Aufgaben und Lösungshinweise

zur zweiten schriftliche Überprüfung zur Vorlesung

Grundlagen der Programmierung

vom 16. Mai 2000

Aufgabe 1 (2 Punkte)

Geben Sie die Definitionen der Kompositions-Regel und der while-Regel des Hoare-Kalküls an.

Aufgabe 2 (2+2 Punkte)

Sei $sig = (\{\mathsf{any}\}, \{\mathsf{a}, \mathsf{b}, \mathsf{f}\}, \alpha)$ mit $\alpha(\mathsf{a}) = \to\mathsf{any}$, $\alpha(\mathsf{b}) = \to\mathsf{any}$, $\alpha(\mathsf{f}) = \mathsf{any}, \mathsf{any} \to \mathsf{any}$ und $x, y, z \in V_{\mathsf{any}}$.

1. Sei die Substitution σ gegeben durch $\sigma = \{x/\mathsf{a}, y/\mathsf{f}(x, \mathsf{f}(y, z)), z/x\}$. Bestimmen Sie das Ergebnis von:
$$\sigma\,(\forall x.\,(\mathsf{f}(x, y) = \mathsf{a} \;\wedge\; \exists y.\mathsf{f}(y, \mathsf{f}(x, z)) = \mathsf{b}))$$

2. Es seien folgende Formeln gegeben:
$$\begin{array}{lcl} A & \equiv & \forall x.\,(\,\mathsf{f}(\mathsf{a}, x) = \mathsf{a} \;\wedge\; \mathsf{f}(x, \mathsf{b}) = x\,) \\ B & \equiv & \forall x.\forall y.\,(\,\mathsf{f}(x, y) = \mathsf{f}(y, x)\,) \end{array}$$
Geben Sie eine sig-Algebra $\mathcal{A}$ an mit $\mathcal{A} \models A$, aber nicht $\mathcal{A} \models B$. Beweisen Sie Ihre Behauptung.

Aufgabe 3 (2+2 Punkte)

Gegeben sei folgendes Programm α mit Eingabevariable X_1 und Ausgabevariable X_0 über der Algebra $\mathcal{A}$ der natürlichen Zahlen (Die Anweisungen sind für die Teilaufgaben auf der rechten Seite durchnummeriert):

$$\begin{array}{lll} \alpha: & X_0 := 0; & \}\ \alpha_1 \\ & U \ := 0; & \}\ \alpha_2 \\ & V \ := 1; & \}\ \alpha_3 \\ & \left.\begin{array}{ll} \mathsf{while}\ \ U < X_1\ \ \mathsf{do} & \\ \quad X_0 := X_0 + V; & \}\ \alpha_5 \\ \quad U \ := U + 1; & \}\ \alpha_6 \\ \quad V \ := V + 2; & \}\ \alpha_7 \\ \mathsf{end}; & \end{array}\right\} & \alpha_4 \end{array}$$

1. Wir schreiben eine Konfiguration (β, z) in der Form $(\beta, \langle z(X_0), z(X_1), z(U), z(V)\rangle)$. Sei der Startzustand z_0 gegeben durch $z_0(X_1) = 2$. Berechnen Sie die Konfigurationsfolge zur Startkonfiguration (α, z_0).

   Welche Funktion $f : \mathbb{N} \to \mathbb{N}$ berechnet α? (Ohne Beweis)

2. Die Vorbedingung zu α sei $X_1 = a$. Bestimmen Sie eine Schleifeninvariante φ für die while-Schleife α_4, indem Sie folgende Formel vervollständigen (ohne Beweis):
$$\varphi \quad\equiv\quad (X_0 = \quad \ldots \quad) \wedge (X_1 = \quad \ldots \quad) \wedge (U \leq \quad \ldots \quad) \wedge (V = \quad \ldots \quad)$$

zu 1.:

$0: \quad (\alpha, \qquad \langle -,2,-,-\rangle)$

$1: \quad (\alpha_2\,\alpha_3\,\alpha_4,\ \langle 0,2,-,-\rangle)$

$2:$

$\vdots$

Aufgabe 4 (5 Punkte)

Gegeben sei folgendes Programm α über der Algebra $\mathcal{A}$ *der ganzen Zahlen* $\mathbb{Z}$.

$$
\begin{array}{ll}
\alpha: & U := X_1 + 1; \\
& V := -X_1; \\
& \mathsf{if}\ \ U > 0\ \ \mathsf{then} \\
& \quad X_0 := X_1; \\
& \mathsf{else} \\
& \quad X_0 := V; \\
& \mathsf{end;}
\end{array}
$$

Beweisen Sie $\{X_1 = a\}\,\alpha\,\{X_0 = |a|\}$ mit Hilfe des Hoare-Kalküls. Sie dürfen die abgeleiteten Regeln aus der Vorlesung verwenden.

