Korrekte Software durch Formale

Christoph Lüth

Wintersemester 1998/99

Die Sprache **IMP**

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

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

- Bool'sche Ausdrücke: **Bexp**

  $b ::= \texttt{True} \mid \texttt{False} \mid a_0 \texttt{ = } a_1 \mid a_0 \texttt{ <= } a_1 \mid \texttt{not } b \mid b$

- Kommandos: **Com**

  $$c ::= \texttt{skip} \mid X := a \mid c_0; c_1 \mid$$
  $$\texttt{if } b \texttt{ then } c_0 \texttt{ else } c_1 \texttt{ fi} \mid \texttt{while } b \texttt{ c}$$

Programming in **IMP**

$Fac \equiv$

```
M := 1;
while 0 < N do
  M:= N* M;
  N:= N- 1
done
```

$Euclid \equiv$

```
while (not
  if (M<= N
  then N:=
  else M:=
  fi
done
```

Semantik von **IMP**

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

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

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

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

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

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

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

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

$$\frac{\langle b, \sigma \rangle \to \bot}{\langle \texttt{not}\ \ b, \sigma \rangle \to \top} \qquad \frac{\langle b, \sigma \rangle \to \top}{\langle \texttt{not}\ \ b, \sigma \rangle \to \bot}$$

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

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

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \texttt{ and } b_1, \sigma\rangle \to \bot}$$

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle -}{\langle b_0 \texttt{ and } b_1, \sigma\rangle \to \bot}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \bot}{\langle b_0 \texttt{ and } b_1, \sigma\rangle \to \bot}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle -}{\langle b_0 \texttt{ and } b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \texttt{ or } b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \top \quad \langle b_1, \sigma\rangle -}{\langle b_0 \texttt{ or } b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle \to \top}{\langle b_0 \texttt{ or } b_1, \sigma\rangle \to \top}$$

$$\frac{\langle b_0, \sigma\rangle \to \bot \quad \langle b_1, \sigma\rangle -}{\langle b_0 \texttt{ or } b_1, \sigma\rangle \to \bot}$$

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

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

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

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

Operationelle Semantik von **IMP**: Anweisungen

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

$$\frac{\langle a, \sigma \rangle \to n}{\langle X := a, \sigma \rangle \to \sigma[n/X]}$$

$$\frac{\langle c_0, \sigma \rangle \to \tau \quad \langle c_1, \tau \rangle}{\langle c_0;\ c_1, \sigma \rangle \to \tau'}$$

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

$$\frac{\langle b, \sigma \rangle \to \bot \quad \langle c}{\langle \texttt{if}\ b\ \texttt{then}\ c_0\ \texttt{else}}$$

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

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

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

  Relation $\prec \subset X \times X$ ist *wohlfundiert* wenn es kein steigenden Ketten $x_0 \prec x_1 \prec x_2 \prec x_3 \prec \ldots$ gibt *od* Teilmenge $Q \subseteq X$ hat ein minimales Element.

  Wohlfundierte Induktion:

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

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

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

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

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