \} \\
& a \leqslant b
\end{aligned}
$$

Aus dem Verbindungslemma lassen sich interessante Schlüsse ziehen, indem man die Ungleichung mit bekannten Fakten instantiiert, zum Beispiel (B.24a) und (B.28a):

$$
a \sqcap (a \sqcup b) = a \iff a \leqslant a \sqcup b
$$

$$
a \sqcap b \leqslant b \iff (a \sqcap b) \sqcup b = b
$$

Wir erhalten die Adjunktivgesetze, die das Zusammenspiel von $\sqcup$ und $\sqcap$ regeln.

Ist P eine totale Ordnung, dann ist das Supremum $a \sqcup b$ das Maximum von a und b und $a \sqcap b$ das Minimum — eine direkte Konsequenz aus dem Verbindungslemma.

$$
a \sqcup b = a \ \vee \ a \sqcup b = b \iff a \leqslant b \ \vee \ b \leqslant a \iff a \sqcap b = a \ \vee \ a \sqcap b = b
$$

Verbände als algebraische Strukturen Als einstweiliges Fazit halten wir fest, dass aus der ordnungstheoretischen Definition des Verbands die algebraischen Eigenschaften der Operationen folgen, die wir schon im Zusammenhang mit Booleschen Algebren kennengelernt haben, siehe Abbildung B.2.

$$
\begin{aligned}
&\text{(Supremum)} \ \wedge \ \text{(Infimum)} \iff \\
&\qquad \text{(Assoziativität)} \ \wedge \ \text{(Kommutativität)} \ \wedge \ \text{(Idempotenz)} \ \wedge \ \text{(Adjunktivität)}
\end{aligned}
$$

Auch die Umkehrung gilt: Eine algebraische Struktur mit zwei Operationen $\oplus$ und $\otimes$, die assoziativ, kommutativ und idempotent sind und die die Adjunktivgesetze erfüllen, definiert einen Verband. Für den Beweis konzentrieren wir uns zunächst auf eine einzelne Operation: Ist $\oplus$ assoziativ, kommutativ und idempotent, so wird mit

$$
a \leqslant b \quad :\iff \quad a \oplus b = b
$$

eine partielle Ordnung definiert — eine Hälfte des Verbindungslemmas gilt damit *per definitionem*. Die Reflexivität von $\leqslant$ folgt aus der Idempotenz von $\oplus$, die Transitivität aus der Assoziativität und die Antisymmetrie aus der Kommutativität. Weiterhin ist $\oplus$ das Supremum. Die Gültigkeit von (B.22) zeigen wir mit einem Ping-Pong Beweis.

»⟹«: Wir nehmen an, dass $a_1 \oplus a_2 \leqslant b$ bzw. $a_1 \oplus a_2 \oplus b = b$ gilt, und zeigen $a_1 \leqslant b$ bzw. $a_1 \oplus b = b$ und $a_2 \leqslant b$ bzw. $a_2 \oplus b = b$:

$$
\begin{aligned}
& a_1 \oplus b \\
= & \quad \{ \text{ Annahme: } a_1 \oplus a_2 \oplus b = b \} \\
& a_1 \oplus a_1 \oplus a_2 \oplus b \\
= & \quad \{ \text{ Idempotenz } \} \\
& a_1 \oplus a_2 \oplus b \\
= & \quad \{ \text{ Annahme: } a_1 \oplus a_2 \oplus b = b \} \\
& b
\end{aligned}
$$

»⟸«: Wir nehmen an, dass $a_1 \leqslant b$ bzw. $a_1 \oplus b = b$ und $a_2 \leqslant b$ bzw. $a_2 \oplus b = b$ gelten, und zeigen $a_1 \oplus a_2 \leqslant b$ bzw. $a_1 \oplus a_2 \oplus b = b$:

$$
\begin{aligned}
& a_1 \oplus a_2 \oplus b \\
= & \quad \{ \text{ Annahme: } a_2 \oplus b = b \} \\
& a_1 \oplus b \\
= & \quad \{ \text{ Annahme: } a_1 \oplus b = b \} \\
& b
\end{aligned}
$$

Ein analoger Beweis zeigt $a_2 \oplus b = b$.

Wir haben einen sogenannten Halbverband vor uns — eine Ordnung P heißt ***Halbverband***, wenn das Supremum stets existiert.

Zwei Halbverbände über der gleichen Grundmenge formen einen Verband, wenn die beiden Operationen $\oplus$ und $\otimes$ das Adjunktivgesetz erfüllen. Dann gilt das Verbindungslemma (B.25), $a \oplus b = b \iff a \otimes b = a$, wie der folgende Ping-Pong Beweis zeigt.

»⟹«: Wir nehmen an, dass $a \oplus b = b$ gilt, und zeigen $a \otimes b = a$:

$$
\begin{aligned}
& a \otimes b \\
= & \quad \{ \text{ Annahme: } a \oplus b = b \} \\
& a \otimes (a \oplus b) \\
= & \quad \{ \text{ Adjunktivität } \} \\
& a
\end{aligned}
$$

»⟸«: Wir nehmen an, dass $a \otimes b = a$ gilt, und zeigen $a \oplus b = b$:

$$
\begin{aligned}
& a \oplus b \\
= & \quad \{ \text{ Annahme: } a \otimes b = a \} \\
& (a \otimes b) \oplus b \\
= & \quad \{ \text{ Adjunktivität } \} \\
& b
\end{aligned}
$$

Verbände mit kleinstem und größtem Element Besitzt ein Verband ein kleinstes bzw. ein größtes Element, so sind diese neutrale bzw. absorbierende Elemente des Supremums bzw. Infimums — eine weitere Konsequenz aus dem Verbindungslemma.

$$\bot \sqcap b = \bot \iff \bot \leqslant b \iff \bot \sqcup b = b$$
$$a \sqcap \top = a \iff a \leqslant \top \iff a \sqcup \top = \top$$

Aus der Definition der Ordnung $a \leqslant b \iff a \oplus b = b$ bzw. $a \leqslant b \iff a \otimes b = a$ folgt auch die Umkehrung und somit:

$$\text{(kleinstes Element)} \ \wedge \ \text{(größtes Element)} \iff \text{(Neutralität)} \ \wedge \ \text{(Extreme)}$$

Verbandshomomorphismen Seien $(L, \vee, \wedge)$ und $(K, \sqcup, \sqcap)$ zwei Verbände. Eine Funktion $f : L \to K$ heißt ***Verbandshomomorphismus***, wenn f Suprema und Infima erhält.

$$f(a \vee b) = f(a) \sqcup f(b) \qquad f(a \wedge b) = f(a) \sqcap f(b)$$

Jeder Verbands- ist auch ein Ordnungshomomorphismus, sprich eine monotone Funktion; die Umkehrung gilt nur abgeschwächt (Aufgabe B.4.12 fragt nach einem Beweis).

$$f(a) \sqcup f(b) \sqsubseteq f(a \vee b) \iff f \text{ monoton} \iff f(a \wedge b) \sqsubseteq f(a) \sqcap f(b) \tag{B.26a}$$
$$f(a) \uparrow f(b) = f(a \uparrow b) \iff f \text{ monoton} \iff f(a \downarrow b) = f(a) \downarrow f(b) \tag{B.26b}$$

Axiome der Booleschen Verbände:

(Supremum)	$a_1 \sqcup a_2 \leqslant b$	$\iff$	$a_1 \leqslant b \ \wedge \ a_2 \leqslant b$
(Infimum)	$a \leqslant b_1 \ \wedge \ a \leqslant b_2$	$\iff$	$a \leqslant b_1 \sqcap b_2$
(kleinstes Element)	$\bot \leqslant b$	$\iff$	*true*
(größtes Element)	*true*	$\iff$	$a \leqslant \top$
(Komplement)	$a \sqcap p \leqslant b$	$\iff$	$a \leqslant b \sqcup p'$
(Komplement')	$a \sqcap p' \leqslant b$	$\iff$	$a \leqslant b \sqcup p$

Das Axiom (Komplement') folgt aus den übrigen Axiomen; gleiches gilt für (Komplement). Folgende Axiompaare sind jeweils dual zueinander: (Supremum) zu (Infimum), (kleinstes Element) zu (größtes Element) und (Komplement) zu (Komplement').

Folgerungen aus den Axiomen:

(obere Schranke)	$a_1 \leqslant a_1 \sqcup a_2$		$a_2 \leqslant a_1 \sqcup a_2$	
(untere Schranke)	$b_1 \sqcap b_2 \leqslant b_1$		$b_1 \sqcap b_2 \leqslant b_2$	(B.28a)
(Monotonie)	$a_1 \leqslant b_1 \ \wedge \ a_2 \leqslant b_2$	$\Longrightarrow$	$a_1 \sqcup a_2 \leqslant b_1 \sqcup b_2$	
(Monotonie)	$a_1 \leqslant b_1 \ \wedge \ a_2 \leqslant b_2$	$\Longrightarrow$	$a_1 \sqcap a_2 \leqslant b_1 \sqcap b_2$	(B.28b)
(Komplementärgesetze)	$p' \sqcap p \leqslant \bot$		$\top \leqslant p \sqcup p'$	
(Antitonie)	$a \leqslant b$	$\Longrightarrow$	$b' \leqslant a'$	

Abbildung B.7.: Axiome der Booleschen Verbände und Folgerungen aus den Axiomen.

Zum Beispiel folgen aus (B.26b) die Distributivgesetze $(a \uparrow b) + c = (a + c) \uparrow (b + c)$ und $(a \downarrow b) + c = (a + c) \downarrow (b + c)$, da $f(x) = x + c$ monoton ist (sogar eine Ordnungseinbettung).

Übungen.

10. Zeige mit Hilfe indirekter Beweise, dass Assoziativität und Idempotenz des Supremums aus (B.22) folgt.

11. Zeige die folgenden Eigenschaften des Maximums und des Mininums.

$$x \leqslant a \uparrow b \iff x \leqslant a \ \vee \ x \leqslant b \qquad \text{(B.27a)}$$

$$a \downarrow b \leqslant x \iff a \leqslant x \ \vee \ b \leqslant x \qquad \text{(B.27b)}$$

12. Zeige (B.26a) und (B.26b).

13. In einem Verband gelten nicht notwendigerweise die Distributivgesetze:

$$(a \sqcap b) \sqcup x = (a \sqcup x) \sqcap (b \sqcup x) \qquad (a \sqcup b) \sqcap x = (a \sqcap x) \sqcup (b \sqcap x)$$

Zeige, dass von den fünf 5-elementigen Verbänden nur der Diamant ($\mathbf{M}_3$) und das Pentagon ($\mathbf{N}_5$) die Distributivgesetze *nicht* erfüllen.

B.4.3. Boolesche Verbände⋆

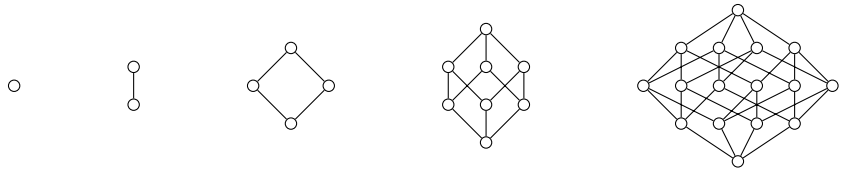
Sei L ein Verband und $p \in \mathrm{L}$. Das Element p besitzt genau dann ein ***Komplement*** p', wenn für alle $a, b \in \mathrm{L}$ gilt:

$$\text{(Komplement)} \qquad a \sqcap p \leqslant b \iff a \leqslant b \sqcup p' \tag{B.29a}$$

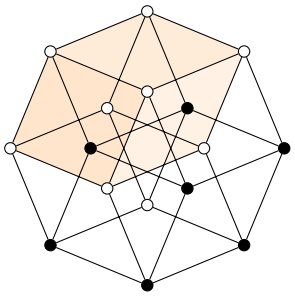
$$\text{(Komplement')} \qquad a \sqcap p' \leqslant b \iff a \leqslant b \sqcup p \tag{B.29b}$$

Ein Verband mit einem kleinsten und einem größten Element, $\bot$ und $\top$, heißt ***Boolescher Verband***, wenn jedes Element ein (notwendigerweise eindeutiges) Komplement besitzt. *Beachte:* Der Apostroph ist ein Postfix-Operator, kein Namensbestandteil.

Die Anforderungen an Boolesche Verbände sind hoch und diese damit sehr rar. Man kann zeigen, dass jeder *endliche* Boolesche Verband isomorph zu einem Potenzmengenverband ist. Die unten aufgeführten Diagramme zeigen die fünf kleinsten Booleschen Verbände, die Potenzmengenverbände über einer n-elementigen Grundmenge ($0 \leqslant n \leqslant 4$).



Im Würfel liegen die komplementären Elemente jeweils an den gegenüberliegenden Ecken, die durch Pfade der Länge drei miteinander verbunden sind. Der jeweils nächst größere Verband enthält zwei gegeneinander versetzte Kopien des vorangegangenen Diagramms: Aus einem Punkt wird so eine Linie, aus einer Linie ein Quadrat, aus einem Quadrat ein Würfel und aus einem Würfel ein ***Tesserakt***, ein 4-dimensionaler ***Hyperwürfel***. Positioniert man die Knoten im letzten Hassediagramm etwas anders, wird der 4-dimensionale Raum greifbarer — sehen Sie die beiden Würfel?



Komplementäre Elemente lassen sich in dieser Darstellung leicht ausmachen: Das Komplement eines Elements auf dem »äußeren Kreis« liegt auf der genau gegenüberliegenden Seite, verbunden durch einen Pfad der Länge vier. Entsprechendes gilt für Elemente auf dem »inneren Kreis«.

Wenden wir uns dem Beweisen zu. Aus der Definition des Komplements (B.29a) folgen die Komplementärgesetze der Booleschen Algebra.

$$\text{(Komplementärgesetze)} \qquad p' \sqcap p \leqslant \bot \qquad\qquad \top \leqslant p \sqcup p' \tag{B.30}$$

Die linke Ungleichung erhalten wir, wenn wir in (B.29a) a durch p' und b durch $\bot$ ersetzen; die rechte, wenn wir a durch $\top$ und b durch p ersetzen. (Beachte, dass $a \leqslant \bot$ äquivalent zu $a = \bot$ ist und $\top \leqslant b$ zu $\top = b$ — warum?)

In einem Verband regeln die Adjunktivgesetze bzw. das Verbindungslemma das Zusammenspiel von Supremum und Infimum. In einem Booleschen Verband gelten sogar die Distributivgesetze, wie die folgenden indirekten Beweise zeigen.

$$
\begin{array}{ll}
 & (a \sqcup b) \sqcap c \leqslant x \\
\iff & \quad \{ \text{ Komplement (B.29a) } \} \\
 & a \sqcup b \leqslant x \sqcup c' \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
 & a \leqslant x \sqcup c' \ \wedge \ b \leqslant x \sqcup c' \\
\iff & \quad \{ \text{ Komplement (B.29a) } \} \\
 & a \sqcap c \leqslant x \ \wedge \ b \sqcap c \leqslant x \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
 & (a \sqcap c) \sqcup (b \sqcap c) \leqslant x
\end{array}
\qquad
\begin{array}{ll}
 & x \leqslant (a \sqcap b) \sqcup c \\
\iff & \quad \{ \text{ Komplement' (B.29b) } \} \\
 & x \sqcap c' \leqslant a \sqcap b \\
\iff & \quad \{ \text{ Infimum (B.23) } \} \\
 & x \sqcap c' \leqslant a \ \wedge \ x \sqcap c' \leqslant b \\
\iff & \quad \{ \text{ Komplement' (B.29b) } \} \\
 & x \leqslant a \sqcup c \ \wedge \ x \leqslant b \sqcup c \\
\iff & \quad \{ \text{ Infimum (B.23) } \} \\
 & x \leqslant (a \sqcup c) \sqcap (b \sqcup c)
\end{array}
$$

Der linke Beweis ist dual zum rechten Beweis.

Die Umkehrung gilt ebenfalls: Aus dem Distributivgesetz und den Komplementärgesetzen folgen (B.29a) und (B.29b). Wir zeigen (B.29a) mit einem Ping-Pong Beweis.

Wir nehmen an, dass $a \leqslant b \sqcup p'$ gilt, und zeigen $a \sqcap p \leqslant b$.

$$
\begin{array}{ll}
 & a \sqcap p \\
\leqslant & \quad \{ \text{ Annahme u. Monotonie (B.28b) } \} \\
 & (b \sqcup p') \sqcap p \\
\leqslant & \quad \{ \text{ Distributivität } \} \\
 & (b \sqcap p) \sqcup (p' \sqcap p) \\
\leqslant & \quad \{ \text{ Komplementärgesetz (B.30) } \} \\
 & (b \sqcap p) \sqcup \bot \\
\leqslant & \quad \{ \ \bot \text{ neutrales Element } \} \\
 & b \sqcap p \\
\leqslant & \quad \{ \text{ untere Schranke (B.28a) } \} \\
 & b
\end{array}
$$

Wir nehmen an, dass $a \sqcap p \leqslant b$ gilt, und zeigen $a \leqslant b \sqcup p'$.

$$
\begin{array}{ll}
 & a \\
\leqslant & \quad \{ \text{ obere Schranke (B.24a) } \} \\
 & a \sqcup p' \\
\leqslant & \quad \{ \ \top \text{ neutrales Element } \} \\
 & (a \sqcup p') \sqcap \top \\
\leqslant & \quad \{ \text{ Komplementärgesetz (B.30) } \} \\
 & (a \sqcup p') \sqcap (p \sqcup p') \\
\leqslant & \quad \{ \text{ Distributivität } \} \\
 & (a \sqcap p) \sqcup p' \\
\leqslant & \quad \{ \text{ Annahme u. Monotonie (B.24b) } \} \\
 & b \sqcup p'
\end{array}
$$

Wiederum ist der linke Beweis dual zum rechten Beweis, der am besten von unten nach oben gelesen wird.

Das Komplement lässt sich sowohl ordnungstheoretisch als auch algebraisch definieren.

(Komplement) $\iff$ (Distributivität) $\wedge$ (Komplementärgesetze)

Summa summarum folgen aus den Gesetzen der Booleschen Verbände die Axiome der Booleschen Algebra und umgekehrt. Boolesche Algebren und Boolesche Verbände definieren die gleiche mathematische Struktur, einmal aus algebraischer und einmal aus ordnungstheoretischer Sicht. Beide Perspektiven sind erhellend und hilfreich. So erklärt zum Beispiel die ordnungstheoretische Sicht die Adjunktivgesetze: $\sqcup$ induziert die Ordnung $\leqslant$ und $\sqcap$ die duale Ordnung $\geqslant$.

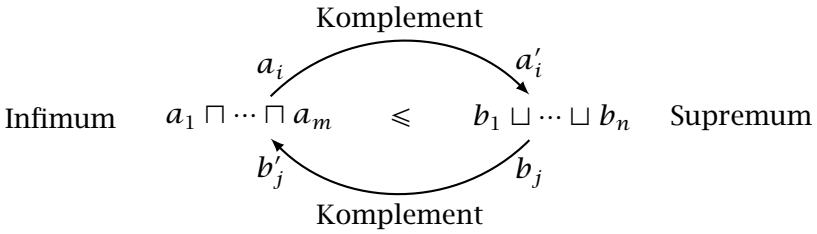
(Boolesche Algebra) $\iff$ (Boolescher Verband)

Abbildung B.7 fasst die Axiome Boolescher Verbände zusammen. Es sei noch einmal an das ***Dualitätsprinzip*** erinnert: Durch systematisches Ersetzen, $\leqslant \leftrightarrow \geqslant$, $\bot \leftrightarrow \top$ und $\sqcup \leftrightarrow \sqcap$, erhält man zu einer Formel die *duale* Formel. In einem Verband ist eine Formel genau dann wahr, wenn die duale Formel wahr ist.

Rechnen mit dem Komplement Schauen wir uns zum Schluss an, wie die Axiome für das Komplement systematisch in Beweisen verwendet werden. Wir halten zunächst fest, dass in einem Verband mit einem kleinsten und einem größten Element jede *endliche* Teilmenge eine kleinste obere und eine größte untere Schranke hat.

$$\bigsqcap\{a_1,\dots,a_m\} = a_1 \sqcap \dots \sqcap a_m \qquad \bigsqcup\{b_1,\dots,b_n\} = b_1 \sqcup \dots \sqcup b_n$$

Ist $m = 0$, dann gilt vereinbarungsgemäß $a_1 \sqcap \dots \sqcap a_m = \top$; ist $n = 0$, entsprechend $b_1 \sqcup \dots \sqcup b_n = \bot$. Die Axiome (B.29a) und (B.29b) erlauben es, in einer Formel der folgenden Form[9] Elemente von der einen auf die andere Seite zu transferieren.



Beim Transfer kommt entweder ein »Strich« hinzu oder ein »Strich« wird entfernt. Aus den Axiomen folgt, dass das Komplement eine antitone Ordnungseinbettung ist.

(Antitonie) $$a \leqslant b \iff a' \geqslant b' \tag{B.31}$$

Wir zeigen die Aussage, indem wir a und b auf die jeweils andere Seite transferieren.

$$\begin{aligned}
& a \leqslant b \\
\iff & \quad \{\ \top \text{ neutrales Element } \} \\
& \top \sqcap a \leqslant b \\
\iff & \quad \{\ \text{Komplement (B.29a)}\ \} \\
& \top \leqslant b \sqcup a' \\
\iff & \quad \{\ \sqcup \text{ kommutativ } \} \\
& \top \leqslant a' \sqcup b \\
\iff & \quad \{\ \text{Komplement' (B.29b)}\ \} \\
& \top \sqcap b' \leqslant a' \\
\iff & \quad \{\ \top \text{ neutrales Element } \} \\
& b' \leqslant a'
\end{aligned}$$

Man sieht, wir mischen ordnungstheoretische und algebraische Eigenschaften. (Wenn man etwas Erfahrung beim Beweisen gewonnen hat, lässt man Schritte, die Assoziativität, Kommutativität oder Neutralität verwenden, typischerweise aus.)

Die Folgerungen aus den Axiomen der Booleschen Algebra, siehe Abbildung B.2, lassen sich nach diesen Vorüberlegungen leicht mittels indirekter Beweise zeigen. Zunächst einmal ist $\top$ das Komplement von $\bot$ und umgekehrt: $\bot' = \top$ und $\top' = \bot$.

$$\begin{aligned}
& \bot' \leqslant x \\
\iff & \quad \{\ \text{Komplement' (B.29b)}\ \} \\
& \top \leqslant x \sqcup \bot \\
\iff & \quad \{\ \bot \text{ neutrales Element } \} \\
& \top \leqslant x
\end{aligned}
\qquad\qquad
\begin{aligned}
& x \leqslant \top' \\
\iff & \quad \{\ \text{Komplement (B.29a)}\ \} \\
& x \sqcap \top \leqslant \bot \\
\iff & \quad \{\ \top \text{ neutrales Element } \} \\
& x \leqslant \bot
\end{aligned}$$

[9] In der Logik heißt eine Formel der Form $a_1 \wedge \dots \wedge a_m \Longrightarrow b_1 \vee \dots \vee b_n$ auch ***Klausel***.

Die Beweise sind dual zueinander—aufgrund des Dualitätsprinzips muss tatsächlich nur einer geführt werden.

Das Komplement ist eine sogenannte ***Involution***. Wird die Operation zweimal in Folge angewendet, so erhält man das ursprüngliche Element: $a'' = a$.

$$\begin{aligned} & a'' \leqslant x \\ \iff & \quad \{ \text{ Komplement' (B.29b) } \} \\ & \top \leqslant x \sqcup a' \\ \iff & \quad \{ \text{ Komplement (B.29a) } \} \\ & a \leqslant x \end{aligned}$$

Schließlich gelten die ***De Morganschen Gesetze***: $(a \sqcup b)' = a' \sqcap b'$ und $(a \sqcap b)' = a' \sqcup b'$.

$$\begin{aligned} & (a \sqcup b)' \leqslant x \\ \iff & \quad \{ \text{ Komplement' (B.29b) } \} \\ & \top \leqslant x \sqcup a \sqcup b \\ \iff & \quad \{ \text{ Komplement' (B.29b) } \} \\ & a' \leqslant x \sqcup b \\ \iff & \quad \{ \text{ Komplement' (B.29b) } \} \\ & a' \sqcap b' \leqslant x \end{aligned} \qquad \begin{aligned} & x \leqslant (a \sqcap b)' \\ \iff & \quad \{ \text{ Komplement (B.29a) } \} \\ & x \sqcap a \sqcap b \leqslant \bot \\ \iff & \quad \{ \text{ Komplement (B.29a) } \} \\ & x \sqcap b \leqslant a' \\ \iff & \quad \{ \text{ Komplement (B.29a) } \} \\ & x \leqslant a' \sqcup b' \end{aligned}$$

Zuerst wird $a \sqcup b$ auf die rechte Seite transportiert; dann nacheinander a und b auf die linke. Die Beweise sind wiederum dual zueinander.

Übungen.

14. Sei L ein Verband. Zwei Elemente $a \in \mathrm{L}$ und $b \in \mathrm{L}$ heißen ***komplementär***, wenn $a \sqcap b = \bot$ und $\top = a \sqcup b$. Zeigen Sie, dass in einem *distributiven* Verband jedes Element ein *eindeutiges* Komplement besitzt. Finden Sie Beispiele für nicht eindeutige Komplemente in nicht distributiven Verbänden.

15. Aufgabe B.4.14 hat gezeigt, dass in einem distributiven Verband komplementäre Elemente eindeutig sind. Diese Eigenschaft lässt sich wie folgt formalisieren.

$$a' = b \quad \iff \quad a \sqcap b = \bot \ \wedge \ a \sqcup b = \top$$

Von links nach rechts gelesen besagt die Äquivalenz, dass a' das Komplement von b ist. Die umgekehrte Richtung formalisiert die Eindeutigkeit. Verwenden Sie diese Eigenschaft, um die Dualitätsgesetze, Involution und die De Morganschen Gesetze zu zeigen.

16. Zeigen Sie, dass das Axiom (B.29b) aus den übrigen Axiomen der Booleschen Verbände folgt. *Hinweis:* Folgern Sie zunächst, dass das Komplement eine Involution ist: $x = x''$.

B.4.4. Vollständige Verbände ⋆

Um zu zeigen, dass eine Ordnung P ein vollständiger Verband ist, muss man gemäß Definition nachweisen, dass $\bigsqcup \mathrm{A}$ und $\bigsqcap \mathrm{B}$ für beliebige Teilmengen $\mathrm{A}, \mathrm{B} \subseteq \mathrm{P}$ existieren. Tatsächlich ist der Aufwand nur halb so groß: Wenn beliebige Suprema existieren, dann existieren auch alle Infima und umgekehrt. Es gilt:

$$\bigsqcup \mathrm{A} = \bigsqcap \mathrm{A}^{upper} \qquad \text{mit } \mathrm{X}^{upper} = \{ u \in \mathrm{P} \mid \forall x \in \mathrm{X} \,.\, x \leqslant u \} \tag{B.32a}$$

$$\bigsqcap \mathrm{B} = \bigsqcup \mathrm{B}^{lower} \qquad \text{mit } \mathrm{X}^{lower} = \{ \ell \in \mathrm{P} \mid \forall x \in \mathrm{X} \,.\, \ell \leqslant x \} \tag{B.32b}$$

Die Menge A^{upper} enthält alle oberen Schranken von A; wir behaupten, dass $\bigsqcap A^{upper}$ die *kleinste* obere Schranke von A ist. Dazu zeigen wir zunächst, dass $\bigsqcap A^{upper}$ selbst eine obere Schranke ist: $\bigsqcap A^{upper} \in A^{upper}$.

$$
\begin{array}{ll}
 & \bigsqcap A^{upper} \in A^{upper} \\
\iff & \quad \{ \text{ Definition von } X^{upper} \text{ (B.32a) } \} \\
 & \forall a \in A \;.\; a \leqslant \bigsqcap A^{upper} \\
\iff & \quad \{ \text{ größte untere Schranke (B.19) } \} \\
 & \forall a \in A \;.\; \forall u \in A^{upper} \;.\; a \leqslant u \\
\iff & \quad \{ \text{ Definition von } X^{upper} \text{ (B.32a) } \} \\
 & \forall a \in A \;.\; \forall u \in P \;.\; (\forall a' \in A \;.\; a' \leqslant u) \implies a \leqslant u
\end{array}
$$

Die letzte Aussage folgt aus den Gesetzen der Prädikatenlogik. Im zweiten Schritt zeigen wir, dass $\bigsqcap A^{upper}$ die Eigenschaft des Supremums (B.18) erfüllt.

$$
\begin{array}{ll}
 & \bigsqcap A^{upper} \leqslant b \\
\implies & \quad \{ \bigsqcap A^{upper} \in A^{upper} \iff \forall a \in A \;.\; a \leqslant \bigsqcap A^{upper} \text{ und Transitivität } \} \\
 & \forall a \in A \;.\; a \leqslant b \\
\iff & \quad \{ \text{ Definition von } X^{upper} \text{ (B.32a) } \} \\
 & b \in A^{upper} \\
\implies & \quad \{ \text{ untere Schranke, siehe (B.28a) } \} \\
 & \bigsqcap A^{upper} \leqslant b
\end{array}
$$

Damit ist $\bigsqcap A^{upper}$ die *kleinste* der oberen Schranken.

Das obige Resultat hat nicht nur eine »ökonomische« Bedeutung durch Halbierung der Beweislast. In konkreten Anwendungen findet man häufig eine asymmetrische Situation vor: Eine der Schranken lässt sich leicht definieren, die andere nicht. In diesem Fall springt einem das obige Resultat zur Seite: Man begnügt sich mit der formalen Definition der einfacheren Variante und leitet die andere aus (B.32a) bzw. (B.32b) ab.

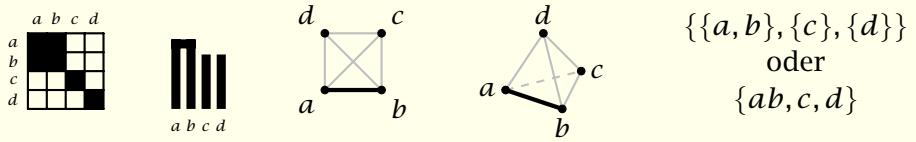
Zum Beispiel bildet die Menge aller Äquivalenzrelationen $(Eq(U), \subseteq)$ über einer Grundmenge U einen ***vollständigen Verband***. Dabei sind die Relationen gemäß der Teilmengenbeziehung angeordnet, siehe Abbildungen B.8 und B.9. Das Infimum ist durch den mengentheoretischen Durchschnitt gegeben: Sei I eine beliebige Indexmenge und $\equiv_i$ für jedes $i \in I$ eine Äquivalenzrelation. Dann ist $\equiv$ mit

$$a \equiv b \quad :\iff \quad \forall\, i \in I \;.\; a \equiv_i b \tag{B.33}$$

ebenfalls eine Äquivalenzrelation. (Überzeugen Sie sich, dass $\equiv$ der Durchschnitt aller $\equiv_i$ ist.) Dazu müssen wir zeigen, dass $\equiv$ reflexiv und symmetrisch,

$$
\begin{array}{ll}
 & a \equiv a \\
\iff & \quad \{ \text{ Definition } \equiv \text{ (B.33) } \} \\
 & \forall\, i \in I \;.\; a \equiv_i a \\
\iff & \quad \{ \equiv_i \text{ ist reflexiv } \} \\
 & \forall\, i \in I \;.\; \mathit{true} \\
\iff & \quad \{ \text{ Logik } \} \\
 & \mathit{true}
\end{array}
\qquad
\begin{array}{ll}
 & a \equiv b \\
\iff & \quad \{ \text{ Definition } \equiv \text{ (B.33) } \} \\
 & \forall\, i \in I \;.\; a \equiv_i b \\
\iff & \quad \{ \equiv_i \text{ ist symmetrisch } \} \\
 & \forall\, i \in I \;.\; b \equiv_i a \\
\iff & \quad \{ \text{ Definition } \equiv \text{ (B.33) } \} \\
 & b \equiv a
\end{array}
$$

Äquivalenzrelationen lassen sich ganz unterschiedlich darstellen, als Tabellen\Matrizen, als ungerichtete Graphen oder als Partitionen. Die Relation $a \equiv a$, $a \equiv b$, $b \equiv a$, $b \equiv b$, $c \equiv c$, $d \equiv d$ über der Grundmenge $\{a, b, c, d\}$ kann zum Beispiel wie folgt repräsentiert werden.



$\{\{a, b\}, \{c\}, \{d\}\}$
oder
$\{ab, c, d\}$

Jede Darstellung betont unterschiedliche Aspekte und hat so ihre eigenen, spezifischen Stärken und Schwächen. Die Repräsentation als Tabelle\Matrix spiegelt sehr direkt die definierenden Eigenschaften einer Äquivalenzrelation wider: Reflexivität (die Einträge in der Hauptdiagonalen sind gesetzt), Symmetrie (die Tabelle ist spiegelsymmetrisch an der Hauptdiagonalen), Transitivität (werden Zeilen und Spalten so permutiert, dass äquivalente Elemente benachbart sind, füllen diese ein Quadrat).

Der ***Graph*** einer Relation visualisiert die Beziehungen: Zwei Elemente sind äquivalent, wenn die entsprechenden Knoten durch eine Kante verbunden sind. Das Zeichnen von Graphen ist eine Kunst; die »Lesbarkeit« hängt essentiell von der Platzierung der Knoten ab. Für unser Minibeispiel mit vier Elementen bieten sich drei Varianten an: 1-dimensional (als nebeneinander platzierte, vertikale Balken), 2-dimensional (als Ecken eines Quadrats) oder 3-dimensional (als Ecken eines Tetraeders).

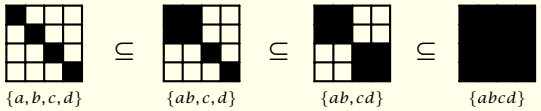
Am kompaktesten ist die Darstellung einer Äquivalenzrelation als ***Partition***. Eine Partition unterteilt eine Grundmenge U in nichtleere, paarweise disjunkte Teilmengen, deren Vereinigung wieder die Grundmenge ergibt. Eine k-Partition enthält genau k Teilmengen oder ***Klassen***. Die von einer Äquivalenzrelation $\mathrm{R} \subseteq \mathrm{U} \times \mathrm{U}$ abgeleiteten Teilmengen heißen ***Äquivalenzklassen***; die Menge aller Äquivalenzklassen ergibt die Partition $\{\, \mathrm{R}(a) \mid a \in \mathrm{U} \,\}$ mit $\mathrm{R}(a) = \{\, b \in \mathrm{U} \mid a \,\mathrm{R}\, b \,\}$. Eine vierelementige Grundmenge lässt sich auf 15 Weisen partitionieren; wir erhalten eine 4-Partition, sechs 3-Partitionen, sieben 2-Partitionen und eine 1-Partition (ab kürzt $\{a, b\}$ ab etc.):

$$\{a,b,c,d\},\ \{ab,c,d\},\ \{ac,b,d\},\ \{ad,b,c\},\ \{a,c,d\},\ \{a,d,c\},\ \{a,b,cd\},$$
$$\{abc,d\},\ \{abd,c\},\ \{acd,b\},\ \{bcd,a\},\ \{ab,cd\},\ \{ac,bd\},\ \{ad,bc\},\ \{abcd\}$$

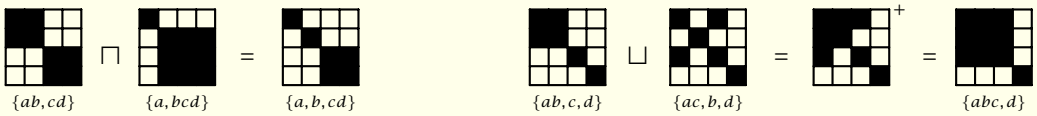
Die Partitionen über einer Grundmenge U lassen sich nach dem »Grad der Diskriminierung« anordnen: im obigen Beispiel ist $\{\{a\}, \{b\}, \{c\}, \{d\}\}$ die *feinste* Partition, alle Elemente werden unterschieden; $\{\{a, b, c, d\}\}$ ist die *gröbste* Partition, es gibt keine Unterschiede (»all men are created equal«). Die Anordnung lässt sich am einfachsten nachvollziehen, wenn wir zur Tabellendarstellung zurückkehren. Aus der Partition $\mathcal{P} \subseteq \mathcal{P}(\mathrm{U})$ erhält man die Äquivalenzrelation $a \,\mathrm{R}\, b \;:\Longleftrightarrow\; \exists\, \mathrm{P} \in \mathcal{P} \,.\, a \in \mathrm{P} \wedge b \in \mathrm{P}$ — zwei Elemente sind äquivalent, wenn sie in der gleichen Teilmenge enthalten sind. Jeder Partition wird so umkehrbar eindeutig eine Äquivalenzrelation zugeordnet — Äquivalenzrelationen und Partitionen stehen in Eins-zu-eins-Korrespondenz.

Abbildung B.8.: Äquivalenzrelationen, Partitionen und etwas Kombinatorik (Teil 1).

Da eine Relation eine Menge von Paaren ist, lassen sich Relationen, insbesondere Äquivalenzrelationen, mit der Teilmengenbeziehung anordnen.

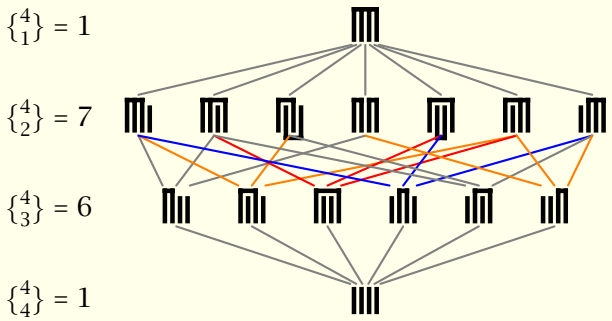


Je kleiner eine Äquivalenzrelation, desto feinere Unterscheidungen trifft sie; je größer, desto gröber. Die Menge aller Äquivalenzrelationen über einer Grundmenge bildet einen ***vollständigen Verband***. Da der Durchschnitt die definierenden Eigenschaften einer Äquivalenzrelation erhält, ist das Infimum durch den mengentheoretischen Durchschnitt gegeben, $R \sqcap S := R \cap S$. Für die Vereinigung gilt dies nicht:



Da die Vereinigung von Relationen nur Reflexivität und Symmetrie erhält, ist das Supremum die ***transitive Hülle*** der Vereinigung, $R \sqcup S := (R \cup S)^+$ (siehe Abschnitt B.6.4).

Die fünfzehn Partitonen einer 4-elementigen Menge werden wie folgt angeordnet.



$$\left\{ {0 \atop k} \right\} = [k = 0]$$

$$\left\{ {n+1 \atop k} \right\} = k \cdot \left\{ {n \atop k} \right\} + \left\{ {n \atop k-1} \right\}$$

$$B_0 = 1$$

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \cdot B_k$$

Die k-te Ebene von oben enthält alle k-Partitionen — k-Partitionen sind unvergleichbar. (Warum?) Aus einer k-Partition erhält man eine $(k+1)$-Partition, indem eine Klasse in zwei Klassen aufgetrennt wird; werden umgekehrt zwei Klassen zu einer Klasse vereinigt, entsteht aus einer $(k+1)$-Partition eine k-Partition.

Etwas Kombinatorik gefällig? Die ***Stirling-Zahl zweiter Art*** $\left\{ {n \atop k} \right\}$ gibt die Zahl der k-Partitionen einer n-elementigen Menge an. Für $n = 0$ gibt es nur die leere Partition. Um $n+1$ Elemente auf k Klassen zu verteilen, gibt es zwei Möglichkeiten: (1) n Elemente werden in k Klassen aufgeteilt und das restliche Element zu einer dieser Klassen hinzugefügt; oder (2) n Elemente werden in $k-1$ Klassen aufgeteilt, das restliche Element bildet eine eigene Klasse. Dieses Verfahren führt zur obigen Rekursionsformel.

Die ***Bellzahl*** $B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}$ gibt die Zahl aller Partitionen einer n-elementigen Menge an. Die obige Rekursionsformel erschließt sich mit einem kombinatorischen Argument: Für jedes k gibt es $\binom{n}{k} = \binom{n}{n-k}$ Möglichkeiten für die Auswahl einer k-elementigen Menge und B_{n-k} Möglichkeiten für die Partitionierung der Restmenge. Die Folge der Bellzahlen, $1, 1, 2, 5, 15, 52, 203, 877, 4140, \ldots$, ist als A000110 in OEIS aufgeführt.

Abbildung B.9.: Äquivalenzrelationen, Partitionen und etwas Kombinatorik (Teil 2).

und transitiv ist:

$$
\begin{aligned}
& a \equiv b \ \wedge \ b \equiv c \\
\iff & \quad \{ \text{ Definition } \equiv \text{ (B.33) } \} \\
& (\forall\, i \in \mathrm{I} \,.\, a \equiv_i b) \ \wedge \ (\forall\, i \in \mathrm{I} \,.\, b \equiv_i c) \\
\iff & \quad \{ \text{ Logik } \} \\
& \forall\, i \in \mathrm{I} \,.\, a \equiv_i b \ \wedge \ b \equiv_i c \\
\iff & \quad \{ \equiv_i \text{ ist transitiv } \} \\
& \forall\, i \in \mathrm{I} \,.\, a \equiv_i c \\
\iff & \quad \{ \text{ Definition } \equiv \text{ (B.33) } \} \\
& a \equiv c
\end{aligned}
$$

Während das Infimum durch den Durchschnitt gegeben ist, entspricht das Supremum *nicht* der mengentheoretischen Vereinigung, da die Transitivität nicht erhalten wird, siehe Abbildung B.9.

Übungen.

17. Bildet die Menge aller Quasiordnungen ebenfalls einen vollständigen Verband? Und die Menge aller Ordnungen?

B.5. Arithmetik

Zählen und messen — ausgehend von diesen konkreten Anwendungen der natürlichen Zahlen entstanden im Laufe der Jahrhunderte immer größere Zahlenbereiche. Einige kennen Sie wahrscheinlich aus der Schulmathematik, andere vielleicht aus (begleitenden) Mathematikvorlesungen.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$$

Eine beeindruckende Hierarchie mit bewegter Geschichte: $\mathbb{N}$ für *n*atürliche Zahlen, $\mathbb{Z}$ für ganze *Z*ahlen, $\mathbb{Q}$ für Bruchzahlen oder *Q*uotienten (eingeführt von Giuseppe Peano, ital. *q*uoziente), $\mathbb{R}$ für *r*eelle Zahlen (die Nomenklatur geht auf René Descartes zurück, der zwischen *reellen* und *imaginären* Zahlen unterschied — letzteres war durchaus verächtlich gemeint), $\mathbb{C}$ für komplexe Zahlen (lat. *c*omplexus), $\mathbb{H}$ für *H*amilton-Zahlen oder Quaternionen (benannt nach Sir William Rowan Hamilton) und $\mathbb{O}$ für *O*ktaven oder *O*ktonionen.

Mit der Rechenbrille auf der Nase erkennen wir eine scharfe Grenze, die zwischen den rationalen Zahlen $\mathbb{Q}$ und den reellen Zahlen $\mathbb{R}$ verläuft. Das mechanische Rechnen mit rationalen Zahlen gelingt in voller Schönheit: Jede rationale Zahl lässt sich geeignet repräsentieren, die arithmetischen Operationen können durch Rechenregeln eingefangen werden. Die reellen Zahlen lassen sich hingegen nur unvollkommen nachbilden, da sie zu zahlreich sind: Die Menge $\mathbb{R}$ ist überabzählbar. Man kann Kompromisse eingehen (Stichwort: Fließkommaarithmetik) oder sich mit den Grenzen der Berechenbarkeit arrangieren (Stichwort: berechenbare Zahlen, engl. computable reals). Wir machen uns das Leben leicht und konzentrieren uns im vorliegenden Skript auf das Machbare:

Abschnitt B.5.1 kehrt zu den Anfängen des Rechnens zurück, dem Rechnen mit natürlichen Zahlen. Ein besonderes Augenmerk richten wir auf die natürliche Subtraktion (Monus $\dot{-}$) und die natürliche Division. Abschnitt B.5.2 wendet sich den ganzen Zahlen zu, diskutiert Konversionsfunktionen (Boden $\lfloor \text{-} \rfloor$ und Decke $\lceil \text{-} \rceil$) und stellt verschiedene Erweiterungen der natürlichen Division vor. Wenn wir rechnen, dann arbeiten wir mit Zahlenrepräsentationen, mit konkreten

Darstellungen der abstrakten Größen. Zwei Zahlensysteme beleuchten wir genauer: Stellenwertsysteme in Abschnitt B.5.3 und Residuenzahlensysteme in Abschnitt B.5.5 — Abschnitt B.5.4 bereitet das Rechnen mit Resten mit einem kurzen Abstecher in die Zahlentheorie vor.

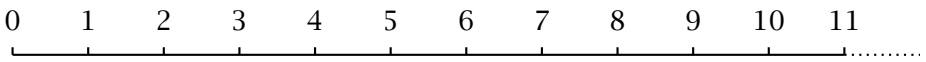
B.5.1. Rechnen mit natürlichen Zahlen

And the moral of the story is that we had better regard —
after all those centuries! — zero as a most natural number.
— Edsger W. Dijkstra (1930–2002), *Why numbering should start at zero — EWD831*

Am Anfang stand das Zählen: eine Kuh, zwei Kühe, drei Kühe. Seitdem Menschen Informationen schriftlich niederlegen, haben sie auch Zahlen notiert. Aus konkreten Vielfachheiten wurden im Laufe der Zeit abstrakte Größen, 1, 2, 3, mit denen man sich losgelöst von den konkreten Ursprüngen beschäftigt hat, die oder zumindest eine der Geburtsstunden der Mathematik. Die uns vertrauten Zahlzeichen 0123456789 sind übrigens indisch-arabischen Ursprungs. Zum Vergleich: In der indischen Schrift Devanagari lesen sich die Ziffern ०१२३४५६७८९ — die enge Verwandtschaft ist nicht zu übersehen.

So alt die Zahlen und das Rechnen, so vergleichsweise jung ist die auf Giuseppe Peano zurückgehende Präzisierung der grundlegenden Annahmen über das »Zählen«, siehe Abbildungen 3.6 und B.10. Was muss ich annehmen, welche Axiome postulieren, um daraus die liebgewonnenen Rechenoperationen und deren Eigenschaften präzise ableiten zu können? Nicht allzu viel, wie Abbildung B.10 zeigt. (Abschnitt B.3 hat sich ausführlich mit Peanos Induktionsaxiom beschäftigt; jetzt wenden wir uns den Rechenoperationen zu.) Peanos erste Formalisierung postulierte übrigens die 1 als erste natürliche Zahl. Eine unglückliche Wahl, die er später korrigierte — mit der 0 geht der Addition ihr neutrales Element verloren.

Zurück zu den Ursprüngen des Zählens. Man hat sicherlich auch gezählt, um zu vergleichen: Ich habe drei Kühe, du nur zwei. Mit anderen Worten, die natürlichen Zahlen lassen sich anordnen.



Peanos Axiomatisierung schweigt sich über diesen Aspekt aus, muss sich dazu aber auch nicht äußern, da die Ordnungsrelation auf die Addition zurückgeführt werden kann (siehe auch Abschnitt B.4.1).

$$a \leqslant b \text{ in } \mathbb{N} \iff \exists\, d \in \mathbb{N} \,.\, d + a = b \tag{B.34}$$

Die natürliche Zahl a ist kleiner als b, wenn man von a weiterzählend b erreicht. Auf diese Weise wird eine *totale* Ordnung definiert: $\leqslant$ ist reflexiv, transitiv, antisymmetrisch und total (siehe Abschnitt B.4.1; Übung B.5.1 fragt nach Beweisen).

Auf den natürlichen Zahlen besteht eine enge Beziehung zwischen der strikten Ordnung $<$ und der nicht strikten Ordnung $\leqslant$:

$$a < b \text{ in } \mathbb{N} \iff a + 1 \leqslant b \text{ in } \mathbb{N} \tag{B.35a}$$
$$a \leqslant b \text{ in } \mathbb{N} \iff a < b + 1 \text{ in } \mathbb{N} \tag{B.35b}$$

Da jede natürliche Zahl n eine nächstgrößere Zahl besitzt, ihren Nachfolger $n + 1$, lässt sich »$<$« auf »$\leqslant$« zurückführen und umgekehrt. Damit ist auch klar, dass die Beziehung *nicht* für die rationalen Zahlen gilt.

Auf den natürlichen Zahlen sind $\text{-} + p$ und $\text{-} \cdot p$ mit $p > 0$ Ordnungseinbettungen, sie erhalten und reflektieren die Ordnung.

$$a \leqslant b \text{ in } \mathbb{N} \iff a + p \leqslant b + p \text{ in } \mathbb{N} \tag{B.36a}$$
$$a \leqslant b \text{ in } \mathbb{N} \iff a \cdot p \leqslant b \cdot p \text{ in } \mathbb{N} \qquad \text{für alle } p > 0 \tag{B.36b}$$

Peanos ***Axiomensystem*** für die natürlichen Zahlen umfasst die folgenden fünf Axiome:

- $0 \in \mathbb{N}$
- $\forall\, n \in \mathbb{N}\ .\ s(n) \in \mathbb{N}$
- $\forall\, m \in \mathbb{N}\ .\ \forall\, n \in \mathbb{N}\ .\ s(m) = s(n) \implies m = n$
- $\forall\, n \in \mathbb{N}\ .\ 0 \neq s(n)$
- ***Induktionsaxiom***: für jede Menge $N \subseteq \mathbb{N}$ natürlicher Zahlen gilt:

$$0 \in N \ \wedge\ (\forall\, n \in \mathbb{N}\ .\ n \in N \implies s(n) \in N) \quad\implies\quad (\forall\, n \in \mathbb{N}\ .\ n \in N)$$

Die ersten beiden Axiome beschreiben, wie natürliche Zahlen gebildet werden: mit Hilfe der ***Konstruktoren*** 0 und s (engl. *s*uccessor). Die nächsten beiden Axiome legen die ***Gleichheit*** fest: Zwei natürliche Zahlen sind gleich, wenn sie mit 0 und s auf die gleiche Art gebildet werden. (Konstruktoren sind injektiv; verschiedene Konstruktoren konstruieren unterschiedliche Zahlen.) Das ***Induktionsaxiom*** formalisiert, dass jede natürliche Zahl mit Hilfe von 0 und s konstruiert werden kann. Die Annahmen sind übrigens die gleichen, die man für den rekursiven Variantentyp *Peano* aus Abschnitt 4.2.2 macht.

Operationen auf den natürlichen Zahlen wie Gleichheit, Ungleichheit, Addition, natürliche Subtraktion (»monus«) und Multiplikation können rekursiv definiert werden.

$$\begin{aligned} 0 = 0 &= \mathit{true} \\ 0 = s(n) &= \mathit{false} \\ s(m) = 0 &= \mathit{false} \\ s(m) = s(n) &= m = n \end{aligned}$$

$$\begin{aligned} 0 \leqslant n &= \mathit{true} \\ s(m) \leqslant 0 &= \mathit{false} \\ s(m) \leqslant s(n) &= m \leqslant n \end{aligned}$$

$$\begin{aligned} m < 0 &= \mathit{false} \\ 0 < s(n) &= \mathit{true} \\ s(m) < s(n) &= m < n \end{aligned}$$

$$\begin{aligned} 0 + n &= n \\ s(m) + n &= s(m + n) \end{aligned}$$

$$\begin{aligned} 0 \dot{-} n &= 0 \\ m \dot{-} 0 &= m \\ s(m) \dot{-} s(n) &= m \dot{-} n \end{aligned}$$

$$\begin{aligned} 0 * n &= 0 \\ s(m) * n &= (m * n) + n \end{aligned}$$

Existenz und Eindeutigkeit der so definierten Operationen weist man mit dem Induktionsaxiom nach. Dank der Möglichkeit des Musterabgleichs lassen sich alle Funktionen sehr direkt in Mini-F# programmieren. Eine kleine Auswahl:

```
type Peano =| Zero | Succ of Peano
let rec equ (m:Peano, n:Peano) : bool =
  match (m, n) with
    | (Zero,    Zero   ) → true
    | (Zero,    Succ n') → false
    | (Succ m', Zero   ) → false
    | (Succ m', Succ n') → equ (m', n')
let rec add (m:Peano, n:Peano) : Peano =
  match m with
    | Zero    → n
    | Succ m' → Succ (add (m', n))
```

Abbildung B.10.: Axiomensystem für die natürlichen Zahlen von Peano.

Aus der Schule sind wir gewohnt, mit den rationalen oder mit den reellen Zahlen zu rechnen. Bei Umformungen etwa beim Lösen von Gleichungen nutzen wir aus, dass elementare arithmetische Operationen wie Addition und Multiplikation Umkehroperationen besitzen (additive Inverse: Gegenzahl $-x$; multiplikative Inverse: Kehrwert $\frac{1}{x}$). So bequem gestaltet sich das Rechnen mit den natürlichen Zahlen nicht. Glücklicherweise ist nicht alles verloren: Im Folgenden wollen wir uns anschauen, wie wir »Quasi-Inverse« von Addition und Multiplikation auf den natürlichen Zahlen definieren können. Wir werden sehen, dass diese Quasi-Inverse viele Eigenschaften mit der reellen Subtraktion und Division gemeinsam haben — viele, aber eben nicht alle.

Natürliche Subtraktion Die folgende indirekte Definition führt für jede natürliche Zahl $p \in \mathbb{N}$ eine Quasi-Inverse von $\text{-} + p$ ein: die natürliche Subtraktion $\text{-} \dot{-} p$ (»monus«).[10] Für alle $a, b \in \mathbb{N}$ gilt:

$$a \dot{-} p \leqslant b \quad \Longleftrightarrow \quad a \leqslant b + p \qquad \text{(Minuend } \dot{-} \text{ Subtrahend = Differenz)} \tag{B.37}$$

Für konkrete Werte lässt sich $\dot{-}$ leicht ausrechnen: $7 \dot{-} 2$ ist die kleinste natürliche Zahl b, so dass $7 \leqslant b + 2$, also $7 \dot{-} 2 = 5$; entsprechend ist $2 \dot{-} 7$ ist die kleinste natürliche Zahl b, so dass $2 \leqslant b + 7$, also $2 \dot{-} 7 = 0$.

Setzen wir $b := a \dot{-} p$ in (B.37) ein, dann ist die linke Seite trivialerweise erfüllt und wir erhalten $a \leqslant (a \dot{-} p) + p$. Setzen wir umgekehrt $a := b + p$ ein, dann ist die rechte Seite trivialerweise erfüllt und wir erhalten $(b + p) \dot{-} p \leqslant b$. Da $\text{-} + p$ injektiv ist, gilt sogar $(b + p) \dot{-} p = b$. Versuchen Sie sich an einem Beweis. Wir zeigen die Aussage später in einem allgemeineren Kontext, siehe Abschnitt B.6.5.

$$a \leqslant (a \dot{-} p) + p \qquad\qquad (b + p) \dot{-} p = b \tag{B.38}$$

Die beiden Eigenschaften heißen auch Rechenregeln (engl. computation rules) oder ***Vereinfachungsregeln*** (engl. simplification rules), da sich mit ihrer Hilfe Ausdrücke vereinfachen lassen. Man sieht, monus ist fast, aber eben nur fast invers zu plus. Statt der Gleichheit $a = (a - p) + p$ in $\mathbb{Z}$, gilt in $\mathbb{N}$ im Allgemeinen nur die Abschätzung $a \leqslant (a \dot{-} p) + p$, zum Beispiel ist $2 < (2 \dot{-} 7) + 7 = 7$.

Aus der Definition (B.37) folgt unmittelbar, dass $a \dot{-} b \leqslant 0$ und somit $a \dot{-} b = 0$, wenn der Subtrahend b größer ist als der Minuend a, also $a \leqslant b$. Gilt umgekehrt $a \geqslant b$, dann kehrt die natürliche Subtraktion die Addition um: $(a \dot{-} b) + b = a$.

$$a \dot{-} b = 0 \quad \Longleftrightarrow \quad a \leqslant b \quad \Longleftrightarrow \quad (b \dot{-} a) + a = b \tag{B.39}$$

Die zweite Äquivalenz zeigen wir mit einem Ping-Pong Beweis. »$\Longleftarrow$«: Diese Richtung folgt direkt aus der Definition der Ordnung (B.34).[11] »$\Longrightarrow$«: Es gibt ein d mit $d + a = b$, daraus folgt:

$$\begin{aligned}
& (b \dot{-} a) + a \\
= \quad & \{ \text{ Annahme: } d + a = b \ \} \\
& ((d + a) \dot{-} a) + a \\
= \quad & \{ \text{ Vereinfachungsregel (B.38) } \} \\
& d + a \\
= \quad & \{ \text{ Annahme: } d + a = b \ \} \\
& b
\end{aligned}$$

[10] Wie immer bei indirekten Definitionen ist nicht unmittelbar klar, ob die eingeführte Funktion tatsächlich existiert. Wir ignorieren diesen wichtigen Aspekt für den Moment und greifen ihn erst später in Abschnitt B.5.2 wieder auf.

[11] Hier kommt eine Eigenschaft des Existenzquantors zum Tragen: Sei $\mathrm{P}(d) :\Longleftrightarrow d + a = b$, dann gilt $\mathrm{P}(b \dot{-} a) \Longrightarrow \exists\, d \,.\, \mathrm{P}(d)$. Die »Differenz« $b \dot{-} a$ ist sozusagen ein fleischgewordener Existenzquantor, ein konkreter Zeuge, dass ein d mit der gewünschten Eigenschaft existiert. In der Logik nennt man »$\dot{-}$« auch ***Skolemfunktion*** — da der Existenzquantor $\exists d$ im Geltungsbereich zweier Allquantoren steht, $\forall a$ und $\forall b$, wird aus d die zweistellige Funktion $b \dot{-} a$.

