Semantik und Programmverifikation

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

Hausaufgabe mit Lösungsvorschlag 4

Hausaufgabe 4.1 (Stetigkeit eines Funktionals) **(1 + 2 = 3 Punkte)**

Sei $(E, \sqsubseteq_E)$ eine vollständige Halbordnung, in der jede $\sqsubseteq_E$–Kette endlich ist, und sei $\phi \in [E \to E]$.

(a) Zeigen Sie, dass $\langle \phi_i \circ \phi_i \rangle_{i \in \mathbb{N}}$ eine $\sqsubseteq_{E\to E}$-Kette in $[E \to E]$ ist, falls $\langle \phi_i \rangle_{i \in \mathbb{N}}$ eine $\sqsubseteq_{E\to E}$-Kette in $[E \to E]$ ist. Hierbei bezeichnet $\circ$ die Funktionskomposition, also $(\phi \circ \phi)(x) = \phi(\phi(x))$.

Lösungsvorschlag:

zu zeigen: $\langle \phi_i \circ \phi_i \rangle_{i \in \mathbb{N}}$ ist eine $\sqsubseteq_{E\to E}$-Kette. Man muss also zeigen:

$$\forall i \in \mathbb{N}, e \in E : \phi_i(\phi_i(e)) \sqsubseteq_E \phi_{i+1}(\phi_{i+1}(e)).$$

Nach Voraussetzung ist $\langle \phi_i \rangle_{i \in \mathbb{N}}$ eine Kette. Also gilt $\forall i \in \mathbb{N}, e \in E : \phi_i(e) \sqsubseteq_E \phi_{i+1}(e)$ (1.).
Seien $i \in \mathbb{N}$ und $e \in E$ beliebig, so folgt mit (1.) $\phi_i(\phi_i(e)) \sqsubseteq_E \phi_i(\phi_{i+1}(e))$ (2.) Da aber $\phi_{i+1}(e) \in E$, folgt aus (1.) auch $\phi_i(\phi_{i+1}(e)) \sqsubseteq_E \phi_{i+1}(\phi_{i+1}(e))$ (3.). Aus (2.) und (3.) folgt mit der Transitivität von $\sqsubseteq_E$: $\phi_i(\phi_i(e)) \sqsubseteq_E \phi_{i+1}(\phi_{i+1}(e))$. Da i und e beliebig waren folgt: $\forall i \in \mathbb{N}.\phi_i \circ \phi_i \sqsubseteq \phi_{i+1} \circ \phi_{i+1}$ $\Rightarrow \langle \phi_i \circ \phi_i \rangle$ ist eine Kette.

(b) Zeigen Sie, dass das Funktional $\mathcal{SQ} : [E \to E] \to [E \to E]$ mit $\mathcal{SQ}[\![\phi]\!] = \phi \circ \phi$ für alle $\phi \in [E \to E]$ bezüglich der Relation $\sqsubseteq_{E\to E}$ stetig ist.

Hinweis: zeigen Sie $\mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!] = \sup_i \langle \mathcal{SQ}[\![\phi_i]\!] \rangle$ durch den Beweis von

$$\begin{array}{lccc} 1. & \sup_i \langle \mathcal{SQ}[\![\phi_i]\!] \rangle & \sqsubseteq_{E\to E} & \mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!] \\ 2. & \mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!] & \sqsubseteq_{E\to E} & \sup_i \langle \mathcal{SQ}[\![\phi_i]\!] \rangle \end{array}$$

Verwenden Sie für die zweite Beziehung Lemma 2.3.9. (vgl. Übung 2.3.8)

Lösungsvorschlag:

Zu zeigen: $\mathcal{SQ}$ ist stetig.

