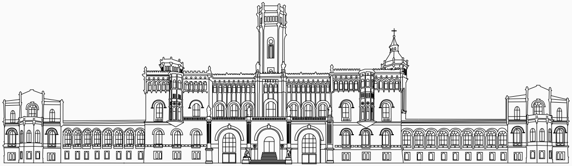
Die Presburger Arithmetik ist hart für EXPTIME

Seminar Berechenbarkeit und Logik

Leo Kayser

Sommersemester 2021

Institut für Theoretische Informatik



Die Axiome der minimalen Arithmetik

Signatur: $\sigma = (<; +, \cdot, '; 0)$

Standardinterpretation: Arithmetik der natürlichen Zahlen $\mathcal{N}^* = (\mathbb{N}; <; +, \cdot, '; 0)$

(Q1) $0 \neq x'$

(Q2) $x' = y' \to x = y$

(Q3) $x + 0 = x$

(Q4) $x + y' = (x + y)'$

(Q5) $x \cdot 0 = 0$

(Q6) $x \cdot y' = (x \cdot y) + y$

(Q7) $\neg x < 0$

(Q8) $x < y' \leftrightarrow (x < y \lor x = y)$

(Q9) $x < y \lor x = y \lor y < x$

Die Axiome der ~~minimalen~~ Presburger Arithmetik

Signatur: $\sigma = (<; +, '\,; 0)$

Interpretation: Additive Arithmetik der natürlichen Zahlen $\mathcal{A} = (\mathbb{N}; <; +, '\,; 0)$

(PA1) $0 \neq x'$

(PA2) $x' = y' \rightarrow x = y$

(PA3) $x + 0 = x$

(PA4) $x + y' = (x + y)'$

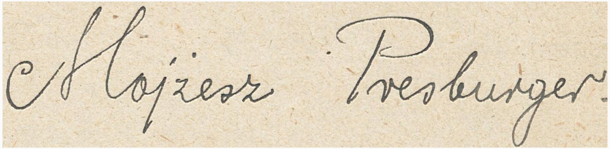
(PA5) $\neg x < 0$

(PA6) $x < y' \leftrightarrow (x < y \vee x = y)$

(PA7) $x < y \vee x = y \vee y < x$

www.hejibits.com

Eine entscheidbare Theorie!



Mojżesz Presburger (1904-1943), Public domain, via Wikimedia Commons

Die Presburger Arithmetik (PA) ist

- vollständig
- konsistent
- entscheidbar

(vgl. [Sta84])

> Die ist ja langweilig, weil entscheidbar.
>
> *Florian Chudigiewitsch*, kürzlich

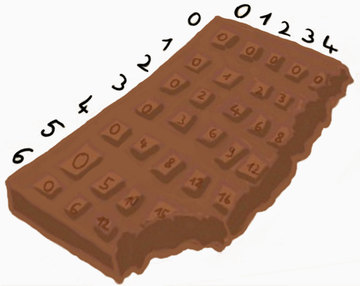
Mini-Multiplikation macht's möglich

Satz 1: (Vgl. [Mac78, Proposition 6.4.1] oder [Pau78, Lemma 6.52])

Für $k \in \mathbb{N}$ gibt es Formeln $M_k(x_1, x_2, x_3)$ in der PA, sodass für $m, n, p \in \mathbb{N}$ gilt

$$M_k(m, n, p) \qquad \text{genau dann wenn} \qquad m \cdot n = p \wedge m < 2^{2^k}.$$

Dabei ist $|M_k| \in O(k)$.



Konstruktion von $M_k(m, n, p) \Leftrightarrow (m \cdot n = p \wedge m < 2^{2^k})$

- Definiere M_k mittels Induktion nach k, den Anfang macht

$$M_0(x_1, x_2, x_3) := (x_1 = 0 \wedge x_3 = 0) \vee (x_1 = 1 \wedge x_2 = x_3).$$

- Beobachte: $x_1 \cdot x_2 = x_3 \wedge x_1 < 2^{2^{k+1}}$ gdw. $\exists u_1, u_2, u_3 < 2^{2^k}$ mit

$$x_1 = u_1 \cdot u_1 + u_2 + u_3 \qquad \text{und} \qquad x_3 = u_1 \cdot (u_1 \cdot x_2) + u_2 \cdot x_2 + u_3 \cdot x_2.$$

- Naiver Ansatz: Definiere $M_{k+1}(x_1, x_2, x_3)$ folgendermaßen:

$$\begin{aligned}
&\exists u_1 \exists u_2 \exists u_3 \exists p_1 \dots \exists p_5 \big[\\
&(x_1 = p_1 + (u_2 + u_3)) \wedge M_k(u_1, u_1, p_1) \wedge \\
&(x_3 = p_3 + (p_4 + p_5)) \wedge M_k(u_1, x_2, p_2) \wedge M_k(u_1, p_2, p_3) \wedge M_k(u_2, x_2, p_4) \wedge M_k(u_3, x_2, p_5) \big]
\end{aligned}$$

$\lightning$ Problem: $|M_k| > 5^k$!