Vergleichen wir (B.39) mit dem Verbindungslemma (B.25), dann wird klar, dass $(b \dot{-} a) + a$ das Supremum der Zahlen a und b ist bzw. deren Maximum, da die Ordnung auf den natürlichen Zahlen total ist.

$$(a \dot{-} b) + b = a \uparrow b = (b \dot{-} a) + a \tag{B.40}$$

Kommen wir zu den ordnungstheoretischen und algebraischen Eigenschaften der natürlichen Subtraktion. Wie die ganzzahlige Subtraktion »–« ist auch die natürliche Subtraktion »$\dot{-}$« monoton im ersten Argument (Minuend) und antiton im zweiten (Subtrahend).

$$a_1 \leqslant a_2 \;\wedge\; b_1 \geqslant b_2 \quad\Longrightarrow\quad a_1 \dot{-} b_1 \leqslant a_2 \dot{-} b_2$$

Da »monus« durch eine indirekte Definition eingeführt worden ist, führen wir zum Nachweis der Monotonie einen indirekten Beweis.

$$\begin{aligned}
& a_1 \dot{-} b_1 \leqslant x \\
\Longleftrightarrow\quad & \{\ \text{Definition } \dot{-}\ (\text{B.37})\ \} \\
& a_1 \leqslant x + b_1 \\
\Longleftarrow\quad & \{\ \text{Annahme: } a_1 \leqslant a_2\ \} \\
& a_2 \leqslant x + b_1 \\
\Longleftarrow\quad & \{\ \text{Annahme: } b_1 \geqslant b_2 \text{ und Addition ist monoton}\ \} \\
& a_2 \leqslant x + b_2 \\
\Longleftrightarrow\quad & \{\ \text{Definition } \dot{-}\ (\text{B.37})\ \} \\
& a_2 \dot{-} b_2 \leqslant x
\end{aligned}$$

Der Beweis macht deutlich, dass die Antitonie im Subtrahenden aus der Monotonie der Addition folgt. Allgemein induzieren Eigenschaften von $+$ Eigenschaften von $\dot{-}$.

$$a \dot{-} 0 = a \tag{B.41a}$$
$$a \dot{-} (b + c) = (a \dot{-} c) \dot{-} b \tag{B.41b}$$
$$(a \dot{-} b) \dot{-} c = (a \dot{-} c) \dot{-} b \tag{B.41c}$$
$$(a + x) \dot{-} (b + x) = a \dot{-} b \tag{B.41d}$$

Erkennen Sie, welches Gesetz sich aus welcher Eigenschaft der Addition ergibt? Das erste Gesetz (B.41a) folgt aus der Tatsache, dass 0 das neutrale Element der Addition ist.

$$\begin{aligned}
& a \dot{-} 0 \leqslant x \\
\Longleftrightarrow\quad & \{\ \text{Definition } \dot{-}\ (\text{B.37})\ \} \\
& a \leqslant x + 0 \\
\Longleftrightarrow\quad & \{\ 0 \text{ neutrales Element der Addition}\ \} \\
& a \leqslant x
\end{aligned}$$

Das zweite Gesetz (B.41b) folgt aus der Assoziativität der Addition — beachte, dass die Reihen-

folge von b und c vertauscht wird.

$$
\begin{aligned}
& a \dot{-} (b + c) \leqslant x \\
\iff & \quad \{ \text{ Definition } \dot{-} \text{ (B.37) } \} \\
& a \leqslant x + (b + c) \\
\iff & \quad \{ \text{ Addition ist assoziativ } \} \\
& a \leqslant (x + b) + c \\
\iff & \quad \{ \text{ Definition } \dot{-} \text{ (B.37) } \} \\
& a \dot{-} c \leqslant x + b \\
\iff & \quad \{ \text{ Definition } \dot{-} \text{ (B.37) } \} \\
& (a \dot{-} c) \dot{-} b \leqslant x
\end{aligned}
$$

Die Reihenfolge, in der b und c abgezogen werden (B.41c), spielt keine Rolle, wenn + zusätzlich kommutativ ist — dies ist der Fall. Das vierte Gesetz (B.41d) ist eine direkte Folgerung aus (B.41b). (Übung B.5.3 fragt nach Beweisen für diese Behauptungen.)

Natürliche Division Wie die natürliche Subtraktion führen wir auch die natürliche Division mittels einer indirekten Definition[12] ein: Für jede natürliche Zahl $p \in \mathbb{N}$ mit $p > 0$ wird $\cdot$ ***div*** p als Quasi-Inverse von $\cdot \cdot p$ definiert. Für alle $a, b \in \mathbb{N}$ gilt:

$$a \cdot p \leqslant b \quad \iff \quad a \leqslant b \ \textbf{\textit{div}}\ p \qquad \text{(Dividend } \textbf{\textit{div}} \text{ Divisor = Quotient)} \tag{B.42}$$

Für konkrete Werte lässt sich ***div*** leicht ausrechnen: 7 ***div*** 3 ist die *größte* natürliche Zahl a, so dass $a \cdot 3 \leqslant 7$, also 7 ***div*** $3 = 2$. Warum schließen wir $p = 0$ aus? Nun, b ***div*** 0 wäre die größte Zahl a, so dass $a \cdot 0 \leqslant b$. Da letztere Ungleichung stets erfüllt ist, müsste a die größte natürliche Zahl sein — die natürliche Zahlen sind aber nach oben unbeschränkt.[13]

Da die natürliche Division ebenso wie die natürliche Subtraktion durch eine indirekte Definition eingeführt wird, können wir ein ähnliches Programm abspulen: Aus (B.42) leiten sich Vereinfachungsregeln ab, Eigenschaften der Multiplikation induzieren Eigenschaften der Division usw. Wir fassen uns hier etwas kürzer als im letzten Paragraphen und verbannen einige Beweise in Übungsaufgaben.

Aus der Definition (B.42) lassen sich zwei direkte Folgerungen ziehen, indem man eine der beiden Ungleichungen erfüllt: $b := a \cdot p$ oder $a := b$ ***div*** p. Da $\cdot \cdot p$ für $p > 0$ injektiv ist, lässt sich die resultierende Ungleichung $a \leqslant (a \cdot p)$ ***div*** p zu einer Gleichung verstärken. Wir erhalten die folgenden ***Vereinfachungsregeln***.

$$a = (a \cdot p) \ \textbf{\textit{div}}\ p \qquad\qquad (b \ \textbf{\textit{div}}\ p) \cdot p \leqslant b \tag{B.43}$$

Wenn man möchte, kann man die Eigenschaften auch als ***Kürzungsregeln*** auffassen. Aus (B.43) folgt unmittelbar, dass p ***div*** $p = 1$.

Ähnlich wie die natürliche Subtraktion ist die natürliche Division monoton im ersten Argument (Dividend) und antiton im zweiten (Divisor).

$$a_1 \leqslant a_2 \ \wedge \ b_1 \geqslant b_2 \quad \iff \quad a_1 \ \textbf{\textit{div}}\ b_1 \leqslant a_2 \ \textbf{\textit{div}}\ b_2 \tag{B.44}$$

[12] Auch an dieser Stelle kümmern wir uns nicht darum, ob die eingeführte Funktion existiert. Abschnitt B.5.2 holt das Versäumnis nach.

[13] Man könnte die natürlichen Zahlen um ein größtes Element erweitern: $\mathbb{N} \cup \{\infty\}$ mit $n \leqslant \infty$ für alle $n \in \mathbb{N}$. Dann gälte b ***div*** $0 = \infty$. Allerdings müsste man sich überlegen, wie man $0 \cdot \infty$, $1 \cdot \infty$, b ***div*** ∞ usw. definiert. Führen Sie das Gedankenexperiment weiter, wenn sie Lust haben.

Weiterhin induzieren Eigenschaften von »·« Eigenschaften von ***div***.

$$a \;\mathbf{div}\; 1 = a \tag{B.45a}$$
$$a \;\mathbf{div}\; (b \cdot c) = (a \;\mathbf{div}\; c) \;\mathbf{div}\; b \tag{B.45b}$$
$$(a \;\mathbf{div}\; b) \;\mathbf{div}\; c = (a \;\mathbf{div}\; c) \;\mathbf{div}\; b \tag{B.45c}$$
$$(a \cdot x) \;\mathbf{div}\; (b \cdot x) = a \;\mathbf{div}\; b \tag{B.45d}$$

Erkennen Sie, welches Gesetz sich aus welcher Eigenschaft der Multiplikation ergibt? Vergleichen Sie die Gesetze mit den Eigenschaften (B.41a)–(B.41d) der natürlichen Subtraktion — welche Gemeinsamkeiten entdecken Sie?

Aus (B.42) lassen sich weitere Schlüsse ziehen, indem man die Kontraposition der Äquivalenz bildet und dabei ausnutzt, dass die Ordnung auf den natürlichen Zahlen *total* ist:

$$\begin{array}{ll} & a \cdot p \leqslant b \iff a \leqslant b \;\mathbf{div}\; p \\ \iff & \quad \{\text{ Kontraposition: } (a \iff b) \iff (\neg a \iff \neg b) \;\} \\ & \neg(a \cdot p \leqslant b) \iff \neg(a \leqslant b \;\mathbf{div}\; p) \\ \iff & \quad \{\text{ totale Ordnung: } \neg(a \leqslant b) \iff a > b \;\} \\ & a \cdot p > b \iff a > b \;\mathbf{div}\; p \end{array}$$

Wir erhalten eine Charakterisierung der natürlichen Division, in der ***div*** auf der *linken* Seite einer Ungleichung der Form $x < y$ auftritt.

$$b \;\mathbf{div}\; p < a \quad\iff\quad b < a \cdot p \tag{B.46}$$

Auch diese Variante lässt sich verwenden, um ***div*** für konkrete Werte auszurechnen: Zum Beispiel ist $7 \;\mathbf{div}\; 3 + 1$ die *kleinste* Zahl a, so dass $7 < a \cdot 3$, also $7 \;\mathbf{div}\; 3 + 1 = 3$.

Wenn wir unsere bisherigen Ergebnisse zusammentragen, können wir die natürliche Division exakt »einkreisen«.

$$\begin{array}{ll} & b \;\mathbf{div}\; p = a \\ \iff & \quad \{\text{ Ping-Pong Beweis (B.14) } \} \\ & a \leqslant b \;\mathbf{div}\; p \;\wedge\; b \;\mathbf{div}\; p \leqslant a \\ \iff & \quad \{\text{ Definition } \mathbf{div} \text{ (B.42) } \} \\ & a \cdot p \leqslant b \;\wedge\; b \;\mathbf{div}\; p \leqslant a \\ \iff & \quad \{\text{ strikte Ordnung (B.35a) } \} \\ & a \cdot p \leqslant b \;\wedge\; b \;\mathbf{div}\; p < a + 1 \\ \iff & \quad \{\text{ Charakterisierung } \mathbf{div} \text{ (B.46) mit } a := a + 1 \;\} \\ & a \cdot p \leqslant b \;\wedge\; b < (a + 1) \cdot p \end{array}$$

Wir halten fest:

$$b \;\mathbf{div}\; p = a \quad\iff\quad a \cdot p \leqslant b < (a + 1) \cdot p \tag{B.47}$$

Divisionsrest Laut Kürzungsregel (B.43) ist das Produkt $(b \;\mathbf{div}\; p) \cdot p$ höchstens so groß wie der Dividend: $(b \;\mathbf{div}\; p) \cdot p \leqslant b$, das heißt, es gibt eine natürliche Zahl d, so dass $d + (b \;\mathbf{div}\; p) \cdot p = b$ (B.34). Geben wir der existenzquantifizierten Größe einen Namen: $b \;\mathbf{mod}\; p$ — die Funktion heißt auch ***Teilerrest*** oder ***Modulo***.[14] Gemäß Definition gilt somit die ***Divisionsregel***:

$$(b \;\mathbf{mod}\; p) + (b \;\mathbf{div}\; p) \cdot p = b \tag{B.48a}$$

[14] Der Modulo-Operator ist ein weiteres Beispiel für eine ***Skolemfunktion***.

Der Teilerrest ist stets kleiner als der Divisor:

$$b \;\mathbf{mod}\; p < p \tag{B.48b}$$

Zum Beweis der Schranke greifen wir auf (B.46) zurück: Mit $a := b \;\mathbf{div}\; p + 1$ folgt unmittelbar $b < (b \;\mathbf{div}\; p + 1) \cdot p = (b \;\mathbf{div}\; p) \cdot p + p$ und somit

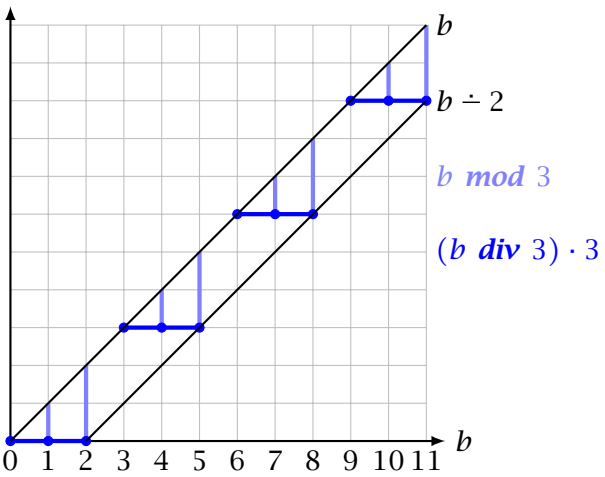
$$\begin{array}{ll} & b < (b \;\mathbf{div}\; p) \cdot p + p \\ \iff & \quad \{\ (\text{B.48a})\ \} \\ & (b \;\mathbf{mod}\; p) + (b \;\mathbf{div}\; p) \cdot p < (b \;\mathbf{div}\; p) \cdot p + p \\ \iff & \quad \{\ \text{-} + n \text{ Ordnungseinbettung } (\text{B.36a})\ \} \\ & b \;\mathbf{mod}\; p < p \end{array}$$

Die folgende Grafik illustriert die natürliche Division mit Rest für $p = 3$ (obwohl $\div$ und ***div*** nur für natürliche Zahlen definiert sind, sind die Funktionsgraphen aus Gründen der Lesbarkeit mit *durchgezogenen* Linien dargestellt).

$$(b \;\mathbf{div}\; 3) \cdot 3 + b \;\mathbf{mod}\; 3 = b$$

$$0 \leqslant b \;\mathbf{mod}\; 3 \leqslant 2$$

$$b \div 2 \leqslant (b \;\mathbf{div}\; 3) \cdot 3 \leqslant b$$



Der Abstand der Funktion $(b \;\mathbf{div}\; 3) \cdot 3$ zur Diagonalen b entspricht dem Divisionsrest $b \;\mathbf{mod}\; 3$. Aus den Graphen lässt sich ablesen, dass die ganzzahlige Division eine Treppenfunktion ist (mit diskreten Stufen) und dass der Divisionsrest periodisch ist.

Die Operationen ***div*** und ***mod*** werden durch die Eigenschaften (B.48a) und (B.48b) eindeutig festgelegt. Mit anderen Worten, die Eigenschaften können als alternative Definition von ***div*** verwendet werden. Eine Funktion, zwei Definitionen — wir sollten uns vergewissern, dass diese äquivalent sind. Da die Divisionsregel aus (B.42) folgt, haben wir die Hälfte der Arbeit schon erledigt. Für die Rückrichtung müssen wir zeigen, dass eine durch (B.48a)–(B.48b) festgelegte Divisionsoperation die Äquivalenz (B.42) erfüllt. Dazu genügt es, die folgenden drei Eigenschaften nachzuweisen:

- $\text{-} \cdot p$ ist monoton;
- $(b \;\mathbf{div}\; p) \cdot p \leqslant b$;
- $a \cdot p \leqslant b \implies a \leqslant b \;\mathbf{div}\; p$.

Die erste Eigenschaft gilt laut (B.36b); die zweite Eigenschaft folgt direkt aus (B.48a) und der Definition der Ordnung (B.34); wir zeigen die Kontraposition der dritten Eigenschaft: $b \;\mathbf{div}\; p <$

$a \implies b < a \cdot p$. Wir nehmen $b \;\mathbf{div}\; p < a$ an. Gemäß (B.35a) gilt $1 + b \;\mathbf{div}\; p \leqslant a$ und weiterhin

$$
\begin{array}{ll}
 & b \\
= & \quad \{ \text{ Eigenschaft von } \mathbf{div} \text{ (B.48a) } \} \\
 & (b \;\mathbf{mod}\; p) + (b \;\mathbf{div}\; p) \cdot p \\
< & \quad \{ \text{ Eigenschaft von } \mathbf{mod} \text{ (B.48b) } \} \\
 & p + (b \;\mathbf{div}\; p) \cdot p \\
= & \quad \{ \text{ Distributivgesetz } \} \\
 & (1 + b \;\mathbf{div}\; p) \cdot p \\
\leqslant & \quad \{ \text{ Annahme: } 1 + b \;\mathbf{div}\; p \leqslant a \} \\
 & a \cdot p
\end{array}
$$

Im zweiten Schritt nutzen wir aus, dass die Addition auch die strikte Ordnung erhält — formal kommt die Kontraposition von (B.36a) zum Einsatz.

Übungen.

1. Zeigen Sie, dass die durch (B.34) definierte Relation eine totale Ordnung ist und dass die Addition bezüglich dieser Ordnung monoton ist. *Hinweis:* Verwenden sie dazu Eigenschaften der Addition und/oder das Induktionsaxiom.

2. In $\mathbb{N}$ gilt stets $a \leqslant a + p$. Welche Eigenschaften von $\dot{-}$ lassen sich daraus ableiten?

3. Beweisen Sie die Vereinfachungsregeln (B.41c) und (B.41d), siehe auch Aufgabe B.5.8.

4. Beweisen Sie die folgenden Eigenschaften der natürlichen Subtraktion.

$$a \dot{-} a \leqslant 0$$
$$a \dot{-} c \leqslant (a \dot{-} b) + (b \dot{-} c)$$

Welche Eigenschaften von 0 und + werden jeweils benötigt? Siehe auch Aufgabe B.5.9.

5. Verwenden Sie die vorherige Aufgabe, um zu zeigen, dass d mit

$$d(a,b) = (a \dot{-} b) + (b \dot{-} a)$$

eine ***Metrik*** ist. *Hinweis:* Es gilt $d(a,b) = \mathrm{abs}(a - b)$, siehe auch Aufgabe B.1.10.

6. Ergänzen Sie die Einträge in der folgenden Tabelle — wie lassen sich die Ausdrücke auf der linken Seite jeweils umformen?

$a + (b + c) = (a + b) + c$	$(a + b) + c = ?$
$a + (b \dot{-} c) = ?$	$(a + b) \dot{-} c = ?$
$a \dot{-} (b + c) = ?$	$(a \dot{-} b) + c = ?$
$a \dot{-} (b \dot{-} c) = ?$	$(a \dot{-} b) \dot{-} c = a \dot{-} (b + c)$

Hinweis: In mehreren Fällen sind Fallunterscheidungen angezeigt.

7. Zeigen Sie, dass $\mathbf{div}$ monoton ist (B.44).

8. Beweisen Sie die Vereinfachungsregeln (B.45a)–(B.45d), siehe auch Aufgabe B.5.3.

9. Produkte von »Brüchen« lassen sich wie folgt vereinfachen (auch für monus gibt es korrespondierende Regeln, siehe Aufgabe B.5.4).

$$1 \leqslant a \;\mathbf{div}\; a \tag{B.49}$$

$$(a \;\mathbf{div}\; b) \cdot (b \;\mathbf{div}\; c) \leqslant a \;\mathbf{div}\; c \tag{B.50}$$

10. Lisa Lista hat die Definition der natürlichen Subtraktion mit der Definition der natürlichen Division verglichen und festgestellt, dass die Subtraktion auf der linken Seite einer Ungleichung steht, während die Division rechts steht. Harry Hacker meint, dass die Position keine große Rolle spielt und man genauso gut die folgenden indirekten Definitionen verwenden könnte.

$$\begin{aligned} a + p \leqslant b &\iff a \leqslant b \dot{-} p \\ a \;\mathbf{div}\; p \leqslant b &\iff a \leqslant b \cdot p \end{aligned}$$

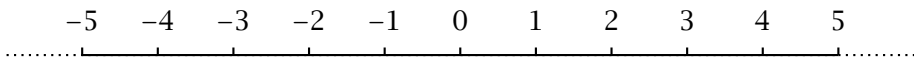
Was denken Sie?

B.5.2. Rechnen mit ganzen Zahlen

A physicist, a biologist, and a mathematician are sitting in a street café watching people entering and leaving the house on the other side of the street. First they see two people entering the house. Time passes. After a while they notice three people leaving the house. The physicist says, »The measurement wasn't accurate.« The biologist says, »They must have reproduced.« The mathematician says, »If one more person enters the house, then it will be empty.«

Ein kleiner Strich, eine große Wirkung: Aus 4711 wird −4711, aus einem Guthaben wird eine Schuld. Zahlengeschichtlich gesehen ist das Minuszeichen »−« vergleichsweise jung. Es wurde im 15. Jahrhundert zur Kennzeichnung von Überschuss und Mangel eingeführt, siehe Abbildung 2.1 (»was auß − ist das ist minus ⟨…⟩ und das + das ist meer«).

Führen wir zu jeder natürlichen Zahl a eine ***Gegenzahl*** $-a$ ein, so dass $-a + a = 0$, erhalten wir die ganzen Zahlen. Aus der Definition der Gegenzahl folgt, dass 0 ihre eigene Gegenzahl ist, $-0 = 0$, und dass die Gegenzahl eine ***Involution*** ist: $-(-a) = a$. Die Ordnung auf den natürlichen Zahlen lässt sich problemlos auf die ganzen Zahlen erweitern — der Zahlenstrahl wird durch Spiegelung zu einer Zahlengeraden.



Wie gehabt wird die Ordnungsrelation auf die Addition zurückgeführt.

$$a \leqslant b \text{ in } \mathbb{Z} \iff \exists\, d \in \mathbb{N} \;.\; d + a = b \tag{B.51}$$

Auch die enge Beziehung zwischen der strikten Ordnung $<$ und der nicht strikten Ordnung $\leqslant$ bleibt erhalten:

$$m + 1 \leqslant n \text{ in } \mathbb{Z} \iff m < n \text{ in } \mathbb{Z} \iff m \leqslant n - 1 \text{ in } \mathbb{Z} \tag{B.52}$$

Die Abbildungen $- + p$ und $- \cdot p$ mit $p > 0$ sind ebenfalls Ordnungseinbettungen auf den ganzen Zahlen. Für negative Faktoren kehrt sich bei der Multiplikation, wie auch bei der Gegenzahl, die Ordnung um:

$$a \leqslant b \text{ in } \mathbb{Z} \iff a + p \leqslant b + p \text{ in } \mathbb{Z} \tag{B.53a}$$

$$a \geqslant b \text{ in } \mathbb{Z} \iff -a \leqslant -b \text{ in } \mathbb{Z} \tag{B.53b}$$

$$a \leqslant b \text{ in } \mathbb{Z} \iff a \cdot p \leqslant b \cdot p \text{ in } \mathbb{Z} \quad \text{für alle } p > 0 \tag{B.53c}$$

$$a \geqslant b \text{ in } \mathbb{Z} \iff a \cdot p \leqslant b \cdot p \text{ in } \mathbb{Z} \quad \text{für alle } p < 0 \tag{B.53d}$$

Ganzzahlige Subtraktion Auf den natürlichen Zahlen hat die Addition $\text{-} + p$ (»p Dinge hinzufügen«) nur die unvollkommene Umkehrung $\text{-} \dot{-} p$ (»p Dinge wegnehmen«). Wegnehmen ist ***linksinvers***[15] zum Hinzufügen — hinzufügen und dann wieder wegnehmen ergibt die ursprüngliche Anzahl: $(b+p) \dot{-} p = b$ — aber nicht ***rechtsinvers*** — erst wegnehmen und dann hinzufügen ergibt möglicherweise mehr: $a \leqslant (a \dot{-} p) + p$. Auf den ganzen Zahlen hat sich das »Problem« erledigt: Die ganzzahlige Subtraktion definiert durch $a - p := a + (-p)$ ist eine waschechte Inverse der Addition: $(b + p) - p = b$ und $a = (a - p) + p$.

Die Subtraktion bzw. die Gegenzahl lässt sich alternativ mittels einer indirekten Definition einführen. Es genügt, eine der beiden unten aufgeführten Äquivalenzen zu postulieren, die andere ergibt sich als Folgerung. (Vergleichen Sie: Auf ähnliche Weise haben wir das Komplement in Abschnitt B.4.3 eingeführt.)

$$\begin{aligned} a + (-p) \leqslant b \quad &\Longleftrightarrow \quad a \leqslant b + p \\ a + p \leqslant b \quad &\Longleftrightarrow \quad a \leqslant b + (-p) \end{aligned}$$

Aus den resultierenden Vereinfachungsregeln, $a \leqslant a + (-p) + p$ und $b + p + (-p) \leqslant b$, folgt unmittelbar, dass $-p$ die additive Inverse von p ist: $0 \leqslant (-p) + p \leqslant 0$. Minus kann somit als symmetrische Variante von Monus aufgefasst werden: »$\dot{-}$« erfüllt nur die erste Äquivalenz, nicht aber die zweite (jeweils eingeschränkt auf die natürlichen Zahlen).

Auch auf die Gefahr hin, etwas Offensichtliches zu benennen: Minus ist *keine* Erweiterung von Monus: es gilt $0 \dot{-} 1 = 0$, aber $0 - 1 = -1$. Um Monus auf die ganzen Zahlen zu erweitern, können wir auf Eigenschaft (B.40) zurückgreifen.

$$\begin{aligned} & (a \dot{-} b) + b = a \uparrow b \\ \Longleftrightarrow \quad & \{ \text{ Inverse } \} \\ & a \dot{-} b = (a \uparrow b) - b \\ \Longleftrightarrow \quad & \{ \text{ } \text{-} - p \text{ ist monoton und (B.26b) } \} \\ & a \dot{-} b = (a - b) \uparrow 0 \end{aligned}$$

Maximum und Monus sind somit auf den ganzen Zahlen interdefinierbar.

$$a \dot{-} b = (a - b) \uparrow 0 \qquad\qquad a \uparrow b = (a \dot{-} b) + b$$

Wir können die natürliche Subtraktion als »bewachte« ganzzahlige Subtraktion auffassen: $a \dot{-} b = [a \geqslant b] \cdot (a - b)$ — die in der Iverson Klammer eingeschlossene Bedingung wacht sozusagen über die Anwendung der ganzzahligen Subtraktion.

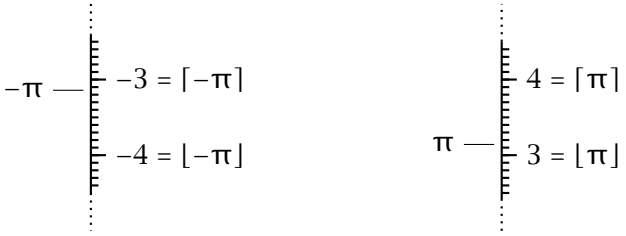
Um andere Funktionen wie Division oder Wurzel von den reellen auf die ganzen Zahlen zu »portieren«, sind die im Folgenden eingeführten Konversionsfunktionen nützlich.

GOD is REAL (unless declared INTEGER).

— Fortran Witz

Boden und Decke Die ***Bodenfunktion*** $\lfloor \text{-} \rfloor : \mathbb{R} \to \mathbb{Z}$ (kurz: Boden, engl. floor) ordnet einer reellen Zahl $x \in \mathbb{R}$ die größte ganze Zahl zu, die kleiner ist als x. Umgekehrt bildet die ***Deckenfunktion*** $\lceil \text{-} \rceil : \mathbb{R} \to \mathbb{Z}$ (kurz: Decke, engl. ceiling) eine reelle Zahl auf die kleinste ganze Zahl ab, die größer ist. Zum Beispiel: $\lfloor \pi \rfloor = 3 < 4 = \lceil \pi \rceil$, $\lfloor -\pi \rfloor = -4 < -3 = \lceil -\pi \rceil$, $\lfloor \frac{4}{3} \rfloor = 1 < 2 = \lceil \frac{4}{3} \rceil$ und $\lfloor 47 \rfloor = 47 = \lceil 47 \rceil$.

[15] Gilt $f \circ g = id$, dann ist f linksinvers zu g und g rechtsinvers zu f.



Die Notation lässt sich leicht einprägen, wenn man an einen Fahrstuhl denkt: Die reelle Zahl ist die aktuelle Position des Fahrstuhls; die ganzen Zahlen sind die Stockwerke; die Klammern geben die Fahrtrichtung an: ⌊-⌋ nach unten und ⌈-⌉ nach oben. Also: $\lfloor x \rfloor$ befördert x in das nächst tieferliegende Stockwerk und $\lceil x \rceil$ in das nächst höherliegende.

Die Abbildungen werden, wie mittlerweile gewohnt, mittels indirekter Definitionen eingeführt. Für alle $n \in \mathbb{Z}$ und $x \in \mathbb{R}$ gilt:

$$n \leqslant x \text{ in } \mathbb{R} \iff n \leqslant \lfloor x \rfloor \text{ in } \mathbb{Z} \tag{B.54a}$$
$$\lceil x \rceil \leqslant n \text{ in } \mathbb{Z} \iff x \leqslant n \text{ in } \mathbb{R} \tag{B.54b}$$

Mit Hilfe von »Boden« und »Decke« lässt sich eine Ungleichung zwischen einer ganzen Zahl und einer reellen Zahl (» in $\mathbb{R}$«) in eine äquivalente Ungleichung zwischen ganzen Zahlen überführen (» in $\mathbb{Z}$«).

Aus (B.54a) folgt unmittelbar, dass $\lfloor x \rfloor \leqslant x$, $n \leqslant \lfloor n \rfloor$ und damit $\lfloor n \rfloor = n$, insbesondere $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$. Entsprechend folgt aus (B.54b), dass $x \leqslant \lceil x \rceil$, $\lceil n \rceil \leqslant n$ und damit $\lceil n \rceil = n$, insbesondere $\lceil \lceil x \rceil \rceil = \lceil x \rceil$.

$$\lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil \tag{B.55a}$$
$$\lfloor n \rfloor = n = \lceil n \rceil \tag{B.55b}$$

Beide Abbildungen sind monoton.

$$x \leqslant y \implies \lfloor x \rfloor \leqslant \lfloor y \rfloor \tag{B.56a}$$
$$x \leqslant y \implies \lceil x \rceil \leqslant \lceil y \rceil \tag{B.56b}$$

Die indirekte Form der Definition legt nahe, zum Nachweis indirekte Beweise zu führen.

$$\begin{aligned} & n \leqslant \lfloor x \rfloor \\ \iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\ & n \leqslant x \\ \implies & \quad \{ \text{ Annahme: } x \leqslant y \} \\ & n \leqslant y \\ \iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\ & n \leqslant \lfloor y \rfloor \end{aligned} \qquad \begin{aligned} & \lceil x \rceil \leqslant n \\ \iff & \quad \{ \text{ Definition Decke (B.54b) } \} \\ & x \leqslant n \\ \impliedby & \quad \{ \text{ Annahme: } x \leqslant y \} \\ & y \leqslant n \\ \iff & \quad \{ \text{ Definition Decke (B.54b) } \} \\ & \lceil y \rceil \leqslant n \end{aligned}$$

Die Position der Abbildung diktiert die verwendete Beweistechnik: Da der »Boden« in (B.54a) auf der rechten Seite der Ungleichung auftritt, verwenden wir (B.15d) für den Nachweis der Monotonie; die »Decke« tritt in (B.54b) links auf, so dass (B.15c) zum Einsatz kommt.

Aus der Kontraposition von (B.54a) und (B.54b) lassen sich weitere interessante Schlüsse zie-

hen, wenn man ausnutzt, dass die Ordnungen in $\mathbb{Z}$ und $\mathbb{R}$ total sind.

$$
\begin{aligned}
& n \leqslant x \text{ in } \mathbb{R} \iff n \leqslant \lfloor x \rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Kontraposition: } (a \iff b) \iff (\neg a \iff \neg b) \} \\
& \neg(n \leqslant x) \text{ in } \mathbb{R} \iff \neg(n \leqslant \lfloor x \rfloor) \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ totale Ordnung: } \neg(a \leqslant b) \iff a > b \} \\
& n > x \text{ in } \mathbb{R} \iff n > \lfloor x \rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ strikte und nicht strikte Ordnung in } \mathbb{Z} \text{ (B.52) } \} \\
& \lfloor x \rfloor + 1 \leqslant n \text{ in } \mathbb{Z} \iff x < n \text{ in } \mathbb{R}
\end{aligned}
$$

Durch die Negation im ersten Schritt wechselt der »Boden« im Vergleich zu (B.54a) die Seite. Eine analoge Rechnung ergibt ein analoges Ergebnis für die Decke. Für alle $n \in \mathbb{Z}$ und $x \in \mathbb{R}$ gilt:

$$\lfloor x \rfloor + 1 \leqslant n \text{ in } \mathbb{Z} \iff x < n \text{ in } \mathbb{R} \tag{B.57a}$$

$$n < x \text{ in } \mathbb{R} \iff n \leqslant \lceil x \rceil - 1 \text{ in } \mathbb{Z} \tag{B.57b}$$

Aus den Äquivalenzen folgt unmittelbar, dass $x < \lfloor x \rfloor + 1$ und $\lceil x \rceil - 1 < x$. Fassen wir die bisherigen Abschätzungen zusammen, erhalten wir die folgenden Charakterisierungen von Boden und Decke.

$$n \leqslant x < n + 1 \iff \lfloor x \rfloor = n \iff x - 1 < n \leqslant x \tag{B.58a}$$

$$n - 1 < x \leqslant n \iff \lceil x \rceil = n \iff x \leqslant n < x + 1 \tag{B.58b}$$

Mit anderen Worten, »Boden« und »Decke« sind ***Treppenfunktionen*** — allerdings Treppen mit unendlich vielen Stufen.

Wie interagieren Boden und Decke mit den arithmetischen Operationen wie Addition und Multiplikation? Die Treppeneigenschaft legt nahe, dass sich ganze Zahlen aus den Klammern herausziehen lassen. Es gelten die ***Verschiebungsregeln*** (engl. shift rules):

$$\lfloor x + n \rfloor = \lfloor x \rfloor + n \qquad \lceil x + n \rceil = \lceil x \rceil + n \tag{B.59}$$

Beliebige reelle Zahlen lassen sich nicht »herausziehen«: $\lfloor \frac{1}{2} + \frac{1}{2} \rfloor = 1 \neq \frac{1}{2} = \lfloor \frac{1}{2} \rfloor + \frac{1}{2}$. In den Beweis von (B.59) fließt die Annahme, dass n eine ganze Zahl ist, im zweiten Schritt ein: Die Umformung ist nur gültig, wenn $z - n$ eine ganze Zahl ist.

$$
\begin{aligned}
& z \leqslant \lfloor x \rfloor + n \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ additive Inverse } \} \\
& z - n \leqslant \lfloor x \rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) und } z - n \in \mathbb{Z} \} \\
& z - n \leqslant x \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ additive Inverse } \} \\
& z \leqslant x + n \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) und } z \in \mathbb{Z} \} \\
& z \leqslant \lfloor x + n \rfloor \text{ in } \mathbb{Z}
\end{aligned}
$$

Gilt auch $\lfloor x \cdot n \rfloor = \lfloor x \rfloor \cdot n$? Nein, ein Gegenbeispiel ist schnell gefunden: $\lfloor \frac{1}{2} \cdot 2 \rfloor = 1 \neq 0 = \lfloor \frac{1}{2} \rfloor \cdot 2$. (Wo läuft der obige Beweis schief, wenn wir »+« durch »·« ersetzen?)

Die Gegenzahl stellt alles auf den Kopf: Aus Böden werden Decken und umgekehrt.

$$\lfloor -x \rfloor = -\lceil x \rceil \qquad \lceil -x \rceil = -\lfloor x \rfloor \tag{B.60}$$

Wir weisen die erste Gleichung nach, indem wir zeigen, dass $-\lceil x \rceil$ die definierende Eigenschaft von $\lfloor -x \rfloor$ (B.54a) erfüllt.

$$
\begin{aligned}
& n \leqslant -\lceil x \rceil \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Negation ist eine antitone Ordnungseinbettung (B.53b) } \} \\
& \lceil x \rceil \leqslant -n \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Decke (B.54b) und } -n \in \mathbb{Z} \} \\
& x \leqslant -n \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Negation ist eine antitone Ordnungseinbettung (B.53b) } \} \\
& n \leqslant -x \text{ in } \mathbb{R}
\end{aligned}
$$

In den Beweis fließt im Wesentlichen ein, dass die Negation antiton ist.

Ganzzahlige Division mit Rest Die Multiplikation besitzt im Gegensatz zur Addition keine Inverse in $\mathbb{Z}$, so dass wir die natürliche Division ***div*** (B.42) auf die ganzen Zahlen erweitern wollen. Leider ist die Erweiterung nicht eindeutig — während die *natürliche* Division durch die Eigenschaften (B.48a) und (B.48b) eindeutig festgelegt wird, gilt das für die *ganzzahlige* Division nicht. In Positive gewendet haben wir als »Sprachdesigner/-in« einen gewissen Spielraum, den wir nutzen können, um uns eine passende Definition zurechtzulegen. In der Tat findet man in verschiedenen Programmiersprachen verschiedene Varianten der ganzzahligen Division mit unterschiedlichen Eigenschaften.

Abrundende Division Als Ausgangspunkt dient uns die indirekte Definition (B.42) von ***div***. Zur Erinnerung: 7 ***div*** 3 ist die größte Zahl a mit $a \cdot 3 \leqslant 7$. Diese Zahl lässt sich mit Hilfe des Bodens ausdrücken: $\lfloor 7/3 \rfloor$. Das klappt auch für beliebige *ganze* Zahlen:

$$
\begin{aligned}
& a \cdot p \leqslant b \text{ in } \mathbb{Z} \\
\iff & \quad \{ a \cdot p \in \mathbb{Z} \text{ und } b \in \mathbb{Z} \} \\
& a \cdot p \leqslant b \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse } \textit{und } p > 0 \} \\
& a \leqslant b/p \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Boden (B.54a) } \} \\
& a \leqslant \lfloor b/p \rfloor \text{ in } \mathbb{Z}
\end{aligned}
\qquad
\begin{aligned}
& a \cdot p \leqslant b \text{ in } \mathbb{Z} \\
\iff & \quad \{ a \cdot p \in \mathbb{Z} \text{ und } b \in \mathbb{Z} \} \\
& a \cdot p \leqslant b \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse } \textit{und } p < 0 \} \\
& a \geqslant b/p \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Decke (B.54b) } \} \\
& a \geqslant \lceil b/p \rceil \text{ in } \mathbb{Z}
\end{aligned}
$$

Die linke Herleitung verallgemeinert ***div***s indirekte Definition (B.42) von $\mathbb{N}$ auf $\mathbb{Z}$ — allerdings müssen wir voraussetzen, dass der Divisor p positiv ist. Damit gilt insbesondere b ***div*** $p = \lfloor b/p \rfloor$ für alle natürlichen Zahlen b und p. Die beiden Rechnungen verdeutlichen, dass die Eigenschaften der Multiplikation die Eigenschaften ihrer Quasiinversen bestimmen. Zur Erinnerung: für $p > 0$ ist $\text{-} \cdot p$ eine isotone (B.53c) Ordnungseinbettung, für $p < 0$ eine antitone (B.53d) und für $p = 0$ eine konstante Funktion. Für negative Divisoren kehrt sich die Ordnung somit um und anstelle des Bodens kommt die Decke zum Einsatz. Als erste, wichtige Erkenntnis nehmen wir mit, dass Dividend und Divisor bezüglich ihres Vorzeichens ganz unterschiedlich gehandhabt werden!

Neben der Division müssen wir auch den Divisionsrest auf die ganzen Zahlen erweitern. An dieser Stelle machen wir uns das Leben leicht: Der Divisionsrest wird so definiert, dass die ***Divi-***

sionsregel (B.48a) qua Konstruktion gültig ist (für $b \neq 0$).[16]

$$a \;\mathbf{div}\; b := \lfloor a/b \rfloor \tag{B.61a}$$
$$a \;\mathbf{mod}\; b := a - (a \;\mathbf{div}\; b) \cdot b = a - \lfloor a/b \rfloor \cdot b \tag{B.61b}$$

(Die Definitionen sind nicht nur für ganze, sondern sogar für reelle Zahlen gültig — wir werden allerdings keinen Gebrauch davon machen.)

Wenn der Rest von Null verschieden ist, dann wird das Vorzeichen von $a \;\mathbf{mod}\; b$ durch das Vorzeichen des Divisors b bestimmt:

$$0 \leqslant a \;\mathbf{mod}\; b < b \quad \Longleftarrow \quad b > 0 \tag{B.62a}$$
$$b < a \;\mathbf{mod}\; b \leqslant 0 \quad \Longleftarrow \quad b < 0 \tag{B.62b}$$

Die Umkehrung der Ungleichungen liegt wiederum im Monotonieverhalten der Multiplikation begründet. *Vorsicht:* Es ist nicht der Fall, dass $\operatorname{sign}(a \;\mathbf{mod}\; b) = \operatorname{sign} b$, da der Rest gleich Null sein kann; vielmehr gilt $\operatorname{sign}(a \;\mathbf{mod}\; b) = \operatorname{sign} b \cdot [a/b \notin \mathbb{Z}]$.

$$\begin{aligned}
& 0 \leqslant a \;\mathbf{mod}\; b < b \;\text{ in }\; \mathbb{Z} \\
\Longleftrightarrow \quad & \{\text{ Definition Rest (B.61b) }\} \\
& 0 \leqslant a - \lfloor a/b \rfloor \cdot b < b \;\text{ in }\; \mathbb{R} \\
\Longleftrightarrow \quad & \{\text{ additive Inverse }\} \\
& \lfloor a/b \rfloor \cdot b \leqslant a < \lfloor a/b \rfloor \cdot b + b \;\text{ in }\; \mathbb{R} \\
\Longleftrightarrow \quad & \{\text{ mult. Inverse } \textit{und}\ b > 0 \;\} \\
& \lfloor a/b \rfloor \leqslant a/b < \lfloor a/b \rfloor + 1 \;\text{ in }\; \mathbb{R}
\end{aligned}$$

$$\begin{aligned}
& b < a \;\mathbf{mod}\; b \leqslant 0 \;\text{ in }\; \mathbb{Z} \\
\Longleftrightarrow \quad & \{\text{ Definition Rest (B.61b) }\} \\
& b < a - \lfloor a/b \rfloor \cdot b \leqslant 0 \;\text{ in }\; \mathbb{R} \\
\Longleftrightarrow \quad & \{\text{ additive Inverse }\} \\
& \lfloor a/b \rfloor \cdot b + b < a \leqslant \lfloor a/b \rfloor \cdot b \;\text{ in }\; \mathbb{R} \\
\Longleftrightarrow \quad & \{\text{ mult. Inverse } \textit{und}\ b < 0 \;\} \\
& \lfloor a/b \rfloor + 1 > a/b \geqslant \lfloor a/b \rfloor \;\text{ in }\; \mathbb{R}
\end{aligned}$$

Die finalen Ungleichungen folgen jeweils aus (B.58a) mit $x := a/b$.

Aufrundende Division Von den rationalen oder reellen Zahlen kennen wir die Vorzeichenregeln $(-a)/b = -(a/b) = a/(-b)$. Da bei einem Vorzeichenwechsel Boden- und Deckenfunktion vertauscht werden, $\lfloor -a/b \rfloor = -\lceil a/b \rceil$, sind die Regeln für die ganzzahlige Division nicht ganz so einprägsam. Zunächst einmal drängt es sich geradezu auf, neben der abrundenden (engl. rounding down) zusätzlich eine *aufrundende* (engl. rounding up) Variante der Division einzuführen.[17]

$$a \;\overline{\mathbf{div}}\; b := \lceil a/b \rceil \tag{B.63a}$$
$$a \;\overline{\mathbf{mod}}\; b := a - (a \;\overline{\mathbf{div}}\; b) \cdot b = a - \lceil a/b \rceil \cdot b \tag{B.63b}$$

Wenn wir beide Varianten in einer Formel verwenden, notieren wir die abrundende Division mit $\underline{\mathbf{div}}$ und $\underline{\mathbf{mod}}$, um Verwechslungen vorzubeugen. Damit erhalten wir folgende Vorzeichenregeln.

$$a \;\underline{\mathbf{div}}\; (-p) = -(a \;\overline{\mathbf{div}}\; p) \qquad a \;\underline{\mathbf{mod}}\; (-p) = a \;\overline{\mathbf{mod}}\; p \tag{B.64a}$$
$$(-a) \;\underline{\mathbf{div}}\; p = -(a \;\overline{\mathbf{div}}\; p) \qquad (-a) \;\underline{\mathbf{mod}}\; p = -(a \;\overline{\mathbf{mod}}\; p) \tag{B.64b}$$

[16] Quotient und Divisionsrest sind als Einheit zu betrachten. Man kann sich darauf beschränken, eine der beiden Funktionen zu definieren; die jeweils andere wird dann so definiert, dass die Divisionsregel (B.48a) qua Konstruktion gilt. Kombinationen, die die Divisionsregel *nicht* erfüllen, sind schlicht und einfach nicht zu gebrauchen (ISO Standard Pascal definiert so eine nutzlose Variante). Die enge Zusammengehörigkeit spiegelt sich auch in der Hardware wider: Der x86 Instruktionssatz bietet nur Instruktionen an, die gleichzeitig den Quotienten und den Rest berechnen, zum Beispiel, `IDIV` (Signed Divide).

[17] Ähnlich wie Sinus und Cosinus sind auch ab- und aufrundende Division ein eng verbundenes Paar von Funktionen. Die trigonometrischen Funktionen sind wie die Divisionen interdefinierbar: $\sin\alpha = \cos(90° - \alpha)$ und $\cos\alpha = \sin(90° - \alpha)$, aber kein Mathematiker würde auf die Idee kommen, nur eine der beiden Funktionen einzuführen.

Beachte: Beim Divisionsrest verschwindet das Vorzeichen des Divisors, während das Vorzeichen des Dividenden propagiert wird. Kombinieren wir die Vorzeichenregeln für den Rest mit (B.62a)–(B.62b), erhalten wir unmittelbar:

$$-b < a \mathbin{\overline{\mathbf{mod}}} b \leqslant 0 \quad \Longleftarrow \quad b > 0$$
$$0 \leqslant a \mathbin{\overline{\mathbf{mod}}} b < -b \quad \Longleftarrow \quad b < 0$$

Der Rest $a \mathbin{\overline{\mathbf{mod}}} b$ ist nichtpositiv für positive b und nichtnegativ für negative b.

Die aufrundende Division lässt sich genau wie die abrundende Division alternativ durch eine indirekte Definition einführen.

$$\begin{aligned}
a \cdot p \leqslant b &\iff a \leqslant b \mathbin{\underline{\mathbf{div}}} p && \text{falls } p > 0\\
a \mathbin{\underline{\mathbf{div}}} p \geqslant b &\iff a \leqslant b \cdot p && \text{falls } p < 0\\
a \mathbin{\overline{\mathbf{div}}} p \leqslant b &\iff a \leqslant b \cdot p && \text{falls } p > 0\\
a \cdot p \leqslant b &\iff a \geqslant b \mathbin{\overline{\mathbf{div}}} p && \text{falls } p < 0
\end{aligned}$$

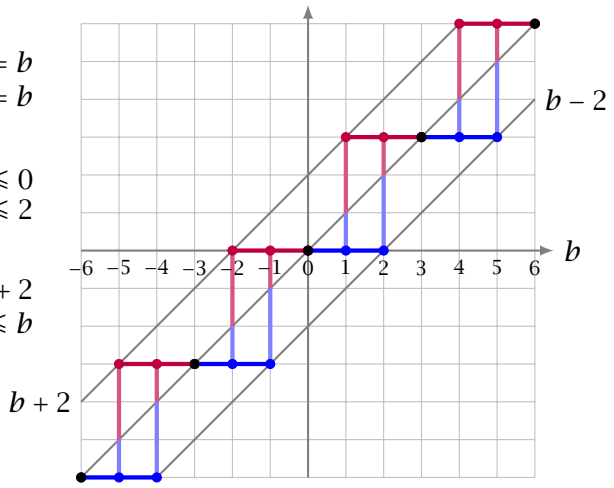
Da $a \mathbin{\overline{\mathbf{div}}} p$ die *kleinste* Zahl b mit $a \leqslant b \cdot p$ ist, steht die aufrundende Division auf der *linken* Seite einer Ungleichung. Zum Vergleich: $b \mathbin{\underline{\mathbf{div}}} p$ ist die *größte* Zahl a mit $a \cdot p \leqslant b$; entsprechend steht die abrundende Division auf der *rechten* Seite einer Ungleichung (damit haben wir Aufgabe B.5.10 zumindest teilweise beantwortet).

Es ist hilfreich, sich die Eigenschaften der ab- und der aufrundenden Division graphisch vor Augen zu führen.

$$(b \mathbin{\overline{\mathbf{div}}} 3) \cdot 3 + b \mathbin{\overline{\mathbf{mod}}} 3 = b$$
$$(b \mathbin{\underline{\mathbf{div}}} 3) \cdot 3 + b \mathbin{\underline{\mathbf{mod}}} 3 = b$$

$$-2 \leqslant b \mathbin{\overline{\mathbf{mod}}} 3 \leqslant 0$$
$$0 \leqslant b \mathbin{\underline{\mathbf{mod}}} 3 \leqslant 2$$

$$b \leqslant (b \mathbin{\overline{\mathbf{div}}} 3) \cdot 3 \leqslant b + 2$$
$$b - 2 \leqslant (b \mathbin{\underline{\mathbf{div}}} 3) \cdot 3 \leqslant b$$



Die blauen Punkte stellen die Funktion $\lfloor b/3 \rfloor \cdot 3$ dar, die violetten $\lceil b/3 \rceil \cdot 3$; für Vielfache von 3 geht die Division glatt auf, so dass die Funktionswerte übereinstimmen: $\lfloor b/3 \rfloor \cdot 3 = \lceil b/3 \rceil \cdot 3$, angezeigt durch schwarze Punkte. Der Abstand der beiden Funktionen zur Diagonalen b visualisiert den jeweiligen Divisionsrest, der nichtnegativ für $\lfloor b/3 \rfloor$ ist und nichtpositiv für $\lceil b/3 \rceil$. Der eine Graph geht durch Punktspiegelung im Ursprung in den anderen Graphen über: $\lfloor -b/3 \rfloor \cdot 3 = -\lceil b/3 \rceil \cdot 3$.

Zwei weitere Eigenschaften lassen sich aus den Graphen ablesen: Die ganzzahlige Division ist eine Treppenfunktion und der Divisionsrest ist ***periodisch*** — die Funktionswerte wiederholen sich nach p Schritten (oben ist $p := 3$).

$$(a + b \cdot p) \mathbin{\mathbf{div}} p = a \mathbin{\mathbf{div}} p + b \qquad (a + b \cdot p) \mathbin{\overline{\mathbf{div}}} p = a \mathbin{\overline{\mathbf{div}}} p + b \qquad \text{(B.65a)}$$
$$(a + b \cdot p) \mathbin{\mathbf{mod}} p = a \mathbin{\mathbf{mod}} p \qquad (a + b \cdot p) \mathbin{\overline{\mathbf{mod}}} p = a \mathbin{\overline{\mathbf{mod}}} p \qquad \text{(B.65b)}$$

Die Periodizität leitet sich aus einer zentralen Eigenschaft des Bodens bzw. der Decke ab: Ganzzahlige Terme können aus der Klammer herausgezogen werden (B.59).

$$
\begin{aligned}
& (a + b \cdot p) \ \textbf{\textit{div}} \ p \\
\iff & \quad \{ \text{ Definition } \textbf{\textit{div}} \text{ (B.61a) } \} \\
& \lfloor (a + b \cdot p)/p \rfloor \\
\iff & \quad \{ \text{ Arithmetik } \} \\
& \lfloor a/p + b \rfloor \\
\iff & \quad \{ \text{ Verschiebungsregel (B.59) } \} \\
& \lfloor a/p \rfloor + b \\
\iff & \quad \{ \text{ Definition } \textbf{\textit{div}} \text{ (B.61a) } \} \\
& a \ \textbf{\textit{div}} \ p + b
\end{aligned}
$$

Umrechnungsformeln\Interdefinierbarkeit Auf- und abrundende Division sind nicht unabhängig voneinander, eine Variante der ganzzahligen Division kann in die andere überführt werden. Die resultierenden Formeln kommen zum Beispiel zum Einsatz, wenn eine Programmiersprache nur eine Form der Division anbietet, aber eine andere benötigt wird. (Ähnliche Problemstellungen treten bei der ***Portierung*** von Programmen auf: Ein in der Sprache X geschriebenes Programm muss in die Sprache Y übersetzt werden.)

Geht die Division glatt auf, $a/p \in \mathbb{Z}$, dann stimmen ab- und aufrundende Division überein (das ist beruhigend), anderenfalls differieren die Quotienten um eins (das ist *merk*würdig).

$$a \ \overline{\textbf{\textit{div}}} \ p - a \ \underline{\textbf{\textit{div}}} \ p = [a/p \notin \mathbb{Z}] \qquad\qquad a \ \underline{\textbf{\textit{mod}}} \ p - a \ \overline{\textbf{\textit{mod}}} \ p = [a/p \notin \mathbb{Z}] \cdot p \tag{B.66}$$

Die ***Umrechnungsformeln*** setzen drei Varianten der Division zueinander in Beziehung: die reelle, die auf- und die abrundende. Ob die Division glatt aufgeht, zeigt der Rest an.

$$a \ \underline{\textbf{\textit{mod}}} \ p = 0 \quad \iff \quad a/p \in \mathbb{Z} \quad \iff \quad a \ \overline{\textbf{\textit{mod}}} \ p = 0$$

Dieser Zusammenhang folgt aus der Divisionsregel (B.48a). Zur Erinnerung: Die Modulo-Operation ist jeweils so definiert worden, dass die Divisionsregel qua Konstruktion gilt.

Die Umrechnungsformeln (B.66) fußen auf Eigenschaften der Rundungsfunktionen. Boden und Decke hängen eng zusammen: Sie stimmen auf den ganzen Zahlen überein — bildlich gesprochen befindet sich der Fahrstuhl in einem Stockwerk. Befindet sich der Fahrstuhl zwischen zwei Stockwerken, so ist die Decke um eins größer als der Boden.

$$\lceil x \rceil - \lfloor x \rfloor = [x \notin \mathbb{Z}] \tag{B.67}$$

Dank der Iverson Klammer deckt die Formel beide Fälle ab: Für $x \in \mathbb{Z}$ ist die rechte Seite Null und damit $\lfloor x \rfloor = \lceil x \rceil$; für $x \notin \mathbb{Z}$ ergibt sich eine Differenz von eins.

Die Umrechnungsformeln (B.66) gelten übrigens für beliebige *reelle* Zahlen $a, p \in \mathbb{R}$. Beschränken wir uns auf *ganze* Zahlen, $a, p \in \mathbb{Z}$, lassen sich alternative Beziehungen herleiten, die ohne den Test auf Teilbarkeit auskommen. Die nachfolgende Herleitung ist auf den ersten Blick etwas mysteriös, aber nur auf den ersten. Wir nutzen aus, dass der Boden in (B.54a) und die Decke in (B.57b) jeweils auf der rechten Seite einer Ungleichung auftritt, so dass wir die beiden Divisio-

nen durch einen indirekten Beweis miteinander in Beziehung setzen können.

$$
\begin{aligned}
& z \leqslant \lceil a/p \rceil - 1 \ \text{ in } \ \mathbb{Z} \\
\iff & \quad \{ \text{ Kontraposition Decke (B.57b) } \} \\
& z < a/p \ \text{ in } \ \mathbb{R} \\
\iff & \quad \{ \text{ Inverse und } p > 0 \ \} \\
& z \cdot p < a \ \text{ in } \ \mathbb{R} \\
\iff & \quad \{ \ z \cdot p \in \mathbb{Z} \text{ und } a \in \mathbb{Z} \ \} \\
& z \cdot p < a \ \text{ in } \ \mathbb{Z} \\
\iff & \quad \{ \text{ strikte Ordnung (B.52) } \} \\
& z \cdot p \leqslant a - 1 \ \text{ in } \ \mathbb{Z} \\
\iff & \quad \{ \ z \cdot p \in \mathbb{Z} \text{ und } a - 1 \in \mathbb{Z} \ \} \\
& z \cdot p \leqslant a - 1 \ \text{ in } \ \mathbb{R} \\
\iff & \quad \{ \text{ Inverse und } p > 0 \ \} \\
& z \leqslant (a-1)/p \ \text{ in } \ \mathbb{R} \\
\iff & \quad \{ \text{ Boden (B.54a) } \} \\
& z \leqslant \lfloor (a-1)/p \rfloor \ \text{ in } \ \mathbb{Z}
\end{aligned}
$$

Wir wechseln insgesamt viermal (!) zwischen den Welten ($\mathbb{Z}$ und $\mathbb{R}$) hin und her. Die beiden mittleren Wechsel (von $\mathbb{R}$ nach $\mathbb{Z}$ und zurück) dienen nur einem einzigen Zweck: die strikte Ordnung »loszuwerden«, so dass wir (B.54a) anwenden können. Da die Beziehung zwischen »<« und »⩽« (B.52) nur für ganze Zahlen gilt, müssen wir voraussetzen, dass $a, p \in \mathbb{Z}$. Aus der Herleitung ergibt sich eine zweite Voraussetzung: $p > 0$. Wie bereits gewohnt, müssen wir eine Fallunterscheidung über das Vorzeichen des Divisors vornehmen (mit einer analogen Herleitung wird die zweite Gleichung bestimmt).

$$
\begin{aligned}
\lceil a/p \rceil - \lfloor (a-1)/p \rfloor &= 1 && \text{falls } p > 0 \\
\lceil a/p \rceil - \lfloor (a+1)/p \rfloor &= 1 && \text{falls } p < 0
\end{aligned}
$$

Im Vergleich zu (B.66) stellen wir sozusagen sicher, dass die Differenz stets 1 beträgt, indem wir den Dividenden leicht verändern. Somit lässt sich die aufrundende auf die abrundende Division zurückführen:

$$
\begin{aligned}
a \ \overline{\boldsymbol{div}} \ p &= (a-1) \ \underline{\boldsymbol{div}} \ p + 1 & a \ \overline{\boldsymbol{mod}} \ p &= (a-1) \ \underline{\boldsymbol{mod}} \ p - (p-1) && \text{falls } p > 0 \\
a \ \overline{\boldsymbol{div}} \ p &= (a+1) \ \underline{\boldsymbol{div}} \ p + 1 & a \ \overline{\boldsymbol{mod}} \ p &= (a+1) \ \underline{\boldsymbol{mod}} \ p - (p+1) && \text{falls } p < 0
\end{aligned}
$$

Symmetrische Division Auch auf die Gefahr hin, etwas Offensichtliches zu benennen: $a \ \boldsymbol{div} \ b := \lfloor a/b \rfloor$ und $a \ \overline{\boldsymbol{div}} \ b := \lceil a/b \rceil$ sind *Spezifikationen*, keine *Implementierungen*. Die ganzzahligen Divisionen werden *nicht* realisiert, indem zunächst die exakte Division durchgeführt und das Ergebnis anschließend gerundet wird. Der Grund ist so einfach, wie schmerzvoll: Reelle Zahlen lassen sich auf dem Rechner nur unvollkommen darstellen; ebenso lassen sich Operationen auf den reellen Zahlen auf dem Rechner nur unvollkommen nachbilden. Die meisten (alle?) Prozessoren implementieren (aus historischen Gründen?) weder $\underline{\boldsymbol{div}}$ noch $\overline{\boldsymbol{div}}$, sondern eine Variante, die die von der reellen Division gewohnten Vorzeichenregeln erfüllt.

$$
a \ \boldsymbol{quot} \ b := \operatorname{sign} a \cdot \operatorname{sign} b \cdot \lfloor \operatorname{abs} a / \operatorname{abs} b \rfloor = \operatorname{sign} a \cdot \operatorname{sign} b \cdot \operatorname{abs} a \ \boldsymbol{div} \ \operatorname{abs} b \tag{B.68a}
$$

$$
a \ \boldsymbol{rem} \ b := a - (a \ \boldsymbol{quot} \ b) \cdot b = \operatorname{sign} a \cdot \operatorname{abs} a \ \boldsymbol{mod} \ \operatorname{abs} b \tag{B.68b}
$$

Man rechnet schnell nach, dass die folgenden Regeln gelten.

$$a \;\mathbf{quot}\; (-b) = -(a \;\mathbf{quot}\; b) \qquad a \;\mathbf{rem}\; (-b) = a \;\mathbf{rem}\; b$$
$$(-a) \;\mathbf{quot}\; b = -(a \;\mathbf{quot}\; b) \qquad (-a) \;\mathbf{rem}\; b = -(a \;\mathbf{rem}\; b)$$

Wir erhalten im Wesentlichen die gleichen Formeln wie für die rundenden Divisionen, nur dass der Vorzeichenwechsel keinen Funktionswechsel nach sich zieht. Die Formeln für die symmetrische Division sehen im direkten Vergleich attraktiver aus. Aber, wo Licht ist, ist auch Schatten: ***rem*** ist *nicht* periodisch. Man überlegt sich leicht, dass Symmetrie (attraktive Vorzeichenregeln) und Periodizität inkompatibel sind; man kann keinen Divisionsrest definieren, der beide Eigenschaften miteinander vereint: Mit der Vorzeichenregel gilt $(-5) \;\mathbf{rem}\; 3 = -(5 \;\mathbf{rem}\; 3) = -2$; mit der Treppenregel erhalten wir hingegen $(-5) \;\mathbf{rem}\; 3 = (-5 + 6) \;\mathbf{rem}\; 3 = 1$.