Monotonie: Wir zeigen zuerst: $\mathcal{SQ}$ ist monoton.
Seien also $\phi, \psi \in [E \to E]$ beliebig mit $\phi \sqsubseteq_{[E\to E]} \psi$, also $\forall e \in E.\, \phi(e) \sqsubseteq_E \psi(e)$ (1.). Wegen der Monotonie von ϕ folgt $\forall e \in E.\phi(\phi(e)) \sqsubseteq_E \phi(\psi(e))$ (2.). Da $\forall e \in E.\psi(e) \in E$ folgt aus (1.) auch $\forall e \in E.\phi(\psi(e)) \sqsubseteq_E \psi(\psi(e))$ (3.). Mit der Transitivität von $\sqsubseteq_E$ folgt aus (2.) und (3.) $\phi(\phi(e)) \sqsubseteq_E \psi(\psi(e))$. Also gilt $\mathcal{SQ}[\![\phi]\!] \sqsubseteq_{E\to E} \mathcal{SQ}[\![\psi]\!]$.

zu (1):

$$\begin{array}{lll} & \forall i \in \mathbb{N}.\phi_i \sqsubseteq_{E\to E} \sup_i \langle \phi_i \rangle & \text{Monotonie von } \mathcal{SQ} \\ \Rightarrow & \mathcal{SQ}[\![\phi_i]\!] \sqsubseteq_{E\to E} \mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!] & \mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!] \text{ obere Schranke} \\ \Rightarrow & \sup_i \langle \mathcal{SQ}[\![\phi_i]\!] \rangle \sqsubseteq_{E\to E} \mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!] & \end{array}$$

zu (2): Sei $e \in E$ beliebig.

$$(*) \left\{ \begin{array}{lll} & \mathcal{SQ}[\![\sup_i \langle \phi_i \rangle]\!](e) & \text{Definition } \mathcal{SQ} \\ = & \sup_i \langle \phi_i \rangle (\sup_i \langle \phi_i \rangle (e)) & \text{Lemma (2.3.9)} \\ = & \sup_i \langle \phi_i \rangle (\phi_{k_1}(e)) & \text{Lemma (2.3.9)} \\ = & \phi_{k_2}(\phi_{k_1}(e)) & \text{alle } \sqsubseteq_E\text{-Ketten endlich} \\ = & \phi_k(\phi_k(e)) & \\ = & \mathcal{SQ}[\![\phi_k]\!](e) & \end{array} \right.$$

wobei $k_1, k_2 \in \mathbb{N}$ und $k = \max\{k_1, k_2\}$. Nach (a) ist $\langle \mathcal{SQ}[\![\phi_i]\!]\rangle_{i\in\mathbb{N}}$ eine Kette. Und da $[E \to E]$ eine vollständige Halbordnung ist (siehe Hausaufgabe 6.3), existiert $\sup_i\langle \mathcal{SQ}[\![\phi_i]\!]\rangle$ und es gilt

$$\begin{array}{lll} & \mathcal{SQ}[\![\phi_k]\!] \sqsubseteq_{E\to E} \sup_i\langle \mathcal{SQ}[\![\phi_i]\!]\rangle & \\ \Rightarrow & \mathcal{SQ}[\![\phi_k]\!](e) \sqsubseteq_{E} \sup_i\langle \mathcal{SQ}[\![\phi_i]\!]\rangle(e) & (*) \\ \Rightarrow & \mathcal{SQ}[\![\sup_i\langle\phi_i\rangle]\!](e) \sqsubseteq_{E} \sup_i\langle \mathcal{SQ}[\![\phi_i]\!]\rangle(e) & \text{e beliebig} \\ \Rightarrow & \mathcal{SQ}[\![\sup_i\langle\phi_i\rangle]\!] \sqsubseteq_{E\to E} \sup_i\langle \mathcal{SQ}[\![\phi_i]\!]\rangle & \end{array}$$

Hausaufgabe 4.2 (Kleinster Fixpunkt einer Iterationsfolge) **(5 Punkte)**

Sei $P = \langle F_1, F_2\rangle$ ein funktionales Programm mit $F_1 =$

$$\begin{array}{lll} \textbf{function } f_1(x : nat) : nat & \Leftarrow & \textbf{if } x = 0 \\ & & \quad \textbf{then } 0 \\ & & \quad \textbf{else if } x = 1 \\ & & \qquad\quad \textbf{then } 0 \\ & & \qquad\quad \textbf{else } 1 + f_1(x-2) \\ & & \qquad \textbf{fi} \\ & & \textbf{fi} \end{array}$$

