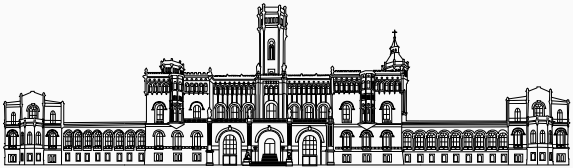
Der Satz von Smolensky

Seminar Theorie Boole'scher Schaltkreise

Leo Kayser

Sommersemester 2022

Institut für Theoretische Informatik



A modulo mio

Definition 1: $(\mathrm{MOD}_p, \mathcal{B}_1(p), \mathrm{AC}^0[p])$

(i) Zu $p \in \mathbb{N}$ sei $\mathrm{MOD}_p = (\mathrm{mod}_p^n)_{n\in\mathbb{N}}$ die Familie der booleschen Funktionen

$$\mathrm{mod}_p^n(x_1, \ldots, x_n) \coloneqq [\![x_1 + \cdots + x_n \equiv 0 \bmod p]\!].$$

(ii) Es sei $\mathcal{B}_1(p) \coloneqq \mathcal{B}_1 \cup \{\mathrm{MOD}_p\}$ und $\mathrm{AC}^0[p] \coloneqq \mathrm{SIZE\text{-}DEPTH}_{\mathcal{B}_1(p)}(n^{O(1)}, 1)$.

Beobachtung: Ist p prim, dann folgt aus dem kleinen Fermat

$$a^p \equiv a \bmod p,$$

dass man MOD_p durch Polynome über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ darstellen kann:

$$\mathrm{mod}_p^n(x_1, \ldots, x_n) \equiv 1 - (x_1 + \cdots + x_n)^{p-1} \bmod p.$$

Aus Schaltkreis mach' Polynom

Definition 2: (MOD_p-$\wedge$-Schaltkreis, Ordnung)

Ein MOD_p-$\wedge$-Schaltkreis der Ordnung $\leq d$ besteht aus drei Ebenen:

- Ausgabegatter ist ein MOD_p-Gatter;
- Vorgänger des MOD_p-Gatters sind $\wedge$-Gatter mit fan-in $\leq d$;
- Vorgänger der $\wedge$-Gatter sind Eingabevariablen oder deren Negation.

Satz 3: (MOD_p-$\wedge$-Schaltkreis $\rightsquigarrow$ Polynom)

Sei p prim und C ein MOD_p-$\wedge$-Schaltkreis der Ordnung d_0. Dann gibt es ein $q \in \mathbb{F}_p[X_1, \ldots, X_n]$ vom Grad $(p-1)d_0$, mit

$$f_C(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) \in \{0,1\} \subseteq \mathbb{F}_p \qquad \forall \overline{x} \in \{0,1\}^n.$$

Beweis von Satz 3

Beweis.

- Sei G ein $\wedge^d$-Gatter in C mit Vorgängern $\{x_{i_1}, \ldots, x_{i_j}, \neg x_{i_{j+1}}, \ldots, \neg x_{i_d}\}$
- Wir dürfen oBdA annehmen, dass $i_k \neq i_{k'}$ für $k \neq k'$
- Folgendes Polynom berechnet den Teilschaltkreis über G:

$$t_G(X_1, \ldots, X_n) \coloneqq X_{i_1} \cdots X_{i_j} \cdot (1 - X_{i_{j+1}}) \cdots (1 - X_{i_d})$$

- Wähle als Polynom

$$q(X_1, \ldots, X_n) \coloneqq 1 - \left(\sum_G t_G(X_1, \ldots, X_n) \right)^{p-1}$$

- $\deg q = (p-1) \deg(\sum_G t_G) \leq (p-1) d_0$ □

$\mathrm{AC}^0[p]$-Sprachen kann man durch Polynome gut annähern...

