Ludwig-Maximilians-Universität München
Institut für Informatik
Prof. Dr. A. Knapp

WS 2006/07
Blatt 11

Übungen zu Semantik von Programmiersprachen

Aufgabe 41 Partielle Korrektheit (4 Punkte)

Geben Sie eine Ableitung des Hoare-Tripels

$$\{\mathtt{x} = M \wedge \mathtt{y} = N \wedge M \geq 0 \wedge N > 0\}$$
`z := 0; while y <= x do x := x-y; z := z+1`
$$\{\mathtt{z} = M \operatorname{div} N \wedge \mathtt{x} = M \bmod N\}$$

im Hoare-Kalkül für partielle Korrektheit an.

Aufgabe 42 Hoare-Kalkül und natürliche Semantik von **IMP** (4 Punkte)

Ein Hoare-Tripel $\{A\}\, S\, \{A'\}$ heißt *gültig bzgl. der natürlichen Semantik* von **IMP**, falls gilt:

$$\forall I \in \mathit{Val}\,.\, \forall \sigma, \sigma' \in \Sigma\,.\, (I, \sigma \models A \wedge \langle S, \sigma \rangle \to \sigma' \Rightarrow I, \sigma' \models A')$$

Zeigen Sie die Korrektheit der Regeln $(\mathrm{seq}_{\mathrm{hp}})$ und $(\mathrm{while}_{\mathrm{hp}})$ des Hoare-Kalküls für partielle Korrektheit für die Gültigkeit bzgl. der natürlichen Semantik von **IMP**, ohne den Korrektheitssatz für den Hoare-Kalkül für partielle Korrektheit bzgl. der denotationellen Semantik von **IMP** zu benutzen.

Aufgabe 43 Hoare-Kalkül für Variablendeklarationen

Erweitern Sie den Hoare-Kalkül für partielle Korrektheit auf die Sprache **IMP** mit Variablendeklarationen der Form `newvar` x `:=` a `in` S.

Aufgabe 44 β-Prädikat

Sei das Prädikat $\beta(a, b, i, x)$ über den natürlichen Zahlen definiert durch:

$$\beta(a, b, i, x) \iff (x = a \bmod (1 + (1 + i) \cdot b))$$

Sei $n_0, \ldots, n_k$ eine Folge natürlicher Zahlen. Zeigen Sie:

a) Sei $m = (\max\{k, n_0, \ldots, n_k\})!$. Dann sind die Zahlen $p_i = 1 + (1 + i) \cdot m$ mit $0 \leq i \leq k$ paarweise teilerfremd und es gilt $n_i < p_i$ für alle $0 \leq i \leq k$.

b) Sei weiter $c_i = (p_0 \cdots p_k)/p_i$ für $0 \le i \le k$. Dann gibt es für alle $0 \le i \le k$ ein eindeutig bestimmtes d_i mit $0 \le d_i < p_i$, sodaß $(c_i \cdot d_i) \bmod p_i = 1$.

c) Sei weiter $n = \sum_{i=0}^{k} c_i \cdot d_i \cdot n_i$. Dann gilt $n_i = n \bmod p_i$ für alle $0 \le i \le k$.

d) Es gibt natürliche Zahlen m und n, sodaß für alle $0 \le i \le k$ und alle natürlichen Zahlen x gilt: $\beta(n, m, i, x) \iff x = n_i$.

Abgabe und Besprechung: Mittwoch, 7.2.2007