Technische Universität München **WS 2006/07**
Institut für Informatik
Prof. Manfred Broy
A. Gruler, B. Spanfelner **Musterlösung zu Blatt 9**

Übungen zu „Formale Methoden“

Aufgabe 1 *wp*–Berechnung [LÖSUNG]

Folgendes Programm P ist zu betrachten, wobei a und b zwei natürliche Zahlen seien:

x, y, z := a, b, 1;
do $y > 0$ **then**
  if $odd(y)$ **then** $y := y - 1$; $z := z * x$
  [] $even(y)$ **then** $x := x * x$; $y := y \div 2$
  fi
od

(Hinweis: Nach Ablauf von $P(x, y)$ hat die Variable z den Wert x^y.)

(a) Berechnung von $wp(IF, C)$ für die **if**-Anweisung innerhalb der **do**-Schleife, für ein beliebiges Prädikat C.

$$\begin{aligned}&wp(IF, C)\\ \equiv\ & (odd(y) \vee even(y)) \quad \wedge \quad (odd(y) \Rightarrow wp(y := y-1; z := z * x, C)) \quad \wedge\\ & (even(y) \Rightarrow wp(x := x * x; y := y \div 2, C))\end{aligned}$$

{Def. von wp, $a \vee \neg a =$ **true**, $odd(k) = \neg even(k)$}

$$\equiv \big(odd(y) \Rightarrow C[(y-1)/y, (z*x)/z]\big) \quad \wedge \quad \big(even(y) \Rightarrow C[(x*x)/x, (y \div 2)/y]\big)$$

$\{(A \Rightarrow B) \wedge (\neg A \Rightarrow D) \ = \ (A \wedge B) \vee (\neg A \wedge D)\}$

$$\equiv \big(odd(y) \ \wedge \ C[(y-1/y, (z*x)/z]\big) \quad \vee \quad \big(even(y) \ \wedge \ C[(x*x)/x, (y \div 2)/y]\big)$$

(b) Berechnung des Funktionals τ mit $z = a^b$ als Nachbedingung der **do**-Schleife.

$$\begin{aligned}\tau[C] \ &\equiv\ (\neg(y > 0) \Rightarrow z = a^b) \quad \wedge \quad (y > 0 \Rightarrow wp(IF, C))\\ &\equiv\ (y \leq 0 \Rightarrow z = a^b) \quad \wedge \quad (y > 0 \Rightarrow wp(IF, C))\end{aligned}$$

$\{ (A \Rightarrow B) \wedge (\neg A \Rightarrow D) \ = \ (A \wedge B) \vee (\neg A \wedge D),$ Distributivgesetze$\}$

$$\begin{aligned}\equiv\ & \big(y \leq 0 \wedge z = a^b\big) \quad \vee \quad \big(y > 0 \ \wedge \ odd(y) \ \wedge \ C[(y-1)/y, (z*x)/z]\big) \ \vee\\ & \big(y > 0 \ \wedge \ even(y) \ \wedge \ C[(x*x)/x, (y \div 2)/y]\big)\end{aligned}$$

Vergleich mit dem Programm $P2$ (**if** ... **fi** ist aufgelöst und nun haben wir eine **do**-Schleife mit 2 Wächtern):

$x, y, z := a, b, 1;$
do $(y > 0 \wedge odd(y))$ **then** $y := y - 1; z := z * x$
$[](y > 0 \wedge even(y))$ **then** $x := x * x; y := y \div 2$
od

(c) Beweis durch Induktion, dass für τ gilt:

$$\tau^n(\mathbf{false}) \quad \Leftarrow \quad (y \leq 0 \wedge z = a^b) \ \vee \ (0 < y \leq n-1 \wedge z * x^y = a^b)$$

Induktionsanfang: $n = 1$

$$\begin{aligned}\tau^1[\mathbf{false}] \quad &= \quad (y \leq 0 \wedge z = a^b) \ \vee \ (y > 0 \wedge odd(y) \wedge \mathbf{false}) \ \vee \ (y > 0 \wedge even(y) \wedge \mathbf{false}) \\ & \quad \{\text{Definition: } \mathbf{false} \wedge A = \mathbf{false} \text{ und } \mathbf{false} \vee A = A\} \\ &= \quad (y \leq 0 \wedge z = a^b)\end{aligned}$$

Damit ist auch gezeigt, dass $false$ kein Fixpunkt für die Nachbedingung $z = a^b$ ist.

