Vorlesung vom 02.05.06: Korrektheit des Hoare-Kalküls

Wo sind wir?

- *Letze Woche*: Erinnerungen an den Hoare-Kalkül
- *Diese Woche*: Korrektheit des Hoare-Kalküls
- *Nächste Woche*: Vollständigkeit des Hoare-Kalküls

Fahrplan

Korrektheit des Hoare-Kalküls: $\{A\}c\{B\}$ *ableitbar* wenn *gültig*.

1. Genaue Definition von $\{A\}c\{B\}$: Vor- & Nachbedingung: *Zusicherungen*
2. Definition von *Ableitbarkeit* $\vdash \{A\}c\{B\}$
3. Definition von *Gültigkeit* $\models \{A\}c\{B\}$:
   - Gültigkeit von *Zusicherungen* $\sigma \models A$ in *Zustand* σ
   - $\models \{A\}c\{B\}$ gdw: wenn A in Zustand σ gilt, dann gilt B im Zustand nach Ausführung von c
   - Dazu: Zustandsübergang $\longrightarrow$ *denotationelle Semantik*

Die Sprache IMP (Wiederholung)

- *Zahlen*: $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$
- *Variablen*: **Loc**
- *Arithmetische* Ausdrücke: $a \in$ **Aexp**

  $a ::= n \mid x \mid a + a \mid a - a \mid a * a \qquad n \in \mathbf{N}, x \in \mathbf{Loc}$
- *Boolsche* Ausdrücke: $b \in$ **Bexp**

  $b ::= \texttt{True} \mid \texttt{False} \mid a = a \mid a \texttt{<=} a \mid \texttt{not}\ b \mid b \texttt{ and } b \mid b \texttt{ or } b$
- *Anweisungen*:

  Com$c ::= \texttt{skip} \mid x := a \mid c; c \mid$
  $\texttt{if}\ b\ \texttt{then}\ c\ \texttt{else}\ c\ \texttt{fi} \mid \texttt{while}\ b\ \texttt{do}\ c\ \texttt{od}$

Bedeutung von IMP

- *Operationale* Semantik: $\longleftarrow$ *FMSE I*
  - *Syntaxgesteuerte* Ableitungsregeln (Zustandsübergang)
  - Für: *Sprachdefinition*, *Compilerverifikation*
- *Denotationale* Semantik: $\longleftarrow$ *FMSE I*
  - Abbildung $\mathcal{D}$: **Com** $\rightarrow \mathcal{S}$ in *semantischen Bereich*
  - Für: *Programmentwicklung* und *Programmtransformation*
- *Axiomatische* Semantik:
  - *Vor-* und *Nachbedingungen* für jede Anweisung
  - Für: *Programmverifikation*

Denotationale Semantik für IMP

- Programm als *Funktion zwischen Systemzuständen*
- *Systemzustand*: $\Sigma \stackrel{def}{=}$ **Loc** $\rightharpoonup \mathbb{N}$
- Semantische *Funktionen*:
  - Arithmetische Ausdrücke: $\mathcal{E}$: **Aexp** $\rightarrow (\Sigma \rightarrow \mathbb{N})$
  - Boolsche Ausdrücke: $\mathcal{B}$: **Bexp** $\rightarrow (\Sigma \rightarrow Bool)$
  - Anweisungen: $\mathcal{D}$: **Com** $\rightarrow (\Sigma \rightharpoonup \Sigma)$

Denotationale Semantik für IMP: Anweisungen

$$
\begin{aligned}
\mathcal{C}[\![\texttt{skip}]\!] &\stackrel{def}{=} \lambda\sigma^{\Sigma}.\sigma \\
\mathcal{C}[\![X := a]\!] &\stackrel{def}{=} \lambda\sigma^{\Sigma}.\sigma[\mathcal{E}[\![a]\!]\sigma/X] \\
\mathcal{C}[\![c_0; c_1]\!] &\stackrel{def}{=} \mathcal{C}[\![c_1]\!] \circ \mathcal{C}[\![c_0]\!] \\
\mathcal{C}[\![\texttt{if}\ b\ \texttt{then}\ c_0\ \texttt{else}\ c_1\ \texttt{fi}]\!] &\stackrel{def}{=} \lambda\sigma^{\Sigma}.\begin{cases} \mathcal{C}[\![c_0]\!]\sigma & \mathcal{B}[\![b]\!]\sigma = true \\ \mathcal{C}[\![c_1]\!]\sigma & \mathcal{B}[\![b]\!]\sigma = false \end{cases} \\
\mathcal{C}[\![\texttt{while}\ b\ \texttt{do}\ c\ \texttt{od}]\!] &\stackrel{def}{=} \mathit{fix}\ \Gamma \\
\text{mit } \Gamma(\phi) &\stackrel{def}{=} \lambda\sigma^{\Sigma}.\begin{cases} \phi \circ \mathcal{C}[\![c]\!]\sigma & \mathcal{B}[\![b]\!]\sigma = true \\ \sigma & \mathcal{B}[\![b]\!]\sigma = false \end{cases}
\end{aligned}
$$

Zusicherungen

- Warum nicht einfach *boolsche Ausdrücke*?
- Menge von *Variablen*: **Intvar**(*logische* Variablen, vgl. **Loc**)
- Erweiterte *arithmetische Ausdrücke* **Aexpv**

  $a ::= i \mid n \mid x \mid a + a \mid a - a \mid a * a \quad i \in \mathbf{Intvar}, n \in \mathbf{N}, x \in \mathbf{Loc}$
- Zusicherungen sind erweiterte *boolsche Ausdrücke* **Assn**:

  $b ::= \texttt{True} \mid \texttt{False} \mid a = a \mid a \texttt{<=} a \mid \texttt{not}\ b \mid b \texttt{ and } b \mid$
  $b \texttt{ or } b \mid b \Rightarrow b \mid \forall i.b \mid \exists i.b$
- Substitution:
  - $a\,[a'/i]$ ($a' \in$ **Aexpv**, $a \in$ **Aexp**, $i \in$ **Intvar**)
  - $b\,[a/i]$ ($b \in$ **Assn**, $a \in$ **Aexp**, $i \in$ **Intvar**)
  - Definiert durch strukturelle Induktion.