und $F_2 =$

$$\begin{array}{lll} \textbf{function } f_2(x : nat) : nat & \Leftarrow & \textbf{if } x = 0 \\ & & \quad \textbf{then } f_2(0) \\ & & \quad \textbf{else if } x = 1 \\ & & \qquad\quad \textbf{then } 0 \\ & & \qquad\quad \textbf{else } 1 + f_2(f_1(x)) \\ & & \qquad \textbf{fi} \\ & & \textbf{fi}, \end{array}$$

wobei $1 + x$ abkürzend für $succ(x)$ und $x - 2$ für $pred(pred(x))$ steht. Bestimmen Sie für das Funktional $\mathcal{R}_P$ des Programmes P die Iterationsfolge $\langle(\phi_{1,i}, \phi_{2,i})\rangle_{i\in\mathbb{N}}$ sowie den kleinsten Fixpunkt $(\phi_1, \phi_2) = fix_{\mathcal{R}_P}$ von $\mathcal{R}_P$ (vgl. Übung 2.3.11.(ii)).

Lösungsvorschlag:

Wir geben zuerst das Funktional an: $\mathcal{R}_P = (\mathcal{R}_{F_1}, \mathcal{R}_{F_2})$ mit

$$\begin{array}{lcl} \mathcal{R}_{F_1}[\![\phi_1, \phi_2]\!](d) & = & \delta_{if}(\delta_{eq}(d, 0), 0, \delta_{if}(\delta_{eq}(d, 1), 0, \delta_{succ}(\phi_1(\delta_{pred}(\delta_{pred}(d)))))) \\ \mathcal{R}_{F_1}[\![\phi_1, \phi_2]\!](d) & = & \delta_{if}(\delta_{eq}(d, 0), \phi_2(0), \delta_{if}(\delta_{eq}(d, 1), 0, \delta_{succ}(\phi_2(\phi_1(d))))) \end{array}$$

Wir vereinfachen das Funktional zu $\mathcal{R}_{F_1}[\![\phi_1, \phi_2]\!](d) = \begin{cases} \varnothing, & \text{falls } d = \varnothing \\ 0 & \text{falls } d \in \{0, 1\} \\ \delta_{succ}(\phi_1(\delta_{pred}(\delta_{pred}(d)))), & \text{sonst} \end{cases}$

$$\mathcal{R}_{F_2}[\![\phi_1, \phi_2]\!](d) = \begin{cases} \varnothing, & \text{falls } d = \varnothing \\ \phi_2(0), & \text{falls } d = 0 \\ 0, & \text{falls } d = 1 \\ \delta_{succ}(\phi_2(\phi_1(d))), & \text{sonst} \end{cases}$$

Um die Iterationsfolge zu bestimmen, berechnen wir einige Glieder dieser Folge:

$$\phi_{1,0}(d)=\varnothing \qquad \phi_{2,0}(d)=\varnothing$$

$$\phi_{1,1}(d)=\begin{cases}0, & \text{falls } d\in\{0,1\}\\ \varnothing, & \text{sonst}\end{cases} \qquad \phi_{2,1}(d)=\begin{cases}0, & \text{falls } d=1\\ \varnothing, & \text{sonst}\end{cases}$$

$$\phi_{1,2}(d)=\begin{cases}0, & \text{falls } d\in\{0,1\}\\ 1, & \text{falls } d\in\{2,3\}\\ \varnothing, & \text{sonst}\end{cases} \qquad \phi_{2,2}(d)=\begin{cases}0, & \text{falls } d=1\\ \varnothing, & \text{sonst}\end{cases}$$

$$\phi_{1,3}(d)=\begin{cases}0, & \text{falls } d\in\{0,1\}\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5\}\\ \varnothing, & \text{sonst}\end{cases} \qquad \phi_{2,3}(d)=\begin{cases}0, & \text{falls } d=1\\ 1, & \text{falls } d\in\{2,3\}\\ \varnothing, & \text{sonst}\end{cases}$$

$$\phi_{1,4}(d)=\begin{cases}0, & \text{falls } d\in\{0,1\}\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5\}\\ 3, & \text{falls } d\in\{6,7\}\\ \varnothing, & \text{sonst}\end{cases} \qquad \phi_{2,4}(d)=\begin{cases}0, & \text{falls } d=1\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5\}\\ \varnothing, & \text{sonst}\end{cases}$$

