Semantik und Programmverifikation

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

Übungsblatt mit Lösungsvorschlag 1

Aufgabe 1.1 (Terme)

Sei $\mathcal{S} = \{s1, s2\}$ und sei Σ eine $\mathcal{S}$-sortierte Signatur mit

$$\begin{array}{rcl}
\Sigma^{\mathrm{c}}_{\lambda,s1} & = & \{a\}, \\
\Sigma^{\mathrm{c}}_{\lambda,s2} & = & \{b\}, \\
\Sigma^{\mathrm{c}}_{s1,s1} & = & \{f\}, \\
\Sigma^{\mathrm{c}}_{s1\,s2,s2} & = & \{g\}, \\
\Sigma^{\mathrm{d}}_{s1\,s2,s1} & = & \{h\}.
\end{array}$$

Weiter seien $\{x, z\} \subset \mathcal{V}_{s1}$ und $y \in \mathcal{V}_{s2}$.

(a) Bilden Sie alle Terme aus $\mathcal{T}(\Sigma, \{x, y, z\})$, die höchstens zwei Funktionssymbole enthalten.

Lösungsvorschlag:

0 Symbole: x, y, z

1 Symbol: $a, b, f(x), f(z), g(x, y), g(z, y), h(x, y), h(z, y)$

2 Symbole: $f(a), f(f(x)), f(f(z)), f(h(x, y)), f(h(z, y)),$
$g(a, y), g(f(x), y), g(f(z), y)g(h(x, y), y), g(h(z, y), y),$
$g(x, b), g(x, g(x, y)), g(x, g(z, y)),$
$g(z, b), g(z, g(x, y)), g(z, g(z, y)),$
$h(a, y), h(f(x), y), h(f(z), y), h(h(x, y), y), h(h(z, y), y),$
$h(x, b), h(x, g(x, y)), h(x, g(z, y)),$
$h(z, b), h(z, g(x, y)), h(z, g(z, y))$

(b) Welche dieser Terme sind Konstruktorgrundterme?

Lösungsvorschlag:

$a, b, f(a)$

(c) Wenden Sie die Substitution $\{x/f(x), y/b\}$ auf die Terme aus (a) an. Welche der nun entstandenen Terme sind Konstruktorgrundterme?

Lösungsvorschlag:

$a, b, f(a), g(a, b)$

(d) Sei t der Term $h(f(x), g(f(x), y))$. Geben Sie die Menge Occ(t) seiner Stellen an. Für welche Stellen π_1, π_2 gilt $t|_{\pi_1} \leq_{\mathcal{T}} t|_{\pi_2}$?
Bilden Sie die Terme $t_1 = t[1\,1 \leftarrow a]$ und $t_2 = t[1 \leftarrow f(x)]\,[2\,1 \leftarrow f(a)]\,[1\,1 \leftarrow a]$. Gibt es Substitutionen σ_1, σ_2, so daß $t_1 = \sigma_1(t)$ oder $t_2 = \sigma_2(t)$ gilt?

Lösungsvorschlag:

$$\begin{aligned} \mathrm{Occ(t)} &= \{\epsilon, 1, 11, 2, 21, 211, 22\} \\ t_1 &= h(f(a), g(f(x), y)) \\ t_2 &= h(f(a), g(f(a), y)) \\ \sigma_2 &= \{x/a\} \end{aligned}$$

$\pi_1 \backslash \pi_2$	ϵ	1	11	2	21	211	22
ϵ	$=$						
1	$<$	$=$		$<$	$=$		
11	$<$	$<$	$=$	$<$	$<$	$=$	
2	$<$			$=$			
21	$<$	$=$		$<$	$=$		
211	$<$	$<$	$=$	$<$	$<$	$=$	
22	$<$			$<$			$=$

Aufgabe 1.2 (Substitutionen)

Seien $\mathcal{S}$, Σ und $\mathcal{V}$ wie in Aufgabe 1.1 gegeben.
Welche der nachfolgenden Abbildungen sind Substitutionen? Begründen Sie jeweils ihre Antwort.

(a) $\sigma_1 := \{x/f(x), y/b\}$

Lösungsvorschlag:

Dies ist eine Substitution gemäß Definition 1.1.6.

(b) $\sigma_2 := \{x/g(a, b), y/g(a, b), z/f(x)\}$

Lösungsvorschlag:

Dies ist keine Substitution, da die Abbildung nicht sortenerhaltend ist: $x \in \mathcal{V}_{s1}$ aber $g \in \Sigma_{s1s2,s2}$

(c) $\sigma_3 := \{f^i(x)/f^{i+1}(x) \mid i \in \mathbb{N}\}$ mit $f^0(x) = x$ und $f^{i+1}(x) = f(f^i(x))$

Lösungsvorschlag:

Hier liegt keine Substitution vor, da es sich nicht um eine Abbildung von $\mathcal{V}$ nach $\mathcal{T}(\Sigma, \mathcal{V})$ handelt.

(d) $\sigma_4 := \{x/f(h(x, b)), y/b, z/h(f(x), g(a, y))\}$

Lösungsvorschlag:

Dies ist eine Substitution gemäß Definition 1.1.6.