Euklidische Division Legt man auf einen periodischen Divisionsrest Wert, gibt es neben ***div*** und $\overline{\mathbf{div}}$ eine weitere Option, die sogenannte ***euklidische Division***. Für positive Divisoren verhält sich ***ediv*** wie ***div***, für negative wie $\overline{\mathbf{div}}$.

$$a \;\mathbf{ediv}\; b := \operatorname{sign} b \cdot \lfloor a / \operatorname{abs} b \rfloor = \operatorname{sign} b \cdot a \;\; \mathbf{div} \;\; \operatorname{abs} b \tag{B.69a}$$
$$a \;\mathbf{emod}\; b := a - (a \;\mathbf{ediv}\; b) \cdot b = a \;\; \mathbf{mod} \;\; \operatorname{abs} b \tag{B.69b}$$

Daraus folgt, dass der Divisionsrest nichtnegativ ist.

$$0 \leqslant a \;\mathbf{emod}\; p < \operatorname{abs} p$$

Diese Eigenschaft legt zusammen mit der Divisionsregel (B.48a) die Funktionen ***ediv*** und ***emod*** eindeutig fest.

Theorie und Praxis Einige, wenige Programmiersprachen bieten alle Varianten der ganzzahligen Division an. F# gehört leider nicht dazu: Von Haus aus gibt es nur die hardware-nahe, symmetrische Variante, notiert $a \div p$ und $a \,\%\, p$. Wir haben gesehen, dass sich alle Varianten in Abhängigkeit vom Vorzeichen der Operanden auf $\lceil a/p \rceil$ und $\lfloor a/p \rfloor$ zurückführen lassen — und umgekehrt. Steht in einer Sprache nur eine Variante zur Verfügung, bleibt einem nichts anderes übrig, als die andere zu programmieren. Zum Beispiel lassen sich ***div*** und ***mod*** in F# unter Verwendung von (B.66) wie folgt realisieren.

```
let divMod a p =
  let q = a ÷ p
  let r = a % p
  if sign r = -sign p then (q - 1, r + p)      // sign p <> 0
                      else (q, r)
let div a p     = fst (divMod a p)
let (mod) a p = snd (divMod a p)               // mod ist ein Infixoperator
```

Das Ergebnis der symmetrischen Division muss korrigiert werden, wenn die Division nicht glatt aufgeht ($a/p \notin \mathbb{Z}$), also der Rest von Null verschieden ist ($r \neq 0$), *und* sich die Vorzeichen der Operanden unterscheiden ($\operatorname{sign} a = -\operatorname{sign} p$). Die Implementierung nutzt aus, dass sich beide

Bedingungen zusammenfassen lassen: $\operatorname{sign} r = -\operatorname{sign} p$.

$$
\begin{array}{ll}
 & \operatorname{sign}(a \;\boldsymbol{rem}\; p) = -\operatorname{sign} p \\
\Longleftrightarrow & \quad \{ \text{ Definition Rest (B.68b) und } \operatorname{sign}(\operatorname{abs} a \;\boldsymbol{mod}\; \operatorname{abs} p) = [a/p \notin \mathbb{Z}] \; \} \\
 & \operatorname{sign} a \cdot [a/p \notin \mathbb{Z}] = -\operatorname{sign} p \\
\Longleftrightarrow & \quad \{ \text{ Fallunterscheidung: } p \iff (c \Rightarrow p) \wedge (\neg c \Rightarrow p) \; \} \\
 & (a/p \in \mathbb{Z} \;\Rightarrow\; \operatorname{sign} a \cdot [a/p \notin \mathbb{Z}] = -\operatorname{sign} p) \;\wedge\; (a/p \notin \mathbb{Z} \;\Rightarrow\; \operatorname{sign} a \cdot [a/p \notin \mathbb{Z}] = -\operatorname{sign} p) \\
\Longleftrightarrow & \quad \{ \; p \neq 0 \text{ und damit } \operatorname{sign} p \neq 0 \; \} \\
 & (a/p \in \mathbb{Z} \;\Rightarrow\; \mathit{false}) \;\wedge\; (a/p \notin \mathbb{Z} \;\Rightarrow\; \operatorname{sign} a = -\operatorname{sign} p) \\
\Longleftrightarrow & \quad \{ \text{ Logik: } (c \Rightarrow \mathit{false}) \wedge (\neg c \Rightarrow p) \iff \neg c \wedge p \; \} \\
 & a/p \notin \mathbb{Z} \;\wedge\; \operatorname{sign} a = -\operatorname{sign} p
\end{array}
$$

Sehr subtil!

Fassen wir zusammen: Es existieren mindestens vier verschiedene Varianten der ganzzahligen Division. Implementierungen in Hardware (***quot***) sind symmetrisch, aber nicht periodisch.

Ganzzahlige Division

quot rundet gegen 0 (engl. rounding towards 0); ***$\underline{\text{div}}$*** rundet ab (engl. rounding towards $-\infty$), ***$\overline{\text{div}}$*** rundet auf (engl. rounding towards ∞).

$a \;\boldsymbol{quot}\; p$	$a \leqslant 0$	$a \geqslant 0$
$p > 0$	$\lceil a/p \rceil$	$\lfloor a/p \rfloor$
$p < 0$	$\lfloor a/p \rfloor$	$\lceil a/p \rceil$

Die abrundende, die aufrundende und die Euklidische Division sind im Gegensatz dazu periodisch, aber nicht symmetrisch.

$a \;\boldsymbol{\underline{div}}\; p$	$a \leqslant 0$	$a \geqslant 0$
$p > 0$	$\lfloor a/p \rfloor$	$\lfloor a/p \rfloor$
$p < 0$	$\lfloor a/p \rfloor$	$\lfloor a/p \rfloor$

$a \;\boldsymbol{ediv}\; p$	$a \leqslant 0$	$a \geqslant 0$
$p > 0$	$\lfloor a/p \rfloor$	$\lfloor a/p \rfloor$
$p < 0$	$\lceil a/p \rceil$	$\lceil a/p \rceil$

$a \;\boldsymbol{\overline{div}}\; p$	$a \leqslant 0$	$a \geqslant 0$
$p > 0$	$\lceil a/p \rceil$	$\lceil a/p \rceil$
$p < 0$	$\lceil a/p \rceil$	$\lceil a/p \rceil$

Welche Eigenschaft ist wichtiger? Eine Güterabwägung fällt schwer; im direkten Vergleich wird man der Periodizität Vorrang einräumen, siehe auch Abschnitt B.5.5.

Anwendung: natürliche Quadratwurzel In Abschnitt 3.7 haben wir die natürliche Quadratwurzel in Mini-F# implementiert, einmal mit Hilfe des Peano Entwurfsmusters und ein zweites Mal mit Hilfe des Leibniz Entwurfsmusters. Die Korrektheit beider Implementierungen basiert darauf, dass im Rekursionsschritt das Ergebnis des ursprünglichen Funktionsaufrufs und das Ergebnis des rekursiven Aufrufs um höchstens 1 differieren.

$$0 \leqslant \left\lfloor \sqrt{n+1} \right\rfloor - \left\lfloor \sqrt{n} \right\rfloor \leqslant 1 \qquad\qquad 0 \leqslant \left\lfloor \sqrt{n} \right\rfloor - \left\lfloor \sqrt{n \;\boldsymbol{div}\; 4} \right\rfloor \cdot 2 \leqslant 1$$

Die Ungleichungen bieten eine willkommene Gelegenheit, unsere rechnerischen Fähigkeiten weiter zu trainieren. Fangen wir mit der einfachsten Aussage an — der Schwierigkeitsgrad steigt von links nach rechts. Dass $\lfloor \sqrt{n} \rfloor$ höchstens so groß wie $\lfloor \sqrt{n+1} \rfloor$ ist, folgt aus der Monotonie der

beteiligten Funktionen.

$$
\begin{aligned}
& 0 \leqslant \lfloor\sqrt{n+1}\rfloor - \lfloor\sqrt{n}\rfloor \\
\iff & \quad \{ \text{ additive Inverse } \} \\
& \lfloor\sqrt{n}\rfloor \leqslant \lfloor\sqrt{n+1}\rfloor \\
\impliedby & \quad \{ \text{ Monotonie des Bodens (B.56a) } \} \\
& \sqrt{n} \leqslant \sqrt{n+1} \\
\impliedby & \quad \{ \text{ Monotonie der Wurzel } \} \\
& n \leqslant n+1
\end{aligned}
$$

Die obere Schranke ist ebenfalls nicht allzu schwer nachzuweisen.

$$
\begin{aligned}
& \lfloor\sqrt{n+1}\rfloor - \lfloor\sqrt{n}\rfloor \leqslant 1 \\
\iff & \quad \{ \text{ additive Inverse } \} \\
& \lfloor\sqrt{n+1}\rfloor \leqslant \lfloor\sqrt{n}\rfloor + 1 \\
\iff & \quad \{ \text{ Boden und Addition (B.59) } \} \\
& \lfloor\sqrt{n+1}\rfloor \leqslant \lfloor\sqrt{n}+1\rfloor \\
\impliedby & \quad \{ \text{ Monotonie des Bodens (B.56a) } \} \\
& \sqrt{n+1} \leqslant \sqrt{n}+1
\end{aligned}
\qquad
\begin{aligned}
& \sqrt{a^2+b^2} \leqslant a+b \\
\iff & \quad \{ \text{ Quadratwurzel } \} \\
& a^2+b^2 \leqslant (a+b)^2 \\
\iff & \quad \{ \text{ binomische Formel } \} \\
& a^2+b^2 \leqslant a^2+2\cdot a\cdot b+b^2 \\
\iff & \quad \{ \text{ additive Inverse } \} \\
& 0 \leqslant a\cdot b
\end{aligned}
$$

Die finale Ungleichung folgt aus der Hilfsrechnung mit $a := \sqrt{n}$ und $b := 1$.

Die beiden anderen Ungleichungen stellen uns vor eine größere Herausforderung, da Böden dort geschachtelt vorkommen: Wenn wir die ganzzahlige auf die reelle Division zurückführen, erhalten wir die Formel $0 \leqslant \lfloor\sqrt{n}\rfloor - \left\lfloor\sqrt{\lfloor n/4\rfloor}\right\rfloor \cdot 2 \leqslant 1$ — im Subtrahenden wird sowohl das Argument als auch das Ergebnis der Wurzelfunktion abgerundet. Die Ungleichungen erinnern an die Eigenschaft des Divisionsrests: $0 \leqslant a - \lfloor a/2\rfloor \cdot 2 < 2$. Wenn wir $a := \lfloor\sqrt{n}\rfloor$ setzen, müssen wir $\lfloor\sqrt{\lfloor n/4\rfloor}\rfloor = \lfloor\lfloor\sqrt{n}\rfloor/2\rfloor$ zeigen. Versuchen wir uns an einem indirekten Beweis — um zielgerichtet vorgehen zu können, fangen wir an »beiden Enden« gleichzeitig an (Rechnung links und Rechnung rechts).

$$
\begin{aligned}
& z \leqslant \left\lfloor\sqrt{\lfloor n/4\rfloor}\right\rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& z \leqslant \sqrt{\lfloor n/4\rfloor} \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Quadratwurzel und } z \geqslant 0 \} \\
& z^2 \leqslant \lfloor n/4\rfloor \text{ in } \mathbb{R} \\
\iff & \quad \{ \, z^2 \in \mathbb{Z} \, \} \\
& z^2 \leqslant \lfloor n/4\rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& z^2 \leqslant n/4 \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Arithmetik } \} \\
& z^2 \cdot 4 \leqslant n \text{ in } \mathbb{R}
\end{aligned}
\qquad
\begin{aligned}
& z \leqslant \left\lfloor\left\lfloor\sqrt{n}\right\rfloor/2\right\rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& z \leqslant \lfloor\sqrt{n}\rfloor/2 \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Arithmetik } \} \\
& z \cdot 2 \leqslant \lfloor\sqrt{n}\rfloor \text{ in } \mathbb{R} \\
\iff & \quad \{ \, z \cdot 2 \in \mathbb{Z} \, \} \\
& z \cdot 2 \leqslant \lfloor\sqrt{n}\rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& z \cdot 2 \leqslant \sqrt{n} \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Quadratwurzel und } z \geqslant 0 \} \\
& z^2 \cdot 4 \leqslant n \text{ in } \mathbb{R}
\end{aligned}
$$

Voilà — indem wir die Variable n schrittweise isolieren, treffen wir uns »in der Mitte.« Zwei Details verdienen dabei besondere Beachtung. Zum Ersten erstreckt sich die Variable z auf die *natürlichen* Zahlen, $z \in \mathbb{N}$, denn nur für positive z sind die Schritte, in denen die Quadratwurzel eliminiert wird, Äquivalenzumformungen. Zum Zweiten protokollieren wir mit dem Zusatz »$\text{ in } \mathbb{Z}$« bzw. »$\text{ in } \mathbb{R}$« pedantisch, welche Ordnung jeweils betrachtet wird. Im mittleren Schritt

überführen wir eine Ungleichung zwischen reellen Zahlen in eine Ungleichung zwischen ganzen Zahlen — die Umformung erfordert, dass z^2 bzw. $z \cdot 2$ eine ganze Zahl ist. Der Wechsel der Ordnung ist notwendig, um auch die eingeschachtelten Böden eliminieren zu können.

Aus dem Beweis lassen sich mit etwas Phantasie allgemeine Eigenschaften der Quadratwurzel und der Division ableiten: In geschachtelten Formeln können innere Böden weggelassen werden.

$$\left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = \left\lfloor \sqrt{x} \right\rfloor \qquad \left\lfloor \lfloor x \rfloor / p \right\rfloor = \lfloor x/p \rfloor \quad \text{für } p \in \mathbb{Z} \text{ und } p > 0 \tag{B.70}$$

Übung B.5.16 fragt nach einem Beweis der Aussagen und diskutiert, unter welchen Bedingungen sich die Eigenschaft auf andere Funktionen verallgemeinern lässt. Zum Beispiel gilt $\left\lfloor \lfloor x \rfloor / p \right\rfloor = \lfloor x/p \rfloor$ nicht für beliebige Divisoren; für $p := \frac{1}{2}$ ist zum Beispiel die linke Seite echt kleiner: $\left\lfloor \lfloor \frac{1}{2} \rfloor \cdot 2 \right\rfloor = 0 < 1 = \lfloor \frac{1}{2} \cdot 2 \rfloor$.

Übungen.

11. Drücken Sie das Maximum zweier Zahlen mit Hilfe des Minimums aus und umgekehrt.

12. Zeigen Sie die Vorzeichenregeln (B.64a) und (B.64b).

13. Die folgenden Vorzeichenregeln sind dem Artikel »The Euclidean definition of the functions div and mod« von Raymond T. Boute entnommen. Zeigen Sie die Aussagen.

$$a \ \textbf{\textit{div}} \ (-b) = -(a \ \textbf{\textit{div}} \ b) - [a/b \notin \mathbb{Z}] \qquad a \ \textbf{\textit{mod}} \ (-b) = a \ \textbf{\textit{mod}} \ b - [a/b \notin \mathbb{Z}] \cdot b$$
$$(-a) \ \textbf{\textit{div}} \ b = -(a \ \textbf{\textit{div}} \ b) - [a/b \notin \mathbb{Z}] \qquad (-a) \ \textbf{\textit{mod}} \ b = [a/b \notin \mathbb{Z}] \cdot b - a \ \textbf{\textit{mod}} \ b$$

14. Beweisen Sie die Umrechnungsformeln (B.66).

15. Wikipedia schreibt: »Steht in einer Sprache wie C(++) oder Java nur die symmetrische Variante zur Verfügung, kann man Ergebnisse nach der mathematischen Variante erhalten mit:

$$a \ \textbf{\textit{mod}} \ b = ((a \,\%\, b) + b) \,\%\, b$$

wobei % die symmetrische Modulooperation bezeichnet und ***mod*** die mathematische.« Mit mathematischer[18] Modulooperation ist hier der Rest der abrundenden Division gemeint. Einen Beweis bleibt Wikipedia schuldig; füllen Sie die Lücke.

16. Unter bestimmten Bedingungen können in geschachtelten Formeln innere Böden bzw. innere Decken entfallen.

(a) Beweisen Sie die entsprechenden Eigenschaften der Quadratwurzel (B.70) und der ganzzahligen Division, $\lfloor x \rfloor$ ***div*** $p = x$ ***div*** p, mittels indirekter Beweise.

(b) Verwenden Sie die Eigenschaften, um $\left\lfloor \sqrt{\lfloor n/4 \rfloor} \right\rfloor = \left\lfloor \lfloor \sqrt{n} \rfloor / 2 \right\rfloor$ mit einem direkten Gleichheitsbeweis zu zeigen.

(c) Zeigen Sie die folgende Verallgemeinerung von (B.70), indem Sie die Beweise aus Teil (a) verallgemeinern. Sei f eine stetige und streng monoton wachsende Funktion mit der Eigenschaft, dass ganzzahlige Funktionswerte ganzzahlige Argumente bedingen: $f(x) \in \mathbb{Z} \Longrightarrow x \in \mathbb{Z}$. Unter diesen Voraussetzungen können innere Böden bzw. innere Decken entfallen:

$$\left\lfloor f(\lfloor x \rfloor) \right\rfloor = \lfloor f(x) \rfloor \qquad \left\lceil f(\lceil x \rceil) \right\rceil = \lceil f(x) \rceil \tag{B.71}$$

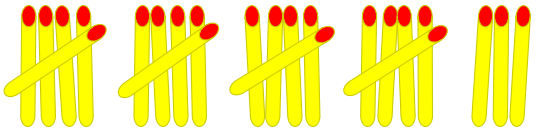
(d) Vergewissern Sie sich, dass $g(x) := \sqrt{x}$ und $h(x) := x/p$ mit $p \in \mathbb{Z}$ und $p > 0$ den Anforderungen genügen.

(e) Welche Eigenschaften erfüllt eigentlich die streng monoton *fallende* Funktion $h(x) := x/p$ mit $p \in \mathbb{Z}$ und $p < 0$?

[18] Das Adjektiv »mathematisch« soll wohl andeuten, dass die abrundende Division aus mathematischer Sicht besonders elegant ist. Die symmetrische Variante ist natürlich nicht weniger »mathematisch« als die abrundende Division — auch sie genießt eine präzise mathematische Definition.

B.5.3. Stellenwertsysteme\Zahlendarstellungen

Wenn wir rechnen, dann arbeiten wir mit ***Zahlenrepräsentationen***, mit konkreten Darstellungen der abstrakten Größen. Aufgrund des Ursprungs im Zählen waren die ersten Zahlendarstellungen sicherlich ***unär***: Die Zahl dreiundzwanzig wird durch dreiundzwanzig »Dinge« repräsentiert, durch dreiundzwanzig Einkerbungen in einem Knochen, durch dreiundzwanzig Striche an der Höhlenwand oder durch ebendiese Zahl an Hölzern. Vielleicht hat man die »Dinge« gruppiert, um nicht den Überblick zu verlieren.

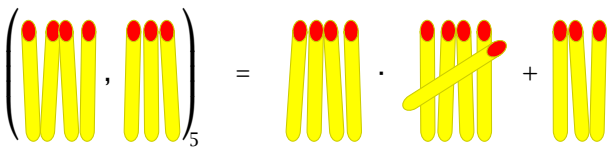


Auch Peano hat die natürlichen Zahlen auf Basis eines unären Zahlensystems formalisiert, siehe Abbildung B.10: Die Zahl dreiundzwanzig wird durch eine entsprechende Zahl von Anwendungen der Nachfolgerfunktion auf die Null repräsentiert.

$$s(s(s(s(s(\ s(s(s(s(s(\ s(s(s(s(s(\ s(s(s(s(s(\ s(s(s(0)))))))))))))))))))))$$

Der Nachteil der unären Darstellung liegt auf der Hand: Sie skaliert schlecht — Dutzende von Hölzern lassen sich noch handhaben, nicht aber Tausende oder gar Millionen.

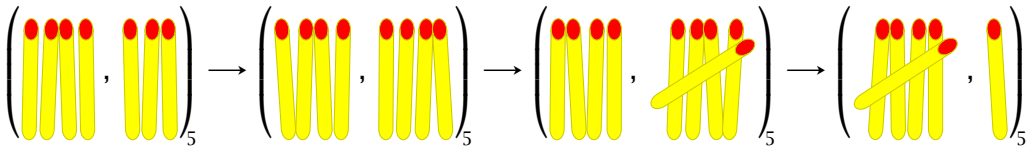
Man kann sich behelfen, indem man die Hölzer wie oben gruppiert und dann — das ist die zündende Idee — die 5er-Gruppen zählt: dreiundzwanzig wird durch *vier* 5er-Gruppen und *drei* weitere Hölzer repräsentiert, also $23 = 4 \cdot 5 + 3 = (4,3)_5$. Interessant: Die Multiplikation betritt die Bühne.



Wenn man die maximale Haufengröße auf fünf beschränkt, lassen sich mit zwei Haufen Zahlen bis $5 \cdot 5 + 5 = 30$ repräsentieren. Erlaubt man, dass der linke Haufen mehr als 5 Hölzer umfasst, dann wird die Darstellung mit zunehmender Anzahl erneut unübersichtlich. Die Lösung liegt auf der Hand: Man wendet den Gruppierungstrick ein weiteres Mal an, mit dem kleinen Unterschied, dass der neu hinzugekommene Haufen 25er-Gruppen zählt: Aus $(23,3)_5$ wird so $(4,3,3)_5$. Erlaubt man drei Haufen von jeweils maximal fünf Hölzern, erhält man Darstellungen der Zahlen bis $(5 \cdot 5 + 5) \cdot 5 + 5 = 155$, zum Beispiel $123 = (4 \cdot 5 + 4) \cdot 5 + 3 = (4,4,3)_5$. Man sieht, die gleiche Haufengröße hat in Abhängigkeit von ihrer Position eine unterschiedliche Bedeutung, ein unterschiedliches Gewicht: Die erste vier zählt $4 \cdot 5^2 = 100$, die zweite nur $4 \cdot 5^1 = 20$ — wir erhalten ein positionelles Zahlensystem oder ***Stellenwertsystem*** zur Basis 5.

Eine natürliche Zahl wird im »quinären Streichholzsystem« durch eine *Folge* von Haufen repräsentiert, wobei jeder Haufen zwischen einem und fünf Hölzer enthält. Und die Zahl 0? Die natürlichste aller natürlichen Zahlen wird konsequenterweise durch die *leere* Folge repräsentiert. (Für menschliche Rechner stellt das oft ein Problem dar, für maschinelle aber nicht.) Das quinäre System hat den Vorteil, große Zahlen kompakt darstellen zu können — die Anzahl der Haufen vermittelt sehr direkt einen Eindruck von der Größenordnung der dargestellten Zahl. Allerdings gestaltet sich das Zählen schwieriger, der Übergang von einer natürlichen Zahl zur nächsten. Im unären Streichholzsystem haben wir einfach ein Streichholz hinzugefügt — fertig. Im quinären System müssen wir uns etwas mehr anstrengen: Aus der 23 wird die 24 und dann die 25, indem

wir jeweils ein Holz zum Haufen ganz rechts hinzufügen.



Enthält der Haufen ganz rechts aber bereits fünf Hölzer, dann ersetzen wir ihn durch ein Streichholz und inkrementieren die weiter links stehenden Haufen *auf die gleiche Art und Weise.* Also, ein Streichholz wird zum linken Nachbarhaufen hinzugefügt, es sei denn, dieser enthält bereits fünf Hölzer usw. So wird zum Beispiel aus $(4,5,5)_5$ die Folge $(5,1,1)_5$ und aus $(5,5,5)_5$ die Folge $(1,1,1,1)_5$ — aus einem nicht-existenten Haufen wird im letzten Schritt ein einelementiger Haufen. Unten sind zur Illustration die Codierungen der Zahlen von $0 = ()_5$ bis $50 = (1,4,5)_5$ aufgeführt (da keine Verwechslungsgefahr besteht, haben wir die Kommata zwischen den Ziffern weggelassen).

$()_5$ $(1)_5$ $(2)_5$ $(3)_5$ $(4)_5$ $(5)_5$ $(11)_5$ $(12)_5$ $(13)_5$ $(14)_5$ $(15)_5$
$(21)_5$ $(22)_5$ $(23)_5$ $(24)_5$ $(25)_5$ $(31)_5$ $(32)_5$ $(33)_5$ $(34)_5$ $(35)_5$
$(41)_5$ $(42)_5$ $(43)_5$ $(44)_5$ $(45)_5$ $(51)_5$ $(52)_5$ $(53)_5$ $(54)_5$ $(55)_5$
$(111)_5$ $(112)_5$ $(113)_5$ $(114)_5$ $(115)_5$ $(121)_5$ $(122)_5$ $(123)_5$ $(124)_5$ $(125)_5$
$(131)_5$ $(132)_5$ $(133)_5$ $(134)_5$ $(135)_5$ $(141)_5$ $(142)_5$ $(143)_5$ $(144)_5$ $(145)_5$

Man sieht, dass sich für jede natürliche Zahl eine Streichholzrepräsentation konstruieren lässt — das oben skizzierte Zählverfahren lässt sich als *konstruktiver Beweis* für die Vollständigkeit des Zahlensystems ansehen.

Stellenwertsysteme

Die Arithmetik *unbeschränkt* großer Zahlen wird auf die Arithmetik *beschränkt* großer Ziffern zurückgeführt — Algorithmen am Werk.

Man sieht aber auch, dass das Zählen komplizierter wird. Aus einem einfachen Schritt im unären System wird eine Abfolge von Schritten im quinären System. Das Ergebnis der Überlegungen ist ein Algorithmus, eine Rechenvorschrift, die pedantisch befolgt werden muss — die Geburtsstunde der Informatik. Mit den Zahlen kamen die Zahlensysteme und mit ihnen die Algorithmen. Der Hinweis »auf die gleiche Art und Weise« zeigt übrigens an, dass es sich um eine ***rekursive*** Rechenvorschrift handelt.

Haben Sie es bemerkt? Wir kommen beim Zählen in unserem Zahlensystem ohne leere Haufen, also ohne die Ziffer 0 aus. (Verwendet man tatsächlich Haufen und Hölzer zum Zählen, dann sind leere Haufen problematisch, da man sie schlicht und einfach nicht sieht.) Das quinäre Streichholzsystem ist eine sogenannte »0-freie« Repräsentation (engl. zeroless representation). Im Unterschied dazu ist das uns so wohlvertraute Dezimalsystem eine »0-haltige« Repräsentation: Basierend auf der Basis 10 verwendet es neben den »sichtbaren« Ziffern ৭২৩৪৫৬৭৮৯ bzw. 123456789 die »unsichtbare« Ziffer ০ bzw. 0. Am Anfang ihrer Geschichte war die Ziffer 0 tatsächlich eine Leerstelle; erst im Laufe der Zeit wurde aus dem leeren Platz ein kleiner Punkt und dann ein ordentliches Symbol. (Leerstellen sind problematisch, da man eine Leerstelle schlecht von zwei oder drei aufeinanderfolgenden Leerstellen unterscheiden kann.)

Unser quintäres Zahlensystem hat die angenehme Eigenschaft, dass jede natürliche Zahl eine *eindeutige* Darstellung besitzt. Daraus folgt, dass zwei Folgen von Haufen die gleiche natürliche Zahl repräsentieren, wenn sie die gleichen Haufen in der gleichen Reihenfolge enthalten. Die semantische Gleichheit von Zahlen lässt sich somit auf die syntaktische Gleichheit ihrer Repräsentationen zurückführen. Das ist nicht so offensichtlich, wie man vielleicht denkt. Erlaubt man zum Beispiel 6er-Haufen, dann erhält man ein sogenanntes ***redundantes*** Zahlensystem: Die Zahl 11 wird zum Beispiel sowohl von $(2,1)_5$ als auch von $(1,6)_5$ repräsentiert.

Versuchen wir uns an einem Beweis, dass das quinäre Streichholzsystem irredundant ist. Eine nicht-leere Ziffernfolge bezeichnet die Zahl $5 \cdot n + d$, wobei d der Wert der letzten Ziffer und n der Wert der restlichen Ziffernfolge ist. Da $d > 0$, ist die dargestellte Zahl ebenfalls positiv. Daraus folgt, dass die Zahl 0 eine eindeutige Repräsentation besitzt, die leere Ziffernfolge. (Im Dezimalsystem hat die Null hingegen viele verschiedene Repräsentationen: $()_{10}$, $(0)_{10}$, $(00)_{10}$ usw.) Wenden wir uns den positiven Zahlen zu und nehmen an, es gäbe zwei Darstellungen der gleichen positiven Zahl:

$$5 \cdot n_1 + d_1 = 5 \cdot n_2 + d_2$$

Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $n_1 \leqslant n_2$. Gemäß der Definition der Ordnung (B.34) gibt es ein d, so dass $n_1 + d = n_2$.

$$\begin{aligned}
& 5 \cdot n_1 + d_1 = 5 \cdot n_2 + d_2 \\
\iff & \quad \{ \text{ Annahme: } n_1 + d = n_2 \ \} \\
& 5 \cdot n_1 + d_1 = 5 \cdot (n_1 + d) + d_2 \\
\iff & \quad \{ \text{ Distributivgesetz } \} \\
& 5 \cdot n_1 + d_1 = 5 \cdot n_1 + 5 \cdot d + d_2 \\
\iff & \quad \{ \text{ - + } p \text{ ist injektiv } \} \\
& d_1 = 5 \cdot d + d_2 \\
\implies & \quad \{ \ d_1, d_2 \in \{1, \ldots, 5\} \ \} \\
& d = 0 \ \wedge \ d_1 = d_2
\end{aligned}$$

Wenn $d_1 = d_2$ gilt, muss auch $n_1 = n_2$ gelten, da - + p und - · q (für $q \neq 0$) injektiv sind. Damit ist die Eindeutigkeit der Darstellung gezeigt. (Sind auch 6-er Haufen zulässig, dann scheitert der letzte Beweisschritt, da $6 = 5 \cdot 1 + 1$.)

Je nachdem, wieviele Hölzer wir pro Haufen zulassen, ergeben sich verschiedene Zahlensysteme mit unterschiedlichen Eigenschaften:

- $0 \leqslant d \leqslant 4$: redundant; nur eindeutig, wenn man führende Nullen verbietet;
- $1 \leqslant d \leqslant 5$: irredundant;
- $2 \leqslant d \leqslant 6$: irredundant, aber unvollständig: 7, 8 usw. lassen sich nicht darstellen;
- $0 \leqslant d \leqslant 5$: redundant: 5, 10 usw. haben verschiedene Darstellungen;
- $1 \leqslant d \leqslant 6$: redundant: 6, 11 usw. haben verschiedene Darstellungen.

Vollständig sollten Zahlensysteme sein, irredundant nicht unbedingt: Es gibt interessante und wichtige Anwendungen für redundante Zahlensysteme.

Stellenwertsysteme In einem ***Stellenwertsystem*** oder positionellen Zahlensystem werden natürliche Zahlen durch Folgen von Ziffern $d_{k-1}, \ldots, d_0$ repräsentiert. Die Ziffern werden aus einer festgelegten Menge $D \subseteq \mathbb{N}$ entnommen. Jede Ziffer $d_i \in D$ hat gemäß ihrer Position eine Wertigkeit, die durch eine ***Basis*** $b \in \mathbb{N}$ festgelegt wird. Die Bedeutung der Ziffernfolge lässt sich wahlweise rekursiv oder iterativ festlegen.[19]

$$\begin{aligned}
()_b &= 0 \\
(ds, d)_b &= (ds)_b \cdot b + d
\end{aligned}
\qquad\qquad
(d_{k-1}, \ldots, d_0)_b = \sum_{i=0}^{k-1} d_i \cdot b^i \tag{B.72}$$

[19] Die rekursive Vorschrift auf der linken Seite nennt man auch ***Hornerschema***, benannt nach dem englischen Mathematiker William George Horner (1786–1837).

Ist die Bedeutungsfunktion injektiv, dann heißt das Zahlensystem (festgelegt durch die Ziffernmenge D und die Basis b) irredundant, anderenfalls ***redundant***. Ist die Bedeutungsfunktion surjektiv, dann heißt das Zahlensystem ***vollständig***.

Ein technisches Detail: In der oben vereinbarten Darstellung steht die ***höchstwertige Ziffer*** (engl. most significant digit) ganz links und die ***niedrigstwertige*** (engl. least significant digit) entsprechend ganz rechts — eine willkürliche Festlegung. Je nach Kontext sind unterschiedliche Konventionen gebräuchlich: Dezimalzahlen starten mit der höchstwertigen Ziffer; für Binärzahlen (siehe unten) sind beide Formate gebräuchlich (in der Computertechnik spricht man auch von »bit order« oder »endianness«); im Englischen kommen beide Varianten gleichzeitig zum Einsatz: 17 schreibt man seventeen, 47 aber fourty-seven; bei größeren Zahlen wird im Englischen wie im Deutschen bunt gemischt: 547 als fünfhundert(und)siebenundvierzig und 517 als five hundred and seventeen. (Haben Sie sich jemals gefragt, warum Ihnen das Erlernen der Zahlwörter so große Mühe bereitet hat?)

Wieviele Ziffern man braucht, um die natürliche Zahl n darzustellen, hängt von der Basis b und vom Ziffernvorrat D ab. Wenn wir annehmen, dass $b-1$ die größte, verfügbare Ziffer ist, ergibt sich folgende Abschätzung.

$$
\begin{aligned}
& n \leqslant \sum_{i=0}^{k-1} (b-1) \cdot b^i \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ geometrische Reihe, siehe auch Abbildung 5.10 } \} \\
& n \leqslant b^k - 1 \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse: Addition und Subtraktion } \} \\
& n + 1 \leqslant b^k \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse: Logarithmus und Exponentialfunktion und } n \geqslant 0 \} \\
& \log_b(n+1) \leqslant k \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Decke (B.54b) } \} \\
& \lceil \log_b(n+1) \rceil \leqslant k \text{ in } \mathbb{Z}
\end{aligned}
$$

Um n darzustellen, genügen somit $\lceil \log_b(n+1) \rceil$ Ziffern.

Viele verschiedene Basen sind oder waren im Laufe der Menschheitsgeschichte gebräuchlich.

- unär ($b = 1$): Das erste und einfachste Zahlensystem (Einkerbungen in einem Knochen, Striche an der Höhlenwand) haben wir bereits diskutiert.

- binär ($b = 2$): Das Binärsystem, das mit den digitalen Rechnern seinen Siegeszug angetreten hat, wird allgemein dem Universalgelehrten Gottfried Wilhelm Leibniz (1646–1716) zugeschrieben, siehe auch Abbildung 3.7. Die Idee ist aber jahrtausendealt und findet sich bereits in alten indischen und chinesischen Schriften.

  Stellenwertsysteme reduzieren Addition und Multiplikation von Zahlen auf die korrespondierenden Operationen für Ziffern. Führt man die Operationen von Hand aus, muss man sich, neben dem eigentlichen Algorithmus, Summen und Produkte von Ziffern merken — erinnern Sie sich noch, wie Sie in der Grundschule Additions- und Multiplikationstafeln für das Dezimalsystem auswendig gelernt haben? Tafeln mit $10 \cdot 10 = 100$ Einträgen. Aus dem Blickwinkel der Erlernbarkeit ist das Binärsystem wesentlich bequemer, da man nur Tafeln mit $2 \cdot 2 = 4$ Einträgen memorieren muss.

+	0	1
0	0	1
1	1	10

·	0	1
0	0	0
1	0	1

Einen kleinen Preis zahlt man für die Bequemlichkeit: Binärzahlen sind mehr als dreimal so lang wie Dezimalzahlen, da $\log 10/\log 2 \approx 3.322$. Die Binärdarstellung von 1000000 umfasst 20 Ziffern: $(11110100001001000000)_2$.

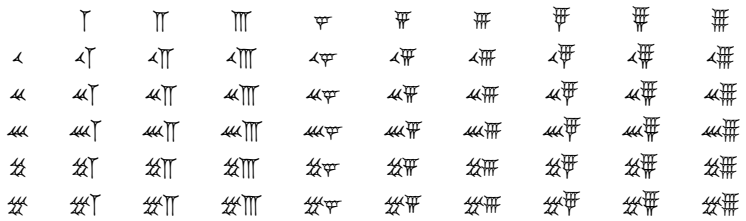
- quinär ($b = 5$): Das Zahlensystem der Wahl, wenn man Ziffern durch die Finger einer Hand darstellen möchte (siehe auch Abbildung B.11).

- oktal ($b = 8$): Oktalzahlen werden oft als kompakte Darstellungen von Binärzahlen verwendet: Da $8 = 2^3$, lassen sich drei Binärziffern durch eine Oktalziffer kodieren, zum Beispiel $(11\,110\,100\,001\,001\,000\,000)_2 = (3641100)_8$.

- dezimal ($b = 10$): Das Zahlensystem der Wahl, wenn man Ziffern durch die Finger zweier Hände darstellen möchte.

- hexadezimal oder sedezimal ($b = 16$): Wie Oktalzahlen werden auch Hexadezimalzahlen gerne als Darstellungen von Binärzahlen verwendet: Da $16 = 2^4$, lassen sich vier Binärziffern zu einer Hexadezimalziffer zusammenfassen, zum Beispiel $(1111\,0100\,0010\,0100\,0000)_2 = (15, 4, 2, 4, 0)_{16}$. (Ein technisches Detail: Um die Kommata auslassen zu können, werden die Ziffern von 10 bis 15 oft durch die Buchstaben von A bis F notiert, also $1000000 = (\mathtt{F4240})_{16}$.)

- sexagesimal ($b = 60$): Haben Sie sich jemals gefragt, warum eine Stunde 60 Minuten hat und eine Minute 60 Sekunden? Die Einteilung geht auf das sexagesimale Stellenwertsystem der Sumerer und Babylonier zurück. Basis 60 — wow! Interessanterweise haben die Babylonier aber nicht 60 grundverschiedene Zeichen verwendet — 60 grundverschiedene Symbole sind schwer zu memorieren. Vielmehr besteht jede Ziffer aus zwei Komponenten:



  Die babylonischen Ziffern setzen sich aus zwei Dezimalziffern zusammen, die ihrerseits unär mit verschiedenen »Keilen« codiert werden: Zum Beispiel wird die *Ziffer* 37 durch » 𒌋𒐗 « dargestellt. Da unterschiedliche Keile für 10-er und 1-er Positionen verwendet werden, lassen sich die Ziffern problemlos zu Zahlen aneinanderreihen, zum Beispiel $4711 = (1 \cdot 60 + 18) \cdot 60 + 31$ besteht aus den drei Ziffern 1, 18 und 31, in Keilnotation » 𒐕 𒌋𒐗 𒌋𒐕 «.

  Na ja, fast problemlos. Da die Babylonier kein Symbol für die Ziffer 0 haben, wird diese durch eine Leerstelle repräsentiert mit den schon erwähnten Problemen. Erkennen Sie den Unterschied zwischen » 𒁹𒐕 𒐕 « und » 𒁹𒐕 𒐕 «? Die erste Ziffernfolge ist $(11, 0, 1)_{60}$, die zweite $(11, 0, 0, 1)_{60}$.

- gigantär $b = 4294967296$ oder $b = 18446744073709551616$: Die Hardware eines Computers rechnet von Haus aus nur mit beschränkter Genauigkeit (mehr dazu in Abschnitt B.5.5). Arithmetik mit beliebiger Genauigkeit, also das Rechnen mit den natürlichen oder den ganzen Zahlen, wird in Software realisiert. Zur Erinnerung: Stellenwertsysteme reduzieren Addition und Multiplikation von beliebig großen *Zahlen* auf korrespondierende Operationen für eine begrenzte Anzahl von *Ziffern*. So werden die hardware-seitig verfügbaren *Zahlen*, $2^{32} = 4294967296$ oder $2^{64} = 18446744073709551616$ an der Zahl, software-seitig als *Ziffern* verwendet — die Babylonier haben es vorgemacht. Die Rechengenauigkeit wird auf

```
type Digit =  | I | II | III | IIII | IIIII
type Quinary = Digit list
let rec succ : Quinary → Quinary = function
  | [ ]        → [I]
  | I    :: ds → II    :: ds
  | II   :: ds → III   :: ds
  | III  :: ds → IIII  :: ds
  | IIII :: ds → IIIII :: ds
  | IIIII :: ds → I    :: succ ds      // Übertrag (engl. carry)
let rec natural : Quinary → Nat = function
  | [ ]        → 0
  | I    :: ds → 1 + 5 * natural ds
  | II   :: ds → 2 + 5 * natural ds
  | III  :: ds → 3 + 5 * natural ds
  | IIII :: ds → 4 + 5 * natural ds
  | IIIII :: ds → 5 + 5 * natural ds
let rec quinary (n : Nat) : Digit list =
  if n = 0 then [ ]
           else let r = n % 5 in
                if   r = 1   then I    :: quinary (n ÷ 5)
                elif r = 2   then II   :: quinary (n ÷ 5)
                elif r = 3   then III  :: quinary (n ÷ 5)
                elif r = 4   then IIII :: quinary (n ÷ 5)
                (* r = 0 *) else IIIII :: quinary (n ÷ 5 - 1)
```

Abbildung B.11.: Das quinäre Streichholzsystem in Mini–F#.

diese Weise lediglich durch den verfügbaren Speicherplatz beschränkt — Rechnungen mit exorbitanten Größen wie der Zahl der Atome im sichtbaren Weltall oder der Anzahl der Nanosekunden seit dem Urknall gehen aber flott von der Hand.

Zahlenumwandlung\Konvertierung Die Vielfalt an verschiedenen Zahlensystemen hat ihren Preis: Sind mehrere Systeme im Einsatz, muss man sich darum kümmern, verschiedene Darstellungen ineinander zu überführen. Konvertierungen werden zum Beispiel bei Ausgaben vorgenommen: Der Computer rechnet zwar binär, aber da wir uns so an das Dezimalsystem gewöhnt haben, werden Binärzahlen in der Regel als Dezimalzahlen ausgegeben. Allgemein stellt sich die Aufgabe, eine Darstellung zur Basis b und Ziffernmenge D in eine äquivalente Darstellung zur Basis b' und Ziffernmenge D′ zu überführen.

Im Folgenden nehmen wir vereinfachend an, dass »kanonische« Ziffermengen vorliegen: $D = \{0, \ldots, b-1\}$ und $D' = \{0, \ldots, b'-1\}$. Im einfachsten Fall ist eine Basis eine natürliche Potenz der anderen Basis: $b^k = b'$. Dann ist die Zahlenkonvertierung ein Klacks, ein »no-brainer": k aufeinanderfolgende Ziffern im b-adischen System entsprechen einer Ziffer im b'-adischen System. In der Anfangszeit des maschinellen Rechnens hat man Binärzahlen oft kompakt als Oktal- oder Hexadezimalzahlen notiert und dabei auf Tabellen wie die folgende zurückgegriffen (bin steht

abkürzend für binär, $b = 2$, okt für oktal, $b = 2^3$, und hex für hexadezimal, $b = 2^4$).

bin	okt	hex	bin	okt	hex	bin	okt	hex	bin	okt	hex
000	0	0	100	4	4	1000	10	8	1100	14	C
001	1	1	101	5	5	1001	11	9	1101	15	D
010	2	2	110	6	6	1010	12	A	1110	16	E
011	3	3	111	7	7	1011	13	B	1111	17	F

Eine Oktalzahl bestehend aus m Ziffern wird binär durch $3 \cdot m$ Ziffern repräsentiert. Umgekehrt korrespondiert eine n-ziffrige Binärzahl zu einer Oktalzahl mit $\lceil n/3 \rceil$ Ziffern.

Sind die Basen nicht so direkt miteinander verbandelt, müssen wir uns etwas mehr abstrampeln und anfangen zu rechnen. Man unterscheidet zwei prinzipielle Verfahren:

$$\text{b-adisch} \xRightarrow{\text{Multiplikationsverfahren}} \mathbb{N} \xRightarrow{\text{Divisionsverfahren}} \text{b-adisch}$$

Wir können eine b-adische Zahl in ein *beliebiges* anderes Zahlensystem überführen und umgekehrt, wenn wir in ebendiesem System rechnen können — oben steht $\mathbb{N}$ stellvertretend für ein solches Zahlensystem. Das ***Multiplikationsverfahren*** kennen wir schon: Es ist ein anderer Name für die ***Bedeutungsfunktion*** (B.72), mit der wir die Semantik einer Ziffernfolge festlegt haben. Das ***Divisionsverfahren*** ist nichts anderes als die Umkehrung der Bedeutungsfunktion, ihre Linksinverse. Konkret: Die Bedeutung des quinären Numerals $(102421)_5$ berechnet sich nach dem Hornerschema wie folgt.

$$(102421)_5 = (((((0 \cdot 5 + 1) \cdot 5 + 0) \cdot 5 + 2) \cdot 5 + 4) \cdot 5 + 2) \cdot 5 + 1 = 3486$$

Machen wir die Teilrechnungen explizit, ergibt sich die Abfolge von Schritten unten links.

$$\begin{array}{rrrrrr}
| & 0 \cdot 5 + | & = 1 & 3486 \;\boldsymbol{div}\; 5 = 697 & 3486 \;\boldsymbol{mod}\; 5 = & | \\
 & 1 \cdot 5 + & = 5 & 697 \;\boldsymbol{div}\; 5 = 139 & 697 \;\boldsymbol{mod}\; 5 = & || \\
|| & 5 \cdot 5 + || & = 27 & 139 \;\boldsymbol{div}\; 5 = 27 & 139 \;\boldsymbol{mod}\; 5 = & |||| \\
|||| & 27 \cdot 5 + |||| & = 139 & 27 \;\boldsymbol{div}\; 5 = 5 & 27 \;\boldsymbol{mod}\; 5 = & || \\
|| & 139 \cdot 5 + || & = 697 & 5 \;\boldsymbol{div}\; 5 = 1 & 5 \;\boldsymbol{mod}\; 5 = & \\
| & 697 \cdot 5 + | & = 3486 & 1 \;\boldsymbol{div}\; 5 = 0 & 1 \;\boldsymbol{mod}\; 5 = & |
\end{array}$$

In jedem Schritt wird das Teilergebnis mit der Basis multipliziert und die jeweilige Ziffer hinzuaddiert — daher der Name Multiplikationsverfahren. Um umgekehrt eine Zahl in das quinäre System zu überführen, wenden wir die Schritte in umgekehrter Reihenfolge an, dabei wird aus der Multiplikation die ganzzahlige Division, der Divisionsrest entspricht der hinzuaddierten Ziffer — daher der Name Divisionsverfahren. Da die Schritte in umgekehrter Reihenfolge durchgeführt werden, steht die höchstwertige Ziffer auf der linken Seite oben, rechts hingegen unten. Links starten wir mit dem Wert 0; auf der rechten Seite rechnen wir solange, bis die Division 0 ergibt. Wir erhalten jeweils $(102421)_5 = (3486)_{10}$. Abbildung B.11 implementiert die beiden Verfahren in Mini-F# — allerdings mit einem Twist, da die Ziffer 0 nicht verfügbar ist.

Dass ein Schritt im Divisionsverfahren den korrespondierenden Schritt im Multiplikationsverfahren umkehrt, liegt an den Eigenschaften der ganzzahligen Division, mit der wir uns bereits ausführlich beschäftigt haben.

$$n = q \cdot 5 + r \;\wedge\; r < 5 \quad\Longleftrightarrow\quad q = n \;\boldsymbol{div}\; 5 \;\wedge\; r = n \;\boldsymbol{mod}\; 5$$

Wir zeigen die Äquivalenz mit einem Ping-Pong Beweis. »$\Longleftarrow$«: folgt unmittelbar aus der Divisionsregel (B.48a) und (B.48b). »$\Longrightarrow$«: Aus der Annahme $r < 5$ folgt mit (B.47) $r \;\boldsymbol{div}\; 5 = 0$ und $r \;\boldsymbol{mod}\; 5 = r$; der Rest ist Routine.

$$
\begin{aligned}
& (q \cdot 5 + r) \ \textbf{\textit{div}}\ 5 \\
= \quad & \{ \text{ Treppeneigenschaft (B.65a) } \} \\
& q + (r \ \textbf{\textit{div}}\ 5) \\
= \quad & \{ r < 5 \text{ und somit } r \ \textbf{\textit{div}}\ 5 = 0 \} \\
& q
\end{aligned}
\qquad
\begin{aligned}
& (q \cdot 5 + r) \ \textbf{\textit{mod}}\ 5 \\
= \quad & \{ \text{ Periodizität (B.65b) } \} \\
& r \ \textbf{\textit{mod}}\ 5 \\
= \quad & \{ r < 5 \text{ und somit } r \ \textbf{\textit{mod}}\ 5 = r \} \\
& r
\end{aligned}
$$

Die Divisionsregel (B.48a) ist die Grundlage aller Stellenwertsysteme.

Konvertierung von Hand Zum Schluss noch ein paar amüsante Betrachtungen, die vielleicht angesichts von elektronischen Helfern wie Taschenrechnern, Handys und Laptops etwas aus der Zeit fallen. Führt man die Konvertierungen von Hand durch, wird man versuchen, schwierige Operationen wie Multiplikation mit 5 oder Division durch 5 zu vermeiden — ein Rechenfehler ist schnell passiert.

Schauen wir uns zunächst die Konvertierung von quinär nach dezimal an. Die Kürzungsregel (B.43) hilft, die Multiplikation mit 5 zu umgehen: $n \cdot 5 = (n \cdot 5 \cdot 2) \ \textbf{\textit{div}}\ 2 = (n \cdot 10) \ \textbf{\textit{div}}\ 2$. Stattdessen multiplizieren wir mit 10 und halbieren anschließend das Ergebnis. Multiplikation mit der Basis ist in einem Stellenwertsystem einfach: Ans Ende der Ziffernfolge wird eine 0 gehängt.

0.𝍸 || |||| || |	0/2 = 0
5.|| |||| || |	50/2 = 25
2 7.|||| || |	270/2 = 135
1 3 9.|| |	1390/2 = 695
6 9 7.|	6970/2 = 3485
3 4 8 6	

Der Dezimalpunkt trennt das Zwischenergebnis von der nächsten zu verarbeitenden Ziffer. In jedem Schritt wird das Zehnfache der Dezimalzahl halbiert und die quinäre Ziffer hinzuaddiert. (Wie man sieht, funktioniert das Multiplikationsverfahren für beliebige Ziffern — die Einschränkung $r < 5$ ist unnötig.)

Bei der Konversion von dezimal nach quinär gilt es, komplizierte Divisionen zu vermeiden. Dabei hilft die Kürzungsregel (B.45d): $n \ \textbf{\textit{div}}\ 5 = (n \cdot 2) \ \textbf{\textit{div}}\ (5 \cdot 2) = (n \cdot 2) \ \textbf{\textit{div}}\ 10$. Statt durch 5 zu teilen, verdoppeln wir und teilen dann das Ergebnis durch 10. Ganzzahlige Division durch die Basis ist in einem Stellenwertsystem einfach: Die letzte Ziffer, der Divisionsrest, wird gestrichen. Weiterhin gilt: $n \ \textbf{\textit{mod}}\ 5 = (n \ \textbf{\textit{mod}}\ 10) \ \textbf{\textit{mod}}\ 5$. (Warum?) Um die Quinärziffer zu bestimmen, genügt es also, die letzte Dezimalziffer zu betrachten.

3 4 8 6.	3486 · 2 = 6972
6 9 7.|	697 · 2 = 1394
1 3 9.|| |	139 · 2 = 278
2 7.|||| || |	27 · 2 = 54
5.|| |||| || |	5 · 2 = 10
1. || |||| || |	1 · 2 = 2
| || |||| ||	

In jedem Schritt wird die Dezimalzahl verdoppelt und dann die letzte Ziffer gestrichen.

Das Divisionsverfahren gibt eine Ziffernfolge bestehend aus den Ziffern von 0 bis $b-1$ zurück. Hätten wir gerne eine 0-freie Darstellung mit den Ziffern \|, \|\|, \|\|\|, \|\|\|\| und 𝍸, dann müssen wir den Rest 0 gesondert behandeln (siehe auch Abbildung B.11).

$$n = n \ \textbf{\textit{div}}\ 5 \cdot 5 + 0 = (n \ \textbf{\textit{div}}\ 5 \dot{-} 1) \cdot 5 + 5$$

Ähnlich wie bei der schriftlichen Subtraktion »borgen« wir uns einen Fünfer, zum Beispiel, indem wir vom doppelten Wert Zehn abziehen: n ***div*** $5 - 1 = (n \cdot 2 - 10)$ ***div*** 10.

1 0 0 0 .	$1000 \cdot 2 - 10$	=	1990
1 9 9 . 𝍸	$199 \cdot 2$	=	398
3 9 . |||| 𝍸	$39 \cdot 2$	=	78
7 . |||| |||| 𝍸	$7 \cdot 2$	=	14
1 . || |||| |||| 𝍸	$1 \cdot 2$	=	2
| || |||| |||| 𝍸			

B.5.4. Elementare Zahlentheorie⋆

You probably have seen Euclid's proof of the infinitude of the primes somewhere, but if not, you have missed out on one of the most crucial pillars of human knowledge that ever have been found. It would be a gap in your experience of life as sad as never having tasted chocolate or never having heard a piece of music. I can't tolerate such crucial gaps in my readers' knowledge, so here goes nothing!

— Douglas Richard Hofstadter (1945), *I Am a Strange Loop*

In Vorbereitung auf den nächsten Abschnitt unternehmen wir einen kurzen Ausflug in die elementare ***Zahlentheorie***.

Teilbarkeit Wir haben bereits angesprochen, dass die Teilbarkeitsrelation »\« eine partielle Ordnung auf den natürlichen Zahlen definiert. Erweitern wir die Relation auf die ganzen Zahlen,

$$a \setminus b \iff \exists\, q \in \mathbb{Z}\ .\ q \cdot a = b \tag{B.73}$$

erhalten wir eine partielle *Quasiordnung*. Da das Vorzeichen bezüglich der Teilbarkeit keine Rolle spielt,

$$a \setminus b \iff (-a) \setminus b \iff a \setminus (-b) \tag{B.74}$$

geht die Antisymmetrie flöten; es gilt lediglich:

$$a \setminus b \ \wedge\ b \setminus a \iff a = b \ \vee\ a = -b \iff \mathsf{abs}\, a = \mathsf{abs}\, b \ \Longleftrightarrow:\ a \sim b \tag{B.75}$$

Teilbarkeit lässt sich auch mit Hilfe des Modulo-Operators ausdrücken: a teilt b genau dann, wenn sich b ohne Rest durch a dividieren lässt.

$$a \setminus b \iff b \ \textbf{\textit{mod}}\ a = 0 \qquad \text{falls } a \neq 0 \tag{B.76}$$

Abbildung B.12 zeigt einen winzigen Ausschnitt der partiellen Quasiordnung $(\mathbb{Z}, \setminus)$, die im Vergleich zur totalen Ordnung $(\mathbb{Z}, \leqslant)$ wesentlich interessanter daherkommt. Zahl und Gegenzahl nehmen in der Ordnung den gleichen Platz ein, angezeigt durch $\pm n$. Das »kleinste« Element ist ± 1, das »größte« 0! (Also, die Zahl Null, nicht Null Fakultät.) Die direkten, positiven »Nachfolger« von 1 heißen ***Primzahlen***: 2, 3, 5 usw. Eine Primzahl p besitzt genau zwei Teiler: ± 1 und $\pm p$.[20] Die Menge aller Primzahlen bezeichnen wir mit $\mathbb{P}$. Der kleinste Teiler $d \geqslant 2$ einer Zahl $n \geqslant 2$ ist stets eine Primzahl. (Warum?) Auf der nächst höheren Ebene befinden sich die Produkte zweier Primzahlen: $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $9 = 3 \cdot 3$ usw. Allgemein sind auf der k-ten Ebene von unten die

[20] Ein direkter Nachfolger $\bot \prec a$ des kleinsten Elements $\bot$ heißt auch ***Atom***: a ist Atom, wenn a echt größer als $\bot$ ist und kein anderes Element zwischen $\bot$ und a liegt: $\bot < a \ \wedge\ \neg(\exists x\ .\ \bot < x < a)$.

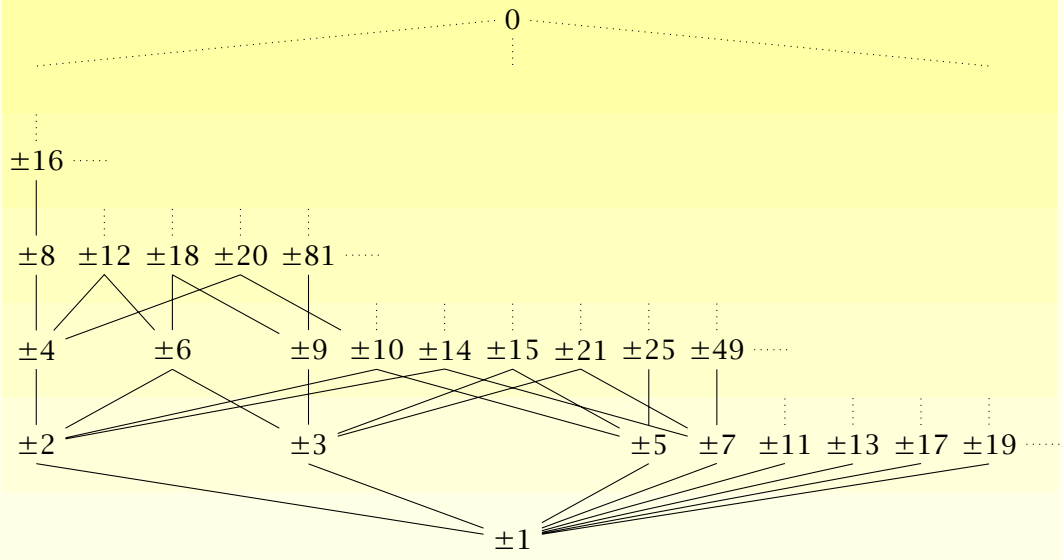


Abbildung B.12.: Ein Ausschnitt aus dem Quasiverband $(\mathbb{Z}, \backslash)$.

