Grundlagen der Programmierung

SS 05
Prof. Dr. K. Madlener
Lösungshinweise zu Übungsblatt 4

Aufgabe 4.1. Sei α eine Schleife über (S, Σ) und V (d.h. $\alpha =$ **while** B **do** β **end**;).

$I.V.^{\text{groß}}$: Für alle Zustände z,z' über A und V und alle Teilprogramme β von α gilt:
$z[\![\beta]\!]_A z'$ $gdw.$ $\exists t \in \mathbb{N} : I_A^t(\beta, z) = (\varepsilon, z')$.

$\rightarrow$: Es gelte $z[\![\alpha]\!]z'$,d.h. es gibt $n \in \mathbb{N}$ und Zustände $z_0, \ldots, z_n$ mit $z = z_0$, $A \models_{z_i} B$ und $z_i[\![\beta]\!]z_{i+1}$ f.a. $0 \leq i < n$, $A \not\models_{z_n} B$ und $z_n = z'$.
Nach I.V., gibt es $t_1, \ldots, t_n \in \mathbb{N}$ mit $I_A^{t_i}(\beta, z_i) = (\varepsilon, z_{i+1})$ f.a. $0 \leq i < n$. Wähle t_i jeweils minimal.
Es gilt nun:

$$\begin{aligned}
I_A^{(1+t_1)+\ldots+(1+t_n)+1}(\alpha, z) &= I_A^{t_1+\ldots+(1+t_n)+1}(\beta\alpha, z_0) && (A \models_{z_0} B)\\
&= I_A^{(1+t_2)+\ldots+(1+t_n)+1}(\alpha, z_1)\\
&\;\;\vdots\\
&= I_A^{(1+t_n)+1}(\alpha, z_{n-1})\\
&= I_A^{t_n+1}(\beta\alpha, z_{n-1}) && (A \models_{z_{n-1}} B)\\
&= I_A(\alpha, z_n)\\
&= (\varepsilon, z'). && (A \not\models_{z_n} B)
\end{aligned}$$

Für $t := n + 1 + \sum_{i=1}^{n} t_i$ gilt also $I_A^t(\alpha, z) = (\varepsilon, z')$.

$\leftarrow$: Es gelte $I_A^t(\alpha, z) = (\varepsilon, z')$.
Zu zeigen ist $z[\![\alpha]\!]_A z'$. Beweis per Induktion über t:
$t = 1$: $I_A(\alpha, z) = (\varepsilon, z') \rightarrow A \not\models_z B \rightarrow z[\![\alpha]\!]_A z$ und $z = z'$.
$t > 1$: Es gelte $I_A^t(\alpha, z) = (\varepsilon, z')$.
(Wir nehmen o.B.d.A. an, dass $I_A^{t'}(\alpha, z) \neq (\varepsilon, z')$ für alle $t' < t$ gilt.)
Da $t > 1$, gilt $A \models_z B$.
$\exists t'' \in \mathbb{N} : I_A^{t''}(\beta, z) = (\varepsilon, z'')$, da sonst $I_A^t(\alpha, z)$ nicht definiert wäre. Ferner ist $1 \leq t'' \leq t - 1$.
Es ist $(\varepsilon, z') = I_A^t(\alpha, z) = I_A^{t-1}(\beta;\ \alpha, z) = I_A^{t-1-t''}(\alpha, z'')$.
Nach $I.V.^{\text{klein}}$ gilt $z''[\![\alpha]\!]_A z'$ und nach $I.V.^{\text{gross}}$ gilt $z[\![\beta]\!]_A z''$.
Also: $z[\![\beta;\ \alpha]\!]_A z'$.
Wegen $A \models_z B$ ist also auch $z[\![\alpha]\!]_A z'$ gültig.

Aufgabe 4.2.

