# Grundlagen der Programmierung

SS 05
Prof. Dr. K. Madlener
Lösungshinweise zu Übungsblatt 5

**Aufgabe 5.1.** a) Beh.: $A \models \{\varphi\}\alpha\{\psi\}^{(1)}$ und $A \models_z \varphi^{(2)} \rightarrow z \in \mathrm{wlp}_A(\alpha, \psi)$.
Bew.: Wegen (1) gilt f.a. Zustände $z, z' : A \models_z \varphi$ und $z[\alpha]_A z' \rightarrow A \models_{z'} \psi$.
Wegen (2) gilt also (bei gegebenem $z$) f.a. Zustände $z'$:
$z[\alpha]_A z' \rightarrow A \models_{z'} \psi$,
also nach Def. $z \in \mathrm{wlp}_A(\alpha, \psi)$.

Alt.:
- Falls ein $z'$ existiert mit $z[\![\alpha]\!]_A z'$, erhalten wir $A \models_{z'} \psi$ (wegen $A \models \{\varphi\}\alpha\{\psi\}$). Es gilt $z \in \mathrm{wlp}(\alpha, \psi)$.
- Falls $[\![\alpha]\!]_A(z)$ nicht definiert ist, ist die Aussage $\forall z'(z[\![\alpha]\!]_A z' \Rightarrow A \models_{z'} \varphi)$ wahr und es gilt $z \in \mathrm{wlp}(\alpha, \psi)$.

b) Beh.: $A \models \{\varphi\}\alpha\{\psi\}^{(1)}$ und $z' \in spc_A(\varphi, \alpha)^{(2)} \rightarrow A \models_{z'} \psi$.
Bew.: Wegen (2) gilt: es gibt einen Zustand $z$, so dass $A \models_z \varphi$ und $z[\![\alpha]\!]_A z'$.
Wegen (1) gilt nach Definition $A \models_{z'} \psi$.

c) Beh.: Sei $\mathrm{wlp}_A(\alpha, \psi)$ durch $W_{\alpha,\psi}$ definierbar.

(i) $A \models \{W_{\alpha,\psi}\}\alpha\{\psi\}$

(ii) $\forall \xi : A \models \{\xi\}\alpha\{\psi\} \longrightarrow A \models (\xi \rightarrow W_{\alpha,\psi})$

Bew.: (i) Sei $z$ und $z'$ Zustände mit $A \models_z W_{\alpha,\psi}$ und $z[\![\alpha]\!]_A z'$.
Dann ist nach Definition $z \in wlp_A(\alpha, \psi)$. Damit gilt $A \models_{z'} \psi$,
also auch $A \models \{W_{\alpha,\psi}\}\alpha\{\psi\}$.

(ii) Es gelte $A \models \{\xi\}\alpha\{\psi\}^{(1)}$.
Für alle Zustände $z$ mit $A \not\models_z \xi$ gilt $A \models_z \xi \rightarrow W_{\alpha,\psi}$.

Sei nun $z$ ein Zustand mit $A \models_z \xi$.
- i Falls ein $z'$ mit $z[\![\alpha]\!]z'$ existiert, wissen wir mit (1), dass $A \models_{z'} \psi$ und somit $z \in \mathrm{wlp}(\alpha, \psi)$ gilt.
  Also gilt $A \models_z W_{\alpha,\psi}$ und damit $A \models_z \xi \rightarrow W_{\alpha,\psi}$.
- ii Falls $[\![\alpha]\!](z)$ nicht definiert ist, gilt $\forall z'(z[\![\alpha]\!]z' \Rightarrow A \models_{z'} \psi)$.
  Somit ist $z \in \mathrm{wlp}(\alpha, \psi)$, und damit $A \models_z \xi \rightarrow W_{\alpha,\psi}$.

Also $A \models \xi \rightarrow W_{\alpha,\psi}$.

d) Beh.: Sei $spc_A(\varphi, \alpha)$ durch $S_{\varphi,\alpha}$ definierbar.

