Semantik und Programmverifikation

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

Hausaufgabe mit Lösungsvorschlag 3

Hausaufgabe 3.1 (Unterschied zwischen $\equiv$ und eq_{nat}) **(8 × 0.5 = 4 Punkte)**

Zeigen Sie die folgenden Aussagen:

(a) $D_{\mathrm{BM}} \models [\forall n : nat\ n \equiv n]$

Lösungsvorschlag:

$$\begin{array}{ll} & D_{BM} \models [\forall n : nat.n \equiv n] \\ \Leftrightarrow & \forall \bar{n} \in D_{nat}.D_{BM}[n/\bar{n}] \models n \equiv n \\ \Leftrightarrow & \forall \bar{n} \in D_{nat}.\bar{n} = \bar{n}\surd \\ \Rightarrow & \text{also ist auch die ursprüngliche Aussage wahr} \end{array}$$

(b) $D_{\mathrm{BM}} \not\models [\forall n : nat\ eq_{\mathrm{nat}}(n, n) \equiv true]$

Lösungsvorschlag:

$$\begin{array}{lll} \text{Annahme:} & D_{BM} \models [\forall n : nat.eq(n, n) \equiv true] \\ & \Leftrightarrow & \forall \bar{n} \in D_{nat}.D_{BM}[n/\bar{n}] \models eq(n, n) = true \\ & \Leftrightarrow & \forall \bar{n} \in D_{nat}.\delta_{BM,eq}(\bar{n}, \bar{n}) = true \end{array}$$

Für $\bar{n} = \varnothing_{nat}$ gilt aber: $\delta_{BM,eq}(\bar{n}, \bar{n}) = \varnothing_{bool} \neq true.$ $\Rightarrow$ Aussage ist falsch $\Rightarrow$ $D_{BM} \not\models [\forall n : nat.eq(n, n) \equiv true]$

(c) $D_{\mathrm{BM}} \models [\forall n : nat\ n \equiv 0 \vee n \equiv succ(pred(n))]$

Lösungsvorschlag:

$\Leftrightarrow \forall \bar{n} \in D_{nat}.\bar{n} = 0$ oder $\bar{n} = \delta_{succ}(\delta_{pred}(\bar{n}))$

Fall $\bar{n} = \varnothing_{nat}$**:** $\Rightarrow \delta_{succ}(\delta_{pred}(\bar{n})) = \delta_{succ}(\varnothing_{nat}) = \varnothing_{nat}\surd$

Fall $\bar{n} = 0$**:** Behauptung trivialerweise erfüllt

Fall $\bar{n} = succ^n(0), n > 1$**:** $\Rightarrow \delta_{succ}(\delta_{pred}(succ^n(0))) = \delta_{succ}(succ^{n-1}(0)) = succ^n(0)\surd$

$\Rightarrow$ Behauptung insgesamt wahr

(d) $D_{\mathrm{BM}} \not\models [\forall n : nat\ eq_{\mathrm{nat}}(n, 0) \equiv true \vee eq_{\mathrm{nat}}(n, succ(pred(n))) \equiv true]$

Lösungsvorschlag:

$$\begin{array}{ll} \text{Annahme} & D_{BM} \models \forall n : nat.eq_{nat}(n, 0) \equiv true \vee eq_{nat}(n, succ(pred(n))) = true \\ \Leftrightarrow & \forall \bar{n} \in D_{nat}.\delta_{eq,nat}(\bar{n}, 0) = true \text{ oder } \delta_{eq,nat}(\bar{n}, \delta_{succ}(\delta_{pred}(\bar{n}))) = true \\ \text{aber} & \bar{n} = \varnothing_{nat} \Rightarrow \delta_{eq,nat}(\bar{n}, 0) = \varnothing_{bool}, \delta_{eq,nat}(\bar{n}, \delta_{succ}(\delta_{pred}(\bar{n}))) = \varnothing_{bool} \\ \Rightarrow & \text{Annahme falsch} \\ \Rightarrow & D_{BM} \not\models \forall n : nat.eq_{nat}(n, 0) \equiv true \vee eq_{nat}(n, succ(pred(n))) = true \end{array}$$