$z(M)>0:$	$z(X)>0:$	$z'(Z)=\lfloor\frac{z(X)}{z(M)}\rfloor$	
		$z'(Y)=z(X)-\lfloor\frac{z(X)}{z(M)}\rfloor z(M)$	
	$z(X)=0:$	$z'(Z)=0=\lfloor\frac{z(X)}{z(M)}\rfloor$	
		$z'(Y)=z(X)$	
		$\quad=z(X)-\underbrace{\lfloor\frac{z(X)}{z(M)}\rfloor}_{=0}z(M)$	
	$z(X)<0:$	$z'(Z)=0,$	$\lfloor\frac{z(X)}{z(M)}\rfloor\leq -1$
		$z'(Y)=z(X);$	$z(X)-\underbrace{\lfloor\frac{z(X)}{z(M)}\rfloor}_{\leq -1}\underbrace{z(M)}_{>0}>z(X)$
$z(M)=0:$	$z(X)>0:$	$\uparrow$	
	$z(X)=0:$	$\uparrow$	
	$z(X)<0:$	$z'(Z)=0;$	$\lfloor\frac{z(X)}{z(M)}\rfloor$nicht def.
		$z'(Y)=z(X);$	$z(X)-\lfloor\frac{z(X)}{z(M)}\rfloor z(M)$nicht def.
$z(M)<0:$	$z(X)>0:$	$\uparrow$	
	$z(X)\geq z(M):$	$\uparrow$	
	$z(X)<z(M):$	$z'(Z)=0;$	$\lfloor\frac{z(X)}{z(M)}\rfloor\geq 1$
		$z'(Y)=z(X);$	$z(X)-\underbrace{\lfloor\frac{z(X)}{z(M)}\rfloor}_{\geq 1}\underbrace{z(M)}_{<0}>z(X)$

D.h.: $[\![\alpha]\!]_A(z)\uparrow$ gdw. $z(X)\geq z(M)$ und $z(M)\leq 0$.
bzw. $[\![\alpha]\!]_A(z)\downarrow$ gdw. $z(X)<z(M)$ oder $z(M)>0$.

Sei z Zustand mit $[\![\alpha]\!]_A(z)\downarrow$ und $z'=[\![\alpha]\!]_A(z)$.
Also
$z'(X)=z(X)$, $z'(M)=z(M)$.

$$z'(Z)=\begin{cases}\lfloor\frac{z(X)}{z(M)}\rfloor & \text{, falls } z(M)>0 \text{ und } z(X)\geq 0\\ 0 & \text{, sonst}\end{cases}$$

$$z'(Y)=\begin{cases}z(X)-\lfloor\frac{z(X)}{z(M)}\rfloor z(M) & \text{, falls } z(M)>0 \text{ und } z(X)\geq 0\\ z(X) & \text{, sonst.}\end{cases}$$

Alternative Lösung
Kriterium: $\exists n\in\mathbb{N}(z(M)>\frac{z(X)}{1+n}) \iff \exists z'(z[\![\alpha]\!]z')$.
Sei β der Teil
while $Y\geq M$ **do** $Y:=Y-M;\ Z:=Z+1;$
end;
von α.

a) $\leftarrow$: α terminiert gdw. β terminiert. Dann existiert $n, z_0, ...z_n$ mit $z_0 = z(Y/z(X), Z/0)$, $z_n = z'$, $\mathbb{Z} \not\models_{z_n} M \leq Y$ und für alle i mit $0 \leq i < n$ gilt $z_i[\![Y := Y - M;\ Z := Z + 1;\ ]\!]z_{i+1}$ und $\mathbb{Z} \models_{z_i} M \leq Y$.

Zuerst zeigen wir, dass für alle i mit $0 \leq i \leq n$ die Gleichung $z_i = z(Y/z(X) - iz(M), Z/i)$ gilt. Behauptung ist für z_0 klar (IA).

I.V: $i < n \wedge z_i = z(Y/z(X) - iz(M), Z/i)$.

Wegen $z_i[\![Y := Y - M;\ Z := Z + 1;\ ]\!]z_{i+1}$ erhalten wir
$z_{i+1} = z(Y/z(x) - (i+1)z(M), Z/i+1)$.

Somit gilt $z_n = z(Y/z(X) - nz(M), Z/n)$ und wegen $\mathbb{Z} \not\models_{z_n} M \leq Y$ folgt

$$\begin{array}{rcl} \mathbb{Z} \models_{z_n} M > Y & \iff & \mathbb{Z} \models z_n(M) > z_n(Y) \\ & \iff & \mathbb{Z} \models z(M) > (z(x) - nz(M)) \\ & \iff & z(M) > \frac{z(X)}{1+n} \end{array}$$

b) $\rightarrow$: Zuerst beweisen wir:

$$\forall k \in N\ k \leq \frac{z(X)}{z(M)} - 1 \rightarrow I_Z^{2+3k}(\alpha, z) = (\beta, z(Y/z(X) - kz(M), Z/k))$$

Für $i = 0$ ist die Behauptung erfüllt.

