Teil IV

Werte II

7. Quiz: Werte

Gegeben sei die Definition

let *not* = ***fun*** (*x* : *Bool*) → ***if*** *x* ***then*** *false* ***else*** *true*

Welche der folgenden Ausdrücke *sind* (nicht: haben) Werte?

Ja, ist ein Wert ⟸ *true*

7. Quiz: Werte

Gegeben sei die Definition

let *not* = ***fun*** (*x* : *Bool*) → ***if*** *x* ***then*** *false* ***else*** *true*

Welche der folgenden Ausdrücke *sind* (nicht: haben) Werte?

not ⟹ Nein, ist kein Wert

7. Quiz: Werte

Gegeben sei die Definition

let *not* = ***fun*** (*x* : *Bool*) → ***if*** *x* ***then*** *false* ***else*** *true*

Welche der folgenden Ausdrücke *sind* (nicht: haben) Werte?

not true ⟹ Nein, ist kein Wert

7. Quiz: Werte

Gegeben sei die Definition

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

Welche der folgenden Ausdrücke *sind* (nicht: haben) Werte?

. . . .

$\xleftarrow{\text{Ja, ist ein Wert}}$ $\boxed{\textbf{fun}\ (x : \mathit{Nat}) \to \mathit{not}}$

Streng genommen ist auch ***fun*** $(x : \mathit{Nat}) \to$ *not* kein Wert; ein Funktionsausdruck wertet ja zu einem Funktionsabschluss aus.

7. Quiz: Werte

Gegeben sei die Definition

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

Welche der folgenden Ausdrücke *sind* (nicht: haben) Werte?

. . . .

$\boxed{(\textbf{fun}\ (x : \mathit{Nat}) \to \mathit{not})\ 4711}$ $\xrightarrow{\text{Nein, ist kein Wert}}$

8. A tribute to Évariste Galois (1811–1832)

Der französische Mathematiker Évariste Galois starb früh im Alter von 20 Jahren bei einem Duell. Er erlangte postum Anerkennung durch seine Arbeiten zur Lösung algebraischer Gleichungen.

Sehr vage Idee: nutze 1-1 Beziehungen aus; definiere eine komplizierte Funktion durch eine einfache; löse ein kompliziertes Problem durch ein einfaches.

8. Was noch zu beweisen ist …

$$0 \leq \lfloor\sqrt{n+1}\rfloor - \lfloor\sqrt{n}\rfloor \leq 1$$
$$0 \leq \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\sqrt{n \div 4}\rfloor \leq 1$$

8. Boden und Decke: Definition

Definition von Boden und Decke:

$$n \leq \lfloor x \rfloor : \mathbb{Z} \iff n \leq x : \mathbb{R} \tag{1a}$$
$$\lceil x \rceil \leq n : \mathbb{Z} \iff x \leq n : \mathbb{R} \tag{1b}$$

für alle $n \in \mathbb{Z}$ und $x \in \mathbb{R}$.

Einfache Folgerungen:

- $\lfloor x \rfloor \leq x$;
- $n \leq \lfloor n \rfloor$ und damit $\lfloor n \rfloor = n$ und insbesondere $\lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor$;
- $x \leq \lceil x \rceil$;
- $\lceil n \rceil \leq n$ und damit $\lceil n \rceil = n$ und insbesondere $\lceil \lceil x \rceil \rceil = \lceil x \rceil$.

8. Boden und Decke: einfache Folgerungen

Kontraposition von (1a) und (1b):

$$\neg(n \leq \lfloor x \rfloor) : \mathbb{Z} \iff \neg(n \leq x) : \mathbb{R}$$
$$\neg(\lceil x \rceil \leq n) : \mathbb{Z} \iff \neg(x \leq n) : \mathbb{R}$$

Die Negation von $a \leq b$ ist $a > b$. Somit:

$$n > \lfloor x \rfloor : \mathbb{Z} \iff n > x : \mathbb{R}$$
$$\lceil x \rceil > n : \mathbb{Z} \iff x > n : \mathbb{R}$$

Ungleichungen zwischen ganzen Zahlen:

$$m + 1 \leq n : \mathbb{Z} \iff m < n : \mathbb{Z} \iff m \leq n - 1 : \mathbb{Z} \tag{3}$$

☞ Gleichungen gelten in $\mathbb{Z}$, nicht aber in $\mathbb{R}$. Insgesamt:

$$n \geq \lfloor x \rfloor + 1 : \mathbb{Z} \iff n > x : \mathbb{R}$$
$$\lceil x \rceil - 1 \geq n : \mathbb{Z} \iff x > n : \mathbb{R}$$

8. Boden und Decke: einfache Folgerungen

Kontraposition der Definitionen:

$$n \geq \lfloor x \rfloor + 1 : \mathbb{Z} \iff n > x : \mathbb{R} \tag{4a}$$
$$\lceil x \rceil - 1 \geq n : \mathbb{Z} \iff x > n : \mathbb{R} \tag{4b}$$

für alle $n \in \mathbb{Z}$ und $x \in \mathbb{R}$.

