Semantik und Programmverifikation

Prof. Dr. Christoph Walther / Simon Siegler
Technische Universität Darmstadt — Wintersemester 2008/09

Übungsblatt mit Lösungsvorschlag 5

Aufgabe 5.1 (Fixpunkte)

Gegeben sei die Funktionsprozedur $F_{modifac} =$

$$\begin{array}{lll} \textbf{function } modifac(x : nat) : nat & \Leftarrow & \textbf{if } x = 0 \\ & & \quad \textbf{then } modifac(0) \\ & & \quad \textbf{else } x \otimes modifac(pred(x)) \\ & & \textbf{fi}. \end{array}$$

(a) Stellen Sie zu dieser Funktionsprozedur eine Fixpunktgleichung der Form $\phi = \mathcal{R}_F[\![\phi]\!]$ für $\phi \in \{\mathbb{N} \to \mathbb{N} \cup \{\bot\}\}$ auf. Bestimmen Sie die Lösungen dieser Gleichung, wenn Sie das Zeichen $\otimes$ in obiger Funktionsprozedur als die übliche Multiplikation interpretieren. Sie brauchen keinen Nachweis zu führen, dass Ihre Aufzählung *alle* Lösungen beinhaltet.

Lösungsvorschlag:

$$\phi(n) = \begin{cases} \phi(0), & \text{falls } n = 0 \\ n \otimes \phi(n-1), & \text{sonst} \end{cases}$$

Menge der Lösungen für diese Gleichung: $\{\omega_{\mathbb{N}\to\mathbb{N}\cup\{\bot\}}\} \cup \{fac_n | n \in \mathbb{N}\}$ wobei $fac_n : \mathbb{N} \to \{\bot\}$ mit $fac_n(m) = n \cdot m!$. Man beachte: $n \otimes m = \begin{cases} n \cdot m, & \text{für } n, m \in \mathbb{N} \\ \bot, & \text{sonst} \end{cases}$

(b) Wie lautet der kleinste Fixpunkt von $\mathcal{R}_F$ bezüglich der Relation $\sqsubseteq_{\mathbb{N}\to\mathbb{N}\cup\{\bot\}}$?

Lösungsvorschlag:

kleinster Fixpunkt ist $\omega_{\mathbb{N}\to\mathbb{N}\cup\{\bot\}}$.

Aufgabe 5.2 (Fixpunkt einer Iterationsfolge)

Sei $P = \langle F \rangle$ ein funktionales Programm mit $F =$

$$\begin{array}{lll} \textbf{function } f(x : nat) : nat & \Leftarrow & \textbf{if } x = 0 \\ & & \quad \textbf{then } 0 \\ & & \quad \textbf{else if } x = 1 \\ & & \qquad \textbf{then } f(x+2) - 1 \\ & & \qquad \textbf{else } 1 + f(x-2) \\ & & \quad \textbf{fi} \\ & & \textbf{fi}, \end{array}$$

wobei $x + 2$ abkürzend für $succ(succ(x))$ und $x - 2$ für $pred(pred(x))$ steht. Bestimmen Sie für das Funktional $\mathcal{R}_P$ des Programms P die Iterationsfolge $\langle \phi_i \rangle_{i \in \mathbb{N}}$ sowie den kleinsten Fixpunkt $\phi = fix_{\mathcal{R}_P}$ von $\mathcal{R}_P$ (vgl. 2.3.11.(i)).

Lösungsvorschlag:

nach Definition 2.3.15 gilt: $\mathfrak{R}_P[\![\phi]\!] = \mathfrak{R}_F[\![\phi]\!]$ mit $\mathfrak{R}_F[\![\phi]\!](n) = d(\phi)[x/n](R_f)$.

Es gilt: $d(\phi)[x/n](R_f) = \delta_{if}(\delta_{eq}(n,0), 0, \delta_{if}(\delta_{eq}(n,1), \delta_{pred}(\phi(\delta^2_{succ}(n))), \delta_{succ}(\phi(\delta^2_{succ}(n)))))$

Das kann man vereinfachen zu: $d(\phi)[x/n](R_f) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0 & \text{falls } n = 0 \\ \delta_{pred}(\phi(\delta^2_{succ}(n))) & \text{falls } n = 1 \\ \delta_{succ}(\phi(\delta^2_{succ}(n)))) & \text{sonst} \end{cases}$

Damit haben wir das wir das Funktional bestimmt.

Zur bestimmung der Iterationsfolge geben wir zuerst einige Elemente an, geben dann eine Vermutung für die allgemeine Form an, die wir anschliessend beweisen.