Wenn die Behauptung für $i \leq \frac{z(X)}{z(M)} - 2$ richtig ist, dann

$$\begin{array}{rcl} I_{\mathbb{Z}}^{2+3(i+1)}(\alpha, z) & = & I_{\mathbb{Z}}^{3}(\beta, z(Y/z(X) - iz(M), Z/i)) \\ & & \text{weil } i \leq \frac{z(X)}{z(M)} - 2 \\ & = & I_{\mathbb{Z}}^{2}(Y := Y - M;\ Z := Z + 1;\ \beta, z(Y/z(X) - iz(M), Z/i)) \\ & = & (\beta, z(Y/z(X) - (i+1)z(M), Z/(i+1)) \end{array}$$

Sei $n \in \mathbb{N}$ minimal mit $(z(M) > \frac{z(X)}{1+n})$. Für alle $k < n$ gilt $z(M) \leq \frac{z(X)}{1+k}$, d.h. $\forall k < n\ k \leq \frac{z(X)}{z(M)} - 1$.

$$\begin{array}{rcl} I_{\mathbb{Z}}^{2+3(n-1)+3+1}(\beta, z) & = & I_{\mathbb{Z}}^{3+1}(\beta, z(Y/z(X) - (n-1)z(M), Z/(n-1))) \\ & & \text{weil } n - 1 < n \\ & = & I_{\mathbb{Z}}(\beta, z(Y/z(X) - nz(M), Z/n)) \\ & & \text{weil } z(M) > \frac{z(X)}{1+n} \\ & = & (\epsilon, z(Y/z(X) - nz(M), Z/n)) \end{array}$$

Wegen der Äquivalenz der Semantikbegriffe gilt $z[\![\alpha]\!]z(Y/z(x) - nz(M), Z/n)$.

Aufgabe 4.3. *Lösung zu Aufgabenteil (1)* Siehe Beispiel 4.30 aus Vorlesung.

Lösung zu Aufgabenteil (2)

[1] Zunächst wird das Programm mit den entsprechenden Kommentaren $\varphi_i, i = 0, \ldots, 8$ versehen.

$\{\text{true}\} \equiv \varphi_0$
$Z := X;$
$\{Z = X\} \equiv \varphi_1$
$Z' := 0;$
$\{Z = X \wedge Z' = 0\} \equiv \varphi_2$
$\{(Z' < Y \vee Z' = Y) \wedge Z = X + Z'\} \equiv \varphi_3 (\equiv \xi)$
while $\neg Y = Z'$ do
$\{((Z' < Y \vee Z' = Y) \wedge Z = X + Z') \wedge \neg Y = Z'\} \equiv \varphi_4 (\equiv \xi \wedge B)$
$Z := succ(Z);$
$\{((Z' < Y \vee Z' = Y) \wedge Z = \text{succ}(X + Z')) \wedge \neg Y = Z'\} \equiv \varphi_5$
$Z' := succ(Z');\ \{(Z' < Y \vee Z' = Y) \wedge Z = X + Z'\} \equiv \varphi_6 (\equiv \xi)$
end;
$\{((Z' < Y \vee Z' = Y) \wedge Z = X + Z') \wedge \neg\neg Y = Z'\} \equiv \varphi_7 (\equiv \xi \wedge \neg B)$
$\{Z = X + Y\} \equiv \varphi_8$

[2] Danach werden die Beweisaufgaben aus dem kommentierten Programm extrahiert und einzeln aufgeführt.
[2.1] $\text{true} \rightarrow [\varphi_1]\{Z/X\}$
[2.2] $\varphi_1 \rightarrow [\varphi_2]\{Z'/0\}$
[2.3] $\varphi_2 \rightarrow \varphi_3$
[2.4] $\varphi_4 \rightarrow [\varphi_5]\{Z/\text{succ}(Z)\}$
[2.5] $\varphi_5 \rightarrow [\varphi_6]\{Z'/\text{succ}(Z')\}$
[2.6] $\varphi_7 \rightarrow \varphi_8$

