Analyse und Verifikation

(185.276, VU 2.0, ECTS 3.0)

Übungsblatt 4

Bernhard Urban
Matr.Nr.: 0725771 KNZ: 067 937
lewurm@gmail.com

Thomas Reinbacher
Matr.Nr.: 0828472 KNZ: 786 881
treinbacher@ecs.tuwien.ac.at

17.05.2011

Aufgabe 2.1:

Es gilt zu zeigen, dass die Ausführungszeit des Programms zur Berechnung der Fakultät in der Größenordnung von $\mathcal{O}(1)$ liegt (wobei x den Wert 3 hat).

$$
\begin{array}{l}
\{\, Pre\colon x = 3 \,\} \\
y := 1; \\
\textsf{while}\ x \neq 1\ \textsf{do} \\
\quad y := y * x; \\
\quad x := x - 1; \\
\textsf{od} \\
\{\, Post\colon 1 \Downarrow true \,\}
\end{array}
$$

Wir definieren zuerst ein Prädikat p_c, dass die Invariante der while Schleife beschreibt.

$$p_c(z) = (3 \geq x > 0 \land x = z + 1)$$

Wir führen nun die frische logische Variable u_1 ein, die wir für die while Schleife verwenden. Unter Anwendung der $[\mathsf{ass}_e]$ Regel erhalten wir:

$$
\begin{array}{l}
\{\, (p_c(z) \land x \leq u_1)[x - 1/x] \,\} \\
\quad x := x - 1; \\
\{\, 1 \Downarrow p_c(z) \land x \leq u_1 \,\}
\end{array}
$$

Wir führen nun eine zweite frische logische Variable u_2 ein. Eine weitere Anwendung der $[\mathsf{ass}_e]$ Regel für die zweite Zuweisung in der Schleife ergibt:

$$
\begin{array}{l}
\{\, ((p_c(z) \wedge x \leq u_1)[x-1/x] \wedge 1 \leq u_2)[y*x/y] \,\} \\
\quad y := y * x; \\
\{\, 1 \Downarrow (p_c(z) \wedge x \leq u_1)[x-1/x] \wedge 1 \leq u_2 \,\}
\end{array}
$$

Die Anwendung der [comp_e] Regel macht es notwendig die Ausdrücke $x \leq u_1$ sowie $1 \leq u_2$ per [cons_e] Regel in die Form $e' = u$ zu bringen (Folie 255). Die Bedingung:

$$\{\, ((p_c(z) \wedge x \leq u_1)[x-1/x] \wedge 1 \leq u_2)[y*x/y] \,\}$$

wird gestärkt zu

$$\{\, p_c(z+1) \wedge x - 1 = u_1 \wedge 1 = u_2 \,\}$$

Nun kann die Kompositionsregel mit $e_1 = 1$ und $e'_2 = 1$ angewendet werden:

$$
\begin{array}{l}
\{\, p_c(z+1) \wedge x - 1 = u_1 \,\} \\
\quad y := y * x; \\
\quad x := x - 1; \\
\{\, 1 + 1 \Downarrow p_c(z) \wedge x \leq u_1 \,\}
\end{array}
$$

Für die Anwendung der [while_e] Regel müssen die folgenden Implikationen gezeigt werden (Folie 256), wobei wir $e = 3$ wählen.

$$
\begin{array}{lrcl}
(1) & p_c(z+1) & \succ & (x \neq 1) \wedge e \geq e_1 + e' \\
 & 3 \geq x > 0 \wedge x = (z+1) + 1 & \succ & (x \neq 1) \wedge 3 \geq 1 + (x-1) \\
 & 3 \geq x > 0 \wedge x = z + 2 & \succ & (x \neq 1) \wedge 3 \geq x \quad \checkmark \\
 & & & \\
(2) & p_c(0) & \succ & (x = 1) \wedge 1 \leq e \\
 & 3 \geq x > 0 \wedge x = 0 + 1 & \succ & (x = 1) \wedge 1 \leq 3 \quad \checkmark
\end{array}
$$

