Vollständigkeit und Korrektheit für die Prädikatenlogik

Satz (vgl. Folie 5.11)

Seien Γ eine Menge von Σ-Formeln und φ eine Σ-Formel. Dann gilt

$$\Gamma \vdash \varphi \iff \Gamma \models \varphi\,.$$

Insbesondere ist eine Σ-Formel genau dann allgemeingültig, wenn sie ein Theorem ist.

Beweis: Folgt unmittelbar aus Korrektheitssatz auf Folie 9.16 und Vollständigkeitssatz auf Folie 9.26. □

Folgerung 1: Kompaktheit

Satz (vgl. Folie 5.20 f.)

Seien Γ eine u.U. unendliche Menge von Σ-Formeln und φ eine Σ-Formel mit $\Gamma \models \varphi$. Dann existiert $\Gamma' \subseteq \Gamma$ endlich mit $\Gamma' \models \varphi$.

Beweis:

$\Gamma \models \varphi$

$\Longrightarrow \Gamma \vdash \varphi$ (nach dem Vollständigkeitssatz von Folie 9.26)

$\Longrightarrow$ es gibt Deduktion von φ mit Hypothesen $\gamma_1, \ldots, \gamma_n \in \Gamma$

$\Longrightarrow \Gamma' = \{\gamma_1, \ldots, \gamma_n\} \subseteq \Gamma$ endlich mit $\Gamma' \vdash \varphi$

$\Longrightarrow \Gamma' \models \varphi$ (nach dem Korrektheitssatz von Folie 9.16). $\square$

Folgerung (Kompaktheits- oder Endlichkeitssatz)

Sei Γ eine u.U. unendliche Menge von Σ-Formeln. Dann gilt

$$\Gamma \text{ erfüllbar} \iff \forall\, \Gamma' \subseteq \Gamma \text{ endlich: } \Gamma' \text{ erfüllbar}$$

Beweis:

Γ unerfüllbar

$\iff$ $\Gamma \cup \{\neg\bot\}$ unerfüllbar

$\iff$ $\Gamma \models \bot$ (vgl. Folie 5.7)

$\iff$ es gibt $\Gamma' \subseteq \Gamma$ endlich: $\Gamma' \models \bot$

$\iff$ es gibt $\Gamma' \subseteq \Gamma$ endlich: $\Gamma' \cup \{\neg\bot\}$ unerfüllbar (vgl. Folie 5.7)

$\iff$ es gibt $\Gamma' \subseteq \Gamma$ endlich: Γ' unerfüllbar $\square$

Beispiel

Sei Δ eine u.U. unendliche Menge von Σ-Formeln, so daß für jedes $n \in \mathbb{N}$ eine endliche Struktur $\mathcal{A}_n$ mit $\mathcal{A}_n \models \Delta$ existiert, die wenigstens n Elemente hat.

Dann existiert eine unendliche Struktur $\mathcal{A}$ mit $\mathcal{A} \models \Delta$.

Beweis: für $n \in \mathbb{N}$ setze

$$\begin{aligned} \varphi_{\geq n} &= \exists x_1 \exists x_2 \ldots \exists x_n \bigwedge\nolimits_{1 \leq i < j \leq n} x_i \neq x_j \text{ und} \\ \Gamma &= \Delta \cup \{\varphi_{\geq n} \mid n \geq 0\}. \end{aligned}$$

Sei $\Gamma' \subseteq \Gamma$ endlich. Dann existiert $n \in \mathbb{N}$ mit $\Gamma' \subseteq \Delta \cup \{\varphi_{\geq i} \mid 0 \leq i \leq n\}$.
$\Longrightarrow \mathcal{A}_n \models \Gamma'$, d.h. jede endliche Teilmenge von Γ ist erfüllbar.
$\xRightarrow{\text{Kompaktheitssatz}}$ es gibt Struktur $\mathcal{A}$ mit $\mathcal{A} \models \Gamma$
Ist $\mathcal{A}$ endlich, so existiert $m \in \mathbb{N}$ mit $\mathcal{A} \models \neg\varphi_{\geq m}$, im Widerspruch zu $\mathcal{A} \models \Gamma$ und $\varphi_{\geq m} \in \Gamma$.Also ist $\mathcal{A}$ unendlich. $\square$

