Prof. Dr. J. Giesl
D. Dlugosz

5. Übung zu „Automatisierte Programmverifikation“, SS 03
Abgabe: Mi, 04.06.03, in der Frontalübung

Aufgabe 1 (1 + 0.5 Punkte)

Sei P ein terminierendes Programm mit zugehöriger Signatur Σ. Beweisen Sie die folgenden Aussagen:

a) Für alle Grundterme $t \in \mathcal{T}(\Sigma)$ gilt $M_P(t) = eval_P(t)$.

b) Für alle Konstruktorgrundterme $q \in \mathcal{T}(\Sigma^c)$ gilt $M_P(q) = q$.

Aufgabe 2 (2 Punkte)

Sei P ein terminierendes Programm. Beweisen Sie: Für jede definierende Gleichung $f(t^*) \equiv r$ mit den Variablen x^* der Sorten w gilt: $M_P \models \forall x^* : w \;\; f(t^*) \equiv r$.

Aufgabe 3 (2+2 Punkte)

Das Programm P bestehe aus der Datenstruktur number und den folgenden Algorithmen:

$$
\begin{array}{lll}
\multicolumn{3}{l}{\textbf{function } \mathsf{double} : \mathsf{number} \rightarrow \mathsf{number}} \\
\mathsf{double}(\mathcal{O}) & \equiv & \mathcal{O} \\
\mathsf{double}(\mathsf{succ}(x)) & \equiv & \mathsf{succ}(\mathsf{succ}(\mathsf{double}(x)))
\end{array}
$$

$$
\begin{array}{lll}
\multicolumn{3}{l}{\textbf{function } \mathsf{half} : \mathsf{number} \rightarrow \mathsf{number}} \\
\mathsf{half}(\mathcal{O}) & \equiv & \mathcal{O} \\
\mathsf{half}(\mathsf{succ}(\mathcal{O})) & \equiv & \mathcal{O} \\
\mathsf{half}(\mathsf{succ}(\mathsf{succ}(x))) & \equiv & \mathsf{succ}(\mathsf{half}(x))
\end{array}
$$

a) Beweisen Sie durch strukturelle Induktion über $q \in \mathcal{T}(\Sigma^c)_{\mathsf{number}}$:

$$\text{Für alle } q \in \mathcal{T}(\Sigma^c)_{\mathsf{number}} \text{ gilt } \; q \equiv \mathsf{half}(\mathsf{double}(q)) \in Th_P.$$

b) Sei AX_P die Menge der allquantifizierten definierenden Gleichungen E_P, d.h. $AX_P = \{\forall x^* : w \;\; l \equiv r \mid l \equiv r \in E_P$ mit den Variablen x^* der Sorten $w\}$. Zeigen Sie: $AX_P \not\models \forall x : \mathsf{number} \;\; x \equiv \mathsf{half}(\mathsf{double}(x))$

Hinweis: Geben Sie eine Interpretation $I = (\mathcal{A}, \alpha)$ an, die ein Modell von AX_P und kein Modell von $\forall x : \mathsf{number} \;\; x \equiv \mathsf{half}(\mathsf{double}(x))$ ist. Eine Möglichkeit ist, hierbei $\mathcal{A}_{\mathsf{number}} = \mathbb{N} \cup \{\top, \bot\}$ für zwei zusätzliche Objekte $\top, \bot$ zu wählen.