

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 9.14 und Vollständigkeitssatz auf Folie 9.24. □

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:

$\Gamma \models \varphi$

$\implies \Gamma \vdash \varphi$ (nach dem Vollständigkeitsatz von Folie 9.24)

\implies es gibt Deduktion von φ mit Hypothesen $\gamma_1, \dots, \gamma_n \in \Gamma$

$\implies \Gamma' = \{\gamma_1, \dots, \gamma_n\} \subseteq \Gamma$ endlich mit $\Gamma' \vdash \varphi$

$\implies \Gamma' \models \varphi$ (nach dem Korrektheitssatz von Folie 9.14). □

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

$$\iff \Gamma \cup \{\neg \perp\} \text{ unerfüllbar}$$

$$\iff \Gamma \models \perp \text{ (vgl. Folie 5.7)}$$

$$\iff \text{es gibt } \Gamma' \subseteq \Gamma \text{ endlich: } \Gamma' \models \perp$$

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

$$\iff \text{es gibt } \Gamma' \subseteq \Gamma \text{ endlich: } \Gamma' \text{ unerfüllbar}$$



Satz

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

$$\varphi_n = \exists x_1 \exists x_2 \dots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$$

und

$$\Gamma = \Delta \cup \{\varphi_n \mid n \geq 0\}.$$

Für $\Gamma' \subseteq \Gamma$ endlich existiert $n \in \mathbb{N}$ mit $\varphi_m \notin \Gamma'$ für alle $m \geq n$
 $\implies \mathcal{A}_n \models \Gamma'$, d.h. jede endliche Teilmenge von Γ ist erfüllbar.

Kompaktheitssatz
 \implies es gibt Struktur \mathcal{A} mit $\mathcal{A} \models \Gamma$

$\mathcal{A} \models \varphi_n$
 $\implies \mathcal{A}$ hat $\geq n$ Elemente (für alle $n \in \mathbb{N}$)

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 .



L. Löwenheim
(1878-1957)



T. Skolem
(1887-1963)

Beweis:

Γ erfüllbar $\implies \Gamma \not\vdash \perp$

\implies (Folie 9.14) $\Gamma \not\vdash \perp$, d.h. Γ konsistent

\implies (Folie 9.26) Γ hat ein höchstens abzählbar unendliches Modell. □

Die Frage auf der vorherigen Folie muß also verneint werden:

angenommen, Γ wäre eine solche Menge

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

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

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

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

$\iff \varphi$ Theorem

\iff 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

$$\varphi \text{ allgemeingültig} \iff \neg\varphi \text{ unerfüllbar}$$

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

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

Definition

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

$$\forall x_1 \forall x_2 \dots \forall x_n ((\neg\perp \wedge \alpha_1 \wedge \alpha_2 \wedge \dots \wedge \alpha_m) \rightarrow \beta),$$

wobei $\alpha_1, \dots, \alpha_m$ und β atomare Σ -Formeln sind.

[Beweis überspringen](#)

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

Im folgenden sei also $I = ((u_1, v_1), (u_2, v_2), \dots, (u_k, v_k))$ 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 $\Sigma = (\Omega, \text{Rel}, \text{ar})$ mit

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

Zur Abkürzung schreiben wir

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

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

Zunächst betrachten wir die folgende Horn-Formel ψ_I :

$$\begin{aligned} & R(e, e) \\ \wedge & \bigwedge_{1 \leq j \leq k} \forall x, y (R(x, y) \rightarrow R(f_{u_j}(x), f_{v_j}(y))) \\ \wedge & \bigwedge_{a \in A} \forall x (e = f_a(x) \rightarrow \perp) \end{aligned}$$

Beispiel

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

- $e^{\mathcal{A}} = \varepsilon$
- $f_a^{\mathcal{A}}(u) = au$
- $R^{\mathcal{A}} = \{(u_{i_1} u_{i_2} \dots u_{i_n}, v_{i_1} v_{i_2} \dots v_{i_n}) \mid n \geq 0, 1 \leq i_1, i_2, \dots, i_n \leq k\}$

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 $\varphi_I = \psi_I \wedge \forall x (R(x, x) \rightarrow x = e)$ erfüllbar.