$$\phi_{1,5}(d)=\begin{cases}0, & \text{falls } d\in\{0,1\}\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5\}\\ 3, & \text{falls } d\in\{6,7\}\\ 4, & \text{falls } d\in\{8,9\}\\ \varnothing, & \text{sonst}\end{cases} \qquad \phi_{2,5}(d)=\begin{cases}0, & \text{falls } d=1\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5,6,7\}\\ \varnothing, & \text{sonst}\end{cases}$$

$$\phi_{1,6}(d)=\begin{cases}0, & \text{falls } d\in\{0,1\}\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5\}\\ 3, & \text{falls } d\in\{6,7\}\\ 4, & \text{falls } d\in\{8,9\}\\ 5, & \text{falls } d\in\{10,11\}\\ \varnothing, & \text{sonst}\end{cases} \qquad \phi_{2,6}(d)=\begin{cases}0, & \text{falls } d=1\\ 1, & \text{falls } d\in\{2,3\}\\ 2, & \text{falls } d\in\{4,5,6,7\}\\ 3, & \text{falls } d\in\{8,9\}\\ \varnothing, & \text{sonst}\end{cases}$$

Es ergibt sich die Vermutung: $\phi_{1,i}(d)=\psi_{1,i}(d)$ und $\phi_{2,i}(d)=\psi_{2,i}(d)$ mit (*)

$$\psi_{1,i}(d)=\begin{cases} succ^{\lfloor \frac{x}{2}\rfloor}(0), & \text{für } x<2i \text{ und } d=succ^x(0)\\ \varnothing, \text{sonst}\end{cases}$$

$$\psi_{2,0}(d)=\varnothing, \psi_{2,i}(d)=\begin{cases}\varnothing, & \text{falls } d=0\\ 0, & \text{falls } d=1\\ succ^{\lfloor \log_2 x\rfloor}(0), & \text{falls } 1\le x<2i-2 \text{ und } d=succ^x(0)\\ \varnothing, & \text{sonst}\end{cases} \quad \text{für } i>0.$$

Wir beweisen (*) mit Induktion über i:

Basis: $\phi_{1,0}=\psi_{1,0}$, $\phi_{2,0}=\psi_{2,0}$ trivial erfüllt.

Schritt: nach Induktionshypothese gilt $\phi_{1,i}=\psi_{1,i}$, $\phi_{2,i}=\psi_{2,i}$.

Weiter gilt $(\phi_{1,i+1},\phi_{2,i+1})=(\mathcal{R}_{F_1}[\![\phi_{1,i},\phi_{2,i}]\!],\mathcal{R}_{F_2}[\![\phi_{1,i},\phi_{2,i}]\!])\underbrace{=}_{IH}(\mathcal{R}_{F_1}[\![\psi_{1,i},\psi_{2,i}]\!],\mathcal{R}_{F_2}[\![\psi_{1,i},\psi_{2,i}]\!])$

Also bleibt lediglich zu zeigen:

$$\begin{array}{lcl} 1.\ \psi_{1,i+1} & = & \mathcal{R}_{F_1}[\![\psi_{1,i}, \psi_{2,i}]\!] \\ 2.\ \psi_{2,i+1} & = & \mathcal{R}_{F_2}[\![\psi_{1,i}, \psi_{2,i}]\!] \end{array}$$

zu 1.: Fallunterscheidung über d (orientiert sich an $\mathcal{R}_{F_1}$)

Fall $d = \varnothing:\ \Rightarrow \psi_{1,i+1}(d) = \varnothing = \mathcal{R}_{F_1}[\![\psi_{1,i}, \psi_{2,i}]\!]$

Fall $d \in \{0, 1\}$**:** $\Rightarrow \psi_{1,i+1}(d) = 0 = \mathcal{R}_{F_1}[\![\psi_{1,i}, \psi_{2,i}]\!]$

Fall sonst ($d = succ^x(0)$ **mit** $x > 1$)**:**

$\mathcal{R}_{F_1}[\![\psi_{1,i}, \psi_{2,i}]\!] = \delta_{succ}(\psi_{1,i}(\delta^2_{pred}(d))) = \delta_{succ}(\psi_{1,i}(succ^{x-2}(0))) = (*)$

Fall $x - 2 < 2i$**:** $(*) = \delta_{succ}(succ^{\lfloor \frac{x-2}{2} \rfloor}(0)) = succ^{\lfloor \frac{x}{2} \rfloor}(0))$.