$\phi_0(n) = \varnothing$

$\phi_1(n) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0, & \text{falls } n = 0 \\ \varnothing, & \text{sonst} \end{cases}$

$\phi_2(n) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0, & \text{falls } n = 0 \\ 1, & \text{falls } n = 2 \\ \varnothing, & \text{sonst} \end{cases}$

$\phi_3(n) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0, & \text{falls } n = 0 \\ 1, & \text{falls } n = 2 \\ 2, & \text{falls } n = 4 \\ \varnothing, & \text{sonst} \end{cases}$

$\phi_4(n) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0, & \text{falls } n = 0 \\ 1, & \text{falls } n = 2 \\ 2, & \text{falls } n = 4 \\ 3, & \text{falls } n = 6 \\ \varnothing, & \text{sonst} \end{cases}$

Es ergibt sich allgemein die folgende Vermutung:

$\forall i \in \mathbb{N}. \underbrace{\forall n \in D_{nat}. \phi_i(n) = \psi_i(n)}_{P(i)}$ mit $\psi_i(n) = \begin{cases} succ^m(0), & \text{falls } n = succ^{2m}(0) \text{ und } m < i \\ \varnothing, & \text{sonst} \end{cases}$

Wir beweisen dies durch natürliche Induktion über i:

Basisfall $P(0)$**:** $\Rightarrow \phi_0(n) = \varnothing \wedge \psi_0(n) = \varnothing \surd$.

Schrittfall $P(n) \Rightarrow P(n+1)$**:** $\phi_{i+1}(n) = \mathfrak{R}_F\,[\![\phi_i]\!]\,(n) \underbrace{=}_{IH} \mathfrak{R}_F\,[\![\psi_i]\!]\,(n) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0, & \text{falls } n = 0 \\ \delta_{pred}(\phi(\delta^2_{succ}(n))) & \text{falls } n = 1 \\ \delta_{succ}(\phi(\delta^2_{succ}(n)))) & \text{sonst} \end{cases}$

Wir müssen also zeigen $\psi_{i+1}(n) = \begin{cases} \varnothing, & \text{falls } n = \varnothing \\ 0, & \text{falls } n = 0 \\ \delta_{pred}(\phi(\delta^2_{succ}(n))) & \text{falls } n = 1 \\ \delta_{succ}(\phi(\delta^2_{succ}(n)))) & \text{sonst} \end{cases}$

Fall $n = \varnothing$**:** $\psi_{i+1}(n) = \varnothing\surd$

Fall $n = 0$**:** $0 < i + 1$ und $n = succ^{2\cdot 0}(0) \Rightarrow \psi_{i+1}(0) = 0\surd$

Fall $n = 1$**:** $\Rightarrow \delta^2_{succ}(n) = 3 \Rightarrow$ es gibt kein $m \in \mathbb{N}$ mit $\delta^2_{succ}(n) = succ^{2m}(0) \Rightarrow \psi_i(\delta^2_{succ}(n)) = \varnothing$ $\Rightarrow \delta_{pred}(\psi_i(\delta^2_{succ}(n))) = \varnothing$
Wir müssen also zeigen: $\psi_{i+1}(n) = \varnothing\ n = 1 \Rightarrow$ es gibt kein $m \in \mathbb{N}$ mit $n = succ^{2m}(0)$ $\Rightarrow \psi_{i+1}(n) = \varnothing\surd$

Fall $n \neq \varnothing \wedge n \neq 0 \wedge n \neq 1$**:**

Fall $\forall m \in \mathbb{N}.n \neq succ^{2m}(0)$**:** $\Rightarrow \psi_{i+1}(n) = \varnothing$ und $\delta_{succ}(\psi_i(\delta^2_{pred}(n))) = \varnothing$

Fall $n = succ^{2m}(0)$ **für ein** $m \in \mathbb{N}$ **und** $m < i + 1$**:** $\Rightarrow \psi_{i+1}(n) = succ^m(0)$ weiter gilt:
$\delta_{succ}(\psi_i(\delta^2_{pred}(n))) \underbrace{=}_{n\geq 2} \delta_{succ}(\psi_i(succ^{2(m-1)}(0))) \underbrace{=}_{m-1<i} \delta_{succ}(succ^{m-1}(0)) = succ^m(0)$

Fall $n = succ^{2m}(0)$ **für ein** $m \in \mathbb{N}$ **und** $m \geq i + 1$**:**

$\Rightarrow \psi_{i+1}(n) = \varnothing, \delta_{succ}(\psi_i(\delta^2_{pred}(n))) = \varnothing$. Also $\psi_{i+1}(n) = \delta_{succ}(\psi_i(\delta^2_{pred}(n)))$

$\Rightarrow$ Induktion abgeschlossen $\Rightarrow \forall i \in \mathbb{N}.\phi_i = \psi_i$

$\Rightarrow$ kleinster Fixpunkt $\phi(n) = \begin{cases} succ^m(0), & \text{falls } n = succ^{2m}(0) \text{ für ein } m \in \mathbb{N} \\ \varnothing, & \text{sonst} \end{cases}$

Aufgabe 5.3 (Ordnung zwischen semantischen Funktionen)

Sei $P = \langle$ **function** $fie(x, y : nat) : nat \Leftarrow succ(x)$,

function $foo(x, y : nat) : nat \Leftarrow$
$if_{nat}(eq(x, y), succ(y), succ(x))\ \rangle$.