Lösungshinweise

1. Kompositions- und while-Regel:

$$
\frac{\{\varphi\}\ \alpha\ \{\varphi'\} \quad \{\varphi'\}\ \beta\ \{\psi\}}{\{\varphi\}\ \alpha\,\beta\ \{\psi\}}
\qquad\qquad
\frac{\{\xi \wedge B\}\ \beta\ \{\xi\}}{\{\xi\}\ \mathsf{while}\ B\ \mathsf{do}\ \beta\ \mathsf{end;}\ \{\xi \wedge \neg B\}}
$$

2.1

$$
\begin{array}{l}
\sigma(\forall x.(\mathsf{f}(x,y) = \mathsf{a}\ \wedge\ \exists y.\mathsf{f}(y,\mathsf{f}(x,z)) = \mathsf{b})) \\
= \\
\forall x'.\sigma((\mathsf{f}(x,y) = \mathsf{a}\ \wedge\ \exists y.\mathsf{f}(y,\mathsf{f}(x,z)) = \mathsf{b})^{x,x'}) \\
= \\
\forall x'.(\mathsf{f}(x',\sigma(y)) = \mathsf{a}\ \wedge\ \sigma(\exists y.\mathsf{f}(y,\mathsf{f}(x',z)) = \mathsf{b})) \\
= \\
\forall x'.(\mathsf{f}(x',\sigma(y)) = \mathsf{a}\ \wedge\ \exists y'.\sigma((\mathsf{f}(y,\mathsf{f}(x',z)) = \mathsf{b})^{y,y'})) \\
= \\
\forall x'.(\mathsf{f}(x',\sigma(y)) = \mathsf{a}\ \wedge\ \exists y'.\mathsf{f}(y',\mathsf{f}(x',\sigma(z))) = \mathsf{b}) \\
= \\
\forall x'.(\mathsf{f}(x',\mathsf{f}(x,\mathsf{f}(y,z))) = \mathsf{a}\ \wedge\ \exists y'.\mathsf{f}(y',\mathsf{f}(x',x)) = \mathsf{b})
\end{array}
$$

2.2 Eine mögliche *sig*-Algebra ist zum Beispiel: $\mathcal{A} = \big(\{A_{\mathsf{any}}\}, \{\mathsf{a}^{\mathcal{A}}, \mathsf{b}^{\mathcal{A}}, \mathsf{f}^{\mathcal{A}}\}, \varnothing\big)$ mit $A_{\mathsf{any}} = \mathbb{N}$, $\mathsf{a}^{\mathcal{A}} = 0$, $\mathsf{b}^{\mathcal{A}} = 1$ und $\mathsf{f}^{\mathcal{A}}(n,m) = n = \pi_1^2(n,m)$ für alle $n,m \in \mathbb{N}$. Es gilt $\mathcal{A} \models A$, da für alle $n \in \mathbb{N}$: $\mathsf{f}^{\mathcal{A}}(\mathsf{a}^{\mathcal{A}},n) = \pi_1^2(0,n) = 0 = \mathsf{a}^{\mathcal{A}}$ und $\mathsf{f}^{\mathcal{A}}(n,\mathsf{b}^{\mathcal{A}}) = \pi_1^2(n,1) = n$. Weiterhin gilt $\mathcal{A} \not\models B$, da beispielsweise $\mathsf{f}^{\mathcal{A}}(0,1) = 0 \neq 1 = \mathsf{f}^{\mathcal{A}}(1,0)$.

