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

Prof. Dr. Jürgen Giesl
Darius Dlugosz

Automatisierte Programmverifikation

Übungsblatt 8

Alle Aufgaben werden korrigiert. Die Abgabe ist bis Dienstag, 23. Januar 2001, in der Übung, Vorlesung oder im Raum 4211 möglich. Die Aufgaben werden in der Übung am 23. Januar 2001 besprochen.

Aufgabe 1: (0.5 Punkte)

Das Programm P bestehe aus folgenden Datenstrukturen und Algorithmen:

structure bool

true	:	bool
false	:	bool

structure number

$\mathcal{O}$	:	number
succ	:	number $\rightarrow$ number

structure list

empty	:	list
add	:	number $\times$ list $\rightarrow$ list

function if : bool $\times$ number $\times$ number $\rightarrow$ number

if(true, x, y)	$\equiv$	x
if(false, x, y)	$\equiv$	y

function plus : number $\times$ number $\rightarrow$ number

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

function times : number $\times$ number $\rightarrow$ number

times($\mathcal{O}$, y)	$\equiv$	$\mathcal{O}$
times(succ(x), y)	$\equiv$	plus(y, times(x, y))

$$
\begin{array}{l}
\textbf{function}\ \ \mathsf{minus} : \mathsf{number} \times \mathsf{number} \to \mathsf{number} \\
\quad \begin{array}{lcl}
\mathsf{minus}(x, \mathcal{O}) & \equiv & x \\
\mathsf{minus}(\mathcal{O}, \mathsf{succ}(y)) & \equiv & \mathcal{O} \\
\mathsf{minus}(\mathsf{succ}(x), \mathsf{succ}(y)) & \equiv & \mathsf{minus}(x, y)
\end{array} \\
\\
\textbf{function}\ \ \mathsf{fac} : \mathsf{number} \to \mathsf{number} \\
\quad \begin{array}{lcl}
\mathsf{fac}(\mathcal{O}) & \equiv & \mathsf{succ}(\mathcal{O}) \\
\mathsf{fac}(\mathsf{succ}(x)) & \equiv & \mathsf{times}(\mathsf{succ}(x), \mathsf{fac}(x))
\end{array} \\
\\
\textbf{function}\ \ \mathsf{ge} : \mathsf{number} \times \mathsf{number} \to \mathsf{bool} \\
\quad \mathsf{ge}(x, \mathcal{O}) \equiv \mathsf{true} \\
\quad \mathsf{ge}(\mathcal{O}, \mathsf{succ}(y)) \equiv \mathsf{false} \\
\quad \mathsf{ge}(\mathsf{succ}(x), \mathsf{succ}(y)) \equiv \mathsf{ge}(x, y) \\
\\
\textbf{function}\ \ \mathsf{gcd} : \mathsf{number} \times \mathsf{number} \to \mathsf{number} \\
\quad \begin{array}{lcl}
\mathsf{gcd}(x, \mathcal{O}) & \equiv & x \\
\mathsf{gcd}(\mathcal{O}, \mathsf{succ}(y)) & \equiv & \mathsf{succ}(y) \\
\mathsf{gcd}(\mathsf{succ}(x), \mathsf{succ}(y)) & \equiv & \mathsf{if}(\mathsf{ge}(x, y), \\
 & & \quad \mathsf{gcd}(\mathsf{minus}(x, y), \mathsf{succ}(y)), \\
 & & \quad \mathsf{gcd}(\mathsf{succ}(x), \mathsf{minus}(y, x)))
\end{array} \\
\\
\textbf{function}\ \ \mathsf{append} : \mathsf{list} \times \mathsf{list} \to \mathsf{list} \\
\quad \begin{array}{lcl}
\mathsf{append}(\mathsf{empty}, l) & \equiv & l \\
\mathsf{append}(\mathsf{add}(x, k), l) & \equiv & \mathsf{add}(x, \mathsf{append}(k, l))
\end{array}
\end{array}
$$

Geben Sie für alle Algorithmen von P die veränderbaren Positionen an.

Aufgabe 2: (1 Punkt)

Sei P das Programm aus Aufgabe 1. Geben Sie für die Formeln

(a) $(x \equiv y \to z_1 \equiv z_2) \to (\mathsf{if}(\mathsf{ge}(x, y), z_1, z_2) \equiv \mathsf{if}(\mathsf{ge}(y, x), z_2, z_1))$

(b) $(x \equiv y \to z_1 \equiv z_2) \ \to \ (x \equiv y \to \mathsf{gcd}(z_1, \mathsf{minus}(x, y)) \equiv \mathsf{gcd}(\mathsf{minus}(y, x), z_2))$

die veränderbaren Positionen an und bestimmen Sie die geeigneten Induktionsaxiome.

Aufgabe 3: (2 Punkte)

Sei P das Programm aus Aufgabe 1. Berechnen Sie $\mathsf{IB}_P(\{\langle \psi, \ \varnothing \rangle\})$ mit Angabe der Zwischenergebnisse für

(a) $\psi = \ \mathsf{plus}(x_1, x_2) \equiv \mathsf{plus}(x_2, x_1)$

(b) $\psi = \ \mathsf{append}(l_1, l_2) \equiv \mathsf{append}(l_2, l_1)$.

Aufgabe 4: (3 Punkte)

Sei P das Programm aus Aufgabe 1. Beweisen Sie unter Verwendung von Lemmata die folgenden Aussagen:

(a) $\forall n, x_2, x_3 : \mathsf{number} \ \ \mathsf{plus}(\mathsf{fac}(n), \mathsf{plus}(x_2, x_3)) \equiv \mathsf{plus}(\mathsf{plus}(\mathsf{fac}(n), x_2), x_3) \quad \in Th_P$

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

(c) $\forall x_1, x_2 : \mathsf{number} \ \ \mathsf{gcd}(x_1, x_2) \equiv \mathsf{gcd}(x_2, x_1) \quad \in Th_P$

Hinweis: In Teil (c) können folgende Lemmata erfolgreich verwendet werden:

$\forall x, y, z_1, z_2 : \mathsf{number} \ \ (x \equiv y \rightarrow z_1 \equiv z_2) \rightarrow (\mathsf{if}(\mathsf{ge}(x, y), z_1, z_2) \equiv \mathsf{if}(\mathsf{ge}(y, x), z_2, z_1))$

$\forall x, y, z_1, z_2 : \mathsf{number} \ \ (x \equiv y \rightarrow z_1 \equiv z_2) \ \rightarrow \ (x \equiv y \rightarrow \mathsf{gcd}(z_1, \mathsf{minus}(x, y)) \equiv \mathsf{gcd}(\mathsf{minus}(y, x), z_2))$