Grundlagen der Programmierung

SS 05
Prof. Dr. K. Madlener
Lösungshinweise zu Übungsblatt 3

Aufgabe 3.1. ad 1: (Strukturelle Induktion im Termkalkül)

$\left[\frac{}{X}\right]$: X ist Variable vom Typ s. Nach Definition ist $val_{A,z}(X) = z(X)$. Der Zustand z über A und V ordnet der Variablen X einen Wert $z(X)$ in der Menge s_A zu (Definition).

$\left[\frac{}{c}\right]$: $c :\rightarrow s$ Konstante. Es ist $val_{A,z}(c) = c_A$ und es gilt $c_A \in s_A$ (Def.)

$\left[\frac{t_1, \ldots, t_n}{f(t_1, \ldots, t_n)}\right]$: Sei Behauptung für $t_1, \ldots, t_n$ erfüllt. Dann ist nach Definition:
$val_{A,z}(f(t_1, \ldots, t_n)) = f_A(val_{A,z}(t_1), \ldots, val_{A,z}(t_n))$.

Wegen $f_A : s_A^1 \times \cdots \times s_A^n \rightarrow s_A$ und Ind. Vor. gilt $f_A(val_{A,z}(t_1), \ldots, val_{A,z}(t_n)) \in s_A$.
q. e. d.

ad 2: (Strukturelle Induktion im Termkalkül).

$\left[\frac{}{X}\right]$:
$$\begin{aligned} \rightsquigarrow val_{A,z}(X) &= z(X) \\ &= z'(X) \\ &= val_{A,z'}(X) \end{aligned}$$

$\left[\frac{}{c}\right]$: $val_{A,z}(c) = c_A = val_{A,z'}(c)$

$\left[\frac{t_1, \ldots, t_n}{f(t_1, \ldots, t_n)}\right]$: Sei Behauptung für $t_1, \ldots, t_n$ erfüllt. Dann gilt
$$\begin{aligned} val_{A,z}(f(t_1, \ldots, t_n)) &= f_A(val_{A,z}(t_1), \ldots, val_{A,z}(t_n)) \\ &= f_A(val_{A,z'}(t_1), \ldots, val_{A,z'}(t_n)) \\ &= val_{A,z'}(f(t_1, \ldots, t_n)) \end{aligned}$$

q. e. d.

Aufgabe 3.2. Lösung

Lösung zu Aufgabenteil (1)
Sei $V \supseteq \{X, Y, Z, X', Y', Z' : nat\}$ eine Variablenmenge.

(1) $0 + 0$
(2) $\exists X' \exists Y' \neg X' = Y'$
(3) $\exists X' \, (X' = 0 \wedge \mathrm{succ}(Y) < X')$
(4) $\forall Y' (\exists X' \, X' = 0 \wedge Y' < 0)$

Lösung zu Aufgabenteil (2)

[1] Wir zeigen zunächst die Existenz einer solchen Substitution.
Sei $\sigma = \{X_i/s_i \mid i = 1, \ldots, m\}$ und $\rho = \{Y_i/t_i \mid i = 1, \ldots, n\}$.
Definiere

$$\begin{aligned}\gamma := \quad & \{X_i/(s_i\rho) \mid i = 1,\ldots,m \text{ und } X_i \neq s_i\rho\} \cup \\ & \{Y_i/t_i \mid i = 1,\ldots,n \text{ und } Y_i \notin \{X_1,\ldots,X_m\}\}\end{aligned}$$

[1.1] Mit strukturellen Induktion im Termkalkül zeigen wir nun

$$t\gamma = (t\sigma)\rho \text{ für alle Terme } t \text{ über } (S,\Sigma) \text{ und } V.$$

[1.1.1] $t = X$: Wir unterscheiden drei Fälle:

[1.1.1.1] $X = X_i$ für ein $i \in \{1,\ldots,m\}$.

Dann ist

$$\begin{aligned}X_i\gamma &= \begin{cases} s_i\rho & \text{falls } X_i \neq s_i\rho \\ X_i & \text{falls } X_i = s_i\rho \end{cases} \\ &= s_i\rho \\ &= (X_i\sigma)\rho\end{aligned}$$

[1.1.1.2] $X = Y_i$ für ein $i \in \{1,\ldots,n\}$.