- Reduziere auf „eine einzige“ Multiplikation

$$
\begin{aligned}
&\exists u_1 \ldots \exists p_5 \forall \tilde{x}_1 \forall \tilde{x}_2 \forall \tilde{x}_3 \big[(x_1 = p_1 + (u_2 + u_3)) \wedge (x_3 = p_2 + (p_3 + p_4)) \wedge (\\
&M_k(u_1, u_1, p_1) \qquad ((\tilde{x}_1 = u_1 \wedge \tilde{x}_2 = u_1 \wedge \tilde{x}_3 = p_1)\\
&M_k(u_1, x_2, p_2) \qquad \vee (\tilde{x}_1 = u_1 \wedge \tilde{x}_2 = x_2 \wedge \tilde{x}_3 = p_2)\\
&M_k(u_1, p_2, p_3) \qquad \vee (\tilde{x}_1 = u_1 \wedge \tilde{x}_2 = p_2 \wedge \tilde{x}_3 = p_3)\\
&M_k(u_2, x_2, p_4) \qquad \vee (\tilde{x}_1 = u_2 \wedge \tilde{x}_2 = x_2 \wedge \tilde{x}_3 = p_4)\\
&M_k(u_3, x_2, p_5) \qquad \vee (\tilde{x}_1 = u_3 \wedge \tilde{x}_2 = x_2 \wedge \tilde{x}_3 = p_5)) \to M_k(\tilde{x}_1, \tilde{x}_2, \tilde{x}_3))\big]
\end{aligned}
$$

- Setze rekursiv die Formel für M_k ein unter *geeigneter Umbenennung und Wiederverwendung* der Variablen (insgesamt „nur“ 14 gebundene Variablen!) □

Die Klasse EXP

Echs, P., via Pixabay

Definition: (EXP, EXP-schwer)

Die Klasse der Sprachen mit exponentieller Zeitkomplexität ist

$$\mathrm{EXP} = \mathrm{TIME}(2^{n^{O(1)}}) = \bigcup_{c \in \mathbb{N}} \mathrm{TIME}(2^{n^c}).$$

Eine Sprache A ist EXP-schwer, falls $B \leq_{\mathrm{m}}^{\mathrm{P}} A$ für alle $B \in \mathrm{EXP}$.

Die Presburger Arithmetik ist EXP-schwer

Satz 2

Die Sprache $A = \{ \langle F \rangle \mid F \in \mathrm{Th}(\mathcal{A}) \}$ ist EXP-schwer.

Korollar 3: (Vgl. [Pau78, Korollar 6.51])

Es gibt keinen Polynomialzeitalgorithmus, welcher die Gültigkeit eines gegebenen Satzes in der PA entscheidet.

Beweis. Angenommen doch, dann wäre $A \in \mathrm{P}$. da A EXP-schwer ist, folgt $\mathrm{EXP} \subseteq \mathrm{P}$ im Widerspruch zum Zeithierarchiesatz! $\lightning$ $\square$

Beweisidee zu Satz 2

Es sei $B \in \mathrm{EXP}$ gegeben, oBdA $B \subseteq \{0,1\}^*$.

- Fixiere Turingmaschine

$$M = (Z, \{0,1\}, \{0,1,\square\}, \delta, z_0, z_+, z_-),$$

welche $x \overset{?}{\in} B$ in $\leq 2^{p(|x|)}$ Schritten entscheidet

- Wissen, wie man mit Formeln über $\mathcal{N}^*$ Turingmaschinen simulieren kann
- Ausdruck hat polynomielle Länge in $|x|$

$\exists t\, \exists p \exists s$ — Es gibt eine Folge von s Konfigurationen, sodass:

$\exists x_1\, \exists x_2\, \exists x_3\, (\varphi_i(n, x_1, x_2, x_3)$ — Es gibt eine Startkonfiguration …

$\quad \wedge\, \beta(t,p,0) = x_1 \wedge \beta(t,p,1) = x_2$

$\quad \wedge\, \beta(t,p,2) = x_3)$ — … welche die erste Konfiguration der Folge ist.