$\psi_{1,i+1}(d) = \psi_{1,i+1}(succ^x(0)) \underbrace{=}_{x<2i+2=2(i+1)} succ^{\lfloor \frac{x}{2} \rfloor}(0))$

Fall $x - 2 \geq 2i$**:** $(*) = \varnothing$.

$\psi_{1,i+1}(succ^x(0)) \underbrace{=}_{x \geq 2(i+1)} \varnothing$

zu 2.: Fallunterscheidung über d (orientiert sich an $\mathcal{R}_{F_2}$)

Fall $d = \varnothing$**:** $\psi_{2,i+1}(d) = \varnothing = \mathcal{R}_{F_2}[\![\psi_{1,i}, \psi_{2,i}]\!](d)$

Fall $d = 0$**:** $\psi_{2,i+1}(d) = \varnothing = \psi_{2,i}(d) = \mathcal{R}_{F_2}[\![\psi_{1,i}, \psi_{2,i}]\!](d)$

Fall $d = 1$**:** $\psi_{2,i+1}(d) = 0 = \mathcal{R}_{F_2}[\![\psi_{1,i}, \psi_{2,i}]\!](d)$

Fall sonst ($d = succ^x(0)$ **mit** $x > 1$)**:** Fallunterscheidung über x in Abhängigkeit von $i + 1$:

Fall $x < 2(i + 1) - 2$**:** $(\Leftrightarrow x < 2i)$

$\Rightarrow \psi_{2,i+1}(d) = succ^{\lfloor \log_2 x \rfloor}(0)$

$$\begin{array}{cll} & \mathcal{R}_{F_2}[\![\psi_{1,i}, \psi_{2,i}]\!](d) & \\ = & \delta_{succ}(\psi_{2,i}(\psi_{1,i}(succ^x(0)))) & \text{da } x < 2i \\ = & \delta_{succ}(\psi_{2,i}(succ^{\lfloor \frac{x}{2} \rfloor}(0))) & \text{da } 1 \leq \lfloor \frac{x}{2} \rfloor < i \leq 2i + 2 (\text{da } i \geq 2) \\ = & \delta_{succ}(succ^{\lfloor \log_2 \lfloor \frac{x}{2} \rfloor \rfloor}(0)) & \\ = & succ^{\lfloor \log_2 \lfloor \frac{x}{2} \rfloor \rfloor + 1}(0)) & \end{array}$$

wir müssen nun zeigen: $\lfloor \log_2 x \rfloor = \lfloor \log_2 \frac{x}{2} + 1$

Fall x gerade: $\lfloor \log_2 \lfloor \frac{x}{2} \rfloor \rfloor + 1 = \lfloor \log_2 \frac{x}{2} \rfloor + 1 = \lfloor \log_2 x - \log_2 2 \rfloor + 1 = \lfloor \log_2 x \rfloor - 1 + 1 = \lfloor \log_2 x \rfloor$

Fall x ungerade: $\lfloor \log_2 \lfloor \frac{x}{2} \rfloor \rfloor + 1 = \lfloor \log_2 (x-1) - \log_2 2 \rfloor + 1 = \lfloor \log_2 (x-1) \rfloor = \lfloor \log_2 x \rfloor$

$\Rightarrow$ insgesamt $\lfloor \log_2 x \rfloor = \lfloor \log_2 \lfloor \frac{x}{2} \rfloor \rfloor + 1$

Fall $x \geq 2(i + 1) - 2$**:** $\Rightarrow x \geq 2i$

$\psi_{2,i+1}(d) = \varnothing$

$\mathcal{R}_{F_2}[\![\psi_{1,i}, \psi_{2,i}]\!](d) = \delta_{succ}(\psi_{2,i}(\psi_{1,i}(succ^x(0)))) = \delta_{succ}(\psi_{2,i}(\varnothing)) = \varnothing$