(i) $A \models \{\varphi\}\alpha\{S_{\varphi,\alpha}\}$.

(ii) $\forall \xi : A \models \{\varphi\}\alpha\{\xi\} \longrightarrow A \models (S_{\varphi,\alpha} \rightarrow \xi)$.

Bew.: (i) Es seien $z$ und $z'$ Zustände mit $A \models_z \varphi$ und $z[\alpha]_A z'$.
Dann ist nach Definition $z' \in spc(\varphi, \alpha)$. Damit gilt $A \models_{z'} S_{\varphi,\alpha}$,
also auch $A \models \{\varphi\}\alpha\{S_{\varphi,\alpha}\}$.

(ii) Es gelte $A \models \{\varphi\}\alpha\{\xi\}$(1).
Sei $z'$ ein Zustand mit $A \models_{z'} S_{\varphi,\alpha}$, d.h. $z' \in spc_A(\varphi, \alpha)$.
Dann gibt es einen Zustand $z$ mit $A \models_z \varphi$ und $z[\alpha]_A z'$.
Wegen (1) gilt nun $A \models_{z'} \xi$.
Damit gilt $A \models_{z'} (S_{\varphi,\alpha} \to \xi)$ und somit $A \models (S_{\varphi,\alpha} \to \xi)$.

e) Beh.: $spc_A(\varphi, X := t_i)$ ist durch $S_{\varphi,X:=t_i} = \exists Y([\varphi]\{X/Y\} \wedge (X = t\{X/Y\})))$ definierbar ($Y \notin VAR(\varphi) \cup VAR(t) \cup \{X\}$). (Sei $s$ der Typ von $X$ und $t$.)

Bew.: Wir brauchen die folgende Sätze:
Wenn $Y \notin VAR(X, t, \varphi)$ mit $Typ(Y) = Typ(X)$ ist, gilt:

$$val_{A,z'(Y/\alpha)}(t\{X/Y\}) = val_{A,z'(X/\alpha)}(t)$$

und für jeden Wert $\alpha \in s_A$ mit $Typ(\alpha) = Typ(X)$:

$$A \models_{z'(Y/\alpha)} [\varphi]\{X/Y\} \text{ gdw } A \models_{z'(X/\alpha)} \varphi$$

(siehe Vorlesung, Lemma 4.15 und 4.22).
Zeige nun:

$$A \models_{z'} \exists Y([\varphi]\{X/Y\} \wedge X = t\{X/Y\}) \Leftrightarrow z' \in \mathrm{spc}_A(\varphi, \alpha)$$

"⇒":

$$\begin{aligned}
& A \models_{z'} \exists Y([\varphi]\{X/Y\} \wedge (X = t\{X/Y\})) \\
\Rightarrow\ & \exists \alpha \in S_A[A \models_{z'(Y/\alpha)} [\varphi]\{X/Y\} \\
& \text{und } A \models_{z'(Y/\alpha)} (X = t\{X/Y\})] \\
\Rightarrow\ & \exists \alpha \in S_A[A \models_{z'(Y/\alpha)} [\varphi]\{X/Y\} \\
& \text{und } z'(Y/\alpha)(X) = z'(X) = val_{A,z'(Y/\alpha)}(t\{X/Y\})
\end{aligned}$$

Sei $z = z'(X/\alpha)$. Es gilt:
$z' = z(X/val_{A,z}(t))$ (weil $z'(X) = val_{A,z'(Y/\alpha)}(t\{X/Y\}) = val_{A,z'(X/\alpha)}(t) = val_{A,z}(t)$)
sowie $A \models_{z'(Y/\alpha)} [\varphi]\{X/Y\}$ gdw. $A \models_{z'(X/\alpha)} \varphi$ gdw. $A \models_z \varphi$
d.h. es gibt Zustand $z$ mit $A \models_z \varphi$ und $z' = z(X/val_{A,z}(t))$.