Dann ist

$$\begin{aligned}Y_i\gamma &= \begin{cases} t_i & \text{falls } Y_i \notin \{X_1,\ldots,X_m\} \\ s_j\rho & \text{falls } Y_i = X_j \text{ für ein } j \in \{1,\ldots,m\} \end{cases} \\ &= \begin{cases} Y_i\rho & \text{falls } Y_i \notin \{X_1,\ldots,X_m\} \\ (X_j\sigma)\rho & \text{falls } Y_i = X_j \text{ für ein } j \in \{1,\ldots,m\} \end{cases} \\ &= (Y_i\sigma)\rho\end{aligned}$$

[1.1.1.3] $X \notin \{X_i \mid i = 1,\ldots,m\} \cup \{Y_i \mid i = 1,\ldots,n\}$.

Dann ist $X\gamma = X = (X\sigma) = (X\sigma)\rho$

[1.1.2] $t = c$: Behauptung folgt unmittelbar aus Definition 4.10.

[1.1.3] $t = f(t_1,\ldots,t_n)$: Sei Behauptung für $t_1,\ldots,t_n$ erfüllt.

Dann ist

$$\begin{aligned}f(t_1,\ldots,t_n)\gamma &= f(t_1\gamma,\ldots,t_n\gamma) && \text{(Definition 4.10)} \\ &= f((t_1\sigma)\rho,\ldots,(t_n\sigma)\rho) && \text{(Vor.)} \\ &= f(t_1\sigma,\ldots,t_n\sigma)\rho && \text{(Definition 4.10)} \\ &= (f(t_1,\ldots,t_n)\sigma)\rho && \text{(Definition 4.10)}\end{aligned}$$

Also existiert eine (!) Substitution mit der geforderten Eigenschaft.

q.e.d. [[1.1]]

[2] Es muss noch die Eindeutigkeit der Substitution gezeigt werden.

Sei also γ' weitere Substitution mit $t\gamma' = (t\sigma)\rho$ für alle t über (S,Σ) und V.

Dann gilt insbesondere $X\gamma' = (X\sigma)\rho = X\gamma$ für alle $X \in V$.

[2.1] Wir zeigen

$$\tau = \tau' \text{ gdw } X\tau = X\tau' \text{ für alle } X \in V$$

[2.1.1] Aus $\tau = \tau'$ folgt unmittelbar $X\tau = X\tau'$ für alle $X \in V$.

[2.1.2] Sei umgekehrt $X\tau = X\tau'$ für alle X erfüllt.

Sei $\tau = \{X_i/s_i \mid i = 1,\ldots,m\}$ und $X_j/s_j \in \tau$ für ein $j \in \{1,\ldots,m\}$.

Dann gilt

$$\begin{aligned}X_j\tau &= s_j && \text{(nach Definition 4.10)} \\ &= X_j\tau' && \text{(nach Vor.)}\end{aligned}$$

Da $X_j \neq s_j$ folgt $X_j\tau' \neq X_j$. Somit ist $X_j/s_j \in \tau'$ und insgesamt $\tau \subseteq \tau'$. Analog folgert man $\tau' \subseteq \tau$ und damit $\tau = \tau'$.

q.e.d.

Aufgabe 3.3. *Lösung zu (1)*
Wir zeigen die Gültigkeit der Formel $\varphi \equiv \forall X X + 0 = X$ in Nat (siehe 4.4) unter Verwendung der Definitionen 4.17 und 4.18. Sei dazu $V \supseteq \{X : Nat, Y : Nat\}$ eine geeignet gewählte Variablenmenge.