Produkte von k Primzahlen aufgeführt. Da es unendlich viele Primzahlen gibt (vergleiche obiges Zitat, siehe Abbildung B.13), erstreckt sich jede Ebene unendlich nach rechts. Von Ebene zu Ebene werden die Zahlen größer; das Vielfache einer Zahl ist mindestens so groß wie die Zahl selbst mit Ausnahme des größten Elements, der Zahl Null.

$$a \setminus b \quad \Longrightarrow \quad \operatorname{abs} a \leqslant \operatorname{abs} b \qquad \text{falls } b \neq 0 \tag{B.77}$$

Produkte erhalten die Teilbarkeit oder mit anderen Worten: Die Multiplikation ist bezüglich »\« eine monotone Operation.

$$a_1 \setminus b_1 \ \wedge \ a_2 \setminus b_2 \quad \Longrightarrow \quad (a_1 \cdot a_2) \setminus (b_1 \cdot b_2) \tag{B.78}$$

Daraus folgt unmittelbar, dass $a \setminus (a \cdot b)$ und weiterhin $(a \cdot n) \setminus (b \cdot n)$ falls $a \setminus b$. Umgekehrt lassen sich gemeinsame Faktoren »kürzen«.

$$(a \cdot n) \setminus (b \cdot n) \quad \Longleftrightarrow \quad a \setminus b \qquad \text{falls } n \neq 0 \tag{B.79a}$$

$$(a \cdot n) \setminus b \quad \Longleftrightarrow \quad a \setminus (b/n) \qquad \text{falls } n \neq 0 \tag{B.79b}$$

Summen erhalten die Teilbarkeit hingegen nicht: Es gilt $2 \setminus 2$ und $3 \setminus 6$, aber nicht $5 \setminus 8$. Summen vertragen sich stattdessen mit ***gemeinsamen Teilern*** — ein gemeinsamer Teiler ist eine untere Schranke bezüglich der Teilbarkeitsrelation. Ist a ein gemeinsamer Teiler zweier Zahlen, dann teilt a auch beliebige Linearkombinationen der Zahlen.

$$a \setminus b_1 \ \wedge \ a \setminus b_2 \quad \Longrightarrow \quad a \setminus (n_1 \cdot b_1 + n_2 \cdot b_2) \tag{B.80}$$

Auf den natürlichen Zahlen bildet die Teilbarkeitsrelation einen vollständigen Verband, auf den ganzen Zahlen einen ***vollständigen Quasiverband***. Die in Abschnitt B.4.2 skizzierte Theorie der Verbände lässt sich in gleicher Weise für Quasiverbände entwickeln. Man muss sich lediglich daran gewöhnen bzw. akzeptieren, dass viele Konzepte nur noch modulo der von der Quasiordnung induzierten Äquivalenzrelation »∼« definiert sind. Zum Beispiel kann es mehrere kleinste Elemente geben, die aber notwendigerweise äquivalent sind. Im Fall von $(\mathbb{Z}, \backslash)$ existieren zwei

Um zu zeigen, dass es unendlich viele Primzahlen gibt, führen wir einen ***Widerspruchsbeweis***. Dazu nehmen wir an, dass es nur endlich viele ihrer Art gibt: $p_1, p_2, p_3, \ldots, p_n$. Das Produkt der aufgeführten Primzahlen

$$\mathrm{P} = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n$$

wird von allen Primzahlen geteilt, nicht aber dessen Nachfolger P + 1. Die ganzzahlige Division ergibt stets einen Rest: $(\mathrm{P}+1)$ ***mod*** $p_i = 1$ ***mod*** $p_i = 1$, da $p_i \setminus \mathrm{P}$.

$$\forall i \;.\; \neg(p_i \setminus \mathrm{P}+1)$$

Der kleinste, von 1 verschiedene Teiler von P+1 ist aber eine Primzahl, der ***kleinste Primfaktor***, und somit eine der Zahlen, die auf der obigen Liste aufgeführt sind.

$$\exists i \;.\; p_i \setminus \mathrm{P}+1$$

Damit ergibt sich ein Widerspruch, so dass die Annahme, dass es nur endlich viele Primzahlen gibt, falsch sein muss.

.....

Aus dem Beweis lässt sich ein faszinierender ***Primzahlen-Generator*** ableiten: Wir fügen die neue Primzahl, den kleinsten Primfaktor von P + 1, zur ursprünglichen Primzahlenfolge hinzu und wiederholen die Schritte mit der erweiterten Folge. Wenn wir mit der Folge $2, 3, 5$ starten, erhalten wir $2 \cdot 3 \cdot 5 + 1 = 31$. Da 31 eine Primzahl ist, ergibt sich im nächsten Schritt $2 \cdot 3 \cdot 5 \cdot 31 + 1 = 931$. Das Ergebnis ist durch 7 teilbar, so dass es mit $2 \cdot 3 \cdot 5 \cdot 31 \cdot 7 + 1 = 6511$ weitergeht. Starten wir mit der einelementigen Folge, die nur aus der 2 besteht, ergibt sich eine wild oszillierende Folge:

$$\begin{aligned}
2+1 &= 3\\
2\cdot 3+1 &= 7\\
2\cdot 3\cdot 7+1 &= 43\\
2\cdot 3\cdot 7\cdot 43+1 &= 1807\\
2\cdot 3\cdot 7\cdot 43\cdot 13+1 &= 23479\\
2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53+1 &= 1244335\\
2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53\cdot 5+1 &= 6221671\\
2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53\cdot 5\cdot 6221671+1 &= 38709183810571\\
2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53\cdot 5\cdot 6221671\cdot 38709183810571+1 &= 1498400911280533294827535471\\
2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53\cdot 5\cdot 6221671\cdot 38709183810571\cdot 139+1 &= \cdots
\end{aligned}$$

Insgesamt 51 Glieder der sogenannten ***Euklid-Mullin-Sequenz*** sind bekannt; das erste unbekannte Glied ist der kleinste Primfaktor einer Zahl mit 335 Ziffern.

2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, 23003, 30693651606209,
37, 1741, 1313797957, 887, 71, 7127, 109, 23, 97, 159227, 643679794963466223081509857, 103,
1079990819, 9539, 3143065813, 29, 3847, 89, 19, 577, 223, 139703, 457, 9649, 61, 4357,
87991098722552272708281251793312351581099392851768893748012603709343, 107, 127, 3313,
22743268910858953275498491507577484838667143956826042075441494078076124589 3, 59, 31, 211, ...

Die Euklid-Mullin-Sequenz steckt voller Rätsel: Man weiß nicht, ob auf diese Weise alle Primzahlen generiert werden. Ebensowenig ist bekannt, ob man *formal* entscheiden kann, ob eine gegebene Primzahl in der Folge enthalten ist.

Abbildung B.13.: Der Satz von Euklid und die Euklid-Mullin-Sequenz.

kleinste Elemente, –1 und 1, die sich nur im Vorzeichen unterscheiden — $a \sim b :\Longleftrightarrow \operatorname{abs} a = \operatorname{abs} b$ gemäß (B.75). Entsprechendes gilt für Infimum und Supremum: Das Infimum ist durch den ***größten gemeinsamen Teiler*** gegeben (***gcd*** oder hcf, engl. *g*reatest *c*ommon *d*ivisor oder *h*ighest *c*ommon *f*actor), das Supremum durch das ***kleinste gemeinsame Vielfache*** (***lcm***, engl. *l*east *c*ommon *m*ultiple).

$$a_1 \operatorname{\mathbf{lcm}} a_2 \setminus b \iff a_1 \setminus b \ \wedge\ a_2 \setminus b \tag{B.81a}$$

$$a \setminus b_1 \ \wedge\ a \setminus b_2 \iff a \setminus b_1 \operatorname{\mathbf{gcd}} b_2 \tag{B.81b}$$

Insbesondere gilt $a \operatorname{\mathbf{lcm}} b \setminus a \cdot b$, da das Produkt $a \cdot b$ ein gemeinsames Vielfaches von a und b ist.

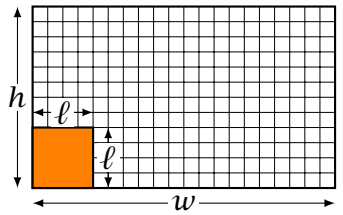
Die indirekten Definitionen legen ***lcm*** und ***gcd*** nur bis auf das Vorzeichen fest, zum Beispiel, $gcd(2 \cdot 3, 3 \cdot 5) \sim -3$. Ins Positive gewendet heißt das, dass man sich das Vorzeichen »aussuchen« kann. Wir treffen an dieser Stelle keine voreiligen (mehr oder minder willkürlichen) Festlegungen. Das stellt kein großes Problem dar — man muss nur aufpassen, dass man keine Schlüsse zieht, bei denen das Vorzeichen eine Rolle spielt.

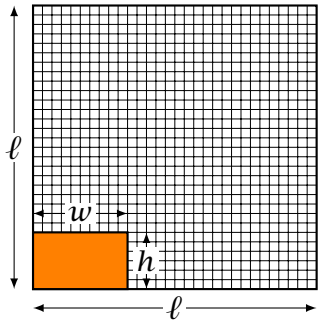
Die folgende Tabelle stellt noch einmal die Notation der Ordnung $(\mathbb{Z}, \leqslant)$ und der Quasiordnung $(\mathbb{Z}, \setminus)$ nach Konzepten geordnet gegenüber.

Ordnung	strikte Ordnung	Äquivalenz-relation	kleinstes Element	größtes Element	kleinste obere Schranke	größte untere Schranke
$a \leqslant b$	$a < b$	$a = b$	0	—	$a \uparrow b$	$a \downarrow b$
$a \setminus b$	keine Notation	$a \sim b$	1	0	$a \operatorname{\mathbf{lcm}} b$	$a \operatorname{\mathbf{gcd}} b$

Gemeinsame Teiler und Vielfache lassen sich wunderbar mit Kachelungsproblemen illustrieren. Mit dem größten gemeinsamen Teiler wird die größte, quadratische Kachel bestimmt, mit der sich ein rechteckiger Fußboden kacheln lässt. Umgekehrt ermittelt das kleinste gemeinsame Vielfache die kleinste, quadratische Fläche, die mit einer gegebenen, rechteckigen Kachel ausgelegt werden kann.

$$\ell \setminus w \ \wedge\ \ell \setminus h \iff \ell \setminus w \operatorname{\mathbf{gcd}} h$$





$$w \setminus \ell \ \wedge\ h \setminus \ell \iff w \operatorname{\mathbf{lcm}} h \setminus \ell$$

Der größte gemeinsame Teiler wird in der Bruchrechnung verwendet, um Brüche zu kürzen, sie auf den kleinsten Nenner zu bringen.

$$\frac{174}{48} = \frac{29 \cdot 6}{8 \cdot 6} = \frac{29}{8} \qquad 48 \operatorname{\mathbf{gcd}} 174 = 6$$

Umgekehrt kommt das kleinste gemeinsame Vielfache zum Einsatz, um Brüche zu erweitern, zum Beispiel als vorbereitenden Schritt bei der Addition.

$$\frac{1}{6} + \frac{9}{14} = \frac{1 \cdot 7}{42} + \frac{9 \cdot 3}{42} = \frac{34}{42} = \frac{17 \cdot 2}{21 \cdot 2} = \frac{17}{21} \qquad 6 \operatorname{\mathbf{lcm}} 14 = 42$$

```
let rec gcd (a : bigint, b : bigint) : bigint =      // euklidischer Algorithmus
  if a = 0 then abs b
           else gcd (b % a, a)
let rec egcd (a : bigint, b : bigint) =              // erweiterter euklidischer Algorithmus
  if a = 0 then (abs b, 0, bigint (sign b))
           else let (d, m, n) = egcd (b % a, a)
                (d, n - m * (b / a), m)
let lcm (a : bigint, b : bigint) : bigint =          // kleinstes gemeinsames Vielfaches
  if a = 0 || b = 0 then 0
                    else (a * b) / gcd (a, b)
```

Abbildung B.14.: Berechnung des größten gemeinsamen Teilers in Mini–F#.

Berechnet man Teiler und Vielfache von Hand, kann man versuchen, gemeinsame Faktoren herauszuziehen: zum Beispiel gilt $48 \mathbin{\textbf{\textit{gcd}}} 174 = 2 \cdot (24 \mathbin{\textbf{\textit{gcd}}} 87) = 2 \cdot 3 \cdot (8 \mathbin{\textbf{\textit{gcd}}} 29) = 6$ und $6 \mathbin{\textbf{\textit{lcm}}} 14 = 2 \cdot (3 \mathbin{\textbf{\textit{lcm}}} 7) = 42$. Den Rechnungen liegen die ***Distributivgesetze*** zugrunde:

$$(a \cdot x) \mathbin{\textbf{\textit{lcm}}} (b \cdot x) = (a \mathbin{\textbf{\textit{lcm}}} b) \cdot \operatorname{abs} x \tag{B.82a}$$

$$(a \cdot x) \mathbin{\textbf{\textit{gcd}}} (b \cdot x) = (a \mathbin{\textbf{\textit{gcd}}} b) \cdot \operatorname{abs} x \tag{B.82b}$$

Die Gleichungen gelten offensichtlich für $x = 0$. Für $x \neq 0$ zeigen wir, dass der Quotient $((a \cdot x) \mathbin{\textbf{\textit{gcd}}} (b \cdot x))/x$ der größte gemeinsame Teiler von a und b ist bzw. dass $(a \mathbin{\textbf{\textit{lcm}}} b) \cdot x$ das kleinste gemeinsame Vielfache von $a \cdot x$ und $b \cdot x$ ist.

$$\begin{array}{ll}
 & n \setminus ((a \cdot x) \mathbin{\textbf{\textit{gcd}}} (b \cdot x))/x \\
\iff & \quad \{ \text{(B.79b) und } x \neq 0 \} \\
 & n \cdot x \setminus (a \cdot x) \mathbin{\textbf{\textit{gcd}}} (b \cdot x) \\
\iff & \quad \{ \text{Infimum (B.19)} \} \\
 & n \cdot x \setminus a \cdot x \;\wedge\; n \cdot x \setminus b \cdot x \\
\iff & \quad \{ \text{(B.79b) und } x \neq 0 \} \\
 & n \setminus a \;\wedge\; n \setminus b
\end{array}
\qquad
\begin{array}{ll}
 & (a \mathbin{\textbf{\textit{lcm}}} b) \cdot x \setminus n \\
\iff & \quad \{ \text{(B.79b) und } x \neq 0 \} \\
 & a \mathbin{\textbf{\textit{lcm}}} b \setminus n/x \\
\iff & \quad \{ \text{Supremum (B.18)} \} \\
 & a \setminus n/x \;\wedge\; b \setminus n/x \\
\iff & \quad \{ \text{(B.79b) und } x \neq 0 \} \\
 & a \cdot x \setminus n \;\wedge\; b \cdot x \setminus n
\end{array}$$

Euklidischer Algorithmus Der größte gemeinsame Teiler lässt sich mit dem ***euklidischen Verfahren*** bestimmen, dem *ältesten bekannten Algorithmus*, der rund 300 v. Chr. von dem griechischen Mathematiker ***Euklid*** beschrieben wurde. Eine rekursive Implementierung, siehe Abbildung B.14, beruht auf den folgenden Eigenschaften.

$$0 \mathbin{\textbf{\textit{gcd}}} b \sim b \tag{B.83a}$$

$$a \mathbin{\textbf{\textit{gcd}}} b \sim (b \mathbin{\textbf{\textit{mod}}} a) \mathbin{\textbf{\textit{gcd}}} a \tag{B.83b}$$

Die erste Äquivalenz ist eine Instanz des Neutralitätsgesetzes: Das maximale Element (hier: 0) ist das neutrale Element des Infimums (hier: ***gcd***). Die zweite Äquivalenz basiert auf der Tatsache, dass ein gemeinsamer Teiler auch Linearkombinationen teilt.

$$n \setminus a \;\wedge\; n \setminus b \quad\iff\quad n \setminus (b \mathbin{\textbf{\textit{mod}}} a) \;\wedge\; n \setminus a \tag{B.84}$$

Mit Hilfe der liebgewonnenen Divisionsregel (B.48a) lässt sich der Rest als Linearkombination von a und b ausdrücken, $b \;\mathbf{mod}\; a = 1 \cdot b - (b \;\mathbf{div}\; a) \cdot a$. Durch Umstellung der Gleichung kann man umgekehrt b als Linearkombination von a und $b \;\mathbf{mod}\; a$ ausdrücken, $b = 1 \cdot (b \;\mathbf{mod}\; a) + (b \;\mathbf{div}\; a) \cdot a$. Beide Richtungen der obigen Äquivalenz sind damit Spezialfälle von (B.80). Nach diesen Vorüberlegungen kann man Eigenschaft (B.83b) mit einem indirekten Beweis zeigen.[21]

$$
\begin{array}{ll}
 & n \setminus a \;\mathbf{gcd}\; b \\
\iff & \quad \{\ \text{Infimum (B.19)}\ \} \\
 & n \setminus a \;\wedge\; n \setminus b \\
\iff & \quad \{\ \text{Teilbarkeit (B.84)}\ \} \\
 & n \setminus (b \;\mathbf{mod}\; a) \;\wedge\; n \setminus a \\
\iff & \quad \{\ \text{Infimum (B.19)}\ \} \\
 & n \setminus (b \;\mathbf{mod}\; a) \;\mathbf{gcd}\; a
\end{array}
$$

Schauen wir uns den euklidischen Algorithmus in Aktion an:

$$
\begin{array}{rll}
48 \;\mathbf{gcd}\; 174 & 174 = 30 + 3 \cdot 48 & 6 = 2 \cdot 48 - 3 \cdot (174 - 3 \cdot 48) = -3 \cdot 174 + 11 \cdot 48 \\
30 \;\mathbf{gcd}\; 48 & 48 = 18 + 1 \cdot 30 & 6 = -1 \cdot 30 + 2 \cdot (48 - 1 \cdot 30) = 2 \cdot 48 - 3 \cdot 30 \\
18 \;\mathbf{gcd}\; 30 & 30 = 12 + 1 \cdot 18 & 6 = 18 - 1 \cdot (30 - 1 \cdot 18) = -1 \cdot 30 + 2 \cdot 18 \\
12 \;\mathbf{gcd}\; 18 & 18 = 6 + 1 \cdot 12 & 6 = 18 - 1 \cdot 12 \\
6 \;\mathbf{gcd}\; 12 & 12 = 0 + 2 \cdot 6 & \\
0 \;\mathbf{gcd}\; 6 & &
\end{array}
$$

Der größte gemeinsame Teiler von $48 = 2^4 \cdot 3$ und $174 = 2 \cdot 3 \cdot 29$ ist $6 = 2 \cdot 3$. Um die Rechenschritte nachvollziehen zu können, führt die zweite Spalte die verwendeten Instanzen von (B.48a) auf — wie wird die größere der beiden Zahlen jeweils zerlegt? Wir machen eine interessante Beobachtung: Formen wir die Gleichungen von unten nach oben um, können wir 6 als Linearkombination der beiden Ausgangswerte 48 und 174 darstellen: $6 = 11 \cdot 48 - 3 \cdot 174$. Eine Kuriosität am Rande? Nein, ganz und gar nicht. Die Gleichung lässt sich als Urkunde oder ***Zertifikat*** (engl. certificate) auffassen, dass 6 tatsächlich der größte gemeinsame Teiler von 48 und 174 ist. Nehmen wir an, wir hätten Zweifel an der Aussage — ein Rechenfehler ist schnell passiert. (Falls die Zahlen zu klein sind, um Zweifel aufkommen zu lassen, betrachten Sie $411015 \;\mathbf{gcd}\; 1508738 = 11$ mit dem Zertifikat $11 = 34663 \cdot 411015 - 9443 \cdot 1508738$.) Dass 6 ein gemeinsamer Teiler ist, lässt sich schnell verifizieren: $48 \;\mathbf{mod}\; 6 = 0$ und $174 \;\mathbf{mod}\; 6 = 0$. Aber wie können wir uns davon überzeugen, dass 6 tatsächlich der *größte* aller gemeinsamen Teiler ist? Nun, sei d ein beliebiger gemeinsamer Teiler; da d sowohl 48 als auch 174 teilt, muss d gemäß (B.80) auch deren Linearkombination teilen:

$$d \setminus 48 \;\wedge\; d \setminus 178 \quad\Longrightarrow\quad d \setminus (11 \cdot 48 - 3 \cdot 174) \quad\Longleftrightarrow\quad d \setminus 6$$

Da unser Kandidat 6 teilt, muss 6 der größte gemeinsame Teiler sein.

Halten wir fest: Der größte gemeinsame Teiler lässt sich stets als Linearkombination der beiden Ausgangswerte schreiben.

$$\forall\, a \;.\; \forall\, b \;.\; \exists\, a' \;.\; \exists\, b' \;.\; a \;\mathbf{gcd}\; b = a' \cdot a + b' \cdot b \tag{B.85}$$

[21] Wir verwenden das Prinzip des indirekten Beweises (B.15b) mit »\« als Ordnungsrelation — versuchen Sie, $a \setminus b$ als Ordnung zu lesen (»a ist kleiner als oder gleich b«).

Wir zeigen die Behauptung durch Induktion über die Anzahl der rekursiven Aufrufe. **Induktionsbasis:** Die Aussage folgt mit $0 \;\boldsymbol{gcd}\; b = b = 0 \cdot 0 + 1 \cdot b$. **Induktionsschritt:** Gemäß Induktionsannahme gibt es Koeffizienten a' und b', so dass $(b \;\boldsymbol{mod}\; a) \;\boldsymbol{gcd}\; a = a' \cdot (b \;\boldsymbol{mod}\; a) + b' \cdot a$.

$$
\begin{aligned}
& a' \cdot (b \;\boldsymbol{mod}\; a) + b' \cdot a \\
= \quad & \{ \text{ Divisionsregel (B.48a) } \} \\
& a' \cdot (b - (b \;\boldsymbol{div}\; a) \cdot a) + b' \cdot a \\
= \quad & \{ \text{ Arithmetik } \} \\
& (b' - a' \cdot (b \;\boldsymbol{div}\; a)) \cdot a + a' \cdot b
\end{aligned}
$$

Wir erhalten wie gewünscht eine Linearkombination von a und b. Fügt man diese Berechnungen zum Originalalgorithmus hinzu, siehe Abbildung B.14, erhält man den ***erweiterten euklidischen Algorithmus***. Bei der Erweiterung handelt es sich um einen ***selbst-zertifizierenden*** Algorithmus (engl. self-certifying algorithm), da er neben dem eigentlichen Ergebnis zusätzlich einen Beweis seiner Korrektheit mitliefert. Cool!

Kleinstes gemeinsames Vielfaches Ein ähnlich eleganter Algorithmus zur Bestimmung des kleinsten gemeinsamen Vielfachen ist nicht bekannt. Man behilft sich mit dem folgenden Zusammenhang, der es erlaubt, das kleinste gemeinsame Vielfache auf den größten gemeinsamen Teiler zurückzuführen, siehe auch Abbildung B.14.

$$a \cdot b = (a \;\boldsymbol{gcd}\; b) \cdot (a \;\boldsymbol{lcm}\; b) \tag{B.86}$$

Ist eine der Zahlen negativ, wählen wir die Vorzeichen von ***lcm*** und ***gcd*** so, dass die Gleichung (B.86) erfüllt ist: $a \;\boldsymbol{gcd}\; b \geqslant 0$ und $\operatorname{sign}(a \;\boldsymbol{lcm}\; b) = \operatorname{sign}(a \cdot b)$, siehe Abbildung B.14. Sie erinnern sich? Wir haben bezüglich der Vorzeichen die freie Wahl. Wir können uns also für den Beweis auf natürliche Zahlen beschränken: $a, b \in \mathbb{N}$. Der Beweis teilt sich in zwei Schritte auf: Wir zeigen (B.86) zunächst für den einfachen Fall, dass a und b teilerfremd sind. Anschließend führen wir den allgemeinen Fall auf den Spezialfall zurück.

Wenn a und b teilerfremd sind, dann ist das kleinste gemeinsame Vielfache das Produkt der Zahlen a und b.

$$a \cdot b = a \;\boldsymbol{lcm}\; b \quad \Longleftarrow \quad a \;\boldsymbol{gcd}\; b = 1$$

Wir zeigen, dass $a \cdot b$ die Definition des kleinsten gemeinsamen Vielfachen erfüllt (B.81a).

$$a \setminus x \;\wedge\; b \setminus x \quad \Longleftrightarrow \quad a \cdot b \setminus x$$

»$\Longleftarrow$«: Aus $a \setminus a \cdot b$ und $b \setminus a \cdot b$ folgt die Aussage mit Hilfe der Transitivität. »$\Longrightarrow$«: Aus den Annahmen $a \setminus x$ und $b \setminus x$ schließen wir zunächst $a \cdot b \setminus b \cdot x$ und $a \cdot b \setminus a \cdot x$ (B.78).

$$
\begin{aligned}
& a \;\boldsymbol{gcd}\; b = 1 \\
\Longrightarrow \quad & \{ \text{ erweiterter euklidischer Algorithmus (B.85) } \} \\
& \exists\, a' \;.\; \exists\, b' \;.\; a' \cdot a + b' \cdot b = 1 \\
\Longrightarrow \quad & \{ \text{ Arithmetik } \} \\
& \exists\, a' \;.\; \exists\, b' \;.\; a' \cdot a \cdot x + b' \cdot b \cdot x = x \\
\Longrightarrow \quad & \{ \; a \cdot b \setminus a \cdot x,\; a \cdot b \setminus b \cdot x \text{ und (B.80) } \} \\
& a \cdot b \setminus x
\end{aligned}
$$

Wir führen die Aussage $a \;\boldsymbol{lcm}\; b = a \cdot b/g$ auf den Spezialfall zurück, indem wir a und b »kürzen«. Sei $g := a \;\boldsymbol{gcd}\; b$, dann

$$
\begin{aligned}
& a \ \textbf{\textit{lcm}}\ b \\
= \quad & \{ \text{ Arithmetik } \} \\
& ((a/g) \cdot g) \ \textbf{\textit{lcm}}\ ((b/g) \cdot g) \\
= \quad & \{ \text{ Distributivgesetz (B.82a) } \} \\
& ((a/g) \ \textbf{\textit{lcm}}\ (b/g)) \cdot g \\
= \quad & \{ \text{ Spezialfall: } (a/g) \ \textbf{\textit{gcd}}\ (b/g) = 1 \ \} \\
& (a/g) \cdot (b/g) \cdot g \\
= \quad & \{ \text{ Arithmetik } \} \\
& a \cdot b/g
\end{aligned}
\qquad
\begin{aligned}
& a \ \textbf{\textit{gcd}}\ b \\
= \quad & \{ \text{ Arithmetik } \} \\
& ((a/g) \cdot g) \ \textbf{\textit{gcd}}\ ((b/g) \cdot g) \\
= \quad & \{ \text{ Distributivgesetz (B.82b) } \} \\
& ((a/g) \ \textbf{\textit{gcd}}\ (b/g)) \cdot g
\end{aligned}
$$

Die Hilfsrechnung auf der rechten Seite zeigt, dass sich »gekürzte« Brüche nicht weiter kürzen lassen: (a/g) ***gcd*** $(b/g) = (a$ ***gcd*** $b)/g = 1$.

Übungen.

17. Zeigen Sie $2 \setminus n \ \vee \ 2 \setminus n+1$ durch natürliche Induktion; folgern Sie $2 \setminus n \cdot (n+1)$.

18. Denken Sie sich eine beliebige ungerade Zahl aus. Quadrieren Sie die Zahl und ziehen vom Ergebnis 1 ab. Zeigen Sie, dass die resultierende Zahl immer durch 8 teilbar ist.

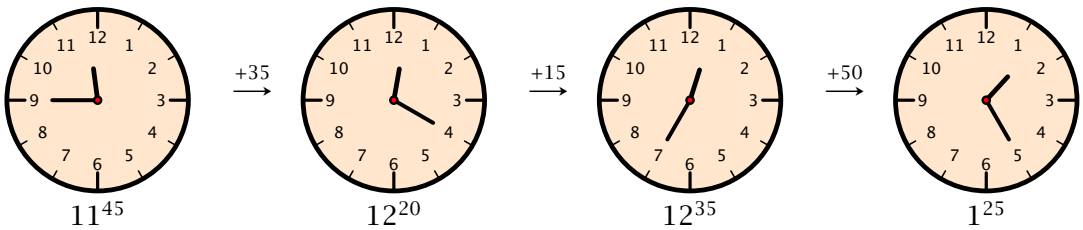
19. Wie wär's mit einer Aufgabe aus einem Abschlussexamen in Mathematik der Universität Oxford (um 1850): »The difference of the squares of any two odd numbers is divisible by 8.«

20. Beweisen Sie den Zusammenhang zwischen der Teilbarkeitsordnung und der »normalen« Ordnung auf den ganzen Zahlen (B.77). Die Einschränkung $b \neq 0$ sollte sich in natürlicher Weise aus dem Beweis ergeben.

21. Zeigen Sie, dass die Funktion *gcd*, siehe Abbildung B.14, für alle Argumente terminiert ($a, b \in \mathbb{Z}$). Die Funktion verwendet den symmetrischen Divisionsrest ***rem*** an Stelle des abrundenden Rests ***mod*** — spielt das eine Rolle für Korrektheit und Terminierung des Verfahrens?

B.5.5. Modulararithmetik⧹Rechnen mit Resten

Gelegentlich drehen wir uns beim Zählen im Kreis: Um 11^{45} beginnt die Vorlesung »Grundlagen der Programmierung«, 100 Minuten später strömen die Studierenden in die Mensa, die Uhr zeigt 1^{25} — verwirrend. Die Analoguhr illustriert die den Uhrzeiten zugrundeliegende Modulararithmetik sehr schön.



Wir schreiben $a \equiv b \pmod{m}$, wenn die Differenz $a - b$ durch m teilbar ist. Für die obigen Zeitangaben in Stunden und Minuten gilt: $45+35 \equiv 20 \pmod{60}$ im ersten Schritt, und $12+1 \equiv 1 \pmod{12}$ und $35+50 \equiv 25 \pmod{60}$ im letzten Schritt. Die Periodizität der Stunden spiegelt den naturgegebenen, sich wiederholenden Wechsel von Tag und Nacht wider — hervorgerufen durch die Erdrotation.

Informatisch gesehen sind Zeitangaben ein Beispiel für ein Zahlensystem mit einer bunten Mischung von Basen[22] (engl. mixed-base oder mixed-radix number system). Die Zeitangabe »y Jahre, d Tage, h Stunden, m Minuten und s Sekunden« entspricht[23]

$$((((0 \cdot 1 + y) \cdot 365 + d) \cdot 24 + h) \cdot 60 + m) \cdot 60 + s \text{ Sekunden.}$$

Warum umfasst eine Stunde 60 Minuten und eine Minute 60 Sekunden? Die Einteilung geht wie bereits erwähnt auf das sexagesimale Stellenwertsystem der Sumerer und Babylonier zurück. Die Basis 60 ist nicht zuletzt deswegen so attraktiv, weil sich 60 glatt durch 2, 3, 4, 5 und 6 und damit auch durch 30, 20, 15, 12 und 10 teilen lässt, siehe Hassediagramm der Teilbarkeitsordnung in Abschnitt B.4.1.

Zahlensysteme mit gemischten Basen verallgemeinern Stellenwertsysteme: Jede Position hat ihr spezielles Gewicht und ihren eigenen Vorrat an Ziffern. Wie bei normalen Stellenwertsystemen wird die Arithmetik unbeschränkt großer Zahlen auf die Arithmetik von Ziffern zurückgeführt. Mit der Ziffernarithmetik beschäftigen wir uns im Folgenden. Vorher werfen wir noch einen kurzen Blick auf die Zahlentypen, die F# von Haus aus mitbringt.

Wir haben schon anklingen lassen, dass Prozessoren nur mit beschränkter Genauigkeit rechnen. Die hardware-seitig verfügbare Arithmetik spiegelt sich software-seitig in verschiedenen Zahlentypen wider. F# bietet neben den natürlichen und ganzen Zahlen, *Nat* und *bigint*, acht Zahlentypen mit beschränkter Genauigkeit an.

- *byte*: natürliche Zahlen von 0 bis $2^8 - 1 = 255$;
- *sbyte*: ganze Zahlen von $-2^7 = -128$ bis $2^7 - 1 = 127$ (signed byte);
- *int16*: ganze Zahlen von $-2^{15} = -32768$ bis $2^{15} - 1 = 32767$;
- *uint16*: natürliche Zahlen von 0 bis $2^{16} - 1 = 65535$ (unsigned int16);
- *int* und *uint32*: dito mit 32 Bit;
- *int64* und *uint64*: dito mit 64 Bit.

Je nach Wortbreite, 1, 2, 4 oder 8 Byte, ergeben sich unterschiedliche Genauigkeiten. Ein Byte besteht aus acht Bits und kann somit 2^8 verschiedene Werte darstellen. Mit 2^i Bytes bzw. $n = 8 \cdot 2^i$ Bits lassen sich somit $2^n = 2^{8 \cdot 2^i}$ natürliche Zahlen (engl. unsigned) darstellen oder ebensoviele ganze Zahlen (engl. signed), aufgeteilt in 2^{n-1} negative Zahlen, die Zahl Null und $2^{n-1} - 1$ positive Zahlen.

Rechnen mit beschränkter Genauigkeit hat seine Tücken (der Suffix *uy* deutet an, dass wir mit *u*nsigned b*y*tes rechnen):

```
>>> 1uy * 2uy * 3uy * 4uy * 5uy
120uy
>>> 1uy * 2uy * 3uy * 4uy * 5uy * 6uy * 7uy * 8uy * 9uy * 10uy
0uy
>>> 255uy + 1uy
0uy
```

[22] Basen ist der Plural von Basis.

[23] Man sollte sich klarmachen, dass Zeitangaben eine bequeme Abstraktion sind; die Wirklichkeit ist um einiges komplizierter. Die Natur legt keinen Wert auf Teilbarkeit: Die Dauer des Erdumlaufs um die Sonne ist kein ganzzahliges Vielfaches der Dauer einer Erdrotation. Erstere beträgt ungefähr $365\frac{1}{4}$ Tage, so dass Schaltjahre eingeführt werden. Auch die Erdrotation ist natürlichen Schwankungen unterworfen. Die Abweichungen vom Referenztag mit einer Länge von $24 \cdot 60 \cdot 60 = 86.400$ Sekunden betragen zwar nur wenige Millisekunden; diese summieren sich aber im Laufe der Zeit auf, so dass gelegentlich Schaltsekunden vonnöten sind.

Wie erwartet ist 5! = 120, aber warum hat 10! das Ergebnis 0? Mathematisch gesehen wird mit Resten gerechnet:

$$a \oplus b = (a + b) \ \textbf{\textit{mod}} \ m \tag{B.87a}$$
$$a \ominus b = (a - b) \ \textbf{\textit{mod}} \ m \tag{B.87b}$$
$$a \odot b = (a \cdot b) \ \textbf{\textit{mod}} \ m \tag{B.87c}$$

wobei m die Gesamtzahl der repräsentierbaren Werte ist; im obigen Beispiel ist $m := 2^8$. Tatsächlich gilt $1 \odot 2 \odot 3 \odot 4 \odot 5 \odot 6 \odot 7 \odot 8 \odot 9 \odot 10 \equiv 0 \pmod{2^8}$. Das Rätsel lösen wir im Folgenden.

Kongruenzen Man nennt zwei ganze Zahlen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ ***kongruent modulo*** m, wenn sich ihre Differenz durch m teilen lässt.

$$a \equiv b \pmod{m} \quad :\Longleftrightarrow \quad m \setminus (a - b) \tag{B.88}$$

Für jeden Modulo $m \in \mathbb{Z}$ wird eine ***Äquivalenzrelation*** definiert, eine ***reflexive***, ***symmetrische*** und ***transitive*** Relation.

(Reflexivität)	$a \equiv a$
(Symmetrie)	$a \equiv b \quad \Longrightarrow \quad b \equiv a$
(Transitivität)	$a \equiv b \ \wedge \ b \equiv c \quad \Longrightarrow \quad a \equiv c$

Statt $a \equiv b \pmod{m}$ schreiben wir auch kurz $a \equiv_m b$, insbesondere wenn wir uns auf die Äquivalenzrelation selbst beziehen wollen. Zwei Spezialfälle verdienen besondere Beachtung. Für $m = 0$ entspricht die definierte Äquivalenzrelation der »normalen« Gleichheit, der diskriminierensten aller Äquivalenzrelationen: $a \equiv b \pmod{0} \Longleftrightarrow 0 \setminus (a - b) \Longleftrightarrow a = b$. Das andere Extrem ergibt sich für $m = 1$: Da $a \equiv b \pmod{1} \Longleftrightarrow 1 \setminus (a - b) \Longleftrightarrow \mathit{true}$, werden alle Zahlen zueinander in Beziehung gesetzt. Wir erhalten die All- oder Universalrelation, den großen Gleichmacher, die am wenigsten diskriminierende Äquivalenzrelation. Da der Fall $m = 0$ nicht allzu interessant ist, findet man oft folgende alternative Definition der Kongruenz.

$$a \equiv b \pmod{m} \quad :\Longleftrightarrow \quad a \ \textbf{\textit{mod}} \ m = b \ \textbf{\textit{mod}} \ m \qquad \text{für } m \neq 0 \tag{B.89}$$

Etwas Vorsicht ist angebracht. Wir haben in Abschnitt B.5.2 verschiedene ganzzahlige Divisionen kennengelernt; die obige Äquivalenz gilt *nur* für periodische Restfunktionen wie ***mod***, $\overline{\textbf{\textit{mod}}}$ und ***emod***. Die in F# als Operator % vordefinierte Restfunktion ***rem*** gehört nicht dazu: $1 \equiv -1 \pmod{2}$, aber $1 \ \textbf{\textit{rem}} \ 2 = 1 \neq -1 = (-1) \ \textbf{\textit{rem}} \ 2$.

Summe, Differenz und Produkt kongruenter Zahlen ergeben wieder kongruente Zahlen. Man sagt auch, die Äquivalenzrelation verträgt sich mit der algebraischen Struktur der ganzen Zahlen, oder etwas knackiger: $\equiv$ ist eine ***Kongruenzrelation***.

$$a_1 \equiv b_1 \pmod{m} \ \wedge \ a_2 \equiv b_2 \pmod{m} \ \Longrightarrow \ a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \tag{B.90a}$$
$$a_1 \equiv b_1 \pmod{m} \ \wedge \ a_2 \equiv b_2 \pmod{m} \ \Longrightarrow \ a_1 - a_2 \equiv b_1 - b_2 \pmod{m} \tag{B.90b}$$
$$a_1 \equiv b_1 \pmod{m} \ \wedge \ a_2 \equiv b_2 \pmod{m} \ \Longrightarrow \ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m} \tag{B.90c}$$

Zum Beweis formen wir die Differenzen geschickt um.

$$
\begin{array}{ll}
 & a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & m \setminus ((a_1 + a_2) - (b_1 + b_2)) \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & m \setminus ((a_1 - b_1) + (a_2 - b_2)) \\
\impliedby & \quad \{ \text{ Linearkombinationen (B.80) } \} \\
 & m \setminus (a_1 - b_1) \ \wedge \ m \setminus (a_2 - b_2) \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & a_1 \equiv b_1 \pmod{m} \ \wedge \ a_2 \equiv b_2 \pmod{m}
\end{array}
\qquad
\begin{array}{ll}
 & a_1 - a_2 \equiv b_1 - b_2 \pmod{m} \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & m \setminus ((a_1 - a_2) - (b_1 - b_2)) \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & m \setminus ((a_1 - b_1) - (a_2 - b_2)) \\
\impliedby & \quad \{ \text{ Linearkombinationen (B.80) } \} \\
 & m \setminus (a_1 - b_1) \ \wedge \ m \setminus (a_2 - b_2) \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & a_1 \equiv b_1 \pmod{m} \ \wedge \ a_2 \equiv b_2 \pmod{m}
\end{array}
$$

Nicht ganz so offensichtlich ist die Umformung im Fall der Multiplikation.

$$
\begin{array}{ll}
 & a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m} \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & m \setminus ((a_1 \cdot a_2) - (b_1 \cdot b_2)) \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & m \setminus ((a_1 - b_1) \cdot a_2 + b_1 \cdot (a_2 - b_2)) \\
\impliedby & \quad \{ \text{ Linearkombinationen (B.80) } \} \\
 & m \setminus (a_1 - b_1) \ \wedge \ m \setminus (a_2 - b_2) \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & a_1 \equiv b_1 \pmod{m} \ \wedge \ a_2 \equiv b_2 \pmod{m}
\end{array}
$$

Anwendung: Kachelung Aus der Kongruenzregel für die Multiplikation (B.90c) folgt mit einem Induktionsbeweis, dass auch natürliche Potenzen Kongruenzen erhalten:

$$a \equiv b \pmod{m} \quad \Longrightarrow \quad a^n \equiv b^n \pmod{m}$$

für alle $n \in \mathbb{N}$. In Abschnitt B.3 haben wir uns mit der Kachelung von Schachbrettern beschäftigt. Wenn ein $2^n \times 2^n$ großes Schachbrett mit L-Trominos gekachelt wird, muss notwendigerweise ein Feld frei bleiben, da $2^n \times 2^n \equiv 4^n \equiv 1^n \equiv 1 \pmod{3}$. Welche Spielfeldgrößen, sprich welche Quadratzahlen, lassen sich überhaupt ohne Rest durch 3 teilen? Nur Spielfelder mit einer durch 3 teilbaren Seitenlänge:

$$
\begin{aligned}
(3 \cdot k + 0)^2 &\equiv 9 \cdot k^2 + 6 \cdot k \cdot 0 + 0 \equiv 0 \equiv 0 \pmod{3} \\
(3 \cdot k + 1)^2 &\equiv 9 \cdot k^2 + 6 \cdot k \cdot 1 + 1 \equiv 1 \equiv 1 \pmod{3} \\
(3 \cdot k + 2)^2 &\equiv 9 \cdot k^2 + 6 \cdot k \cdot 2 + 4 \equiv 4 \equiv 1 \pmod{3}
\end{aligned}
$$

Da $9 \equiv 6 \equiv 0 \pmod{3}$, fallen die ersten beiden Summenglieder jeweils weg.

Anwendung: Teilbarkeitsregeln Apropos Teilbarkeit durch 3, Sie erinnern sich bestimmt noch an den Rechentrick mit der Quersumme. Um im Kopf zu überprüfen, ob eine *Dezimal*zahl durch 3 teilbar ist, bildet man zunächst deren ***Quersumme***, die Summe ihrer Ziffern, und prüft anschließend, ob die Quersumme durch 3 teilbar ist — gegebenenfalls, indem man den Trick rekursiv auf die Quersumme anwendet. Für alle kleinen Teiler gibt es ähnliche, »magische« Kopfrechentricks (Lesebrille auf die Nase; Zahl meint jeweils *Dezimal*zahl; Aufgabe B.5.23 beschäftigt sich mit der Korrektheit der Tricks):

Eine Zahl ist genau dann durch 2 teilbar, wenn ihre letzte Ziffer gerade ist.
Eine Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.
Eine Zahl ist genau dann durch 4 teilbar, wenn die Zahl, die aus ihren letzten beiden Ziffern gebildet wird, durch 4 teilbar ist.
Eine Zahl ist genau dann durch 5 teilbar, wenn ihre letzte Ziffer durch 5 teilbar ist.
Eine Zahl ist genau dann durch 6 teilbar, wenn sie durch 2 und durch 3 teilbar ist.
Eine Zahl ist genau dann durch 7 teilbar, wenn ihre alternierende 3er-Quersumme durch 7 teilbar ist.
Eine Zahl ist genau dann durch 8 teilbar, wenn die Zahl, die aus ihren letzten drei Ziffern gebildet wird, durch 8 teilbar ist.
Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.
Eine Zahl ist genau dann durch 10 teilbar, wenn ihre letzte Ziffer durch 10 teilbar ist.
Eine Zahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

Auch für das »quinäre Streichholzsystem« lassen sich entsprechende Regeln aufstellen. Im quinären System kann man mit der Quersumme die Teilbarkeit durch 2 überprüfen.

$$(|,||,||||,\text{𝍸},||)_5 \equiv |+||+||||+\text{𝍸}+|| \equiv (||,||||)_5 \equiv ||+|||| \equiv (|,|)_5 \equiv |+| \equiv (||)_5 \pmod{||}$$

Für die Teilbarkeit durch 3 greift man auf die ***alternierende Quersumme*** zurück: Beginnend mit der *niedrigstwertigen* Ziffer, also ganz rechts, werden die Ziffern abwechselnd addiert und subtrahiert.

$$(|,||,||||,\text{𝍸},||)_5 \equiv |-||+||||-\text{𝍸}+|| \equiv ()_5 \pmod{|||}$$

Die Quinärzahl $(|,||,||||,\text{𝍸},||)_5$ ist somit sowohl durch $||$ als auch durch $|||$ teilbar. Beide Verfahren basieren auf der gleichen Überlegung: Die Teilbarkeit einer Quinärzahl, einer Zahl der Form $r + q \cdot 5$, lässt sich in einfacher Weise auf die Teilbarkeit von r und q zurückführen, wenn die Basis 5 zu einem einfachem Faktor, etwa -1, 0 oder 1, kongruent ist. Aus $5 \equiv 1 \pmod 2$ folgt zum Beispiel mit den Kongruenzregeln $r + q \cdot 5 \equiv r + q \pmod 2$. Die Quinärzahl hat den gleichen 2-er Rest wie ihre Quersumme — da die Ziffer r beliebig ist, gilt dies sogar unabhängig vom Ziffernvorrat. Ähnlich abkürzende Rechenwege lassen sich für alle Teiler von 2 bis 6 finden:

$$\begin{array}{llll}
r + q \cdot \text{𝍸} \equiv r + q & \pmod{||} & \text{da} \quad \text{𝍸} \equiv | & \pmod{||} \\
r + q \cdot \text{𝍸} \equiv r - q & \pmod{|||} & \text{da} \quad \text{𝍸} \equiv -| & \pmod{|||} \\
r + q \cdot \text{𝍸} \equiv r + q & \pmod{||||} & \text{da} \quad \text{𝍸} \equiv | & \pmod{||||} \\
r + q \cdot \text{𝍸} \equiv r & \pmod{\text{𝍸}} & \text{da} \quad \text{𝍸} \equiv & \pmod{\text{𝍸}} \\
r + q \cdot \text{𝍸} \equiv r - q & \pmod{\text{𝍸}|} & \text{da} \quad \text{𝍸} \equiv -| & \pmod{\text{𝍸}|}
\end{array}$$

Wenn man möchte, kann man die Formeln wieder in prosaische Kopfrechenregeln übersetzen — die jetzt vielleicht etwas von ihrer Magie eingebüßt haben.

Eine Quinärzahl ist genau dann durch 2 teilbar, wenn ihre Quersumme durch 2 teilbar ist.
Eine Quinärzahl ist genau dann durch 3 teilbar, wenn ihre alternierende Quersumme durch 3 teilbar ist.
Eine Quinärzahl ist genau dann durch 4 teilbar, wenn ihre Quersumme durch 4 teilbar ist.
Eine Quinärzahl ist genau dann durch 5 teilbar, wenn ihre letzte Ziffer durch 5 teilbar ist.
Eine Quinärzahl ist genau dann durch 6 teilbar, wenn ihre alternierende Quersumme durch 6 teilbar ist.

Modulararithmetik Wenden wir uns wieder dem Ausgangspunkt unserer Überlegungen, der Modulararithmetik, zu und überlegen zunächst, welche liebgewonnenen Rechengesetze für die »gekringelten« Operationen (B.87a)–(B.87c) gelten. Sind $\oplus$ und $\odot$ assoziativ, distribuiert $\odot$ über $\oplus$? Zur Klärung dieser Fragen setzen wir die Restfunktion mit der Kongruenzrelation in Beziehung:

$$a \ \textbf{\textit{mod}} \ m \equiv a \pmod m$$

Offensichtlich, oder? Ein Beweis kann aber nicht schaden:

$$\begin{array}{ll}
 & a \ \textbf{\textit{mod}} \ m \equiv a \pmod m \\
\iff & \quad \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
 & m \setminus a \ \textbf{\textit{mod}} \ m - a \\
\iff & \quad \{ \text{ Divisionsregel (B.48a) } \} \\
 & m \setminus a - a \ \textbf{\textit{div}} \ m \cdot m - a \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & m \setminus -a \ \textbf{\textit{div}} \ m \cdot m
\end{array}$$

Da wir für den Nachweis im Wesentlichen die Divisionsregel verwenden, gilt die Eigenschaft für beliebige Restfunktionen (insbesondere auch für ***rem***). Weiterhin folgt, dass $a \oplus b \equiv a + b \pmod{m}$, $a \ominus b \equiv a - b \pmod{m}$ und $a \odot b \equiv a \cdot b \pmod{m}$. Somit erben die Operationen der Modulararithmetik die Eigenschaften der Standardarithmetik, zum Beispiel ist $\oplus$ assoziativ:

$$(a \oplus b) \oplus c \equiv (a + b) + c \equiv a + (b + c) \equiv a \oplus (b \oplus c)$$

Beim Führen von Beweisen können wir uns aussuchen, ob wir mit den gekringelten Operationen ($\oplus$, $\ominus$ und $\odot$) und der Gleichheit ($=$) rechnen, oder alternativ mit den normalen Operationen ($+$, $-$ und $\cdot$) und den Kongruenzen ($\equiv$). Letztere Option hat den kleinen Vorteil, dass die Notation es uns leicht macht, den Modulo explizit anzugeben oder implizit zu lassen. Außerdem sind wir mit Addition, Subtraktion und Multiplikation seit der Grundschule vertraut.

Ach ja, wir müssen noch klären, warum 10! kongruent zu 0 ist.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv 1 \cdot 3 \cdot 5 \cdot 3 \cdot 7 \cdot 9 \cdot 2^8 \equiv 0 \pmod{2^8}$$

In den einzelnen Faktoren sind gerade soviele 2-er Potenzen enthalten, dass das Ergebnis durch 2^8 teilbar ist.

Beweise und Beweistechniken

Mettant des choses égales à la place, l'égalité demeure.

— Gottfried Wilhelm Leibniz (1646 – 1716), *Opera Philosophica*

An dieser Stelle ergreifen wir die Gelegenheit beim Schopfe, ein paar prinzipielle Betrachtungen zum Rechnen und Beweisen anzustellen. Durch jahrelanges Training geschult (gedrillt?) ersetzen wir routinemäßig Teilausdrücke durch gleichwertige Ausdrücke: So wird aus $2 \cdot (3 + 5)$ der Ausdruck $2 \cdot 8$, da $3+5$ gleich 8 ist. Um es in den Worten von Leibniz zu sagen: »Wenn man Gleiches an die Stelle setzt, bleibt die Gleichung bestehen.« (Identitätsprinzip oder Prinzip der Ersetzbarkeit). Dieses Prinzip lässt sich sogar zur *definierenden* Eigenschaft der Gleichheit erheben.[24]

$$a = b \quad :\Longleftrightarrow \quad \forall\, \mathrm{P}\ .\ \mathrm{P}(a) \Longrightarrow \mathrm{P}(b)$$

Zwei Objekte sind gleich, wenn es keine Eigenschaft gibt, anhand derer sich die Objekte unterscheiden lassen (Prinzip der Identität des Ununterscheidbaren, lat. principium identitatis indiscernibilium). Ähnliche Überlegungen liegen den indirekten Beweisen (B.15a)-(B.15d) zugrunde: Zwei Objekte sind gleich, wenn sie sich zu allen Objekte gleich verhalten. Kommen wir noch einmal auf unser Ausgangsbeispiel zurück: $2 \cdot (3 + 5) = 2 \cdot 8$. Setzen wir $f(x) := 2 \cdot x$, so folgern wir aus $3 + 5 = 8$ den Zusammenhang $f(3 + 5) = f(8)$. Das zugrundeliegende Beweisprinzip lässt sich aus der Definition der Gleichheit ableiten.[25]

$$a = b \quad \Longrightarrow \quad f(a) = f(b)$$

Auf gleiche Argumente angewendet, liefert eine Funktion gleiche Ergebnisse.

[24] Da in der Formel über Prädikate quantifiziert wird, verlassen wir die Prädikatenlogik 1. Stufe. Es ist vielleicht nicht unmittelbar klar, dass auf diese Weise überhaupt eine *Äquivalenzrelation* definiert wird. Während Reflexivität und Transitivität nicht schwer nachzuweisen sind, erscheint die Symmetrie fraglich. Ist sie aber nicht: Wir müssen zum Nachweis nur die außerordentliche Ausdruckskraft der Logik 2. Stufe ausnutzen. Es gilt, aus $a = b$ die Aussage $b = a$ zu folgern. Dazu definieren wir das Prädikat $\mathrm{P}(x) := (x = a)$. Aufgrund der Reflexivität gilt $\mathrm{P}(a)$; mit der Annahme $a = b$ können wir dann aus $\mathrm{P}(a)$ wie gewünscht die Aussage $\mathrm{P}(b)$ schließen.

[25] Dazu gehen wir ähnlich wie beim Nachweis der Symmetrie vor. Wir definieren das Prädikat $\mathrm{P}(x) := (f(a) = f(x))$. Aufgrund der Reflexivität gilt $\mathrm{P}(a)$; mit der Annahme $a = b$ können wir dann aus $\mathrm{P}(a)$ die Aussage $\mathrm{P}(b)$ schließen.

Wenn wir statt Gleichungen Ungleichungen betrachten, gilt die Implikation nicht länger uneingeschränkt. (Beachte: Die beteiligten Ordnungen können verschieden sein.)

$$a \leqslant b \quad \Longrightarrow \quad f(a) \sqsubseteq f(b)$$

Die Funktion muss sich mit den beiden Ordnungen vertragen; sie muss ordnungserhaltend oder monoton sein: $f(x) = 2 \cdot x$ ist zulässig, ebenso $g(x) = -2 \cdot x$ (die Ordnung wird auf den Kopf gestellt), nicht aber $h(x) = x^2$, da $h(-1) \geqslant h(0) \leqslant h(1)$.

Analoge Einschränkungen gelten für die Arbeit mit Kongruenzen.

$$a \equiv b \pmod{m} \quad \Longrightarrow \quad f(a) \equiv f(b) \pmod{n}$$

Die Funktion muss sich mit den beiden Kongruenzrelationen vertragen. Die Kongruenzregeln (B.90a)–(B.90c) garantieren die Verträglichkeit von Addition, Subtraktion und Multiplikation für den Fall $m = n$. Wir haben in den vorangegangenen Rechnungen regen Gebrauch von dieser Eigenschaft gemacht, zum Beispiel haben wir aus $5 \equiv 1 \pmod 2$ die Kongruenz $r + q \cdot 5 \equiv r + q \cdot 1 \pmod 2$ gefolgert — »mitten in einem Ausdruck« wird 5 durch 1 ersetzt. In Abwandlung von Leibniz' Worten können wir darauf vertrauen, dass »Wenn man Kongruentes an die Stelle setzt, bleibt die Kongruenz bestehen.«

Auf der Liste der zulässigen Funktionen gibt es eine verdächtige Lücke: Weder die ganzzahlige Division noch die Restfunktion sind aufgeführt. Zu Recht! Treppenfunktionen vertragen sich nicht mit Kongruenzen: $6 \equiv 10 \pmod 2$, aber $6 \mathbin{\textbf{\textit{div}}} 3 \not\equiv 10 \mathbin{\textbf{\textit{div}}} 3 \pmod 2$ und $6 \mathbin{\textbf{\textit{mod}}} 3 \not\equiv 10 \mathbin{\textbf{\textit{mod}}} 3 \pmod 2$. Obwohl die Argumente gerade sind, besitzen Quotient und Rest jeweils eine unterschiedliche Parität. Selbst wenn die Division glatt aufgeht, darf man nicht einfach kürzen: $2 \equiv 4 \pmod 2$, aber $2 \mathbin{\textbf{\textit{div}}} 2 \not\equiv 4 \mathbin{\textbf{\textit{div}}} 2 \pmod 2$. Mit anderen Worten, aus $1 \cdot 2 \equiv 2 \cdot 2 \pmod 2$ dürfen wir *nicht* $1 \equiv 2 \pmod 2$ folgern. Es gelten lediglich die folgenden Vereinfachungs- bzw. Kürzungsregeln:

$$a + d \equiv b + d \pmod{m} \quad \Longleftrightarrow \quad a \equiv b \pmod{m} \tag{B.91a}$$

$$a \cdot d \equiv b \cdot d \pmod{m} \quad \Longleftrightarrow \quad a \equiv b \pmod{m} \qquad \text{falls } d \mathbin{\textbf{\textit{gcd}}} m = 1 \tag{B.91b}$$

Die erste Äquivalenz zeigen wir mit einem Ping-Pong Beweis.

$$\begin{aligned}
& a + d \equiv b + d \pmod{m} \\
\Longrightarrow \quad & \{ \text{ Kongruenzregel Subtraktion (B.90b) } \} \\
& (a + d) - d \equiv (b + d) - d \pmod{m} \\
\Longleftrightarrow \quad & \{ \text{ Inverse } \} \\
& a \equiv b \pmod{m} \\
\Longrightarrow \quad & \{ \text{ Kongruenzregel Addition (B.90a) } \} \\
& a + d \equiv b + d \pmod{m}
\end{aligned}$$

Der Beweis illustriert exemplarisch, wie Inverse bei der Manipulation von Formeln eingesetzt werden. Losgelöst von konkreten Operationen sieht die Argumentation wie folgt aus: $a \sim b \Longleftrightarrow f(a) \equiv f(b)$ ist erfüllt (die Kongruenzen können verschieden sein), wenn f eine Linksinverse g besitzt, $g(f(x)) = x$, und wenn f *und* g kongruenzerhaltend sind.

$$a \sim b \quad \Longrightarrow \quad f(a) \equiv f(b) \quad \Longrightarrow \quad g(f(a)) \sim g(f(b)) \quad \Longleftrightarrow \quad a \sim b$$

Eine analoge Argumentation wendet man bei Ungleichungen an: $a \leqslant b \Longleftrightarrow f(a) \sqsubseteq f(b)$ ist erfüllt (die Ordnungen können verschieden sein), wenn f eine Linksinverse g besitzt, $g(f(x)) = x$,

und wenn f *und* g ordnungserhaltend sind. (Zur Erinnerung: In diesem Fall nennt man f eine ***Ordnungseinbettung***.)

$$a \leqslant b \quad\Longrightarrow\quad f(a) \sqsubseteq f(b) \quad\Longrightarrow\quad g(f(a)) \leqslant g(f(b)) \quad\Longleftrightarrow\quad a \leqslant b$$

Es wird oft übersehen, dass *sowohl f als auch die Linksinverse g* die jeweilige mathematische Struktur erhalten müssen.