Vergleichen Sie $\delta_{P,fie}$ und $\delta_{P,foo}$ bezüglich $\sqsubseteq_{\mathcal{D}_{nat,nat}\to\mathcal{D}_{nat}}$ (vgl. Übung 2.3.12).

Lösungsvorschlag:

Die Funktionen nehmen folgende Werte an:

x	y	$\delta_{P,foo}(x, y)$	$\delta_{P,fie}(x, y)$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$\varnothing$	$t \neq \varnothing$	$\varnothing$	$\varnothing$
$t \neq \varnothing$	$\varnothing$	$\varnothing$	$\delta_{succ}(t)$
$t \neq \varnothing$	$s \neq \varnothing$	$\delta_{succ}(t)$	$\delta_{succ}(t)$

Damit gilt also, $\forall d \in \mathcal{D}_{nat}.\ \delta_{P,foo}(d) \sqsubseteq_{\mathcal{D}_{nat}} \delta_{P,fie}(d)$ und damit $\delta_{P,foo} \sqsubseteq_{\mathcal{D}_{nat,nat}\to\mathcal{D}_{nat}} \delta_{P,fie}$

Aufgabe 5.4 (eval_P-Auswertungen)

Zeigen Sie unter Verwendung von Übung 2.3.2.(iv), dass für alle $f \in \Sigma(P)_{w,s}$ mit $w = s_1 \dots s_n$, alle $t_1 \dots t_n \in \mathcal{T}(\Sigma(P))_w$ und alle $i \in \{1, \dots, n\}$ gilt: Aus $\mathsf{eval}_P(t_i) = \propto$ folgt $\mathsf{eval}_P(f(t_1, \dots, t_n)) = \propto$ oder $\mathsf{eval}_P(f(t_1, \dots, t_n)) = \mathsf{eval}_P(f(t_1, \dots, t_{i-1}, t, t_{i+1}, \dots, t_n))$ für alle $t \in \mathcal{T}(\Sigma(P))_{s_i}$ (vgl. Übung 2.4.1).

Lösungsvorschlag:

Es gilt: $\mathsf{eval}_P(t_i) = \propto \Rightarrow \mathsf{sem}_{\mathrm{op}}[\![P]\!](t_i) = \propto \Leftrightarrow \mathsf{sem}_{\mathrm{dn}}[\![P]\!](t_i) = \propto \Rightarrow D_P(t_i) = \varnothing_{s_i}$ Da nach Lemma 2.3.15 D_P monoton ist, ist auch $\delta_{P,f}$ monoton. Mit Übung 2.3.2.(iv) gilt dann für jedes $t \in \mathcal{T}(\Sigma(P))_{s_i}$:

(1): $\delta_{P,f}(D_p(t_1), \dots, \varnothing_{s_i}, \dots, D_P(t_n)) = \varnothing_s$ oder

(2): $\delta_{P,f}(D_P(t_1), \dots, \varnothing_{s_i}, \dots, D_P(t_n)) = \delta_{P,f}(D_P(t_1), \dots, D_P(t), \dots, D_P(t_n))$.

(1): In diesem Fall ist $D_p(f(t_1, \dots, \varnothing_{s_i}, \dots, t_n)) = \varnothing_s$, also ist $\mathsf{sem}_{\mathrm{dn}}[\![P]\!](f(t_1, \dots, t_n)) = \propto$ und damit $\mathsf{sem}_{\mathrm{op}}[\![P]\!](f(t_1, \dots, t_n)) = \propto$, also folgt $\mathsf{eval}_P(f(t_1, \dots, t_n)) = \propto$

(2): In diesem Fall ist $D_p(f(t_1, \dots, \varnothing_{s_i}, \dots, t_n)) = D_p(f(t_1, \dots, t, \dots, t_n))$, also ist $\mathsf{sem}_{\mathrm{dn}}[\![P]\!](f(t_1, \dots, t_n)) = \mathsf{sem}_{\mathrm{dn}}[\![P]\!](f(t_1, \dots, t, \dots, t_n))$ und damit $\mathsf{sem}_{\mathrm{op}}[\![P]\!](f(t_1, \dots, t_n)) = \mathsf{sem}_{\mathrm{op}}[\![P]\!](f(t_1, \dots, t, \dots, t_n))$, also folgt $\mathsf{eval}_P(f(t_1, \dots, t_n)) = \mathsf{eval}_P(f(t_1, \dots, t, \dots, t_n))$

Insgesamt folgt also die Behauptung.