Semantik und Programmverifikation

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

Hausaufgabe mit Lösungsvorschlag 1

Hausaufgabe 1.1 (Folgerungsrelation) **(1 + 1 + 1 = 3 Punkte)**

Seien φ und ψ beliebige Formeln über Σ und $\mathcal{V}$. φ besitze die freie Variable $x \in \mathcal{V}_s$. Beweisen oder widerlegen Sie die folgenden Aussagen:

(a) $\{\forall x : s\ \varphi\} \models \varphi$,

Lösungsvorschlag:

zu zeigen: $\{\forall x : s.\varphi\} \models \varphi$.

Sei $I = (\mathcal{A}, a)$ eine beliebige Σ-Interpretation mit $I \models \{\forall x : s.\varphi\}$

$$I \models \forall x : s.\varphi \Rightarrow I[x/\bar{a}] \models \varphi \text{ für alle } \bar{a} \in \mathcal{A}_s.$$

Da $a(x) \in \mathcal{A}_s$ folgt insbesondere $I[x/a(x)] \models \varphi$. Mit $I = I[x/a(x)]$ folgt $I \models \varphi$. Insgesamt also: $\{\forall x : s.\varphi\} \models \varphi$.

(b) $\{\varphi\} \models \forall x : s\ \varphi$,

Lösungsvorschlag:

Wir konstruieren ein Gegenmodell I und zeigen so, dass $\{\varphi\} \not\models \forall x : s\ \varphi$.

Wir wählen $\mathcal{S} = \{s\}, \Sigma = \emptyset, \mathcal{A}_s = \{\square, *\}, a(x) = *, a(y) = *, I = (\mathcal{A}, a), \varphi = x \equiv y$. Dann gilt zwar $a(x) = a(y)$ und somit $I \models x \equiv y$. Aber $I \not\models \forall x : s.x \equiv y$, denn $I[x/\square] \not\models x \equiv y$. Die Behauptung ist also falsch.

(c) $\{\varphi\} \models \psi$ gdw. $\emptyset \models \varphi \rightarrow \psi$ (*Deduktionstheorem*)

Lösungsvorschlag:

$\emptyset \models \varphi \rightarrow \psi$
$\Leftrightarrow$ für jede Interpretation I gilt: $I \models \varphi \rightarrow \psi$
$\Leftrightarrow$ für jede Interpretation I gilt: $I \models \neg\varphi \vee \psi$
$\Leftrightarrow$ für jede Interpretation I gilt: $I \models \neg(\varphi \wedge \neg\psi)$
$\Leftrightarrow$ für jede Interpretation I gilt: $I \not\models \varphi \wedge \neg\psi$
$\Leftrightarrow$ es keine Interpretation I gibt, so dass $I \models \varphi \wedge \neg\psi$
$\Leftrightarrow$ es keine Interpretation I gibt, so dass $I \models \varphi$ und $I \models \neg\psi$
$\Leftrightarrow$ für jede Interpretation I mit $I \models \varphi$ gilt: $I \not\models \neg\psi$)
$\Leftrightarrow$ für jede Interpretation I mit $I \models \varphi$ gilt: $I \models \neg\neg\psi$)
$\Leftrightarrow$ für jede Interpretation I mit $I \models \varphi$ gilt: $I \models \psi$)
$\Leftrightarrow \{\varphi\} \models \psi$

Hausaufgabe 1.2 (Theorien) (1 + 1 + 1 = 3 Punkte)

Zeigen Sie, daß für jede Σ-Algebra A gilt:

(a) $\mathrm{Th}(A) \neq \emptyset$,

Lösungsvorschlag:

Für jede Σ-Algebra A gilt $A \models \text{TRUE} \Rightarrow \text{TRUE} \in \mathrm{Th}(A) \Rightarrow \mathrm{Th}(A) \neq \emptyset$.

(b) $\forall \varphi \in \mathrm{Th}(A).\ \neg\varphi \notin \mathrm{Th}(A)$, d.h. $\mathrm{Th}(A)$ ist *konsistent*,

Lösungsvorschlag:

zu zeigen: für alle $\varphi \in \mathrm{Th}(A)$: $\neg\varphi \notin \mathrm{Th}(A)$.

