RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

LEHR- UND FORSCHUNGSGEBIET INFORMATIK II
RWTH Aachen · D-52056 Aachen · GERMANY
http://www-i2.informatik.rwth-aachen.de/lufgi2.html

Jürgen Giesl
Darius Dlugosz

Automatisierte Programmverifikation

Übungsblatt 5

Alle Aufgaben werden korrigiert. Die Abgabe ist bis Dienstag, 19. Dezember 2001, in der Übung, Vorlesung oder im Raum 4211 möglich. Die Aufgaben werden in der Übung am 19. Dezember 2000 besprochen.

Aufgabe 1: (2 Punkte) Das Programm P bestehe aus den folgenden Datenstrukturen und Algorithmen:

structure bool
true : bool
false : bool

structure number
$\mathcal{O}$: number
succ : number $\to$ number

function le : number $\times$ number $\to$ bool
$\mathsf{le}(\mathcal{O}, y) \equiv \mathsf{true}$
$\mathsf{le}(\mathsf{succ}(x), \mathcal{O}) \equiv \mathsf{false}$
$\mathsf{le}(\mathsf{succ}(x), \mathsf{succ}(y)) \equiv \mathsf{le}(x, y)$

function plus : number $\times$ number $\to$ number
$\mathsf{plus}(\mathcal{O}, y) \equiv y$
$\mathsf{plus}(\mathsf{succ}(x), y) \equiv \mathsf{succ}(\mathsf{plus}(x, y))$

function double : number $\to$ number
$\mathsf{double}(\mathcal{O}) \equiv \mathcal{O}$
$\mathsf{double}(\mathsf{succ}(x)) \equiv \mathsf{succ}(\mathsf{succ}(\mathsf{double}(x)))$

function half : number $\to$ number
$\mathsf{half}(\mathcal{O}) \equiv \mathcal{O}$
$\mathsf{half}(\mathsf{succ}(\mathcal{O})) \equiv \mathcal{O}$
$\mathsf{half}(\mathsf{succ}(\mathsf{succ}(x))) \equiv \mathsf{succ}(\mathsf{half}(x))$

Berechnen Sie durch Angabe der Auswertungsfolgen die Ergebnisse der symbolischen Auswertung von

(a) $\neg\neg \mathsf{plus}(\mathsf{succ}(x), y) \equiv \mathsf{plus}(\mathsf{succ}(x), y)$,

(b) $\mathsf{le}(\mathsf{double}(\mathsf{half}(\mathcal{O})), \mathcal{O}) \ \equiv\ \mathsf{true}$,

(c) $\mathsf{le}(\mathsf{double}(\mathsf{half}(\mathsf{succ}(\mathcal{O}))), \mathsf{succ}(\mathcal{O})) \ \equiv\ \mathsf{true}$,

(d) $\mathsf{le}(\mathsf{plus}(\mathsf{succ}(\mathcal{O}), \mathsf{half}(\mathsf{succ}(\mathsf{succ}(\mathcal{O})))), \mathsf{succ}(\mathsf{succ}(x))) \ \equiv\ \mathsf{true} \ \to\ \mathsf{plus}(\mathsf{succ}(\mathcal{O}), x) \ \equiv\ \mathsf{succ}(\mathcal{O})$,

(e) $\neg\, \mathsf{double}(\mathsf{half}(\mathcal{O})) \ \equiv\ \mathcal{O} \ \vee\ \neg\, \mathsf{half}(\mathsf{succ}(\mathcal{O})) \ \equiv\ \mathsf{double}(\mathsf{half}(\mathsf{succ}(\mathcal{O}))$.

Aufgabe 2: (2 Punkte) Sei P ein terminierendes Programm.

(i) Skizzieren Sie ein Verfahren, mit dem "$\varphi \in Th_P$" für alle $\varphi \in \mathcal{F}_g(\Sigma, \varnothing)$ bewiesen oder widerlegt werden kann.

(ii) Eine Formel $\varphi \in \mathcal{F}_g(\Sigma, \mathcal{V})$ heißt Existenzformel gdw. $\mathcal{V}(\varphi) = \varnothing$ oder $\varphi = (\exists x_1 : s_1\, (\ldots (\exists x_n : s_n \ \ \psi) \ldots))$, ψ ist quantorfrei und $\mathcal{V}(\psi) \subseteq \{x_1, \ldots, x_n\}$. Skizzieren Sie ein Verfahren, mit dem "$\varphi \in Th_P$" für jede Existenzformel $\varphi \in Th_P$ bewiesen werden kann. Wie verhält sich ihr Verfahren bei Eingabe einer Existenzformel $\varphi \notin Th_P$?

Aufgabe 3: (1 Punkt) Sei P das Programm aus Aufgabe 1. Berechnen Sie durch Angabe der Auswertungsschritte die Ergebnisse von

(i) $\mathsf{SA}_P(\mathsf{le}(\mathsf{double}(\mathsf{half}(\mathsf{succ}(\mathsf{succ}(y)))), \mathsf{succ}(\mathsf{succ}(y)))) \ \equiv\ \mathsf{true}$,
$\{\forall x : \mathsf{number}\ \mathsf{le}(\mathsf{double}(\mathsf{half}(x)), x) \ \equiv\ \mathsf{true}\})$,

(ii) $\mathsf{SA}_P(\mathsf{le}(\mathsf{double}(\mathsf{half}(\mathsf{succ}(y))), \mathsf{succ}(y)) \ \equiv\ \mathsf{true}$,
$\{\forall x : \mathsf{number}\ \mathsf{le}(\mathsf{double}(\mathsf{half}(x)), x) \ \equiv\ \mathsf{true}\})$.

Aufgabe 4: (2 Punkte) Das Programm P aus Aufgabe 1 sei um die folgenden Algorithmen erweitert:

function $\mathsf{pred} : \mathsf{number} \to \mathsf{number}$
$\mathsf{pred}(\mathcal{O}) \equiv \mathcal{O}$
$\mathsf{pred}(\mathsf{succ}(x)) \equiv x$

function $\mathsf{minus} : \mathsf{number} \times \mathsf{number} \to \mathsf{number}$
$\mathsf{minus}(x, \mathcal{O}) \equiv x$
$\mathsf{minus}(x, \mathsf{succ}(y)) \equiv \mathsf{minus}(\mathsf{pred}(x), y)$

Beweisen Sie die folgende Aussage durch Peano-Induktion über x_2. Verwenden Sie dabei symbolische Auswertung unter Hypothesen.

$$(\forall x_1, x_2, x_3 : \mathsf{number}\ \ \mathsf{minus}(x_1, \mathsf{plus}(x_2, x_3)) \equiv \mathsf{minus}(\mathsf{minus}(x_1, x_2), x_3))\ \in Th_P$$

Hinweis: Das hierbei verwendete Induktionsprinzip hat die Form

$$\psi[x/\mathcal{O}]\ \ \wedge\ \ \forall y : \mathsf{number}\ \ (\psi[x/y]\ \rightarrow\ \psi[x/\mathsf{succ}(y)])\ \ \rightarrow\ \ \forall x : \mathsf{number}\ \ \psi$$

Allgemein kann man also "$(\forall x : \mathsf{number}\ \ \psi) \in Th_P$" beweisen, indem man stattdessen die folgenden Aussagen zeigt:

$$(\psi[x/\mathcal{O}])\ \in Th_P$$
$$(\forall y : \mathsf{number}\ \ (\psi[x/y]\ \rightarrow\ \psi[x/\mathsf{succ}(y)]))\ \in Th_P$$