Wenden wir uns dem Beweis von (B.91b) zu: Die obige Argumentation verfängt bei der Multiplikation nicht, da diese nur eine Quasiinverse, aber keine Inverse besitzt. Wir führen einen Ping-Pong Beweis. »$\Longleftarrow$«: Die Rückrichtung folgt aus der Kongruenzeigenschaft der Multiplikation (B.90c). »$\Longrightarrow$«: Aus der Annahme d ***gcd*** $m = 1$ erhalten wir mit dem erweiterten Euklidischen Algorithmus (B.85) Konstanten d' und m', so dass $d' \cdot d + m' \cdot m = 1$. Daraus folgt unmittelbar, dass $d' \cdot d \equiv 1 \pmod{m}$. Damit lässt sich der Faktor kürzen:

$$\begin{aligned}
& a \cdot d \equiv b \cdot d \pmod{m} \\
\Longrightarrow\quad & \{\ \text{Kongruenzregel Multiplikation (B.90c)}\ \} \\
& a \cdot d \cdot d' \equiv b \cdot d \cdot d' \pmod{m} \\
\Longrightarrow\quad & \{\ d' \cdot d \equiv 1 \pmod{m}\ \} \\
& a \equiv b \pmod{m}
\end{aligned}$$

Rechnen mit unterschiedlichen Resten Bis dato haben wir bei der Umformung von Kongruenzen den Modulo nicht verändert. Lassen wir diese Einschränkung fallen, ergeben sich neue »Manipulationsmöglichkeiten«. Zum Beispiel hat die Kürzungsregel (B.79a) aus Abschnitt B.5.4 ein direktes Pendant:

$$a \cdot d \equiv b \cdot d \pmod{m \cdot d} \quad\Longleftrightarrow\quad a \equiv b \pmod{m} \qquad \text{falls } d \neq 0 \tag{B.92}$$

Ein Faktor lässt sich kürzen, wenn dieser auf beiden Seiten der Kongruenz *und* zusätzlich im Modulo auftritt.

$$\begin{aligned}
& a \cdot d \equiv b \cdot d \pmod{m \cdot d} \\
\Longleftrightarrow\quad & \{\ \text{Definition »}\equiv\text{« (B.88)}\ \} \\
& m \cdot d \setminus (a \cdot d - b \cdot d) \\
\Longleftrightarrow\quad & \{\ \text{Distributivgesetz}\ \} \\
& m \cdot d \setminus (a - b) \cdot d \\
\Longleftrightarrow\quad & \{\ \text{Kürzungsregel (B.79a) und } d \neq 0\ \} \\
& m \setminus (a - b) \\
\Longleftrightarrow\quad & \{\ \text{Definition »}\equiv\text{« (B.88)}\ \} \\
& a \equiv b \pmod{m}
\end{aligned}$$

Die beiden Kürzungsregeln für Produkte, (B.91b) und (B.92), lassen sich zu einer Regel zusammenfassen.

$$a \cdot d \equiv b \cdot d \pmod{m} \quad\Longleftrightarrow\quad a \equiv b \pmod{m/(d \textbf{ gcd } m)} \tag{B.93}$$

Umgekehrt lässt sich die verallgemeinerte Regel auf die beiden Spezialfälle zurückführen. Sei $g := d$ ***gcd*** m, dann

$$\begin{aligned}
& a \equiv b \pmod{m/g} \\
\Longleftrightarrow\quad & \{\ \text{(B.91b) und } (d/g) \textbf{ gcd } (m/g) = 1\ \} \\
& a \cdot d/g \equiv b \cdot d/g \pmod{m/g} \\
\Longleftrightarrow\quad & \{\ \text{(B.92)}\ \} \\
& a \cdot d \equiv b \cdot d \pmod{m}
\end{aligned}$$

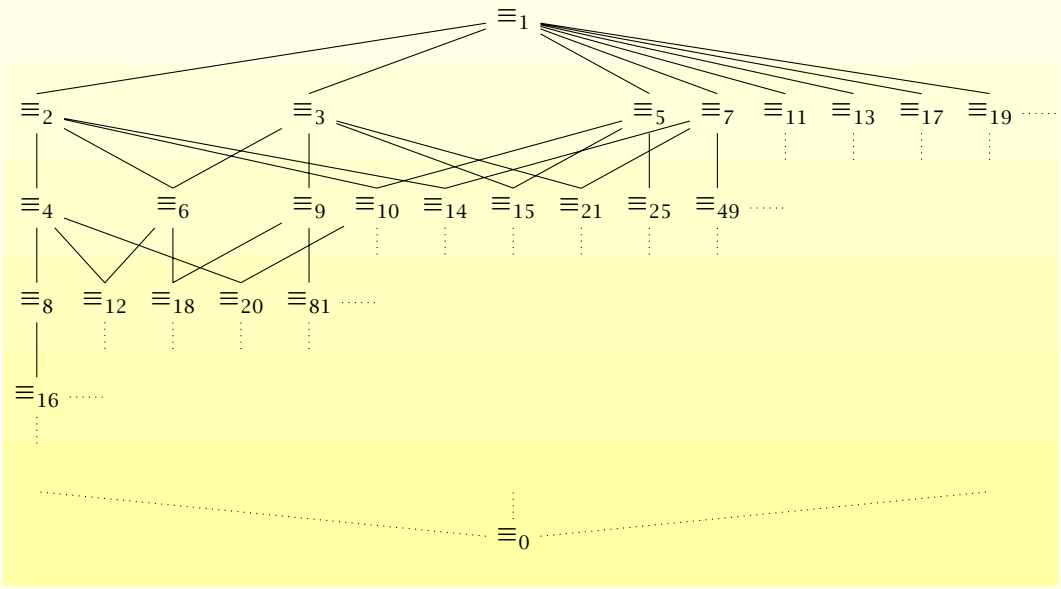


Abbildung B.15.: Ein Ausschnitt aus dem Verband der Kongruenzrelationen $(\{\equiv_m \mid m \in \mathbb{Z}\}, \subseteq)$.

Teilbarkeit und Äquivalenzrelationen Mit Hilfe von Definition B.88 wird jeder ganzen Zahl eine Äquivalenzrelation zugeordnet: $m \mapsto \equiv_m$. Im Folgenden wollen wir uns die Eigenschaften dieser Zuordnung genauer anschauen. Äquivalenzrelationen lassen sich mit der Teilmengenbeziehung anordnen, siehe Abbildungen B.8 und B.9. Wie wir in Abschnitt B.4.4 gesehen haben, bildet die Menge aller Äquivalenzrelationen $(Eq(\mathrm{U}), \subseteq)$ über einer Grundmenge U sogar einen vollständigen Verband. Betrachten wir ein paar Beispiele: Die Relation $\equiv_{100}$ unterscheidet positive Dezimalzahlen bezüglich der letzten beiden Ziffern; $\equiv_{10}$ nur bezüglich der letzten. Die Relation $\equiv_{100}$ ist feiner als $\equiv_{10}$; umgekehrt ist $\equiv_{10}$ gröber als $\equiv_{100}$, als Mengeninklusion geschrieben: $(\equiv_{10}) \supseteq (\equiv_{100})$. Im Allgemeinen gilt der folgende Zusammenhang:

$$m \setminus n \quad \Longleftrightarrow \quad (\equiv_m) \supseteq (\equiv_n) \tag{B.94}$$

Mit anderen Worten, die Zuordnung von Zahlen zu Äquivalenzrelationen, $m \mapsto \equiv_m$, ist eine *ordnungsumkehrende Einbettung* von $(\mathbb{Z}, \setminus)$ nach $(Eq(\mathbb{Z}), \subseteq)$. Der Beweis macht deutlich, dass $(\equiv_m) \supseteq (\equiv_n)$ im Wesentlichen eine »indirekte Variante« von $m \setminus n$ ist (siehe letzte Umformung).

$$
\begin{aligned}
& (\equiv_m) \supseteq (\equiv_n) \\
\Longleftrightarrow \quad & \{ \text{ Definition Obermenge } \} \\
& \forall\, a \;.\; \forall\, b \;.\; a \equiv_m b \quad \Longleftarrow \quad a \equiv_n b \\
\Longleftrightarrow \quad & \{ \text{ Definition »}\equiv\text{«} \text{ (B.88) } \} \\
& \forall\, a \;.\; \forall\, b \;.\; m \setminus a - b \quad \Longleftarrow \quad n \setminus a - b \\
\Longleftrightarrow \quad & \{ \text{ »}\Longrightarrow\text{«: } a := x \text{ und } b := 0\text{; »}\Longleftarrow\text{«: } x := a - b \} \\
& \forall\, x \;.\; m \setminus x \quad \Longleftarrow \quad n \setminus x \\
\Longleftrightarrow \quad & \{ \text{ indirekter Beweis (B.15c) } \} \\
& m \setminus n
\end{aligned}
$$

Versorgen wir die Relationen $\equiv_m$ und $\equiv_n$ mit Argumenten, dann lässt sich die Links-nach-rechts-Richtung von (B.94) etwas lesbarer aufschreiben:

$$a \equiv b \pmod{m} \quad \Longleftarrow \quad a \equiv b \pmod{n} \qquad \text{falls } m \setminus n \tag{B.95}$$

Sowohl $(\mathbb{Z}, \setminus)$ als auch $(Eq(\mathbb{Z}), \subseteq)$ ist ein vollständiger Verband. Die Zuordnung von Zahlen zu Äquivalenzrelationen, $m \mapsto \equiv_m$, erhält auch Suprema: Aufgrund der Antitonie wird das kleinste gemeinsame Vielfache, das *Supremum* in $(\mathbb{Z}, \setminus)$, auf den Durchschnitt von Relationen, das *Infimum* in $(Eq(\mathbb{Z}), \subseteq)$, abgebildet. Die Abbildung B.12 wird durch die Zuordnung auf den Kopf gestellt, siehe Abbildung B.15.

$$(\equiv_{m \,\mathbf{lcm}\, n}) = (\equiv_m) \cap (\equiv_n)$$

Setzen wir die Definitionen ein, erhalten wir die folgende Äquivalenz.

$$a \equiv b \pmod{m \;\mathbf{lcm}\; n} \quad \Longleftrightarrow \quad a \equiv b \pmod{m} \;\wedge\; a \equiv b \pmod{n} \tag{B.96}$$

Ein Spezialfall dieser Regel ist uns übrigens schon untergekommen, als wir Kopfrechentricks für die Teilbarkeit von Dezimalzahlen diskutiert haben.

Eine Zahl ist genau dann durch 6 teilbar, wenn sie durch 2 und durch 3 teilbar ist.

Der Beweis von (B.96) ist erschreckend einfach.

$$\begin{aligned}
& a \equiv b \pmod{m \;\mathbf{lcm}\; n} \\
\Longleftrightarrow \quad & \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
& m \;\mathbf{lcm}\; n \setminus (a - b) \\
\Longleftrightarrow \quad & \{ \text{ Supremum (B.18) } \} \\
& m \setminus (a - b) \;\wedge\; n \setminus (a - b) \\
\Longleftrightarrow \quad & \{ \text{ Definition »}\equiv\text{« (B.88) } \} \\
& a \equiv b \pmod{m} \;\wedge\; a \equiv b \pmod{n}
\end{aligned}$$

Zum Schluss des Abschnitts wenden wir uns noch einer Anwendung zu.

Residuenzahlensysteme Durch die Rechenbrille betrachtet besagt (B.96), dass wir eine Rechnung mit größerer Genauigkeit durch zwei voneinander *unabhängige* Rechnungen mit geringerer Genauigkeit realisieren können. Zum Beispiel gilt $a \equiv b + c \pmod{(m \;\mathbf{lcm}\; n)}$ genau dann, wenn sowohl $a \equiv b + c \pmod{m}$ als auch $a \equiv b + c \pmod{n}$ erfüllt sind. Im sogenannten ***Residuenzahlensystem*** wird die Zahl z durch die beiden Reste $(z \;\mathbf{mod}\; m, z \;\mathbf{mod}\; n)$ repräsentiert — wenn man möchte, kann man die Komponenten des Paares als Ziffern ansehen. Die arithmetischen Operationen werden komponentenweise, jeweils modulararithmetisch durchgeführt.

$$\begin{aligned}
(a_1, a_2) \oplus (b_1, b_2) &= ((a_1 + b_1) \;\mathbf{mod}\; m, (a_2 + b_2) \;\mathbf{mod}\; n) \\
(a_1, a_2) \ominus (b_1, b_2) &= ((a_1 - b_1) \;\mathbf{mod}\; m, (a_2 - b_2) \;\mathbf{mod}\; n) \\
(a_1, a_2) \odot (b_1, b_2) &= ((a_1 \cdot b_1) \;\mathbf{mod}\; m, (a_2 \cdot b_2) \;\mathbf{mod}\; n)
\end{aligned}$$

Schauen wir uns ein konkretes Beispiel an ($m := 2$ und $n := 3$).

z	x	y	$3 \cdot x - 2 \cdot y$
0	0	0	0
1	1	1	1
2	0	2	−4
3	1	0	3
4	0	1	−8
5	1	2	−1

$$\begin{aligned}
x &= z \;\mathbf{mod}\; 2 \\
y &= z \;\mathbf{mod}\; 3 \\
z &= (3 \cdot x - 2 \cdot y) \;\mathbf{mod}\; 6
\end{aligned}$$

Zum Beispiel wird die Zahl 3 durch $(1,0)$ und die Zahl 5 durch $(1,2)$ repräsentiert; die Summe der beiden Zahlen ist $(0,2)$ also 2, das Produkt $(1,0)$ also 3; und tatsächlich gilt: $3+5 \equiv 2 \pmod 6$ und $3 \cdot 5 \equiv 3 \pmod 6$.

Wenn m und n teilerfremd sind, $m \mathbin{\textbf{\textit{gcd}}} n = 1$ und somit $m \mathbin{\textbf{\textit{lcm}}} n = m \cdot n$, dann enthält die Tabelle alle möglichen Paare. (Welche Paare fehlen, wenn das nicht der Fall ist, zum Beispiel, für $m := 6$ und $n := 10$?) Mit anderen Worten, die Zuordnung von Zahlen zu Ziffernpaaren ist umkehrbar eindeutig. Für die »Hinrichtung« bilden wir wie schon besprochen eine Zahl auf die beiden Reste ab: $z \mapsto (z \mathbin{\textbf{\textit{mod}}} m, z \mathbin{\textbf{\textit{mod}}} n)$. Die »Rückrichtung« ist weniger offensichtlich. Im obigen Beispiel lassen sich die Ziffern mittels $(x,y) \mapsto (3 \cdot x - 2 \cdot y) \mathbin{\textbf{\textit{mod}}} 6$ zur ursprünglichen Zahl zusammensetzen. Aber, wie kommt man auf diese Linearkombination?

Als erstes Etappenziel bestimmen wir Koeffizienten a und b, so dass x und y kongruent zu einer Linearkombination von x und y sind. (Sehen Sie, warum uns dieser Schritt weiterhilft?)

$$x \equiv a \cdot x + b \cdot y \pmod m \qquad\qquad y \equiv a \cdot x + b \cdot y \pmod n \tag{B.97a}$$

Machen wir uns das Leben leicht: Wenn einer der Koeffizienten kongruent zu Null und der andere kongruent zu Eins ist, dann wird (B.97a) offensichtlich erfüllt.

$$\begin{aligned} a \equiv 1 \pmod m \;\wedge\; b \equiv 0 \pmod m \quad &\Longrightarrow \quad x \equiv a \cdot x + b \cdot y \pmod m \\ a \equiv 0 \pmod n \;\wedge\; b \equiv 1 \pmod n \quad &\Longrightarrow \quad y \equiv a \cdot x + b \cdot y \pmod n \end{aligned}$$

Die Anforderung $a \equiv 0 \pmod n$ bedeutet, dass a ein Vielfaches von n ist und $b \equiv 0 \pmod m$ entsprechend, dass b ein Vielfaches von m ist. Die beiden übrigen Anforderungen lassen sich erfüllen, wenn $a + b = 1$ ist: Dann gilt $a \equiv a + 0 \equiv a + b \equiv 1 \pmod m$ und $b \equiv 0 + b \equiv a + b \equiv 1 \pmod n$. Zahlen mit den erforderlichen Eigenschaften ermittelt der erweiterte Euklidische Algorithmus (der mittlerweile zum unentbehrlichen Helfer avanciert):

$$m \mathbin{\textbf{\textit{gcd}}} n = m' \cdot m + n' \cdot n = 1 \qquad a := n' \cdot n \qquad b := m' \cdot m \tag{B.97b}$$

Wie gewünscht ist a ein Vielfaches von n, b ein Vielfaches von m und $a + b = 1$, sofern m *und* n *teilerfremd sind.* Für unser laufendes Beispiel erhalten wir $a := 3$ und $b := -2$, da $2 \mathbin{\textbf{\textit{gcd}}} 3 = -1 \cdot 2 + 1 \cdot 3 = 1$.

Der sogenannte ***Chinesische Restsatz***[26] fasst unsere Überlegungen zusammen: Wenn m und n teilerfremd sind, dann

$$x \equiv z \pmod m \;\wedge\; y \equiv z \pmod n \iff a \cdot x + b \cdot y \equiv z \pmod{m \cdot n} \tag{B.97c}$$

wobei a und b wie in (B.97b) definiert sind. Der Beweis führt die Aussage auf (B.96) zurück.

$$\begin{aligned} & x \equiv z \pmod m \;\wedge\; y \equiv z \pmod n \\ \iff & \quad \{ \text{ Annahme (B.97a) und Transitivität } \} \\ & a \cdot x + b \cdot y \equiv z \pmod m \;\wedge\; a \cdot x + b \cdot y \equiv z \pmod n \\ \iff & \quad \{ \text{ (B.96) und } m \mathbin{\textbf{\textit{gcd}}} n = 1 \} \\ & a \cdot x + b \cdot y \equiv z \pmod{m \cdot n} \end{aligned}$$

[26] Der Chinesische Restsatz wird oft als Existenzaussage formuliert:

$$\forall\, x \,.\, \forall\, y \,.\, \exists_1 z \,.\, 0 \leqslant z < m \cdot n \quad \wedge \quad x \equiv z \pmod m \quad \wedge \quad y \equiv z \pmod n$$

Wir ersetzen den Existenzquantor durch eine 2-parametrige Skolemfunktion:

$$\forall\, x \,.\, \forall\, y \,.\, \exists_1 z \,.\, x \equiv z \pmod m \;\wedge\; y \equiv z \pmod n \quad \iff \quad f(x,y) \equiv z \pmod{m \cdot n}$$

Die Funktion f wählt einen Repräsentanten für z aus; die Rückrichtung »$\Longleftarrow$« besagt, dass $f(x,y)$ die geforderte Eigenschaft besitzt; die Hinrichtung »$\Longrightarrow$« formalisiert, dass z eindeutig modulo $m \cdot n$ bestimmt ist.

Der Chinesische Restsatz etabliert eine Eins-zu-eins-Korrespondenz zwischen Zahlen und Ziffernpaaren und bildet so die Grundlage von Residuenzahlensystemen:

$$\{0,\ldots,m\cdot n-1\}\cong\{0,\ldots,m-1\}\times\{0,\ldots,n-1\} \tag{B.98}$$

Zum Nachweis nehmen wir an, dass $0\leqslant x<m$, $0\leqslant y<n$ und $0\leqslant z<m\cdot n$. Wenn wir die linke Seite von (B.97c) wahr machen, indem wir $x:=z$ und $y:=z$ setzen, dann erhalten wir $a\cdot z+b\cdot z\equiv z \pmod{m\cdot n}$ und damit $(a\cdot z+b\cdot z)\ \textbf{\textit{mod}}\ (m\cdot n)=z$. Umgekehrt, wenn wir die rechte Seite wahr machen, indem wir $z:=a\cdot x+b\cdot y$ setzen, dann erhalten wir $x\equiv a\cdot x+b\cdot y \pmod{m}$ und $y\equiv a\cdot x+b\cdot y \pmod{n}$ und somit $x=(a\cdot x+b\cdot y)\ \textbf{\textit{mod}}\ m$ und $y=a\cdot x+b\cdot y\ \textbf{\textit{mod}}\ n$. Mit anderen Worten, die Abbildungen $z\mapsto(z\ \textbf{\textit{mod}}\ m, z\ \textbf{\textit{mod}}\ n)$ und $(x,y)\mapsto a\cdot x+b\cdot y$ sind invers zueinander.

Natürlich ist das nicht die einzige Möglichkeit, Zahlen und Ziffernpaare in eine umkehrbare Beziehung zu setzen. Es gibt Myriaden von Optionen, insgesamt $(m\cdot n)!$ an der Zahl. (Warum?) Eine andere Option haben wir schon kennengelernt: Stellenwertsysteme. Die folgende Gegenüberstellung kontrastiert die Ansätze (für $m=3$ und $n=5$).

Residuenzahlensystem

(x,y)

(0,0)	(1,1)	(2,2)
(0,3)	(1,4)	(2,0)
(0,1)	(1,2)	(2,3)
(0,4)	(1,0)	(2,1)
(0,2)	(1,3)	(2,4)

$(x,y)\mapsto -5\cdot x+6\cdot y$

$z\mapsto(z\ \textbf{\textit{mod}}\ 3, z\ \textbf{\textit{mod}}\ 5)$

z/z'

0/0	1/5	2/10
3/1	4/6	5/11
6/2	7/7	8/12
9/3	10/8	11/13
12/4	13/9	14/14

z zeilenweise

z' spaltenweise

Stellenwertsystem

(x',y')

(0,0)	(1,0)	(2,0)
(0,1)	(1,1)	(2,1)
(0,2)	(1,2)	(2,2)
(0,3)	(1,3)	(2,3)
(0,4)	(1,4)	(2,4)

$(x',y')\mapsto x'+3\cdot y'$

$z\mapsto(z\ \textbf{\textit{mod}}\ 3, z\ \textbf{\textit{div}}\ 3)$

$(x',y')\mapsto 5\cdot x'+y'$

$z'\mapsto(z'\ \textbf{\textit{div}}\ 5, z'\ \textbf{\textit{mod}}\ 5)$

Während Residuenzahlensysteme auf dem Chinesischen Restsatz (B.97c) basieren, liegt den Stellenwertsystemen die Divisionsregel (B.48a) zugrunde. Anschaulich gesehen werden beim Stellenwertsystem die Kästchen eines $m\times n$-Spielfeldes fortlaufend nummeriert; die Koordinaten der Kästchen entsprechen dann den Ziffernpaaren. Zwei prinzipielle Varianten lassen sich unterscheiden: zeilenweise Nummerierung (engl. row-major order) und spaltenweise Nummerierung (engl.column-major order). Die erste Koordinate entspricht oben dem Divisionsrest der zeilenweisen Nummerierung ($z\ \textbf{\textit{mod}}\ 3=z'\ \textbf{\textit{div}}\ 5$), die zweite Koordinate dem Divisionsrest der spaltenweisen Nummerierung ($z\ \textbf{\textit{div}}\ 3=z'\ \textbf{\textit{mod}}\ 5$). Im Unterschied dazu werden beim Residuenzahlensystem *beide* Reste von der zeilenweisen Zählung gebildet (oder alternativ beide von der spaltenweisen Zählung, diese Option ist aber oben nicht aufgeführt).

Als entscheidender Vorteil des Residuenzahlensystems können arithmetische Operationen unabhängig voneinander, sprich parallel auf den Ziffern ausgeführt werden. Beim Stellenwertsystem erschweren Datenabhängigkeiten die Parallelisierung: Bei der Addition müssen Überträge von niederwertigen Positionen berücksichtigt werden (Überträge können kaskadieren: $9999+1=10000$). Aber wo Licht ist, ist auch Schatten: Die Umsetzung der ganzzahligen Division gestaltet sich im Residuenzahlensystem schwierig, ebenso die Implementierung der Vergleichsoperationen. Letz-

teres stellt im Stellenwertsystem kein Problem dar: Die ***lexikographische Ordnung*** auf den Ziffernpaaren spiegelt die Ordnung auf den Zahlen wider.

Übungen.

22. Zeigen Sie (B.89).

23. Erklären Sie die Kopfrechenregeln für die Teilbarkeitstests.

24. Lisa hat sich eine Zahl ausgedacht: *abcdefghij*. Die zehn Ziffern a, …, j sind paarweise verschieden.

- a ist durch 1 teilbar;
- *ab* ist durch 2 teilbar;
- *abc* ist durch 3 teilbar;
- *abcd* ist durch 4 teilbar;
- *abcde* ist durch 5 teilbar;
- *abcdef* ist durch 6 teilbar;
- *abcdefg* ist durch 7 teilbar;
- *abcdefgh* ist durch 8 teilbar;
- *abcdefghi* ist durch 9 teilbar;
- *abcdefghij* ist durch 10 teilbar.

Um welche Zahl handelt es sich? (Um Mißverständnissen vorzubeugen: Die Variablen bezeichnen Ziffern, nicht Zahlen; abc bedeutet entsprechend $100 \cdot a + 10 \cdot b + c$, *nicht* $a \cdot b \cdot c$.)

B.6. Kleene Algebren und Quantale⋆

In diesem Abschnitt führen wir zwei algebraische Strukturen ein, die in der Informatik eine wichtige Rolle spielen: ***Kleene Algebren*** und ***Quantale***. Kurz und knapp: Kleene Algebra ist die Algebra der *regulären* Sprachen; Quantale fangen die Algebra der Sprachen ein. Quantale basieren im Vergleich zu Kleene Algebren auf einem stärkeren Axiomensystem — die Mathematik der Quantale ist eleganter und interessanter, aber auch anspruchsvoller.

Kleene Algebra beschäftigt sich mit dem Zusammenspiel von drei elementaren Operationen — Alternative\Vereinigung ($a \sqcup b$), Komposition ($a \cdot b$) und Wiederholung\Iteration (a^*) — und kann daher mit Fug und Recht als die Algebra der Informatik bezeichnet werden. (Wenn Sie die optionalen Abschnitte 5.5 und 6.3 studiert haben, sind Sie schon mit den Grundzügen der Kleene Algebra vertraut.) Wir haben die Operationen in Kapitel 6 am konkreten Beispiel regulärer Sprachen kennengelernt. Jetzt abstrahieren wir von diesem wichtigen Spezialfall. Wir führen Kleene Algebren in vier Schritten ein: Abschnitt B.6.1 beschäftigt sich mit der algebraischen Struktur einer einzelnen binären Operation, Abschnitt B.6.2 widmet sich dem Zusammenspiel zweier Operationen, Abschnitt B.6.3 bereitet die Axiomatisierung des Sternoperators a^* vor und Abschnitt B.6.4 schließt die Axiomatisierung ab.

Abschnitt B.6.5 diskutiert das Konzept der Galoisverbindungen, eines Juwels der Mathematik. Darauf aufbauend führt Abschnitt B.6.6 schließlich Quantale ein.

Wie auch in den vorherigen Abschnitten führen wir viele Beweise; insbesondere zeigen wir alle in Kapitel 6 verwendeten Eigenschaften von Sprachen und Graphen\Matrizen.

B.6.1. Monoide

Eine der einfachsten algebraischen Strukturen ist die des ***Monoids***: eine Menge M mit einem ausgezeichneten Element $0 \in \mathrm{M}$ und einer binären Operation $+ : \mathrm{M} \times \mathrm{M} \to \mathrm{M}$, so dass $+$ assoziativ ist mit 0 als neutralem Element.

$$0 + a = a = a + 0 \tag{B.99a}$$
$$(a + b) + c = a + (b + c) \tag{B.99b}$$

Wie bereits angesprochen, erlaubt das Assoziativgesetz, mehrere Elemente zu verknüpfen, ohne Klammern setzen zu müssen: $a_1 + a_2 + \cdots + a_n$. Auch der Fall $n = 0$ ist abgedeckt: Dann ist die »Summe« vereinbarungsgemäß 0. Betrachten wir ein paar Beispiele:

Auf den Wahrheitswerten lassen sich verschiedene Monoide definieren. Von den 16 Operationen des Typs $\mathbb{B} \times \mathbb{B} \to \mathbb{B}$ sind 4 assoziativ und besitzen ein neutrales Element.

$$(\mathbb{B}, \mathit{true}, \wedge) \qquad (\mathbb{B}, \mathit{false}, \vee) \qquad (\mathbb{B}, \mathit{true}, =) \qquad (\mathbb{B}, \mathit{false}, \neq)$$

Überzeugen Sie sich, dass sowohl die Gleichheit (Äquivalenz) als auch die Ungleichheit (Nichtäquivalenz, exklusives Oder) assoziativ sind.[27] Konjunktion und Disjunktion sind darüber hinaus kommutativ und idempotent; Gleichheit und Ungleichheit sind kommutativ, aber nicht idempotent. Zwei weitere Boolesche Operationen sind assoziativ, besitzen aber kein neutrales Element: $a \swarrow b := a$ und $a \searrow b := b$ ignorieren ein Argument und geben das jeweils andere unverändert zurück.

Abbildungen des Typs $\mathrm{A} \to \mathrm{A}$ (manchmal etwas kryptisch ***Endofunktionen*** genannt) bilden ebenfalls ein Monoid: Die Funktionskomposition »$\circ$« dient als binäre Operation, die Identität *id* ist ihr neutrales Element. Die Komposition von Funktionen ist weder kommutativ, noch idempotent.

Auch Sequenzen A^* über einer Grundmenge A formen ein Monoid, das sogenannte ***freie Monoid***: Die Konkatenation »$\cdot$« ist assoziativ mit der leeren Sequenz ε als neutralem Element (siehe auch Abschnitt 2.1). Wie die Funktionskomposition ist auch die Konkatenation weder kommutativ, noch idempotent.

B.6.2. Halbringe

Ein einzelnes Monoid macht noch keine allzu interessante algebraische Struktur. Ein ***Halbring*** verknüpft zwei Monoide über der gleichen Grundmenge: ein kommutatives Monoid (additiv notiert: 0 und »+«) und ein Monoid (multiplikativ notiert: 1 und »$\cdot$«).

$$\begin{gathered} a + 0 = a = 0 + a \\ a + (b + c) = (a + b) + c \\ a + b = b + a \end{gathered} \qquad\qquad \begin{gathered} a \cdot 1 = a = 1 \cdot a \\ a \cdot (b \cdot c) = (a \cdot b) \cdot c \end{gathered}$$

Es ist nicht unmittelbar ersichtlich, warum wir verlangen, dass die »Addition« kommutativ ist. Wir nehmen das für den Moment so hin und greifen die Frage später noch einmal auf, wenn wir uns Beispielen zuwenden.

Die Interaktion zwischen den beiden algebraischen Strukturen wird durch die Distributivgesetze geregelt: »$\cdot$« distribuiert sowohl von links als auch von rechts über »+«.

$$x \cdot 0 = 0 \qquad\qquad 0 \cdot x = 0 \tag{B.100a}$$
$$x \cdot (a + b) = (x \cdot a) + (x \cdot b) \qquad\qquad (a + b) \cdot x = (a \cdot x) + (b \cdot x) \tag{B.100b}$$

[27] Der geschachtelte Ausdruck $(a = b) = c$ ist dabei *nicht* konjunktiv als $(a = b) \wedge (b = c)$ zu lesen.

Damit kann eine Multiplikation von links $x \cdot$ - oder von rechts - $\cdot x$ über eine endliche Summe verteilt werden: $x \cdot (a_1 + a_2 + \cdots + a_n) = x \cdot a_1 + x \cdot a_2 + \cdots + x \cdot a_n$ bzw. $(a_1 + a_2 + \cdots + a_n) \cdot x = a_1 \cdot x + a_2 \cdot x + \cdots + a_n \cdot x$. Auch der Fall $n = 0$ ist dank der Gesetze (B.100a) abgedeckt — man sagt auch, das neutrale Element 0 ist ***links-*** und ***rechtsabsorbierend***. Betrachten wir einige Beispiele:

Klar, die natürlichen Zahlen mit Addition und Multiplikation bilden einen Halbring: $(\mathbb{N}, 0, +, 1, \cdot)$. Die Distributivgesetze weisen die Multiplikation als iterierte Addition aus: $x \cdot (1 + 1 + \cdots + 1) = x + x + \cdots + x$.

Statt Addition und Multiplikation können wir auch Minimum »↓« und Addition »+« betrachten. Da $x +$ - monoton ist, distribuiert die Addition über das Minimum (B.26b). Allerdings besitzt die Minimumoperation kein neutrales Element, da $\mathbb{N}$ nach oben unbegrenzt ist. Erweitern wir die natürlichen Zahlen um ein größtes Element, erhalten wir einen Halbring: $(\mathbb{N} \cup \{\infty\}, \infty, \downarrow, 0, +)$, den sogenannten ***tropischen Halbring*** (engl. tropical semiring), in dem die multiplikative Operation durch die Addition gegeben ist! Das Axiom (B.100a) legt fest, wie die Addition auf $\mathbb{N} \cup \{\infty\}$ erweitert werden muss: $\infty + x = \infty = x + \infty$. Die Minimumoperation ist im Gegensatz zur Addition von Zahlen idempotent, ein Spezialfall, der besondere Beachtung verdient:

Ist die additive Verknüpfung ***idempotent***[28],

$$a \sqcup a = a \tag{B.101}$$

bildet das additive Monoid, wie in Abschnitt B.4.2 besprochen, einen ***Halbverband***. Zur Erinnerung: Mit Hilfe von »⊔« lässt sich eine Ordnung definieren (B.25), so dass die Vereinigung »⊔« bezüglich dieser Ordnung monoton ist (B.24b). Aus den Distributivgesetzen folgt, dass auch die Multiplikation »·« monoton ist. Dazu müssen wir zeigen:

$$\begin{aligned}
& a_1 \leqslant b_1 \;\wedge\; a_2 \leqslant b_2 \;\Longrightarrow\; a_1 \cdot a_2 \leqslant b_1 \cdot b_2 \\
\Longleftrightarrow\quad & \{\ \text{Verbindungslemma (B.25)}\ \} \\
& a_1 \sqcup b_1 = b_1 \;\wedge\; a_2 \sqcup b_2 = b_2 \;\Longrightarrow\; (a_1 \cdot a_2) \sqcup (b_1 \cdot b_2) = b_1 \cdot b_2
\end{aligned}$$

Für den Nachweis der Implikation rechnen wir:

$$\begin{aligned}
& a_1 \cdot a_2 \sqcup b_1 \cdot b_2 \\
= \quad & \{\ \text{Annahmen: } a_1 \sqcup b_1 = b_1 \text{ und } a_2 \sqcup b_2 = b_2\ \} \\
& a_1 \cdot a_2 \sqcup (a_1 \sqcup b_1) \cdot (a_2 \sqcup b_2) \\
= \quad & \{\ \text{Distributivgesetze (B.100b)}\ \} \\
& a_1 \cdot a_2 \sqcup a_1 \cdot a_2 \sqcup a_1 \cdot b_2 \sqcup b_1 \cdot a_2 \sqcup b_1 \cdot b_2 \\
= \quad & \{\ \text{Idempotenz (B.101)}\ \} \\
& a_1 \cdot a_2 \sqcup a_1 \cdot b_2 \sqcup b_1 \cdot a_2 \sqcup b_1 \cdot b_2 \\
= \quad & \{\ \text{Distributivgesetze (B.100b)}\ \} \\
& (a_1 \sqcup b_1) \cdot (a_2 \sqcup b_2) \\
= \quad & \{\ \text{Annahmen: } a_1 \sqcup b_1 = b_1 \text{ und } a_2 \sqcup b_2 = b_2\ \} \\
& b_1 \cdot b_2
\end{aligned}$$

Idempotente Halbringe verallgemeinern Verbände: Da die Anforderungen geringer sind, ist jeder Verband mit Extremelementen ein idempotenter Halbring, aber nicht umgekehrt. Insbesondere sind »⊔« und »·« nicht notwendigerweise dual zueinander, da wir nur fordern, dass die »Multiplikation« über die »Addition« distribuiert. Die größere Flexibilität illustriert die folgende allgemeine Konstruktion.

[28] Eine Bemerkung zur Notation: Idempotente Operationen notieren wir mit dem Vereinigungssymbol »⊔« statt eines Pluszeichens (das Axiom $a + a = a$ sieht etwas merkwürdig aus); entsprechend verwenden wir für das neutrale Element das Symbol $\perp$ statt der Null.

Beispiel: Potenzmengenmonoide Ist $(M, 1, \cdot)$ ein beliebiges Monoid, dann bildet die Potenzmenge $(\mathscr{P}(M), \emptyset, \cup, 1, \cdot)$ einen idempotenten Halbring, wobei 1 und »$\cdot$« wie folgt definiert sind.

$$1 := \{1\} \tag{B.102a}$$
$$A \cdot B := \{\, a \cdot b \mid a \in A, b \in B \,\} \tag{B.102b}$$

Wir ***überladen*** die Notation: Die Operationen auf Mengen (linke Seite) werden auf die korrespondierenden Operationen des zugrundeliegenden Monoids (rechte Seite) zurückgeführt — man sagt auch, 1 und »$\cdot$« werden auf Mengen ***fortgesetzt***. Wir zeigen exemplarisch die Distributivgesetze.

$$\begin{aligned}
& x \cdot c \in X \cdot \emptyset \\
\iff & \quad \{ \text{ Definition »}\cdot\text{« (B.102b) } \} \\
& x \in X \ \wedge \ c \in \emptyset \\
\iff & \quad \{ \text{ leere Menge } \} \\
& \mathit{false} \\
\iff & \quad \{ \text{ leere Menge } \} \\
& x \cdot c \in \emptyset
\end{aligned}$$

$$\begin{aligned}
& x \cdot c \in X \cdot (A \cup B) \\
\iff & \quad \{ \text{ Definition »}\cdot\text{« (B.102b) } \} \\
& x \in X \ \wedge \ c \in A \cup B \\
\iff & \quad \{ \text{ Vereinigung } \} \\
& x \in X \ \wedge \ (c \in A \ \vee \ c \in B) \\
\iff & \quad \{ \text{ Logik: Distributivgesetz } \} \\
& (x \in X \ \wedge \ c \in A) \ \vee \ (x \in X \ \wedge \ c \in B) \\
\iff & \quad \{ \text{ Definition »}\cdot\text{« (B.102b) } \} \\
& x \cdot c \in X \cdot A \ \vee \ x \cdot c \in X \cdot B \\
\iff & \quad \{ \text{ Vereinigung } \} \\
& x \cdot c \in (X \cdot A) \cup (X \cdot B)
\end{aligned}$$

Der Halbring der Sprachen $(\mathscr{P}(\mathbb{A}^*), \emptyset, \cup, \varepsilon, \cdot)$, Mengen von Wörtern über einem Alphabet, ist ein Spezialfall der obigen Konstruktion; das zugrundeliegende Monoid ist $(\mathbb{A}^*, \varepsilon, \cdot)$, das freie Monoid über dem Alphabet $\mathbb{A}$.

Beispiel: Matrizen Die obige Konstruktion befördert einen Monoid zu einem Halbring. Die folgende Konstruktion macht aus einem »alten« Halbring einen »neuen« Halbring.

Sei I eine beliebige Menge (eine Indexmenge). Ist $\mathbb{S}$ ein Halbring, dann bilden die *quadratischen* Matrizen $I \times I \to \mathbb{S}$ ebenfalls einen Halbring.

$$\mathbf{0}_{ij} := 0 \tag{B.103a}$$
$$(A + B)_{ij} := A_{ij} + B_{ij} \tag{B.103b}$$
$$\mathbf{1}_{ij} := [i = j] \tag{B.103c}$$
$$(A \cdot B)_{ik} := \sum_{j \in I} A_{ij} \cdot B_{jk} \tag{B.103d}$$

Wir ***überladen*** wiederum die Notation: Die Operationen auf Matrizen (linke Seite) werden auf die korrespondierenden Operationen des zugrundeliegenden Halbrings (rechte Seite) zurückgeführt. Das Nullelement und die Addition werden ***komponentenweise*** definiert; gleiches gilt für die induzierte Ordnung.

$$A \sqsubseteq B \quad :\iff \quad \forall\, i \in I \,.\, \forall\, j \in I \,.\, A_{ij} \sqsubseteq B_{ij} \tag{B.104}$$

Komponentenweise Definitionen sind angenehm in der Handhabung: Alle Eigenschaften der zugrundeliegenden Operationen übertragen sich auf die Matrixoperationen. So ist die Matrixaddition kommutativ und assoziativ mit der Nullmatrix als neutralem Element; ist die zugrundeliegende Addition idempotent, gilt das auch für die Matrixaddition.

Es verbleibt zu zeigen, dass die Matrixmultiplikation assoziativ mit der Einheitsmatrix als neutralem Element ist und dass die Distributivgesetze gelten. Man rechnet schnell nach, dass die Einheitsmatrix neutral ist.[29]

$$
\begin{aligned}
& (\mathrm{A} \cdot \mathbf{1})_{ik} \\
= & \quad \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{j \in \mathrm{J}} \mathrm{A}_{ij} \cdot \mathbf{1}_{jk} \\
= & \quad \{ \text{ Definition } \mathbf{1} \text{ (B.103c) } \} \\
& \sum_{j \in \mathrm{J}} \mathrm{A}_{ij} \cdot [j = k] \\
= & \quad \{ \text{ Iverson Klammer } \} \\
& \mathrm{A}_{ik}
\end{aligned}
\qquad
\begin{aligned}
& (\mathbf{1} \cdot \mathrm{A})_{ik} \\
= & \quad \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{j \in \mathrm{J}} \mathbf{1}_{ij} \cdot \mathrm{A}_{jk} \\
= & \quad \{ \text{ Definition } \mathbf{1} \text{ (B.103c) } \} \\
& \sum_{j \in \mathrm{J}} [i = j] \cdot \mathrm{A}_{jk} \\
= & \quad \{ \text{ Iverson Klammer } \} \\
& \mathrm{A}_{ik}
\end{aligned}
$$

Der Nachweis der Assoziativität gestaltet sich interessanter; wir fangen an beiden »Enden« der Gleichung $\mathrm{A} \cdot (\mathrm{B} \cdot \mathrm{C}) = (\mathrm{A} \cdot \mathrm{B}) \cdot \mathrm{C}$ an und arbeiten uns in die Mitte vor.

$$
\begin{aligned}
& (\mathrm{A} \cdot (\mathrm{B} \cdot \mathrm{C}))_{il} \\
= & \quad \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{j \in \mathrm{J}} \mathrm{A}_{ij} \cdot (\mathrm{B} \cdot \mathrm{C})_{jl} \\
= & \quad \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{j \in \mathrm{J}} \mathrm{A}_{ij} \cdot \left(\sum_{k \in \mathrm{K}} \mathrm{B}_{jk} \cdot \mathrm{C}_{kl} \right) \\
= & \quad \{ \text{ Distributivgesetze (B.100b) } \} \\
& \sum_{j \in \mathrm{J}} \sum_{k \in \mathrm{K}} \mathrm{A}_{ij} \cdot (\mathrm{B}_{jk} \cdot \mathrm{C}_{kl})
\end{aligned}
\qquad
\begin{aligned}
& ((\mathrm{A} \cdot \mathrm{B}) \cdot \mathrm{C})_{il} \\
= & \quad \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{k \in \mathrm{K}} (\mathrm{A} \cdot \mathrm{B})_{ik} \cdot \mathrm{C}_{kl} \\
= & \quad \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{k \in \mathrm{K}} \left(\sum_{j \in \mathrm{J}} \mathrm{A}_{ij} \cdot \mathrm{B}_{jk} \right) \cdot \mathrm{C}_{kl} \\
= & \quad \{ \text{ Distributivgesetze (B.100b) } \} \\
& \sum_{k \in \mathrm{K}} \sum_{j \in \mathrm{J}} (\mathrm{A}_{ij} \cdot \mathrm{B}_{jk}) \cdot \mathrm{C}_{kl}
\end{aligned}
$$

Sind die resultierenden Ausdrücke äquivalent? Ja! In den Nachweis fließen sowohl Eigenschaften der zugrundeliegenden Multiplikation als auch der Addition ein. Zunächst einmal spielt die Klammerung der Produkte keine Rolle, da die zugrundeliegende Multiplikation assoziativ ist — das war zu erwarten: Um die Assoziativität der Matrixmultiplikation zu zeigen, benötigen wir die Assoziativität der zugrundeliegenden Multiplikation. Das ist aber nicht der einzige Unterschied zwischen den Ausdrücken: Die Summen werden in unterschiedlicher Reihenfolge gebildet, einmal zeilenweise und einmal spaltenweise. Das folgende Minibeispiel illustriert die Unterschiede.

a	b	c
d	e	f

$$(a + b + c) + (d + e + f) = (a + d) + (b + e) + (c + f)$$

Die unterschiedlichen Summationen sind nur gleich, wenn die zugrundeliegende Addition assoziativ *und* kommutativ ist. Ein ähnliches Bild ergibt sich beim Nachweis der Distributivgesetze — wir zeigen ein Gesetz, das andere folgt mit einem symmetrischen Argument. (Den Nachweis, dass die Nullmatrix Faktoren absorbiert, sparen wir uns ebenfalls.)

[29] Die beteiligten Matrizen müssen nicht notwendigerweise quadratisch sein; gleiches gilt für den Nachweis der Assoziativität.

$$
\begin{aligned}
& (X \cdot (A + B))_{ik} \\
= \quad & \{ \text{ Definition Produkt (B.103d) } \} \\
& \sum_{j \in J} X_{ij} \cdot (A + B)_{jk} \\
= \quad & \{ \text{ Definition Summe (B.103b) } \} \\
& \sum_{j \in J} X_{ij} \cdot (A_{jk} + B_{jk})
\end{aligned}
\qquad
\begin{aligned}
& ((X \cdot A) + (X \cdot B))_{ik} \\
= \quad & \{ \text{ Definition Summe (B.103b) } \} \\
& (X \cdot A)_{ik} + (X \cdot B)_{ik} \\
= \quad & \{ \text{ Definition Produkt (B.103d) } \} \\
& \left(\sum_{j \in J} X_{ij} \cdot A_{jk} \right) + \left(\sum_{j \in J} X_{ij} \cdot B_{jk} \right)
\end{aligned}
$$

Die resultierenden Ausdrücke sind äquivalent, da im Halbring S das Distributivgesetz gilt *und* da die zugrundeliegende Addition assoziativ und kommutativ ist.

Diese Beobachtungen motivieren, warum in der Axiomatisierung von Halbringen verlangt wird, dass die Addition kommutativ ist — zwei einfache Monoide machen keine allzu interessante algebraische Struktur.

B.6.3. Präfixpunkte⋆

Der Sternoperator entspricht der Vereinigung aller endlichen Potenzen.

$$a^* = a^0 \sqcup a^1 \sqcup a^2 \sqcup a^3 \sqcup \cdots \qquad a^0 := 1 \qquad a \cdot a^n =: a^{n+1} := a^n \cdot a$$

Wie können wir diese informelle Beschreibung mathematisch präzise fassen? Wenn wir den Umstand ignorieren, dass wir es mit einer unendlichen Summe zu tun haben, können wir die rechte Seite mit Hilfe des Distributivgesetzes umformen.[30]

$$a^* = a^0 \sqcup a^1 \sqcup a^2 \sqcup a^3 \sqcup \cdots = 1 \sqcup a \cdot (a^0 \sqcup a^1 \sqcup a^2 \sqcup \cdots) = 1 \sqcup a \cdot a^*$$

Der resultierende Ausdruck fängt die umgangssprachliche Beschreibung des Sternoperators ein: Eine beliebige Wiederholung von a ist entweder die 0-malige Wiederholung ($a^0 = 1$) oder eine 1-malige Wiederholung ($a^1 = a$) gefolgt von einer beliebigen Wiederholung (a^*).

Wir könnten somit a^* als *Lösung* der Gleichung $x = 1 \sqcup a \cdot x$ in der Unbekannten x oder äquivalent als Fixpunkt der Funktion $f(x) = 1 \sqcup a \cdot x$ definieren — x heißt ***Fixpunkt*** von f genau dann, wenn $f(x) = x$. Definiert man ein mathematisches Objekt mittels einer Gleichung, muss man sich um zwei Dinge kümmern: die *Existenz* und die *Eindeutigkeit* von Lösungen. Wir thematisieren zunächst die Eindeutigkeit und kümmern uns in einem zweiten Schritt um die Existenz.

Leider gibt es keine Garantie, dass die Lösung der obigen Gleichung eindeutig ist — im Allgemeinen ist sie es nicht: Unendlich viele Sprachen erfüllen zum Beispiel die Gleichung $X = \{\varepsilon\} \cup \{a, \varepsilon\} \cdot X$; neben der offensichtlichen Lösung $\{a\}^*$ ist auch jede Sprache L^* mit $\{a\} \subseteq L$ eine Lösung der Gleichung, zum Beispiel $\{a, b\}^*$. Was ist zu tun? Da es keine eindeutige Lösung gibt, könnten wir eine spezielle Lösung auszeichnen; es scheint natürlich, die *kleinste* Lösung zu wählen, also $\{a\}^*$ im obigen Beispiel — die Lösung $\{a, b\}^*$ ist weniger naheliegend, da der Buchstabe b in der Gleichung gar nicht auftritt. Wenn wir die Lösungen anordnen und so Gebrauch von der zugrundeliegenden Ordnung machen, liegt es nahe, nicht nur Lösungen von Gleichungen, sondern auch Lösungen von Ungleichungen zu betrachten:

Sei S ein idempotenter Halbring und $f : S \to S$ eine monotone Funktion. Ein Element x mit $f(x) \leqslant x$ heißt ***Präfixpunkt*** von f. Die Funktion f besitzt einen ***kleinsten Präfixpunkt*** μf genau

[30] Wir werden in Abschnitt B.6.6 sehen, dass man auch mit unendlichen Summen prima rechnen kann — allerdings muss man etwas stärkere Annahmen treffen.

dann, wenn die beiden folgenden Eigenschaften erfüllt sind.

$$f(\mu f) \leqslant \mu f \tag{B.105a}$$
$$\mu f \leqslant x \iff f(x) \leqslant x \tag{B.105b}$$

Eigenschaft (B.105a) besagt, dass μf tatsächlich ein Präfixpunkt ist. Das Prinzip der ***Fixpunkt-Induktion*** (B.105b) formalisiert, dass μf der kleinste aller Präfixpunkte ist.

Der kleinste Präfixpunkt von f ist stets auch ein Fixpunkt der Funktion. Die Aussage $f(\mu f) = \mu f$ zeigen wir mit einem Ping-Pong Beweis. Eine Hälfte folgt direkt aus (B.105a); für die andere Hälfte argumentieren wir:

$$\begin{aligned}
& \mu f \leqslant f(\mu f) \\
\Longleftarrow \quad & \{ \text{ Fixpunkt-Induktion (B.105b) } \} \\
& f(f(\mu f)) \leqslant f(\mu f) \\
\Longleftarrow \quad & \{ \text{ Annahme: } f \text{ ist monoton } \} \\
& f(\mu f) \leqslant \mu f \\
\Longleftrightarrow \quad & \{ \ \mu f \text{ ist ein Präfixpunkt (B.105a) } \} \\
& \mathit{true}
\end{aligned}$$

Die letzten beiden Schritte zeigen, dass $f(\mu f)$ ebenfalls ein Präfixpunkt von f ist.

Kommen wir zur Existenz von Präfixpunkten. Im Allgemeinen ist nicht garantiert, dass eine monotone Funktion einen Präfixpunkt besitzt; die Nachfolgerfunktion $s(n) = n + 1$ besitzt zum Beispiel keinen. Machen wir stärkere Annahmen über die zugrundeliegende Ordnung, dann sieht die Situation rosiger aus: Ist P ein vollständiger Verband, dann bildet auch die Menge der Präfixpunkte von f einen vollständigen Verband. Insbesondere besitzt f einen kleinsten Präfixpunkt. Dazu zeigen wir, dass Präfixpunkte unter dem Durchschnitt abgeschlossen sind: Ist A eine Menge von Präfixpunkten, dann ist auch $\bigsqcap \mathrm{A}$ ein Präfixpunkt. (Das Supremum von Präfixpunkten ist hingegen *nicht* durch das Supremum des zugrundeliegenden Verbands gegeben.)

$$\begin{aligned}
& f(\bigsqcap \mathrm{A}) \leqslant \bigsqcap \mathrm{A} \\
\Longleftrightarrow \quad & \{ \text{ Infimum (B.19) } \} \\
& \forall a \in \mathrm{A} \ . \ f(\bigsqcap \mathrm{A}) \leqslant a \\
\Longleftarrow \quad & \{ \text{ Annahme: } a \text{ ist ein Präfixpunkt: } f(a) \leqslant a \ \} \\
& \forall a \in \mathrm{A} \ . \ f(\bigsqcap \mathrm{A}) \leqslant f(a) \\
\Longleftarrow \quad & \{ \text{ Annahme: } f \text{ ist monoton } \} \\
& \forall a \in \mathrm{A} \ . \ \bigsqcap \mathrm{A} \leqslant a \\
\Longleftarrow \quad & \{ \text{ untere Schranke (B.28a) } \} \\
& \mathit{true}
\end{aligned}$$

Der kleinste Präfixpunkt ergibt sich dann als Infimum aller Präfixpunkte:

$$\mu f = \bigsqcap \{ a \mid f(a) \leqslant a \} \tag{B.106}$$

Wir müssen schließlich nachweisen, dass das Infimum die Eigenschaften des kleinsten Präfixpunkts erfüllt. Wir haben oben bereits gezeigt, dass das Infimum selbst ein Präfixpunkt ist — somit gilt (B.105a); das Prinzip der Fixpunkt-Induktion (B.105b) ergibt sich unmittelbar aus der Definition des Infimums (B.19).

Kleene Algebra ist die Algebra von drei elementaren Operationen der Informatik: Alternative\Vereinigung, Komposition und Wiederholung\Iteration.
Vereinigung und Komposition bilden einen idempotenten Halbring:

$$\begin{array}{ccc} a \sqcup \bot = \bot = \bot \sqcup a & & x \cdot \bot = \bot \\ a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c & a \cdot 1 = a = 1 \cdot a & x \cdot (a \sqcup b) = x \cdot a \sqcup x \cdot b \\ a \sqcup b = b \sqcup a & a \cdot (b \cdot c) = (a \cdot b) \cdot c & \bot \cdot x = \bot \\ a \sqcup a = a & & (a \sqcup b) \cdot x = a \cdot x \sqcup b \cdot x \end{array}$$

Die Wiederholung a^* ist sowohl ein Präfixpunkt von $a \cdot - \sqcup 1$ als auch von $1 \sqcup - \cdot a$; weiterhin gelten die Invariantenaxiome:

$$\begin{array}{ll} a \cdot a^* \sqcup 1 \leqslant a^* & 1 \sqcup a^* \cdot a \leqslant a^* \\ a^* \cdot i \leqslant i \iff a \cdot i \leqslant i & i \cdot a^* \leqslant i \iff i \cdot a \leqslant i \end{array}$$

Abbildung B.16.: Axiome der Kleene Algebra.

Übungen.

1. Zeigen Sie die sogenannte ***Rollregel*** (engl. rolling rule).

$$f(\mu(g \circ f)) = \mu(f \circ g)$$

Der Sternoperator a^* schließt die 0-malige Wiederholung von a ein; sein Kumpel a^+ schließt sie aus. Die mindestens einmalige Wiederholung a^+ von a lässt sich als kleinster Präfixpunkt der Funktion $h(x) := a \sqcup a \cdot x$ definieren. Zeigen Sie $a^* = a \cdot a^+$ mit Hilfe der Rollregel. *Hinweis:* Betrachten Sie die Funktionen $f(x) := a \cdot x$ und $g(x) := 1 \sqcup x$.

B.6.4. Kleene Algebren⋆

Kleene Algebra ist die Algebra der regulären Sprachen. Mit Hilfe der in Abbildung B.16 aufgeführten Axiome lässt sich die Gleichheit $L_1 = L_2$ bzw. die Ungleichheit $L_1 \leqslant L_2$ von regulären Sprachen durch symbolische Formelmanipulation nachweisen.

Nach den Ausführungen des letzten Abschnitts würden wir vielleicht erwarten, dass a^* als kleinster Präfixpunkt von $f(x) := a \cdot x \sqcup 1$ eingeführt wird.

$$a \cdot a^* \sqcup 1 \leqslant a^* \tag{B.107a}$$
$$a^* \leqslant x \iff a \cdot x \sqcup 1 \leqslant x \tag{B.107b}$$

Wenn wir a^* von *links* mit a multiplizieren und 1 hinzufügen, erhalten wir mindestens a^*. Statt von links können wir natürlich auch von *rechts* mit a multiplizieren, so dass a^* alternativ als kleinster Präfixpunkt von $g(x) = 1 \sqcup x \cdot a$ eingeführt werden kann.

$$1 \sqcup a^* \cdot a \leqslant a^* \tag{B.108a}$$
$$a^* \leqslant x \iff 1 \sqcup x \cdot a \leqslant x \tag{B.108b}$$

Da die Multiplikation im Gegensatz zur Addition in der Regel nicht kommutativ ist, erscheinen beide Anforderungen sinnvoll und nötig. Aber selbst wenn wir (B.107a)–(B.108b) postulieren, ist das resultierende Axiomensystem nicht stark genug, um alle gewünschten Eigenschaften nachzuweisen: $a^* \cdot a^* \leqslant a^*$ lässt sich zum Beispiel nicht folgern, da es keine Regel gibt, die es uns erlaubt,

a^* *im Kontext* eines Produkts zu vereinfachen. (Summen sind unproblematisch, da sie mit Hilfe von Eigenschaft (B.18) zerlegt werden können.) Das motiviert die folgende Axiomatisierung:

Wir fordern, dass $a^* \cdot b$ der kleinste Präfixpunkt von $f(x) \coloneqq a \cdot x \sqcup b$ ist,

$$a \cdot a^* \cdot b \sqcup b \leqslant a^* \cdot b \tag{B.109a}$$
$$a^* \cdot b \leqslant x \iff a \cdot x \sqcup b \leqslant x \tag{B.109b}$$

und dass $b \cdot a^*$ der kleinste Präfixpunkt von $g(x) \coloneqq b \sqcup x \cdot a$ ist — f rückwärts gelesen.

$$b \sqcup b \cdot a^* \cdot a \leqslant b \cdot a^* \tag{B.110a}$$
$$b \cdot a^* \leqslant x \iff b \sqcup x \cdot a \leqslant x \tag{B.110b}$$

Abbildung B.16 enthält ein etwas einfacheres, aber äquivalentes System von Axiomen. Axiom (B.109a) wird durch das äquivalente Axiom (B.107a) ersetzt und (B.110a) entsprechend durch (B.108a). Das Axiom der Fixpunkt-Induktion (B.109b) lässt sich vereinfachen, indem wir b und x identifizieren und analog für (B.110b). Wir erhalten die sogenannten ***Invariantenaxiome***:

$$a^* \cdot i \leqslant i \iff a \cdot i \leqslant i \tag{B.111a}$$
$$i \cdot a^* \leqslant i \iff i \cdot a \leqslant i \tag{B.111b}$$

Ist i ein Präfixpunkt von $a \cdot$ -, dann ist i auch ein Präfixpunkt von $a^* \cdot$ - und analog für die Multiplikation von rechts. Zum Beispiel folgen aus $\bot \cdot i \leqslant i$ und $1 \cdot i \leqslant i$ die Inklusionen $\bot^* \cdot i \leqslant i$ und $1^* \cdot i \leqslant i$ und damit

$$\bot^* = 1 = 1^* \tag{B.112}$$

Wir haben bereits angemerkt, dass jeder Verband $(\mathrm{L}, \bot, \sqcup, \top, \sqcap)$ mit Extremelementen einen idempotenten Halbring bildet. Da die Funktion $f(x) = (a \sqcap x) \sqcup \top = \top$ konstant ist, existiert der kleinste Präfixpunkt von f und es gilt $a^* = \top$ — somit ist der Verband L auch eine Kleene Algebra. Insbesondere bildet der Verband der Wahrheitswerte mit $a^* = \mathit{true}$ eine Kleene Algebra, die sogenannte ***Erreichbarkeitsalgebra*** (engl. reachability algebra). Aus dem gleichen Grund ist auch der tropische Halbring eine Kleene Algebra: $f(x) = (a + x) \downarrow 0 = 0$ ist konstant und somit $a^* = 0$. Die Erweiterung des tropischen Halbrings heißt auch ***Kostenalgebra*** (engl. least cost algebra): Die natürlichen Zahlen modellieren Kosten (Fahrtkosten, Leitungskosten); + summiert Kosten; $\downarrow$ wählt die kostengünstigste Alternative.