$$\begin{aligned} & (y \leq 0 \wedge z = a^b) \ \vee (0 < y \leq n-1 \wedge z * x^y = a^b) \\ = \quad & (y \leq 0 \wedge z = a^b) \ \vee (0 < y \leq 0 \wedge z * x^y = a^b) \\ & \{\text{Definition: } 0 < y \leq 0 = \mathbf{false}\} \\ = \quad & (y \leq 0 \wedge z = a^b) \\ \Rightarrow \quad & \tau[\mathbf{false}]\end{aligned}$$

Induktionsschritt: Wir nehmen nun an, dass die Implikation

$$\tau^n(\mathbf{false}) \ \Leftarrow \ (y \leq 0 \wedge z = a^b) \ \vee \ (0 < y \leq n-1 \wedge z * x^y = a^b)$$

für n gilt und zeigen, dass sie auch für $n + 1$ gilt.

Sei $Q_n = (y \leq 0 \wedge z = a^b) \ \vee \ (0 < y \leq n-1 \wedge z * x^y = a^b)$.
Die Monotonie von τ stellt sicher, dass $\tau^{n+1}[false] \Leftarrow \tau[Q_n]$ gilt.
Es genügt zu zeigen, dass $\tau[Q_n] \Leftarrow Q_{n+1}$ gilt.

$\tau[Q_n]$
$= (y \leq 0 \wedge z = a^b) \vee$
$(y > 0 \wedge odd(y) \wedge Q_n[(y-1)/y, (z*x)/z]) \vee$
$(y > 0 \wedge even(y) \wedge Q_n[(x*x)/x, (y \div 2)/y])$

$= (y \leq 0 \wedge z = a^b) \vee$
$(y > 0 \wedge odd(y) \wedge ((y-1 \leq 0 \wedge z*x = a^b) \ \vee (0 < y-1 \leq n-1 \wedge z*x*x^{y-1} = a^b))) \vee$
$(y > 0 \wedge even(y) \wedge (((y \div 2) \leq 0 \wedge z = a^b) \ \vee (0 < (y \div 2) \leq n-1 \wedge z*(x*x)^{y \div 2} = a^b)))$

$= (y \leq 0 \wedge z = a^b) \vee$
$(odd(y) \wedge (1 < y \leq n) \wedge (z*x^y = a^b)) \vee$
$(even(y) \wedge (0 < y \leq 2*(n-1)) \wedge (z*x^y = a^b))$

$\Leftarrow (y \leq 0 \wedge z = a^b) \ \vee \ (0 < y \leq n \wedge z*x^y = a^b) = Q_{n+1}$

Es gilt also, dass $\forall\ n : \tau^n[\textbf{false}] \Leftarrow Q_n$

(d) Da $wp(P, C)$ stetig ist, läßt sich der stärkste Fixpunkt von τ bestimmen.

Aus $\forall\ n : \tau^n[\textbf{false}] \Leftarrow Q_n$ können wir unmittelbar schließen, dass gilt:
$\exists\ n : \tau^n[\textbf{false}] \Leftarrow \exists\ n : Q_n$.
Da $\exists\ n : \tau^n[\textbf{false}]$ das stärkste Prädikat von τ ist, wissen wir auch, dass für alle R mit $R = \tau[R]$ gilt:

$\exists\ n : \tau^n[\textbf{false}] \Leftarrow R$

Wenn wir zeigen können, dass $\exists\ n : Q_n = \tau[\exists n : Q_n]$, so gilt auch:

$\exists\ n : \tau^n[\textbf{false}] \Leftrightarrow \exists\ n : \tau[Q_n]$

Nun zeigen wir also, dass $\exists\ n : Q_n = \tau[\exists n : Q_n]$.

$$
\begin{aligned}
\tau[\exists n : Q_n] \quad & = (y \leq 0 \land z = a^b) \lor \\
& (y > 0 \land odd(y) \land \exists n : Q_n[(y-1)/y, (z * x)/z]) \lor \\
& (y > 0 \land even(y) \land \exists n : Q_n[(x * x)/x, (y \div 2)/y])
\end{aligned}
$$