Die eigentliche Anwendung der [while_e] Regel liefert:

$$
\begin{array}{l}
\{\, \exists z.\ p_c(z) \,\} \\
\mathsf{while}\ x \neq 1\ \mathsf{do} \\
\quad y := y * x; \\
\quad x := x - 1; \\
\mathsf{od} \\
\{\, 3 \Downarrow p_c(0) \,\}
\end{array}
$$

Für die Initialisierung $y := 1$ wenden wir die [ass_e] Regel an und führen eine neue frische logische Variable u_3 ein:

$$
\begin{array}{l}
\{\, (\exists z. p_c(z) \wedge 1 \leq u_3)[1/y] \,\} \\
\quad y := 1; \\
\{\, 1 \Downarrow \exists z. p_c(z) \wedge 1 \leq u_3 \,\}
\end{array}
$$

Unter Berücksichtigung der Precondition $\{ x = 3 \}$ ergibt sich mit der $[\mathsf{cons}_e]$ Regel:

$$\begin{array}{l}
\{ x = 3 \land 1 = u_3 \} \\
\quad y := 1; \\
\{ 1 \Downarrow \exists z. p_c(z) \land 1 \leq u_3 \}
\end{array}$$

Die Anwendung von $[\mathsf{comp}_e]$ auf die Initialisierung und die Schleife liefert:

$$\begin{array}{l}
\{ x = 3 \} \\
\quad y := 1; \\
\quad \mathsf{while}\ x \neq 1\ \mathsf{do} \\
\quad\quad y := y * x; \\
\quad\quad x := x - 1; \\
\quad \mathsf{od} \\
\{ 1 + 3 \Downarrow p_c(0) \}
\end{array}$$

Mit $p_c(0) \succ \mathit{true}$ und $1+3 \leq 4*1$ können wir ein letztes Mal die $[\mathsf{cons}_e]$ Regel anwenden und erhalten:

$$\begin{array}{l}
\{ x = 3 \} \\
\quad y := 1; \\
\quad \mathsf{while}\ x \neq 1\ \mathsf{do} \\
\quad\quad y := y * x; \\
\quad\quad x := x - 1; \\
\quad \mathsf{od} \\
\{ 1 \Downarrow \mathit{true} \}
\end{array}$$

$\square$

Aufgabe 2.2:
Es gilt zu zeigen, dass die Ausführungszeit des Programms zur Berechnung der Fakultät in der Größenordnung von $\mathcal{O}(x)$ liegt.

$$\begin{array}{l}
\{ \mathit{Pre}\colon x > 0 \} \\
y := 1; \\
\mathsf{while}\ x \neq 1\ \mathsf{do} \\
\quad y := y * x; \\
\quad x := x - 1; \\
\mathsf{od} \\
\{ \mathit{Post}\colon x \Downarrow \mathit{true} \}
\end{array}$$

Wir definieren zuerst ein Prädikat p_l, dass die Invariante der while Schleife beschreibt.

$$p_l(z) = (x > 0 \land x = z + 1)$$

Wir führen nun die frische logische Variable u_1 ein, die wir für die while Schleife verwenden. Unter Anwendung der $[\mathsf{ass}_e]$ Regel erhalten wir:

$$\begin{array}{l} \{\, (p_l(z) \wedge x \leq u_1)[x-1/x] \,\} \\ \quad x := x - 1; \\ \{\, 1 \Downarrow p_l(z) \wedge x \leq u_1 \,\} \end{array}$$

Wir führen nun eine zweite frische logische Variable u_2 ein. Eine weitere Anwendung der $[\mathsf{ass}_e]$ Regel für die zweite Zuweisung in der Schleife ergibt:

$$\begin{array}{l} \{\, ((p_l(z) \wedge x \leq u_1)[x-1/x] \wedge 1 \leq u_2)[y * x/y] \,\} \\ \quad y := y * x; \\ \{\, 1 \Downarrow (p_l(z) \wedge x \leq u_1)[x-1/x] \wedge 1 \leq u_2 \,\} \end{array}$$