(e) $D_{\mathrm{BM}} \models [\forall n, m : nat\ eq_{\mathrm{nat}}(n, m) \equiv true \rightarrow n \equiv m]$

Lösungsvorschlag:

$$\begin{array}{ll} \Leftrightarrow & \forall \bar{m}, \bar{n} \in D_{nat} D_{BM}[n/\bar{n}, m/\bar{m}] \models eq_{nat}(n,m) \equiv true \rightarrow n \equiv m \\ \Leftrightarrow & \forall \bar{m}, \bar{n} \in D_{nat} D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv true \wedge \neg n \equiv m) \end{array}$$

Fall $\bar{n} = \varnothing_{nat}$ **oder** $\bar{m} = \varnothing_{nat}$**:**

$$\begin{array}{ll} \Rightarrow & \delta_{eq}(\bar{n}, \bar{m}) = \varnothing_{bool} \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n,m) \equiv true \wedge \neg n \equiv m \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv true \wedge \neg n \equiv m) \end{array}$$

Fall $\bar{n} \neq \varnothing_{nat}$ **und** $\bar{m} \neq \varnothing_{nat}$**:**

Fall $\bar{n} = \bar{m}$**:**

$$\begin{array}{ll} \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models \neg n \equiv m \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n,m) = true \wedge \neg n \equiv m \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) = true \wedge \neg n \equiv m) \end{array}$$

Fall $\bar{n} \neq \bar{m}$**:**

$$\begin{array}{ll} \Rightarrow & \delta_{eq_{nat}}(\bar{n}, \bar{m}) = false \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n,m) \equiv true \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv true \wedge \neg n \equiv m) \end{array}$$

(f) $D_{\mathrm{BM}} \models [\forall n, m : nat\ eq_{\mathrm{nat}}(n,m) \equiv false \rightarrow \neg n \equiv m]$

Lösungsvorschlag:

$$\begin{array}{ll} \Leftrightarrow & \forall \bar{m}, \bar{n} \in D_{nat} D_{BM}[n/\bar{n}, m/\bar{m}] \models eq_{nat}(n,m) \equiv false \rightarrow \neg n \equiv m \\ \Leftrightarrow & \forall \bar{m}, \bar{n} \in D_{nat} D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv false \wedge \neg\neg n \equiv m) \end{array}$$

Fall $\bar{n} = \varnothing_{nat}$ **oder** $\bar{m} = \varnothing_{nat}$**:**

$$\begin{array}{ll} \Rightarrow & \delta_{eq}(\bar{n}, \bar{m}) \neq false \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n,m) \equiv false \wedge \neg\neg n \equiv m \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv false \wedge \neg\neg n \equiv m) \end{array}$$

Fall $\bar{n} \neq \varnothing_{nat}$ **und** $\bar{m} \neq \varnothing_{nat}$**:**

Fall $\bar{n} = \bar{m}$**:**

$$\begin{array}{ll} \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq(n,m) \equiv false \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n,m) \equiv false \wedge \neg\neg n \equiv m \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv false \wedge \neg\neg n \equiv m) \end{array}$$

Fall $\bar{n} \neq \bar{m}$**:**

$$\begin{array}{ll} \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models n \equiv m \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \models \neg(eq_{nat}(n,m) \equiv false \wedge \neg\neg n \equiv m) \end{array}$$

(g) $D_{\mathrm{BM}} \models [\forall n, m : nat\ eq_{\mathrm{nat}}(n,m) \equiv true \rightarrow \neg eq_{\mathrm{nat}}(n,m) \equiv false]$

Lösungsvorschlag:

$$\Leftrightarrow \quad \forall \bar{m}, \bar{n} \in D_{nat} D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n,m) \equiv true \wedge \neg\neg eq_{nat}(n,m) \equiv false$$

Fall $\bar{n} = \varnothing_{nat}$ oder $\bar{m} = \varnothing_{nat}$:

$$\begin{array}{ll} \Rightarrow & \delta_{eq}(\bar{n}, \bar{m}) = \varnothing_{bool} \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n, m) \equiv true \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n, m) \equiv true \wedge \neg\neg eq_{nat}(n, m) \equiv false \end{array}$$