Einfache Folgerungen:

- $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$;
- $\lceil x \rceil - 1 < x \leq \lceil x \rceil$.

8. Division mit Rest: *div* und *mod*

Eigenschaften der Division mit Rest:

$$b \cdot (a \;\mathbf{div}\; b) + (a \;\mathbf{mod}\; b) = a \tag{5a}$$
$$0 \leq a \;\mathbf{mod}\; b < b \qquad \text{wenn } b > 0 \tag{5b}$$
$$b < a \;\mathbf{mod}\; b \leq 0 \qquad \text{wenn } b < 0 \tag{5c}$$

8. Division mit Rest: ***div*** und ***mod***

Definition der Division mit Rest: sei $b \neq 0$,

$$a \ \textbf{\textit{div}}\ b = \lfloor a/b \rfloor \tag{6a}$$
$$a \ \textbf{\textit{mod}}\ b = a - b \cdot \lfloor a/b \rfloor \tag{6b}$$

Beweis von (5b):

$$\begin{array}{ll} & 0 \leq a \ \textbf{\textit{mod}}\ b < b \\ \iff & \quad \{ \text{ Definition Rest (6b) } \} \\ & 0 \leq a - b \cdot \lfloor a/b \rfloor < b \\ \iff & \quad \{ \text{ Inverse } \textit{und } b > 0 \} \\ & \lfloor a/b \rfloor \leq a/b < \lfloor a/b \rfloor + 1 \\ \Longleftarrow & \quad \{ x := a/b \} \\ & \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \end{array}$$

8. Beweistechnik: indirekte Beweise

Indirekter Beweis für Gleichungen: zwei Elemente sind gleich, wenn sie mit allen anderen Elementen gleich interagieren.

$$a = b \iff (\forall x \,.\, x \leq a \iff x \leq b) \tag{7a}$$
$$a = b \iff (\forall x \,.\, b \leq x \iff a \leq x) \tag{7b}$$

Aus einem Gleichheitsbeweis wird ein Äquivalenzbeweis.

Indirekter Beweis für Ungleichungen:

$$a \leq b \iff (\forall x \,.\, x \leq a \implies x \leq b) \tag{7c}$$
$$a \leq b \iff (\forall x \,.\, b \leq x \implies a \leq x) \tag{7d}$$

8. Beispiel: Monotonie

Der Boden ist monoton:

$$x \leq y \implies \lfloor x \rfloor \leq \lfloor y \rfloor \tag{8}$$

Indirekter Beweis (7c):

$$\begin{array}{ll} & n \leq \lfloor x \rfloor \\ \iff & \quad \{ \text{ Definition Boden (1a) } \} \\ & n \leq x \\ \implies & \quad \{ \text{ Annahme: } x \leq y \} \\ & n \leq y \\ \iff & \quad \{ \text{ Definition Boden (1a) } \} \\ & n \leq \lfloor y \rfloor \end{array}$$

8. Beispiel: Boden und Addition

Interaktion von Boden und Addition:

$$\lfloor x + n \rfloor = \lfloor x \rfloor + n \tag{9}$$

Indirekter Beweis (7c):

$$\begin{array}{ll} & a \leq \lfloor x \rfloor + n \ : \ \mathbb{Z} \\ \iff & \quad \{ \text{ inverse Operationen } \} \\ & a - n \leq \lfloor x \rfloor \ : \ \mathbb{Z} \\ \iff & \quad \{ \text{ Definition Boden (1a) } \} \\ & a - n \leq x \ : \ \mathbb{R} \\ \iff & \quad \{ \text{ inverse Operationen } \} \\ & a \leq x + n \ : \ \mathbb{R} \\ \iff & \quad \{ \text{ Definition Boden (1a) } \} \\ & a \leq \lfloor x/n \rfloor \ : \ \mathbb{Z} \end{array}$$

☞ Gilt auch $\lfloor x \cdot n \rfloor = \lfloor x \rfloor \cdot n$? Nein! Wo läuft der Beweis schief?

8. Beispiel: $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$

Indirekter Beweis (7c):

$$\begin{array}{ll}
 & a \leq \lfloor \sqrt{\lfloor x \rfloor} \rfloor \\
\iff & \quad \{ \text{ Definition Boden (1a) } \} \\
 & a \leq \sqrt{\lfloor x \rfloor} \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & a^2 \leq \lfloor x \rfloor \lor a < 0 \\
\iff & \quad \{ \text{ Definition Boden (1a) } \} \\
 & a^2 \leq x \lor a < 0 \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & a \leq \sqrt{x} \\
\iff & \quad \{ \text{ Definition Boden (1a) } \} \\
 & a \leq \lfloor \sqrt{x} \rfloor
\end{array}$$

Somit gilt insbesondere $\lfloor \sqrt{n \div 4} \rfloor = \lfloor \sqrt{\lfloor n/4 \rfloor} \rfloor = \lfloor \sqrt{n/4} \rfloor$.