Erreichbarkeitsalgebra	$(\mathbb{B}, \mathit{false}, \vee, \mathit{true}, \wedge, (\text{-})^*)$	mit $a^* = \mathit{true}$
Kostenalgebra	$(\mathbb{N} \cup \{\infty\}, \infty, \downarrow, 0, +, (\text{-})^*)$	mit $a^* = 0$

Aus dem Axiomensystem in Abbildung B.16 folgen eine Reihe von Eigenschaften, die wir in den Kapitel 5 und 6 ohne Beweis benutzt haben und die wir jetzt zeigen wollen.

Hülleneigenschaften Die folgenden Eigenschaften

(reflexiv)	$1 \leqslant a^*$
(transitiv)	$a^* \cdot a^* = a^*$
(extensiv)	$a \leqslant a^*$
(idempotent)	$(a^*)^* = a^*$

(B.113)

erklären, warum a^* auch die ***reflexive, transitive Hülle*** von a heißt — ein Hüllenoperator ist gemäß Definition ***extensiv*** und ***idempotent***. Die beiden Ungleichungen folgen unmittelbar aus Axiom (B.107a):

$$\begin{aligned}
& a \cdot a^* \sqcup 1 \leqslant a^* \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& a \cdot a^* \leqslant a^* \ \wedge \ 1 \leqslant a^*
\end{aligned}$$

Somit gilt auch $a = a \cdot 1 \leqslant a \cdot a^* \leqslant a^*$ — dabei nutzen wir aus, dass die Multiplikation monoton ist. Der Beweis von $a^* \cdot a^* \leqslant a^*$ illustriert das Invariantenaxiom.

$$\begin{aligned}
& a^* \cdot a^* \leqslant a^* \\
\impliedby & \quad \{ \text{ Invariantenaxiom (B.111a) } \} \\
& a \cdot a^* \leqslant a^* \\
\iff & \quad \{ \text{ siehe oben } \} \\
& \mathit{true}
\end{aligned}$$

Da weiterhin $a^* = 1 \cdot a^* \leqslant a^* \cdot a^*$ gilt, folgt die Gleichheit. Um $(a^*)^* \leqslant a^*$ zu zeigen, argumentieren wir wie folgt.

$$\begin{aligned}
& (a^*)^* \leqslant a^* \\
\impliedby & \quad \{ \text{ Fixpunkt-Induktion (B.107b) } \} \\
& a^* \cdot a^* \sqcup 1 \leqslant a^* \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& a^* \cdot a^* \leqslant a^* \ \wedge \ 1 \leqslant a^* \\
\iff & \quad \{ \text{ siehe oben } \} \\
& \mathit{true}
\end{aligned}$$

Aus $a \leqslant a^*$ folgt mit $a := a^*$ weiterhin $a^* \leqslant (a^*)^*$ und somit die Gleichheit.

Bocksprungregeln und Spiegelregel Die folgenden Regeln sind nach einem alten Kinderspiel benannt, dem Bockspringen (engl. leapfrog, franz. saute-mouton).

$$x \cdot a^* \leqslant b^* \cdot x \quad \impliedby \quad x \cdot a \leqslant b \cdot x \tag{B.114a}$$

$$a^* \cdot x \leqslant x \cdot b^* \quad \impliedby \quad a \cdot x \leqslant x \cdot b \tag{B.114b}$$

$$x \cdot a^* = b^* \cdot x \quad \impliedby \quad x \cdot a = b \cdot x \tag{B.114c}$$

Der Name »Bocksprungregel« leitet sich aus einer phantasievollen Interpretation der Voraussetzung $x \cdot a \leqslant b \cdot x$ ab: Der Bockspringer x springt über a; um einen sicheren Stand zu haben, bückt sich a vor dem Sprung und stützt sich dabei mit den Händen auf den Oberschenkeln ab; nach dem Sprung richtet sich a auf — aus a wird b. Die ***Bocksprungregel*** besagt, dass unter dieser Voraussetzung der Bockspringer auch über eine Reihe von as springen kann und diese sich dabei in bs verwandeln. Der Beweis von (B.114a) verwendet das Prinzip der Fixpunkt-Induktion.

$$\begin{aligned}
& x \cdot a^* \leqslant b^* \cdot x \\
\impliedby & \quad \{ \text{ Fixpunkt-Induktion (B.110b) } \} \\
& x \sqcup b^* \cdot x \cdot a \leqslant b^* \cdot x \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& x \leqslant b^* \cdot x \ \wedge \ b^* \cdot x \cdot a \leqslant b^* \cdot x
\end{aligned}$$

Die beiden Glieder der Konjunktion sind schnell verifiziert.

2.

$$\begin{array}{ll} & x \\ \leqslant & \{\text{ neutrales Element }\} \\ & 1 \cdot x \\ \leqslant & \{\text{ Hülle (B.113): } 1 \leqslant r^* \} \\ & b^* \cdot x \end{array} \qquad \begin{array}{ll} & b^* \cdot x \cdot a \\ \leqslant & \{\text{ Annahme: } x \cdot a \leqslant b \cdot x \} \\ & b^* \cdot b \cdot x \\ \leqslant & \{\text{ Hülle (B.113): } r^* \cdot r \leqslant r^* \} \\ & b^* \cdot x \end{array}$$

Ein symmetrischer Beweis zeigt die symmetrische Bocksprungregel (B.114b); die beiden Regeln (B.114a) und (B.114b) implizieren schließlich (B.114c).

Aus den Bocksprungregeln folgt unmittelbar, dass der Sternoperator monoton ist.

$$a \leqslant b \implies a^* \leqslant b^*$$

Zum Beweis setze $x := 1$ in (B.114a). Wir halten fest: Alle drei Operationen, Vereinigung, Komposition und Wiederholung, sind monoton — eine wichtige Eigenschaft beim Führen von Ungleichheitsbeweisen.

Eine alternierende Folge von as und bs, die mit einem a anfängt und in einem a endet, lässt sich auf zwei äquivalente Weisen definieren.

$$(a \cdot b)^* \cdot a = a \cdot (b \cdot a)^* \tag{B.115}$$

Diese sogenannte ***Spiegelregel*** (engl. mirror rule) ist ein Spezialfall der Bocksprungregel (B.114c): Setze $a := a \cdot b$, $b := b \cdot a$ und $x := a$; die Voraussetzung ist trivialerweise erfüllt, da $a \cdot b \cdot a$ ein Palindrom ist.

Dekompositionsregel Die ***Dekompositionsregel*** (engl. decomposition rule oder star-sum rule) erlaubt es, eine iterierte Summe umzuschreiben.

$$a^* \cdot (b \cdot a^*)^* = (a \sqcup b)^* = (a^* \cdot b)^* \cdot a^* \tag{B.116}$$

Es genügt eine Gleichung nachzuweisen; die andere folgt mit der Spiegelregel (B.115). Die erste Gleichung zeigen wir mit einem Ping-Pong Beweis. Für die eine Richtung verwenden wir die Hülleneigenschaften.

$$\begin{array}{ll} & a^* \cdot (b \cdot a^*)^* \\ \leqslant & \{\text{ obere Schranke (B.24a): } a \leqslant a \sqcup b \text{ und } b \leqslant a \sqcup b \} \\ & (a \sqcup b)^* \cdot ((a \sqcup b) \cdot (a \sqcup b)^*)^* \\ \leqslant & \{\text{ Hülle (B.113): } r \cdot r^* \leqslant r^*, (r^*)^* \leqslant r^* \text{ und } r^* \cdot r^* \leqslant r^* \} \\ & (a \sqcup b)^* \end{array}$$

Für die andere Richtung greifen wir auf Fixpunkt-Induktion zurück. Sei $x = a^* \cdot (b \cdot a^*)^*$,

$$\begin{array}{ll} & (a \sqcup b)^* \leqslant x \\ \Longleftarrow & \{\text{ Fixpunkt-Induktion (B.107b) }\} \\ & 1 \sqcup (a \sqcup b) \cdot x \leqslant x \\ \Longleftrightarrow & \{\text{ Distributivgesetze (B.100b) }\} \\ & 1 \sqcup a \cdot x \sqcup b \cdot x \leqslant x \\ \Longleftrightarrow & \{\text{ Supremum (B.18) }\} \\ & 1 \leqslant x \ \wedge \ a \cdot x \leqslant x \ \wedge \ b \cdot x \leqslant x \end{array}$$

Die drei Ungleichungen folgen jeweils aus den Hülleneigenschaften (B.113).

$$
\begin{aligned}
& a \cdot a^* \cdot (b \cdot a^*)^* \\
\leqslant \quad & \{ \text{ Hülle (B.113): } r \cdot r^* \leqslant r^* \} \\
& a^* \cdot (b \cdot a^*)^*
\end{aligned}
\qquad
\begin{aligned}
& b \cdot a^* \cdot (b \cdot a^*)^* \\
\leqslant \quad & \{ \text{ Hülle (B.113): } r \cdot r^* \leqslant r^* \} \\
& (b \cdot a^*)^* \\
\leqslant \quad & \{ \text{ Hülle (B.113): } 1 \leqslant r^* \} \\
& a^* \cdot (b \cdot a^*)^*
\end{aligned}
$$

Beispiel: Potenzmengenmonoide Die in Abschnitt B.6.2 eingeführten Potenzmengenmonoide erfüllen ebenfalls die Anforderungen einer Kleene Algebra — es lässt sich ein Sternoperator mit den gewünschten Eigenschaften definieren. Das liegt an der Vollständigkeit von Potenzmengenverbänden; wir zeigen später in einem etwas allgemeineren Kontext, dass die unbeschränkte Wiederholung A^* der Vereinigung aller endlichen Wiederholungen A^n entspricht (siehe Motivation des Sternoperators in Abschnitt B.6.3 und Abschnitt B.6.6).

$$A^* := \bigcup_{n \in \mathbb{N}} A^n \qquad A^0 := 1 \qquad A \cdot A^n =: A^{n+1} := A^n \cdot A$$

Insbesondere bilden Sprachen Kleene Algebra — dieser wichtige Spezialfall bildet die Grundlage von Kapitel 6.

Potenzmengenmonoid	$(\mathcal{P}(M), \varnothing, \cup, 1, \cdot, (\text{-})^*)$
Algebra der Sprachen	$(\mathcal{P}(\mathbb{A}^*), \varnothing, \cup, \{\varepsilon\}, \cdot, (\text{-})^*)$

Die ***Erreichbarkeitsalgebra*** $(\mathbb{B}, \mathit{false}, \vee, \mathit{true}, \wedge, (\text{-})^*)$ kann übrigens als Spezialfall der Potenzmengenkonstruktion angesehen werden. Ausgangspunkt ist das einfachste aller Monoide, $(\{\varepsilon\}, \varepsilon, \cdot)$, das nur aus einem, sprich *dem* neutralen Element besteht. Setzen wir dieses uninteressante Monoid auf Mengen fort, erhalten wir eine Kleene Algebra mit zwei Elementen: $\varnothing$ korrespondiert zu *false* und $\{\varepsilon\}$ zu *true*.

Beispiel: Matrizen\Graphen Wir haben bereits gezeigt, dass quadratische Matrizen $I \times I \to \mathbb{S}$ einen Halbring bilden, sofern $\mathbb{S}$ selbst ein Halbring ist. Wenn i eine *endliche* Indexmenge ist und $\mathbb{S}$ sogar eine Kleene Algebra, dann lassen sich auch quadratische Matrizen in den Status einer Kleene Algebra erheben. Abbildung 6.10 skizziert den induktiven Beweis — wir konzentrieren uns hier auf ein fehlendes »Detail«:

In Abschnitt 6.3.1 haben wir ***Conways Formel*** für die Berechnung der Hülle A^* mit Hilfe von Pfaden in Graphen motiviert. Im Folgenden wollen wir die Formel systematisch *herleiten*. Als Ausgangspunkt dient Axiom (B.107a), spezialisiert auf 2×2-Matrizen:

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} \geqslant \begin{pmatrix} 1 & \bot \\ \bot & 1 \end{pmatrix} \sqcup \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} w & x \\ y & z \end{pmatrix} \quad \text{wobei } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ und } A^* = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

Die zu berechnende Matrix für die Hülle A^* haben wir durch eine Matrix mit vier Unbekannten ersetzt (w, x, y und z), die es durch systematisches Umformen zu bestimmen gilt. Dabei nutzen wir aus, dass eine Ungleichung zwischen Matrizen einem *System von Ungleichungen* zwischen

Skalaren entspricht (die *Ungleichungssysteme* sind unten in geschweifte Klammern gesetzt).

$$
\begin{aligned}
& \begin{pmatrix} w & x \\ y & z \end{pmatrix} \geqslant \begin{pmatrix} 1 & \bot \\ \bot & 1 \end{pmatrix} \sqcup \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} w & x \\ y & z \end{pmatrix} \\
\iff & \quad \{ \text{ Definition von Vereinigung (B.103b) und Multiplikation (B.103d) } \} \\
& \begin{pmatrix} w & x \\ y & z \end{pmatrix} \geqslant \begin{pmatrix} 1 \sqcup a \cdot w \sqcup b \cdot y & a \cdot x \sqcup b \cdot z \\ c \cdot w \sqcup d \cdot y & 1 \sqcup c \cdot x \sqcup d \cdot z \end{pmatrix} \\
\iff & \quad \{ \text{ punktweise Ordnung (B.104) } \} \\
& \begin{Bmatrix} w \geqslant 1 \sqcup a \cdot w \sqcup b \cdot y \\ x \geqslant a \cdot x \sqcup b \cdot z \\ y \geqslant c \cdot w \sqcup d \cdot y \\ z \geqslant 1 \sqcup c \cdot x \sqcup d \cdot z \end{Bmatrix} \\
\impliedby & \quad \{ \text{ siehe unten } (\circledast) \} \\
& \begin{Bmatrix} w = (a \sqcup b \cdot d^* \cdot c)^* \\ x = a^* \cdot b \cdot z = a^* \cdot b \cdot (c \cdot a^* \cdot b \sqcup d)^* \\ y = d^* \cdot c \cdot w = d^* \cdot c \cdot (a \sqcup b \cdot d^* \cdot c)^* \\ z = (c \cdot a^* \cdot b \sqcup d)^* \end{Bmatrix} \\
\iff & \quad \{ \text{ punktweise Ordnung (B.104) } \} \\
& \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} (a \sqcup b \cdot d^* \cdot c)^* & a^* \cdot b \cdot (c \cdot a^* \cdot b \sqcup d)^* \\ d^* \cdot c \cdot (a \sqcup b \cdot d^* \cdot c)^* & (c \cdot a^* \cdot b \sqcup d)^* \end{pmatrix}
\end{aligned}
$$

Im vorletzten Schritt lösen wir die Ungleichungen durch wiederholte Anwendung der Fixpunkt-Induktion. Es gilt die Vorkommen der Unbekannten auf den rechten Seiten zu eliminieren. In einem ersten Schritt vereinfachen wir die Ungleichungen für x und y:

$$
\begin{aligned}
& x \geqslant a \cdot x \sqcup b \cdot z \\
\implies & \quad \{ \text{ Fixpunkt-Induktion (B.109b) } \} \\
& x \geqslant a^* \cdot b \cdot z
\end{aligned}
\qquad\qquad
\begin{aligned}
& y \geqslant c \cdot w \sqcup d \cdot y \\
\implies & \quad \{ \text{ Fixpunkt-Induktion (B.109b) } \} \\
& y \geqslant d^* \cdot c \cdot w
\end{aligned}
$$

Die »Abschätzungen« für x und y setzen wir in einem zweiten Schritt in die Ungleichungen für w und z ein:

$$
\begin{aligned}
& w \\
\geqslant & \quad \{ \text{ siehe oben } \} \\
& 1 \sqcup a \cdot w \sqcup b \cdot y \\
\geqslant & \quad \{ \text{ siehe oben } \} \\
& 1 \sqcup a \cdot w \sqcup b \cdot d^* \cdot c \cdot w \\
= & \quad \{ \text{ Distributivgesetze (B.100b) } \} \\
& 1 \sqcup (a \sqcup b \cdot d^* \cdot c) \cdot w
\end{aligned}
\qquad\qquad
\begin{aligned}
& z \\
\geqslant & \quad \{ \text{ siehe oben } \} \\
& 1 \sqcup c \cdot x \sqcup d \cdot z \\
\geqslant & \quad \{ \text{ siehe oben } \} \\
& 1 \sqcup c \cdot a^* \cdot b \cdot z \sqcup d \cdot z \\
= & \quad \{ \text{ Distributivgesetze (B.100b) } \} \\
& 1 \sqcup (c \cdot a^* \cdot b \sqcup d) \cdot z
\end{aligned}
$$

Mit (B.107b) folgt schließlich $w \geqslant (a \sqcup b \cdot d^* \cdot c)^*$ und $z \geqslant (c \cdot a^* \cdot b \sqcup d)^*$. Jetzt kommt der entscheidende Schritt: Definieren wir die Unbekannten durch die rechten Seiten, dann erfüllen diese die ursprünglichen Ungleichungen — beachte die Richtung der Implikation im vorletzten, mit $(\circledast)$ markierten Schritt der Herleitung! Dabei nutzen wir aus, dass kleinste Präfixpunkte insbesondere Fixpunkte sind. Als Lohn der Mühen erhalten wir ***Conways Formel***:

$$
\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* := \begin{pmatrix} w & a^* \cdot b \cdot z \\ d^* \cdot c \cdot w & z \end{pmatrix} \quad \text{wobei} \quad \begin{cases} w := (a \sqcup b \cdot d^* \cdot c)^* \\ z := (c \cdot a^* \cdot b \sqcup d)^* \end{cases} \tag{B.117}
$$

Der Rest ist reine Fleißarbeit: Wir müssen verifizieren, dass unser Kandidat für A^* auch die entsprechenden Axiome erfüllt. Axiom (B.107a) gilt qua Konstruktion (aber Nachrechnen schadet nicht); im Folgenden zeigen wir die Gültigkeit des Invariantenaxioms (B.111a). Den Nachweis der symmetrischen Axiome (B.108a) und (B.111b) überlassen wir der geneigten Leserin bzw. dem geneigten Leser zur Übung.

Wir gehen ähnlich wie bei der Herleitung von Conways Formel vor und überführen Ungleichungen zwischen Matrizen in Ungleichungssysteme zwischen Skalaren, zunächst für die Voraussetzung des Invariantenaxioms (B.111a).

$$
\begin{aligned}
& \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \leqslant \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
\iff & \quad \{ \text{ punktweise Ordnung (B.104) } \} \\
& \left\{ \begin{array}{l} a \cdot i \sqcup b \cdot k \leqslant i \\ a \cdot j \sqcup b \cdot l \leqslant j \\ c \cdot i \sqcup d \cdot k \leqslant k \\ c \cdot j \sqcup d \cdot l \leqslant l \end{array} \right\} \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& \left\{ \begin{array}{llll} a \cdot i \leqslant i & \wedge & b \cdot k \leqslant i \\ a \cdot j \leqslant j & \wedge & b \cdot l \leqslant j \\ c \cdot i \leqslant k & \wedge & d \cdot k \leqslant k \\ c \cdot j \leqslant l & \wedge & d \cdot l \leqslant l \end{array} \right\}
\end{aligned}
$$

Wir erhalten acht Invarianten für die Skalare a, b, c und d. Daraus folgen vier Invarianten für die Hilfsgrößen w und z.

$$w \cdot i \leqslant i \qquad w \cdot j \leqslant j \qquad z \cdot k \leqslant k \qquad z \cdot l \leqslant l$$

Wir zeigen exemplarisch die erste Folgerung.

$$
\begin{aligned}
& w \cdot i \leqslant i \\
\impliedby & \quad \{ \text{ Invariantenaxiom (B.111a) } \} \\
& (a \sqcup b \cdot d^* \cdot c) \cdot i \leqslant i \\
\iff & \quad \{ \text{ Distributivgesetze (B.100b) } \} \\
& a \cdot i \sqcup b \cdot d^* \cdot c \cdot i \leqslant i \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& a \cdot i \leqslant i \quad \wedge \quad b \cdot d^* \cdot c \cdot i \leqslant i
\end{aligned}
$$

Laut Annahme gilt $a \cdot i \leqslant i$; um $b \cdot d^* \cdot c \cdot i \leqslant i$ nachzuweisen, rechnen wir.

$$
\begin{aligned}
& b \cdot d^* \cdot c \cdot i \\
\leqslant & \quad \{ \text{ Annahme: } c \cdot i \leqslant k \} \\
& b \cdot d^* \cdot k \\
\leqslant & \quad \{ \text{ Annahme: } d \cdot k \leqslant k \text{ und Invariantenaxiom (B.111a) } \} \\
& b \cdot k \\
\leqslant & \quad \{ \text{ Annahme: } b \cdot k \leqslant i \} \\
& i
\end{aligned}
$$

Damit können wir den Nachweis von (B.111a) antreten:

$$
\begin{aligned}
& \begin{pmatrix} a & b \\ c & d \end{pmatrix}^* \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \leqslant \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
\iff & \quad \{ \text{ Definition der Hülle (B.117) } \} \\
& \begin{pmatrix} w & a^* \cdot b \cdot z \\ d^* \cdot c \cdot w & z \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \leqslant \begin{pmatrix} i & j \\ k & l \end{pmatrix} \\
\iff & \quad \{ \text{ Definition Multiplikation (B.103d) und punktweise Ordnung (B.104) } \} \\
& \begin{Bmatrix} w \cdot i \sqcup a^* \cdot b \cdot z \cdot k \leqslant i \\ w \cdot j \sqcup a^* \cdot b \cdot z \cdot l \leqslant j \\ d^* \cdot c \cdot w \cdot i \sqcup z \cdot k \leqslant k \\ d^* \cdot c \cdot w \cdot j \sqcup z \cdot l \leqslant l \end{Bmatrix} \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& \begin{Bmatrix} w \cdot i \leqslant i & \wedge & a^* \cdot b \cdot z \cdot k \leqslant i \\ w \cdot j \leqslant j & \wedge & a^* \cdot b \cdot z \cdot l \leqslant j \\ d^* \cdot c \cdot w \cdot i \leqslant k & \wedge & z \cdot k \leqslant k \\ d^* \cdot c \cdot w \cdot j \leqslant l & \wedge & z \cdot l \leqslant l \end{Bmatrix}
\end{aligned}
$$

Vier der acht Ungleichungen haben wir bereits gezeigt; die restlichen vier weist man mit analogen Rechnungen nach: zum Beispiel $a^* \cdot b \cdot z \cdot k \leqslant a^* \cdot b \cdot k \leqslant a^* \cdot i \leqslant i$.

Übungen.

3. Folgern Sie die folgenden Äquivalenzen aus den Axiomen der Kleene Algebra.

$$a \leqslant 1 \iff a^* \leqslant 1 \iff a^* = 1 \tag{B.118}$$

4. Zeigen Sie, dass die beiden Axiomatisierungen von Kleene Algebren äquivalent sind: Axiom (B.109a) ist äquivalent zu (B.107a); das Axiom der Fixpunkt-Induktion (B.109b) ist äquivalent zu (B.111a).

5. Zeigen Sie mit Hilfe der Axiome, dass a^* der kleinste Präfixpunkt von vier verschiedenen Funktionen ist: sowohl von f, g, h als auch von k.

$$f(x) \coloneqq 1 \sqcup a \cdot x \qquad g(x) \coloneqq 1 \sqcup x \cdot a \qquad h(x) \coloneqq 1 \sqcup a \cdot x \sqcup x \cdot a \qquad k(x) \coloneqq 1 \sqcup a \sqcup x \cdot x$$

Zeigen Sie weiterhin, dass $a^* \cdot b \cdot c^*$ der kleinste Präfixpunkt von ℓ ist.

$$\ell(x) \coloneqq a \cdot x \sqcup b \sqcup x \cdot c$$

6. Zeigen Sie, dass die Umkehrungen der Bocksprungregeln (B.114a)–(B.114c) im Allgemeinen nicht gelten.

7. Zeigen Sie, dass in einem Potenzmengenmonoid die folgenden Identitäten gelten ($\mathrm{X} - \mathrm{Y}$ bezeichnet die Mengendifferenz).

$$(\mathrm{A} - 1)^* = \mathrm{A}^* = (\mathrm{A} \cup 1)^* \tag{B.119}$$

Hinweis: Das ist ein Fall für Dekompositionsregel (B.116).

Die Formale Begriffsanalyse (engl. Formal Concept Analysis) ermöglicht es, Zusammenhänge in Datenmengen zu erkennen und diese hierarchisch in einem Verband zu organisieren. Den Ausgangspunkt der Überlegungen bilden: eine Menge G von »Gegenständen« (engl. entities), eine Menge M von »Merkmalen« (engl. attributes) und eine Tabelle $T \subseteq G \times M$, die festhält, welche Gegenstände welche Merkmale besitzen.

	1	2	3	4	5	6	7	8	9	10
composite				×		×		×	×	×
even		×		×		×		×		×
odd	×		×		×		×		×	
prime		×	×		×		×			
square	×			×					×	

Im obigen Beispiel sind die Gegenstände Zahlen und die Merkmale Eigenschaften von Zahlen. Die Natur der Gegenstände bzw. Merkmale spielt für die Begriffsanalyse keine Rolle. Wir erhalten die gleichen Ergebnisse, wenn wir statt Zahlen Personen und deren Charakteristika untersuchen—die folgende Tabelle hält die Ergebnisse eines psychologischen Experiments fest.

	Andy	Bert	Charlie	Denis	Evan	Fred	George	Harry	Ivan	Jim
complicated				×		×		×	×	×
even-handed		×		×		×		×		×
odd	×		×		×		×		×	
prim		×	×		×		×			
square	×			×					×	

Die Funktion L ordnet einer Menge $A \subseteq G$ von Gegenständen deren gemeinsame Merkmale zu; umgekehrt bildet R eine Menge $B \subseteq M$ von Merkmalen auf die Gegenstände ab, die diese Merkmale besitzen.

$$L(A) = \{\, b \in M \mid \forall a \in A \,.\, (a,b) \in T \,\} \qquad R(B) = \{\, a \in G \mid \forall b \in B \,.\, (a,b) \in T \,\}$$

Sowohl L als auch R sind ***antiton***: je mehr Gegenstände betrachtet werden, desto weniger gemeinsame Merkmale gibt es und umgekehrt: $L(\{3,7\}) = \{o,p\}$, $L(\{2,3,7\}) = \{p\}$, $L(\{2,3,4,7\}) = \varnothing$ und $R(\{c,e\}) = \{4,6,8,10\}$, $R(\{c\}) = \{4,6,8,9,10\}$.

Ein ***Begriff*** oder ***Konzept*** (engl. concept) ist ein Paar (A,B) bestehend aus einer Gegenstandsmenge $A \subseteq G$ und einer Merkmalsmenge $B \subseteq M$, so dass die Gegenstände eindeutig die Merkmale bestimmen und umgekehrt: $L(A) = B$ und $A = R(B)$. Die Menge A heißt ***Umfang*** des Begriffs (engl. extent) und B ihr ***Inhalt*** (engl. intent).

Zum Beispiel sind $(\{4\},\{c,e,s\})$, $(\{4,6,8,10\},\{c,e\})$ und $(\{3,5,7\},\{o,p\})$ Konzepte. Die Gegenstandsmenge $\{1,4\}$ ist hingegen *nicht* Umfang eines Konzepts, da $L(\{1,4\}) = \{s\}$, aber $R(\{s\}) = \{1,4,9\}$.

Abbildung B.17.: Formale Begriffsanalyse (1. Teil).

Die Funktionen L und R bilden eine ***Galoisverbindung*** zwischen den Potenzmengenverbänden $(\mathscr{P}(\mathrm{M}), \supseteq)$ und $(\mathscr{P}(\mathrm{G}), \subseteq)$. Es gilt: $\mathrm{L}(\mathrm{A}) \supseteq \mathrm{B} \iff \mathrm{A} \subseteq \mathrm{R}(\mathrm{B})$. Daraus leiten sich eine Reihe von Eigenschaften ab, mit deren Hilfe sich die in einer Tabelle »verborgenen« Konzepte systematisch ermitteln lassen.

$$\mathrm{A} \subseteq \mathrm{R}(\mathrm{L}(\mathrm{A})) \qquad \mathrm{B} \subseteq \mathrm{L}(\mathrm{R}(\mathrm{B})) \qquad \mathrm{L}(\mathrm{A}) = \mathrm{L}(\mathrm{R}(\mathrm{L}(\mathrm{A}))) \qquad \mathrm{R}(\mathrm{B}) = \mathrm{R}(\mathrm{L}(\mathrm{R}(\mathrm{B})))$$

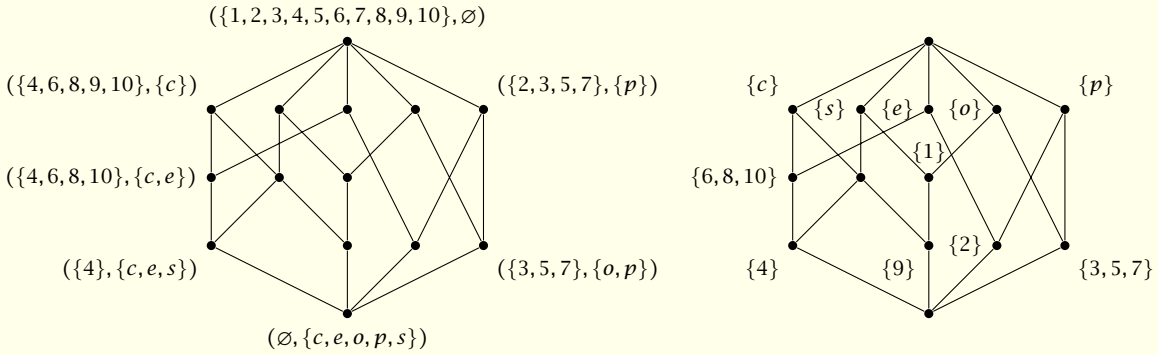
Man erhält zum Beispiel alle Konzepte, wenn man $(\mathrm{R}(\mathrm{L}(\mathrm{X})), \mathrm{L}(\mathrm{X}))$ für alle $\mathrm{X} \subseteq \mathrm{G}$ oder $(\mathrm{R}(\mathrm{Y}), \mathrm{L}(\mathrm{R}(\mathrm{Y})))$ für alle $\mathrm{Y} \subseteq \mathrm{M}$ berechnet.
Konzepte lassen sich nach ihrem Umfang bzw. nach ihrem Inhalt anordnen: Je größer der Umfang eines Begriffs, desto kleiner sein Inhalt und umgekehrt.

$$\mathrm{A}_1 \subseteq \mathrm{A}_2 \iff: (\mathrm{A}_1, \mathrm{B}_1) \leqslant (\mathrm{A}_2, \mathrm{B}_2) :\iff \mathrm{B}_1 \supseteq \mathrm{B}_2$$

Für die Zahlen von 1 bis 10 und deren Merkmale erhalten wir unter anderem:

$$(\{9\}, \{c, o, s\}) \leqslant (\{1, 9\}, \{o, s\}) \leqslant (\{1, 3, 5, 7, 9\}, \{o\})$$

Insgesamt lassen sich aus der Tabelle 14 Konzepte ableiten, die wie unten links angeordnet sind. (Versuchen Sie die fehlenden Beschriftungen zu ergänzen.)



Der Begriffsverband enthält die gleichen Informationen wie die ursprüngliche Tabelle:

$$(g, m) \in \mathrm{T} \iff p(g) \leqslant q(m)$$

wobei die Funktionen $p(g) = (\mathrm{R}(\mathrm{L}(\{g\})), \mathrm{L}(\{g\}))$ und $q(m) = (\mathrm{R}(\{m\}), \mathrm{L}(\mathrm{R}(\{m\})))$ einem Gegenstand bzw. einem Merkmal seine »Position« innerhalb des Verbands zuordnen. Beschriftet man wie oben rechts die Positionen mit ihren p- und q-Urbildern, erhält man eine kompaktere Darstellung, aus der sich die ursprüngliche Tabelle leicht rekonstruieren lässt: Zum Beispiel gilt $(4, s) \in \mathrm{T}$, da $p(4)$ unterhalb von $q(s)$ liegt. Allgemein liegen alle Merkmale eines Gegenstands g oberhalb seiner Position $p(g)$ und dual alle Gegenstände eines Merkmals unterhalb seiner Position $q(m)$. Der Gegenstand 4 hat zum Beispiel die Merkmale $\{c, s, e\}$; das Merkmal o besitzen die Gegenstände $\{1, 3, 5, 7, 9\}$. Der unbeschriftete Punkt in der Mitte links ist der Begriff $(\{4, 9\}, \{c, s\})$, da 4 und 9 unterhalb und c und s oberhalb liegen.

Abbildung B.18.: Formale Begriffsanalyse (2. Teil).

B.6.5. Galoisverbindungen⋆⋆

Was haben die folgenden Operationen gemeinsam? Natürliche Subtraktion ($\dot{-}$), ganzzahlige Division (***div***), Boden ($\lfloor\text{-}\rfloor$), Decke ($\lceil\text{-}\rceil$), Negation, Konjunktion und Implikation, Mengendifferenz und -vereinigung, Supremum, Infimum. Aus der Nähe betrachtet lassen sich nur schwer Gemeinsamkeiten ausmachen (bzw. nur oberflächliche: es handelt sich bei allen Beispielen um Funktionen), begeben wir uns also in die Vogelperspektive …

Seien $(\mathrm{P},\leqslant)$ und $(\mathrm{Q},\sqsubseteq)$ zwei Ordnungen[31] und $\ell : \mathrm{P} \leftarrow \mathrm{Q}$ und $r : \mathrm{P} \rightarrow \mathrm{Q}$ zwei Funktionen zwischen den Ordnungen. Die Funktionen ℓ und r bilden genau dann eine ***Galoisverbindung*** (engl. Galois connection), wenn für alle $a \in \mathrm{Q}$ und für alle $b \in \mathrm{P}$ gilt:

$$\ell(a) \leqslant b \text{ in } \mathrm{P} \iff a \sqsubseteq r(b) \text{ in } \mathrm{Q} \qquad (\mathrm{P},\leqslant) \underset{r}{\overset{\ell}{\underset{\longrightarrow}{\overset{\longleftarrow}{\bot}}}} (\mathrm{Q},\sqsubseteq) \tag{B.120}$$

Die Funktion ℓ heißt ***Linksadjunkte*** und r ***Rechtsadjunkte***; die Beziehung zwischen den Adjunkten notieren wir kurz mit $\ell \dashv r$. Gelegentlich werden ℓ und r auch ***quasiinverse*** Funktionen genannt, ein Begriff, den wir auch schon verwendet haben.

Eigenschaften von Galoisverbindungen Die definierende Äquivalenz (B.120) kommt etwas unscheinbar daher, aber aus ihr folgen eine Reihe von Eigenschaften, die wir im Folgenden herleiten und diskutieren.

Zunächst einmal sind die adjunkten Funktionen monoton.

$$a_1 \sqsubseteq a_2 \implies \ell(a_1) \leqslant \ell(a_2) \tag{B.121a}$$
$$b_1 \leqslant b_2 \implies r(b_1) \sqsubseteq r(b_2) \tag{B.121b}$$

Um die Monotonie von ℓ und r zu zeigen, führen wir indirekte Beweise.

$$\begin{array}{ll} & \ell(a_1) \leqslant x \\ \iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\ & a_1 \sqsubseteq r(x) \\ \impliedby & \quad \{\ \text{Annahme: } a_1 \sqsubseteq a_2\ \} \\ & a_2 \sqsubseteq r(x) \\ \iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\ & \ell(a_2) \leqslant x \end{array} \qquad \begin{array}{ll} & x \sqsubseteq r(b_1) \\ \iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\ & \ell(x) \leqslant b_1 \\ \implies & \quad \{\ \text{Annahme: } b_1 \leqslant b_2\ \} \\ & \ell(x) \leqslant b_2 \\ \iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\ & x \sqsubseteq r(b_2) \end{array}$$

Die Position der Adjunkten in (B.120) bestimmt die verwendete Beweistechnik: (B.15c) oder (B.15d). Wenn Sie zurückblättern, werden Sie feststellen, dass wir diese Beweise schon mehrfach für konkrete Galoisverbindungen geführt haben. (Welche?)

Aus der Äquivalenz (B.120) lassen sich zwei direkte Folgerungen ziehen, indem wir eine der beiden Ungleichungen »wahr machen«: Setzen wir $b := \ell(a)$, dann gilt die linke Seite per definitionem und somit auch die rechte Seite und umgekehrt für $a := r(b)$. Wir erhalten die sogenannten ***Vereinfachungsregeln*** (engl. simplification rules):

$$\text{(extensiv)} \qquad a \sqsubseteq r(\ell(a)) \qquad id \sqsubseteq r \circ \ell \tag{B.122a}$$
$$\text{(intensiv)} \qquad \ell(r(b)) \leqslant b \qquad \ell \circ r \leqslant id \tag{B.122b}$$

[31] Die Eigenschaft der Reflexivität ist tatsächlich entbehrlich — die Theorie der Galoisverbindungen lässt sich etwas allgemeiner, aber in gleicher Weise für *Quasiordnungen* entwickeln.

Jedes Element $a \in \mathrm{Q}$ ist ein Postfixpunkt von $r \circ \ell$ und jedes Element $b \in \mathrm{P}$ ist ein Präfixpunkt von $\ell \circ r$. Oder anders ausgedrückt: $r \circ \ell$ ist ***extensiv*** und $\ell \circ r$ ist ***intensiv***.

Wenden wir die Funktionen ein weiteres Mal an, erhalten wir Fixpunkte.

$$\ell(a) = \ell(r(\ell(a))) \qquad \ell = \ell \circ r \circ \ell \tag{B.122c}$$

$$r(\ell(r(b))) = r(b) \qquad r \circ \ell \circ r = r \tag{B.122d}$$

Links-rechts-links hat den gleichen Effekt wie einmal links und entsprechend rechts-links-rechts ist das Gleiche wie einmal rechts: $\ell(a)$ ist ein Fixpunkt von $\ell \circ r$ und $r(b)$ ist ein Fixpunkt von $r \circ \ell$. Der Nachweis gelingt mit einem einfachen Ping-Pong Beweis: Da ℓ monoton ist, folgt aus $a \sqsubseteq r(\ell(a))$ die Ungleichung $\ell(a) \leqslant \ell(r(\ell(a)))$; die andere Richtung folgt aus $\ell(r(b)) \leqslant b$ mit $b := \ell(a)$ — und analog für die andere Gleichung.

Die Folgerungen (B.122c)–(B.122d) heißen auch ***Abschlusseigenschaften*** (engl. closure rules). Insbesondere folgt aus ihnen, dass sowohl $r \circ \ell$ als auch $\ell \circ r$ idempotent sind: $(r \circ \ell) \circ (r \circ \ell) = (r \circ \ell)$ und $(\ell \circ r) \circ (\ell \circ r) = (\ell \circ r)$. Damit ist $r \circ \ell$ ein sogenannter ***Hüllenoperator*** (engl. closure operator): eine monotone, extensive und idempotente Funktion. Die gespiegelte Komposition $\ell \circ r$ exemplifiziert das duale Konzept des ***Kernoperators*** (engl. kernel operator): eine monotone, intensive und idempotente Funktion.

Ist eine der beiden Adjunkten injektiv, dann ist die andere surjektiv und umgekehrt.

$$\ell \text{ injektiv} \iff id = r \circ \ell \iff r \text{ surjektiv} \tag{B.123a}$$

$$r \text{ injektiv} \iff \ell \circ r = id \iff \ell \text{ surjektiv} \tag{B.123b}$$

Aus $id = r \circ \ell$ folgt unmittelbar, dass r surjektiv und ℓ injektiv ist. Umgekehrt impliziert $\ell(a) = \ell(r(\ell(a)))$ (B.122c) die Gleichung $a = r(\ell(a))$, sofern ℓ injektiv ist; wenn r surjektiv ist, folgt die Gleichung aus $r(\ell(r(b))) = r(b)$ (B.122d).

Kommen wir zur wohl wichtigsten Eigenschaft von Galoisverbindungen:

Galoisverbindungen: Erhaltungseigenschaften

Linksadjunkte erhalten Suprema und Rechtsadjunkte erhalten Infima.

Diese zentrale Eigenschaft formalisieren die sogenannten ***Erhaltungssätze***:

$$\ell\left(\bigsqcup_{i\in\mathrm{I}} a_i\right) = \bigvee_{i\in\mathrm{I}} \ell(a_i) \qquad r\left(\bigwedge_{i\in\mathrm{I}} b_i\right) = \bigsqcap_{i\in\mathrm{I}} r(b_i) \tag{B.124}$$

Zum Nachweis greifen wir wieder auf die Technik des indirekten Beweises zurück.

$$\begin{aligned}
& \ell\left(\bigsqcup_{i\in\mathrm{I}} a_i\right) \leqslant x \\
\iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\
& \bigsqcup_{i\in\mathrm{I}} a_i \sqsubseteq r(x) \\
\iff & \quad \{\ \text{Supremum (B.18)}\ \} \\
& \forall i \in \mathrm{I} \,.\, a_i \sqsubseteq r(x) \\
\iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\
& \forall i \in \mathrm{I} \,.\, \ell(a_i) \leqslant x \\
\iff & \quad \{\ \text{Supremum (B.18)}\ \} \\
& \bigvee_{i\in\mathrm{I}} \ell(a_i) \leqslant x
\end{aligned}
\qquad
\begin{aligned}
& x \sqsubseteq r\left(\bigwedge_{i\in\mathrm{I}} b_i\right) \\
\iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\
& \ell(x) \leqslant \bigwedge_{i\in\mathrm{I}} b_i \\
\iff & \quad \{\ \text{Infimum (B.19)}\ \} \\
& \forall i \in \mathrm{I} \,.\, \ell(x) \leqslant b_i \\
\iff & \quad \{\ \ell \dashv r \text{ (B.120)}\ \} \\
& \forall i \in \mathrm{I} \,.\, x \sqsubseteq r(b_i) \\
\iff & \quad \{\ \text{Infimum (B.19)}\ \} \\
& x \sqsubseteq \bigsqcap_{i\in\mathrm{I}} r(b_i)
\end{aligned}$$

Im linken Beweis räumen wir zunächst die Linksadjunkte ℓ »aus dem Weg«, um die Eigenschaft des Supremums (B.18) anwenden zu können; dann wird ℓ zurückgeholt und (B.18) rückwärts angewendet.

Es lohnt sich, vier Spezialfälle festzuhalten: Die Linksadjunkte ℓ erhält $\bot$ und $\sqcup$; die Rechtsadjunkte r erhält $\top$ und $\sqcap$.

$$\ell(\bot) = \bot \qquad\qquad r(\top) = \top \tag{B.125a}$$

$$\ell(a_1 \sqcup a_2) = \ell(a_1) \vee \ell(a_2) \qquad\qquad r(b_1 \wedge b_2) = r(b_1) \sqcap r(b_2) \tag{B.125b}$$

Die Eigenschaften können insbesondere verwendet werden, um zu zeigen, dass eine gegebene Funktion *nicht* links- oder rechtsadjunkt ist. Zum Beispiel kann die Abbildung $f : \mathscr{P}(\mathrm{U}) \to \mathscr{P}(\mathrm{U})$ mit $f(\mathrm{X}) = \{a\} \cup \mathrm{X}$ keine Linksadjunkte sein, da $f(\varnothing) = \{a\} \neq \varnothing$. (Wir werden später sehen, dass f aber rechtsadjunkt ist.)

Existenz von Galoisverbindungen Die zentrale Eigenschaft von Galoisverbindungen lässt sich auch umkehren: Wenn ℓ beliebige Suprema erhält, dann ist ℓ linksadjunkt; wenn r beliebige Infima erhält, dann ist r rechtsadjunkt. Ihre jeweiligen Adjunkten sind durch die folgenden Formeln gegeben.

$$r(b) := \bigsqcup_{x \in \mathrm{X}} x \text{ mit } \mathrm{X} := \{\, x \mid \ell(x) \leqslant b \,\} \qquad\qquad \ell(a) := \bigvee_{y \in \mathrm{Y}} x \text{ mit } \mathrm{Y} := \{\, y \mid a \leqslant r(y) \,\}$$

Erinnern Sie sich, wie wir die natürliche Subtraktion in Abschnitt B.5.1 eingeführt haben? In der umgangssprachlichen Beschreibung haben wir $a \dot{-} p$ als die kleinste natürliche Zahl x definiert, so dass $a \leqslant x + p$ gilt. (Damit ist Monus $\dot{-} \dot{-} p$ als linksadjunkt geoutet.)

Die Äquivalenz (B.120) zeigen wir jeweils mit einem Ping-Pong Beweis.

$$\begin{aligned}
& \ell(a) \leqslant b \\
\Longrightarrow\quad & \{\, a \in \mathrm{X} \,\} \\
& a \sqsubseteq \bigsqcup_{x \in \mathrm{X}} x \\
\Longrightarrow\quad & \{\, \ell \text{ ist monoton} \,\} \\
& \ell(a) \leqslant \ell\Big(\bigsqcup_{x \in \mathrm{X}} x\Big) \\
\Longrightarrow\quad & \{\, \text{Annahme: } \ell \text{ erhält Suprema} \,\} \\
& \ell(a) \leqslant \bigvee_{x \in \mathrm{X}} \ell(x) \\
\Longrightarrow\quad & \{\, \bigvee_{x \in \mathrm{X}} \ell(x) \leqslant b \,\} \\
& \ell(a) \leqslant b
\end{aligned}
\qquad\qquad
\begin{aligned}
& a \sqsubseteq r(b) \\
\Longrightarrow\quad & \{\, b \in \mathrm{Y} \,\} \\
& \bigvee_{y \in \mathrm{Y}} y \leqslant b \\
\Longrightarrow\quad & \{\, r \text{ ist monoton} \,\} \\
& r\Big(\bigvee_{y \in \mathrm{Y}} y\Big) \sqsubseteq r(b) \\
\Longrightarrow\quad & \{\, \text{Annahme: } r \text{ erhält Infima} \,\} \\
& \bigsqcup_{y \in \mathrm{Y}} r(y) \sqsubseteq r(b) \\
\Longrightarrow\quad & \{\, a \sqsubseteq \bigsqcup_{y \in \mathrm{Y}} r(y) \,\} \\
& a \sqsubseteq r(b)
\end{aligned}$$

Im zweiten Schritt nutzen wir jeweils aus, dass Funktionen, die Suprema oder Infima erhalten, insbesondere monoton sind (Beweis zur Übung).

Beispiele für Galoisverbindungen Adjunkte bzw. quasiinverse Funktionen verallgemeinern inverse Funktionen. Seien $(\mathrm{A}, =)$ und $(\mathrm{B}, =)$ sogenannte ***diskrete*** Ordnungen. Wenn die Funktionen $f : \mathrm{A} \leftarrow \mathrm{B}$ und $g : \mathrm{A} \to \mathrm{B}$ invers zueinander sind,

$$f(x) = y \quad \Longleftrightarrow \quad x = g(y)$$

dann gilt sowohl $f \dashv g$ als auch $g \dashv f$. Da die diskrete Ordnung symmetrisch ist, sind beide Funktionen sowohl links- als auch rechtsadjunkt. Die Umkehrung gilt ebenfalls: Aus $f \dashv g$ und

$g \dashv f$ folgt, dass f und g invers zueinander sind, eine direkte Konsequenz aus den Vereinfachungsregeln (B.122a)–(B.122b).

Galoisverbindungen findet man zuhauf und in den unterschiedlichsten Teilgebieten der Mathematik — man muss nur genau genug hinschauen. Im Folgenden behandeln wir in loser Folge einige Beispiele aus den einführenden Abschnitten des Kompendiums: Logik, Mengenlehre und Verbandstheorie.

Logik Die ***Negation*** ist ein Beispiel für eine ***selbstadjunkte*** Funktion.

$$(\neg a) \Rightarrow b \text{ in } \mathbb{B} \quad \Longleftrightarrow \quad a \Leftarrow (\neg b) \text{ in } \mathbb{B}$$

Man sollte sich stets klarmachen, welche Ordnungen an einer Galoisverbindung beteiligt sind — eine Verbindung besteht aus *vier* Angaben: den beiden Adjunkten und den beiden Ordnungen. Im Fall der Negation sind auf der linken Seite die Wahrheitswerte mittels Implikation angeordnet (*false* $\Rightarrow$ *true* oder $0 \leqslant 1$). Die Negation ist antiton, so dass auf der rechten Seite die duale Ordnung zum Einsatz kommt (*false* $\Leftarrow$ *true* oder $1 \geqslant 0$). Da die Ordnungen in gegenläufige Richtungen weisen, spricht man genauer von einer ***antitonen*** Galoisverbindung. Mit der Galoisbrille auf der Nase lassen sich viele Gesetze der Booleschen Algebra neu interpretieren. Spezialisieren wir zum Beispiel die Erhaltungsgesetze (B.125a)–(B.125b),

$$\neg \mathit{false} = \mathit{true} \qquad \neg \mathit{true} = \mathit{false}$$
$$\neg(a_1 \vee a_2) = \neg a_1 \wedge \neg a_2 \qquad \neg(b_1 \wedge b_2) = \neg b_1 \vee \neg b_2$$

erhalten wir die Dualitätsgesetze und die De Morganschen Gesetze. Aufgrund der Antitonie wird das Infimum, die Konjunktion, auf das Supremum, die Disjunktion, abgebildet — das Infimum in der dualen Ordnung entspricht dem Supremum in der ursprünglichen Ordnung und umgekehrt.

Auch Disjunktion und Konjunktion sind Komponenten von Galoisverbindungen.

$$(a \wedge p) \Rightarrow b \quad \Longleftrightarrow \quad a \Rightarrow (b \Leftarrow p) \qquad (a \wedge p) \Rightarrow b \quad \Longleftrightarrow \quad a \Rightarrow (b \vee \neg p)$$
$$(a \not\Leftarrow p) \Rightarrow b \quad \Longleftrightarrow \quad a \Rightarrow (b \vee p) \qquad a \wedge \neg p \Rightarrow b \quad \Longleftrightarrow \quad a \Rightarrow b \vee p$$

In beiden Fällen handelt es sich um ***parametrisierte Galoisverbindungen***: Für jedes $p \in \mathbb{B}$ ist $\text{-} \wedge p$ linksadjunkt und $\text{-} \vee p$ rechtsadjunkt. Lassen Sie sich nicht dadurch irritieren, dass die ***Umkehrimplikation*** $\Leftarrow$ im Fall der Negation als Relation verwendet wird und hier als Operation auf Wahrheitswerten. Der Perspektivwechsel beruht auf der Eins-zu-eins-Korrespondenz zwischen Relationen $\mathcal{P}(A \times B)$ und $\mathbb{B}$-wertigen Funktionen $A \times B \to \mathbb{B}$. Die ***Nichtimplikation*** $\not\Leftarrow$ ist die Negation der Implikation: $a \not\Leftarrow b := \neg(a \Rightarrow b)$. Die obigen Äquivalenzen können leicht mit Hilfe von Wahrheitstabellen verifiziert werden:[32]

p	0	0	0	0	1	1	1	1
a	0	0	1	1	0	0	1	1
b	0	1	0	1	0	1	0	1
$(a \wedge p) \Rightarrow b$	1	1	1	1	1	1	0	1
$a \Rightarrow (b \Leftarrow p)$	1	1	1	1	1	1	0	1
$(a \not\Leftarrow p) \Rightarrow b$	1	1	0	1	1	1	1	1
$a \Rightarrow (b \vee p)$	1	1	0	1	1	1	1	1

[32] Die Einträge lassen sich im Kopf bestimmen, indem man versucht, die Formeln zu *falsifizieren*: Zum Beispiel ist $(a \wedge p) \Rightarrow b$ falsch, wenn $a \wedge p$ wahr ist und b falsch; $a \wedge p$ ist wiederum wahr, wenn sowohl a als auch p wahr sind.

Es ist erhellend, wiederum die Erhaltungsgesetze (B.125a)–(B.125b) zu spezialisieren:

$$\begin{aligned} \mathit{false} \wedge p &= \mathit{false} & \qquad \mathit{true} \Leftarrow p &= \mathit{true} \\ (a_1 \vee a_2) \wedge p &= (a_1 \wedge p) \wedge (a_2 \wedge p) & \qquad (b_1 \wedge b_2) \Leftarrow p &= (b_1 \Leftarrow p) \vee (b_2 \Leftarrow p) \\ \mathit{false} \not\Leftarrow p &= \mathit{false} & \qquad \mathit{true} \vee p &= \mathit{true} \\ (a_1 \vee a_2) \not\Leftarrow p &= (a_1 \not\Leftarrow p) \wedge (a_2 \not\Leftarrow p) & \qquad (b_1 \wedge b_2) \vee p &= (b_1 \vee p) \vee (b_2 \vee p) \end{aligned}$$

Wir erhalten die Extremgesetze und die Distributivgesetze. Auch die Umkehrimplikation distribuiert über die Konjunktion: Um $b_1 \wedge b_2$ unter der Voraussetzung p zu zeigen, müssen wir sowohl b_1 als auch b_2 jeweils unter der Voraussetzung p nachweisen.

Soviel zur Aussagenlogik — was können wir für die Prädikatenlogik mitnehmen? Am Anfang steht die vielleicht überraschende Erkenntnis, dass Quantoren nichts anderes sind als Schranken: Der Existenzquantor entspricht dem Supremum und der Allquantor dem Infimum. Die Notation verschleiert den Zusammenhang vielleicht etwas: Statt $\bigsqcup_{i\in \mathrm{I}} a_i$ schreiben wir in der Logik $\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)$ und aus $\bigsqcap_{i\in \mathrm{I}} a_i$ wird $\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)$. (Eine indizierte Familie a_i von Elementen aus U entspricht einer Abbildung $\mathrm{I} \to \mathrm{U}$; eine Aussagenfunktion oder ein ***Prädikat*** P ist formal ebenfalls eine Abbildung $\mathrm{X} \to \mathbb{B}$.) Damit lassen sich die obigen Distributivgesetze wie folgt verallgemeinern.

$$\begin{aligned} (\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \wedge p &= \exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \wedge p \\ (\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \Leftarrow p &= \forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \Leftarrow p \\ (\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \not\Leftarrow p &= \exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \not\Leftarrow p \\ (\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \vee p &= \forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \vee p \end{aligned}$$

Wenn Sie zurückblättern, werden Sie feststellen, dass wir bereits einige der Gesetze in Beweisen verwendet haben.

Mengenlehre Da die Mengenoperationen auf aussagenlogische Verknüpfungen zurückgeführt werden, $\cap$ auf $\wedge$, $\cup$ auf $\vee$ usw., vererben sich die Eigenschaften der Verknüpfungen und die Beziehungen zwischen ihnen. Der Mengendurchschnitt $-\cap \mathrm{P}$ ist zum Beispiel linksadjunkt, die Mengenvereinigung $-\cup \mathrm{P}$ rechtsadjunkt.

$$\begin{aligned} \mathrm{A} \cap \mathrm{P} \subseteq \mathrm{B} &\iff \mathrm{A} \subseteq \mathrm{B} \Leftarrow \mathrm{P} & \qquad \mathrm{A} \cap \mathrm{P} \subseteq \mathrm{B} &\iff \mathrm{A} \subseteq \mathrm{B} \cup \neg \mathrm{P} \\ \mathrm{A} - \mathrm{P} \subseteq \mathrm{B} &\iff \mathrm{A} \subseteq \mathrm{B} \cup \mathrm{P} & \qquad \mathrm{A} \cap \neg \mathrm{P} \subseteq \mathrm{B} &\iff \mathrm{A} \subseteq \mathrm{B} \cup \mathrm{P} \end{aligned}$$

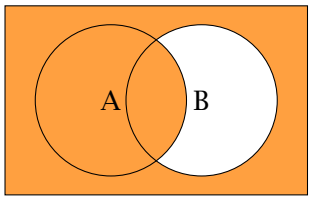
Die Linksadjunkte der Vereinigung ist die Mengendifferenz — ähnlich wie die natürliche Subtraktion hat die Vereinigung zwar keine Inverse, aber eine Quasiinverse. Interessanterweise gibt es weder eine etablierte Notation noch einen Namen für das duale Konzept, die Rechtsadjunkte des Durchschnitts. In Ermangelung einer besseren Alternative übernehmen wir das aussagenlogische Symbol, die Umkehrimplikation, und überladen damit die Notation.[33] Also, seien Sie kreativ und denken sich einen Namen aus (Vorschläge bitte an support@harry-hacker.org). Einstweilen verwenden wir einen Platzhalter:

(⟨Platzhalter⟩) $\qquad \mathrm{A} \Leftarrow \mathrm{B} := \{\, x \mid x \in \mathrm{A} \Leftarrow x \in \mathrm{B} \,\} = \{\, x \mid x \in \mathrm{A} \vee x \notin \mathrm{B} \,\}$

[33] Witzigerweise verhält es sich in der Aussagenlogik genau anders herum: Es gibt keine etablierte Notation für die Linksadjunkte der Disjunktion; wir haben in Ermangelung einer besseren Alternative die »Nichtimplikation« verwendet, aber das Konzept ist, wie Sie vielleicht gemerkt haben, weniger griffig als die Mengendifferenz.

Vielleicht inspiriert Sie ja das Venn-Diagramm bei der Namensgebung.

