Logiken für Programme und Prozesse — Übungsblatt 8

Michael Arndt, WSI für Informatik — **WS 2006/07**

Aufgabe 1 (10 Punkte)

Leiten Sie die folgenden Regeln der Hoare-Logik in DAL her.

(a) Komposition

$$\frac{\{\phi\}\ \alpha\ \{\sigma\} \qquad \{\sigma\}\ \beta\ \{\psi\}}{\{\phi\}\ \alpha;\beta\ \{\psi\}}$$

(b) Konditional

$$\frac{\{\phi \land \sigma\}\ \alpha\ \{\psi\} \qquad \{\neg\phi \land \sigma\}\ \beta\ \{\psi\}}{\{\sigma\}\ \textbf{if}\ \phi\ \textbf{then}\ \alpha\ \textbf{else}\ \beta\ \{\psi\}}$$

(c) Schleife

$$\frac{\{\phi \land \psi\}\ \alpha\ \{\psi\}}{\{\psi\}\ \textbf{while}\ \phi\ \textbf{do}\ \alpha\ \{\neg\phi \land \psi\}}$$

(d) Verstärkung der Vorbedingung

$$\frac{\phi' \to \phi \qquad \{\phi\}\ \alpha\ \{\psi\}}{\{\phi'\}\ \alpha\ \{\psi\}}$$

(e) Abschwächung der Nachbedingung

$$\frac{\{\phi\}\ \alpha\ \{\psi\} \qquad \psi \to \psi'}{\{\phi\}\ \alpha\ \{\psi'\}}$$

Zur Erinnerung: Es ist $\{\phi\}\ \alpha\ \{\psi\}$ erklärt durch $\phi \to [\alpha]\psi$.

Aufgabe 2 (6 Punkte)

Es sei $\mathfrak{A} = \langle \mathbb{N}, b\rangle$ ein Berechnungsbereich über dem Alphabet $\Sigma = \{\mathbf{0}, \mathbf{s}, \mathbf{add}, \mathbf{lt}, \doteq\}$ mit

$$\begin{array}{lcl} b(\mathbf{0}) & = & x \mapsto 0 \\ b(\mathbf{s}) & = & x \mapsto x+1 \\ b(\mathbf{add}) & = & (x,y) \mapsto x+y \\ b(\mathbf{lt}) & = & \{(x, x+y) \mid x,y \in \mathbb{N}, y > 0\} \end{array}$$

Weiterhin sei $u \in \mathfrak{A}^{\mathcal{S}}$ derjenige Zustand des Standardmodells $\mathfrak{M}_{\mathfrak{A}}$ mit $u(x) = 0$ für alle $x \in \mathcal{S}$. Welche der folgenden Behauptungen treffen zu? Geben Sie eine ausführliche Begründung an.

(a) $\mathfrak{M}_{\mathfrak{A}}, u \models \neg(x_0 \doteq \mathbf{0})$

(b) $\mathfrak{M}_{\mathfrak{A}}, u \not\models \langle x_0 := \mathbf{s}(\mathbf{0})\rangle(x_0 \doteq \mathbf{0})$

(c) $\mathfrak{M}_{\mathfrak{A}}, u \models [x_0 := \mathbf{add}(x_0, \mathbf{s}(\mathbf{0}))](x_0 \doteq \mathbf{0})$

(d) $\mathfrak{M}_{\mathfrak{A}}, u \models [x_0 := \mathbf{add}(x_0, x_1)]\ \mathbf{lt}(\mathbf{0}, x_0)$

(e) $\mathfrak{M}_{\mathfrak{A}} \models \neg(x_1 \doteq \mathbf{0}) \to [x_0 := \mathbf{add}(x_0, x_1)]\ \mathbf{lt}(\mathbf{0}, x_0)$

(f) $\mathfrak{M}_{\mathfrak{A}} \not\models (\forall x_0)(\exists x_1)(x_0 \doteq \mathbf{s}(x_1))$