Es gilt: $Nat \models \varphi$ gdw für alle Zustände z über V und Nat gilt $Nat \models_z \varphi$.
Zeige: $Nat \models_z \forall X X + 0 = X$

$$
\begin{array}{ll}
 & Nat \models_z \forall X X + 0 = X \\
\Leftrightarrow & \text{für alle } n \in \mathrm{nat}_{Nat} (= \mathbb{N}) \text{ gilt } Nat \models_{z(X/n)} X + 0 = X \\
\Leftrightarrow & \text{für alle } n \in \mathrm{nat}_{Nat} \text{ gilt } \mathrm{val}_{Nat,z(X/n)}(X + 0) = \mathrm{val}_{Nat,z(X/n)}(X) \\
\Leftrightarrow & \text{für alle } n \in \mathrm{nat}_{Nat} \text{ gilt } \mathrm{val}_{Nat,z(X/n)}(X) +_{Nat} \mathrm{val}_{Nat,z(X/n)}(0) = \mathrm{val}_{Nat,z(X/n)}(X) \\
\Leftrightarrow & \text{für alle } n \in \mathrm{nat}_{Nat} \text{ gilt } z(X/n)(X) +_{Nat} 0_{Nat} = z(X/n)(X) \text{ gdw} \\
\Leftrightarrow & \text{für alle } n \in \mathrm{nat}_{Nat} \text{ gilt } n +_{Nat} 0_{Nat} = n \\
\Leftrightarrow & \text{für alle } n \in \mathrm{nat}_{Nat} \text{ gilt } n = n \\
\Leftrightarrow & true
\end{array}
$$

Verwende Definition 4.17 und 4.18 um zu zeigen, dass die Formel $\neg(X = Y) \rightarrow X \leq Y$ *nicht* in Nat gültig ist. Verwende ein 'Gegenbeispiel', etwa gilt $1 \neq 0$, aber nicht $1 \leq_{Nat} 0$.

Sei also z ein Zustand über V und Nat mit $z(X) = 1$ und $z(Y) = 0$.
Widerlege: $Nat \models_z \neg(X = Y) \rightarrow X \leq Y$

$$
\begin{array}{ll}
 & Nat \models_z \neg(X = Y) \rightarrow X \leq Y \\
\Leftrightarrow & Nat \not\models_z \neg(X = Y) \text{ oder } Nat \models_z X \leq Y \\
\Leftrightarrow & Nat \models_z X = Y \text{ oder } Nat \models_z X \leq Y \\
\Leftrightarrow & \mathrm{val}_{Nat,z}(X) = \mathrm{val}_{Nat,z}(Y) \text{ oder } \mathrm{val}_{Nat,z}(X) \leq_{Nat} \mathrm{val}_{Nat,z}(Y) \\
\Leftrightarrow & z(X) = z(Y) \text{ oder } z(X) \leq_{Nat} z(Y) \\
\Leftrightarrow & 1 = 0 \text{ oder } 1 \leq_{Nat} 0 \\
\Leftrightarrow & false \text{ oder } false \\
\Leftrightarrow & false
\end{array}
$$

Lösung zu (2)
Sei $\varphi \equiv X = 0 \vee (\exists Y X = \mathrm{succ}(Y))$. Das φ zugeordnete Induktionsprinzip lautet:

$$(\varphi_0 \wedge \varphi_{X \rightarrow \mathrm{succ}(X)}) \rightarrow \varphi_{\forall X}$$

mit

$$
\begin{array}{ll}
\varphi_0 & \equiv (0 = 0 \vee \exists Y 0 = \mathrm{succ}(Y)) \\
\varphi_{X \rightarrow \mathrm{succ}(X)} & \equiv \forall X(\varphi \rightarrow (\mathrm{succ}(X) = 0 \vee (\exists Y \mathrm{succ}(X) = \mathrm{succ}(Y)))) \\
\varphi_{\forall X} & \equiv \forall X \varphi
\end{array}
$$

Lösung zu (3)
Sei $\varphi_{Primzahl}$ definiert durch

$$\forall Y \forall Z((X = Y \cdot Z \rightarrow (Y = \text{succ}(0) \vee Z = \text{succ}(0))) \wedge X \neq \text{succ}(0))$$

Es muss gezeigt werden, dass $\varphi_{Primzahl}$ die Menge P der Primzahlen in nat definiert. Verwende hierzu wieder Definitionen 4.17 und 4.18.

Sei $n \in nat_{Nat}$, z Zustand über V und Nat.
Zeige: $Nat \models_{z(X/n)} \varphi_{Primzahl} \Leftrightarrow n$ ist Primzahl.