⟨Platzhalter⟩



$A \Leftarrow B$

Der Nachweis der Galoisverbindungen $\text{-} \cap P \dashv \text{-} \cup \neg P$ und $\text{-} \cap \neg P \dashv \text{-} \cup P$ verdeutlicht noch einmal, dass die Eigenschaften der Mengenoperationen aus den Eigenschaften der aussagenlogischen Verknüpfungen abgeleitet werden.

$$
\begin{array}{ll}
 & A \subseteq B \cup P \\
\iff & \quad \{ \text{ Definition Teilmenge } \} \\
 & \forall x \,.\, x \in A \implies x \in B \cup P \\
\iff & \quad \{ \text{ Definition Vereinigung } \} \\
 & \forall x \,.\, x \in A \implies x \in B \vee x \in P \\
\iff & \quad \{ \text{ Logik: } \text{-} \wedge \neg p \dashv \text{-} \vee p \} \\
 & \forall x \,.\, x \in A \wedge x \notin P \implies x \in B \\
\iff & \quad \{ \text{ Definition Differenz } \} \\
 & \forall x \,.\, x \in A - P \implies x \in B \\
\iff & \quad \{ \text{ Definition Teilmenge } \} \\
 & A - P \subseteq B
\end{array}
\qquad
\begin{array}{ll}
 & A \cap P \subseteq B \\
\iff & \quad \{ \text{ Definition Teilmenge } \} \\
 & \forall x \,.\, x \in A \cap P \implies x \in B \\
\iff & \quad \{ \text{ Definition Durchschnitt } \} \\
 & \forall x \,.\, x \in A \wedge x \in P \implies x \in B \\
\iff & \quad \{ \text{ Logik: } \text{-} \wedge p \dashv \text{-} \vee \neg p \} \\
 & \forall x \,.\, x \in A \implies x \in B \vee x \notin P \\
\iff & \quad \{ \text{ Definition } \langle \text{Platzhalter} \rangle \} \\
 & \forall x \,.\, x \in A \implies x \in B \Leftarrow P \\
\iff & \quad \{ \text{ Definition Teilmenge } \} \\
 & A \subseteq B \Leftarrow P
\end{array}
$$

Es ist lehrreich, wieder einige »Galois-Gesetze« zu spezialisieren. Die Instanzen der Vereinfachungsregeln (B.122a)–(B.122b) kommen einem wahrscheinlich bekannt vor:

$$A \subseteq (A - P) \cup P \qquad\qquad (B \cup P) - P \subseteq B$$

Aus parametrisierten Galoisverbindungen lassen sich oft weitere Verbindungen ableiten, indem die Rolle von Argument und Parameter vertauscht wird. Im Fall der Mengendifferenz erhalten wir zum Beispiel die folgende Verbindung.

$$P - A \subseteq B \iff A \supseteq P - B$$

Die Operation $P - \text{-}$ ist somit selbstadjunkt und *antiton*. Der Beweis zeigt, dass die induzierte Galoisverbindung aus der Kommutativität der Mengenvereinigung folgt.

$$
\begin{array}{ll}
 & P - A \subseteq B \\
\iff & \quad \{ \text{ Mengenlehre: } \text{-} - P \dashv \text{-} \cup P \} \\
 & P \subseteq B \cup A \\
\iff & \quad \{ \cup \text{ ist kommutativ } \} \\
 & P \subseteq A \cup B \\
\iff & \quad \{ \text{ Mengenlehre: } \text{-} - P \dashv \text{-} \cup P \} \\
 & P - B \subseteq A \\
\iff & \quad \{ \text{ duale Ordnung } \} \\
 & A \supseteq P - B
\end{array}
$$

Da die Mengendifferenz isoton im ersten und antiton im zweiten Argument ist, spezialisieren sich die Erhaltungsgesetze (B.125a)–(B.125b) wie folgt (U ist die größte Menge, die Grundmenge oder das Universum).

$$\varnothing - P = \varnothing \qquad\qquad P - U = \varnothing$$
$$(A_1 \cup A_2) - P = (A_1 - P) \cup (A_2 - P) \qquad\qquad P - (B_1 \cap B_2) = (P - B_1) \cup (P - B_2)$$

Verbandstheorie Die Beispiele aus Logik und Mengenlehre haben eindrucksvoll die Bedeutung der Erhaltungsgesetze aufgezeigt. Dass Linksadjunkte Suprema erhalten und Rechtsadjunkte Infima hat einen tieferen Grund: Suprema sind selbst linksadjunkt und Infima sind rechtsadjunkt! Betrachten wir die indirekten Definitionen von $\sqcup$ und $\sqcap$.

$$a_1 \sqcup a_2 \leqslant b \iff a_1 \leqslant b \;\wedge\; a_2 \leqslant b$$
$$a \leqslant b_1 \;\wedge\; a \leqslant b_2 \iff a \leqslant b_1 \sqcap b_2$$

Die Äquivalenzen haben nicht ganz die Form einer Galoisverbindung (B.120): $\sqcup$ und $\sqcap$ sind binäre Operationen, nicht unäre; auf den jeweils gegenüberliegenden Seiten stehen zwei Ungleichungen, nicht eine. Diese Beobachtungen legen den »Verdacht« nahe, dass eine der beteiligten Ordnungen eine Ordnung auf Paaren ist. Mit dieser Idee im Gepäck lassen sich die Äquivalenzen in die richtige Form bringen (am Beispiel des Supremums).

$$\begin{aligned}
& a_1 \sqcup a_2 \leqslant b \iff a_1 \leqslant b \;\wedge\; a_2 \leqslant b \\
\iff & \quad \{ \text{ Ordnung auf Paaren, siehe unten } \} \\
& \sqcup(a_1, a_2) \leqslant b \iff (a_1, a_2) \leqslant (b, b) \\
\iff & \quad \{ \text{ sei } \mathbf{a} := (a_1, a_2) \text{ und } \Delta(b) = (b, b) \} \\
& \sqcup(\mathbf{a}) \leqslant b \iff \mathbf{a} \leqslant \Delta(b)
\end{aligned}$$

Im ersten Schritt machen wir die Paare explizit und notieren $\sqcup$ präfix statt infix. Paare werden ***komponentenweise*** angeordnet. Sind $(P_1, \leqslant_1)$ und $(P_2, \leqslant_2)$ Ordnungen, dann ist auch das kartesische Produkt $(P_1 \times P_2, \leqslant)$ eine Ordnung, wobei $\leqslant$ wie folgt definiert ist.

$$(a_1, a_2) \leqslant (b_1, b_2) \iff a_1 \leqslant_1 b_1 \;\wedge\; a_2 \leqslant_2 b_2$$

Im zweiten Schritt machen wir die Rechtsadjunkte explizit: Die sogenannte ***Diagonalfunktion*** $\Delta : P \to P \times P$ bildet ein Element auf ein Paar ab: $\Delta(b) = (b, b)$.

Ganz entsprechend können auch die indirekten Definitionen von Suprema (B.18) und Infima (B.19) in »Galois-Form« gebracht werden. An die Stelle von Paaren treten Funktionen über einer festen Indexmenge. Sei X eine beliebige Menge und $(P, \leqslant)$ eine Ordnung, dann bildet auch die Menge aller Funktionen $(X \to P, \leqslant)$ eine Ordnung, wobei $\leqslant$ wie folgt definiert ist.

$$f \leqslant g \iff \forall\, x \in X \,.\, f(x) \leqslant g(x) \tag{B.126}$$

Funktionen sind ***punktweise*** angeordnet: f ist kleiner als g, wenn für alle Argumente x der Funktionswert $f(x)$ höchstens so groß ist wie $g(x)$. Punktweise Ordnungen sind angenehm in der Handhabung, da viele Eigenschaften der zugrundeliegenden Ordnung geerbt werden. Zum Beispiel werden Suprema und Infima punktweise gebildet.

$$\amalg\,(x) := \bot \qquad\qquad \top\!\!\top\,(x) := \top \tag{B.127a}$$
$$(f \sqcup g)(x) := f(x) \sqcup g(x) \qquad\qquad (f \sqcap g)(x) := f(x) \sqcap g(x) \tag{B.127b}$$

Zum Nachweis zeigen wir, dass $f \sqcup g$ die Eigenschaft des Supremums (B.22) erfüllt.

$$
\begin{aligned}
& f \sqcup g \leqslant z \\
\iff & \quad \{ \text{ Definition } \sqcup \text{ (B.127b) und punktweise Ordnung (B.126) } \} \\
& \forall\, x \in \mathrm{X} \,.\, f(x) \sqcup g(x) \leqslant z(x) \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& \forall\, x \in \mathrm{X} \,.\, f(x) \leqslant z(x) \;\wedge\; g(x) \leqslant z(x) \\
\iff & \quad \{ \text{ Logik, siehe auch weiter unten } (\circledast) \} \\
& (\forall\, x \in \mathrm{X} \,.\, f(x) \leqslant z(x)) \;\wedge\; (\forall\, x \in \mathrm{X} \,.\, g(x) \leqslant z(x)) \\
\iff & \quad \{ \text{ Definition } \sqcup \text{ (B.127b) und punktweise Ordnung (B.126) } \} \\
& f \leqslant z \;\wedge\; g \leqslant z
\end{aligned}
$$

Schließlich müssen wir noch die Diagonalfunktion anpassen: Sie besitzt nunmehr den Typ $\Delta : \mathrm{P} \to (\mathrm{X} \to \mathrm{P})$ und bildet Elemente auf Funktionen ab: $\Delta(b)(x) = b$ — somit ist Δ eine sogenannte ***Funktion höherer Ordnung***. Die Linksadjunkte dieser unscheinbaren Funktion ist das Supremum und die Rechtsadjunkte das Infimum:

$$
\begin{aligned}
\bigsqcup f \leqslant b \quad &\iff \quad f \leqslant \Delta(b) \\
\Delta(a) \leqslant g \quad &\iff \quad a \leqslant \bigsqcap g
\end{aligned}
$$

Der Charme von Galoisverbindung besteht darin, schwierige Konzepte (hier: Suprema und Infima) auf einfache Konzepte (hier: Diagonalfunktion) zurückzuführen. Auf diese Weise lassen sich oft vergleichsweise schwierige Probleme in einfachere Probleme übersetzen und so einer Lösung zuführen (das Originalproblem, auf das die Galoistheorie zurückgeht, ist ein schönes Beispiel dafür, aber leider zu involviert, um es hier zu reproduzieren). Umgekehrt können oft Eigenschaften der indirekt definierten Konzepte aus einfachen, ja trivialen Eigenschaften der zugrundeliegenden Konzepte hergeleitet werden. Um diese wichtige Idee nicht im Abstrakten zu belassen, lassen Sie uns die zentrale Eigenschaft von Adjunkten, die Erhaltungsgesetze (B.125a)–(B.125b), ein zweites Mal beweisen, dieses Mal etwas »funktionaler« und weniger mengentheoretisch.

$$
\ell\left(\bigsqcup f\right) = \bigvee (\ell \circ f) \qquad\qquad r\left(\bigwedge g\right) = \bigsqcap (r \circ g)
$$

Die Funktion $\Delta(x)$ ist eine *konstante* Funktion: Sie ignoriert ihr Argument und gibt immer x als Funktionswert zurück. Wenn wir eine konstante Funktion mit einer anderen Funktion komponieren, erhalten wir (Überraschung!) wiederum eine konstante Funktion: $f \circ \Delta(x) = \Delta(f(x))$. Auf dieser unscheinbaren Eigenschaft fußen die Erhaltungsgesetze:

$$
\begin{aligned}
& \ell\left(\bigsqcup f\right) \leqslant x \\
\iff & \quad \{\, \ell \dashv r \,\} \\
& \bigsqcup f \sqsubseteq r(x) \\
\iff & \quad \{\, \textstyle\bigsqcup \dashv \Delta \,\} \\
& f \sqsubseteq \Delta(r(x)) \\
\iff & \quad \{\, f \circ \Delta(x) = \Delta(f(x)) \,\} \\
& f \sqsubseteq r \circ \Delta(x) \\
\iff & \quad \{\, \ell \circ \text{-} \dashv r \circ \text{-} \,\} \\
& \ell \circ f \leqslant \Delta(x) \\
\iff & \quad \{\, \textstyle\bigvee \dashv \Delta \,\} \\
& \textstyle\bigvee (\ell \circ f) \leqslant x
\end{aligned}
\qquad\qquad
\begin{aligned}
& x \leqslant r\left(\bigwedge g\right) \\
\iff & \quad \{\, \ell \dashv r \,\} \\
& \ell(x) \sqsubseteq \bigwedge g \\
\iff & \quad \{\, \Delta \dashv \textstyle\bigwedge \,\} \\
& \Delta(\ell(x)) \sqsubseteq g \\
\iff & \quad \{\, f \circ \Delta(x) = \Delta(f(x)) \,\} \\
& \ell \circ \Delta(x) \sqsubseteq g \\
\iff & \quad \{\, \ell \circ \text{-} \dashv r \circ \text{-} \,\} \\
& \Delta(x) \leqslant r \circ g \\
\iff & \quad \{\, \Delta \dashv \textstyle\bigsqcap \,\} \\
& x \leqslant \textstyle\bigsqcap (r \circ g)
\end{aligned}
$$

Neben den Galoisverbindungen, $\bigsqcup \dashv \Delta \dashv \bigsqcap$, $\bigvee \dashv \Delta \dashv \bigwedge$ und $\ell \dashv r$ (aus $\ell \dashv r$ folgt $\ell \circ \text{-} \dashv r \circ \text{-}$, siehe Übung B.6.13), kommt nur die »unscheinbare Eigenschaft« zur Anwendung.

Zum Abschluss spezialisieren wir wie immer die Erhaltungsgesetze (B.125a)–(B.125b) — deren Verallgemeinerung wir gerade gezeigt haben.

$$\bigsqcup(\perp\!\!\!\perp) = \bot \qquad\qquad \bigsqcap(\top\!\!\!\top) = \top$$
$$\bigsqcup(f_1 \sqcup f_2) = \bigsqcup(f_1) \sqcup \bigsqcup(f_2) \qquad\qquad \bigsqcap(g_1 \sqcap g_2) = \bigsqcap(g_1) \sqcap \bigsqcap(g_2)$$

Ersetzen wir Supremum und Infimum durch logische Quantoren, erhalten wir bekannte Gesetze der Prädikatenlogik — links in der kompakten, »punktfreien« Form und rechts in der etwas länglichen, »punkthaltigen« Variante mit expliziten Bindern.

$$\exists(\mathit{false}) = \mathit{false} \qquad (\exists\, x \in \mathrm{X} \,.\, \mathit{false}) \iff \mathit{false}$$
$$\forall(\mathit{true}) = \mathit{true} \qquad (\forall\, x \in \mathrm{X} \,.\, \mathit{true}) \iff \mathit{true}$$
$$\exists(\mathrm{P} \vee \mathrm{Q}) = \exists\mathrm{P} \vee \exists\mathrm{Q} \qquad (\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \vee \mathrm{Q}(x)) \iff (\exists\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \vee (\exists\, x \in \mathrm{X} \,.\, \mathrm{Q}(x))$$
$$\forall(\mathrm{P} \wedge \mathrm{Q}) = \forall\mathrm{P} \wedge \forall\mathrm{Q} \qquad (\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x) \wedge \mathrm{Q}(x)) \iff (\forall\, x \in \mathrm{X} \,.\, \mathrm{P}(x)) \wedge (\forall\, x \in \mathrm{X} \,.\, \mathrm{Q}(x))$$

Die Eigenschaft des Allquantors haben wir übrigens gerade beim Nachweis verwendet, dass Suprema und Infima von Funktionen punktweise gebildet werden — in dem mit $(\circledast)$ markierten Schritt.

Formale Begriffsanalyse Abbildungen B.17 und B.18 skizzieren die Idee der ***formalen Begriffsanalyse***. Die folgende Rechnung zeigt, dass die beteiligten Funktionen $\mathrm{L} : \mathscr{P}(\mathrm{M}) \leftarrow \mathscr{P}(\mathrm{G})$ und $\mathrm{R} : \mathscr{P}(\mathrm{M}) \to \mathscr{P}(\mathrm{G})$ eine Galoisverbindung definieren.

$$\begin{aligned}
& \mathrm{L}(\mathrm{A}) \supseteq \mathrm{B} \\
\iff & \quad \{\ \text{Definition der Teilmenge}\ \} \\
& \forall b \in \mathrm{B} \;.\; b \in \mathrm{L}(\mathrm{A}) \\
\iff & \quad \{\ \text{Definition von L(A)}\ \} \\
& \forall b \in \mathrm{B} \;.\; \forall a \in \mathrm{A} \;.\; (a,b) \in \mathrm{T} \\
\iff & \quad \{\ \text{Logik}\ \} \\
& \forall a \in \mathrm{A} \;.\; \forall b \in \mathrm{B} \;.\; (a,b) \in \mathrm{T} \\
\iff & \quad \{\ \text{Definition von R(B)}\ \} \\
& \forall a \in \mathrm{A} \;.\; a \in \mathrm{R}(\mathrm{B}) \\
\iff & \quad \{\ \text{Definition der Teilmenge}\ \} \\
& \mathrm{A} \subseteq \mathrm{R}(\mathrm{B})
\end{aligned}$$

Die in der Rechnung auftretenden Formeln haben eine ansprechende »geometrische« Interpretation: Ordnen wir die Reihen und Spalten der Tabelle T so um, dass alle Gegenstände aus A benachbart sind und alle Merkmale aus B benachbart sind, dann entspricht die Formel $\forall a \in \mathrm{A} \;.\; \forall b \in \mathrm{B} \;.\; (a,b) \in \mathrm{T}$ einem vollständig »gefüllten«, rechteckigen Tabellenausschnitt. Ein *Konzept* (A,B) mit $\mathrm{L}(\mathrm{A}) = \mathrm{B}$ und $\mathrm{A} = \mathrm{R}(\mathrm{B})$ entspricht dabei einem *maximalen* Rechteck. Die Komponenten eines Konzepts sind Fixpunkte: A ist ein Fixpunkt von $\mathrm{R} \circ \mathrm{L}$ und B ist ein Fixpunkt von $\mathrm{L} \circ \mathrm{R}$. Wir wissen bereits, dass die Fixpunkte von $\mathrm{R} \circ \mathrm{L}$ bzw. $\mathrm{L} \circ \mathrm{R}$ jeweils einen vollständigen Verband bilden; aufgrund der Korrespondenz von L und R erhalten wir in beiden Fällen den identischen Verband, den sogenannten ***Begriffsverband*** von T.

Logik: *Negation, Konjunktion, Disjunktion*

$$(\neg a) \Rightarrow b \iff a \Leftarrow (\neg b) \qquad (\mathbb{B}, \Rightarrow) \underset{\neg}{\overset{\neg}{\underset{\bot}{\leftarrow}}} (\mathbb{B}, \Leftarrow)$$

$$(a \wedge p) \Rightarrow b \iff a \Rightarrow (b \Leftarrow p) \qquad (\mathbb{B}, \Rightarrow) \underset{(\text{-}) \Leftarrow p}{\overset{(\text{-}) \wedge p}{\underset{\bot}{\leftarrow}}} (\mathbb{B}, \Rightarrow)$$

$$(a \not\Rightarrow q) \Rightarrow b \iff a \Rightarrow (b \vee q) \qquad (\mathbb{B}, \Rightarrow) \underset{(\text{-}) \vee q}{\overset{(\text{-}) \not\Rightarrow q}{\underset{\bot}{\leftarrow}}} (\mathbb{B}, \Rightarrow)$$

Mengenlehre: *Durchschnitt, Vereinigung, relatives Komplement*

$$\mathrm{A} \cap \mathrm{P} \subseteq \mathrm{B} \iff \mathrm{A} \subseteq \mathrm{B} \Leftarrow \mathrm{P} \qquad (\mathscr{P}(\mathrm{A}), \subseteq) \underset{(\text{-}) \Leftarrow \mathrm{P}}{\overset{(\text{-}) \cap \mathrm{P}}{\underset{\bot}{\leftarrow}}} (\mathscr{P}(\mathrm{A}), \subseteq)$$

$$\mathrm{A} - \mathrm{Q} \subseteq \mathrm{B} \iff \mathrm{A} \subseteq \mathrm{B} \cup \mathrm{Q} \qquad (\mathscr{P}(\mathrm{A}), \subseteq) \underset{(\text{-}) \cup \mathrm{Q}}{\overset{(\text{-}) - \mathrm{Q}}{\underset{\bot}{\leftarrow}}} (\mathscr{P}(\mathrm{A}), \subseteq)$$

$$\mathrm{S} - \mathrm{A} \subseteq \mathrm{B} \iff \mathrm{A} \supseteq \mathrm{S} - \mathrm{B} \qquad (\mathscr{P}(\mathrm{A}), \subseteq) \underset{\mathrm{S} - (\text{-})}{\overset{\mathrm{S} - (\text{-})}{\underset{\bot}{\leftarrow}}} (\mathscr{P}(\mathrm{A}), \supseteq)$$

Verbandstheorie: *Supremum, Infimum*

$$\bigsqcup f \leqslant b \iff f \leqslant \Delta(b) \qquad (\mathrm{P}, \leqslant) \underset{\Delta}{\overset{\bigsqcup}{\underset{\bot}{\leftarrow}}} (\mathrm{P}^{\mathrm{X}}, \leqslant) \underset{\bigsqcup}{\overset{\Delta}{\underset{\bot}{\leftarrow}}} (\mathrm{P}, \leqslant) \quad \Delta(a) \leqslant g \iff a \leqslant \bigsqcap g$$

Arithmetik: *natürliche Subtraktion, ganzzahlige Division ($p > 0$), Boden, Decke*

$$a \dot{-} p \leqslant b \iff a \leqslant b + p \qquad (\mathbb{N}, \leqslant) \underset{(\text{-}) + p}{\overset{(\text{-}) \dot{-} p}{\underset{\bot}{\leftarrow}}} (\mathbb{N}, \leqslant)$$

$$a \cdot p \leqslant b \iff a \leqslant b \mathbin{\underline{\boldsymbol{div}}} p \qquad (\mathbb{Z}, \leqslant) \underset{(\text{-}) \mathbin{\underline{\boldsymbol{div}}} p}{\overset{(\text{-}) \cdot p}{\underset{\bot}{\leftarrow}}} (\mathbb{Z}, \leqslant) \underset{(\text{-}) \cdot p}{\overset{a \mathbin{\overline{\boldsymbol{div}}} p}{\underset{\bot}{\leftarrow}}} (\mathbb{Z}, \leqslant) \quad a \mathbin{\overline{\boldsymbol{div}}} p \leqslant b \iff a \leqslant b \cdot p$$

$$\lceil x \rceil \leqslant n \iff x \sqsubseteq \iota(n) \qquad (\mathbb{Z}, \leqslant) \underset{\iota}{\overset{\lceil \text{-} \rceil}{\underset{\bot}{\leftarrow}}} (\mathbb{R}, \leqslant) \underset{\lfloor \text{-} \rfloor}{\overset{\iota}{\underset{\bot}{\leftarrow}}} (\mathbb{Z}, \leqslant) \quad \iota(n) \sqsubseteq x \iff n \leqslant \lfloor x \rfloor$$

Die Funktion $\iota : \mathbb{Z} \to \mathbb{R}$ bettet die ganzen Zahlen in die reellen Zahlen ein.

Abbildung B.19.: Ein Potpourri von Galoisverbindungen.

Übungen.

8. Wie jedes gute mathematische Konzept lassen sich auch Galoisverbindungen auf verschiedene Weisen einführen. Eine alternative Definition fordert, dass ℓ und r monoton sind und die Vereinfachungsregeln (B.122a)–(B.122b) erfüllen.

9. Zeigen Sie $a \Rightarrow (p \Leftarrow b) \iff (p \Leftarrow a) \Leftarrow b$. Induzierte antitone GV.

10. $A \cap B = B - (B - A)$. Interpretation mit GV? Via Komplement?

11. Zeigen Sie, dass das kartesische Produkt von Verbänden ein Verband ist und dass dieser Verband Extremelemente besitzt, sofern die einzelnen Verbände welche besitzen. *Hinweis:* .

12. Zeigen Sie die folgenden Verallgemeinerungen der indirekten Beweise (B.15c)–(B.15d). (Die Aussagen sind in informierten Kreisen auch unter dem Namen ***Yoneda-Lemma*** bekannt.) Für monotone Funktionen f und g gilt:

$$f(a) \leqslant b \quad \iff \quad \forall\, x \in P \;.\; x \leqslant a \Longrightarrow f(x) \leqslant b \tag{B.128a}$$
$$a \leqslant g(b) \quad \iff \quad \forall\, x \in P \;.\; a \leqslant g(x) \Longleftarrow b \leqslant x \tag{B.128b}$$

13. Zeigen Sie, dass jede Galoisverbindung $\ell \dashv r$ zwei Galoisverbindungen zwischen Funktionen induziert.

$$\ell \circ - \dashv r \circ - \qquad\qquad - \circ r \dashv - \circ \ell$$

Hinweis: Verwenden Sie für den Nachweis von $- \circ r \dashv - \circ \ell$ die Beweistechniken aus Aufgabe B.6.12.

14. Sei P eine totale Ordnung mit Extremelementen. Zeigen Sie, dass $- \downarrow p$ linksadjunkt und $- \uparrow p$ rechtsadjunkt ist.

15. Finden Sie möglichst kleine Verbände, in denen $- \sqcap p$ *nicht* linksadjunkt und $- \sqcup p$ *nicht* rechtsadjunkt ist.

B.6.6. Quantale⋆⋆

Die Algebra der Quantale ist die Algebra der Sprachen, Mengen von Wörtern über einem Alphabet: $\mathcal{P}(\mathbb{A}^*)$. Quantale basieren im Vergleich zu Kleene Algebren auf einem stärkeren Axiomensystem — stärker und in gewisser Hinsicht eleganter. Im direkten Vergleich: Eine Kleene Algebra verbindet einen Halbverband mit einem Monoid. Ein Quantal verbindet einen *vollständigen* Halbverband mit einem Monoid. (Zur Erinnerung: Ein vollständiger Halbverband ist sogar ein vollständiger *Verband* — ein Quantal verbindet also de facto einen vollständigen Verband mit einem Monoid.) Kleene Algebren regeln die Interaktion zwischen dem Halbverband und dem Monoid mit Distributivgesetzen. Quantale legen die Schnittstelle durch zwei parametrisierte Galoisverbindungen fest. Im Einzelnen:

Ein ***Quantal*** besteht aus einem *vollständigen* Halbverband $(Q, \leqslant, \bigsqcup)$ und einem Monoid $(Q, 1, \cdot)$ über der gleichen Grundmenge Q. Wir verlangen, dass die Multiplikation von links und die Multiplikation von rechts Quasiinverse besitzen:

$$p \cdot a \leqslant b \quad \iff \quad a \leqslant p \setminus b \tag{B.129a}$$
$$a \cdot q \leqslant b \quad \iff \quad a \leqslant b \,/\, q \tag{B.129b}$$

Mit anderen Worten, die Multiplikationsoperationen $p \cdot -$ und $- \cdot q$ sind Linksadjunkte: $p \cdot - \dashv p \setminus -$ und $- \cdot q \dashv - \,/\, q$. Ihre Rechtsadjunkte werden als Divisionsoperationen geschrieben; die Neigung der Symbole »\« und »/« deutet Dividend und Divisor an — wir teilen den Dividenden b durch

den Divisor p bzw. q. Der »Bruch« $p \setminus b$ heißt auch ***Rechtsfaktor*** von b und b / q entsprechend ***Linksfaktor***.

Aus der Theorie der Galoisverbindungen folgt, dass die Multiplikation in beiden Argumenten monoton ist, während die Divisionsoperationen monoton im Dividenden und antiton im Divisor sind.

$$\begin{aligned} a_1 \leqslant a_2 \;\wedge\; b_1 \leqslant b_2 &\implies a_1 \cdot b_1 \leqslant a_2 \cdot b_2 \\ a_1 \geqslant a_2 \;\wedge\; b_1 \leqslant b_2 &\implies a_1 \setminus b_1 \leqslant a_2 \setminus b_2 \\ a_1 \leqslant a_2 \;\wedge\; b_1 \geqslant b_2 &\implies a_1 / b_1 \leqslant a_2 / b_2 \end{aligned}$$

Da $p \cdot \text{-}$ und $\text{-} \cdot q$ Suprema erhalten, gelten Verallgemeinerungen der Distributivgesetze.

$$p \cdot \left(\bigsqcup_{i \in I} a_i \right) = \bigsqcup_{i \in I} p \cdot a_i \qquad p \setminus \left(\bigsqcap_{i \in I} a_i \right) = \bigsqcap_{i \in I} p \setminus a_i \tag{B.130a}$$

$$\left(\bigsqcup_{i \in I} a_i \right) \cdot q = \bigsqcup_{i \in I} a_i \cdot q \qquad \left(\bigsqcap_{i \in I} a_i \right) / q = \bigsqcap_{i \in I} a_i / q \tag{B.130b}$$

Die Multiplikation distribuiert über beliebige Vereinigungen. Die Rechtsadjunkten erhalten Infima und distribuieren entsprechend über beliebige Durchschnitte. Damit ist jedes Quantal ein idempotenter Halbring.

Aus den beiden parametrisierten Galoisverbindungen (B.129a)–(B.129b) lässt sich eine weitere Verbindung ableiten, indem man die Rolle von Argument und Parameter vertauscht. Da die Divisionsoperationen antiton im Divisor sind, erhalten wir notwendigerweise eine antitone Galoisverbindung.

$$a \setminus s \geqslant b \iff a \leqslant s / b \tag{B.131}$$

Der Beweis nutzt aus, dass das Produkt in $a \cdot b \leqslant s$ entweder mittels Division von links oder mittels Division von rechts umgeschrieben werden kann.

$$\begin{aligned} & a \setminus s \geqslant b \\ \iff & \quad \{ \text{ duale Ordnung } \} \\ & b \leqslant a \setminus s \\ \iff & \quad \{ \; p \cdot \text{-} \vdash p \setminus \text{-} \text{ (B.129a) } \} \\ & a \cdot b \leqslant s \\ \iff & \quad \{ \; \text{-} \cdot q \dashv \text{-} / q \text{ (B.129b) } \} \\ & a \leqslant s / b \end{aligned}$$

Auch für die induzierte Galoisverbindung gelten die Erhaltungsgesetze (B.125a)–(B.125b); aufgrund der Antitonie werden allerdings Suprema auf Infima abgebildet: $\bot \setminus s = \top$ und $(a_1 \sqcup a_2) \setminus s = (a_1 \setminus s) \sqcap (a_2 \setminus s)$. Wenn die Multiplikation kommutativ ist, dann sind die beiden Rechtsadjunkten identisch, $a \setminus b = b / a$, und somit selbstadjunkt.

Unsere laufenden Beispiele, die Erreichbarkeits- und die Kostenalgebra, erfüllen auch die Anforderungen an Quantale.

Erreichbarkeitsalgebra	$(\mathbb{B}, \Rightarrow, \exists, \mathit{true}, \wedge)$
Kostenalgebra	$(\mathbb{N} \cup \{\infty\}, \geqslant, \min, 0, +)$

Die Wahrheitswerte mittels Implikation angeordnet bilden einen endlichen und damit vollständigen Verband, wobei das Supremum durch den Existenzquantor gegeben ist. Die Konjunktion ist

linksadjunkt, $p \wedge \text{-} \dashv p \Rightarrow \text{-}$ und $\text{-} \wedge p \dashv \text{-} \Leftarrow p$; da sie kommutativ ist, fallen ihre Rechtsadjunkte zusammen: $a \Rightarrow b = b \Leftarrow a$.

Die natürlichen Zahlen mittels $\geqslant$ angeordnet bilden lediglich einen Verband. (*Beachte:* Wir betrachten die duale Ordnung!) Jede *nichtleere* Menge besitzt ein Infimum, das kleinste Element der Menge. Nur die leere Menge hat keine größte untere Schranke, da $\mathbb{N}$ kein größtes Element besitzt. Dieser »Defekt« lässt sich reparieren, indem ein größtes Element, notiert durch ∞, adjungiert wird, so dass $\min \emptyset = \infty$. Auf den natürlichen Zahlen ist $\text{-} + p$ rechtsadjunkt mit Monus als Gegenspieler. Wie lassen sich die Addition und die natürliche Subtraktion auf $\mathbb{N} \cup \{\infty\}$ fortsetzen? Glücklicherweise müssen wir keine große Phantasie entwickeln — alle Definitionen folgen zwangsläufig aus den Anforderungen: Die Erhaltungsgesetze diktieren, dass $\infty + n = \infty = n + \infty$ und $n \dot{-} \infty = 0$ für alle $n \in \mathbb{N} \cup \{\infty\}$. Weiterhin muss $\infty \dot{-} n = \infty$ für alle $n \in \mathbb{N}$ gelten. (Warum?)

$+$	$b \in \mathbb{Z}$	∞
∞	∞	∞
$a \in \mathbb{Z}$	$a + b$	∞

$\dot{-}$	$b \in \mathbb{Z}$	∞
∞	∞	0
$a \in \mathbb{Z}$	$a - b$	0

Rechnen mit »Brüchen« Die Notation für Rechts- und Linksfaktoren ist bewusst suggestiv gewählt: Mit Faktoren lässt sich so ähnlich rechnen wie mit rationalen Zahlen. Zunächst einmal erhalten wir die folgenden ***Kürzungsregeln*** als Spezialisierung der Vereinfachungsregeln (B.122a)–(B.122b).

$$a \leqslant p \setminus (p \cdot a) \qquad a \leqslant (a \cdot q) / q \tag{B.132a}$$

$$p \cdot (p \setminus b) \leqslant b \qquad (b / q) \cdot q \leqslant b \tag{B.132b}$$

Ähnlich wie im Fall der ganzzahligen Division gelten im Allgemeinen nur Ungleichungen, keine Gleichungen. Zum Beispiel ist $p \setminus p$ in der Regel nicht 1 und $(p \setminus q) \cdot (q \setminus r)$ ist nicht gleich $p \setminus r$. Vielmehr gelten die folgenden, schwächeren Kürzungsregeln, die sich aus den obigen Formeln ableiten.

(»reflexiv«) $\qquad 1 \leqslant p \setminus p \qquad 1 \leqslant q / q$ (B.132c)

(»transitiv«) $\qquad (p \setminus q) \cdot (q \setminus r) \leqslant p \setminus r \qquad (p / q) \cdot (q / r) \leqslant p / r$ (B.132d)

Wir beschränken uns auf den Nachweis der Eigenschaften für Rechtsfaktoren; symmetrische Beweise zeigen die entsprechenden Aussagen für Linksfaktoren.

$$\begin{aligned} & 1 \leqslant p \setminus p \\ \iff & \quad \{\ p \cdot \text{-} \vdash p \setminus \text{-}\ \text{(B.129a)}\ \} \\ & p \cdot 1 \leqslant p \end{aligned} \qquad\qquad \begin{aligned} & (p \setminus q) \cdot (q \setminus r) \leqslant p \setminus r \\ \iff & \quad \{\ p \cdot \text{-} \vdash p \setminus \text{-}\ \text{(B.129a)}\ \} \\ & p \cdot (p \setminus q) \cdot (q \setminus r) \leqslant r \end{aligned}$$

Die beiden Ungleichungen folgen aus den Monoideigenschaften und der Kürzungsregel (B.132b), die doppelt zum Einsatz kommt: $p \cdot (p \setminus q) \cdot (q \setminus r) \leqslant q \cdot (q \setminus r) \leqslant r$.

Vertrauter sind vielleicht die folgenden Regeln, die ebenfalls aus den Monoideigenschaften abgeleitet werden.

$$1 \setminus b = b \qquad b / 1 = b \tag{B.133a}$$

$$(p_1 \cdot p_2) \setminus b = p_2 \setminus (p_1 \setminus b) \qquad b / (q_1 \cdot q_2) = (b / q_2) / q_1 \tag{B.133b}$$

Etwas Vorsicht ist aber geboten: Da die Multiplikation in der Regeln nicht kommutativ ist, spielt die Reihenfolge der Divisionen eine Rolle: Wir teilen erst durch p_1 und dann durch p_2 bzw. erst durch q_2 und dann durch q_1. Der Beweis auf der rechten Seite verdeutlicht, warum sich die Reihenfolge der Divisoren vertauscht.

$$
\begin{aligned}
& x \leqslant 1 \setminus b \\
\iff & \quad \{\ p \cdot \text{-} \vdash p \setminus \text{-}\ \text{(B.129a)}\ \} \\
& 1 \cdot x \leqslant b \\
\iff & \quad \{\ \text{Monoid: 1 neutral}\ \} \\
& x \leqslant b
\end{aligned}
\qquad\qquad
\begin{aligned}
& x \leqslant (p_1 \cdot p_2) \setminus b \\
\iff & \quad \{\ p \cdot \text{-} \vdash p \setminus \text{-}\ \text{(B.129a)}\ \} \\
& (p_1 \cdot p_2) \cdot x \leqslant b \\
\iff & \quad \{\ \text{Monoid: »·« assoziativ}\ \} \\
& p_1 \cdot (p_2 \cdot x) \leqslant b \\
\iff & \quad \{\ p \cdot \text{-} \vdash p \setminus \text{-}\ \text{(B.129a)}\ \} \\
& p_2 \cdot x \leqslant p_1 \setminus b \\
\iff & \quad \{\ p \cdot \text{-} \vdash p \setminus \text{-}\ \text{(B.129a)}\ \} \\
& x \leqslant p_2 \setminus (p_1 \setminus b)
\end{aligned}
$$

Wenn wir nacheinander erst p_1 und dann p_2 auf die andere Seite transferieren, vertauscht sich ähnlich wie beim Rangieren von Zugwagons die Reihenfolge.

Sternoperator Da Quantale auf vollständigen Verbänden basieren, besitzen alle monotonen Funktionen über einem Quantal einen kleinsten Präfixpunkt. Das können wir ausnutzen, um den Sternoperator zu definieren und zu zeigen, dass jedes Quantal eine Kleene Algebra ist. Bei der Formalisierung haben wir die Qual der Wahl: a^* kann unter anderem als kleinster Präfixpunkt der folgenden drei Funktionen definiert werden.

$$f(x) \coloneqq a \cdot x \sqcup 1 \qquad h(x) \coloneqq 1 \sqcup a \sqcup x \cdot x \qquad g(x) \coloneqq 1 \sqcup x \cdot a$$

Wir wählen die symmetrische Variante in der Mitte und definieren $a^* \coloneqq \mu h$. Wir müssen jetzt zeigen, dass die vier Axiome für den Sternoperator erfüllt sind: (B.107a), (B.108a), (B.111a) und (B.111b).

Zunächst einmal ist jeder Präfixpunkt von h auch ein Präfixpunkt von f und g.

$$f(x) \leqslant x \quad \Longleftarrow \quad h(x) \leqslant x \quad \Longrightarrow \quad g(x) \leqslant x$$

Da insbesondere a^* ein Präfixpunkt von h ist (B.105a), gilt sowohl $f(a^*) \leqslant a^*$ (B.107a) als auch $g(a^*) \leqslant a^*$ (B.108a).

Die Invariantenaxiome (B.111b) und (B.111a) lassen sich mit Hilfe der Galoisverbindungen umschreiben: $x \cdot i \leqslant i$ wird zu $x \leqslant i \,/\, i$ und aus $i \cdot x \leqslant i$ wird $x \leqslant i \setminus i$.

$$
\begin{aligned}
a^* &\leqslant i \setminus i \quad \Longleftarrow \quad a \leqslant i \setminus i \\
a^* &\leqslant i \,/\, i \quad \Longleftarrow \quad a \leqslant i \,/\, i
\end{aligned}
$$

So umformuliert lassen sich die Invariantenaxiome mit Hilfe der »normalen« Fixpunkt-Induktion nachweisen.

$$
\begin{aligned}
& a^* \leqslant i \setminus i \\
\Longleftarrow \quad & \{\ \text{Fixpunkt-Induktion (B.105b)}\ \} \\
& 1 \sqcup a \sqcup (i \setminus i) \cdot (i \setminus i) \leqslant i \setminus i \\
\iff \quad & \{\ \text{Supremum (B.18)}\ \} \\
& 1 \leqslant i \setminus i \ \wedge \ a \leqslant i \setminus i \ \wedge \ (i \setminus i) \cdot (i \setminus i) \leqslant i \setminus i \\
\iff \quad & \{\ \text{Kürzungsregeln (B.132c) und (B.132d)}\ \} \\
& a \leqslant i \setminus i
\end{aligned}
$$

Ein analoger Beweis zeigt das andere Axiom. In die Beweise fließt im Wesentlichen ein, dass $i \setminus i$ und $i \,/\, i$ »reflexiv« und »transitiv« sind. Es folgt weiterhin, dass $\mu f = \mu h = \mu g$. (Warum?) Kleene

Algebren *postulieren* die Gleichheit dieser Präfixpunkte; mit dem Axiomensystem von Quantalen können wir die Gleichheit *schlussfolgern*. Quantale sind flexibler in der Handhabung von Produkten: $a \cdot b \leqslant x$ lässt sich zu $b \leqslant a \setminus x$ oder $a \leqslant x / b$ umformen — einzelne Faktoren lassen sich auf diese Weise isolieren und weiteren Manipulationen zugänglich machen. Kleene Algebren müssen hingegen den Sternoperator *im Kontext* eines Produkts axiomatisieren.

Da Quantale auf vollständigen Verbänden basieren, lässt sich der Sternoperator alternativ als kleinste obere Schranke aller endlichen Potenzen definieren.

$$a^* := \bigsqcup_{n\in\mathbb{N}} a^n \qquad a^0 := 1 \qquad a \cdot a^n =: a^{n+1} := a^n \cdot a$$

Um die Äquivalenz der Definitionen nachzuweisen, zeigen wir, dass a^* der kleinste Präfixpunkt von $f(x) = a \cdot x \sqcup 1$ ist. Zunächst einmal ist a^* ein Präfixpunkt:

$$\begin{aligned}
& 1 \sqcup a \cdot \bigsqcup_{n\in\mathbb{N}} a^n \leqslant a^* \\
\iff & \quad \{\ a \cdot \text{- erhält Suprema (B.130a)}\ \} \\
& 1 \sqcup \bigsqcup_{n\in\mathbb{N}} a \cdot a^n \leqslant a^* \\
\iff & \quad \{\ \text{Definition von } a^0 \text{ und } a^{n+1}\ \} \\
& a^0 \sqcup \bigsqcup_{n\in\mathbb{N}} a^{n+1} \leqslant a^* \\
\iff & \quad \{\ \text{Supremum (B.18)}\ \} \\
& a^0 \leqslant a^* \ \wedge\ \forall\, n \in \mathbb{N} \,.\, a^{n+1} \leqslant a^*
\end{aligned}$$

Die resultierenden Ungleichungen folgen direkt aus den Eigenschaften der oberen Schranke (B.24a). Weiterhin erfüllt a^* das Prinzip der Fixpunkt-Induktion (B.107b): Wir setzen $1 \sqcup a \cdot x \leqslant x$, das heißt $1 \leqslant x$ und $a \cdot x \leqslant x$, voraus und zeigen $a^* \leqslant x$.

$$\begin{aligned}
& a^* \leqslant x \\
\iff & \quad \{\ \text{Supremum (B.18)}\ \} \\
& \forall n \in \mathbb{N} \ .\ a^n \leqslant x
\end{aligned}$$

Dass x alle endlichen Potenzen dominiert, zeigt ein Induktionsbeweis.

$$\begin{aligned}
& a^0 \\
= & \quad \{\ \text{Definition } a^0\ \} \\
& 1 \\
\leqslant & \quad \{\ \text{Voraussetzung: } 1 \leqslant x\ \} \\
& x
\end{aligned}$$

$$\begin{aligned}
& a^{n+1} \\
= & \quad \{\ \text{Definition } a^{n+1}\ \} \\
& a \cdot a^n \\
\leqslant & \quad \{\ \text{Induktionsannahme}\ \} \\
& a \cdot x \\
\leqslant & \quad \{\ \text{Voraussetzung: } a \cdot x \leqslant x\ \} \\
& x
\end{aligned}$$

Beispiel: Potenzmengenmonoide In Abschnitt B.6.2 haben wir gezeigt, dass $(\mathcal{P}(\mathrm{M}), \varnothing, \cup, 1, \cdot)$ einen idempotenten Halbring bildet, sofern $(\mathrm{M}, 1, \cdot)$ ein Monoid ist. Da Potenzmengenverbände vollständig sind, ist die Hoffnung begründet, dass die Konstruktion tatsächlich ein Quantal hervorbringt. Dazu müssen wir zeigen, dass die Multiplikation von links und die Multiplikation von rechts Quasiinverse besitzen. Wir leiten die Definition des Rechtsfaktors her; eine analoge

Rechnung bestimmt die Definition des Linksfaktors.

$$
\begin{aligned}
& P \cdot A \subseteq B \\
\iff & \quad \{ \text{ Definition Teilmenge } \} \\
& \forall\, w \;.\; w \in P \cdot A \implies w \in B \\
\iff & \quad \{ \text{ Definition Konkatenation (B.102b) } \} \\
& \forall\, w \;.\; (\exists\, p \in P \;.\; \exists\, a \in A \;.\; w = p \cdot a) \implies w \in B \\
\iff & \quad \{ \text{ Logik } \} \\
& \forall\, w \;.\; \forall\, p \in P \;.\; \forall\, a \in A \;.\; w = p \cdot a \implies w \in B \\
\iff & \quad \{ \text{ Logik } \} \\
& \forall\, a \;.\; a \in A \implies \forall\, p \;.\; p \in P \implies p \cdot a \in B \\
\iff & \quad \{ \text{ definiere } P \setminus B := \{\, a \mid \forall\, p \;.\; p \in P \implies p \cdot a \in B \,\} \,\} \\
& \forall\, a \;.\; a \in A \implies a \in P \setminus B \\
\iff & \quad \{ \text{ Definition Teilmenge } \} \\
& A \subseteq P \setminus B
\end{aligned}
$$

Damit erhalten wir die folgenden Definitionen.

$$P \setminus B := \{\, x \mid \forall\, p \in P \;.\; p \cdot x \in B \,\} \qquad\qquad B \,/\, Q := \{\, x \mid \forall\, q \in Q \;.\; x \cdot q \in B \,\}$$

Die Formeln verallgemeinern die Definitionen aus Kapitel 6, die den Divisor auf *einelementige* Mengen einschränken. Spezialisieren wir die obigen Formeln für diesen wichtigen Spezialfall, $\{p\} \setminus L =: p \setminus L$ und $B \,/\, \{q\} =: B \,/\, q$, erhalten wir ebendiese Definitionen.

$$p \setminus B = \{\, x \mid p \cdot x \in B \,\} \qquad\qquad B \,/\, q = \{\, x \mid x \cdot q \in B \,\}$$

Als Rechtsadjunkte erhalten die Divisionen beliebige Durchschnitte (B.130a)–(B.130b); die Spezialfälle verhalten sich noch wesentlich disziplinierter: $p \setminus$ - und - $/\, q$ erhalten sowohl Vereinigung, Durchschnitt als auch Differenz.

$$p \setminus (B_1 \cup B_2) = (p \setminus B_1) \cup (p \setminus B_2) \qquad (B_1 \cup B_2) \,/\, q = (B_1 \,/\, q) \cup (B_2 \,/\, q) \tag{B.134a}$$

$$p \setminus (B_1 \cap B_2) = (p \setminus B_1) \cap (p \setminus B_2) \qquad (B_1 \cap B_2) \,/\, q = (B_1 \,/\, q) \cap (B_2 \,/\, q) \tag{B.134b}$$

$$p \setminus (B_1 - B_2) = (p \setminus B_1) - (p \setminus B_2) \qquad (B_1 - B_2) \,/\, q = (B_1 \,/\, q) - (B_2 \,/\, q) \tag{B.134c}$$

Wir zeigen exemplarisch die vorletzte Aussage. Der Nachweis wird »elementweise« geführt: Zwei Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten, $A = B \iff (\forall\, x \;.\; x \in A \iff x \in B)$. Als vorbereitenden Schritt schreiben wir die Definition von $p \setminus B$ als Äquivalenz.

$$x \in p \setminus B \quad \iff \quad p \cdot x \in B \tag{B.135}$$

Jetzt nimmt der Beweis seinen überraschungsfreien Verlauf.

$$
\begin{aligned}
& x \in p \setminus (B_1 - B_2) \\
\iff & \quad \{ \text{ (B.135) } \} \\
& p \cdot x \in B_1 - B_2 \\
\iff & \quad \{ \text{ Definition Mengendifferenz } \} \\
& p \cdot x \in B_1 \;\wedge\; \neg\, (p \cdot x \in B_2) \\
\iff & \quad \{ \text{ (B.135) } \} \\
& x \in p \setminus B_1 \;\wedge\; \neg\, (x \in p \setminus B_2) \\
\iff & \quad \{ \text{ Definition Mengendifferenz } \} \\
& x \in (p \setminus B_1) - (p \setminus B_2)
\end{aligned}
$$

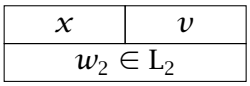
Da die Mengenmitgliedschaft $x \in$ - die Struktur Boolescher Verbände erhält, folgen die anderen Beweise dem exakt gleichen Muster.

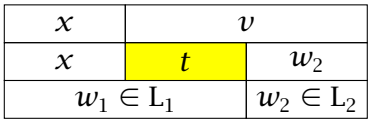
Spezialfall: Sprachen Jetzt haben wir fast alle Formeln beisammen, um die Rechts- bzw. Linksfaktoren eines regulären Ausdrucks zu bestimmen, siehe Abschnitt 6.2.1. Zwei Fälle fehlen noch: Konkatenation und Wiederholung. Die Formeln aus Abschnitt 6.2.1 sind im Allgemeinen nur gültig, wenn wir uns auf Sprachen beschränken, $\mathscr{P}(\mathbb{A}^*)$, das heißt, wenn das zugrundeliegende Monoid des Potenzmengenmonoids ***frei*** ist, $\mathbb{A}^*$.

Im Folgenden ist x ein einzelnes Symbol: $x \in \mathbb{A}$. Wir leiten zunächst die Formel für die Konkatenation her.

$$
\begin{array}{ll}
 & v \in x \setminus (\mathrm{L}_1 \cdot \mathrm{L}_2) \\
\iff & \quad \{ \text{(B.135)} \} \\
 & x \cdot v \in \mathrm{L}_1 \cdot \mathrm{L}_2 \\
\iff & \quad \{ \text{Definition Komposition (B.102b)} \} \\
 & \exists w_1 \;.\; \exists w_2 \;.\; w_1 \in \mathrm{L}_1 \;\wedge\; w_2 \in \mathrm{L}_2 \;\wedge\; x \cdot v = w_1 \cdot w_2
\end{array}
$$

An dieser Stelle nutzen wir aus, dass die Elemente des Monoids Listen sind und nehmen eine Fallunterscheidung über w_1 vor: Entweder w_1 ist leer oder fängt mit dem Buchstaben x an. Die folgende Graphik illustriert die jeweiligen Aufteilungen (t wie »tail«).





Damit lässt sich die Rechnung fortsetzen.

$$
\begin{array}{ll}
\iff & \quad \{ \text{freies Monoid} \} \\
 & (\varepsilon \in \mathrm{L}_1 \;\wedge\; x \cdot v \in \mathrm{L}_2) \quad \vee \quad (\exists t \;.\; \exists w_2 \;.\; x \cdot t \in \mathrm{L}_1 \;\wedge\; w_2 \in \mathrm{L}_2 \;\wedge\; v = t \cdot w_2) \\
\iff & \quad \{ \text{(B.135)} \} \\
 & (\varepsilon \in \mathrm{L}_1 \;\wedge\; v \in x \setminus \mathrm{L}_2) \quad \vee \quad (\exists t \;.\; \exists w_2 \;.\; t \in x \setminus \mathrm{L}_1 \;\wedge\; w_2 \in \mathrm{L}_2 \;\wedge\; v = t \cdot w_2) \\
\iff & \quad \{ \text{Definition Komposition (B.102b)} \} \\
 & (\varepsilon \in \mathrm{L}_1 \;\wedge\; v \in x \setminus \mathrm{L}_2) \quad \vee \quad v \in (x \setminus \mathrm{L}_1) \cdot \mathrm{L}_2 \\
\iff & \quad \{ \text{Iverson Klammer} \} \\
 & v \in [\varepsilon \in \mathrm{L}_1] \cdot (x \setminus \mathrm{L}_2) \quad \vee \quad v \in (x \setminus \mathrm{L}_1) \cdot \mathrm{L}_2 \\
\iff & \quad \{ \text{Definition Mengenvereinigung} \} \\
 & v \in [\varepsilon \in \mathrm{L}_1] \cdot (x \setminus \mathrm{L}_2) \cup (x \setminus \mathrm{L}_1) \cdot \mathrm{L}_2
\end{array}
$$

Um eine explizite Fallunterscheidung zu vermeiden, machen wir Gebrauch von der Iverson Klammer, verallgemeinert auf Halbringe: $[\mathit{false}] = 0 = \varnothing$ und $[\mathit{true}] = 1 = \{\varepsilon\}$.

Kommen wir zum großen Finale, der Formel für die Wiederholung. Im Wesentlichen führen wir die Wiederholung auf die Konkatenation zurück. Um uns das Leben dabei so einfach wie möglich zu machen, bedienen wir uns eines kleinen Tricks: Wir zeigen die Aussage zunächst für den Fall, dass L ε-frei ist (linke Spalte), und führen dann den allgemeinen Fall auf den Spezialfall zurück (rechte Spalte).

$$
\begin{aligned}
x \setminus a &= [a = x] & [\mathit{false}] &:= \varnothing \\
x \setminus \varepsilon &= \varnothing & [\mathit{true}] &:= \varepsilon \\
x \setminus (L_1 \cdot L_2) &= (x \setminus L_1) \cdot L_2 \cup [\varepsilon \in L_1] \cdot (x \setminus L_2) \\
x \setminus \varnothing &= \varnothing \\
x \setminus (L_1 \cup L_2) &= (x \setminus L_1) \cup (x \setminus L_2) \\
x \setminus \mathbb{A}^* &= \mathbb{A}^* \\
x \setminus (L_1 \cap L_2) &= (x \setminus L_1) \cap (x \setminus L_2) \\
x \setminus (L_1 - L_2) &= (x \setminus L_1) - (x \setminus L_2) \\
x \setminus L^* &= (x \setminus L) \cdot L^*
\end{aligned}
$$

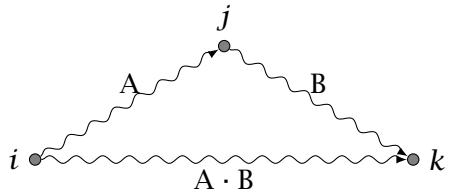
Abbildung B.20.: Eigenschaften der Rechtsfaktors $x \setminus L$ mit $x \in \mathbb{A}$ und $L \subseteq \mathcal{P}(\mathbb{A}^*)$.

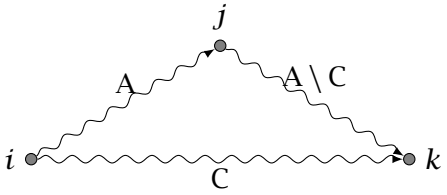
$$
\begin{aligned}
& x \setminus L^* \\
= & \quad \{ \text{ Fixpunkt: } A^* = \varepsilon \cup A \cdot A^* \ \} \\
& x \setminus (\varepsilon \cup L \cdot L^*) \\
= & \quad \{ \text{ Vereinigung (B.134a) } \} \\
& x \setminus \varepsilon \cup x \setminus (L \cdot L^*) \\
= & \quad \{ \text{ Regel für } \varepsilon \ \} \\
& x \setminus (L \cdot L^*) \\
= & \quad \{ \text{ Annahme } \varepsilon \notin L \ \} \\
& (x \setminus L) \cdot L^*
\end{aligned}
\qquad
\begin{aligned}
& x \setminus L^* \\
= & \quad \{ \text{ Eigenschaft der Hülle (B.119) } \} \\
& x \setminus (L - \varepsilon)^* \\
= & \quad \{ \text{ siehe links } \} \\
& (x \setminus (L - \varepsilon)) \cdot (L - \varepsilon)^* \\
= & \quad \{ \text{ Differenz (B.134c) } \} \\
& (x \setminus L) \cdot (L - \varepsilon)^* \\
= & \quad \{ \text{ Eigenschaft der Hülle (B.119) } \} \\
& (x \setminus L) \cdot L^*
\end{aligned}
$$

Voilà. Abbildung B.20 fasst die verschiedenen Formeln für den Rechtsfaktor noch einmal zusammen.

Beispiel: Matrizen\Graphen Wir setzen zum Endspurt an und zeigen: Sei I eine beliebige, nicht notwendigerweise endliche Indexmenge. Ist Q ein Quantal, dann bilden die *quadratischen* Matrizen $I \times I \to Q$ ebenfalls ein Quantal.

Mit anderen Worten: Auch Graphen lassen sich dividieren! Die Multiplikation von Graphen haben wir als Konkatenation von Kanten gedeutet: Gibt es eine Kante von i nach j in A und eine von j nach k in B, dann enthält $A \cdot B$ eine Kante von i nach k.





Die Division kehrt grob gesprochen die Multiplikation um: Die Kante von j nach k in $A \setminus C$ ergibt sich durch Division der Kante von i nach k in C durch die Kante von i nach j in A.

Ähnlich wie die Matrixmultiplikation ist auch die Matrixdivision nicht nur für quadratische Matrizen definiert: Beim Rechtsfaktor müssen Dividend und Divisor lediglich die gleiche »Zeilen-

zahl« besitzen; beim Linksfaktor muss die »Spaltenzahl« identisch sein.

$$\frac{P : I \times J \to Q \qquad B : I \times K \to Q}{P \setminus B : J \times K \to Q} \qquad\qquad \frac{B : I \times K \to Q \qquad Q : J \times K \to Q}{B \,/\, Q : I \times J \to Q}$$

Wir beschränken uns auf die Herleitung des Rechtsfaktors — in der Rechnung verfolgen wir systematisch das Ziel, A auf der linken Seite zu isolieren.

$$\begin{aligned}
& P \cdot A \leqslant B \\
\iff & \quad \{ \text{ komponentenweise Ordnung (B.104) } \} \\
& \forall\, i \in I \;.\; \forall\, k \in K \;.\; (P \cdot A)_{ik} \leqslant B_{ik} \\
\iff & \quad \{ \text{ Definition Komposition (B.103d) } \} \\
& \forall\, i \in I \;.\; \forall\, k \in K \;.\; \bigsqcup_{j \in J} P_{ij} \cdot A_{jk} \leqslant B_{ik} \\
\iff & \quad \{ \text{ Supremum (B.18) } \} \\
& \forall\, i \in I \;.\; \forall\, k \in K \;.\; \forall\, j \;.\; P_{ij} \cdot A_{jk} \leqslant B_{ik} \\
\iff & \quad \{ \text{ Annahme: Q ist ein Quantal } \} \\
& \forall\, i \in I \;.\; \forall\, k \in K \;.\; \forall\, j \in J \;.\; A_{jk} \leqslant P_{ij} \setminus B_{ik} \\
\iff & \quad \{ \text{ Logik } \} \\
& \forall\, j \in I \;.\; \forall\, k \in K \;.\; \forall\, i \in J \;.\; A_{jk} \leqslant P_{ij} \setminus B_{ik} \\
\iff & \quad \{ \text{ Infimum (B.19) } \} \\
& \forall\, j \in I \;.\; \forall\, k \in K \;.\; A_{jk} \leqslant \bigsqcap_{i \in I} P_{ij} \setminus B_{ik} \\
\iff & \quad \{ \text{ definiere } (P \setminus B)_{jk} := \bigsqcap_{i \in I} P_{ij} \setminus B_{ik} \} \\
& \forall\, j \in I \;.\; \forall\, k \in K \;.\; A_{jk} \leqslant (P \setminus B)_{jk} \\
\iff & \quad \{ \text{ komponentenweise Ordnung (B.104) } \} \\
& A \leqslant P \setminus B
\end{aligned}$$

Damit ergeben sich die folgenden Definitionen für die Faktoren.

$$(P \setminus B)_{jk} := \bigsqcap_{i \in I} P_{ij} \setminus B_{ik} \qquad\qquad (B \,/\, Q)_{ij} := \bigsqcap_{k \in K} B_{ik} \,/\, Q_{jk}$$

Die Matrixdivision lässt sich mit Hilfe von Zeilen- und Spaltenvektoren visualisieren.

$$\begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \end{pmatrix} \setminus \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \\ A_{41} & A_{42} & A_{43} \end{pmatrix}$$

Der Eintrag A_{jk} des Matrixquotienten ergibt sich als ***Skalarquotient*** des j-ten Spaltenvektors von P mit dem k-ten Spaltenvektor von B. Beim Skalarquotienten werden die korrespondierenden Komponenten der Vektoren dividiert und die Ergebnisse geschnitten, zum Beispiel:

$$\begin{pmatrix} P_{13} \\ P_{23} \end{pmatrix} \setminus \begin{pmatrix} B_{12} \\ B_{22} \end{pmatrix} = P_{13} \setminus B_{12} \sqcap P_{23} \setminus B_{22} = A_{32}$$

Eine Matrix lässt sich auch durch ein Skalar dividieren:

$$(p \setminus \mathrm{B})_{jk} := p \setminus (\mathrm{B})_{jk} \qquad (\mathrm{B} / q)_{ij} := \mathrm{B}_{ij} / q \tag{B.136}$$

Die Division durch ein Skalar lässt sich als Spezialfall der Matrixdivision ansehen, wobei der Divisor eine sogenannte Skalarmatrix ist. Bei einer ***Skalarmatrix*** stimmen die Elemente auf der Hauptdiagonalen überein; die Elemente außerhalb der Hauptdiagonalen sind $\bot$: $\mathrm{P}_{ij} = [i = j] \cdot p$. (Falls Sie sich wundern: Ja, wir können durch $\bot$ teilen, das Ergebnis ist $\top$, das größte Element des Verbands.)