Daraus ergibt sich folgende Vermutung für die Fixpunkte:

$$\psi_1(d) = \begin{cases} \varnothing, & \text{falls } x = \varnothing \\ \lfloor \frac{x}{2} \rfloor, & \text{sonst} \end{cases} \qquad \psi_2(d) = \begin{cases} \varnothing, & \text{falls } x \in \{\varnothing, 0\} \\ \lfloor \log_2 x \rfloor, & \text{sonst} \end{cases}$$

Zu zeigen:

(a) $\psi_1 = sup\langle \psi_{1,i} \rangle_{i \in \mathbb{N}}$

(b) $\psi_2 = sup\langle \psi_{2,i} \rangle_{i \in \mathbb{N}}$

(a) Beweis von $\forall i \in \mathbb{N}.\, \psi_{1,i} \sqsubseteq \psi_1$ durch Fallunterscheidung über d:

$d = \varnothing$

$$\psi_{1,i}(d) = \varnothing = \psi_1(d)$$

$d = succ^x(0)$ **und** $x < 2i$

$$\psi_{1,i}(d) = succ^{\lfloor \frac{x}{2} \rfloor}(0) = \psi_1(d)$$

$d = succ^x(0)$ **und** $x \geq 2i$

$$\psi_{1,i}(d) = \varnothing \sqsubseteq \psi_1(d)$$

Sei $\overline{\psi_1}$ eine obere Schranke von $\langle \psi_{1,i} \rangle_{i \in \mathbb{N}}$. Zu zeigen: $\psi_1 \sqsubseteq \overline{\psi_1}$. Für $d = succ^x(0)$ gilt offensichtlich $\psi_{1,x}(d) = \psi_1(d)$ und somit $\psi_1(d) \sqsubseteq \overline{\psi_1}(d)$. Im Fall $d = \varnothing$ gilt $\psi_1(d) = \varnothing \sqsubseteq \overline{\psi_1}$. Also ist ψ_1 die kleinste obere Schranke.

(b) Beweis von $\forall i \in \mathbb{N}.\, \psi_{2,i} \sqsubseteq \psi_2$: Für $i = 0$ gilt $\psi_{2,0}(d) = \varnothing \sqsubseteq \psi_2(d)$. Für $i > 0$ zeigen wir die Behauptung durch Fallunterscheidung über d:

$d =\in \{\varnothing, 0\}$

$$\psi_{2,i}(d) = \varnothing = \psi_2(d)$$

$d = 1$

$$\psi_{2,i}(d) = 0 = \psi_2(d)$$

$d = succ^x(0)$ **und** $1 \leq x < 2i - 2$

$$\psi_{2,i}(d) = succ^{\lfloor \log_2 x \rfloor}(0) = \psi_2(d)$$

$d = succ^x(0)$ **und** $x \geq 2i - 2$

$$\psi_{2,i}(d) = \varnothing \sqsubseteq \psi_2(d)$$

Sei $\overline{\psi_2}$ eine obere Schranke von $\langle \psi_{2,i} \rangle_{i \in \mathbb{N}}$. Zu zeigen: $\psi_2 \sqsubseteq \overline{\psi_2}$. Für $d = succ^x(0)$ mit $x \geq 1$ gilt offensichtlich $\psi_{2,x+1}(d) = \psi_2(d)$ und somit $\psi_2(d) \sqsubseteq \overline{\psi_2}(d)$. Im Fall $d =\in \{\varnothing, 0\}$ gilt $\psi_2(d) = \varnothing \sqsubseteq \overline{\psi_2}$. Also ist ψ_2 die kleinste obere Schranke.

Hausaufgabe 4.3 (Aussagen in D_P) (4 Punkte)

Sei $P = \langle$ **function** $double(x : nat) : nat \Leftarrow$
$if_{nat}(eq_{nat}(x, 0), 0, succ(succ(double(pred(x))))),$

function $half(x : nat) : nat \Leftarrow$
$if_{nat}(eq_{nat}(x, 0),$
$0,$
$if_{nat}(eq_{nat}(x, succ(0)), 0, succ(half(pred(pred(x)))))) \rangle.$

Zeigen Sie die folgenden Aussagen:

(a) $D_P \models [\forall n : nat.n \equiv half(double(n))]$,

(b) $D_P \not\models [\forall n : nat.eq_{nat}(n, half(double(n))) \equiv true]$,

(c) $D_P \not\models [\exists n : nat.eq_{nat}(n, half(double(n))) \equiv false]$.