Folgerung 2: Löwenheim-Skolem

Frage

Gibt es eine Menge Γ von Σ-Formeln, so daß für alle Strukturen $\mathcal{A}$ gilt:

$$\mathcal{A} \models \Gamma \iff \mathcal{A} \cong (\mathbb{R}, +, \cdot, 0, 1)\,?$$

Satz von Löwenheim-Skolem

Sei Γ erfüllbare und höchstens abzählbar unendliche Menge von Σ-Formeln.
Dann existiert ein höchstens abzählbar unendliches Modell von Γ.

Beweis:
Γ erfüllbar $\Longrightarrow \Gamma \not\models \bot$
$\Longrightarrow$ (Folie 9.16) $\Gamma \nvdash \bot$, d.h. Γ konsistent
$\Longrightarrow$ (Folie 9.27) Γ hat ein höchstens abzählbar unendliches Modell. $\square$

Die Frage auf der vorherigen Folie muß also verneint werden:

angenommen, Γ wäre eine solche Menge

$\xRightarrow{\Sigma \text{ endlich}} |\Gamma| \leq \aleph_0$

$\Longrightarrow$ (Folie 10.5) Γ hat ein höchstens abzählbar unendliches Modell $\mathcal{A}$

$\xRightarrow{|\mathbb{R}|>\aleph_0} \mathcal{A} \not\cong (\mathbb{R}, +, \cdot, 0, 1)$ $\square$

Folgerung 3: Semi-Entscheidbarkeit

Satz (vgl. Folie 5.12)

Die Menge der allgemeingültigen Σ-Formeln ist semi-entscheidbar.

Beweis: Sei φ Σ-Formel. Dann gilt

φ allgemeingültig

$\Longleftrightarrow$ φ Theorem

$\Longleftrightarrow$ Es gibt hypothesenlose Deduktion mit Konklusion φ

Ein Semi-Entscheidungsalgorithmus kann also folgendermaßen vorgehen:

Teste für jede Zeichenkette w nacheinander, ob sie hypothesenlose Deduktion mit Konklusion φ ist. Wenn ja, so gib aus „φ ist allgemeingültig“. Ansonsten gehe zur nächsten Zeichenkette über. □

Der Satz von Church

Jetzt zeigen wir, daß dieses Ergebnis nicht verbessert werden kann: Die Menge der allgemeingültigen Σ-Formeln ist nicht entscheidbar.

Wegen

$$\varphi \text{ allgemeingültig} \iff \neg\varphi \text{ nicht erfüllbar}$$

reicht es zu zeigen, daß die Menge der erfüllbaren Aussagen nicht entscheidbar ist.

Genauer zeigen wir dies sogar für „Horn-Formeln“:

Definition

Eine Horn-Formel ist eine Konjunktion von Σ-Formeln der Form

$$\forall x_1 \forall x_2 \ldots \forall x_n \left((\neg\bot \wedge \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_m) \to \beta \right),$$

wobei $\alpha_1, \ldots, \alpha_m$ atomare Σ-Formeln und β atomar Σ-Formel oder $\bot$ sind.

Unser Beweis reduziert die unentscheidbare Menge PCP auf die Menge der erfüllbaren Horn-Formeln.

Im folgenden sei also $I = \big((u_1, v_1), (u_2, v_2), \ldots, (u_k, v_k)\big)$ ein Korrespondenzsystem und A das zugrundeliegende Alphabet.

Hieraus berechnen wir eine Horn-Formel φ_I, die genau dann erfüllbar ist, wenn I keine Lösung hat.

Wir betrachten die Signatur $\Sigma = (\mathrm{Fun}, \mathrm{Rel}, \mathrm{ar})$ mit

- $\mathrm{Fun} = \{e\} \cup \{f_a \mid a \in A\}$ mit $\mathrm{ar}(e) = 0$ und $\mathrm{ar}(f_a) = 1$ für alle $a \in A$.
- $\mathrm{Rel} = \{R\}$ mit $\mathrm{ar}(R) = 2$.