"⇐":

$$\begin{aligned}
& \exists z[A \models_z \varphi \text{ und } z' = z(X/val_{A,z}(t))](\implies z = z'(X/z(X))) \\
\Rightarrow\ & A \models_{z'(X/z(X))} \varphi \text{ und } z'(X) = val_{A,z'(X/z(X))}(t) \\
& \text{Sei } Y \text{ neue Variable mit } Y \notin VAR(X, t, \varphi) \\
\Rightarrow\ & A \models_{z'(Y/z(X))} [\varphi]\{X/Y\} \text{ und} \\
& z'(Y/z(X))(X) = z'(X) = \mathrm{val}_{A,z}(t) = \mathrm{val}_{A,z'(Y/z(X))}(t\{X/Y\}) \\
\Rightarrow\ & A \models_{z'(Y/z(X))} [\varphi]\{X/Y\} \text{ und } A \models_{z'(Y/z(X))} X = t\{X/Y\} \\
\Rightarrow\ & A \models_{z'} \exists Y([\varphi]\{X/Y\} \wedge X = t\{X/Y\})
\end{aligned}$$

**Aufgabe 5.2.** a) Wir zeigen, dass die stärkste Nachbedingung

$$spc_{Nat}(X = Y,\, Y := X + Y\,,X := X + Y)$$

durch die Formel $X + X = Y + Y + Y$ definierbar ist.
Dazu reicht es nach 5.2.c) Formeln $\xi$ und $\zeta$ anzugeben, so dass

$$\xi \text{ die } spc_{Nat}(X = Y, X := X + Y)$$

und

$$\zeta \text{ die } spc_{Nat}(\xi,\, Y := X + Y) \text{ definieren.}$$

Aus 5.1.e) ergibt sich zunächst
$S_{X=Y,Y:=X+Y} = \underbrace{\exists U_1(U_1 = X \wedge Y = U_1 + X)}_{=:\xi'}$ $(U_1 \notin \{X, Y\})$
Es gilt: $Nat \models \xi' \leftrightarrow \underbrace{\exists U_1(U_1 = X \wedge Y = U_1 + U_1)}_{=:\xi}$
Daher definiert $\xi$ die $spc_{Nat}(X = Y,\, X := X + Y)$.
Nochmaliges Anwendungen von 5.1.e) ergibt:
$S_{\xi,X:=X+Y} = \underbrace{\exists U_2(\exists U_1(U_1 = U_2 \wedge Y = U_1 + U_1) \wedge (X = Y + U_2))}_{=:\zeta'}$ $(U_1, U_2 \notin \{X, Y\})$.
Es gilt:

$$Nat \models \zeta' \leftrightarrow \underbrace{\exists U(Y = U + U \wedge X = Y + U)}_{\zeta''}$$

$$Nat \models \zeta'' \leftrightarrow \underbrace{\exists U(Y = U + U \wedge X = U + U + U)}_{\zeta'''}$$

$$Nat \models \zeta''' \leftrightarrow \underbrace{Y + Y + Y = X + X}_{\zeta}$$

Daher definiert $\zeta$ die $spc_{Nat}(\xi, X := X+Y)$ und damit wegen 5.2.c) die $spc_{Nat}(X = Y,\, Y := X + Y,\, X := X + Y)$. Mit der Abkürzung $2 = succ(succ(0))$ und $3 = succ(succ(succ(0)))$ ergibt sich $Nat \models Y + Y + Y = X + X \leftrightarrow 3 * Y = 2 * X$.
Damit gilt insgesamt
$Nat \models \{X = Y\}\, Y := X + Y,\, X := X + Y\, \{3 * Y = 2 * X\}$.

b) Für welche $\alpha$, $\varphi$ gilt in einer Algebra $A$

(i) $A \models \{\varphi\}\alpha\{FALSE\}$

(ii) $A \models \{\varphi\}\alpha\{TRUE\}$ ?

