

## Übungen zu „Semantik von Programmiersprachen“, WS 2004/05

Nr. 9, Besprechung mündlicher Aufgaben: 10. Januar 2005 in der Übung,

Abgabe der Hausaufgaben: 12. Januar 2005 vor der Vorlesung

---

### Mündliche Aufgaben

9.1 Leiten Sie mit Hilfe der Hoare-Regeln her:

```
{X = n ∧ Y = m ∧ Z = 1}
while ¬(Y = 0) do
  (while even(Y) do (X := X * X; Y := Y/2);
   Z := Z * X;
   Y := Y - 1)
{Z = n^m}
```

Dabei verwenden wir ganzzahlige Division als Erweiterung der arithmetischen Ausdrücke sowie ein Prädikat *even*, das angibt, ob eine Zahl gerade ist.

### 9.2 Totale Korrektheitsaussagen

Das Prinzip der axiomatischen Semantik lässt sich erweitern, um auch Aussagen über die Termination eines Programms zu machen.

Seien  $P, Q \in \mathbf{Assn}$ ,  $c \in \mathbf{Cmd}$ . Wir definieren:

- Eine Aussage der Form  $\{P\} c \{\Downarrow Q\}$  heißt *totale Korrektheitsaussage*.
- $\{P\} c \{\Downarrow Q\}$  heißt *gültig*, falls für alle  $\sigma \in \Sigma$  und alle  $I \in \mathcal{I}$  gilt:

$$\sigma \models^I P \leadsto \exists \sigma' \in \Sigma : \langle c, \sigma \rangle \rightarrow \sigma' \wedge \sigma' \models^I Q$$

- Zur Herleitung von totalen Korrektheitsaussagen wird eine Hoare-Regel für **while** definiert, in der die Schleifeninvariante  $P$  mit einer logischen Variablen  $n \in \mathbb{N}$  parametrisiert ist.

$$\frac{\models P(n+1) \Rightarrow b \quad \{P(n+1)\} c \{\Downarrow P(n)\} \quad \models P(0) \Rightarrow \neg b}{\{\exists n. P(n)\} \text{ while } b \text{ do } c \{\Downarrow P(0)\}}$$

Die übrigen Hoare-Regeln werden für totale Korrektheitsaussagen lediglich mit dem Zeichen  $\Downarrow$  in der Nachbedingung ergänzt.

Formulieren Sie totale Korrektheitsaussagen für die folgenden Schleifen im Sinne dieser Definition und geben Sie geeignete parametrisierte Schleifeninvarianten an:

- (a) **while**  $\neg(X = 1)$  **do**  $(Y := Y * X; X := X - 1)$  Fakultät, vgl. Vorlesung
- (b) **while**  $\neg(Y = 0)$  **do**  $(Y := Y - 1; X := 2 * X)$  Potenzfunktion, vgl. Aufg. 8.2

Bitte wenden!

## Schriftliche Aufgaben

- 9.3 Finden Sie eine Zusicherung  $C \in \mathbf{Assn}$ , die äquivalent zur schwächsten Vorbedingung der Zusicherung  $Y = i! \wedge i \geq 0$  bezüglich der Anweisung

5 Punkte

**while**  $\neg(X = 1)$  **do**  $(Y := Y * X; X := X - 1)$

ist, d.h. beweisen Sie, dass für alle Interpretationen  $I \in \mathcal{I}$  gilt:

$$C^I = \mathbf{wp}^I[\mathbf{while} \neg(X = 1) \mathbf{do} (Y := Y * X; X := X - 1), Y = i! \wedge i \geq 0].$$

- 9.4 (a) Definieren Sie analog zur schwächsten Vorbedingung das Konzept der *stärksten Nachbedingung*  $\mathbf{sp}^I[A, c] \subseteq \Sigma_{\perp}$  einer Zusicherung  $A \in \mathbf{Assn}$  bezüglich einer Anweisung  $c \in \mathbf{Com}$  unter einer Interpretation  $I \in \mathcal{I}$ .

7 Punkte

- (b) Zeigen Sie, dass für alle  $A, B \in \mathbf{Assn}$ ,  $c \in \mathbf{Com}$  und  $I \in \mathcal{I}$  gilt:

$$\models^I \{A\}c\{B\} \text{ gdw. } \mathbf{sp}^I[A, c] \subseteq B^I.$$

- (c) Zeigen Sie, dass für alle  $A, B, B_0 \in \mathbf{Assn}$  und  $c \in \mathbf{Com}$  mit  $B_0^I = \mathbf{sp}^I[A, c]$  für alle  $I \in \mathcal{I}$  gilt:

$$\models \{A\}c\{B\} \text{ gdw. } \models (B_0 \Rightarrow B).$$