Berechenbarkeit und Komplexität
10. Vorlesung

TECHNISCHE UNIVERSITÄT ILMENAU

Prof. Dr. Dietrich Kuske

welt offenes Thüringen

FG Automaten und Logik, TU Ilmenau

Sommersemester 2024

Satz

Die Menge der allgemeingültigen (prädikatenlogischen) Σ-Formeln ist semi-entscheidbar.

Beweis: Sei φ Σ-Formel. Dann gilt

φ allgemeingültig

$\iff$ φ Theorem (nach Korrektheits- und Vollständigkeitssatz, siehe Logik und Logikprogrammierung Folie 11.11)

$\iff$ 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. $\square$

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

$$\forall x_1 \, \forall x_2 \, \dots \, \forall x_n \Big((\neg\bot \wedge \alpha_1 \wedge \alpha_2 \wedge \cdots \wedge \alpha_m) \to \beta \Big),$$

wobei $\alpha_1, \dots, \alpha_m$ 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 $K = \big((u_1, v_1), (u_2, v_2), \ldots, (u_k, v_k)\big)$ ein Korrespondenzsystem und A das zugrundeliegende Alphabet.

Hieraus berechnen wir eine Horn-Formel φ_K, die genau dann erfüllbar ist, wenn K 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_K:

$$\begin{aligned} & R(e,e) \\ \wedge \quad & \bigwedge_{1\le i\le k} \forall x,y\Big(R(x,y) \to R\big(f_{u_i}(x), f_{v_i}(y)\big)\Big) \\ \wedge \quad & \bigwedge_{a\in A} \forall x\big(e = f_a(x) \to \bot\big) \end{aligned}$$

Beispiel

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

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

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

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

Lemma

Angenommen, das Korrespondenzsystem K hat keine Lösung. Dann ist die Horn-Formel $\varphi_K = \psi_K \wedge \forall x \big(R(x,x) \to x = e\big)$ erfüllbar.

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

Um $\mathcal{A} \models \forall x \big(R(x,x) \to x = e\big)$ 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 K keine Lösung hat, folgt $n = 0$ und damit $w = \varepsilon$. $\square$

Lemma

Sei $\mathcal{B}$ Struktur mit $\mathcal{B} \vDash \psi_K$. Für alle $n \geq 0$, $1 \leq i_1, i_2, \ldots, i_n \leq k$ gilt dann

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

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

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

wegen $\mathcal{B} \vDash \psi_K$.

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 $\mathcal{B} \models \psi_K$ 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 $\square$

Lemma

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

Beweis: Sei $\mathcal{B}$ Σ-Struktur. Gilt $\mathcal{B} \not\models \psi_K$, so folgt $\mathcal{B} \not\models \varphi_K$.
Gelte nun $\mathcal{B} \models \psi_K$. 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 K 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 $\mathcal{B} \models \psi_K$ 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 $\mathcal{B} \not\models \varphi_K$ gezeigt. □

Satz

Die Menge der unerfüllbaren Horn-Formeln ist nicht entscheidbar.

Beweis: Die Abbildung $K \mapsto \varphi_K$ ist berechenbar.

Nach den Lemmata auf Folien 10.6 und 10.9 ist sie eine Reduktion von PCP auf die Menge der unerfüllbaren Horn-Formeln. Da PCP unentscheidbar ist, ist die Menge der unerfüllbaren Horn-Formeln unentscheidbar. $\square$

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

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

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

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 $K = \big((u_1, v_1), \dots, (u_k, v_k)\big)$ ein Korrespondenzsystem über dem Alphabet $A = \big\{1, 2, \dots, |A|\big\}$. 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 $0 \notin A$).

K hat eine Lösung

gdw.

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

gdw.

es gibt $n \in \mathbb{N}$ und $X_0, Y_0, \ldots, X_n, Y_n \in A^*$:

$$\begin{array}{ll} & n > 0 \\ \& & X_0 = Y_0 = \varepsilon \\ \& & \text{für alle } j \in \{0, 1, \ldots, n-1\} \\ & \quad \text{gelten } X_{j+1} = X_j u_i \;\&\; Y_{j+1} = Y_j v_i \text{ für ein } i \in \{1, \ldots, k\} \\ \& & X_n = Y_n \end{array}$$

gdw.

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

$$
\begin{aligned}
& n > 0 \\
\& \quad & x_0 = y_0 = 0 \\
\& \quad & \text{für alle } j \in \{0, 1, \ldots, n-1\} \\
& & \quad \text{gelten } x_{j+1} = x_j \cdot b^{|u_i|} + [u_i] \;\&\; y_{j+1} = y_j \cdot b^{|v_i|} + [v_i] \\
& & \qquad \text{für ein } i \in \{1, \ldots, k\} \\
\& \quad & x_n = y_n
\end{aligned}
$$

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 $0 \le j \le n$ gilt

$$x_j = c \bmod \big(1 + d \cdot (j+1)\big) .$$

Beweis: Setze $m = \max\{n, x_0, x_1, \ldots, x_n\}$ und $d = (m+1)!$. 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

$$x_j \equiv c \pmod{\big(1 + d(j+1)\big)} \text{ für alle } 0 \le j \le n .$$

Wegen $x_j \le m < d < 1 + d(j+1)$ folgt

$$x_j = c \bmod \big(1 + d(j+1)\big) \text{ für alle } 0 \le j \le n . \quad \square$$