Die Anwendung der $[\mathsf{comp}_e]$ Regel macht es notwendig die Ausdrücke $x \leq u_1$ sowie $1 \leq u_2$ per $[\mathsf{cons}_e]$ Regel in die Form $e' = u$ zu bringen (Folie 255). Die Bedingung:

$$\{\, ((p_l(z) \wedge x \leq u_1)[x-1/x] \wedge 1 \leq u_2)[y * x/y] \,\}$$

wird gestärkt zu

$$\{\, p_l(z+1) \wedge x - 1 = u_1 \wedge 1 = u_2 \,\}$$

Nun kann die Kompositionsregel mit $e_1 = 1$ und $e_2' = 1$ angewendet werden:

$$\begin{array}{l} \{\, p_l(z+1) \wedge x - 1 = u_1 \,\} \\ \quad y := y * x; \\ \quad x := x - 1; \\ \{\, 1 + 1 \Downarrow p_l(z) \wedge x \leq u_1 \,\} \end{array}$$

Für die Anwendung der $[\mathsf{while}_e]$ Regel müssen die folgenden Implikationen gezeigt werden (Folie 256), wobei wir $e = x$ wählen.

$$\begin{array}{lrcl} (1) & p_l(z+1) & \succ & (x \neq 1) \wedge e \geq e_1 + e' \\ & x > 0 \wedge x = (z+1)+1 & \succ & (x \neq 1) \wedge x \geq 1 + (x-1) \\ & x > 0 \wedge x = z + 2 & \succ & (x \neq 1) \wedge x \geq x \quad \checkmark \\ \\ (2) & p_l(0) & \succ & (x = 1) \wedge 1 \leq e \\ & x > 0 \wedge x = 0 + 1 & \succ & (x = 1) \wedge 1 \leq x \quad \checkmark \end{array}$$

Die eigentliche Anwendung der $[\mathsf{while}_e]$ Regel liefert:

$$\begin{array}{l} \{\, \exists z.\ p_l(z) \,\} \\ \mathsf{while}\ x \neq 1\ \mathsf{do} \\ \quad y := y * x; \\ \quad x := x - 1; \\ \mathsf{od} \\ \{\, x \Downarrow p_l(0) \,\} \end{array}$$

Für die Initialisierung $y := 1$ wenden wir die $[\mathsf{ass}_e]$ Regel an und führen eine neue frische logische Variable u_3 ein:

$$
\begin{array}{l}
\{\, (\exists z.p_l(z) \wedge 1 \leq u_3)[1/y] \,\} \\
\quad y := 1; \\
\{\, 1 \Downarrow \exists z.p_l(z) \wedge 1 \leq u_3 \,\}
\end{array}
$$

Unter Berücksichtigung der Precondition $\{\, x > 0 \,\}$ ergibt sich mit der [cons_e] Regel:

$$
\begin{array}{l}
\{\, x > 0 \wedge 1 = u_3 \,\} \\
\quad y := 1; \\
\{\, 1 \Downarrow \exists z.p_l(z) \wedge 1 \leq u_3 \,\}
\end{array}
$$

Die Anwendung von [comp_e] auf die Initialisierung und die Schleife liefert:

$$
\begin{array}{l}
\{\, x > 0 \,\} \\
\quad y := 1; \\
\quad \mathsf{while}\ x \neq 1\ \mathsf{do} \\
\qquad y := y * x; \\
\qquad x := x - 1; \\
\quad \mathsf{od} \\
\{\, 1 + x \Downarrow p_l(0) \,\}
\end{array}
$$