Zu (i): Sei $A$ eine geeignete Algebra.

$$A \models \{\varphi\}\alpha\{FALSE\}$$

gdw. F.a. Zustände $z, z'$: $A \models_z \varphi$ und $z[\![\alpha]\!]_A z' \to A \models_{z'} FALSE$
gdw. F.a. Zustände $z, z'$: $\neg(A \models_z \varphi$ und $z[\![\alpha]\!]_A z')$ oder $FALSE$
gdw. F.a. Zustände $z, z'$: $A \not\models \varphi$ oder ($z[\![\alpha]\!]_A z'$ gilt nicht)

gdw. F.a. Zustände $z, z'$: $A \models_z \varphi \to (z[\![\alpha]\!]_A z'$ gilt nicht).
Ist also $\varphi = FALSE$, so gilt $A \models \{\varphi\}\alpha\{FALSE\}$ für beliebige $\alpha$.
Desweiteren gilt $A \models \{\varphi\}\alpha\{FALSE\}$ immer dann, wenn für einen Anfangszustand $z$, mit $A \models_z \varphi$ das Prgoramm $\alpha$ nicht terminiert (d.h. kein $z'$ existiert mit
$z[\![\alpha]\!]_A z'$).

Zu (ii): $A \models \{\varphi\}\alpha\{TRUE\}$ gdw. $\forall z, z'(z[\![\alpha]\!]_A z'$ und $A \models_z \varphi \to A \models_{z'} TRUE)$ gdw. $TRUE$. Also gilt $\{\varphi\}\alpha\{TRUE\}$ für alle $\alpha$ und $\varphi$.

c) (i) Es gilt:

$$\begin{aligned}
\mathrm{wlp}_A(\alpha\beta, \psi) &= \{z \mid \text{ f.a. } z' : z[\![\alpha\beta]\!]_A z' \to A \models_{z'} \psi\} \\
&= \{z \mid \text{ f.a. } z' : [\![\alpha\beta]\!]_A(z) = z' \to A \models_{z'} \psi\} \\
&= \{z \mid \text{ f.a. } z' : [\![\alpha\beta]\!]_A(z) \uparrow \text{ oder } A \models_{[\![\alpha\beta]\!]_A(z)} \psi\} \\
&= \{z \mid [\![\alpha]\!]_A(z) \uparrow \text{ oder } [\![\beta]\!]_A([\![\alpha]\!]_A(z)) \uparrow \text{ oder } A \models_{[\![\beta]\!]_A([\![\alpha]\!]_A(z))} \psi\} \\
&= \{z \mid [\![\alpha]\!]_A(z) \uparrow \text{ oder } [\![\alpha]\!]_A(z) \in \mathrm{wlp}_A(\beta, \psi)\} \\
&= \{z \mid [\![\alpha]\!]_A(z) \uparrow \text{ oder } A \models_{[\![\alpha]\!]_A(z)} W_{\beta,\psi}\} \\
&= \{z \mid \text{ f.a. } z' : [\![\alpha]\!]_A(z) = z' \to A \models_{z'} W_{\beta,\psi}\} \\
&= \{z \mid \text{ f.a. } z' : z[\![\alpha]\!]_A z' \to A \models_{z'} W_{\beta,\psi}\} \\
&= \mathrm{wlp}_A(\alpha, W_{\beta,\psi}).
\end{aligned}$$

(ii) Es gilt

$$\begin{aligned}
\mathrm{spc}_A(\varphi, \alpha\beta) &= \{z' \mid \exists z(z[\![\alpha\beta]\!]_A z' \wedge A \models_z \varphi)\} \\
&= \{z' \mid \exists z(\exists z''(z[\![\alpha]\!]_A z'' \wedge z''[\![\beta]\!]_A z') \wedge A \models_z \varphi)\} \\
&= \{z' \mid \exists z''\exists z(z''[\![\beta]\!]_A z' \wedge z[\![\alpha]\!]_A z'' \wedge A \models_z \varphi)\} \\
&= \{z' \mid \exists z''(z''[\![\beta]\!]_A z' \wedge \exists z(z[\![\alpha]\!]_A z'' \wedge A \models_z \varphi))\} \\
&= \{z' \mid \exists z''(z''[\![\beta]\!]_A z' \wedge z'' \in \mathrm{spc}_A(\varphi, \alpha))\} \\
&= \{z' \mid \exists z''(z''[\![\beta]\!]_A z' \wedge A \models_{z''} S_{\varphi,\alpha})\} \\
&= \mathrm{spc}_A(S_{\varphi,\alpha}, \beta).
\end{aligned}$$