Zur Abkürzung schreiben wir

$$f_{a_1 a_2 \ldots a_n}(x) \text{ für } f_{a_1}(f_{a_2}(\cdots(f_{a_n}(x))\cdots))$$

für alle $a_1, a_2, \ldots, a_n \in A$ und $n \geq 0$ (insbes. steht $f_\varepsilon(x)$ für x).

Wir betrachten die folgende Horn-Formel ψ_I:

$$\begin{aligned} & R(e,e) \\ \wedge \quad & \bigwedge_{1 \le j \le k} \forall x, y \left(R(x,y) \to R\big(f_{u_j}(x), f_{v_j}(y)\big) \right) \\ \wedge \quad & \bigwedge_{a \in A} \forall x \left(e = f_a(x) \to \bot \right) \end{aligned}$$

Beispiel

Betrachte die Σ-Struktur $\mathcal{A}$ mit Universum $U_{\mathcal{A}} = A^*$:

- $e^{\mathcal{A}} = \varepsilon$
- $f_a^{\mathcal{A}}(u) = au$
- $R^{\mathcal{A}} = \left\{ (u_{i_1} u_{i_2} \cdots u_{i_n}, v_{i_1} v_{i_2} \cdots v_{i_n}) \;\middle|\; n \ge 0, 1 \le i_1, i_2, \ldots, i_n \le k \right\}$

Für $u, v \in A^*$ gilt $f_u^{\mathcal{A}}(v) = uv$.

Dann gilt $\mathcal{A} \models \psi_I$.

Lemma

Angenommen, das Korrespondenzsystem I hat keine Lösung. Dann ist die Horn-Formel $\varphi_I = \psi_I \wedge \forall x \left(R(x,x) \to x = e\right)$ erfüllbar.

Beweis: Sei $\mathcal{A}$ die obige Struktur mit $\mathcal{A} \models \psi_I$.

Um $\mathcal{A} \models \forall x \left(R(x,x) \to x = e\right)$ zu zeigen, sei $w \in U_{\mathcal{A}}$ beliebig mit $(w,w) \in R^{\mathcal{A}}$.
Die Definition von $R^{\mathcal{A}}$ sichert die Existenz von $n \geq 0$ und $1 \leq i_1, i_2, \ldots, i_n \leq k$ mit

$$u_{i_1} u_{i_2} \ldots u_{i_n} = w = v_{i_1} v_{i_2} \ldots v_{i_n} .$$

Da I keine Lösung hat, folgt $n = 0$ und damit $w = \varepsilon$. □

Lemma

Sei $\mathcal{B}$ Struktur mit $\mathcal{B} \models \psi_I$. Dann gilt

$$(f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}}), f^{\mathcal{B}}_{v_{i_1} v_{i_2} \ldots v_{i_n}}(e^{\mathcal{B}})) \in R^{\mathcal{B}}$$

für alle $n \geq 0$, $1 \leq i_1, i_2, \ldots, i_n \leq k$.

Beweis: per Induktion über $n \geq 0$.

IA für $n = 0$ gelten

$$f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}}) = e^{\mathcal{B}} \text{ und } f^{\mathcal{B}}_{v_{i_1} v_{i_2} \ldots v_{i_n}}(e^{\mathcal{B}}) = e^{\mathcal{B}}$$

und damit

$$(f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}}), f^{\mathcal{B}}_{v_{i_1} v_{i_2} \ldots v_{i_n}}(e^{\mathcal{B}})) \in R^{\mathcal{B}}$$

wegen $\mathcal{B} \models \psi_I$.

IS Seien $n > 0$ und $1 \leq i_1, i_2, \ldots, i_n \leq k$.

Mit $u = u_{i_2} u_{i_3} \ldots u_{i_n}$ und $v = v_{i_2} v_{i_3} \ldots v_{i_n}$ gilt nach IV $\left(f_u^{\mathcal{B}}(e^{\mathcal{B}}), f_v^{\mathcal{B}}(e^{\mathcal{B}})\right) \in R^{\mathcal{B}}$.