Hinweis: Sie können die zum Beweis notwendigen Deutungen der Funktionssymbole $half$ und $double$ ohne Fixpunktiteration oder Lösung der Fixpunktgleichung direkt angeben (vgl. Übung 2.3.14).

Lösungsvorschlag:

Es gilt

$$\delta_{double}(n) = \begin{cases} \varnothing & n = \varnothing \\ succ^{2x}(0) & n = succ^x(0) \end{cases} \qquad \delta_{half}(n) = \begin{cases} \varnothing & n = \varnothing \\ succ^{\lfloor \frac{x}{2} \rfloor}(0) & n = succ^x(0) \end{cases}$$

(a)

$$\begin{aligned} & D_P \models [\forall n : nat.n \equiv half(double(n))] \\ \Leftrightarrow & \forall a \in D_{nat}.\ a = D_P[n/a](half(double(n))) \\ \Leftrightarrow & \forall a \in D_{nat}.\ a = \delta_{half}(\delta_{double}(a)) \end{aligned}$$

$a = \varnothing_{nat}$

$$\delta_{half}(\delta_{double}(\varnothing_{nat})) = \delta_{half}(\varnothing_{nat}) = \varnothing_{nat}$$

$a = succ^x(0)$

$$\delta_{half}(\delta_{double}(succ^x(0))) = \delta_{half}(succ^{2x}(0)) = succ^x(0)$$

(b)

$$\begin{aligned} & D_P \not\models [\forall n : nat.eq_{nat}(n, half(double(n))) \equiv true] \\ \Leftrightarrow & \exists x \in D_{nat}.\ \delta_{eq}(x, \delta_{half}(\delta_{double}(x))) \neq true \end{aligned}$$

Sei $x = \varnothing_{nat}$, dann ist $\delta_{eq}(\varnothing_{nat}, \delta_{half}(\delta_{double}(\varnothing_{nat}))) = \varnothing_{bool} \neq true$.

(c)

$$\begin{aligned} & D_P \not\models [\exists n : nat.eq_{nat}(n, half(double(n))) \equiv false] \\ \Leftrightarrow & D_P \models [\forall n : nat.eq_{nat}(n, half(double(n))) \not\equiv false] \Leftrightarrow \quad \forall a \in D_{nat}.\ \delta_{eq_{nat}}(a, \delta_{half}(\delta_{double}(a))) \neq false \end{aligned}$$

$a = \varnothing_{nat}$

$$\delta_{eq_{nat}}(\varnothing_{nat}, \delta_{half}(\delta_{double}(\varnothing_{nat}))) = \varnothing_{bool} \neq false$$

$a = succ^x(0)$

$$\delta_{eq_{nat}}(succ^x(0), \delta_{half}(\delta_{double}(succ^x(0)))) = true \neq false$$

Hausaufgabe 4.4 (Länge von eval_P und $\mathsf{cbv\text{-}eval}_P$ Auswertung) **(2 Punkte)**

Sei P ein beliebiges funktionales Programm. Beweisen oder widerlegen Sie folgende Aussagen:

(a) Für alle $t \in \mathcal{T}(\Sigma(P))$ gilt: $|t|_P \geq \|t\|_P$.

Lösungsvorschlag:

Sei $t = f(0, pred(0))$, und `function f(x, y : nat) : nat <= if(x=0, 0, y)`,
dann ist $|t|_P = 3 \not\geq 4 = \|t\|_P$

(b) Für alle $t \in \mathcal{T}(\Sigma(P))$ gilt: $\|t\|_P \geq |t|_P$.

Lösungsvorschlag:

Sei $t = f(pred(0))$, und `function f(x : nat) : nat <= if(x=0, x, 0)`,
dann ist $\|t\|_P = 4 \not\geq 5 = |t|_P$