Universität Karlsruhe (TH)
Lehrstuhl Informatik für Ingenieure und Naturwissenschaftler
Dr. Thomas Worsch
Matthias Schulz

7. Juli 2008

Einführung in die Informatik

Lösungen zu Übungsblatt 11

– Verifikation –

Aufgabe 1:

a) Wir stellen Tabellen für die jeweiligen Werten auf:

Befehl	$\underline{\texttt{x}}$	$\underline{\texttt{y}}$
	3	4
$\texttt{x} \leftarrow \texttt{x} + \texttt{y}$	7	4
$\texttt{y} \leftarrow \texttt{x} - \texttt{y}$	7	3
$\texttt{x} \leftarrow \texttt{x} - \texttt{y}$	4	3

Befehl	$\underline{\texttt{x}}$	$\underline{\texttt{y}}$
	5	2
$\texttt{x} \leftarrow \texttt{x} + \texttt{y}$	7	2
$\texttt{y} \leftarrow \texttt{x} - \texttt{y}$	7	5
$\texttt{x} \leftarrow \texttt{x} - \texttt{y}$	2	5

b) Das Programm vertauscht die Werte der Variablen `x` und `y`.

c) Wir gehen davon aus, dass anfangs $\underline{\texttt{x}} = a$ und $\underline{\texttt{y}} = b$ gilt und nach Ablauf des Programms nach unserer Hypothese $\underline{\texttt{x}} = b$ und $\underline{\texttt{y}} = a$ gilt.

Wir gehen von folgendem Schema aus:

$\langle \underline{\texttt{x}} = a \wedge \underline{\texttt{y}} = b \rangle$
$\texttt{x} \leftarrow \texttt{x} + \texttt{y}$
$\langle \rangle$
$\texttt{y} \leftarrow \texttt{x} - \texttt{y}$
$\langle \rangle$
$\texttt{x} \leftarrow \texttt{x} - \texttt{y}$
$\langle \underline{\texttt{x}} = b \wedge \underline{\texttt{y}} = a \rangle$

Da im letzten Befehl $\texttt{x} \leftarrow \texttt{x} - \texttt{y}$ der Wert von `x` durch $\underline{\texttt{x}} - \underline{\texttt{y}}$ ersetzt wird, ersetzen wir in der letzten Zeile, also der Nachbedingung des letzten Befehls, $\underline{\texttt{x}}$ durch $\underline{\texttt{x}} - \underline{\texttt{y}}$, um die Zeile oberhalb des letzten Befehls, also die Vorbedingung des letzten Befehls, zu erhalten.

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + \mathtt{y}$
$\langle \rangle$
$\mathtt{y} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} - \underline{\mathtt{y}} = b \wedge \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} = b \wedge \underline{\mathtt{y}} = a \rangle$

Da im vorletzten Befehl $\mathtt{y} \leftarrow \mathtt{x} - \mathtt{y}$ der Wert von $\mathtt{x}$ durch $\underline{\mathtt{x}} - \underline{\mathtt{y}}$ ersetzt wird, ersetzen wir in der Nachbedingung $\underline{\mathtt{x}}$ durch $\underline{\mathtt{x}} - \underline{\mathtt{y}}$, um die Vorbedingung des vorletzten Befehls zu erhalten.

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + \mathtt{y}$
$\langle \underline{\mathtt{x}} - (\underline{\mathtt{x}} - \underline{\mathtt{y}}) = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\mathtt{y} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} - \underline{\mathtt{y}} = b \wedge \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} = b \wedge \underline{\mathtt{y}} = a \rangle$

Zur Vereinfachung fügen wir einen Zwischenschritt ein:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + \mathtt{y}$
$\langle \underline{\mathtt{y}} = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}} - (\underline{\mathtt{x}} - \underline{\mathtt{y}}) = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\mathtt{y} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} - \underline{\mathtt{y}} = b \wedge \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} = b \wedge \underline{\mathtt{y}} = a \rangle$

Wir ersetzen nun entsprechend dem ersten Befehl $\underline{\mathtt{x}}$ durch $\underline{\mathtt{x}} + \underline{\mathtt{y}}$.