Wegen $\mathcal{B} \models \psi_I$ folgt

$$\begin{aligned} R^{\mathcal{B}} &\ni \left(f_{u_{i_1}}^{\mathcal{B}}\left(f_u^{\mathcal{B}}(e^{\mathcal{B}})\right), f_{v_{i_1}}\left(f_v^{\mathcal{B}}(e^{\mathcal{B}})\right)\right) \\ &= \left(f_{u_{i_1} u_{i_2} \ldots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}), f_{v_{i_1} v_{i_2} \ldots v_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}})\right) \end{aligned}$$

womit der induktive Beweis abgeschlossen ist □

Lemma

Angenommen, $(i_1, \ldots, i_n)$ ist eine Lösung von I. Dann ist die Σ-Formel φ_I unerfüllbar.

Beweis: Sei $\mathcal{B}$ Σ-Struktur. Gilt $\mathcal{B} \not\models \psi_I$, so folgt $\mathcal{B} \not\models \varphi_I$. Gelte nun $\mathcal{B} \models \psi_I$. Dann folgt aus obigem Lemma

$$\left(f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}}), f^{\mathcal{B}}_{v_{i_1} v_{i_2} \ldots v_{i_n}}(e^{\mathcal{B}})\right) \in R^{\mathcal{B}} .$$

Da $(i_1, \ldots, i_n)$ Lösung von I ist, bedeutet dies

$$\left(f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}}), f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}})\right) \in R^{\mathcal{B}} .$$

Aus $n > 0$ und $\mathcal{B} \models \psi_I$ folgt

$$w := f^{\mathcal{B}}_{u_{i_1} u_{i_2} \ldots u_{i_n}}(e^{\mathcal{B}}) \neq e^{\mathcal{B}} .$$

Also haben wir $w \in U_{\mathcal{B}}$ gefunden mit $w \neq e^{\mathcal{B}}$ und $(w, w) \in R^{\mathcal{B}}$. Damit ist auch in diesem Fall $\mathcal{B} \not\models \varphi_I$ gezeigt. □

Satz

Die Menge der unerfüllbaren Horn-Formeln ist nicht entscheidbar.

Beweis: Die Abbildung $I \mapsto \varphi_I$ ist berechenbar.

Nach den Lemmata auf Folien 10.11 und 10.14 ist sie eine Reduktion von PCP auf die Menge der unerfüllbaren Horn-Formeln. Da PCP unentscheidbar ist (vgl. Automaten, Sprachen und Komplexität), ist die Menge der unerfüllbaren Horn-Formeln unentscheidbar. □

Folgerung (Church 1936)

Die Menge der allgemeingültigen Σ-Formeln ist nicht entscheidbar.

Beweis: Eine Σ-Formel φ ist genau dann unerfüllbar, wenn $\neg\varphi$ allgemeingültig ist. Also ist $\varphi \mapsto \neg\varphi$ eine Reduktion der unentscheidbaren Menge der unerfüllbaren Σ-Formeln auf die Menge der allgemeingültigen Σ-Formeln, die damit auch unentscheidbar ist. □

Allgemeingültige Σ-Formeln gelten in allen Strukturen. Was passiert, wenn wir uns nur auf „interessante“ Strukturen $\mathcal{A}$ einschränken (z.B. auf eine konkrete), d.h. wenn wir die Theorie $\mathrm{Th}(\mathcal{A})$ von $\mathcal{A}$ betrachten?

Theorie der natürlichen Zahlen

Definition

Sei $\mathcal{A}$ eine Σ-Struktur. Dann ist $\mathrm{Th}(\mathcal{A})$ die Menge der Aussagen φ mit $\mathcal{A} \models \varphi$. Diese Menge heißt die (elementare) Theorie von $\mathcal{A}$.

Beispiel

Sei $\mathcal{N} = (\mathbb{N}, \leq, +, \cdot, 0, 1)$. Dann gelten

- $(\forall x \forall y : x + y = y + x) \in \mathrm{Th}(\mathcal{N})$
- $(\forall x \exists y : x + y = 0) \notin \mathrm{Th}(\mathcal{N})$

aber $(\forall x \exists y : x + y = 0) \in \mathrm{Th}\big((\mathbb{Z}, +, 0)\big)$.