Mit $p_l(0) \succ \mathit{true}$ und $x > 0 \succ 1 + x \leq 2 * x$ können wir ein letztes Mal die [cons_e] Regel anwenden und erhalten:

$$
\begin{array}{l}
\{\, x > 0 \,\} \\
\quad y := 1; \\
\quad \mathsf{while}\ x \neq 1\ \mathsf{do} \\
\qquad y := y * x; \\
\qquad x := x - 1; \\
\quad \mathsf{od} \\
\{\, x \Downarrow \mathit{true} \,\}
\end{array}
$$

$\square$

Aufgabe 1:

Sei $\sigma \in \Sigma$ mit $\sigma(x) = 3$, dann gilt:

$$\langle y := 1;\ \textsf{while}\ x \neq 1\ \textsf{do}\ y := y * x;\ x := x - 1\ \textsf{od}, \sigma\rangle \to \sigma[6/y][1/x]$$

$$\dfrac{\dfrac{—}{\langle y := y * x, \sigma[3/y][2/x]\rangle \to^3 \sigma[6/y][2/x]}\,[\text{ass}]_{tns} \qquad \dfrac{—}{\langle x := x - 1, \sigma[6/y][2/x]\rangle \to^3 \sigma[6/y][1/x]}\,[\text{ass}]_{tns}}{\mathbf{V} = \langle y := y * x;\ x := x - 1, \sigma[3/y][2/x]\rangle \to^6 \sigma[6/y][1/x]}\,[\text{comp}]_{tns}$$

$$\dfrac{\mathbf{V} \qquad \dfrac{—}{\langle \textsf{while}\ x \neq 1\ \textsf{do}\ y := y * x;\ x := x - 1\ \textsf{od}, \sigma[6/y][1/x]\rangle \to^6 \sigma[6/y][1/x]}\,[\text{while}]^{ff}_{tns}}{\mathbf{T} = \langle \textsf{while}\ x \neq 1\ \textsf{do}\ y := y * x;\ x := x - 1\ \textsf{od}, \sigma[3/y][2/x]\rangle \to^{17} \sigma[6/y][1/x]}\,[\text{while}]^{tt}_{tns}$$

$$\dfrac{\dfrac{—}{\langle y := 1, \sigma\rangle \to^2 \sigma[1/y]}\,[\text{ass}]_{tns} \qquad \dfrac{\dfrac{\dfrac{—}{\langle y := y * x, \sigma[1/y]\rangle \to^3 \sigma[3/y]}\,[\text{ass}]_{tns} \qquad \dfrac{—}{\langle x := x - 1, \sigma[3/y]\rangle \to^3 \sigma[3/y][2/x]}\,[\text{ass}]_{tns}}{\langle y := y * x;\ x := x - 1, \sigma[1/y]\rangle \to^6 \sigma[3/y][2/x]}\,[\text{comp}]_{tns} \qquad \mathbf{T}}{\langle \textsf{while}\ x \neq 1\ \textsf{do}\ y := y * x;\ x := x - 1\ \textsf{od}, \sigma[1/y]\rangle \to^{28} \sigma[6/y][1/x]}\,[\text{while}]^{tt}_{tns}}{\langle y := 1;\ \textsf{while}\ x \neq 1\ \textsf{do}\ y := y * x;\ x := x - 1\ \textsf{od}, \sigma\rangle \to^{30} \sigma[6/y][1/x]}\,[\text{comp}]_{tns}$$

Anmerkung: Anders als beim Beispiel in den Folien, kommen wir auf insgesamt 30 Zeiteinheiten (statt 33). Der Hintergrund ist, dass in den Folien für die Auswertung von der Schleifenbedingung $x \neq 1$ vier Zeiteinheiten bemessen werden, wir jedoch der Meinung sind es sind nur drei nötig:

$$[\![x \neq 1]\!]_{TB} = [\![x]\!]_{TA} + [\![1]\!]_{TA} + \mathbf{1} = \mathbf{1} + \mathbf{1} + \mathbf{1} = \mathbf{3}$$

Zugegeben, es kommt auf die Definition von $\neq$ an: ist der Operator direkt definiert (unsere Annahme) oder indirekt per $\neg$ und $=$ (Annahme in den Folien?).

$\square$