(Allgemeiner: $\lfloor f \lfloor x \rfloor \rfloor = \lfloor f\, x \rfloor$ wenn f stetig und streng monoton wachsend ist und weiterhin gilt, dass $f\, x \in \mathbb{Z} \implies x \in \mathbb{Z}$.)

8. Beweis: $0 \leq \lfloor \sqrt{n+1} \rfloor - \lfloor \sqrt{n} \rfloor$

$$\begin{array}{ll}
 & 0 \leq \lfloor \sqrt{n+1} \rfloor - \lfloor \sqrt{n} \rfloor \\
\iff & \quad \{ \text{ inverse Operationen } \} \\
 & \lfloor \sqrt{n} \rfloor \leq \lfloor \sqrt{n+1} \rfloor \\
\Longleftarrow & \quad \{ \text{ Monotonie des Bodens (8) } \} \\
 & \sqrt{n} \leq \sqrt{n+1} \\
\Longleftarrow & \quad \{ \text{ Monotonie der Wurzel } \} \\
 & n \leq n+1
\end{array}$$

☞ Gilt somit für alle monotonen Funktionen.

8. Beweis: $\lfloor \sqrt{n+1} \rfloor - \lfloor \sqrt{n} \rfloor \leq 1$

$$\begin{array}{ll}
 & \lfloor \sqrt{n+1} \rfloor - \lfloor \sqrt{n} \rfloor \leq 1 \\
\iff & \quad \{ \text{ inverse Operationen } \} \\
 & \lfloor \sqrt{n+1} \rfloor \leq \lfloor \sqrt{n} \rfloor + 1 \\
\iff & \quad \{ \text{ Boden und Addition (9) } \} \\
 & \lfloor \sqrt{n+1} \rfloor \leq \lfloor \sqrt{n} + 1 \rfloor \\
\Longleftarrow & \quad \{ \text{ Monotonie des Bodens (8) } \} \\
 & \sqrt{n+1} \leq \sqrt{n} + 1 \\
\Longleftarrow & \quad \{ \text{ Monotonie der Wurzel } \} \\
 & n+1 \leq (\sqrt{n}+1)^2 \\
\iff & \quad \{ \text{ Arithmetik } \} \\
 & 0 \leq n
\end{array}$$

Im vorletzten Schritt benutzen wir, dass $\sqrt{a^2} = a$ gdw $0 \leq a$.

8. Beweis: $0 \leq \lfloor \sqrt{n} \rfloor - 2 \cdot \lfloor \sqrt{n \div 4} \rfloor$

Zunächst einmal gilt $\lfloor \sqrt{n \div 4} \rfloor = \lfloor \sqrt{n/4} \rfloor$ (siehe oben) und $\sqrt{n/4} = \sqrt{n}/2$ (Potenzgesetze).

$$\begin{array}{ll}
 & 0 \leq \lfloor \sqrt{n} \rfloor - 2 \cdot \lfloor \sqrt{n}/2 \rfloor \\
\iff & \quad \{ \text{ inverse Operationen } \} \\
 & 2 \cdot \lfloor \sqrt{n}/2 \rfloor \leq \lfloor \sqrt{n} \rfloor \\
\iff & \quad \{ \text{ Definition Boden (1a) } \} \\
 & 2 \cdot \lfloor \sqrt{n}/2 \rfloor \leq \sqrt{n} \\
\iff & \quad \{ \text{ inverse Operationen } \} \\
 & \lfloor \sqrt{n}/2 \rfloor \leq \sqrt{n}/2 \\
\Longleftarrow & \quad \{ x := \sqrt{n}/2 \} \\
 & \lfloor x \rfloor \leq x
\end{array}$$

☞ Allgemein gilt: $0 \leq \lfloor a \rfloor - b \cdot \lfloor a/b \rfloor$ für $b \in \mathbb{Z}$ und $b > 0$.

8. Beweis: $\lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\sqrt{n \div 4}\rfloor \leq 1$

$$
\begin{array}{ll}
 & \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\sqrt{n}/2\rfloor \leq 1 \\
\Longleftarrow & \quad \{\ \text{Transitivität}\ \} \\
 & \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\sqrt{n}/2\rfloor \leq \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\lfloor\sqrt{n}\rfloor/2\rfloor \\
 & \quad \text{und} \quad \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\lfloor\sqrt{n}\rfloor/2\rfloor \leq 1 \\
\Longleftrightarrow & \quad \{\ \text{Antimonotonie und } \lfloor\sqrt{n}\rfloor \leq \sqrt{n}\ \} \\
 & \lfloor\sqrt{n}\rfloor - 2 \cdot \lfloor\lfloor\sqrt{n}\rfloor/2\rfloor \leq 1 \\
\Longleftarrow & \quad \{\ a := \lfloor\sqrt{n}\rfloor\ \} \\
 & a - 2 \cdot \lfloor a/2\rfloor \leq 1
\end{array}
$$