Sei $\varphi \in \mathrm{Th}(A)$ beliebig. $\Rightarrow A \models \varphi \Rightarrow A \not\models \neg\varphi \Rightarrow \neg\varphi \notin \mathrm{Th}(A)$

(c) $\forall \varphi \in \mathcal{F}_g(\Sigma, \mathcal{V}).\ \varphi \in \mathrm{Th}(A) \vee \neg\varphi \in \mathrm{Th}(A)$, d.h. $\mathrm{Th}(A)$ ist *vollständig*.

Lösungsvorschlag:

zu zeigen: für alle $\varphi \in \mathcal{F}_g(\Sigma, \mathcal{V})$: $\varphi \in \mathrm{Th}(A)$ oder $\neg\varphi \in \mathrm{Th}(A)$.

Seien A eine beliebige Σ-Algebra und $\varphi \in \mathcal{F}_g(\Sigma, \mathcal{V})$ eine beliebige geschlossene Formel.

Fall $A \models \varphi$: $\Rightarrow \varphi \in \mathrm{Th}(A) \Rightarrow \varphi \in \mathrm{Th}(A)$ oder $\neg\varphi \in \mathrm{Th}(A)$.

Fall $A \not\models \varphi$: $\Rightarrow A \models \neg\varphi \Rightarrow \neg\varphi \in \mathrm{Th}(A) \Rightarrow \varphi \in \mathrm{Th}(A)$ oder $\neg\varphi \in \mathrm{Th}(A)$.

Hausaufgabe 1.3 (Termerzeugte Algebren, Substitutionslemma) (3 + 1 = 4 Punkte)

Eine Algebra $A = (\mathcal{A}, \alpha)$ heisst *termerzeugt*, falls es für jedes $\mathbf{a} \in \mathcal{A}$ einen Grundterm $t \in \mathcal{T}(\Sigma)$ gibt, so dass $A(t) = \mathbf{a}$ gilt.

(a) Beweisen Sie, daß für beliebige Σ–Interpretationen (A, a), (B, b) die folgende Aussage gilt, falls A und B termerzeugt sind:

$$\begin{aligned} &[\forall \psi \in \mathcal{A}t(\Sigma, \mathcal{V}).\ ((A, a) \models \psi \Leftrightarrow (B, b) \models \psi)] \\ \Longleftrightarrow\ &[\forall \varphi \in \mathcal{F}(\Sigma, \mathcal{V}).\ ((A, a) \models \varphi \Leftrightarrow (B, b) \models \varphi)] \end{aligned}$$

Hinweis: Verwenden Sie das Substitutionslemma 1.2.1.(ii) für Formeln.

Lösungsvorschlag:

„$\Longrightarrow$“ Wir ziehen die Quantifizierung über φ nach aussen, damit eine Induktion über φ möglich wird. Zu zeigen also:

$$\forall \varphi \in \mathcal{F}(\Sigma, \mathcal{V}) : \underbrace{(\underbrace{\forall \psi \in \mathrm{At}(\Sigma, \mathcal{V})(A, a) \models \psi \Leftrightarrow (B, b) \models \psi}_{\text{Hyp}}) \Rightarrow ((A, a) \models \varphi \Leftrightarrow (B, b) \models \varphi)}_{P(\varphi)}$$

Wir zeigen dies durch Induktion über φ, wobei wir als fundierte Relation *nicht* die Teilformelrelation, sondern $>_{|.|}$ verwenden, das wie folgt definiert wird:

$\varphi >_{|\cdot|} \psi :\Leftrightarrow |\varphi| > |\psi|$ mit

$$|\cdot| : \varphi \mapsto \begin{cases} 1 & \text{falls } \varphi = \text{TRUE}, \\ 1 & \text{falls } \varphi = t_1 \equiv t_2 \text{ mit } t_1, t_2 \in \mathcal{T}(\Sigma, \mathcal{V}), \\ 1 + |\varphi_1| & \text{falls } \varphi = \neg\varphi_1 \text{ mit } \varphi_1 \in \mathcal{F}(\Sigma, \mathcal{V}), \\ 1 + |\varphi_1| + |\varphi_2| & \text{falls } \varphi = \varphi_1 \wedge \varphi_2 \text{ mit } \varphi_1, \varphi_2 \in \mathcal{F}(\Sigma, \mathcal{V}), \\ 1 + |\varphi_1| & \text{falls } \varphi = \forall x : s.\varphi_1 \text{ mit } \varphi_1 \in \mathcal{F}(\Sigma, \mathcal{V}), s \in \mathcal{S}, x \in \mathcal{V} \end{cases}$$