Satz 4: (Robin, vor ein paar Minuten)

Sei $A \in \mathrm{AC}^0[p]$ und $k \in \mathbb{N}$. Dann gibt es eine MOD_p-$\wedge$-Schaltkreisfamilie $\mathcal{C}$ der Ordnung $(\log n)^{O(1)}$, sodass

$$\#\{\,\overline{x} \in \{0,1\}^n \mid c_A(\overline{x}) = f_{\mathcal{C}}(\overline{x})\,\} \geq 2^n(1 - n^{-k}).$$

Korollar 5: (Satz 3 + Satz 4)

Sei $A \in \mathrm{AC}^0[p]$, $n, k \in \mathbb{N}$. Es gibt Polynome $q_n \in \mathbb{F}_p[X_1, \ldots, X_n]$ vom Grad $(\log n)^{O(1)}$, sodass für mindestens $2^n(1 - n^{-k})$ der Eingaben $\overline{x} \in \{0,1\}^n$ gilt

$$c_A(x_1 x_2 \ldots x_n) = q_n(x_1, x_2, \ldots, x_n) \in \{0,1\}.$$

...die MOD_r-Funktion hingegen nicht!

Zu $r, i \in \mathbb{N}$ sei $\mathrm{MOD}_{r,i} = (\mathrm{mod}^n_{r,i})_{n\in\mathbb{N}}$ die Familie der booleschen Funktionen

$$\mathrm{mod}^n_{r,i}(x_1, \ldots, x_n) := [\![x_1 + \cdots + x_n \equiv i \bmod r]\!] .$$

Algebrafakt: Ist $\mathrm{ggT}(r, p) = 1$, so gibt es ein $k \in \mathbb{N}$ und ein $1 \neq \omega \in \mathbb{F}_{p^k}$ mit $\omega^r = 1$.

Satz 6: ($\mathrm{MOD}_{r,i}$ ist schlecht polynomiell approximierbar)

Sei p prim, r, k wie eben. Dann gibt es ein n_0, sodass für $n \geq n_0$ gilt:
Für beliebige $F_0, \ldots, F_{r-1} \in \mathbb{F}_{p^k}[X_1, \ldots, X_n]$ vom Grad $\leq \sqrt{n}$ gibt es $\geq \frac{2^n}{10}$ Wörter $\overline{x} \in \{0,1\}^n$ mit

$$F_i(\overline{x}) \neq \mathrm{MOD}_{r,i}(\overline{x}) \quad \text{für mind. ein } 0 \leq i < r.$$

Auf multilineare Polynome kann man zählen

- Ein Monom $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ ist *multilinear*, falls stets $\alpha_i \leq 1$
- $\mathrm{MLM}(n, \leq d)$ = Menge der multilinearen Monome in n Variablen vom Grad $\leq d$

Lemma 7: Technisches Abzählargument Es gibt ein n_0, sodass

$$\#\mathrm{MLM}\big(n, \leq \tfrac{n+\sqrt{n}}{2}\big) \leq \frac{9}{10} \cdot 2^n \qquad \forall n \geq n_0.$$

- *Multilineare Polynome* = Linearkombinationen multilinearer Monome
- Notation $\mathrm{MLP}/\mathbb{F}(n, \leq d)$; erhalten unmittelbar Abschätzung

$$\#\mathrm{MLP}/\mathbb{F}\big(n, \leq \tfrac{n+\sqrt{n}}{2}\big) \leq |\mathbb{F}|^{\frac{9}{10} \cdot 2^n} \qquad \forall n \geq n_0$$

Beweisidee zu Satz 6 ($\#A \leq \frac{9}{10} \cdot 2^n$)