Satz (Turing und Church 1936)

Die Menge $\mathrm{Th}(\mathcal{N})$ aller Aussagen φ mit $\mathcal{N} \models \varphi$ ist nicht entscheidbar.

Beweis: Sei wieder $I = \big((u_1, v_1), \ldots, (u_k, v_k)\big)$ ein Korrespondenzsystem über dem Alphabet $A = \{1, 2, \ldots, |A|\}$. Sei $b = |A| + 1$. Für $w = a_\ell a_{\ell-1} \cdots a_0 \in A^*$ setzen wir

$$[w] = \sum_{0 \le i \le \ell} b^i a_i \,,$$

d.h., $[w]$ ist die von w zur Basis b dargestellte Zahl. Es gelten

- $[\varepsilon] = 0$,
- $[uv] = [u] \cdot b^{|v|} + [v]$ und
- $[.] \colon A^* \to \mathbb{N}$ ist injektiv, aber nicht surjektiv (da $0 \notin A$).

I hat eine Lösung
gdw.

$$\begin{aligned}\text{es gibt } n, i_1, i_2, \ldots, i_n \in \mathbb{N}: \quad & n > 0 \\ \& \quad & 1 \leq i_1, i_2, \ldots, i_n \leq k \\ \& \quad & u_{i_1} u_{i_2} \cdots u_{i_n} = v_{i_1} v_{i_2} \cdots v_{i_n}\end{aligned}$$

gdw.

$$\begin{aligned}&\text{es gibt } n \in \mathbb{N} \text{ und } U_0, V_0, \ldots, U_n, V_n \in A^*: \\ & \qquad n > 0 \\ & \& \quad U_0 = V_0 = \varepsilon \\ & \& \quad \text{für alle } i \in \{0, 1, \ldots, n-1\} \\ & \qquad \text{gelten } U_{i+1} = U_i u_j \ \& \ V_{i+1} = V_i v_j \text{ für ein } j \in \{1, \ldots, k\} \\ & \& \quad U_n = V_n\end{aligned}$$

gdw.

es gibt $n \in \mathbb{N}$ und $x_0, y_0, \ldots, x_n, y_n \in \mathbb{N}$:

$$
\begin{array}{ll}
 & n > 0 \\
\& & x_0 = y_0 = 0 \\
\& & \text{für alle } i \in \{0, 1, \ldots, n-1\} \\
 & \quad \text{gelten } x_{i+1} = x_i \cdot b^{|u_j|} + [u_j] \ \& \ y_{i+1} = y_i \cdot b^{|v_j|} + [v_j] \\
 & \quad\quad \text{für ein } j \in \{1, \ldots, k\} \\
\& & x_n = y_n
\end{array}
$$

Diese Aussage spricht nur über natürliche Zahlen. ☺
Sie ist aber keine Σ-Formel, da die Anzahl der x_i von der Variable n abhängt. ☹
Hier hilft das folgende Lemma:

Zahlentheoretisches Lemma

Für alle $n \in \mathbb{N}$, $x_0, x_1, \ldots, x_n \in \mathbb{N}$ existieren $c, d \in \mathbb{N}$, so daß für alle $0 \leq i \leq n$ gilt

$$x_i = c \bmod \big(1 + d \cdot (i+1)\big)\,.$$

Beweis: Setze $m = \max\{n, x_0, x_1, \ldots, x_n\}$ und $d = 2 \cdot 3 \cdot 4 \cdots (m+1)$. Dann sind die Zahlen

$$1 + d,\ 1 + d \cdot 2,\ 1 + d \cdot 3,\ \ldots,\ 1 + d \cdot (n+1)$$

paarweise teilerfremd. Nach dem Chinesischen Restsatz existiert eine natürliche Zahl c mit

$$x_i \equiv c \quad \Big(\mathrm{mod}\big(1 + d(i+1)\big)\Big) \text{ für alle } 0 \leq i \leq n\,.$$

