Semantik und Programmverifikation

Prof. Dr. Christoph Walther / Simon Siegler
Technische Universität Darmstadt — Wintersemester 2008/09

Hausaufgabe 7

Hausaufgabe 7.1 (Grenzen der formalen Verifikation) **(8 Punkte)**

Gegeben sei das funktionale Programm $P_{plus} = \langle F_{plus} \rangle$, wobei P_{plus} definiert ist durch

$$\begin{array}{l} \textbf{function } plus(x, y : nat) : nat \ \Leftarrow \\ \quad \textbf{if } x = 0 \textbf{ then } y \textbf{ else } 1 + plus(x - 1, y) \textbf{ fi}. \end{array}$$

Zeigen Sie

(a) $\varphi_{kom}, \varphi_{kom,1}, \varphi_{kom,2} \in Th_{P_{plus}}$ und

(b) $\varphi_{kom}, \varphi_{kom,1}, \varphi_{kom,2} \notin (AX_{P_{plus}})^{\models}$.

Dabei sind $\varphi_{kom}, \varphi_{kom,1}$ und $\varphi_{kom,2}$ definiert durch

$$\begin{array}{rcl} \varphi_{kom} & = & \forall x, y : nat.\ plus(x, y) \equiv plus(y, x), \\ \varphi_{kom,1} & = & \forall y : nat.\ plus(0, y) \equiv plus(y, 0), \\ \varphi_{kom,2} & = & \forall x : nat.\ [\forall y : nat. plus(x, y) \equiv plus(y, x) \\ & & \rightarrow\ \forall y : nat. plus(succ(x), y) \equiv plus(y, succ(x))]. \end{array}$$

(vgl. Übung 3.6.1.(ii))

Hausaufgabe 7.2 (Induktionsaxiome) **(5 Punkte)**

Seien P_{plus} und φ_{kom} wie zuvor definiert. Weiter sei $\mathsf{IND}_{P_{\text{plus}}}$ die Menge aller Formeln der Form

$$\begin{array}{ll} & \psi[x/0, y/0] \\ \wedge & \forall x, y : nat\ (\ \psi[x/0, y] \rightarrow \psi[x/0, y/succ(y)]\ ) \\ \wedge & \forall x, y : nat\ (\forall z : nat\ \psi[x, y/z] \rightarrow \psi[x/succ(x), y/0]\ ) \\ \wedge & \forall x, y : nat\ (\forall z : nat\ \psi[x, y/z] \wedge \psi[x/succ(x), y] \rightarrow \psi[x/succ(x), y/succ(y)]\ ) \\ & \rightarrow\ \forall x, y : nat\ \psi[x, y], \end{array}$$

mit $\psi[x, y] \in \mathcal{F}(\Sigma, \mathcal{V})$, $x, y \in \mathcal{V}_{nat}$ und $\mathcal{V}_f(\psi[x, y]) = \{x, y\}$.

(a) Zeigen Sie $\mathsf{IND}_{P_{plus}} \subseteq Th_{P_{plus}}$.

(b) Beweisen Sie $\varphi_{kom} \in Th_{\text{P}_{\text{plus}}}$ unter Verwendung von $\mathsf{IND}_{P_{\text{plus}}}$.

(c) Der im Buch angegebene Beweis für $\varphi_{kom} \in Th_{P_{plus}}$ erfolgt unter Verwendung von Formel (3.7.12). Diskutieren Sie den Unterschied zwischen $\mathsf{IND}_{P_{\text{plus}}}$ und (3.7.12) beim Beweis von $\varphi_{kom} \in Th_{P_{plus}}$.

Hausaufgabe 7.3 (Spezifikation und Verifikation) **(6 Punkte)**

Das funktionale Programm $P_{set} = \langle D_{set}, F_{insert} \rangle$ sei durch folgende Datenstrukturdefinition und folgende Funktionsprozedur definiert:

$$D_{set} = \mathsf{structure}\ \Diamond, cons(element : nat, rest : set) : set$$

$$\begin{aligned} F_{insert} = \quad & \textbf{function}\ insert(n : nat, s : set) : set\ \Leftarrow \\ & \quad \textbf{if}\ s = \Diamond \\ & \quad\ \textbf{then}\ cons(n, \Diamond) \\ & \quad\ \textbf{else if}\ n = element(s) \\ & \qquad\ \textbf{then}\ s \\ & \qquad\ \textbf{else}\ cons(element(s), insert(n, rest(s))) \\ & \quad\ \textbf{fi} \\ & \quad \textbf{fi} \end{aligned}$$

(a) Formulieren Sie durch geeignete Erweiterung des funktionalen Programmes P_{set} durch einen Spezifikationsteil S_{set} die folgenden Aussagen:

(i) Fügt man zweimal hintereinander eine Zahl n in eine Menge s ein, so resultiert daraus die gleiche Menge wie beim einmaligen Einfügen dieser Zahl n in s.

(ii) Eine Zahl, die noch nicht in einer Menge s vorhanden ist, wird beim Einfügen in s an das Ende (der Listenstruktur) gestellt.

(b) Geben Sie die Axiomenmenge $AX_{P_{set}} \setminus AX_{BM}$ an.

(c) Beweisen Sie für die unter (i) aufgestellte Formel ϕ die Aussage $\phi \in Th_P$. (Zeigen Sie hierzu $M_{P_{set}} \models \phi$ mit einem Induktionsbeweis.)