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$
$\langle \underline{\mathtt{y}} = b \wedge (\underline{\mathtt{x}} + \underline{\mathtt{y}}) - \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + \mathtt{y}$
$\langle \underline{\mathtt{y}} = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}} - (\underline{\mathtt{x}} - \underline{\mathtt{y}}) = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\mathtt{y} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} - \underline{\mathtt{y}} = b \wedge \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} = b \wedge \underline{\mathtt{y}} = a \rangle$

Da $\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$ die Zusicherung $\langle \underline{\mathtt{y}} = b \wedge (\underline{\mathtt{x}} + \underline{\mathtt{y}}) - \underline{\mathtt{y}} = a \rangle$ impliziert, erhalten wir:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$
$\Downarrow$
$\langle \underline{\mathtt{y}} = b \wedge (\underline{\mathtt{x}} + \underline{\mathtt{y}}) - \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + \mathtt{y}$
$\langle \underline{\mathtt{y}} = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}} - (\underline{\mathtt{x}} - \underline{\mathtt{y}}) = b \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} = a \rangle$
$\mathtt{y} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} - \underline{\mathtt{y}} = b \wedge \underline{\mathtt{y}} = a \rangle$
$\mathtt{x} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{x}} = b \wedge \underline{\mathtt{y}} = a \rangle$

Damit ist unsere Behauptung verifiziert.

Aufgabe 2:

a) Das Programm berechnet das Negative des Betrags von $\underline{\mathtt{x}}$, als $-|\underline{\mathtt{x}}|$.

Angenommen, anfangs enthält $\mathtt{x}$ den Wert a. Dann ist $b = -|a|$ eindeutig definiert durch $b^2 = a^2 \wedge b \leq 0$.

Wir erhalten also folgendes Schema:

$\langle \underline{\mathtt{x}} = a \rangle$
if $\mathtt{x} > 0$
then $\mathtt{x} \leftarrow -\mathtt{x}$
fi $\langle \underline{\mathtt{x}}^2 = a^2 \wedge \underline{\mathtt{x}} \leq 0 \rangle$

Nach Vorlesung müssen wir überprüfen, dass

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{x}} > 0 \rangle$

eine gültige Vorbedingung ist, wenn

$\langle \underline{\mathtt{x}}^2 = a^2 \wedge \underline{\mathtt{x}} \leq 0 \rangle$

Nachbedingung von

then $\mathtt{x} \leftarrow -\mathtt{x}$

ist, und dass

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{x}} < 0 \rangle$

gültige Vorbedingung ist, wenn

$\langle \underline{\mathtt{x}}^2 = a^2 \wedge \underline{\mathtt{x}} \leq 0 \rangle$

Nachbedingung der leeren Operation ist (da es keinen **else**-Teil gibt).

Letzteres ist einfach:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{x}} < 0 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}}^2 = a^2 \wedge \underline{\mathtt{x}} \leq 0 \rangle$

gilt offensichtlich.

Verifikation des **if**-Teils:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{x}} > 0 \rangle$
$\Downarrow$
$\langle (-\underline{\mathtt{x}})^2 = a^2 \wedge -\underline{\mathtt{x}} \leq 0 \rangle$
$\mathtt{x} \leftarrow -\mathtt{x}$
$\langle \underline{\mathtt{x}}^2 = a^2 \wedge \underline{\mathtt{x}} \leq 0 \rangle$

Damit ist das Programm verifiziert.

b) Wenn anfangs $\underline{\mathtt{x}} = a$ und $\underline{\mathtt{y}} = b$ gilt, berechnet das Programm $|a - b|$ in Variable z. Dies ist gleichbedeutend mit $\underline{\mathtt{z}}^2 = (a - b)^2 \wedge \underline{\mathtt{z}} \geq 0$.

Verifikation des **if**-Teils (wurde von unten nach oben erstellt):

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \wedge (\underline{\mathtt{x}} > \underline{\mathtt{y}}) \rangle$
$\Downarrow$
$\langle (\underline{\mathtt{x}} - \underline{\mathtt{y}})^2 = (a - b)^2 \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} \geq 0 \rangle$
$\mathtt{z} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{z}}^2 = (a - b)^2 \wedge \underline{\mathtt{z}} \geq 0 \rangle$

(Der geklammerte Term in der ersten Zusicherung entspricht der Bedingung in der **if**-Anweisung.)

Verifikation des **else**-Teils (wurde von unten nach oben erstellt):

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \wedge (\underline{\mathtt{x}} \leq \underline{\mathtt{y}}) \rangle$
$\Downarrow$
$\langle (\underline{\mathtt{y}} - \underline{\mathtt{x}})^2 = (a - b)^2 \wedge \underline{\mathtt{y}} - \underline{\mathtt{x}} \geq 0 \rangle$
$\mathtt{z} \leftarrow \mathtt{y} - \mathtt{x}$
$\langle \underline{\mathtt{z}}^2 = (a - b)^2 \wedge \underline{\mathtt{z}} \geq 0 \rangle$

(Der geklammerte Term in der ersten Zusicherung entspricht der Negation der Bedingung in der **if**-Anweisung.)

