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

10. Übung zu „Automatisierte Programmverifikation“, SS 03
Abgabe: Mi, 16.07.03, in der Frontalübung

Aufgabe 1 (2 Punkte)

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

structure list
$\mathsf{nil} : \mathsf{list}$
$\mathsf{cons} : \mathsf{number} \times \mathsf{list} \to \mathsf{list}$

function if : bool × number × number → number
$\mathsf{if}(\mathsf{true}, x, y) \equiv x$
$\mathsf{if}(\mathsf{false}, x, y) \equiv y$

function max : number × number → number
$\mathsf{max}(\mathcal{O}, \mathcal{O}) \equiv \mathcal{O}$
$\mathsf{max}(\mathcal{O}, \mathsf{succ}(y)) \equiv \mathsf{succ}(y)$
$\mathsf{max}(\mathsf{succ}(x), \mathcal{O}) \equiv \mathsf{succ}(x)$
$\mathsf{max}(\mathsf{succ}(x), \mathsf{succ}(y)) \equiv \mathsf{succ}(\mathsf{max}(x, y))$

function ge : number × number → bool
$\mathsf{ge}(x, \mathcal{O}) \equiv \mathsf{true}$
$\mathsf{ge}(\mathcal{O}, \mathsf{succ}(y)) \equiv \mathsf{false}$
$\mathsf{ge}(\mathsf{succ}(x), \mathsf{succ}(y)) \equiv \mathsf{ge}(x, y)$

function gcd : number × number → number
$\mathsf{gcd}(x, \mathcal{O}) \equiv x$
$\mathsf{gcd}(\mathcal{O}, \mathsf{succ}(y)) \equiv \mathsf{succ}(y)$
$\mathsf{gcd}(\mathsf{succ}(x), \mathsf{succ}(y)) \equiv \mathsf{if}(\mathsf{ge}(x, y),$
$\quad \mathsf{gcd}(\mathsf{minus}(x, y), \mathsf{succ}(y)),$
$\quad \mathsf{gcd}(\mathsf{succ}(x), \mathsf{minus}(y, x)))$

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

function fac : number → number
$\mathsf{fac}(\mathcal{O}) \equiv \mathsf{succ}(\mathcal{O})$
$\mathsf{fac}(\mathsf{succ}(x)) \equiv \mathsf{times}(\mathsf{succ}(x), \mathsf{fac}(x))$

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

function append : list × list → list
$\mathsf{append}(\mathsf{nil}, l) \equiv l$
$\mathsf{append}(\mathsf{cons}(x, k), l) \equiv \mathsf{cons}(x, \mathsf{append}(k, l))$

function minus : number × number → number
$\mathsf{minus}(x, \mathcal{O}) \equiv x$
$\mathsf{minus}(\mathcal{O}, \mathsf{succ}(y)) \equiv \mathcal{O}$
$\mathsf{minus}(\mathsf{succ}(x), \mathsf{succ}(y)) \equiv \mathsf{minus}(x, y)$

Berechnen Sie $\mathsf{IB}_P(\{\langle \psi, \varnothing \rangle\})$ mit Angabe der Zwischenergebnisse für

a) $\psi = \mathsf{ge}(\mathsf{max}(x, y), y) \equiv \mathsf{true}$

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

Aufgabe 2 (4 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) $\forall x_1, x_2 : \mathsf{number}\ \ \mathsf{gcd}(x_1, x_2) \equiv \mathsf{gcd}(x_2, x_1) \quad \in Th_P$

Hierbei dürfen Sie nur die beiden Lemmata

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

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

verwenden sowie solche Lemmata, die mit IB_P ohne Lemmaverwendung bewiesen werden können. Sie müssen den Beweis der verwendeten Lemmata aber nicht angeben.

Aufgabe 3 (2 Punkte)

Sei P das Programm aus Aufgabe 1. Geben Sie geeignete Induktionsformeln und die verwendete Induktionsrelation zum Beweis der folgenden Aussage an:

$$\forall x, y, z : \mathsf{number}\ \ \mathsf{ge}(x, y) \equiv \mathsf{true} \ \wedge \ \mathsf{ge}(y, z) \equiv \mathsf{true} \ \rightarrow \ \mathsf{ge}(x, z) \equiv \mathsf{true}$$

Skizzieren Sie den Beweis.

Bemerkung: Die Induktionsformeln müssen nicht mit denen in der Vorlesung vorgestellten Methoden erzeugt werden.