PHILIPPS-UNIVERSITÄT MARBURG D-35032 Marburg
Fachbereich Mathematik und Informatik Hans Meerwein Straße
Prof. Dr. R. Loogen
Dipl.Inf. J.Berthold

8. Dezember 2004

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

Nr. 7, Besprechung mündlicher Aufgaben: 13. Dezember 2004 in der Übung, Abgabe der Hausaufgaben: 15. Dezember 2004 vor der Vorlesung

---

Hinweise: Am Montag, dem 20.12.2004 findet kein Tutorium statt. Die Besprechung der schriftlichen Aufgaben erfolgt also erst am 3.1.2005.

Am Mittwoch, dem 22.12.2004 entfällt die Vorlesung.

Mündliche Aufgaben

7.1 Fixpunktinduktion

Seien $(D, \leq)$ eine kettenvollständige Halbordnung und $f : D \to D$ stetig.

Sei $p : D \to \mathbf{T}$ ein Prädikat über D, so dass für jede Kette $K \subseteq D$ gilt:

$$p(d) = \mathit{true} \text{ für jedes } d \in K \curvearrowright p(\sqcup K) = \mathit{true}$$

und für jedes $d \in D$ gilt: $p(d) = \mathit{true} \curvearrowright f(d) = \mathit{true}$.

Beweisen Sie, dass dann auch $p(\mathit{fix} f) = \mathit{true}$ gilt.

7.2 Formulierung von Zusicherungen

(a) Geben Sie eine Zusicherung $A \in \mathbf{Assn}$ mit zwei logischen Variablen $i, j \in \mathbf{IVar}$ an, welche ausdrückt, dass i Teiler von j ist, d.h. für alle $\sigma \in \Sigma$ und alle $I \in \mathcal{I}$ soll genau dann $\sigma \models^I A$ gelten, wenn gilt: $I(i)|I(j)$.

(b) Geben Sie eine Zusicherung $A \in \mathbf{Assn}$ mit logischen Variablen $i, j, k \in \mathbf{IVar}$ an, welche ausdrückt, dass k kleinstes gemeinsames Vielfaches von i und j ist.

7.3

(a) Definieren Sie, wann eine logische Variable *frei* oder durch Quantoren *gebunden* in einer Zusicherung auftritt. Definieren Sie dazu induktiv eine Funktion $Bnd : \mathbf{Assn} \to \mathbf{IVar}$, welche die Menge der gebundenen Variablen in einer Zusicherung angibt.

(b) Definieren Sie eine Funktion *replace*, welche in einer Zusicherung $A \in \mathbf{Assn}$ bzw. einem arithmetischen Ausdruck $a \in \mathbf{LExp}$ eine logische Variable $i \in \mathbf{IVar}$ durch eine Zahl $z \in \mathbf{N}$ ersetzt (Schreibweise: $A[i \mapsto z]$ bzw. $a[i \mapsto z]$).
(Sie sollten an einer Stelle die Funktion aus Teil a) verwenden.)

(c) Zeigen Sie, dass für alle $a \in \mathbf{LExp}$, $i \in \mathbf{IVar}$, $z \in \mathbf{N}$, $I \in \mathcal{I}$ und $\sigma \in \Sigma$ gilt:

$$\mathcal{L}[\![a]\!] I[i \mapsto z]\sigma = \mathcal{L}[\![a[i \mapsto z]]\!] I\sigma$$

Schriftliche Aufgaben

7.4 Korrektheitsbeweis mit denotationeller Semantik

4 Punkte

Zeigen Sie unter Verwendung der Aussage in Aufgabe 7.1, dass die denotationelle Semantik der Anweisung

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

das folgende Prädikat $q : (\Sigma \dashrightarrow \Sigma) \to \mathbf{T}$ erfüllt:

$q(f) = \mathit{true}$ gilt genau dann, wenn für alle Zustände $\sigma, \sigma' \in \Sigma$ gilt:

$$f(\sigma) = \sigma' \curvearrowright \sigma'(Y) = \sigma(X)! \wedge \sigma(X) > 0.$$

7.5 Denotationelle Semantik für Binärzahlen

5 Punkte

Auf der Menge $BZ = \{0,1\}^+$ der Binärzahlen lässt sich eine binäre Operation $\oplus$ durch die folgende „rekursive Tabelle“ definieren (mit $\beta, \gamma \in BZ$):

$\oplus$	0	1	$\gamma 0$	$\gamma 1$
0	0	1	$\gamma 0$	$\gamma 1$
1	1	10	$\gamma 1$	$(\gamma \oplus 1)0$
$\beta 0$	$\beta 0$	$\beta 1$	$(\beta \oplus \gamma)0$	$(\beta \oplus \gamma)1$
$\beta 1$	$\beta 1$	$(\beta \oplus 1)0$	$(\beta \oplus \gamma)1$	$(\beta \oplus (\gamma \oplus 1))0$

Diese Tabelle beschreibt den üblichen Algorithmus zur Addition von Binärzahlen. Die Korrektheit des Verfahrens soll unter Verwendung der Semantik einer Binärzahl, d.h. ihres Wertes, nachgewiesen werden.

(a) Definieren Sie eine geeignete Semantik für Binärzahlen, d.h. eine Abbildung

$$\psi[\![.]\!] : BZ \to \mathbb{N}.$$

(b) Zeigen Sie für $\beta, \gamma \in BZ$ durch strukturelle Induktion, dass das folgende Diagramm kommutiert

$$\begin{array}{ccc} BZ \times BZ & \xrightarrow{\psi[\![.]\!] \times \psi[\![.]\!]} & \mathbb{N} \times \mathbb{N} \\ \oplus \downarrow & & \downarrow + \\ BZ & \xrightarrow{\psi[\![.]\!]} & \mathbb{N} \end{array}$$

d.h. dass gilt: $\psi[\![\beta \oplus \gamma]\!] = \psi[\![\beta]\!] + \psi[\![\gamma]\!]$.

7.6 Formulierung von Zusicherungen

3 Punkte

Geben Sie für die folgenden Aussagen Zusicherungen $A \in \mathbf{Assn}$ mit logischen Variablen $i, j, k \in \mathbf{IVar}$ an.

(a) i ist eine Quadratzahl.

(b) i ist eine Primzahl.

(c) i und j sind teilerfremd.

(d) i und j sind teilerfremd und beide teilen k.