{Substitution, Eigenschaften von Multiplikation}

$$
\begin{aligned}
& = (y \leq 0 \land z = a^b) \lor \\
& (y > 0 \land odd(y) \land \exists n : (0 < y - 1 \leq n - 1) \land (z * x^y = a^b)) \lor \\
& (y > 0 \land even(y) \land \exists n : (0 < y \leq 2 * (n-1)) \land (z * x^y = a^b))
\end{aligned}
$$

$$
\begin{aligned}
& = (y \leq 0 \land z = a^b) \lor \\
& (y > 0 \land odd(y) \land \exists n : (1 < y \leq n) \land (z * x^y = a^b)) \lor \\
& (y > 0 \land even(y) \land \exists n : (0 < y \leq 2 * (n-1)) \land (z * x^y = a^b))
\end{aligned}
$$

{n kommt nicht in $y > 0 \land odd(y)$ vor: Ersetzung von n durch $n' - 1$ } sowie
{n kommt nicht in $y > 0 \land even(y)$ vor: Ersetzung von $2 * (n-1)$ durch $n' - 1$ }

$$
\begin{aligned}
& = (y \leq 0 \land z = a^b) \lor \\
& \exists n' : (y > 0 \land odd(y) \land (1 < y \leq n' - 1) \land (z * x^y = a^b)) \lor \\
& \exists n' : (y > 0 \land even(y) \land (0 < y \leq n' - 1)) \land (z * x^y = a^b))
\end{aligned}
$$

$$
\begin{aligned}
& = (y \leq 0 \land z = a^b) \lor \\
& \exists n : (y > 0 \land odd(y) \land (1 < y \leq n - 1) \land (z * x^y = a^b)) \lor \\
& \exists n : (y > 0 \land even(y) \land (0 < y \leq n - 1)) \land (z * x^y = a^b))
\end{aligned}
$$

$$
\begin{aligned}
& = (y \leq 0 \land z = a^b) \lor \\
& \exists n : (y > 0 \land odd(y) \land (1 < y \leq n - 1) \land (z * x^y = a^b)) \lor \\
& \exists n : (y > 0 \land even(y) \land (1 < y \leq n - 1)) \land (z * x^y = a^b))
\end{aligned}
$$

$\{\exists n : A \ \lor \ \exists n : B = \exists n : (A \ \lor \ B), odd(y) \ \lor \ even(y) = \mathbf{true}\}$

$$= \exists n : (y \leq 0 \land z = a^b) \ \lor \ ((1 < y \leq n - 1) \land (z * x^y = a^b))$$

$$\Rightarrow \exists n : (y \leq 0 \land z = a^b) \ \lor \ ((0 < y \leq n - 1) \land (z * x^y = a^b))$$

$$= \exists n : Q_n$$

Also, $\tau[\exists n : Q_n] \Rightarrow \exists n : Q_n$

(e) Berechnung von $wp(P,\ z = a^b)$ mit Hilfe der Semikolon-Regel.

$$
\begin{aligned}
& wp(x := a;\ y := b;\ z := 1,\ \exists n : Q_n) \\
= \quad & \exists n : Q_n[a/x, b/y, 1/z] \\
= \quad & \exists n : (b \leq 0 \wedge 1 = a^b) \vee (0 < b \leq n-1 \wedge 1 * a^b = a^b) \\
= \quad & \exists n : (0 < b \leq n-1 \wedge a^b = a^b) \\
= \quad & \exists n : (0 < b \leq n-1) \\
= \quad & \mathbf{true}
\end{aligned}
$$

Aufgabe 2 *wp*–Semantik [LÖSUNG]

(a) Annahme: Alle Ausdrücke liefern wohldefinierte Ergebnisse. Insbesondere evaluieren für die wp-Berechnung die **Def**-Abfragen somit stets zu *true* und werden im Folgenden nicht mehr explizit aufgeführt.

i) $\mathsf{wp}(x := x+1, x \leq 1) \quad \equiv \quad \{x+1 \leq 1\} \quad \equiv \quad \{x \leq 0\}$

ii) $\mathsf{wp}(\ \mathbf{if}\ x \geq y\ \mathbf{then}\ z := x\ []\ y \geq x\ \mathbf{then}\ z := y\ \mathbf{fi}\ , z = max(x,y))$

$$
\begin{aligned}
&\equiv ((x \geq y) \vee (y \geq x)) \quad \wedge \quad (x \geq y \ \Rightarrow\ wp(z := x; z = max(x,y))) \quad \wedge \\
&\quad\ (y \geq x \ \Rightarrow\ wp(z := y; z = max(x,y))) \\
&\equiv \mathbf{true}
\end{aligned}
$$

