PHILIPPS-UNIVERSITÄT MARBURG
Fachbereich Mathematik und Informatik
Prof. Dr. R. Loogen
Dipl.Inf. J.Berthold

D-35032 Marburg
Hans Meerwein Straße

15. Dezember 2004

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

Nr. 8, Besprechung mündlicher Aufgaben: 3. Januar 2005 in der Übung,
Abgabe der Hausaufgaben: 5. Januar 2005 vor der Vorlesung

Hinweise: In der Woche ab dem 20.12.2004 entfallen Vorlesung und Tutorium.
Abgabe und Besprechung der mündlichen Aufgaben erfolgen erst in 2005.

Mündliche Aufgaben

8.1 Leiten Sie die folgenden Aussagen mithilfe der Hoare-Regeln für IMP her:

(a) { **true** } **while true do skip** { **true** }

(b) { **false** } **skip** $\{P\}$ für beliebige $P \in$ **Assn**

Wie sind diese Aussagen bzgl. der Gültigkeit $\models$ zu interpretieren?

(c) Zeigen Sie: $\vdash \{P\}\ S$ { **true** } für beliebige $P \in$ **Assn** , $S \in$ **Cmd**

8.2 Bestimmen Sie geeignete Invarianten, mit deren Hilfe sich die folgenden partiellen Korrektheitsaussagen nachweisen lassen:

(a) $\{Y = i \wedge X = 1\}$
while $\neg(Y = 0)$ **do** $(Y := Y - 1; X := 2 * X)$
$\{X = 2^i\}$

(b) $\{X = n \wedge X > 0 \wedge Z = 1 \wedge Y = 0\}$
while $X > 0$ **do** $(X := X - Z; Z := 2 * Z; Y := Y + 1)$
$\{n + 1 > 2^{Y-1} \wedge 2^Y > n\}$

8.3 Die folgende Aufgabe bereitet einen Beweis der Vorlesung vor. Für eine Codierung von Zustandsfolgen, die sog. *Gödelisierung*, wird eine Bijektion zwischen $\mathbb{N}^k$ und $\mathbb{N}^2$ benötigt, die hier schrittweise konstruiert und bewiesen wird.

(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 $0 \leq i \leq k$ paarweise teilerfremd ("co-prim") sind, d.h. dass für $i \neq j$ der größte gemeinsame Teiler von p_i und p_j gleich 1 ist, sowie 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: $n_i = n \bmod p_i\ \forall 0 \leq i \leq k$.

Begründen Sie mit a) - c), dass $(n_1, \ldots, n_k) \mapsto (n, m)$ Bijektion ist.

Bitte wenden!

Schriftliche Aufgaben

8.4 Gegeben sei die folgende Anweisung $c \in \mathbf{Cmd}$: 5 Punkte

$$Z := 0;\ \mathbf{while}\ Y \leq X\ \mathbf{do}\ (Z := Z + 1; X := X - Y).$$

(a) Formulieren Sie eine partielle Korrektheitsaussage für c, die folgendes ausdrückt:

Wenn die Programmausführung in einem Zustand $\sigma \in \Sigma$ mit $\sigma(X) > 0$ und $\sigma(Y) > 0$ startet und in einem Zustand $\sigma' \in \Sigma$ endet, dann gilt

$$\sigma'(Z) = \sigma(X)\mathbf{div}\ \sigma(Y) \text{ und } \sigma'(X) = \sigma(X)\mathbf{mod}\ \sigma(Y)$$

(b) Weisen Sie die Gültigkeit Ihrer Aussage mit Hilfe der Hoare-Regeln nach.

8.5 **Beweisregel für die while-Schleife** 4 Punkte

Wir zeigen die Korrektheit der Beweisregel für die **while**-Schleife nochmals, diesmal mithilfe der operationellen Semantik:

Es sei $b \in \mathbf{BExp}$, $c \in \mathbf{Com}$ und $A \in \mathbf{Assn}$, so dass $\vdash \{A\}\ \mathbf{while}\ b\ \mathbf{do}\ c\ \{A \wedge (\neg b)\}$. Zeigen Sie, dass für alle $\sigma, \sigma' \in \Sigma$ und $I \in \mathcal{I}$ gilt:

$$\sigma \models^I A \text{ und } \langle\ \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \rightarrow \sigma' \quad \curvearrowright \quad \sigma' \models^I A \wedge \neg b$$

8.6 Geben Sie eine Hoare-Regel für die **repeat** -Schleife an. 3 Punkte

Frohe Weihnachten
und alles Gute im Neuen Jahr