$|\cdot|$ zählt die Anzahl der Junktoren und Quantoren in einer Formel. $(\mathcal{F}(\Sigma, \mathcal{V}), |\cdot|)$ ist nach Satz 1.4.1.(ii) fundiert und wir können über dieser fundierten Menge induzieren. Man beachte, dass wir bei der rekursiven Definition von $|\cdot|$ stillschweigend die Fundiertheit von $>_{\mathcal{F}}$ verwenden, die man in Analogie zu Hausaufgabe 2.2.(b) separat zeigen müßte.

Strukturelle Induktion über die Teilformelrelation $>_{\mathcal{F}}$ würde im Quantor-Schrittfall Probleme bereiten, wie wir sehen werden.

Basisfall φ ist $>_{|\cdot|}$ minimal

$\Rightarrow \varphi$ ist atomar. Mit der Annahme Hyp folgt direkt die Behauptung.

Schrittfall $(\forall \chi \in \mathcal{F}(\Sigma, \mathcal{V}).\varphi >_{|\cdot|} \chi \Rightarrow P(\chi)) \Rightarrow P(\varphi)$**:**

Fall $\varphi = \neg\varphi_1$ mit $\varphi_1 \in \mathcal{F}(\Sigma, \mathcal{V})$:

Da $|\varphi| = |\neg\varphi_1| = 1 + |\varphi_1| > |\varphi|$ ist die Induktionshypothese $P(\varphi_1)$ anwendbar, und mit Annahme Hyp folgt:
$(A, a) \models \varphi_1 \Leftrightarrow (B, b) \models \varphi_1$ (*).
Zu zeigen bleibt $(A, a) \models \neg\varphi_1 \Leftrightarrow (B, b) \models \neg\varphi_1$:

$$\begin{array}{lcll} & (A,a) & \models & \neg\varphi_1 \quad \text{Def 1.2.2.(iii)} \\ \Leftrightarrow & (A,a) & \not\models & \varphi_1 \quad (*) \\ \Leftrightarrow & (B,b) & \not\models & \varphi_1 \quad \text{Def 1.2.2.(iii)} \\ \Leftrightarrow & (B,b) & \models & \neg\varphi_1 \end{array}$$

Fall $\varphi = \varphi_1 \wedge \varphi_2$ mit $\varphi_1, \varphi_2 \in \mathcal{F}(\Sigma, \mathcal{V})$:

Da $|\varphi| = 1 + |\varphi_1| + |\varphi_2|$ gilt: $|\varphi| > |\varphi_1|$ und $|\varphi| > |\varphi_2|$ und die Induktionshypothesen $P(\varphi_1)$ und $P(\varphi_2)$ sind anwendbar. Mit Annahme Hyp folgen:

$$\begin{array}{l} (1.)(A, a) \models \varphi_1 \Leftrightarrow (B, b) \models \varphi_1 \\ (2.)(A, a) \models \varphi_2 \Leftrightarrow (B, b) \models \varphi_2 \end{array}$$

Zu zeigen bleibt: $(A, a) \models \varphi_1 \wedge \varphi_2 \Leftrightarrow (B, b) \models \varphi_1 \wedge \varphi_2$:

$$\begin{array}{lll} & (A, a) \models \varphi_1 \wedge \varphi_2 & \text{Def 1.2.2.(iv)} \\ \Leftrightarrow & (A, a) \models \varphi_1 \text{ und } (A, a) \models \varphi_2 & (1.) \\ \Leftrightarrow & (B, b) \models \varphi_1 \text{ und } (A, a) \models \varphi_2 & (2.) \\ \Leftrightarrow & (B, b) \models \varphi_1 \text{ und } (B, b) \models \varphi_2 & \text{Def 1.2.2.(iv)} \\ \Leftrightarrow & (B, b) \models \varphi_1 \wedge \varphi_2 & \end{array}$$