iii) $\mathsf{wp}(\ \mathbf{if}\ x \geq y\ \mathbf{then}\ z := x\ []\ y \geq x\ \mathbf{then}\ z := y\ \mathbf{fi}\ , z = y-1)$

$$
\begin{aligned}
&\equiv ((x \geq y) \vee (y \geq x)) \quad \wedge \quad (x \geq y \ \Rightarrow\ wp(z := x; z = y-1)) \quad \wedge \\
&\quad\ (y \geq x \ \Rightarrow\ wp(z := y; z = y-1)) \\
&\equiv \mathbf{false}
\end{aligned}
$$

iv) $\mathsf{wlp}(x := x+1, x \leq 1) \equiv \{\ x \leq 0\}$

v) $\mathsf{wlp}(\ \mathbf{if}\ x \geq y\ \mathbf{then}\ z := x\ []\ y \geq x\ \mathbf{then}\ z := y\ \mathbf{fi}\ , z = max(x,y))$

$$
\begin{aligned}
&\equiv (x \geq y \ \Rightarrow\ wlp(z := x; z = max(x,y))) \quad \wedge \\
&\quad\ (y \geq x \ \Rightarrow\ wlp(z := y; z = max(x,y))) \\
&\equiv \mathbf{true}
\end{aligned}
$$

vi) $\mathsf{wlp}(\ \mathbf{if}\ x \geq y\ \mathbf{then}\ z := x\ []\ y \geq x\ \mathbf{then}\ z := y\ \mathbf{fi}\ , z = y-1)$

$$
\begin{aligned}
&\equiv (x \geq y \ \Rightarrow\ wp(z := x; z = y-1)) \quad \wedge \\
&\quad\ (y \geq x \ \Rightarrow\ wp(z := y; z = y-1)) \\
&\equiv \mathbf{false}
\end{aligned}
$$

(b) i) $\mathsf{wp}(\mathbf{nop}; P_1, R) = \mathsf{wp}(P_1;\mathbf{nop}, R)$

Linke Seite: $\mathsf{wp}(\mathbf{nop};P_1,\ R) \equiv \mathsf{wp}(\mathbf{nop},\mathsf{wp}(P_1, R)) \equiv \mathsf{wp}(P_1, R)$

Rechte Seite: $\mathsf{wp}(P_1;\mathbf{nop},\ R) \equiv \mathsf{wp}(P_1,\ \mathsf{wp}(\mathbf{nop},\ R) \equiv \mathsf{wp}(P_1, R)$

ii) $\mathsf{wp}(\mathbf{abort};P_1, R) = \mathsf{wp}(P_1;\mathbf{abort}, R)$

L.S.: $\mathsf{wp}(\mathbf{abort};P_1,\ R) \equiv \mathsf{wp}(\mathbf{abort},\ wp(P_1, R)) \equiv \mathbf{false}$

R.S.: $\mathsf{wp}(P_1;\mathbf{abort},\ R) \equiv \mathsf{wp}(P_1,\ \mathsf{wp}(\mathbf{abort},\ R)) \equiv \mathsf{wp}(P_1,\ \mathbf{false}) \equiv \mathbf{false}$

iii) $\mathsf{wlp}(\mathbf{nop}; P_1, R) = \mathsf{wlp}(P_1;\mathbf{nop}, R)$

$\mathsf{wlp}(\mathbf{nop};P_1,\ R) \equiv \mathsf{wlp}(\mathbf{nop},\mathsf{wlp}(P_1, R)) \equiv \mathsf{wlp}(P_1, R)$

$\mathsf{wlp}(P_1;\mathbf{nop},\ R) \equiv \mathsf{wlp}(P_1,\ \mathsf{wlp}(\mathbf{nop},\ R) \equiv \mathsf{wlp}(P_1, R)$

iv) $\mathsf{wlp}(\mathbf{abort};P_1, R) = \mathsf{wlp}(P_1;\mathbf{abort}, R)$

$\mathsf{wlp}(\mathbf{abort};P_1,\ R) \equiv \mathsf{wlp}(\mathbf{abort},\ \mathsf{wlp}(P_1, R)) \equiv \mathbf{true}$

$\mathsf{wlp}(P_1;\mathbf{abort},\ R) \equiv \mathsf{wlp}(P_1,\ \mathsf{wlp}(\mathbf{abort},\ R)) \equiv \mathsf{wlp}(P_1,\ \mathbf{true}) \equiv \mathbf{true}$