PHILIPPS-UNIVERSITÄT MARBURG
Fachbereich Mathematik und Informatik
Prof. Dr. R. Loogen
Dipl.-Inform. Jost Berthold

D-35032 Marburg
Hans Meerwein Straße
Lahnberge
10. Juni 2003

Übungen zur „Semantik von Programmiersprachen“, SS 2003

Nr. 6, Besprechung der mündlichen Aufgaben: 13. Juni in der Übung, Abgabe der Hausaufgaben: 17. Juni in der Vorlesung

A. Mündliche Aufgaben

6.1 Gödelisierung

(a) Seien $k \geq 1, n_0, .., n_k$ eine Folge natürlicher Zahlen und $m := (\max\{k, n_0, .., n_k\})!$. Zeigen Sie, dass die Zahlen $p_i = 1 + (1 + i) * m$ mit $0 \leq i \leq k$ co-prim sind, d.h. dass für $i \neq j$ der größte gemeinsame Teiler von p_i und p_j gleich 1 ist, und dass $n_i < p_i$.

(b) Sei für $0 \leq i \leq k$: $c_i := p_0 * \ldots * p_k / p_i$. Zeigen Sie, dass für alle i, $0 \leq i \leq k$, ein eindeutiges d_i mit $0 \leq d_i < p_i$ existiert, so dass $(c_i * d_i) \bmod p_i = 1$.

(c) Sei ferner $n := \sum_{i=0}^{k} c_i * d_i * n_i$. Zeigen Sie, dass für alle $0 \leq i \leq k$ gilt:

$$n_i = n \bmod p_i.$$

(d) Beweisen Sie Lemma 5.2 der Vorlesung.

B. Hausaufgaben

Die Abgabe der Hausaufgaben ist in Zweiergruppen erlaubt.

6.2 Bestimmen 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

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

ist, d.h. für alle Interpretationen $I \in \mathcal{I}$ soll gelten:

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

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

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