RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

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

Prof. Dr. J. Giesl
D. Dlugosz

7. Übung zu „Automatisierte Programmverifikation“, SS 03
Abgabe: Mi, 25.06.03, in der Frontalübung

Aufgabe 1 (1 Punkt)

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

structure bool

true	:	bool
false	:	bool

function double : number → number

double($\mathcal{O}$)	≡	$\mathcal{O}$
double(succ(x))	≡	succ(succ(double(x)))

function le : number × number → bool

le($\mathcal{O}, y$)	≡	true
le(succ(x), $\mathcal{O}$)	≡	false
le(succ(x), succ(y))	≡	le(x, y)

function half : number → number

half($\mathcal{O}$)	≡	$\mathcal{O}$
half(succ($\mathcal{O}$))	≡	$\mathcal{O}$
half(succ(succ(x)))	≡	succ(half(x))

Berechnen Sie durch Angabe der Auswertungsschritte die Ergebnisse von

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

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

Aufgabe 2 (2 Punkte)

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

function pred : number → number

pred($\mathcal{O}$)	≡	$\mathcal{O}$
pred(succ(x))	≡	x

function plus : number × number → number

plus($\mathcal{O}, y$)	≡	y
minus(succ(x), y)	≡	succ(plus(x, y))

function minus : number × number → number

minus($x, \mathcal{O}$)	≡	x
minus(x, succ(y))	≡	minus(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 *Induktionsaxiom* 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 *Induktionsformeln* zeigt:

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

Aufgabe 3 (0.5 + 0.5 + 2 Punkte)

Sei P das Programm aus Aufgabe 1 und sei φ die folgende Aussage:

$$\forall x : \mathsf{number}\ \ \mathsf{le}(\mathsf{double}(\mathsf{half}(x)), x) \ \equiv\ \mathsf{true}$$

a) Versuchen Sie, mit Hilfe der Peano-Induktion zu zeigen, dass φ eine wahre Aussage über P ist. Verwenden Sie dabei symbolische Auswertung unter Hypothesen, um die Induktionsformeln zu beweisen. Hierbei soll die Induktion nur einmal durchgeführt werden.

b) Seien $q, p \in \mathcal{T}(\Sigma^c)_{\mathsf{number}}$ und sei $\succ$ eine Relation mit $q \succ p$ gdw. $q = \mathsf{succ}(\mathsf{succ}(p))$. Zeigen Sie, dass $\succ$ fundiert ist.

c) Geben Sie mit Hilfe der Relation $\succ$ aus Teil (b) geeignete Induktionsformeln zum Beweis von $\varphi \in Th_P$ an und zeigen Sie mit der symbolischen Auswertung unter Hypothesen die Gültigkeit Ihrer Induktionsformeln.