Damit ist das gesamte Programm verifiziert:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \rangle$
if $\mathtt{x} > \mathtt{y}$
then
$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \wedge \underline{\mathtt{x}} > \underline{\mathtt{y}} \rangle$
$\Downarrow$
$\langle (\underline{\mathtt{x}} - \underline{\mathtt{y}})^2 = (a - b)^2 \wedge \underline{\mathtt{x}} - \underline{\mathtt{y}} \geq 0 \rangle$
$\mathtt{z} \leftarrow \mathtt{x} - \mathtt{y}$
$\langle \underline{\mathtt{z}}^2 = (a - b)^2 \wedge \underline{\mathtt{z}} \geq 0 \rangle$
else
$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = b \wedge \underline{\mathtt{x}} \leq \underline{\mathtt{y}} \rangle$
$\Downarrow$

$\langle(\underline{\mathtt{y}} - \underline{\mathtt{x}})^2 = (a-b)^2 \wedge \underline{\mathtt{y}} - \underline{\mathtt{x}} \geq 0\rangle$
$\mathtt{z} \leftarrow \mathtt{y} - \mathtt{x}$
$\langle\underline{\mathtt{z}}^2 = (a-b)^2 \wedge \underline{\mathtt{z}} \geq 0\rangle$
fi
$\langle\underline{\mathtt{z}}^2 = (a-b)^2 \wedge \underline{\mathtt{z}} \geq 0\rangle$

Aufgabe 3:

a) Sei anfangs $\underline{\mathtt{x}} = a$. Dann setzt das Programm $\underline{\mathtt{y}}$ und $\underline{\mathtt{z}}$ auf a und $\underline{\mathtt{x}}$ auf 0.

Eine geeignete Schleifeninvariante wäre $\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a\rangle$.

Wir beginnen mit dem Schema aus der Vorlesung:

$\langle\underline{\mathtt{x}} = a\rangle$
$\mathtt{y} \leftarrow 0$
$\mathtt{z} \leftarrow 0$
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a\rangle$
while $\mathtt{x} \neq 0$ **do**
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \wedge (\underline{\mathtt{x}} \neq 0)\rangle$
$\mathtt{x} \leftarrow \mathtt{x} - 1$
$\mathtt{y} \leftarrow \mathtt{y} + 1$
$\mathtt{z} \leftarrow \mathtt{z} + 1$
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a\rangle$
od
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \wedge (\underline{\mathtt{x}} = 0)\rangle$
$\langle\underline{\mathtt{y}} = a \wedge \underline{\mathtt{z}} = a \wedge x = 0\rangle$

Die geklammerten Terme aus der Zusicherung direkt zu Beginn der Schleife und nach Ende der Schleife entspricht der Schleifenbedingung beziehungsweise der Negation der Schleifenbedingung.

Nun füllen wir dieses Schema von unten auf und erhalten:

$\langle\underline{\mathtt{x}} = a\rangle$
$\Downarrow$
$\langle\underline{\mathtt{x}} + 0 = a \wedge \underline{\mathtt{x}} + 0 = a\rangle$
$\mathtt{y} \leftarrow 0$
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + 0 = a\rangle$
$\mathtt{z} \leftarrow 0$
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a\rangle$
while $\mathtt{x} \neq 0$ **do**
$\langle\underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \wedge (\underline{\mathtt{x}} \neq 0)\rangle$
$\Downarrow$
$\langle\underline{\mathtt{x}} - 1 + \underline{\mathtt{y}} + 1 = a \wedge \underline{\mathtt{x}} - 1 + \underline{\mathtt{z}} + 1 = a\rangle$
$\mathtt{x} \leftarrow \mathtt{x} - 1$

$\langle \underline{\mathtt{x}} + \underline{\mathtt{y}} + 1 = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} + 1 = a \rangle$
$\mathtt{y} \leftarrow \mathtt{y} + 1$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} + 1 = a \rangle$
$\mathtt{z} \leftarrow \mathtt{z} + 1$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \rangle$
od
$\langle \underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \wedge (\underline{\mathtt{x}} = 0) \rangle$
$\Downarrow$
$\langle \underline{\mathtt{y}} = a \wedge \underline{\mathtt{z}} = a \wedge x = 0 \rangle$

Hinweis: Auf solche seltsamen Zusicherungen wie

$\langle \underline{\mathtt{x}} + 0 = a \wedge \underline{\mathtt{x}} + 0 = a \rangle$

kommt man fast nur durch Ersetzen von unten nach oben.

b) Sei anfangs $\underline{\mathtt{x}} = a$ und $\underline{\mathtt{z}} = b$. Dann setzt das Programm $\underline{\mathtt{x}}$ auf $a + b$ und $\underline{\mathtt{z}}$ auf 0.