$Nat \models_{z(X/n)} \varphi_{Primzahl}$
$\Leftrightarrow$ {Definition 4.17}
für alle $a, b \in nat_{Nat}$ gilt
$Nat \models_{z(X/n)(Y/a)(Z/b)} ((X = Y \cdot Z \rightarrow (Y = \text{succ}(0) \vee Z = \text{succ}(0))) \wedge X \neq \text{succ}(0))$
$\Leftrightarrow$ {Definition 4.17 wiederholt anwenden}
für alle $a, b \in nat_{Nat}$ gilt $(n \neq a \cdot b$ oder $a = 1$ oder $b = 1)$ und $n \neq 1$
$\Leftrightarrow$ {Algebra}
n ist Primzahl

Lösung zu (4)
Sei φ_{ggT} definiert durch

$$((Z|X \wedge Z|Y) \wedge \forall Z'((Z'|X \wedge Z'|Y) \rightarrow Z'|Z))$$

Die Formel φ_{ggT} besitzt drei freie Variablen, nämlich X, Y, Z. Anschaulich sagt die Formel φ_{ggT}, dass Z ein gemeinsamer Teiler von X und Y ist $(Z|X \wedge Z|Y)$, und dass jeder weitere gemeinsame Teiler Z' von X und Y ein Teiler von Z ist. Die Teilbarkeitsrelation $| \subseteq \text{Nat}^2$ ist ebenfalls in Nat definierbar. Sie lässt sich durch folgende Formel definieren:

$$\varphi_| \equiv \exists Z\, Y = Z \cdot X,$$

d.h. $X|Y$ (X teilt Y), wenn es eine Faktorisierung $Y = Z \cdot X$ gibt.
Es muss gezeigt werden, dass φ_{ggT} die dreistellige Relation $\text{ggT} \subseteq \text{Nat}^3$ definiert. Verfahre hierbei analog zu vorherigem Aufgabenteil.

Aufgabe 3.4. Sei α folgendes Programm über einer beliebigen Signatur und einer Variablenmenge V mit $V \supseteq \{X, Y, T\}$:

$$T := X;\ X := Y;\ Y := T;$$

Dabei seien T, X, Y verschiedene Variablen.

ad (1) Zeige: Es gibt eine Algebra A und Zustände z, z', so dass

$$z[\![\alpha]\!]z' \text{ mit } z' = z(X/val_{A,z}(Y), Y/val_{A,z}(X))$$

nicht gilt.
Wähle z.B. die Algebra Nat und einen Zustand $z : V \rightarrow Nat$ mit $z(T) = 3$, $z(X) = 4$, $z(Y) = 5$. Dann gilt $z[\![\alpha]\!]z(X/5, Y/4, T/4)$, aber nicht $z[\![\alpha]\!]z(X/5, Y/4)$.

ad (2) Für alle Algebren A und Zustände z gilt

$$z[\![\alpha]\!]z(X/val_{A,z}(Y), Y/val_{A,z}(X), T/val_{A,z}(X))$$

Beweis:
Unter Verwendung der Definition 4.27 ergibt sich:

(1) $z[\![T := X;\ ]\!]_A z'$ mit $z' = z(T/val_{A,z}(X))$

(2) $z'[\![X := Y;\ ]\!]_A z''$ mit

$$\begin{aligned} z'' &= z'(X/val_{A,z'}(Y)) \\ &= z(T/val_{A,z}(X))(X/val_{A,z(T/val_{A,z}(X))}(Y)) \\ &= z(T/val_{A,z}(X))(X/val_{A,z}(Y)) \\ &= z(T/val_{A,z}(X), X/val_{A,z}(Y)) \end{aligned}$$

(3) $z''[\![Y := T;\ ]\!]_A z'''$ mit

$$\begin{aligned} z''' &= z''(Y/val_{A,z''}(T)) \\ &= z(T/val_{A,z}(X), X/val_{A,z}(Y))(Y/val_{A,z(T/val_{A,z}(X),X/val_{A,z}(Y))}(T)) \\ &= z(T/val_{A,z}(X), X/val_{A,z}(Y), Y/val_{A,z}(X)) \end{aligned}$$

(4) Mit obigen Ergebnissen ergibt sich insgesamt (vergl. Definition 4.27, Komposition) die Behauptung.