Fall $\varphi = \forall x : s.\varphi_1$ mit $\varphi_1 \in \mathcal{F}(\Sigma, \mathcal{V})$:

Vorüberlegung: durch strukturelle Induktion über t zeigt man leicht, dass für alle $t \in \mathcal{T}(\Sigma, \mathcal{V})_s$ $\forall x : s.\varphi_1 >_{|\cdot|} \varphi_1[x/t]$. Die Induktionshypothese $P(\varphi_1[x/t])$ ist also anwendbar und mit Annahme Hyp folgt

$$\forall t \in \mathcal{T}(\Sigma, \mathcal{V})_s.(A, a) \models \varphi_1[x/t] \Leftrightarrow (B, b) \models \varphi_1[x/t] \quad (*).$$

Anmerkung: weil eben nicht für beliebige $t \in \mathcal{T}(\Sigma, \mathcal{V})_s$ $\forall x : s.\varphi_1 >_{\mathcal{T}} \varphi_1[x/t]$ gilt, funktioniert eine strukturelle Induktion über die Teilformelrelation für den Gesamtbeweis nicht.

Zu zeigen bleibt $(A,a) \models \forall x : s.\varphi_1 \Leftrightarrow (B,b) \models \forall x : s.\varphi_1$:

$$
\begin{array}{lrll}
 & & (A,a) \models \forall x : s.\varphi_1 & \text{Def 1.2.2.(v)} \\
\Leftrightarrow & \forall \bar{a} \in \mathcal{A}_s. & (A, a[x/\bar{a}]) \models \varphi_1 & A \text{ termerzeugt} \\
\Leftrightarrow & \forall t \in \mathcal{T}(\Sigma)_s. & (A, a[x/a(t)]) \models \varphi_1 & \text{Substitutionslemma 1.2.1.(i)} \\
\Leftrightarrow & \forall t \in \mathcal{T}(\Sigma)_s. & (A,a) \models \varphi_1[x/t] & (*) \\
\Leftrightarrow & \forall t \in \mathcal{T}(\Sigma)_s. & (B,b) \models \varphi_1[x/t] & \text{Substitutionslemma 1.2.1.(i)} \\
\Leftrightarrow & \forall t \in \mathcal{T}(\Sigma)_s. & (B, b[x/b(t)]) \models \varphi_1 & B \text{ termerzeugt} \\
\Leftrightarrow & \forall \bar{b} \in \mathcal{B}_s. & (B, b[x/\bar{b}]) \models \varphi_1 & \text{Def 1.2.2.(v)} \\
\Leftrightarrow & & (B,b) \models \forall x : s.\varphi_1 &
\end{array}
$$

„$\Longleftarrow$“ ist trivial, da $\mathrm{At}(\Sigma,\mathcal{V}) \subseteq \mathcal{F}(\Sigma,\mathcal{V})$.

(b) Gilt die Aussage von Teil (a) auch, falls A oder B nicht termerzeugt sind?

Lösungsvorschlag:

Zwar haben wir im Quantorfall die Voraussetzung der Termerzeugtheit von A und B verwendet, daraus allein folgt aber noch nicht, dass es nicht auch ohne gehen könnte.

Wir konstruieren ein Gegenbeispiel und zeigen, dass die Aussage nicht mehr gilt, wenn A oder B nicht termerzeugt ist. Sei $\mathcal{S} = \{s\}$, $A = ((\mathcal{A}_s)_{s\in\mathcal{S}}, \alpha)$, $B = ((\mathcal{B}_s)_{s\in\mathcal{S}}, \beta)$, $\Sigma_{\lambda,s} = \{c\}$, $\mathcal{A}_s = \{\square\}$, $\mathcal{B}_s = \{\square, *\}$, $\alpha_c = \square$, $\beta_c = \square$ ($\Rightarrow B$ nicht termerzeugt, denn kein Term erzeugt $*$).

Neben TRUE sind in $\mathrm{At}(\Sigma,\mathcal{V})$ nur Formeln $y \equiv z$ mit $y, z \in \mathcal{V}_s$ enthalten.

