Vorlesung vom 09.05.06: Vollständigkeit des Hoare-Kalküls

Wo sind wir?

- *Voretze Woche*: Erinnerungen an den Hoare-Kalkül
- *Letzte Woche*: Korrektheit des Hoare-Kalküls
- *Diese Woche*: Vollständigkeit des Hoare-Kalküls
- *Nächste Woche*: Verifikationsbedingungen und Prädikatentransformer

Vollständigkeit des Hoare-Kalküls

- *Korrektheit*: wir können *nur wahre* Folgerungen ableiten
- *Vollständigkeit*: wir können *alle wahren* Folgerungen ableiten
- *Satz (*Unvollständgkeit des Hoare-Kalküls*):* Es kann *keinen korrekten, vollständigen* Beweiskalkül für den Hoare-Kalkül geben.

  Beweis: Vollständiger Beweiskalkül würde Termination entscheiden: $\models \{\texttt{True}\}c\{\texttt{False}\}$ gilt gdw. c divergiert.
- *Satz (*Unvollständigkeit für **Assn***):* Es kann *keinen korrekten, vollständigen* Beweiskalkül für **Assn**geben.
- Aber *relative* Vollständigkeit beweisbar:
  Wenn $\models \{A\}c\{B\}$, dann $\vdash \{A\}c\{B\}$.

Schwächste Vorbedingung

*Def (*Schwächste Vorbedingung*):* Für $c \in$ **Com**, $B \in$ **Assn**, Interpret. I:

$$wp^I[\![c, b]\!] = \{\sigma \in \Sigma_\perp \mid \mathcal{C}[\![c]\!]\sigma \models^I B\}$$

- Wenn es A_0 gibt so dass für alle I $A_0^I = wp^I[\![c, b]\!]$, dann $\models \{A\}c\{B\}$ gdw $\models A \Longrightarrow A_0$.
- Gibt es so ein A_0?

*Def (*Expressivität*):* **Assn** ist expressiv, wenn es so ein A_0 für gibt.

Gödel's β-Prädikat

- Modulus in **Assn**: $x = a \mod b$ ist
  $a \geq 0 \wedge b \geq 0 \wedge \exists k.(k \geq 0 \wedge k * b \geq a \wedge (k+1) * b > a \wedge x = a - (k * b)$
- *Def (*Prädikat β*):*

$$\beta(a, b, i, x) \Longleftrightarrow x = a \mod (1 + (1 + i) * b)$$

- *Lemma:* Für Folge $n_0, \ldots, n_k$ gibt es $n, m \in \mathbb{N}$ so dass für alle j, $0 \leq j \leq k$ und x:

$$\beta(n, m, j, x) \Longleftrightarrow x = n_j$$

- *Kodierung* von *Folgen*
- Technisches Detail: **IMP** hat ganze Zahlen (aber $\mathbb{N} \cong \mathbb{Z}$)

Expressivität von Assn

*Satz (*Expressivität*):* Für $c \in$ **Com**, $B \in$ **Assn** gibt es $w[\![c, b]\!] \in$ **Assn** so dass für alle I

$$wp^I[\![c, B]\!] = w[\![c, B]\!]$$

Beweis: Konstruktion von $w[\![c, B]\!]$ durch Induktion über c:

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

Expressivität von Assn

Lemma: Für $w \equiv \texttt{while}\ b\ \texttt{do}\ c\ \texttt{od}$:

$$\begin{array}{lll} \mathcal{C}[\![w]\!]\sigma = \sigma' & \text{gdw} & \mathcal{B}[\![b]\!]\sigma = \mathit{false} \wedge \sigma = \sigma' \\ & & \vee \\ & & \exists \sigma_0, \ldots, \sigma_n \in \Sigma. \\ & & \sigma = \sigma_0 \wedge \sigma' = \sigma_n \wedge \mathcal{B}[\![b]\!]\sigma_n = \mathit{false} \wedge \\ & & \forall i. 0 \leq i \leq n \Longrightarrow \mathcal{B}[\![b]\!]\sigma_i = \mathit{true} \wedge \mathcal{C}[\![c]\!]\sigma_i = \sigma_{i+1} \end{array}$$

Vollständigkeit

Lemma: Für $c \in$ **Com**, $B \in$ **Assn**, sei $w[\![c, B]\!]$ *eine* schwächste Vorbedingung, dann $\vdash \{w[\![c, b]\!]\}c\{B\}$.

Beweis: Induktion über c. □

*Satz (*Relative Vollständigkeit des Hoare-Kalküls*):*

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

Beweis: Wenn $\models \{A\}c\{B\}$, dann $\vdash \{w[\![c, b]\!]\}c\{B\}$, also mit $\models A \Longrightarrow w[\![c, b]\!]$ folgt $\models \{A\}c\{B\}$ (Folgerungsregel). □

Zusammenfassung

- *Allgemeine* Vollständigkeit *unmöglich* (wenn Kalkül konsistent), da **Assn** zu mächtig.
- Daher: Beweis der *relativen Vollständigkeit*
- Beweise beruht auf
  - schwächster Vorbedingung $wp^I[\![c, B]\!]$: Menge der Zustände, die B nach Ausführung von c wahr machen
  - *Expressivität* von **Assn**: schwächste Vorbedingung als Zusicherung $w[\![c, B]\!]$ ausdrückbar
- Beweis konstruiert $w[\![c, B]\!]$, aber *nicht praktisch nutzbar*.