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

Um $\mathcal{A} \models \forall x (R(x, x) \rightarrow x = e)$ 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 $1 \leq i_1, i_2, \dots, i_n \leq k$ mit

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

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

$$(f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}), f_{v_{i_1} v_{i_2} \dots v_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}})) \in R^{\mathcal{B}}$$

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

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

IA für $n = 0$ gelten

$$f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}) = e^{\mathcal{B}} \text{ und } f_{v_{i_1} v_{i_2} \dots v_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}) = e^{\mathcal{B}}$$

und damit

$$(f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}), f_{v_{i_1} v_{i_2} \dots v_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}})) \in R^{\mathcal{B}}$$

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

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

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

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

$$(f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}), f_{v_{i_1} v_{i_2} \dots v_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}})) = (f_{u_{i_1}}^{\mathcal{B}}(f_u^{\mathcal{B}}(e^{\mathcal{B}})), f_{v_{i_1}}^{\mathcal{B}}(f_v^{\mathcal{B}}(e^{\mathcal{B}}))) \in R^{\mathcal{B}}.$$



Lemma

Angenommen, (i_1, \dots, 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

$$(f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}), f_{v_{i_1} v_{i_2} \dots v_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}})) \in R^{\mathcal{B}}.$$

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

$$(f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}), f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}})) \in R^{\mathcal{B}}.$$

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

$$w := f_{u_{i_1} u_{i_2} \dots u_{i_n}}^{\mathcal{B}}(e^{\mathcal{B}}) \neq e^{\mathcal{B}}.$$

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.



(Alonzo Church,
1903-1995)

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 $\text{Th}(\mathcal{A})$ von \mathcal{A} betrachten?

Theorie der natürlichen Zahlen

Definition

Sei \mathcal{A} eine Struktur. Dann ist $\text{Th}(\mathcal{A})$ die Menge der prädikatenlogischen Σ -Formeln 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

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

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

Satz

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

[Beweis überspringen](#)

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

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

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

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

I hat eine Lösung
gdw.

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

gdw.

es gibt $n \in \mathbb{N}$ und $U_0, V_0, \dots, U_n, V_n \in A^*$:

$$\begin{aligned} & n > 0 \\ & \& \quad U_0 = V_0 = \varepsilon \\ & \& \quad \text{für alle } i \in \{0, 1, \dots, n-1\} \\ & \quad \quad \text{gelten } U_{i+1} = U_i u_j \ \& \ V_{i+1} = V_i v_j \text{ für ein } j \in \{1, \dots, k\} \\ & \& \quad U_n = V_n \end{aligned}$$

gdw.

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

$$n > 0$$

$$\& \quad x_0 = y_0 = 0$$

$\&$ für alle $i \in \{0, 1, \dots, n-1\}$

$$\text{gelten } x_{i+1} = x_i \cdot b^{|u_j|} + [u_j] \ \& \ y_{i+1} = y_i \cdot b^{|v_j|} + [v_j]$$

für ein $j \in \{1, \dots, k\}$

$$\& \quad x_n = y_n$$

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

$$x_i = c \pmod{(1 + d \cdot (i + 1))}.$$

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

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

paarweise teilerfremd. Nach dem Chinesischen Restsatz folgt die Existenz einer natürlichen Zahl c mit

$$x_i \equiv c \pmod{(1 + d(i + 1))} \text{ für alle } 0 \leq i \leq n.$$

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

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

Bemerkung

Es gibt Σ -Formeln

- $\text{mod}(x_1, x_2, y)$ mit $\mathcal{N} \models_{\alpha} \text{mod} \iff \alpha(x_1) \bmod \alpha(x_2) = \alpha(y)$.
z.B. $\text{mod} = \exists k((y < x_2) \wedge (x_1 = k \cdot x_2 + y))$
- $\gamma(x_1, x_2, x_3, y)$ mit
 $\mathcal{N} \models_{\alpha} \gamma \iff \alpha(x_1) \bmod (1 + \alpha(x_2) \cdot (\alpha(x_3) + 1)) = \alpha(y)$.
z.B. $\gamma = \dots$

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

$\exists n, c, d, e, f$:

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

Da diese Σ -Formel aus dem Korrespondenzsystem I berechnet werden kann, haben wir eine Reduktion von PCP auf die Theorie $\text{Th}(\mathcal{N})$ 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 Polynome $p(x_1, \dots, x_n)$ und $q(x_1, \dots, x_n)$ (in mehreren Variablen) mit Koeffizienten aus \mathbb{N} .

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



Y. Matiyasevich
(1947-)

Satz (Presburger 1929)

Die Menge $\text{Th}(\mathbb{N}, \leq, +, 0, 1)$ ist entscheidbar.
Dies ist die Menge der Aussagen φ mit $\mathcal{N} \models \varphi$,
die kein \cdot enthalten.

Beweis: Master-Vorlesung „Automatische
Strukturen“.

Satz (Skolem 1930)

Die Menge $\text{Th}(\mathbb{N}, \cdot, 0, 1)$ ist entscheidbar.
Dies ist die Menge der Aussagen φ mit $\mathcal{N} \models \varphi$,
die weder \leq noch $+$ enthalten.



M. Presburger
(1904-43?)



T. Skolem
(1887-1963)