Logik, Semantik und Verifikation SS 2002:
Musterlösung zum 9. Übungsblatt

Prof. Dr. Gert Smolka, Dipl.-Inform. Tim Priesnitz

Diesmal geht es hauptsächlich um rekursive Definitionen und induktive Beweise, mit Anwendungen bei der Semantik von IMP. Lesen Sie dazu Abschnitt 1.8 über wohlfundierte Induktion, Abschnitt 5.4 über rekursive Definition von Mengen, und Kapitel 6 über IMP.

Aufgabe 9.1: Regelinduktion (8)

(a)

$$\begin{aligned} R &= \{\langle \emptyset, (i,0,i)\rangle \mid i \in \mathbb{N}\} \\ &\cup \{\langle \emptyset, (0,i,i)\rangle \mid i \in \mathbb{N}\} \\ &\cup \{\langle \{(i,j,k)\}, (i+1, j+1, k+1)\rangle \mid i,j,k \in \mathbb{Z}\} \end{aligned}$$

(b)
1.Regel Zu zeigen: $(i,0,i) \in P$ für alle $i \in \mathbb{N}$. Gilt, da $i = \max\{i,0\}$.

2.Regel Zu zeigen: $(0,i,i) \in P$ für alle $i \in \mathbb{N}$. Gilt, da $i = \max\{0,i\}$.

3.Regel Sei $(i,j,k) \in P$. Wir müssen zeigen, dass $(i+1, j+1, k+1) \in P$. Gilt, da aus $k = max\{i,j\}$ die Aussage $k+1 = max\{i+1, j+1\}$ folgt.

(c) Sei $n = 0$: Dann folgt aus der 2. Inferenzregel, dass $(0, m, \max\{0,m\}) \in M$.

Sei nun $n > 0$ und $m \in \mathbb{N}$. Falls $m = 0$, gilt die Behauptung mit Regel 1. Falls $m > 0$, liefert die IA $(n-1, m-1, max\{n-1, m-1\}) \in M$. Mit der 3. Regel bekommen wir $(n, m, 1+max\{n-1, m-1\}) \in M$. Da $max\{n-1, m-1\}+1 = max\{n,m\}$ folgt $(n, m, max\{n,m\}) \in M$.

Aufgabe 9.2: Operationale Semantik (8)

(a) $\Sigma \times Com \times \Sigma$

(b) $\{\langle \emptyset, <\sigma, X := a, \sigma'>\rangle \mid \sigma, \sigma' \in \Sigma, X \in Loc, a \in Aexp, \sigma' = \sigma[\mathcal{A}(a)\sigma / X]\}$

(c) $\{\langle \{<\sigma, c_2, \sigma'>\}, <\sigma, \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma'>\rangle \mid \sigma, \sigma' \in \Sigma, b \in Bexp, c_1, c_2 \in Com, \mathcal{B}(b)\sigma = 0\}$

(d) $I_R = \{<\sigma, c, \sigma'> \mid \sigma, \sigma' \in \Sigma, c \in Com, \mathcal{C}(c)\sigma = \sigma'\}$

Aufgabe 9.3: Regelinduktion (5)

$$\begin{aligned} X &= \Sigma \times Com \times \Sigma \\ P &= \{<\sigma, c, \sigma'> \in X \mid \mathcal{C}(c)\sigma = \sigma'\} \end{aligned}$$

Aufgabe 9.4: Strukturelle Induktion (5)

$$\begin{aligned} X &= Com \\ P &= \{c \in Com \mid \forall \sigma, \sigma' \in \Sigma, \mathcal{C}(c)\sigma = \sigma' \Rightarrow \sigma \vdash c \Rightarrow \sigma'\} \end{aligned}$$

Aufgabe 9.5: Until-Schleifen (8)

(a)

$$\frac{\sigma \vdash c \Rightarrow \sigma' \quad \mathcal{B}(b)\sigma' = 1}{\sigma \vdash \texttt{do } c \texttt{ until } b \Rightarrow \sigma'} \qquad \frac{\sigma \vdash c \Rightarrow \sigma' \quad \mathcal{B}(b)\sigma' = 0 \quad \sigma' \vdash \texttt{do } c \texttt{ until } b \Rightarrow \sigma''}{\sigma \vdash \texttt{do } c \texttt{ until } b \Rightarrow \sigma''}$$

(b)

$$\mathcal{C}(\texttt{do } c \texttt{ until } b) = \text{fix}(\Gamma(\mathcal{B}(b), \mathcal{C}(c)))$$

und

$$\Gamma(\beta, \phi) = \lambda\psi.\lambda\sigma.\text{ if } \phi\sigma = \perp \text{ then } \perp \text{ else if } \beta(\phi\sigma) = 1 \text{ then } \phi\sigma \text{ else } \psi(\phi\sigma)$$

Aufgabe 9.6: For-Schleifen (8)

(a) for x to x do skip;

(b)

$$\frac{\sigma X > \mathcal{A}(a)\sigma}{\sigma \vdash \texttt{for } X \texttt{ to } a \texttt{ do } c \Rightarrow \sigma}$$

$$\frac{\sigma X \leq \mathcal{A}(a)\sigma \quad \sigma \vdash c \Rightarrow \sigma' \quad \sigma'[\sigma' X + 1/X] \vdash \texttt{for } X \texttt{ to } a \texttt{ do } c \Rightarrow \sigma''}{\sigma \vdash \texttt{for } X \texttt{ to } a \texttt{ do } c \Rightarrow \sigma''}$$

(c)

$$\mathcal{C}(\texttt{for } X \texttt{ to } a \texttt{ do } c) = \text{fix}(\Gamma(X, \mathcal{A}(a), \mathcal{C}(c)))$$

und

$$\Gamma(X, \alpha, \phi) = \lambda\psi.\lambda\sigma.\text{ if } \sigma X \leq \alpha\sigma \text{ then if } \phi\sigma = \perp \text{ then } \perp \text{ else } \psi((\phi\sigma)[\phi\sigma X + 1/X]) \text{ else } \sigma$$

Aufgabe 9.7: Formalisierung in ASSN (8)

(a) $(X \leq Y \Rightarrow Z = X) \wedge (Y \leq X \Rightarrow Z = Y)$

(b) $\exists Y\ X = 7 * Y$

(c) $(X \geq 0) \wedge (Y \geq 0) \wedge \exists R(0 \leq R \wedge R < Y \wedge X = Z * Y + R)$

(d) Wir benutzen die folgende Abkürzung aus dem Skript:

$$T(Z, X) = (Z \geq 1 \wedge X \leq 0 \wedge \exists N\ (X = Z * N))$$

$$x \geq 1 \wedge Y \geq 1 \wedge T(Z, X) \wedge T(Z, Y) \wedge \forall U(T(U, X) \wedge T(U, Y) \Rightarrow U \leq Z)$$