Bemerkung

Es gibt Σ-Formeln

- $\mathrm{mod}(z_1, z_2, z)$ mit $\mathcal{N} \models_\alpha \mathrm{mod} \iff \alpha(z_1) \bmod \alpha(z_2) = \alpha(z)$.
  z.B. $\mathrm{mod} = \exists k \big((z_1 = k \cdot z_2 + z) \land (z < z_2)\big)$
- ${\gamma}(z_1, z_2, z_3, z)$ mit
  $\mathcal{N} \models_\alpha \gamma \iff \underbrace{\alpha(z_1)}_{\hat{=} c} \bmod \big(1 + \underbrace{\alpha(z_2)}_{\hat{=} d} \cdot (\underbrace{\alpha(z_3)}_{\hat{=} j} + 1)\big) = \underbrace{\alpha(z)}_{\hat{=} x_j}$.
  z.B. $\gamma = \dots$

Damit ist die Aussage von Folie 10.15 äquivalent zur Gültigkeit der folgenden Σ-Formel in der Struktur $\mathcal{N}$:

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

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

Da diese Σ-Formel aus dem Korrespondenzsystem K 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 10.13

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

Satz

Entscheidbar sind hingegen:

1. $\mathrm{Th}(\mathbb{R}, \leq, +, \cdot, 0, 1)$ (Tarski 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).

Beispiele

1. Strukturen $\mathcal{A}$ mit entscheidbarer Theorie $\mathrm{Th}(\mathcal{A})$:
    - $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$
    - $(\mathbb{N}, +, V_k)$ mit $V_k \colon \mathbb{N} \to \mathbb{N} \colon n \mapsto \begin{cases} 0 & \text{falls } n = 0 \\ \max\{k^m \mid k^m \text{ teilt } n\} & \text{sonst} \end{cases}$
    - $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$
2. Strukturen $\mathcal{A}$, deren Theorie $\mathrm{Th}(\mathcal{A})$ unentscheidbar ist:
    - $(\mathbb{N}, +, \cdot)$, $(\mathbb{N}, +, |)$, $\big(\mathbb{N}, +, \{n^2 \mid n \in \mathbb{N}\}\big)$
    - $(\mathbb{N}, +, V_k, V_\ell)$, falls $i = j = 0$ aus $k^i = \ell^j$ folgt
    - $(\Sigma^*, \cdot)$ für $|\Sigma| \geq 2$

Wir zeigen jetzt, daß jede semi-entscheidbare Theorie sogar entscheidbar ist:

Satz

Sei $\mathcal{A}$ eine Struktur, so daß $\mathrm{Th}(\mathcal{A})$ semi-entscheidbar ist. Dann ist $\mathrm{Th}(\mathcal{A})$ entscheidbar.

Beweis:

Sei B das Komplement von $\mathrm{Th}(\mathcal{A})$, d.h.

$$\begin{aligned} \varphi \in B \quad &\iff \quad \mathcal{A} \not\models \varphi \\ &\iff \quad \mathcal{A} \models \neg\varphi \\ &\iff \quad \neg\varphi \in \mathrm{Th}(\mathcal{A}) \,. \end{aligned}$$

Die Abbildung $\varphi \mapsto \neg\varphi$ ist also eine Reduktion von B auf die semi-entscheidbare Menge $\mathrm{Th}(\mathcal{A})$. Also ist B semi-entscheidbar. Da also $\mathrm{Th}(\mathcal{A})$ und das Komplement B semi-entscheidbar sind, ist $\mathrm{Th}(\mathcal{A})$ nach dem Satz auf Folie 8.13 entscheidbar. $\square$

Korollar

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

Beweis:

Klar mit Sätzen auf Folien 10.13 und 10.22. $\square$

Korollar (1. Gödelscher Unvollständigkeitssatz)

Sei Γ eine semi-entscheidbare Menge von Sätzen mit $\mathcal{N} \models \gamma$ für alle $\gamma \in \Gamma$.

Dann existiert eine Aussage φ mit $\mathcal{N} \models \varphi$, $\Gamma \nvdash \varphi$ und $\Gamma \nvdash \neg\varphi$ (d.h. „Γ ist nicht vollständig").

Beweis: Γ semi-entscheidbar

$\Longrightarrow$ $\{(D, \varphi) \mid D$ Deduktion mit Hypothesen in Γ und Konklusion $\varphi\}$ semi-entscheidbar

$\Longrightarrow$ $\{\varphi \mid \Gamma \vdash \varphi\}$ semi-entscheidbar und (nach Korrektheitssatz) Teilmenge von $\mathrm{Th}(\mathcal{N})$

$\Longrightarrow$ $\{\varphi \mid \Gamma \vdash \varphi\} \subsetneq \mathrm{Th}(\mathcal{N})$ (denn $\mathrm{Th}(\mathcal{N})$ ist nicht semi-entscheidbar)

$\Longrightarrow$ es gibt Aussage φ mit $\underline{\mathcal{N} \models \varphi}$ und $\underline{\Gamma \nvdash \varphi}$

Angenommen, $\Gamma \vdash \neg\varphi$

$\Longrightarrow$ $\mathcal{N} \models \neg\varphi$ (nach Korrektheitsssatz), im Widerspruch zu $\mathcal{N} \models \varphi$

$\Longrightarrow$ $\underline{\Gamma \nvdash \neg\varphi}$. $\square$

Zusammenfassung 10. Vorlesung

in dieser Vorlesung neu

- Menge der allgemeingültigen Aussagen der Prädikatenlogik ist unentscheidbar
- Menge der in $(\mathbb{N}, +, \cdot)$ gültigen Aussagen ist unentscheidbar (nicht einmal semi-entscheidbar)
- 1. Gödelscher Unvollständigkeitssatz

kommende Vorlesung

- Unentscheidbarkeiten bei kontextfreien Sprachen

Automaten und formale Sprachen Folie 8.10 und Vorlesung 15 wiederholen!