Eine geeignete Schleifeninvariante wäre $\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \rangle$.

Wir beginnen mit dem Schema aus der Vorlesung:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{z}} = b \rangle$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \rangle$
while $\mathtt{z} \neq 0$ **do**
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \wedge \underline{\mathtt{z}} \neq 0 \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + 1$
$\mathtt{z} \leftarrow \mathtt{z} - 1$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \rangle$
od
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \wedge \underline{\mathtt{z}} = 0 \rangle$
$\langle \underline{\mathtt{x}} = a + b \wedge \underline{\mathtt{z}} = 0 \rangle$

Nun füllen wir dieses Schema von unten auf und erhalten:

$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{z}} = b \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \rangle$
while $\mathtt{z} \neq 0$ **do**
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \wedge \underline{\mathtt{z}} \neq 0 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}} + 1 + \underline{\mathtt{z}} - 1 = a + b \rangle$
$\mathtt{x} \leftarrow \mathtt{x} + 1$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} - 1 = a + b \rangle$
$\mathtt{z} \leftarrow \mathtt{z} - 1$
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \rangle$
od
$\langle \underline{\mathtt{x}} + \underline{\mathtt{z}} = a + b \wedge \underline{\mathtt{z}} = 0 \rangle$

$\Downarrow$
$\langle \underline{\mathtt{x}} = a + b \wedge \underline{\mathtt{z}} = 0 \rangle$

c) Wenn $\underline{\mathtt{x}}$ anfangs a ist, gilt nach Hintereinanderausführung der beiden Programme $\underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = a \wedge \underline{\mathtt{z}} = 0$.

Wir nennen die Programme P_1 und P_2 und verifizieren die Behauptung:

$\langle \underline{\mathtt{x}} = a \rangle$
P_1
$\langle \underline{\mathtt{x}} = 0 \wedge \underline{\mathtt{y}} = a \wedge \underline{\mathtt{z}} = a \rangle$
P_2
$\langle \underline{\mathtt{x}} = a + 0 \wedge \underline{\mathtt{y}} = a \wedge \underline{\mathtt{z}} = 0 \rangle$
$\Downarrow$
$\langle \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = a \wedge \underline{\mathtt{z}} = 0 \rangle$

d) Das angegebene Programm hält immer, während das Programm aus Teilaufgabe a) für $\underline{\mathtt{x}} < 0$ am Anfang nicht hält (die Verifikation hat also partielle Korrektheit gezeigt, während das Programm nicht total korrekt ist).

Das Endergebnis des Programmes sieht folgendermaßen aus, wenn anfangs $\underline{\mathtt{x}} = a$ gilt:

$\langle \underline{\mathtt{x}} = \min\{0, a\} \wedge \underline{\mathtt{y}} = \max\{0, a\} \wedge \underline{\mathtt{z}} = \max\{0, a\} \rangle$

Dieses Ergebnis ist sehr viel sperriger als das Ergebnis des Programmes in Teilaufgabe a), was auch Auswirkungen auf die Schleifeninvariante hat:

Die Schleifeninvariante $\langle \underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \rangle$ würde nach Beendigung der Schleife nur zur Zusicherung $\langle \underline{\mathtt{x}} + \underline{\mathtt{y}} = a \wedge \underline{\mathtt{x}} + \underline{\mathtt{z}} = a \rangle \wedge x \leq 0$ führen, aus der sich das gewünschte Ergebnis nicht herleiten lässt.

Eine funktionierende Schleifeninvariante wäre zum Beispiel $\langle (a \geq 0 \wedge \underline{\mathtt{x}} \geq 0 \wedge \underline{\mathtt{y}} = a - \underline{\mathtt{x}} \wedge \underline{\mathtt{z}} = a - \underline{\mathtt{x}}) \vee$
$(a < 0 \wedge \underline{\mathtt{x}} = a \wedge \underline{\mathtt{y}} = 0 \wedge \underline{\mathtt{z}} = 0) \rangle$, mit der sehr unhandlich zu rechnen ist.