**Aufgabe 5.3.** ad 1,2: Da $\alpha$ für jeden Startzustand $z$ terminiert, gilt offensichtlich.

$$\mathrm{wlp}_{Nat}(\alpha, \psi) \cap \mathrm{wlp}_{Nat}(\alpha, \neg\psi) = \emptyset \tag{1}$$

In $Nat$ gelten die folgenden partiellen Korrektheitsaussagen:
(i) $Nat \models \{\exists z \quad X = z + z\}\alpha\{\psi\}$
(ii) $Nat \models \{\neg\exists z\, X = z + z\}\alpha\{\neg\psi\}$
Somit gilt $\mathrm{wlp}_{Nat}(\alpha, \psi) = \{z : Nat \models_z \varphi\}$ mit $\varphi = \exists z \quad X = z + z$, denn

$\supseteq$ : Sei $Nat \models_z \varphi$, wegen (i) folgt $z \in \mathrm{wlp}_{Nat}(\alpha, \psi)$. (siehe auch Lemma 5.14, bzw. A6.1).

$\subseteq$ : Sei $z \in \text{wlp}_{Nat}(\alpha, \psi)$. Dann gilt entweder $Nat \models_z \varphi$ oder $Nat \models_z \neg\varphi$. Sei $Nat \models_z \neg\varphi$, dann gilt analog zum Fall $\supseteq$ : $z \in \text{wlp}_{Nat}(\alpha, \neg\psi)$. Aus Gleichung (1) folgt $z \notin \text{wlp}_{Nat}(\alpha, \psi)$. *Widerspruch!* Also gilt $Nat \models_z \varphi$ und insgesamt

$$\text{wlp}_{Nat}(\alpha, \psi) = \{z : Nat \models_z W_{\alpha,\psi}\}$$

mit

$$W_{\alpha,\psi} = \exists z \quad X = z + z$$

ad 3: Es ist

$$\text{wlp}_N(\alpha, \psi) = \{z : z(X) \text{ ist gerade Zahl}\}$$

mit den Aufgabenteilen 1 und 2. Diese Menge lässt sich umschreiben zu

$$\text{wlp}_N(\alpha, \psi) = \{z(X/n) : n \text{ ist gerade Zahl}\}$$

Ann: Es gibt $W_{\alpha,\psi}$ mit $\text{wlp}_N(\alpha, \psi) = \{z : A \models_z W_{\alpha,\psi}\}$. Dann gilt $\{z : A \models_z W_{\alpha,\psi}\} = \{z(X/n) : n \text{ ist gerade Zahl}\}$. Also definiert $W_{\alpha,\psi}$ in $N$ die Menge der geraden Zahlen. Diese Menge ist weder endlich noch co-endlich, und damit in $N$ nicht durch eine Formel definierbar (siehe Beispiel 5.15, e). *Widerspruch!* Also ist $N$ nicht ausdrucksstark.

**Aufgabe 5.4.** Beh.: $f_\pi(x, y, z) = \begin{cases} x & \text{falls } z = 0 \\ y + 1 & \text{falls } z > 0 \end{cases}$ f.a. $x, y, z \in \mathbb{N}$.

Bew.: $f_\pi(x, y, 0) = f_{\text{PROJ(1)}}(x, y, 0) = x$ für alle $x, y \in \mathbb{N}$.

$$\begin{aligned} f_\pi(x, y, z + 1) &= f_{\text{KOMP(SUCC,PROJ(2))}}(x, y, f_\pi(x, y, z), z) \\ &= f_{\text{SUCC}}(f_{\text{PROJ(2)}}(x, y, f_\pi(x, y, z), z)) \\ &= y + 1 \end{aligned}$$

für alle $x, y, z \in \mathbb{N}$.