- „Korrekte“ Eingaben $A := \{ \overline{x} \in \{0,1\}^n \mid \forall i : F_i(\overline{x}) = \mathrm{MOD}_{r,i}(\overline{x}) \}$
- Man kann eine Injektion $\mathrm{Abb}(A, \mathbb{F}_{p^k}) \hookrightarrow \mathrm{MLP}/\mathbb{F}_{p^k}(n, \leq d)$ konstruieren:
  - $A \leftrightarrow \tilde{A} := \{ (\omega^{a_1}, \ldots, \omega^{a_n}) \mid \overline{a} \in A \}$
  - Zu jedem $f : \tilde{A} \to \mathbb{F}_{p^k}$ gibt es ein $q \in \mathrm{MLP}/\mathbb{F}_{p^k}\left(n, \leq \frac{n+\sqrt{n}}{2}\right)$, welches mit f auf $\tilde{A}$ übereinstimmt
- Nach dem Abzählargument: $\#\mathrm{MLP}/\mathbb{F}_{p^k}(n, \leq \frac{n+\sqrt{n}}{2}) \leq \left|\mathbb{F}_{p^k}\right|^{\frac{9}{10} \cdot 2^n} = (p^k)^{\frac{9}{10} \cdot 2^n}$
- Zusammensetzen:

$$(p^k)^{\#A} = \#\mathrm{Abb}(A, \mathbb{F}_{p^k}) \leq \#\mathrm{MLP}/\mathbb{F}_{p^k}(n, \leq \tfrac{n+\sqrt{n}}{2}) \leq (p^k)^{\frac{9}{10} \cdot 2^n}$$

$\Rightarrow \#A \leq \frac{9}{10} \cdot 2^n$ „$\square$“

Der große Coup

Roman Smolensky (1960-1995)

Satz 8: (Smolensky [Smo87])

Für r teilerfremd zu p prim ist $\mathrm{MOD}_r \notin \mathrm{AC}^0[p]$.

Beweis von Satz 8

Beweis. *Angenommen* $\mathrm{MOD}_r \in \mathrm{AC}^0[p]$.

- Nach Korollar 5 gibt es zu $k \in \mathbb{N}$ Polynome $q_n \in \mathbb{F}_p[X_1, \ldots, X_n]$ vom Grad $(\log n)^{O(1)}$, die mod_r^n korrekt auf mindestens $(1 - n^{-k})2^n$ Eingaben berechnen
- Sei $\deg(q_n) \leq (\log n)^c$, wähle $n_1 \geq n_0$ mit

$$2^{n_1}(1 - n_1^{-k}) > \frac{9}{10}2^{n_1 - r} + (2^r - 1)2^{n_1 - r}, \qquad (\log(n_1 + r))^c \leq \sqrt{n_1}$$

- Definiere für $n \geq n_1$ Polynome $F_0, \ldots, F_{r-1} \in \mathbb{F}_{p^k}[X_1, \ldots, X_n]$ durch

$$F_i = q_{n+r}(X_1, \ldots, X_n, \underbrace{0, \ldots, 0}_{i \text{ Mal}}, \underbrace{1, \ldots, 1}_{r - i \text{ Mal}}), \qquad 0 \leq i < r.$$

- Die F_i haben Grad $\leq \sqrt{n}$ und berechnen $\mathrm{mod}_{r,i}^n$ auf $> \frac{9}{10}2^n$ Eingaben korrekt

↯ Widerspruch zu Satz 6! □

Danke! Fragen?

Literaturquellen

[All95] Eric Allender. *Combinatorial Methods in Complexity Theory. Lectures 8 & 9*. 16. Feb. 1995. URL: https://people.cs.rutgers.edu/~allender/papers/notes6.pdf.

[Smo87] Roman Smolensky. „Algebraic methods in the theory of lower bounds for Boolean circuit complexity“. In: *Proceedings of the nineteenth annual ACM symposium on Theory of computing* (1987).

[Vol99] Heribert Vollmer. „Introduction to Circuit Complexity“. In: *Texts in Theoretical Computer Science An EATCS Series*. 1999.

Bildquellen

- Allan Borodin. Tribute to Roman Smolensky. Computational Complexity 6, 195–198 (1996). https://doi.org/10.1007/BF01294252