Spezialfall: Matrizen von Sprachen Es verbleibt, einen Beweis aus Abschnitt 6.3.5 nachzutragen. Zur Erinnerung: Mit Hilfe der Division lässt sich das ***Wortproblem*** für reguläre Sprachen lösen; wird die Sprache durch ein Syntaxdiagramm beschrieben, kommt die Matrixdivision ins Spiel …

Seien S und F Boolesche Vektoren, sei N eine ε-freie Matrix und x ein Symbol. (Ein Vektor bzw. eine Matrix heißt ***Boolesch***, wenn alle Einträge Boolesch sind: $\mathrm{A} \subseteq \mathrm{E}$. Er bzw. sie heißt ***ε-frei***, wenn alle Einträge ε-frei sind: $\mathrm{A} \cap \mathrm{E} = \mathbf{0}$.) Dann gilt:

$$x \setminus (\mathrm{S} \cdot \mathrm{N}^* \cdot \mathrm{F}) = \mathrm{S} \cdot (x \setminus \mathrm{N}) \cdot \mathrm{N}^* \cdot \mathrm{F} \tag{B.137a}$$

$$\varepsilon \in \mathrm{S} \cdot \mathrm{N}^* \cdot \mathrm{F} \quad \Longleftrightarrow \quad \varepsilon \in \mathrm{S} \cdot \mathrm{F} \tag{B.137b}$$

Der Nachweis von (B.137a) nutzt aus, dass sich $x \setminus \mathrm{N}^*$ besonders einfach berechnen lässt, wenn die Übergangsmatrix N wie angenommen ε-frei ist.

$$\begin{aligned}
& x \setminus (\mathrm{S} \cdot \mathrm{N}^* \cdot \mathrm{F}) \\
= & \quad \{ \text{ Annahme: S und F Boolesch (B.138c)–(B.138d) } \} \\
& \mathrm{S} \cdot (x \setminus \mathrm{N}^*) \cdot \mathrm{F} \\
= & \quad \{ \text{ Fixpunkt: } \mathrm{N}^* = \mathbf{1} \cup \mathrm{N} \cdot \mathrm{N}^* \} \\
& \mathrm{S} \cdot (x \setminus (\mathbf{1} \cup \mathrm{N} \cdot \mathrm{N}^*)) \cdot \mathrm{F} \\
= & \quad \{ x \setminus \text{- distribuiert über Vereinigungen (B.134a) } \} \\
& \mathrm{S} \cdot (x \setminus \mathbf{1}) \cup (x \setminus (\mathrm{N} \cdot \mathrm{N}^*)) \cdot \mathrm{F} \\
= & \quad \{ x \setminus \mathbf{1} = \mathbf{0} \} \\
& \mathrm{S} \cdot (x \setminus (\mathrm{N} \cdot \mathrm{N}^*)) \cdot \mathrm{F} \\
= & \quad \{ \text{ Annahme: N ist ε-frei (B.138e) } \} \\
& \mathrm{S} \cdot (x \setminus \mathrm{N}) \cdot \mathrm{N}^* \cdot \mathrm{F}
\end{aligned}$$

Viele Eigenschaften von Sprachen vererben sich auf Matrizen von Sprachen: Ist zum Beispiel L eine Boolesche Sprache, $\mathrm{L} = \varnothing$ oder $\mathrm{L} = \varepsilon$, dann ist $x \setminus \mathrm{L} = \varnothing$. Analog gilt für Boolesche Matrizen $x \setminus \mathrm{A} = \mathbf{0}$ — dass die Eigenschaft »vererbt« wird, liegt daran, dass die Division durch ein Skalar ***komponentenweise*** gebildet wird. Bei der Division können Boolesche Faktoren »übersprungen« werden, im Fall von Sprachen,

$$x \setminus (\mathrm{L}_1 \cdot \mathrm{L}_2) = \mathrm{L}_1 \cdot (x \setminus \mathrm{L}_2) \qquad \text{falls } \mathrm{L}_1 \text{ Boolesch} \tag{B.138a}$$

$$x \setminus (\mathrm{L}_1 \cdot \mathrm{L}_2) = (x \setminus \mathrm{L}_1) \cdot \mathrm{L}_2 \qquad \text{falls } \mathrm{L}_2 \text{ Boolesch} \tag{B.138b}$$

ebenso wie im Fall von Matrizen:

$$x \setminus (\mathrm{A} \cdot \mathrm{B}) = \mathrm{A} \cdot (x \setminus \mathrm{B}) \qquad \text{falls A Boolesch} \tag{B.138c}$$

$$x \setminus (\mathrm{A} \cdot \mathrm{B}) = (x \setminus \mathrm{A}) \cdot \mathrm{B} \qquad \text{falls B Boolesch} \tag{B.138d}$$

Diese beiden Eigenschaften haben wir oben im Beweis im ersten Schritt ausgenutzt. Der Rechtsfaktor eines Produkts lässt sich ebenfalls besonders einfach berechnen, wenn die erste Sprache ε-frei ist.

$$x \setminus (L_1 \cdot L_2) = (x \setminus L_1) \cdot L_2 \qquad \text{falls } L_1 \text{ } \varepsilon\text{-frei}$$

Entsprechendes gilt für Matrizen:

$$x \setminus (A \cdot B) = (x \setminus A) \cdot B \qquad \text{falls } A \text{ } \varepsilon\text{-frei} \tag{B.138e}$$

Wir zeigen exemplarisch einen Beweis — der Nachweis der anderen Aussagen folgt exakt dem gleichen Schema.

$$\begin{aligned}
& (x \setminus (A \cdot B))_{ik} \\
= \quad & \{ \text{ Matrixdivision durch Skalar (B.136) } \} \\
& x \setminus (A \cdot B)_{ik} \\
= \quad & \{ \text{ Definition Matrixprodukt (B.103d) } \} \\
& x \setminus \bigcup_{j \in J} A_{ij} \cdot B_{jk} \\
= \quad & \{ \text{ } x \setminus \text{ - distribuiert über Vereinigungen (B.134a) } \} \\
& \bigcup_{j \in J} x \setminus (A_{ij} \cdot B_{jk}) \\
= \quad & \{ \text{ Annahme: A und damit auch } A_{ij} \text{ Boolesch; Eigenschaft von Sprachen (B.138a) } \} \\
& \bigcup_{j \in J} A_{ij} \cdot (x \setminus B_{jk}) \\
= \quad & \{ \text{ Matrixdivision durch Skalar (B.136) } \} \\
& \bigcup_{j \in J} A_{ij} \cdot (x \setminus B)_{jk} \\
= \quad & \{ \text{ Definition Matrixprodukt (B.103d) } \} \\
& (A \cdot (x \setminus B))_{ik}
\end{aligned}$$

Kommen wir zum Nachweis von (B.137b). Die Eigenschaft besagt, dass die von einem Syntaxdiagramm generierte Sprache genau dann ε enthält, wenn mindestens ein Startknoten gleichzeitig ein Zielknoten ist. Der Beweis nutzt wiederum aus, dass die Übergangsmatrix N ε-frei ist.

$$\begin{aligned}
& \varepsilon \in S \cdot N^* \cdot F \\
\iff \quad & \{ \text{ Fixpunkt: } N^* = \mathbf{1} \cup N \cdot N^* \text{ } \} \\
& \varepsilon \in S \cdot (\mathbf{1} \cup N \cdot N^*) \cdot F \\
\iff \quad & \{ \text{ Distributivgesetze (B.100b) und neutrales Element (B.99a) } \} \\
& \varepsilon \in S \cdot F \cup S \cdot N \cdot N^* \cdot F \\
\iff \quad & \{ \text{ Definition Vereinigung } \} \\
& \varepsilon \in S \cdot F \ \vee \ \varepsilon \in S \cdot N \cdot N^* \cdot F \\
\iff \quad & \{ \text{ Annahme: N ist } \varepsilon\text{-frei (B.139d) } \} \\
& \varepsilon \in S \cdot F
\end{aligned}$$

Ähnlich wie im Fall der Rechtsfaktoren übertragen sich Rechengesetze für Sprachen auf Rechengesetze für Matrizen über Sprachen. So gilt für Sprachen:

$$L_1 \cup L_2 \text{ } \varepsilon\text{-frei} \iff L_1 \text{ } \varepsilon\text{-frei} \ \wedge \ L_2 \text{ } \varepsilon\text{-frei} \tag{B.139a}$$

$$L_1 \cdot L_2 \text{ } \varepsilon\text{-frei} \iff L_1 \text{ } \varepsilon\text{-frei} \ \vee \ L_2 \text{ } \varepsilon\text{-frei} \tag{B.139b}$$

Und analog gilt für Matrizen:

$$\mathrm{A} \cup \mathrm{B}\ \varepsilon\text{-frei} \iff \mathrm{A}\ \varepsilon\text{-frei} \ \wedge\ \mathrm{B}\ \varepsilon\text{-frei} \tag{B.139c}$$

$$\mathrm{A} \cdot \mathrm{B}\ \varepsilon\text{-frei} \impliedby \mathrm{A}\ \varepsilon\text{-frei} \ \vee\ \mathrm{B}\ \varepsilon\text{-frei} \tag{B.139d}$$

Eine kleine Diskrepanz lässt sich ausmachen: Die letzte Aussage ist nur eine Implikation, keine Äquivalenz. Das liegt daran, dass das Matrixprodukt im Unterschied zur Vereinigung *nicht* komponentenweise gebildet wird. (Finden Sie ein Gegenbeispiel für die Links-nach-rechts-Richtung?) Wir zeigen exemplarisch (B.139d) und nehmen dazu an, dass mindestens eine der Matrizen ε-frei ist.

$$\begin{aligned}
& \mathrm{A} \cdot \mathrm{B}\ \varepsilon\text{-frei} \\
\iff & \quad \{\ \text{Definition } \varepsilon\text{-frei}\ \} \\
& \forall\, i \in \mathrm{I}\ .\ \forall\, k \in \mathrm{K}\ .\ \varepsilon \notin (\mathrm{A} \cdot \mathrm{B})_{ik} \\
\iff & \quad \{\ \text{Definition Matrixprodukt (B.103d)}\ \} \\
& \forall\, i \in \mathrm{I}\ .\ \forall\, k \in \mathrm{K}\ .\ \varepsilon \notin \bigcup_{j \in \mathrm{J}} \mathrm{A}_{ij} \cdot \mathrm{B}_{jk} \\
\iff & \quad \{\ \text{Eigenschaft von Sprachen (B.139a)}\ \} \\
& \forall\, i \in \mathrm{I}\ .\ \forall\, k \in \mathrm{K}\ .\ \forall\, j \in \mathrm{J}\ .\ \varepsilon \notin \mathrm{A}_{ij} \cdot \mathrm{B}_{jk} \\
\iff & \quad \{\ \text{Eigenschaft von Sprachen (B.139b)}\ \} \\
& \forall\, i \in \mathrm{I}\ .\ \forall\, k \in \mathrm{K}\ .\ \forall\, j \in \mathrm{J}\ .\ \varepsilon \notin \mathrm{A}_{ij} \ \vee\ \varepsilon \notin \mathrm{B}_{jk} \\
\iff & \quad \{\ \text{Annahme: A oder B } \varepsilon\text{-frei, damit auch } \mathrm{A}_{ij} \text{ oder } \mathrm{B}_{jk}\ \varepsilon\text{-frei}\ \} \\
& \forall\, i \in \mathrm{I}\ .\ \forall\, k \in \mathrm{K}\ .\ \forall\, j \in \mathrm{J}\ .\ \mathit{true} \\
\iff & \quad \{\ \text{Logik}\ \} \\
& \mathit{true}
\end{aligned}$$

Übungen.

16. Zeigen Sie $(p \setminus x) \,/\, s = p \setminus (x \,/\, s)$.

B.6.7. Fusion⋆ ⋆

Seien f und g monotone Funktionen und $\ell \dashv r$ eine Galoisverbindung.

$$g \circlearrowright (\mathrm{P}, \leqslant) \underset{r}{\overset{\ell}{\underset{\longrightarrow}{\overset{\longleftarrow}{\bot}}}} (\mathrm{Q}, \sqsubseteq) \circlearrowleft f$$

Unter diesen Voraussetzungen gilt

$$\ell(\mu f) = \mu g \impliedby \ell \circ f = g \circ \ell \tag{B.140}$$

Das Gesetz firmiert unter dem Namen ***Fixpunkt-Fusion***, da es eine hinreichende Bedingung formuliert, um eine Funktion mit einem Fixpunkt zu einem Fixpunkt zu verschmelzen. (Gemäß dieser Lesart wird $\ell(\mu f) = \mu g$ von links nach rechts angewendet; wendet man das Gesetz umgekehrt von rechts nach links an, dann würde man eher von ***Fixpunkt-Spaltung*** sprechen — die Physik lässt grüßen.) Bevor wir uns dem Beweis zuwenden, schauen wir uns (B.140) zunächst in Aktion an.

In der Welt der Quantale lässt sich die reflexive, transitive Hülle als Fixpunkt ausdrücken: $a^* := \mu f$ mit $f(x) := 1 \sqcup a \cdot x$. Multiplizieren wir a^* mit a, erhalten wir die ***transitive Hülle***: $a \cdot a^* := a^+$,

die wir ebenfalls als Fixpunkt schreiben wollen. Da die Multiplikation linksadjunkt ist, $\ell(x) := a \cdot x$, ist die zentrale Voraussetzung für die Fixpunkt-Fusion erfüllt. Den fehlenden Mosaikstein, die Funktion g, leiten wir aus der Vorbedingung von (B.140) ab.

$$\begin{aligned}
& \ell(f(x)) \\
= \quad & \{ \text{ Definition } \ell \text{ und } f \} \\
& a \cdot (1 \sqcup a \cdot x) \\
= \quad & \{ \text{ Distributivgesetz (B.100b) } \} \\
& a \sqcup a \cdot (a \cdot x) \\
= \quad & \{ \text{ definiere } g(w) := a \sqcup a \cdot w \} \\
& g(\ell(x))
\end{aligned}$$

Bildlich gesprochen schieben wir ℓ in die Funktion f bis zum Parameter x, so dass wir g mehr oder weniger direkt ablesen können. Wir halten fest: Auch die transitive Hülle lässt sich als Fixpunkt schreiben: $a^+ = \mu g$ mit $g(w) := a \sqcup a \cdot w$.

Die Fixpunkt-Fusion selbst zeigen wir mit einem Ping-Pong Beweis (B.14). Der »Pong«

$$\ell(\mu f) \geqslant \mu g \quad \Longleftarrow \quad \ell \circ f \geqslant g \circ \ell$$

ist Routine, da wir unmittelbar die Fixpunkt-Induktion anwenden können:

$$\begin{aligned}
& \ell(\mu f) \geqslant \mu g \\
\Longleftarrow \quad & \{ \text{ Fixpunkt-Induktion (B.105b) } \} \\
& \ell(\mu f) \geqslant g(\ell(\mu f))
\end{aligned}$$

Die zu etablierende Ungleichung folgt direkt aus der Annahme.

$$\begin{aligned}
& \ell(\mu f) \\
\geqslant \quad & \{ \text{ Präfixpunkt (B.105a) und } \ell \text{ monoton } \} \\
& \ell(f(\mu f)) \\
\geqslant \quad & \{ \text{ Annahme: } \ell \circ f \geqslant g \circ \ell \} \\
& g(\ell(\mu f))
\end{aligned}$$

Wir machen interessanterweise keinen Gebrauch von der Annahme, dass ℓ linksadjunkt ist — diese Annahme fließt nur in den »Ping« ein.

$$\ell(\mu f) \leqslant \mu g \quad \Longleftarrow \quad \ell \circ f \leqslant g \circ \ell$$

Dieser Teilbeweis ist schwieriger, da der isolierte Fixpunkt μg auf der falschen Seite der Ungleichung steht, so dass sich die Fixpunkt-Induktion nicht anwenden lässt. Jetzt kommt die Galoisverbindung ins Spiel: Mit ihrer Hilfe lässt sich ℓ »aus dem Weg räumen«.

$$\begin{aligned}
& \ell(\mu f) \leqslant \mu g \\
\Longleftrightarrow \quad & \{ \text{ Annahme: } \dashv r \} \\
& \mu f \leqslant r(\mu g) \\
\Longleftarrow \quad & \{ \text{ Fixpunkt-Induktion (B.105b) } \} \\
& f(r(\mu g)) \leqslant r(\mu g) \\
\Longleftrightarrow \quad & \{ \text{ indirekter Beweis (B.128a) und } f \text{ monoton } \} \\
& \forall\, x \in \mathrm{P} \;.\; x \leqslant r(\mu g) \Longrightarrow f(x) \leqslant r(\mu g) \\
\Longleftrightarrow \quad & \{ \text{ Annahme: } \dashv r \} \\
& \forall\, x \in \mathrm{P} \;.\; \ell(x) \leqslant \mu g \Longrightarrow \ell(f(x)) \leqslant \mu g
\end{aligned}$$

Der Beweis illustriert eine typische Vorgehensweise: Die Linksadjunkte wird auf die rechte Seite der Ungleichung transferiert, um eine bestimmte Umformung (hier: die Fixpunkt-Induktion) anwenden zu können. Beim Transfer verwandelt sich die Links- in die Rechtsadjunkte. Die restliche Rechnung sind wir damit beschäftigt, die Rechtsadjunkten wieder zurückzuverwandeln. Das ist etwas trickreich, da r unter anderem als Argument von f auftritt. Es verbleibt $\ell(f(x)) \leqslant \mu g$ unter der Annahme $\ell(x) \leqslant \mu g$ zu zeigen.

$$
\begin{array}{ll}
 & \ell(f(x)) \\
\leqslant & \quad \{ \text{ Annahme: } \ell \circ f \leqslant g \circ \ell \ \} \\
 & g(\ell(x)) \\
\leqslant & \quad \{ \text{ Annahme: } \ell(x) \leqslant \mu g \text{ und } g \text{ monoton } \} \\
 & g(\mu g) \\
\leqslant & \quad \{ \text{ Präfixpunkt (B.105a) } \} \\
 & \mu g
\end{array}
$$

Zum Abschluss des Kapitels kehren wir zum Ausgangspunkt unserer Überlegungen zurück und untersuchen, wann die Gleichung für den Sternoperator $x = 1 \sqcup a \cdot x$ eine *eindeutige* Lösung besitzt. Allgemein hat eine Funktion f einen eindeutigen Fixpunkt, wenn der ***kleinste Präfixpunkt*** μf und der ***größte Postfixpunkt*** νf zusammenfallen: $\mu f = \nu f$. Ordungstheoretische Konzepte treten immer paarweise auf: kleinstes Element/größtes Element, Supremum/Infimum, Linksadjunkte/Rechtsadjunkte usw. Das Konzept der Dualität lässt grüßen: Das größte Element ist das kleinste Element in der dualen Ordnung; das Infimum ist das Supremum in der dualen Ordnung usw. Entsprechend ist der größte Postfixpunkt der kleinste Präfixpunkt in der dualen Ordnung. Die Eigenschaften von νf lassen sich aus denen für μf ableiten, indem systematisch $\leqslant$ und $\geqslant$, $\bot$ und $\top$, $\sqcup$ und $\sqcap$ usw. ausgetauscht werden.

$$
\begin{array}{l}
f(\nu f) \geqslant \nu f \\
\nu f \geqslant x \iff f(x) \geqslant x
\end{array}
$$

Insbesondere lassen sich Rechtsadjunkte und größte Postfixpunkte fusionieren:

$$\nu f = r(\nu g) \iff f \circ r = r \circ g \tag{B.141}$$

Mit Hilfe der Fixpunkt-Fusion können wir zeigen, dass sich die größte Lösung der Gleichung $x = 1 \sqcup a \cdot x$ aus einer x-beliebigen Lösung ableiten lässt. Sei $f(x) := 1 \sqcup a \cdot x$. Wir suchen eine Funktion g, so dass

$$\nu f = s \sqcup \nu g \iff s = 1 \sqcup a \cdot s \tag{B.142}$$

Um die Fixpunkt-Fusion anwenden zu können, müssen wir annehmen, dass die Vereinigung $s \sqcup$ - rechtsadjunkt ist. Die unbekannte Funktion g leiten wir aus der Voraussetzung der Fixpunkt-Induktion (B.141) her. Sei $r(x) := s \sqcup x$, dann gilt

$$
\begin{array}{ll}
 & f(r(x)) \\
= & \quad \{ \text{ Definition } f \text{ und } r \ \} \\
 & 1 \sqcup a \cdot (s \sqcup x) \\
= & \quad \{ \text{ Distributivgesetz (B.100b) } \} \\
 & 1 \sqcup a \cdot s \sqcup a \cdot x \\
= & \quad \{ \text{ Annahme: } s = 1 \sqcup a \cdot s \ \} \\
 & s \sqcup a \cdot x \\
= & \quad \{ \text{ definiere } g(x) := a \cdot x \ \} \\
 & r(g(x))
\end{array}
$$

Aus (B.142) folgt unmittelbar, dass die Gleichung $x = a \cdot x \sqcup 1$ insbesondere dann eine eindeutige Lösung hat, wenn $\nu g = \bot$ mit $g(x) := a \cdot x$ gilt. Das kleinste Element, das die Gleichung $x = a \cdot x$ löst, ist $\bot$. Somit gilt: $x = a \cdot x \sqcup 1$ ist eindeutig lösbar, wenn nur $x = a \cdot x$ eine eindeutige Lösung besitzt. Lassen Sie uns die Ergebnisse auf unsere laufenden Beispiele spezialisieren:

In der *Kostenalgebra* hat die Gleichung $x = a + x$ genau dann eine eindeutige Lösung, nämlich $x = \infty$, wenn $a \neq 0$. Entsprechend ist $x = 0 \downarrow (a + x)$ eindeutig lösbar, $x = 0$, wenn $a \neq 0$. (Erlauben wir negative Kosten, sprich Gewinne, dann besitzt die Gleichung $x = 0 \downarrow (a + x)$ für $a = 0$ unendlich viele Lösungen.)

Im *Quantal der Sprachen* verhält es sich ähnlich: $X = A \cdot X$ und $X = \{\varepsilon\} \cup A \cdot X$ sind eindeutig lösbar, wenn die Sprache A ε-*frei* ist (siehe Beispiel am Anfang von Abschnitt B.6.3). Sei $\|L\|$ die Länge des *kürzesten* Wortes in L, wobei per definitionem $\|\varnothing\| = \infty$. Mit Hilfe dieser Abbildung können wir Gleichungen zwischen Sprachen auf Kostengleichungen reduzieren:

$$
\begin{array}{ll}
 & X = A \cdot X \\
\Longrightarrow & \quad \{ \text{ Eigenschaft } \|\text{-}\| \ \} \\
 & \|X\| = \|A\| + \|X\| \\
\Longrightarrow & \quad \{ \text{ Annahme: A ist } \varepsilon\text{-frei und somit } \|A\| \neq 0 \ \} \\
 & \|X\| = \infty \\
\Longrightarrow & \quad \{ \text{ Eigenschaft } \|\text{-}\| \ \} \\
 & X = \varnothing
\end{array}
$$

Das Resultat zeigt noch einmal, warum die Unterscheidung zwischen ε-freien und ε-haltigen Sprachen von so zentraler Bedeutung ist.

Kommen wir zu Systemen von Gleichungen, sprich zu *Graphen\Matrizen*. Ist A eine Kostenmatrix, dann hat $X = A \cdot X$ eine eindeutige Lösung, wenn es keine »kostenlosen Reiseabschnitte« gibt: $A_{ij} \neq 0$. Ist A eine Matrix von Sprachen, dann ist $X = A \cdot X$ eindeutig lösbar, wenn wenn A ε-frei ist: $\varepsilon \notin A_{ij}$, also

Übungen.

17. Wann besitzt $x = a \cdot x \sqcup b$ eine *eindeutige* Lösung?

C. Lösungen ausgewählter Aufgaben

2.3.1. Siehe Aufgabe 2.4.1.

3.1.1. Siehe Vorlesungsfolien (Diskussion Lisa & Harry).

3.2.1. Es gibt

(a) unendlich viele Ausdrücke: *false*, *true*, ***if*** *false* ***then*** *false* ***else*** *false* …,

(b) aber nur zwei Werte: *false* und *true*.

3.2.2. Nein, wenn e_1 in $e_1 \leqslant e_2$ zu 0 auswertet, dann ist das Ergebnis zwangsläufig *true*, da 0 die kleinste natürliche Zahl ist.

3.4.1. Wie bei der Konjunktion und der Disjunktion reicht eine Alternative.

```
let leq     (a : Bool, b : Bool) : Bool = if a then b else true
let implies (a : Bool, b : Bool) : Bool = if a then b else true
```

Der Vergleich $\leqslant$ korrespondiert übrigens zur Implikation.

4.1.8. **Fall** $n := 0$**:**

$$
\begin{aligned}
& \phi^0 \\
= \quad & \{ \text{ Potenzgesetze } \} \\
& 1 \\
= \quad & \{ \text{ Definition: } \mathscr{F}_{-1} = 1 \text{ und } \mathscr{F}_0 = 0 \} \\
& \mathscr{F}_{-1} + \mathscr{F}_0 \cdot \phi
\end{aligned}
$$

Fall $n := n + 1$**:**

$$
\begin{aligned}
& \phi^{n+1} \\
= \quad & \{ \text{ Potenzgesetze } \} \\
& \phi^n \cdot \phi \\
= \quad & \{ \text{ Induktionsannahme } \} \\
& (\mathscr{F}_{n-1} + \mathscr{F}_n \cdot \phi) \cdot \phi \\
= \quad & \{ \text{ Distributivgesetz } \} \\
& \mathscr{F}_{n-1} \cdot \phi + \mathscr{F}_n \cdot \phi^2 \\
= \quad & \{ \text{ Goldener Schnitt: } \phi^2 = 1 + \phi \} \\
& \mathscr{F}_{n-1} \cdot \phi + \mathscr{F}_n \cdot (\phi + 1) \\
= \quad & \{ \text{ Distributivgesetz } \} \\
& (\mathscr{F}_{n-1} + \mathscr{F}_n) \cdot \phi + \mathscr{F}_n \\
= \quad & \{ \text{ Definition: } \mathscr{F}_{n+2} = \mathscr{F}_n + \mathscr{F}_{n+1} \} \\
& \mathscr{F}_{n+1} \cdot \phi + \mathscr{F}_n
\end{aligned}
$$

6.1.3. $(d \mid d\ d \mid d\ d\ d)\ (.\ d\ d\ d)^*$.

B.1.2. Mit $a := \mathit{true}$, $b := a$ und $\neg \mathit{true} = \mathit{false}$.

B.1.7. Wir rechnen:

$$
\begin{array}{ll}
 & [x = 0] \cdot x = 0 \\
\iff & \quad \{ \text{ Multiplikation } \} \\
 & [x = 0] = 0 \ \vee \ x = 0 \\
\implies & \quad \{ \text{ Iverson (B.5) } \} \\
 & x \neq 0 \ \vee \ x = 0 \\
\impliedby & \quad \{ \text{ Komplementärgesetz } \} \\
 & \mathit{true}
\end{array}
\qquad
\begin{array}{ll}
 & [x \neq 0] \cdot x \\
= & \quad \{ \text{ Negation à la Boole (B.4) } \} \\
 & (1 - [x = 0]) \cdot x \\
= & \quad \{ \text{ Distributivgesetz } \} \\
 & x - [x = 0] \cdot x \\
= & \quad \{ \text{ siehe links } \} \\
 & x
\end{array}
$$

B.1.8.

$$
\begin{array}{ll}
 & [x \geqslant 0] - [x \leqslant 0] \\
= & \quad \{ \text{ Vereinigung à la Boole (B.4) } \} \\
 & ([x = 0] + [x > 0]) - ([x = 0] + [x < 0]) \\
= & \quad \{ \text{ Arithmetik } \} \\
 & [x > 0] - [x < 0]
\end{array}
$$

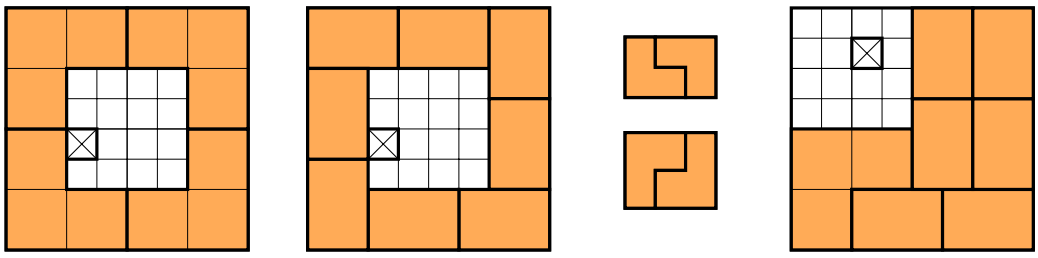
B.1.9. Beweis von $\operatorname{sign}^2 x = [x \neq 0]$:

$$
\begin{array}{ll}
 & \operatorname{sign}^2 x \\
= & \quad \{ \text{ Definition sign (B.3) } \} \\
 & ([x > 0] - [x < 0])^2 \\
= & \quad \{ \text{ binomische Formel: } (a-b)^2 = a^2 - 2 \cdot a \cdot b + b^2 \ \} \\
 & [x > 0]^2 - 2 \cdot [x > 0] \cdot [x < 0] + [x < 0]^2 \\
= & \quad \{ \text{ Durchschnitt à la Boole (B.4) } \} \\
 & [x > 0] + [x < 0] \\
= & \quad \{ \text{ Vereinigung à la Boole (B.4) } \} \\
 & [x \neq 0]
\end{array}
$$

Damit gilt auch $x = \operatorname{sign} x \cdot \operatorname{abs} x = \operatorname{sign} x \cdot \operatorname{sign} x \cdot x = [x \neq 0] \cdot x = x$ (siehe Aufgabe B.1.7).

B.2.7. Jede Zahl hat zwei Darstellungen: z.B. $1/4 = 0.01\bar{0} = 0.00\bar{1}$.

B.3.1. Schachbretter der Größen 1×1, 2×2 und 4×4 lassen tatsächlich nur eine Kachelung zu, aber bereits für 8×8 Schachbretter gibt es mehrere Möglichkeiten. Wenn das freie Feld mittig liegt, kann man den Rand mit 3×2 großen Rechtecken auslegen — jedes der Rechtecke lässt sich auf zwei Weisen mit L-Trominos kacheln. Liegt das freie Feld am Rand, kann man zum Beispiel Rechtecke mit einem vergrößerten L-Tromino kombinieren.



B.4.1. (a) Das Totalitätsaxiom lässt sich besser in Rechnungen verwenden, wenn wir es als Implikation schreiben.

(Totalität) $\qquad \neg(a \leqslant b) \implies b \leqslant a$

Nachweis von (B.20a):

$$\begin{aligned}
& \neg(a \leqslant b) \\
\iff & \quad \{ \text{ Totalität, siehe oben } \} \\
& \neg(a \leqslant b) \ \wedge \ b \leqslant a \\
\iff & \quad \{ \text{ Definition } > \} \\
& a > b
\end{aligned}$$

Die Äquivalenzen (B.20b) ergeben sich als Kontraposition von (B.20a) — über Kreuz.

(b) Nachweis von (B.20c):

$$\begin{aligned}
& a = b \ \vee \ a < b \\
\iff & \quad \{ \text{ Ping-Pong Beweis (B.14) und Definition } < \} \\
& (a \leqslant b \ \wedge \ b \leqslant a) \ \vee \ (a \leqslant b \ \wedge \ \neg(b \leqslant a)) \\
\iff & \quad \{ \text{ Logik } \} \\
& a \leqslant b
\end{aligned}$$

Die Äquivalenzen (B.20d) ergeben sich als Kontraposition von (B.20c) — über Kreuz.

B.4.4. Die Diagramme links und rechts sind gleich; ebenso die mittleren drei.

B.4.6. Abbildungen C.1 und C.2 zeigen alle Ordnungen auf 4 Elementen, einmal als Tabelle und ein zweites Mal als Hassediagramm.

B.4.9. Das sind keine interessanten Konzepte: Eine größte obere Schranke wäre das größte Element; eine kleinste untere Schranke entsprechend das kleinste Element.

B.4.11. »⟸:« folgt aus $a \leqslant a \uparrow b$ und $b \leqslant a \uparrow b$ (diese Richtung gilt immer). »⟹:«

$$\begin{aligned}
& x \leqslant a \uparrow b \ \wedge \ (a \uparrow b = a \ \vee \ a \uparrow b = b) \\
\iff & \quad \{ \text{ Distributivgesetz } \} \\
& (x \leqslant a \uparrow b \ \wedge \ a \uparrow b = a) \ \vee \ (x \leqslant a \uparrow b \ \wedge \ a \uparrow b = b) \\
\implies & \quad \{ \text{ Logik } \} \\
& x \leqslant a \ \vee \ x \leqslant b
\end{aligned}$$

B.5.2. In $\mathbb{N}$ gilt immer $a \leqslant a + p$; daraus folgt $a \dot{-} p \leqslant a$. (Und: Aus $a \leqslant b + a$ folgt $a \dot{-} a \leqslant b$ für alle b, das heißt $a \dot{-} a = 0$.)

B.5.9. Zum Beweis zeigen wir die äquivalente Aussage auf der rechten Seite.

$$\begin{array}{rcl}
1 \leqslant a \ \mathbf{div} \ a & \iff & 1 \cdot a \leqslant a \\
(a \ \mathbf{div} \ b) \cdot (b \ \mathbf{div} \ c) \leqslant a \ \mathbf{div} \ c & \iff & (a \ \mathbf{div} \ b) \cdot (b \ \mathbf{div} \ c) \cdot c \leqslant a
\end{array}$$

Wir müssen zweimal kürzen:

$$\begin{aligned}
& (a \ \mathbf{div} \ b) \cdot (b \ \mathbf{div} \ c) \cdot c \\
\leqslant & \quad \{ \text{ Kürzungsregel (B.43) } \} \\
& (a \ \mathbf{div} \ b) \cdot b \\
\leqslant & \quad \{ \text{ Kürzungsregel (B.43) } \} \\
& a
\end{aligned}$$

B.5.11. Wir können zum Beispiel ausnutzen, dass die Negation (der Vorzeichenwechsel) antiton ist.

$$\begin{aligned}
-(a \uparrow b) &= (-a) \downarrow (-b) \\
-(a \downarrow b) &= (-a) \uparrow (-b)
\end{aligned}$$

Damit ist $a \uparrow b = -((-a) \downarrow (-b))$ und umgekehrt $a \downarrow b = -((-a) \uparrow (-b))$.

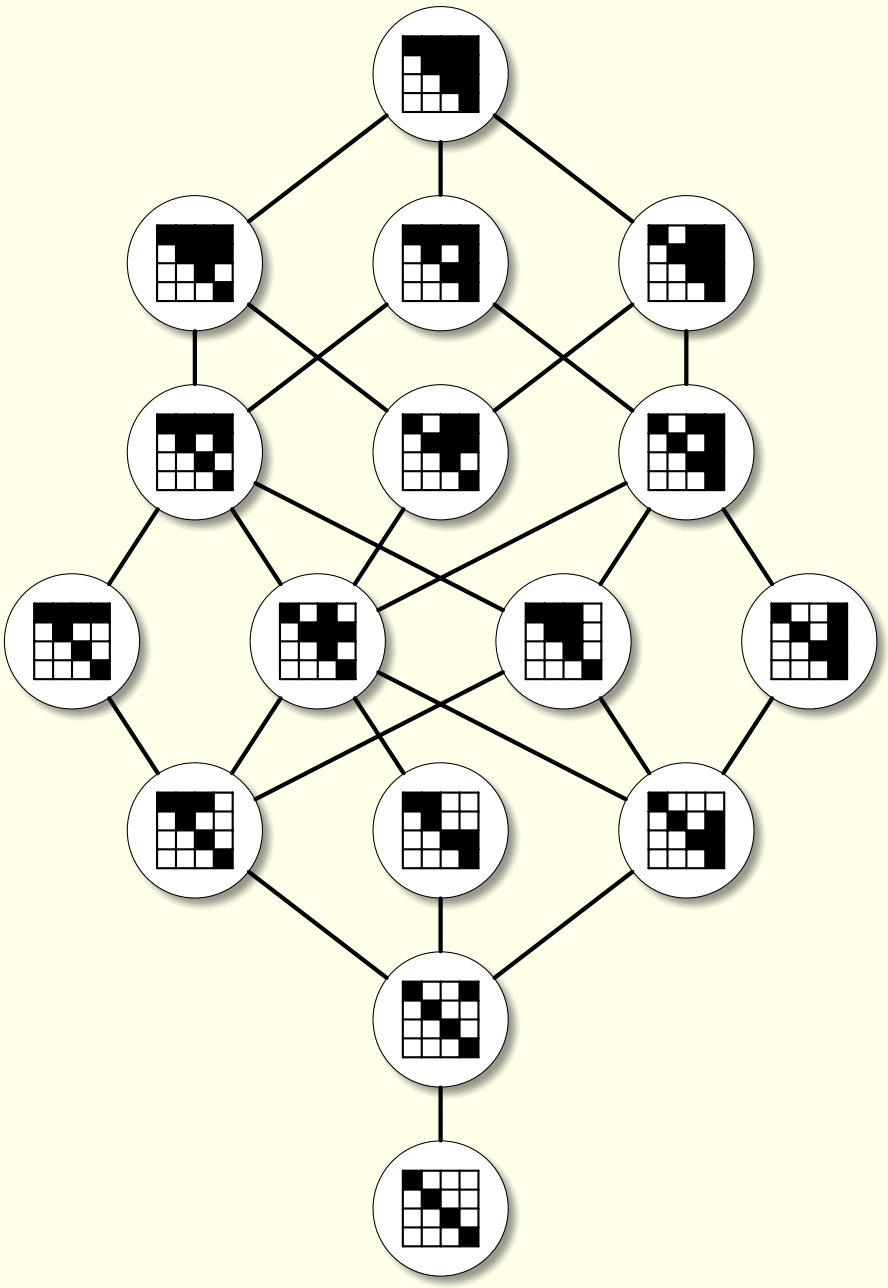


Abbildung C.1.: Alle Ordnungen mit 4 Elementen in Tabellenform.

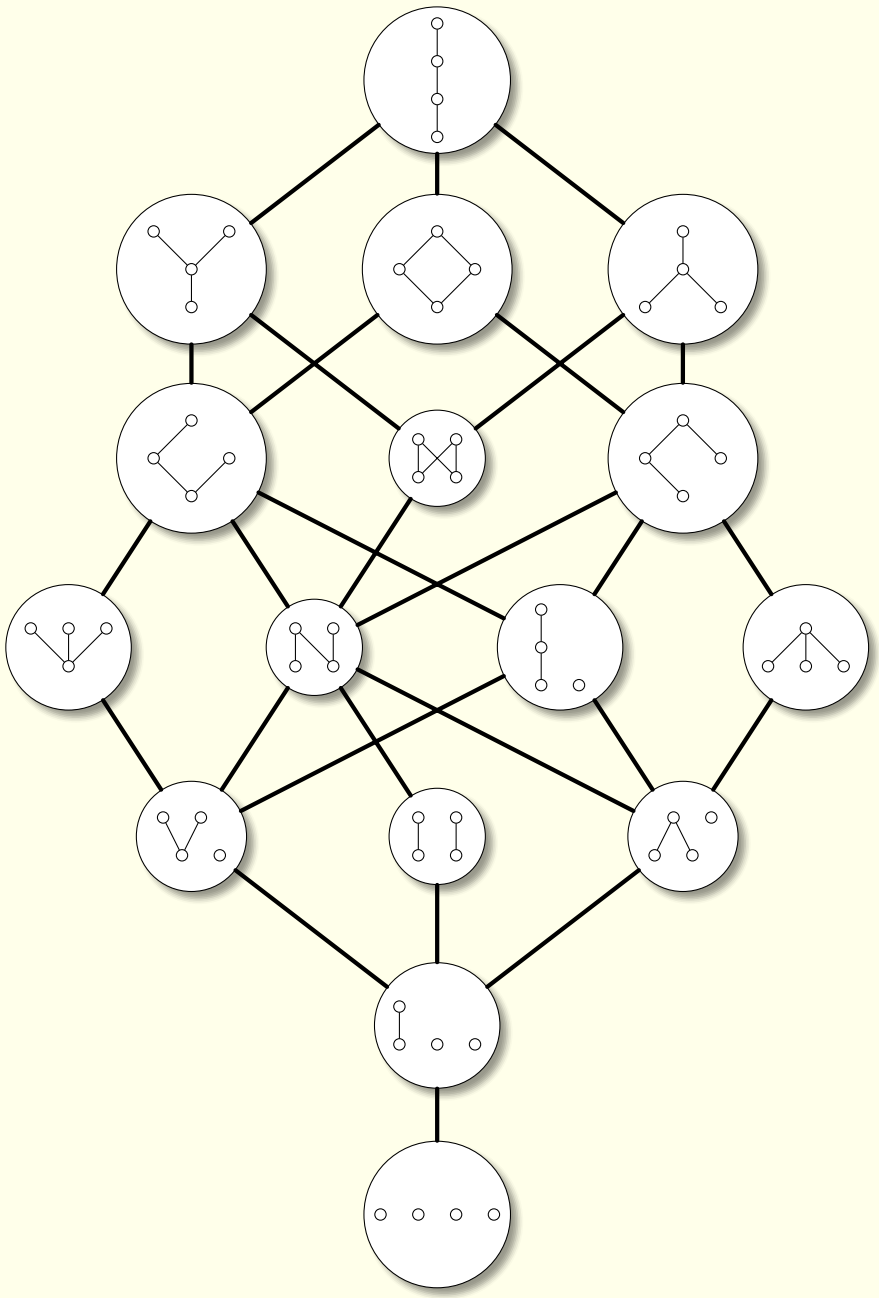


Abbildung C.2.: Hassediagramme aller Ordnungen mit 4 Elementen.

B.5.12.

$$
\begin{aligned}
&a \underline{\boldsymbol{div}} (-p) = \lfloor a/(-p) \rfloor = -\lceil a/p \rceil = -(a \overline{\boldsymbol{div}}\ p)\\
&(-a) \underline{\boldsymbol{div}}\ p = \lfloor (-a)/p \rfloor = -\lceil a/p \rceil = -(a \overline{\boldsymbol{div}}\ p)\\
&a \underline{\boldsymbol{mod}} (-p) = a - a \underline{\boldsymbol{div}} (-p) \cdot (-p) = a - a \overline{\boldsymbol{div}}\ p \cdot p = a \overline{\boldsymbol{mod}}\ p\\
&(-a) \underline{\boldsymbol{mod}}\ p = (-a) - (-a) \underline{\boldsymbol{div}}\ p \cdot p = -(a - a \overline{\boldsymbol{div}}\ p \cdot p) = -(a \overline{\boldsymbol{mod}}\ p)
\end{aligned}
$$

B.5.16. (a) Wir führen für beide Aussagen einen indirekten Beweis (B.15d).

Sei $n \in \mathbb{N}$ und $x \in \mathbb{R}_{\geqslant 0}$:

$$
\begin{aligned}
& n \leqslant \lfloor \sqrt{\lfloor x \rfloor} \rfloor\\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \}\\
& n \leqslant \sqrt{\lfloor x \rfloor}\\
\iff & \quad \{ \text{ Inverse } \}\\
& n^2 \leqslant \lfloor x \rfloor\\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \}\\
& n^2 \leqslant x\\
\iff & \quad \{ \text{ Inverse } \}\\
& n \leqslant \sqrt{x}\\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \}\\
& n \leqslant \lfloor \sqrt{x} \rfloor
\end{aligned}
$$

Sei $n \in \mathbb{Z}$ und $x \in \mathbb{R}$:

$$
\begin{aligned}
& n \leqslant \lfloor \lfloor x \rfloor / p \rfloor\\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \}\\
& n \leqslant \lfloor x \rfloor / p\\
\iff & \quad \{ \text{ Inverse } \}\\
& n \cdot p \leqslant \lfloor x \rfloor\\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \}\\
& n \cdot p \leqslant x\\
\iff & \quad \{ \text{ Inverse } \}\\
& n \leqslant x/p\\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \}\\
& n \leqslant \lfloor x/p \rfloor
\end{aligned}
$$

Der mittlere Schritt ist jeweils *nur* durchführbar, da n^2 bzw. $n \cdot p$ ganze Zahlen sind.

(b) Die Eigenschaft $\lfloor \sqrt{\lfloor n/4 \rfloor} \rfloor = \lfloor \sqrt{n}/2 \rfloor$ lässt sich mit Hilfe von (B.70) direkt nachweisen:

$$
\begin{aligned}
& \lfloor \sqrt{\lfloor n/4 \rfloor} \rfloor\\
= & \quad \{ \text{ geschachtelte Böden (B.70) } \}\\
& \lfloor \sqrt{n/4} \rfloor\\
= & \quad \{ \text{ Potenzgesetze } \}\\
& \lfloor \sqrt{n}/2 \rfloor
\end{aligned}
$$

(c) Aus der ersten Voraussetzung — f ist stetig und streng monoton wachsend — folgt, dass f eine stetige und streng monoton wachsende Umkehrfunktion hat. Die zweite Voraussetzung bedingt, dass die Umkehrfunktion f^{-1} ganze Zahlen auf ganze Zahlen abbildet. Es gilt sogar, dass die folgenden Implikationen äquivalent sind:

$$
\begin{aligned}
f(x) \in \mathbb{Z} &\implies x \in \mathbb{Z}\\
y \in \mathbb{Z} &\implies f^{-1}(y) \in \mathbb{Z}
\end{aligned}
$$

Die beiden obigen Beweise für geschachtelte Böden lassen sich damit unmittelbar verallgemeinern. Die entsprechende Eigenschaft für die Decke zeigen wir mit einem »gespiegelten« indirekten Beweis gemäß (B.15c). Sei $n \in \mathbb{Z}$ und $x \in \mathbb{R}$:

$$
\begin{array}{ll}
& n \leqslant \lfloor f(\lfloor x \rfloor) \rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& n \leqslant f(\lfloor x \rfloor) \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse und } f^{-1}(n) \in \mathbb{Z} \} \\
& f^{-1}(n) \leqslant \lfloor x \rfloor \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& f^{-1}(n) \leqslant x \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse } \} \\
& n \leqslant f(x) \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Definition Boden (B.54a) } \} \\
& n \leqslant \lfloor f(x) \rfloor \text{ in } \mathbb{Z}
\end{array}
\qquad
\begin{array}{ll}
& \lceil f(\lceil x \rceil) \rceil \leqslant n \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Decke (B.54b) } \} \\
& f(\lceil x \rceil) \leqslant n \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse und } f^{-1}(n) \in \mathbb{Z} \} \\
& \lceil x \rceil \leqslant f^{-1}(n) \text{ in } \mathbb{Z} \\
\iff & \quad \{ \text{ Definition Decke (B.54b) } \} \\
& x \leqslant f^{-1}(n) \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Inverse } \} \\
& f(x) \leqslant n \text{ in } \mathbb{R} \\
\iff & \quad \{ \text{ Definition Decke (B.54b) } \} \\
& \lceil f(x) \rceil \leqslant n \text{ in } \mathbb{Z}
\end{array}
$$

Der mittlere Schritt erfordert, dass $f^{-1}(n)$ eine ganze Zahl ist. (Die Funktion $f(x) := x \cdot 2$ erfüllt die Voraussetzung zum Beispiel nicht; entsprechend gilt $\lfloor \lfloor x \rfloor \cdot 2 \rfloor = \lfloor x \cdot 2 \rfloor$ im Allgemeinen *nicht*.)

(d) Die Voraussetzungen sind erfüllt; insbesondere folgt aus $n \in \mathbb{Z}$ sowohl $n^2 \in \mathbb{Z}$ als auch $n \cdot p \in \mathbb{Z}$. (Im Fall der Quadratwurzel müssen wir die Quantoren auf nichtnegative Zahlen einschränken.)

(e) Ist f und damit auch f^{-1} streng monoton fallend, dann erhalten wir aufgrund der Antitonie »gemischte« Formeln:

$$\left\lfloor f(\lceil x \rceil) \right\rfloor = \lfloor f(x) \rfloor \qquad \left\lceil f(\lfloor x \rfloor) \right\rceil = \lceil f(x) \rceil \tag{C.1}$$

In den indirekten Beweisen kehren sich die mittleren Ungleichungen mit f^{-1} um.

B.5.17. Induktionsbasis: $2 \setminus 0 \ \vee \ 2 \setminus 1$ ist wahr, da 0 das größte Element ist. **Induktionsbasis:** Aus $2 \setminus 2$, $2 \setminus -2$ und (B.80) folgt $2 \setminus n \iff 2 \setminus n+2$. Somit $2 \setminus n+1 \ \vee \ 2 \setminus n+2 \iff 2 \setminus n+1 \ \vee \ 2 \setminus n$; letzteres gilt gemäß Induktionsannahme.

$$
\begin{array}{ll}
& 2 \setminus n \ \vee \ 2 \setminus n+1 \\
\implies & \quad \{ \text{ (B.78) — links wird mit } n+1 \text{, rechts mit } n \text{ multipliziert } \} \\
& 2 \setminus n \cdot (n+1) \ \vee \ 2 \setminus (n+1) \cdot n \\
\iff & \quad \{ \text{ Logik } \} \\
& 2 \setminus n \cdot (n+1)
\end{array}
$$

B.5.18.

$$
\begin{array}{ll}
& 8 \setminus (2 \cdot n + 1)^2 - 1 \\
\iff & \quad \{ \text{ binomische Formel: } (a+b)^2 = a^2 + 2 \cdot a \cdot b + b^2 \} \\
& 8 \setminus (4 \cdot n^2 + 4 \cdot n + 1) - 1 \\
\iff & \quad \{ \text{ Arithmetik } \} \\
& 8 \setminus 4 \cdot n \cdot (n+1) \\
\iff & \quad \{ \text{ Kürzungsregel (B.79a) } \} \\
& 2 \setminus n \cdot (n+1)
\end{array}
$$

B.5.19.

$$
\begin{array}{ll}
& 8 \setminus (2 \cdot m + 1)^2 - (2 \cdot n + 1)^2 \\
\iff & \quad \{ \text{ binomische Formel: } (a+b)^2 = a^2 + 2 \cdot a \cdot b + b^2 \ \} \\
& 8 \setminus (4 \cdot m^2 + 4 \cdot m + 1) - (4 \cdot n^2 + 4 \cdot n + 1) \\
\iff & \quad \{ \text{ Arithmetik } \} \\
& 8 \setminus (4 \cdot m^2 + 4 \cdot m) - (4 \cdot n^2 + 4 \cdot n) \\
\iff & \quad \{ \text{ Kürzungsregel (B.79a) } \} \\
& 2 \setminus m \cdot (m+1) - n \cdot (n+1) \\
\impliedby & \quad \{ \text{ Linearkombinationen (B.80) } \} \\
& 2 \setminus m \cdot (m+1) \ \wedge \ 2 \setminus n \cdot (n+1)
\end{array}
$$

B.5.20. Wir zeigen die Aussage für $a, b \in \mathbb{N}$; für die anderen vier Quadranten folgt die Aussage mit (B.74) und der Definition des Absolutwertes.

$$
\begin{array}{ll}
& a \setminus b \\
\iff & \quad \{ \text{ Definition »\«« (B.73) } \} \\
& \exists\, q \in \mathbb{Z} \,.\, q \cdot a = b \\
\iff & \quad \{ \text{ Annahmen: } a \geqslant 0,\ b > 0 \text{ und damit } q > 0; \text{ sei } q := r + 1 \ \} \\
& \exists\, r \in \mathbb{N} \,.\, (r+1) \cdot a = b \\
\iff & \quad \{ \text{ Arithmetik: Distributivgesetz } \} \\
& \exists\, r \in \mathbb{N} \,.\, r \cdot a + a = b \\
\implies & \quad \{ \text{ sei } d := r \cdot a \ \} \\
& \exists\, d \in \mathbb{N} \,.\, d + a = b \\
\iff & \quad \{ \text{ Definition »⩽« (B.51) } \} \\
& a \leqslant b
\end{array}
$$

B.6.6. Es gilt $x \cdot 1^* \leqslant \bot^* \cdot x$, aber nicht $x \cdot 1 \leqslant \bot \cdot x$.

B.6.7. Wir rechnen:

$$
\begin{array}{ll}
& (\mathrm{A} \cup 1)^* \\
= & \quad \{ \text{ Dekompositionsregel (B.116) } \} \\
& 1^* \cdot (\mathrm{A} \cdot 1^*)^* \\
= & \quad \{ \ 1^* = 1 \text{ (B.112) } \} \\
& \mathrm{A}^*
\end{array}
\qquad
\begin{array}{ll}
& \mathrm{A}^* \\
\subseteq & \quad \{ \ \mathrm{A} \subseteq (\mathrm{A} - \mathrm{P}) \cup \mathrm{P} \ \} \\
& ((\mathrm{A} - 1) \cup 1)^* \\
= & \quad \{ \text{ siehe links } \} \\
& (\mathrm{A} - 1)^* \\
\subseteq & \quad \{ \ \mathrm{A} - \mathrm{P} \subseteq \mathrm{A} \ \} \\
& \mathrm{A}^*
\end{array}
$$

Quellenangaben

- Seite 20: Auszug aus Johannes Widmann, »Mercantile Arithmetic« oder »Behende und hüpsche Rechenung auff allen Kauffmanschafft«, Leibzig: Konrad Kachelofen, Seite 60.
  https://de.wikipedia.org/wiki/Johannes_Widmann_(Mathematiker)
- Seite 20: Auszug aus Robert Recorde, »The whetstone of witte, whiche is the seconde parte of Arithmetike: containyng thextraction of Rootes: The Coßike practise, with the rule of Equation: and the woorkes of Surde Nombers«, Seite 238 (Seiten sind nicht nummeriert).
  http://blog.plover.com/math/recorde.html
- Seite 26: Sonnenblume, Bildnachweis: Luca Postpischi.
- Seite 26: Skulptur »Seed« von Peter Randall-Page, Bildnachweis: Marc Hill.
- Seite 37: George Boole,
  https://de.wikipedia.org/wiki/George_Boole
- Seite 37: Auszug aus George Boole, »The Mathematical Analysis of Logic, Being an Essay towards a Calculus of Deductive Reasoning«, London, England: Macmillan, Barclay, & Macmillan, 1847, Seite 56.
  https://books.google.com/books?id=zv4YAQAAIAAJ
- Seite 77: Ölgemälde von Giuseppe Peano, angefertigt im Jahre 1928 von Vittorio Bernardi (dem Ehemann von Peanos Schwester Rosa). Bildnachweis: aus Erika Luciano and Clara Silvia Roero (Herausgeber), »Giuseppe Peano Matematico e Maestro«, Torino, Università di Torino, 2008 (freundlicherweise zur Verfügung gestellt von Clara Silvia Roero).
- Seite 82: © Universitätsbibliothek der Humboldt-Universität zu Berlin, Porträtsammlung: Gottfried Wilhelm Leibniz (Verlag: Bibliogr. Inst. Hildburghausen).
- Seite 82: Auszug aus Godefroy-Guillaume Leibnitz. »Explication de l'arithmétique binaire, qui se sert des seuls caractères O et I avec des remarques sur son utilité et sur ce qu'elle donne le sens des anciennes figures chinoises de Fohy«, Mémoires de mathématique et de physique de l'Académie royale des sciences, Académie royale des sciences, 1703, Seite 86.
  https://hal.archives-ouvertes.fr/ads-00104781.
- Verkehrszeichen, Bildernachweis: Straßenverkehrs-Ordnung.
  https://de.wikipedia.org/wiki/Bildtafel_der_Verkehrszeichen_in_der_Bundesrepublik_Deutschland_seit_2017

Literaturverzeichnis

[Hin09] Ralf Hinze. Functional Pearl: The Bird tree. *Journal of Functional Programming*, 19(5):491–508, 2009.

[Kap00] Robert Kaplan. *Die Geschichte der Null.* Campus Verlag, 2000. ISBN 3593364271.

[KCR98] Revised^5 report on the algorithmic language Scheme. *Higher-Order and Symbolic Computation*, 11(1), August 1998.

[Knu97] Donald E. Knuth. *The Art of Computer Programming, Volume 1: Fundamental Algorithms.* Addison-Wesley Publishing Company, 3rd edition, 1997.

[Lei03] Godefroy-Guillaume Leibnitz. Explication de l'arithmétique binaire, qui se sert des seuls caractères O et I avec des remarques sur son utilité et sur ce qu'elle donne le sens des anciennes figures chinoises de Fohy. *Mémoires de mathématique et de physique de l'Académie royale des sciences*, 1703.

[Man74] Zohar Manna. *Introduction to Mathematical Theory of Computation.* McGraw-Hill, New York, 1974.

Index

Kursiv gesetzte Seitenzahlen verweisen auf die Definition des betreffenden Sachworts, mit einem Stern markierte Seitenzahlen referenzieren in Aufgaben. Die mathematischen Symbole sind zu Beginn aufgeführt und nach Themen geordnet, alphabetische Symbole bilden die zweite Gruppe und sind lexikalisch angeordnet.

Symbole

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

U

V

W

Y

Z

0–9

Inhaltsverzeichnis