$\quad \wedge\, \forall i\, \forall y_1\, \forall y_2\, \forall y_3\, \forall z_1\, \forall z_2\, \forall z_3$

$\quad\quad ((\beta(t,p,3i) = y_1 \wedge \beta(t,p,3i+1) = y_2 \wedge \beta(t,p,3i+2) = y_3$

$\quad\quad \wedge\, \beta(t,p,3i+3) = z_1 \wedge \beta(t,p,3i+4) = z_2 \wedge \beta(t,p,3i+5) = z_3)$

$\quad\quad \rightarrow \varphi_m(y_1, y_2, y_3, z_1, z_2, z_3))$

Für alle $i < s$ geht Konfiguration $i+1$ aus Konfiguration i in einem Schritt von M hervor.

$\quad \wedge\, \beta(t,p,3s) = k$ — Konfiguration s ist akzeptierend.

↯ Multiplikation hier nicht verfügbar

$\Rightarrow$ Ersetze Multiplikation durch M_k

Beweisskizze zur Reduktion $B \leq_{\mathrm{m}}^{\mathrm{P}} A$ $(x \mapsto \langle F \rangle)$

- Stelle eine Folge von Konfigurationen als Wörter über $\Delta := Z \cup \{0, 1, \Box, \#\}$ dar

$$w = \Box z_0 \underbrace{101010}_{=x} \Box \# \Box 0 z_{42} 01010 \Box \# \dots$$

- Die Länge dieser Zeichenkette können wir abschätzen durch

$$|w| \leq \underbrace{(2^{p(|x|)} + 2)}_{\text{Platz einer Konf.}} \cdot \underbrace{(2^{p(|x|)} + 1)}_{\#\text{Konf.} \leq t+1}$$

- Codiert man w zur Basis p, $p > |\Delta|$, so ist die Größe der resultierenden Zahl durch $p^{|w|} \leq 2^{2^{\mathrm{poly}(|x|)}}$ beschränkt

$\Rightarrow$ Ersetze „$a \cdot b = c$“ durch „$M_{\mathrm{poly}(|x|)}(a, b, c)$“ in der Formel für

$$F \equiv \text{„}M \text{ hält auf } x \text{ in Endzustand } z_+\text{“}$$

$\Box$

Es ist noch viel schlimmer!

Michael J. Fischer, Homepage

Michael O. Rabin, Homepage

Satz 4: (Fischer & Rabin, 1974 [FR98, Theorem 1])

Die Sprache A ist schwer für $2\text{-EXP} = \mathrm{TIME}(2^{2^{n^{O(1)}}})$.

Beweisidee: Konstruiere $Prod_k(x_1, x_2, x_3)$, sodass für $m, n, p \in \mathbb{N}$ gilt

$$Prod_k(m, n, p) \qquad \text{genau dann wenn} \qquad m \cdot n = p \wedge m, n, p < g(k),$$

wobei $g(k) \geq 2^{2^{2^{k+1}}}$ und $|Prod_k| \in O(k)$. Dann analoge Reduktion.

https://www.youtube.com/watch?v=CUsPGzA3YEU

Danke! Fragen?

Literaturquellen

[FR98] Michael J. Fischer und Michael O. Rabin. „Super-Exponential Complexity of Presburger Arithmetic“. In: *Quantifier Elimination and Cylindrical Algebraic Decomposition*. Texts and Monographs in Symbolic Computation. Springer, 1998, S. 122–135. ISBN: 9783709194591.

[Mac78] Michael Machtey. *An introduction to the general theory of algorithms*. New York: North-Holland, 1978. ISBN: 0444002278.

[Pau78] Wolfgang Paul. *Komplexitätstheorie*. Stuttgart: Teubner, 1978. ISBN: 3519023415.

[Sta84] Ryan Stansifer. *Presburger's Article on Integer Arithmetic: Remarks and Translation*. Techn. Ber. TR84-639. Cornell University, Computer Science Department, Sep. 1984.

Bildquellen

- Folie 1, 2: Von John Kleckner. https://hejibits.com/post/173307003744/134
- Folie 3: Public Domain, aus Mojżesz Presburgers CV. https://commons.wikimedia.org/wiki/File:Moj%C5%BCesz_Presburger_(signature).jpg
- Folie 4: Eigenes Werk von Nadja Nidzwezki.
- Folie 7: Anrita1705 auf Pixabay, freie Nutzung. https://pixabay.com/de/photos/eidechse-echse-bunt-kopf-blick-4763351/
- Folie 11: Homepage von Michael J. Fisher. http://www.cs.yale.edu/homes/fischer/images/p8311448.jpg
- Folie 11: Homepage von Michael O. Rabin. https://www.seas.harvard.edu/about-us/directory?search=%22Michael%20O.%20Rabin%22
- Letzte Folie: YouTube Video von Hydraulic Press Channel. https://www.youtube.com/watch?v=CUsPGzA3YEU