[3] Sei $V \supseteq \{X, Y, Z, Z'\}$ eine geeignet gewählte Variablenmenge. Sei weiter z ein Zustand über Nat und V.
[3.1] $Nat \models_z \text{true} \rightarrow [\varphi_1]\{X/Z\}$ gdw
$Nat \not\models_z \text{true}$ oder $Nat \models_z Z = Z$ gdw
$\text{val}_{Nat,z}(Z) = \text{val}_{Nat,z}(Z)$ $\surd$
[3.2] $Nat \models_z \varphi_1 \rightarrow [\varphi_2]\{Z'/0\}$ $\surd$
[3.3] $Nat \models_z \varphi_2 \rightarrow \varphi_3$ $\surd$
[3.4] $Nat \models_z \varphi_4 \rightarrow [\varphi_5]\{Z/\text{succ}(Z)\}$ gdw
$Nat \models_z (((Z' < Y \vee Z' = Y) \wedge Z = X + Z') \wedge \neg Y = Z') \rightarrow$
$(((Z' < Y \vee Z' = Y) \wedge \text{succ}(Z) = \text{succ}(X + Z')) \wedge \neg Y = Z')$ gdw
$Nat \not\models_z \varphi_4$ oder
$Nat \models_z (((Z' < Y \vee Z' = Y) \wedge \text{succ}(Z) = \text{succ}(X + Z')) \wedge \neg Y = Z')$
Zeigen Sie nun, dass unter der Voraussetzung $Nat \models_z \varphi_4$ auch
$Nat \models_z (((Z' < Y \vee Z' = Y) \wedge \text{succ}(Z) = \text{succ}(X + Z')) \wedge \neg Y = Z')$ gilt. $\surd$
[3.5] $Nat \models_z \varphi_5 \rightarrow [\varphi_6]\{Z'/\text{succ}(Z')\}$ $\surd$
[3.6] $Nat \models_z \varphi_7 \rightarrow \varphi_8$ $\surd$

Aufgabe 4.4. Lösung
Lösung zu Aufgabenteil (1)

[3.4.1] $Nat \not\models \{true\} X := \text{succ}(X);\ \{X = \text{succ}(X)\}$

Lösung zu Aufgabenteil (2)

[3.4.2] Betrachte folgendes Beispiel in Nat:

$$Nat \models \{X = 0 \wedge Y = 1\} X := Y;\ Y := X; \{X = 1 \wedge Y = 1\}$$

$$Nat \models \{X = 0 \wedge Y = 1\} Y := X;\ X := Y; \{X = 0 \wedge Y = 0\}$$

Also ist Regel ohne die Bedingung an die Variablen *nicht* korrekt! Die Regel für Zuweisungsfolgen (Folien, 5.9) liefert hier

$$\frac{\varphi \rightarrow [\{\psi\}[Y/s]][X/t]}{[\varphi] X := t;\ Y := s;\ [\psi]}$$

In jeder Algebra $\mathcal{A}$ über der entsprechenden Signatur (S, Σ) ist die Formel $[[\psi]\{Y/s\}]\{X/t\}$ logisch äquivalent zu $[\psi]\{X/t, Y/s\}$, wenn die Variablenbedingung erfüllt ist. (Warum?)
Man kann also $\mathcal{HC}$ erweitern um

$$\frac{\varphi \rightarrow [\psi]\{X/t, Y/s\}}{\{\varphi\} X := t;\ Y := s;\ \{\psi\}}$$

$$\frac{\varphi \rightarrow [\psi]\{X/t, Y/s\}}{\{\varphi\} Y := s;\ X := t;\ \{\psi\}}$$

Diese Erweiterung ist nach obiger Argumentation korrekt.
Sei nun $\mathcal{A} \models \{\varphi\} X := t;\ Y := s;\ \{\psi\}$.
Dann gilt in $\mathcal{A}$:

$$\mathcal{A} \models \varphi \rightarrow [\psi](X/t, Y/s)$$

Regel (2) liefert

$$\mathcal{A} \models \{\varphi\} Y := s;\ X := t;\ \{\psi\}$$

Also kann $\mathcal{HC}$ um die Regel

$$\frac{\{\varphi\} X := t;\ Y := s;\ \{\psi\}}{\{\varphi\} Y := s;\ X := t;\ \{\psi\}}$$

erweitert werden (und diese Erweiterung ist korrekt).
q.e.d.