Wegen $x_i \leq m < d < 1 + d(i+1)$ folgt

$$x_i = c \bmod \big(1 + d(i+1)\big) \text{ für alle } 0 \leq i \leq n\,. \quad \square$$

Bemerkung

Es gibt Σ-Formeln

- $\mathrm{mod}(x_1, x_2, y)$ mit $\mathcal{N} \models_\alpha \mathrm{mod} \iff \alpha(x_1) \bmod \alpha(x_2) = \alpha(y)$.
  z.B. $\mathrm{mod} = \exists k \left((x_1 = k \cdot x_2 + y) \wedge (y < x_2) \right)$

- $\gamma(x_1, x_2, x_3, y)$ mit
  $\mathcal{N} \models_\alpha \gamma \iff \alpha(x_1) \bmod \left(1 + \alpha(x_2) \cdot (\alpha(x_3) + 1)\right) = \alpha(y)$.
  z.B. $\gamma = \ldots$

Damit ist die Aussage von Folie 10.20 äquivalent zur Gültigkeit der folgenden Σ-Formel in der Struktur $\mathcal{N}$:

$$
\exists n, c, d, e, f:
\left(
\begin{array}{l}
\quad n > 0 \\
\wedge \gamma(c, d, 0, 0) \wedge \gamma(e, f, 0, 0) \\
\wedge \forall i: 0 \leq i < n \rightarrow \\
\qquad \exists x, x', y, y': \left[
\begin{array}{ll}
 & \gamma(c, d, i, x) \wedge \gamma(c, d, i+1, x') \\
\wedge & \gamma(e, f, i, y) \wedge \gamma(e, f, i+1, y') \\
\wedge & \displaystyle\bigvee_{1 \leq j \leq k} \left(
\begin{array}{ll}
 & x' = x \cdot b^{|u_j|} + [u_j] \\
\wedge & y' = y \cdot b^{|v_j|} + [v_j]
\end{array}
\right)
\end{array}
\right] \\
\wedge \exists z: \gamma(c, d, n, z) \wedge \gamma(e, f, n, z)
\end{array}
\right)
$$

Da diese Σ-Formel aus dem Korrespondenzsystem I berechnet werden kann, haben wir eine Reduktion von PCP auf die Theorie $\mathrm{Th}(\mathcal{N})$ von $\mathcal{N}$. Da PCP unentscheidbar ist, ist also auch diese Theorie unentscheidbar. $\square$

Bereits kleine Fragmente der Prädikatenlogik liefern unentscheidbare Probleme über $\mathcal{N} = (\mathbb{N}, \leq, +, \cdot, 0, 1)$. Ein besonders prominentes Beispiel ist Hilberts 10. Problem:

Satz (Matiyasevich 1970)

Das folgende Problem ist unentscheidbar:

EINGABE: Zwei multivariate Polynome $p(x_1, \ldots, x_n)$ und $q(x_1, \ldots, x_n)$ mit Koeffizienten aus $\mathbb{N}$.

FRAGE: Existieren $a_1, \ldots, a_n \in \mathbb{N}$ mit $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$?

Satz von Folie 10.18

Die Menge $\mathrm{Th}(\mathbb{N}, \leq, +, \cdot, 0, 1)$ ist nicht entscheidbar.

Satz

Entscheidbar sind hingegen:

1. $\mathrm{Th}(\mathbb{R}, \leq, +, \cdot, 0, 1)$ (Tarksi 1931).
2. $\mathrm{Th}(\mathbb{N}, \leq, +, 0, 1)$ (Presburger 1929).
3. $\mathrm{Th}(\mathbb{N}, \cdot, 0, 1)$ (Skolem 1931).
4. $\mathrm{Th}(\mathbb{R}, \mathbb{N}, \leq, +, 0, 1)$ (Weispfenning 1999).

Zusammenfassung 10. Vorlesung

in dieser Vorlesung neu

- Konsequenzen des Vollständigkeits- und Korrektheitssatzes (Kompaktheit, Löwenheim-Skolem, Semi-Entscheidbarkeit)
- zwei Unentscheidbarkeitsergebnisse

kommende Vorlesung

- 1. Gödelscher Unvollständigkeitssatz
- Gleichungsfreiheit