Korrekte Software durch Formale Methoden

Christoph Lüth

Wintersemester 1998/99

Die Sprache **IMP**

- Zahlen: $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$
- Wahrheitswerte: $\mathbf{T} = \{\mathbf{True}, \mathbf{False}\}$
- Variablen: **Loc**
- Arithmetische Ausdrücke: **Aexp**

$$a ::= n \mid X \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 * a_1$$

Die Sprache **IMP**

- Bool'sche Ausdrücke: **Bexp**

$$b ::= \textbf{True} \mid \textbf{False} \mid a_0 = a_1 \mid a_0 \leq a_1 \mid \neg b \mid b_0 \wedge b_1 \mid b_0 \vee b_1$$

- Kommandos: **Com**

$$\begin{array}{rl} c ::= & \textbf{skip} \mid X := a \mid c_0; c_1 \mid \\ & \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1\ \textbf{fi} \mid \textbf{while}\ b\ \textbf{do}\ c\ \textbf{done} \end{array}$$

Programming in **IMP**

$$
\begin{array}{ll}
\mathit{Fac} \equiv & M := 1; \\
& \textbf{while}\ 0 \leq N\ \textbf{do} \\
& \quad M := N * M; \\
& \quad N := N - 1 \\
& \quad \textbf{done}
\end{array}
\qquad
\begin{array}{ll}
\mathit{Euclid} \equiv & \textbf{while}\ \neg(M = N)\ \textbf{do} \\
& \quad \textbf{if}\ M \leq N \\
& \quad \textbf{then}\ N := N - M \\
& \quad \textbf{else}\ M := M - N\ \textbf{fi} \\
& \quad \textbf{done}
\end{array}
$$

Semantik von **IMP**

- **Loc** bezeichnet *symbolische Adressen*
- Systemzustand: $\mathbf{\Sigma} \stackrel{\textit{def}}{=} \mathbf{Loc} \rightharpoonup \mathbb{N}$
- Strukturelle Operationale Semantik:
  - Syntaxgesteuerte Auswertung
  - Relativ zu einem Systemzustand
  - Relation auf *Konfigurationen*: $\langle a, \sigma \rangle$

Operationelle Semantik von **IMP**: Arithmetische Ausdrücke

Zahlen: $\langle n, \sigma \rangle \to n$

Variablen: $\langle X, \sigma \rangle \to \sigma(X)$

Addition: $$\frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 + a_1, \sigma \rangle \to n + m}$$

Subtraktion: $$\frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 - a_1, \sigma \rangle \to n - m}$$

Multiplikation: $$\frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 * a_1, \sigma \rangle \to n * m}$$

Operationelle Semantik von **IMP**: Bool'sche Ausdrücke

$$\langle \textbf{True}, \sigma \rangle \to \top \qquad \langle \textbf{False}, \sigma \rangle \to \bot$$

$$\frac{\langle b, \sigma \rangle \to \bot}{\langle \neg b, \sigma \rangle \to \top} \qquad \frac{\langle b, \sigma \rangle \to \top}{\langle \neg b, \sigma \rangle \to \bot}$$

$$\frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 = a_1, \sigma \rangle \to \top} \ \texttt{if} \ n = m \qquad \frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 = a_1, \sigma \rangle \to \bot} \ \texttt{if} \ n \neq m$$

$$\frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 \leq a_1, \sigma \rangle \to \top} \ \texttt{if} \ n \leq m \qquad \frac{\langle a_0, \sigma \rangle \to n \quad \langle a_1, \sigma \rangle \to m}{\langle a_0 \leq a_1, \sigma \rangle \to \bot} \ \texttt{if} \ n > m$$

Operationelle Semantik von **IMP**: Bool'sche Ausdrücke

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \wedge b_1, \sigma\rangle \to \bot} \qquad \frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \wedge b_1, \sigma\rangle \to \bot}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \wedge b_1, \sigma\rangle \to \bot} \qquad \frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \wedge b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \vee b_1, \sigma\rangle \to \top} \qquad \frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \vee b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \vee b_1, \sigma\rangle \to \top} \qquad \frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \vee b_1, \sigma\rangle \to \bot}$$

Operationelle Semantik von **IMP**: Bool'sche Ausdrücke sequentiell

$$\frac{\langle b_0, \sigma\rangle \to \bot}{\langle b_0 \wedge b_1, \sigma\rangle \to \bot}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \wedge b_1, \sigma\rangle \to \bot} \qquad \frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \wedge b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \top}{\langle b_0 \vee b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \vee b_1, \sigma\rangle \to \top} \qquad \frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \vee b_1, \sigma\rangle \to \bot}$$

Operationelle Semantik von **IMP**: Anweisungen

$$\langle \textbf{skip}, \sigma\rangle \to \sigma$$

$$\frac{\langle a, \sigma\rangle \to n}{\langle X := a, \sigma\rangle \to \sigma[m/X]} \qquad \frac{\langle c_0, \sigma\rangle \to \tau \quad \langle c_1, \tau\rangle \to \tau'}{\langle c_0; c_1, \sigma\rangle \to \tau'}$$

$$\frac{\langle b, \sigma\rangle \to \top \quad \langle c_0, \sigma\rangle \to \tau}{\langle \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1\ \textbf{fi}, \sigma\rangle \to \tau} \qquad \frac{\langle b, \sigma\rangle \to \bot \quad \langle c_1, \sigma\rangle \to \tau}{\langle \textbf{if}\ b\ \textbf{then}\ c_0\ \textbf{else}\ c_1\ \textbf{fi}, \sigma\rangle \to \tau}$$

$$\frac{\langle b, \sigma\rangle \to \bot}{\langle \textbf{while}\ b\ \textbf{do}\ c\ \textbf{done}, \sigma\rangle \to \sigma}$$

$$\frac{\langle b, \sigma\rangle \to \top \quad \langle c, \sigma\rangle \to \tau' \quad \langle \textbf{while}\ b\ \textbf{do}\ c\ \textbf{done}, \tau'\rangle \to \tau}{\langle \textbf{while}\ b\ \textbf{do}\ c\ \textbf{done}, \sigma\rangle \to \tau}$$

- Induktion über Herleitung
- Strukturelle Induktion über Termaufbau.
- Wohlfundierte Induktion (Noether'sche Induktion):

  Relation $\prec \subset X \times X$ ist *wohlfundiert* wenn es keine unendlichen absteigenden Ketten $x_0 \prec x_1 \prec x_2 \prec x_3 \prec \ldots$ gibt *oder* jede nichtleere Teilmenge $Q \subseteq X$ hat ein minimales Element.

  Wohlfundierte Induktion:

$$\forall x \in X. P(x) \Leftrightarrow \forall x. (\forall y \prec x. P(y)) \Rightarrow P(x)$$

Erweiterung von **IMP**: **TINY**

- **TINY**: Ein/Ausgabe, Fehlerbehandlung.
- Systemzustand:

$$
\begin{aligned}
\Sigma &\stackrel{\mathit{def}}{=} \mathbf{Mem} \times \mathbb{N}^* \times \mathbb{N}^* \\
\mathbf{Mem} &\stackrel{\mathit{def}}{=} \mathbf{Loc} \rightharpoonup (\mathbb{N} + \{u\})
\end{aligned}
$$

- Auswertung: $\langle c, \sigma \rangle \to \Sigma + \{e\}$
- Zusätzliche Regeln für Fehlerpropagation, Eingabe, Ausgabe.