3.1

$0:$	$(\alpha,$	$\langle -, 2, -, -\rangle)$	
$1:$	$(\alpha_2\,\alpha_3\,\alpha_4,$	$\langle\ 0,\ 2, -, -\rangle)$	
$2:$	$(\alpha_3\,\alpha_4,$	$\langle\ 0,\ 2,\ 0, -\rangle)$	
$3:$	$(\alpha_4,$	$\langle\ 0,\ 2,\ 0,\ 1\rangle)$	
$4:$	$(\alpha_5\,\alpha_6\,\alpha_7\,\alpha_4,$	$\langle\ 0,\ 2,\ 0,\ 1\rangle)$	da $0 < 2$
$5:$	$(\alpha_6\,\alpha_7\,\alpha_4,$	$\langle\ 1,\ 2,\ 0,\ 1\rangle)$	
$6:$	$(\alpha_7\,\alpha_4,$	$\langle\ 1,\ 2,\ 1,\ 1\rangle)$	
$7:$	$(\alpha_4,$	$\langle\ 1,\ 2,\ 1,\ 3\rangle)$	
$8:$	$(\alpha_5\,\alpha_6\,\alpha_7\,\alpha_4,$	$\langle\ 1,\ 2,\ 1,\ 3\rangle)$	da $1 < 2$
$9:$	$(\alpha_6\,\alpha_7\,\alpha_4,$	$\langle\ 4,\ 2,\ 1,\ 3\rangle)$	
$10:$	$(\alpha_7\,\alpha_4,$	$\langle\ 4,\ 2,\ 2,\ 3\rangle)$	
$11:$	$(\alpha_4,$	$\langle\ 4,\ 2,\ 2,\ 5\rangle)$	
$12:$	$(\varepsilon,$	$\langle\ 4,\ 2,\ 2,\ 5\rangle)$	da nicht $2 < 2$

Es wird die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(x) = x^2$ berechnet.

3.2 $\varphi \equiv (X_0 = U^2) \wedge (X_1 = a) \wedge (U \leq X_1) \wedge (V = 2 \cdot U + 1)$

4. Behauptung: $\{X_1 = a\}\,\alpha\,\{X_0 = |a|\}$
Beweis mit Hilfe des Hoare-Kalküls

(1) $\{X_1 = a\}\,\alpha\,\{X_0 = |a|\}$ abgeleitete Kompositionsregel
$\hookrightarrow$(2) $\{X_1 = a\}\ U := X_1 + 1;\ \{X_1 = a \wedge U = X_1 + 1\}$
$\hookrightarrow$(3) $\{X_1 = a \wedge U = X_1 + 1\}\ V := -X_1;\ \{X_1 = a \wedge U = X_1 + 1 \wedge V = -X_1\}$
$\hookrightarrow$(4) $\{X_1 = a \wedge U = X_1 + 1 \wedge V = -X_1\}$ $\mathsf{if} \ldots \mathsf{end};$ $\{X_0 = |a|\}$

(2) abgeleitete Zuweisungsregel
$\hookrightarrow$(5) $(X_1 = a) \to (X_1 = a \wedge X_1 + 1 = X_1 + 1) \in \mathrm{Th}(\mathcal{A})$

(3) abgeleitete Zuweisungsregel
$\hookrightarrow$(6) $(X_1 = a \wedge U = X_1 + 1) \to (X_1 = a \wedge U = X_1 + 1 \wedge -X_1 = -X_1) \in \mathrm{Th}(\mathcal{A})$

(4) if-Regel
$\hookrightarrow$(7) $\{X_1 = a \wedge U = X_1 + 1 \wedge V = -X_1 \wedge U > 0\}\ X_0 := X_1;\ \{X_0 = |a|\}$
$\hookrightarrow$(8) $\{X_1 = a \wedge U = X_1 + 1 \wedge V = -X_1 \wedge \neg(U > 0)\}\ X_0 := V;\ \{X_0 = |a|\}$

(7) abgeleitete Zuweisungsregel
$\hookrightarrow$(9) $(X_1 = a \wedge U = X_1 + 1 \wedge V = -X_1 \wedge U > 0) \to (X_1 = |a|) \in \mathrm{Th}(\mathcal{A})$
denn für alle $n, m, k \in \mathbb{Z}$ gilt: Aus $k = n$, $m = k + 1$ und $m > 0$ folgt $n = k = m - 1 \geq 0$ und somit $k = n = |n|$.

(8) abgeleitete Zuweisungsregel
$\hookrightarrow$(10) $(X_1 = a \wedge U = X_1 + 1 \wedge V = -X_1 \wedge \neg(U > 0)) \to (V = |a|) \in \mathrm{Th}(\mathcal{A})$
denn für alle $n, m, k, j \in \mathbb{Z}$ gilt: Aus $k = n$, $m = k + 1$, $j = -k$ und nicht $m > 0$ folgt $n = k = m - 1 < 0$ und somit $j = -k = -n = |n|$.

Da alle Teilziele erfolgreich bearbeitet wurden, gilt die Behauptung.