Komplexitätstheorie

Sommersemester 2013

Prof. Dr. Georg Schnitger,
Dipl. Inf. Bert Besser

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Arbeitsgruppe Theoretische Informatik, Institut für Informatik

Blatt 7

Ausgabe: 12.06.2012
Abgabe: **26**.06.2012

Hinweis: Das Blatt ist binnen zwei Wochen zu bearbeiten und es gibt 12 Bonuspunkte zu holen.

Die Primzahl p sei gegeben. Wir betrachten mod_p-Schaltkreise, die außer $\wedge$-, $\vee$- und Negationsgattern auch mod_p-Gatter haben. Ein mod_p-Gatter nimmt den Wert Null genau dann an, wenn die Anzahl der gesetzten Eingabebits ein Vielfaches von p ist.

mod_p-Schaltkreise polynomieller Größe und beschränkter Tiefe sind mächtiger als AC^0-Schaltkreise. Wir vollziehen die Methode von Razborov-Smolensky nach, die eine exponentielle untere Schranke für die Größe eines mod_p-Schaltkreises für $\mathtt{xor}_n$ zeigt.

7.1. Aufgabe (7+5)

Approximation durch Polynome

Gegeben sei ein mod_p-Schaltkreis C der Größe s und der Tiefe d.

a) Für den Parameter t beschreibe eine Menge P von Polynomen des Grades $\Delta = ((p-1)\cdot t)^d$ über $\mathbb{Z}_p$, so dass für alle Eingaben x gilt:

$$\mathrm{pr}_{q\in P}[C(x) \neq q(x)] \leq \frac{s}{p^t}.$$

Hinweis: Approximiere ein Gatter der Tiefe l mit Fehler höchstens $\frac{s'}{p^t}$ durch ein Polynom vom Grad $((p-1)\cdot t)^l$, wobei das Gatter von s' anderen Gattern abhängt.

Zum Einstieg: Das Gatter $G(x) = \bigvee_{i\in I} x_i$ hat Tiefe 1. Zeige, dass G durch das folgende Polynom mit Fehler höchstens $\frac{1}{p^t}$ approximiert wird, wobei die $b_{i,j}$ zufällig aus $\mathbb{Z}_p$ sind:

$$G'(x) = 1 - \prod_{j=1}^{t} \left(1 - \left(\sum_{i\in I} b_{i,j}\cdot x_i\right)^{p-1}\right) \bmod p.$$

Der kleine Satz von Fermat, d.h. die Aussage, dass $a^{p-1} \equiv 1 \bmod p$ für alle $a \not\equiv 0 \bmod p$ gilt, ist hilfreich.

b) Zeige, dass es ein Polynom vom Grad Δ über $\mathbb{Z}_p$ gibt, das auf einer Menge $V \subseteq \{0,1\}^n$ mit $|V| \geq (1-\frac{s}{p^t})\cdot 2^n$ mit der von C berechneten Funktion übereinstimmt.

Die Aussage aus 1b) gilt insbesondere für den Fall, dass C die Funktion $\mathtt{xor}_n$ berechnet. In Aufgabe 2 bereiten wir ein Zählargument vor, das wir in den Aufgaben 3a) und 3b) durchführen und das uns in Aufgabe 3c) einen Rückschluss auf s erlaubt.

7.2. Aufgabe (3+4+5) *Ein Polynom für eine Funktion*

a) Bestimme eine Transformation $T : \{-1,+1\}^n \to \{0,1\}^n$, so dass für $y \in \{-1,+1\}^n$ gilt:

$$\prod_{i=1}^{n} y_i = -1 \;\Leftrightarrow\; \texttt{xor}_n(T(y)) = 1.$$

Gegeben sei ein mod_p-Schaltkreis der Größe s und der Tiefe d für $\texttt{xor}_n$. Zeige, dass es eine Menge $U \subseteq \{-1,+1\}^n$ mit $|U| \geq (1 - \frac{s}{p^t}) \cdot 2^n$ gibt, so dass

b) ein Polynom vom Grad Δ über $\mathbb{Z}_p$ existiert, das auf U mit der Multiplikation übereinstimmt.

c) jede Funktion $f : U \to \mathbb{Z}_p$ durch ein Polynom p_f vom Grad $(n+\Delta)/2$ über $\mathbb{Z}_p$ berechnet werden kann.

Hinweis: Jede Funktion $f : U \to \mathbb{Z}_p$ kann durch ein Polynom aus Monomen vom Grad höchstens n beschrieben werden, denn $U \subseteq \{-1,+1\}^n$. Drücke den Grad jedes Monoms auf $(n+\Delta)/2$, um p_f zu erhalten. Benutze dafür das Polynom aus Teil a).

7.3. Aufgabe (3+4+5) *Die Schranke*

a) Zeige, dass für die Anzahl M der Monome vom Grad höchstens $(n+\Delta)/2$ gilt:

$$M \leq 2^{n-1} + \Delta \cdot \binom{n}{n/2} = 2^{n-1} + \Theta(\Delta \cdot \frac{2^n}{\sqrt{n}}).$$

Gegeben sei ein mod_p-Schaltkreis der Größe s und der Tiefe d für $\texttt{xor}_n$. U sei die Menge aus Aufgabe 2.

b) Zeige $|U| \leq M$.

Hinweis: Wie ist die Anzahl l der Funktionen $f : U \to \mathbb{Z}_p$? Wie ist die Anzahl k der Polynome über $\mathbb{Z}_p$ mit Monomen vom Grad höchstens $(n+\Delta)/2$? Es muss $l \leq k$ gelten!

c) Mit den Schätzungen für $|U|$ zeige $s = 2^{\Omega(n^{1/2d})}$.

Die untere Schranke ist im Vergleich zur Schranke $2^{\Omega(n^{1/(d-1)})}$ für $\{\wedge, \vee, \neg\}$-Schaltkreise zwar schlechter, aber für ein mächtigeres Schaltkreismodell immer noch exponentiell groß.