Semantik von Zusicherungen

- *Problem*: Wie interpretieren wir *Variablen*?
- Eine *Interpretation* ist I : **Intvar** $\to \mathbb{N}$
- Auswertungen mit Interpretationen:
  - Funktion $\mathcal{A}$: **Aexpv** $\to$ (**Intvar** $\to \mathbb{N}) \to (\Sigma \to \mathbb{N})$
  - Prädikat $\sigma \models^I A$ für $A \in$ **Assn**

Semantik von Zusicherungen

- $\mathcal{A}$ definiert durch strukturelle Induktion:

$$\begin{aligned} \mathcal{A}[\![n]\!]^I_\sigma &= n \\ \mathcal{A}[\![X]\!]^I_\sigma &= \sigma(X) \\ \mathcal{A}[\![i]\!]^I_\sigma &= I(i) \\ \mathcal{A}[\![a_0 \texttt{ + } a_1]\!]^I_\sigma &= \mathcal{A}[\![a_0]\!]^I_\sigma + \mathcal{A}[\![a_1]\!]^I_\sigma \\ &\ldots \end{aligned}$$

- *Lemma:* Für $a, a_0 \in$ **Aexpv**, $X \in$ **Loc** und alle $\sigma \in \Sigma$:

$$\mathcal{A}[\![a_0[a/X]]\!]^I_\sigma = \mathcal{A}[\![a_0]\!]^I_{\sigma[\mathcal{A}[\![a]\!]^I_\sigma/X]}$$

- *Lemma:* Für $b \in$ **Assn**, $X \in$ **Loc**, $a \in$ **Aexp** und alle $\sigma \in \Sigma$:

$$\sigma \models^I B[a/X] \Longleftrightarrow \sigma[\mathcal{E}[\![a]\!]\sigma/X] \models^I B$$

Semantik von Zusicherungen

*Def (*Erfüllbarkeit von Zusicherungen*):* Mit $\sigma : \Sigma_\perp$, I : **Intvar** $\to \mathbb{N}$:

$$\begin{array}{ll} \sigma \models^I \texttt{True} & \\ \sigma \models^I a_0 \texttt{ = } a_1 & \text{if } \mathcal{A}[\![a_0]\!]^I_\sigma = \mathcal{A}[\![a_1]\!]^I_\sigma \\ \sigma \models^I a_0 \texttt{ <= } a_1 & \text{if } \mathcal{A}[\![a_0]\!]^I_\sigma \leq \mathcal{A}[\![a_1]\!]^I_\sigma \\ \sigma \models^I b_0 \texttt{ and } b_1 & \text{if } \sigma \models^I b_0 \wedge \sigma \models^I b_0 \\ \sigma \models^I b_0 \texttt{ or } b_1 & \text{if } \sigma \models^I b_0 \vee \sigma \models^I b_0 \\ \sigma \models^I \texttt{not } b & \text{if } \neg\sigma \models^I b \\ \sigma \models^I b_0 \Rightarrow b_1 & \text{if } \sigma \models^I b_0 \Longrightarrow \sigma \models^I b_0 \\ \sigma \models^I \forall i.b & \text{if } \sigma \models^{I[n/i]} b \text{ for all } n \in N \\ \sigma \models^I \exists i.b & \text{if } \sigma \models^{I[n/i]} b \text{ for some } n \in N \\ \perp \models^I a & \end{array}$$

Gültigkeit

*Def (*Satisfaction Relation, Gültigkeit*):* Für Interpretation I, $\sigma \in \Sigma_\perp$:

$$\sigma \models^I \{A\}c\{B\} \Longleftrightarrow (\sigma \models^I A \Longrightarrow \mathcal{C}[\![c]\!]\sigma \models^I B)$$

$$\models^I \{A\}c\{B\} \Longleftrightarrow \forall \sigma : \Sigma_\perp . \sigma \models^I \{A\}c\{B\}$$

$$\models \{A\}c\{B\} \Longleftrightarrow \forall I. \models^I \{A\}c\{B\}$$

Analog für *Zusicherungen* A ($\models A$ etc.)

NB. *Gültigkeit* im Gegensatz zum *herkömmlichen Modellbegriff*.

Beispiel: $\models A \Longrightarrow B$, $\models \{A\}c\{B\}$.

Korrektheit des Hoare-Kalküls

*Def (*Herleitbarkeit*):* $\vdash \{A\}c\{B\}$ durch die Regeln des Hoare-Kalküls

*Satz (*Korrektheit des Hoare-Kalküls*):*

Wenn $\vdash \{A\}c\{B\}$, dann $\models \{A\}c\{B\}$.

Beweis: Fallunterscheidung über den Regeln.

- $c \equiv X := a$
- $c \equiv c_0; c_1$
- $c \equiv$ `if` b `then` c_0 `else` c_1 `fi`
- $c \equiv$ `while` b `do` c `od`
- Implikationsregel

Zusammenfassung

- Heute: *Korrektheit* des Hoare-Kalküls
- Dazu:
  - Zusicherungen **Assn**, syntaktische *Herleitbarkeit*
  - Interpretationen, semantische *Gültigkeit*
  - Korrektheit: Herleitbarkeit impliziert Gültigkeit
- Nächste Woche: *Vollständigkeit* — Gültigkeit impliziert Herleitbarkeit