Mit $a(x) = b(x) = \square$ für alle $x \in \mathcal{V}_s$ gilt zwar sowohl $(A,a) \models \psi$ als auch $(B,b) \models \psi$ für alle $\psi \in \mathrm{At}(\Sigma,\mathcal{V})$, aber $(A,a) \models \forall x : s\, x \equiv y$ und $(B,b) \not\models \forall x : s\, x \equiv y$, denn $(B, b[x/*]) \not\models x \equiv y$.

Hausaufgabe 1.4 (fundierte Mengen) **(1 + 3 + 1 = 5 Punkte)**

Beweisen Sie die folgenden Behauptungen. Verwenden Sie dabei Satz 1.4.1 aus der Vorlesung. Sie können dazu $(\mathbb{N}, >_{\mathbb{N}})$ als fundiert voraussetzen.

(a) Seien $(M, >_M)$ und $(N, >_N)$ fundierte Mengen, seien $f : K \to M$ und $g : K \to N$ Abbildungen und sei $>_K \subset K \times K$ definiert durch:

$$k_1 >_K k_2 \text{ gdw. } f(k_1) >_M f(k_2) \text{ oder } (f(k_1) = f(k_2) \text{ und } g(k_1) >_N g(k_2)).$$

Dann ist $(K, >_K)$ eine fundierte Menge (vgl. Lemma 1.4.3.(i))

Lösungsvorschlag:

Voraussetzung: $(M, >_M), (N, >_N)$ sind fundierte Mengen. Mit Satz 1.4.1.(iii) ist $(M \times N, >_{M\times N})$ mit $(m,n) >_{M\times N} (m',n')$ gdw $m >_M m'$ oder ($m = m'$ und $n >_N n'$) ebenfalls fundierte Menge.

Zu zeigen: $(K, >_K)$ ist eine fundierte Menge.

Wir definieren die Abbildung $F : K \to M \times N, k \mapsto (f(k), g(k))$. Mit Satz 1.4.1.(ii) folgt dann, dass die Relation $k \sqsubset_K k'$ gdw $F(k) >_{M\times N} F(k')$ ebenfalls fundiert ist. Man zeigt leicht $\sqsubset_K = >_K$. Also ist auch $>_K$ fundiert.

(b) $(\mathcal{T}(\Sigma,\mathcal{V}), >_{\mathcal{T}})$ ist eine fundierte Menge (vgl. Beispiel 1.3.1.(ii)).

Hinweis: Verwenden Sie **nicht** die Fundiertheit von $>_{|\cdot|}$.

Lösungsvorschlag:

Vorbemerkung: Es ist zwar sehr verlockend, die Fundiertheit von $>_{\mathcal{T}}$ mit Satz 1.4.1.(i) aus der Fundiertheit von $>_{|\cdot|}$ abzuleiten. Da wir uns aber bei der rekursiven Definition der Funktion $|\cdot|$ (siehe Hausaufgabe 1.4.(c)) bereits auf die Fundiertheit von $>_{\mathcal{T}}$ abgestützt hatten, würde unser Beweis dadurch zirkulär. Wir müssen also die Fundiertheit von $>_{\mathcal{T}}$ ohne einen derartigen Rückgriff zeigen.

(1.) Wir geben eine mengentheoretische Definition von $(\mathcal{T}(\Sigma,\mathcal{V}))_s$ an:

$$\begin{aligned}\mathcal{T}(\Sigma,\mathcal{V},0)_s &:= \mathcal{V}_s \cup \Sigma_{\lambda,s}\\ \mathcal{T}(\Sigma,\mathcal{V},n+1)_s &:= \{f(t_1,\ldots,t_m) | f \in \Sigma_{s_1\ldots s_m,s}, t_i \in \mathcal{T}(\Sigma,\mathcal{V},j)_{s_i}, 1 \leq i \leq m, 0 \leq j \leq n\}\\ \mathcal{T}(\Sigma,\mathcal{V})_s &:= \bigcup_{n=1}^{\infty} \mathcal{T}(\Sigma,\mathcal{V},n)_s\end{aligned}$$

(2.) Wir definieren die Funktion depth : $\mathcal{T}(\Sigma,\mathcal{V}) \to \mathbb{N}, t \mapsto \min\{n \mid\ t \in \mathcal{T}(\Sigma,\mathcal{V},n)\}$. Somit ist depth wohldefiniert, da $(\mathbb{N},>)$ fundiert ist.