Fall $\bar{n} \neq \varnothing_{nat}$ und $\bar{m} \neq \varnothing_{nat}$:

Fall $\bar{n} = \bar{m}$:

$$\begin{array}{ll} \Rightarrow & \delta_{eq}(\bar{n}, \bar{m}) = true \neq false \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models \neg\neg eq_{nat}(n, m) \equiv false \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n, m) = true \wedge \neg\neg eq_{nat}(n, m) = false \end{array}$$

Fall $\bar{n} \neq \bar{m}$:

$$\begin{array}{ll} \Rightarrow & \delta_{eq_{nat}}(\bar{n}, \bar{m}) = false \neq true \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n, m) \equiv true \\ \Rightarrow & D_{BM}[n/\bar{n}, m/\bar{m}] \not\models eq_{nat}(n, m) = true \wedge \neg\neg eq_{nat}(n, m) = false \end{array}$$

(h) Diskutieren Sie nun unter Berücksichtigung der Ergebnisse aus den vorangegangenen Teilaufgaben den Unterschied zwischen eq_{nat} und $\equiv$.

Lösungsvorschlag:

$\equiv$ entspricht der Identität, das heisst, es wird überprüft, ob die Objekte links und rechts identisch sind.

eq wird in D_{BM} als Identität auf $D_{nat} \setminus \{\varnothing_{nat}\}$ interpretiert, stellt somit sozusagen eine strikte Version von $\equiv$ dar. Man beachte aber, dass eq in einer anderen Σ-Algebra anders definiert sein kann!

Hausaufgabe 3.2 (Monotonie, ω-Totalität) **(1 + 4 + 1 = 6 Punkte)**

(a) Gegeben sei die Funktion $\phi_{\text{eq}} : \mathcal{D}_{\text{nat}} \times \mathcal{D}_{\text{nat}} \to \mathcal{D}_{\text{bool}}$ mit $\phi_{\text{eq}}(d, e) = true$, falls $d = e$ und $\phi_{\text{eq}}(d, e) = false$, falls $d \neq e$. Beweisen oder widerlegen Sie, daß ϕ_{eq} monoton ist.

Lösungsvorschlag:

ϕ_{eq} ist nicht monoton, weil $(\varnothing_{nat}, \varnothing_{nat}) \sqsubseteq (\varnothing_{nat}, 0)$, aber $\phi_{eq}(\varnothing_{nat}, \varnothing_{nat}) = true \not\sqsubseteq false = \phi_{eq}(\varnothing_{nat}, 0)$,

(b) Zeigen Sie, daß die Σ(BM)–Algebra D_{BM} monoton ist.

Hinweis: Verwenden Sie die Aussagen aus der Präsenzübung, Aufgabe 4.1.

Lösungsvorschlag:

$\delta_{BM,0}, \delta_{BM,true}, \delta_{BM,false}$**:** monoton, da nach Aufgabe 4.1.(a) alle Konstanten monoton sind.

$\delta_{BM,succ}, \delta_{BM,pred}$**:** da $\delta_{BM,succ}(\varnothing_{nat}) = \varnothing_{nat}$ und $\delta_{BM,pred}(\varnothing_{nat}) = \varnothing_{nat}$, folgt mit Aufgabe 4.1.(b) ihre Monotonie.

$\delta_{BM,eq}$**:** da $\delta_{BM,eq}(e, \varnothing_{nat}) = \varnothing_{bool}$ und $\delta_{BM,eq}(\varnothing_{nat}, e) = \varnothing_{bool}$, folgt mit Aufgabe 4.1.(e) ihre Monotonie.