Aufgabe 4.5. Erweiterung Def. 4.25:

$$\frac{\alpha}{\text{repeat } \alpha \text{ until } B;}\ B \text{ Boolesche-Formel über } (S, \Sigma), V$$

Erweiterung Def. 4.27:

$$z[\![\text{repeat } \alpha \text{ until } B;\ ]\!]_A z' \iff \begin{array}{l} \exists n \text{ und } z_0, z_1 ..., z_{n+1} \\ z_0 = z \\ \forall i(0 \leq i \leq n) z_i [\![\alpha]\!] z_{i+1} \\ \forall i(1 \leq i \leq n) A \not\models_{z_i} B \\ z_{n+1} = z' \text{ und } A \models_{z_{n+1}} B \end{array}$$

Erweiterung Def. 5.4:

$$\frac{\{\varphi\}\alpha\{\xi\}, \{\xi \wedge \neg B\}\alpha\{\xi\}, ((\xi \wedge B) \rightarrow \psi)}{\{\varphi\}\text{repeat } \alpha \text{ until } B;\ \{\psi\}}$$

Erweiterung Satz 5.8:
Sei z und z' mit $A \models_z \varphi, z[\![\text{repeat } \alpha \text{ until } B;\ ]\!] z'$. Sei weiter $\vdash_{HC(A)} \{\varphi\}\text{repeat } \alpha \text{ until } B\{\psi\}$.
Wir werden zeigen, dass $A \models_{z'} \psi$ gilt.
Wegen der Eindeutigkeit des Kalküls $HC(A)$ existiert ξ mit folgenden Eigenschaften:

- $A \models \{\varphi\}\alpha\{\xi\}$
- $A \models \{\xi \wedge \neg B\}\alpha\{\xi\}$
- $A \models ((\xi \wedge B) \rightarrow \psi)$

Nach Voraussetzung existieren n und $(z_i)_{0 \leq i \leq n+1}$ mit folgenden Eigenschaften:

- $z_0 = z$
- $\forall i(0 \leq i \leq n) z_i [\![\alpha]\!] z_{i+1}$
- $\forall i(1 \leq i \leq n) A \not\models_{z_i} B$
- $z_{n+1} = z'$ und $A \models_{z_{n+1}} B$

Zunächst zeigen wir $\forall i(1 \leq i \leq n+1) A \models_{z_i} \xi$.

- $i = 0$: Aus $A \models_z \varphi, z = z_0, z_0 [\![\alpha]\!] z_1$ und $A \models \{\varphi\}\alpha\{\xi\}$ folgt $A \models_{z_1} \xi$.
- $1 \leq i < n+1$: Da $A \models_{z_i} \xi$ und $A \not\models_{z_i} B$, gilt $A \models_{z_i} (\xi \wedge \neg B)$. Wegen $z_i [\![\alpha]\!] z_{i+1}$ und $A \models \{\xi \wedge \neg B\}\alpha\{\xi\}$ erhalten wir $A \models_{z_{i+1}} \xi$.

Wegen $A \models_{z_{n+1}} \xi$ und $A \models_{z_{n+1}} B$ folgt $A \models_{z_{n+1}} \xi \wedge B$. Wegen $A \models ((\xi \wedge B) \rightarrow \psi)$ erhalten wir $A \models_{z_{n+1}} \psi$.

Zusatz: Programme mit Kommentaren
Erweiterung Def. 5.6
Kommentar: { PL-Formel } oder { PL-Formel, PL-Formel }
Syntax von Programmen:

- $\{\varphi\}$ repeat $\{\varphi, (\xi \wedge \neg B)\}\alpha\{\xi\}$ until $B;\ \{\xi \wedge B\}\{\psi\}$

Beweisverpflichtungen: Gezeigt werden müssen:

- $\{\varphi_1\}\alpha\{\psi\}$ und $\{\varphi_2\}\alpha\{\psi\}$,
  wenn $\{\varphi_1, \varphi_2\}\alpha\{\psi\}$ im kommentierten Programmtext vorkommt.

Als Beweisverpflichtungen ergeben sich also im obigen Fall:

- $\{\varphi\}\alpha\{\xi\}$

- $\{\xi \wedge \neg B\}\alpha\{\xi\}$
- $\{\xi \wedge B\}\{\psi\}$

Die sind offensichtlich die Prämissen für die Kalkül-Regel '$\{\varphi\}$ repeat α until B; $\{\psi\}$'.