Man beachte: eine rekursive Definition von depth über die Struktur von t würde wiederum die Fundiertheit von $>_{\mathcal{T}}$ voraussetzen, die wir ja erst beweisen wollen!

(3.) Wir definieren die Relation $>_{\text{depth}} \subseteq \mathcal{T}(\Sigma,\mathcal{V}) \times \mathcal{T}(\Sigma,\mathcal{V})$ mit $t >_{\text{depth}} r \Leftrightarrow \text{depth}(t) >_{\mathbb{N}} \text{depth}(r)$.
Wir definieren die direkte Teiltermrelation $>'_{\mathcal{T}} \subseteq \mathcal{T}(\Sigma,\mathcal{V}) \times \mathcal{T}(\Sigma,\mathcal{V})$ mit $t >'_{\mathcal{T}} r$ gdw $t = f(t_1,\ldots,t_n)$ und $r = t_i$ für $i \in \{1,\ldots,n\}$ mit $f \in \Sigma_{s_1\ldots s_m,s}, t_i \in \mathcal{T}(\Sigma,\mathcal{V})_{s_i}$ und zeigen mit Satz 1.4.1.(i) ihre Fundiertheit, indem wir $>'_{\mathcal{T}} \subseteq >_{\text{depth}}$ beweisen:
Seien $t, r \in \mathcal{T}(\Sigma,\mathcal{V})$ beliebig mit $t >'_{\mathcal{T}} r$. Dann ist $t = f(t_1,\ldots,t_k)$, $r = t_i$ für ein $i \in \{1,\ldots,k\}$. Sei $t \in \mathcal{T}(\Sigma,\mathcal{V},n)$ und $r \in \mathcal{T}(\Sigma,\mathcal{V},m)$. Wegen (1.) muss $m < n$ sein. Mit (2.) ist dann $\text{depth}(r) < \text{depth}(t)$ und mit (3.) folgt dann $t >_{\text{depth}} r$. Damit ist gezeigt, dass $>'_{\mathcal{T}} \subseteq >_{\text{depth}}$

(4.) Nach Definition von $>_{\mathcal{T}}$ gilt $>_{\mathcal{T}} = (>'_{\mathcal{T}})^+$. Da $>'_{\mathcal{T}}$ wie gesehen fundiert ist, folgt mit Lemma 1.3.1 die Fundiertheit von $>_{\mathcal{T}}$.

Anmerkung: Dieser Beweis führt die Fundiertheit von $>_{\mathcal{T}}$ auf die Fundiertheit von $>_{\mathbb{N}}$ zurück, die durch das fünfte Peano-Axiom garantiert wird.

(c) $(\mathcal{T}(\Sigma,\mathcal{V}), >_{||})$ ist eine fundierte Menge, wobei $t >_{||} q$ gdw. $|t| >_{\mathbb{N}} |q|$. Hierbei gibt $|t|$ die Anzahl der Symbole in t an (vgl. Beispiel 1.3.1.(iii)).

Hinweis: Geben Sie zunächst eine Definition für $|\cdot|$ an.

Lösungsvorschlag:

$$|\cdot| : \mathcal{T}(\Sigma,\mathcal{V}) \to \mathbb{N}, t \mapsto \begin{cases} 1 & \text{falls } t \in \mathcal{V},\\ 1 + \sum_{i=1}^{n} |t_i| & \text{falls } f \in \Sigma_{s_1\ldots s_n,s}, w \in S^*, s \in S, t_i \in \mathcal{T}(\Sigma,\mathcal{V}), 1 \leq i \leq n \end{cases}$$

Wegen der zuvor in Hausaufgabe 1.4.(b) nachgewiesenen Fundiertheit von $>_{\mathcal{T}}$ ist $|\cdot|$ wohldefiniert.
$(\mathbb{N},>_{\mathbb{N}})$ ist nach den Peano-Axiomen fundiert. Damit ist auch $(\mathcal{T}(\Sigma,\mathcal{V}), >_{|\cdot|})$ nach Satz 1.4.1.(ii) eine fundierte Menge.