$\delta_{BM,if}$: da $\delta_{BM,if}(\varnothing_{bool}, e_2, e_3) = \varnothing_{bool}$, $\delta_{BM,if}(true, e_2, e_3) = e_2$, $\delta_{BM,if}(false, e_2, e_3) = e_3$ folgt mit Aufgabe 4.1.(e)

$e_1 = \varnothing$: $\delta_{BM,if}(e_1, e_2, e_3) = \varnothing_{bool}$,

$e_2 = \varnothing$: $\delta_{BM,if}(e_1, e_2, e_3) = \varnothing_{bool}$ oder $\delta_{BM,if}(e_1, e_2, e_3) = \delta_{BM,if}(e_1, \varnothing_{nat}, e_3)$

$e_3 = \varnothing$: $\delta_{BM,if}(e_1, e_2, e_3) = \varnothing_{bool}$ oder $\delta_{BM,if}(e_1, e_2, e_3) = \delta_{BM,if}(e_1, e_2, \varnothing_{nat})$

$\Longrightarrow$ insgesamt ist D_{BM} monoton.

(c) Bestimmen Sie alle ω–totalen Funktionen von D_{BM}.

Lösungsvorschlag:

alle Funktionen sind ω total.

Hausaufgabe 3.3 (Supremum einer Iterationenfolge) **(2 Punkte)**

Gegeben sei die Halbordnung $(\mathbb{N} \cup \{\bot\}, \sqsubseteq)$ mit $n \sqsubseteq m$ gdw. $n = m$ oder $n = \bot$. Ferner sei $\langle \phi_i \rangle_{i \in \mathbb{N}}$ eine Funktionenfolge mit $\phi_i \in \{\mathbb{N} \to \mathbb{N} \cup \{\bot\}\}$ und

$$\phi_i(n) := \begin{cases} n!, & \text{falls } n < i, \\ \bot, & \text{sonst.} \end{cases}$$

Beweisen Sie, dass $\sup_i \langle \phi_i \rangle = n!$ gilt.

Lösungsvorschlag:

Zeige: $n!$ ist obere Schranke: zu zeigen: $\forall n, i \in \mathbb{N}. \phi_i(n) \sqsubseteq n!$

Fall $n < i$: $\Rightarrow \phi_i(n) = n! \Rightarrow \phi_i(n) \sqsubseteq n!$

Fall $i \leq n$: $\Rightarrow \phi_i(n) = \bot \Rightarrow \phi_i(n) \sqsubseteq n!$

Wegen Vollständigkeit der Fallunterscheidung $\Rightarrow \forall i \in \mathbb{N}. \phi_i \sqsubseteq \phi$, ϕ ist also obere Schranke.

Zeige: $n!$ ist kleinste obere Schranke: Sei $\bar{\phi}$ eine beliebige obere Schranke von $\langle \phi_i \rangle_{i \in \mathbb{N}}$. $\Rightarrow \forall i, n \in \mathbb{N}. \phi_i(n) \sqsubseteq \bar{\phi}(n) \Rightarrow \forall n \in \mathbb{N}. \phi_{n+1}(n) \sqsubseteq \bar{\phi}(n) \Rightarrow \forall n \in \mathbb{N}. n! \sqsubseteq \bar{\phi}(n)$ also ist ϕ *kleinste* obere Schranke.

Hausaufgabe 3.4 (Ketten und Suprema) **(1 Punkt)**

Seien $(E_1, \sqsubseteq_{E_1})$ eine Halbordnung, $(E_2, \sqsubseteq_{E_2})$ eine vollständige Halbordnung und $\phi \in [E_1 \to E_2]$. Zeigen Sie, dass für jede $\sqsubseteq_{E_1}$-Kette $\langle e_i \rangle_{i \in \mathbb{N}}$ in E_1 $\sup_i \langle \phi(e_i) \rangle$ existiert (vgl. Übung 2.3.7).

Lösungsvorschlag:

	Sei $\langle e_i \rangle_{i \in \mathbb{N}}$ eine Kette in E_1	
$\Rightarrow$	$\forall i \in \mathbb{N}. e_i \sqsubseteq_{E_1} e_{i+1}$	ϕ monoton
$\Rightarrow$	$\forall i \in \mathbb{N}. \phi(e_i) \sqsubseteq_{E_1} \phi(e_{i+1})$	
$\Rightarrow$	$\langle \phi(e_i) \rangle_{i \in \mathbb{N}}$ ist Kette in E_2	$(E_2, \sqsubset_{E_2})$vollständig
$\Rightarrow$	$\sup_i \langle \phi_i \rangle$ existiert.	