(e) $\sigma_5 := \{x/f(h(x, a)), y/a, z/h(f(x), g(b, y))\}$

Lösungsvorschlag:

Dies ist keine Substitution:

- $f(h(x, a))$ ist kein wohldefinierter Term ($a \in \Sigma_{\lambda,s1}$, $h \in \Sigma_{s1s2,s1}$)
- nicht sortenerhaltend: $y \in \mathcal{V}_{s2}$ aber $a \in \Sigma_{\lambda,s1}$
- $h(f(x), g(b, y))$ ist kein wohldefinierter Term ($b \in \Sigma_{\lambda,s2}$, $g \in \Sigma_{s1s2,s2}$

Aufgabe 1.3 (Modell)

Sei $\mathcal{S} = \{s1, s2\}$ und sei Σ eine $\mathcal{S}$–sortierte Signatur mit

$$\begin{aligned}\Sigma^{c}_{\lambda,s1} &= \{a\},\\ \Sigma^{c}_{\lambda,s2} &= \{b\},\\ \Sigma^{c}_{s1,s1} &= \{f\},\\ \Sigma^{c}_{s1\,s1,s1} &= \{g\},\\ \Sigma^{d}_{s1\,s2,s1} &= \{h\}.\end{aligned}$$

Weiter seien $\{x, y\} \subset \mathcal{V}_{s1}$ und $z \in \mathcal{V}_{s2}$.

Betrachten Sie nun die folgende Formelmenge:

$$\begin{aligned}\Phi \quad = \quad \{&\forall x : s1\ \forall y : s1\ \ h(g(x, y), b) \equiv g(y, x),\\ &\forall z : s2\ \ g(a, h(a, z)) \equiv f(f(a))\}.\end{aligned}$$

Geben Sie eine Σ–Algebra an, die Modell von Φ ist.

Lösungsvorschlag:

$$\mathcal{A}_{s1} = \{\Box\}, \mathcal{A}_{s2} = \{\diamond\}, \alpha_a = \Box, \alpha_b = \diamond, \alpha_f(\Box) = \Box, \alpha_g(\Box, \Box) = \Box, \alpha_h(\Box, \diamond) = \Box$$

Aufgabe 1.4 (Fundierte Mengen)

Beweisen Sie die folgenden Behauptungen. Verwenden Sie für (a) und (b) Satz 1.3.2 aus der Vorlesung. Hierbei seien $>_{\mathbb{N}}$ und $>_{\mathbb{Q}^+}$ die üblichen grösser-als-Relationen auf $\mathbb{N}$ bzw. $\mathbb{Q}^+$.

(a) Sei $n <_{\mathbb{N}} m$ gdw. $m >_{\mathbb{N}} n$. Dann ist $(\mathbb{N}, <_{\mathbb{N}})$ keine fundierte Menge.

Lösungsvorschlag:

Angenommen, $(\mathbb{N}, <_{\mathbb{N}})$ sei fundiert, dann gibt es ein $<$-minimales Element m von $\mathbb{N}$. Aber $m < m+1$, also kann m nicht minimal sein. Daher ist $(\mathbb{N}, <_{\mathbb{N}})$ nicht fundiert.

(b) $(\mathbb{Q}^+, >_{\mathbb{Q}^+})$ ist keine fundierte Menge.

Lösungsvorschlag:

Angenommen, $(\mathbb{Q}^+, >_{\mathbb{Q}^+})$ sei fundiert, dann gibt es ein $>_{\mathbb{Q}^+}$-minimales Element q von $\mathbb{Q}^+$. Aber $q >_{\mathbb{Q}^+} \frac{q}{2}$, also kann q nicht minimal sein. Daher ist $(\mathbb{Q}^+, >_{\mathbb{Q}^+})$ nicht fundiert.

(c) Für alle $\epsilon \in \mathbb{Q}^+$ mit $\epsilon >_{\mathbb{Q}^+} 0$ ist $(\mathbb{Q}^+, >_\epsilon)$ mit $q >_\epsilon r$ gdw. $(q - r) >_{\mathbb{Q}^+} \epsilon$ eine fundierte Menge.

Lösungsvorschlag:

Man zeigt leicht als Lemma durch Induktion über n: für alle $n \in \mathbb{N}, q_0, \ldots, q_n \in \mathbb{Q}^+$ mit $q_0 >_\epsilon \ldots >_\epsilon q_n$ gilt, dass $q_0 - q_n > n \cdot \epsilon$

Wir nehmen an, $(\mathbb{Q}, >_\epsilon)$ sei nicht fundiert und führen dies zum Widerspruch. Nach Annahme existiert eine Folge $< q_i >_{i \in \mathbb{N}}$ mit $q_i >_\epsilon q_{i+1}$ für alle $i \in \mathbb{N}$. Mit $q_0 >_\epsilon \ldots >_\epsilon q_n$ und dem Lemma folgt $q_0 - q_n > n \cdot \epsilon$. Wir wählen $n := \lceil \frac{q_0}{\epsilon} \rceil$. Einsetzen von n und Auflösen nach q_n ergibt $\underbrace{q_0 - \lceil \frac{q_0}{\epsilon} \rceil \cdot \epsilon}_{<0} > q_n$. $\Rightarrow 0 > q_n$, im Widerspruch zu $q_n \in \mathbb{Q}^+$. Die Annahme war also falsch, $(\mathbb{Q}, >_\epsilon)$ ist also fundiert.