10.01.2005

Komplexitätstheorie

Ziel: untere Schranken für eingeschränkte Klassen von booleschen Schaltkreisen
- bislang: monotone Schaltkreise (ohne $\neg$)
- jetzt: Schaltkreise *konstanter Tiefe*

Bem.: jede boolesche Funktion kann von Schaltkreisen (exponentieller Größe und) der *Tiefe 2* berechnet werden; und zwar durch Berechnung der DNF dieser Funktion

Paritätsfunktion: $parity(x_1,...,x_n) = (\sum_{i=1}^{n} x_i) \bmod 2$

(entspricht gerader/ungerader Anzahl von 1en)

Wir zeigen: *Parity* $\notin AC^0$
Parity ist nicht berechenbar durch Schaltkreise polynomieller Größe p(n) und Tiefe d für jedes (noch so große) d.

Trick: Repräsentierung boolescher Funktionen durch Polynome, Beispiel:

$\wedge(x_1,...,x_n) = \prod_{i=1}^{n} x^i$ (Polynom vom Grad n)

- hier: Approximation durch Polynom *niedrigen Grades*

Beweis in 2 Schritten:

Ziel 1: Für $f \in AC^0$ gibt es ein Polynom p() kleinen Grades mit $f(\vec{x}) = p(\vec{x})$ für fast alle $\vec{x} \in \{0,1\}$.

Ziel 2: Es gibt kein Polynom q() kleinen Grades mit $q(\vec{x}) = parity(\vec{x})$ für viele $\vec{x} \in \{0,1\}$.

Zusammen folgt die Behauptung.
Für Ziel 1 brauchen wir die Approximation von $\wedge$ und $\vee$. Es reicht, nur $\vee$ zu approximieren, denn:
- wenn $p(x_1,...,x_n) = \vee(x_1,...,x_n)$, dann ist $\wedge(x_1,...,x_n) = 1 - p(1-x_1,...,1-x_n)$.

Polynome zur Approximation von $\vee$ werden *zufällig* konstruiert:

$S_0 := \{1,...,n\}$

$S_{i+1} \leq S_i$, wobei für $k \in S_i$ gilt: $\Pr[k \in S_{i+1}] = \frac{1}{2}$.

Definiere für i=1,...,m

$q_i := \sum_{j \in S_i} x_j$

$p := \prod_{i=0}^{m} (1 - q_i)$ Grad von $p \leq m = O(\log n)$

Falls $\wedge(x_1,...,x_n) = 0$, dann ist $p(x_1,...,x_n) = 1$.

Zu zeigen: Ist $\vee(x_1,...,x_n)=1$, dann ist $\Pr[p(x_1,...,x_n)=0]\geq\frac{1}{2}$, (*)
d.h. $1-p$ approximiert das $\vee$ mit Fehlerwahrscheinlichkeit $\leq(\frac{1}{2})$.

Wahrscheinlichkeitsverstärkung: konstruiere wie oben *unabhängig* $p_1,...,p_t$ und betrachte statt $1-p$ das Polynom $1-p_1*...*p_t$ vom Grad $\leq t(\log_2 n+2)$, das $\vee$ mit approximiert mit Fehlerwahrscheinlichkeit $(\frac{1}{2})^t$.

➔ Fehlerwahrscheinlichkeit kleiner als ε, wenn $t=\log\frac{1}{\varepsilon}$.

Beweis von (*): $p(x_1,...,x_n)=0$, wenn mindestens eines der $q_i=1$ist.

$q_i=1$, wenn $|S_i\cap T|=1$, wobei $T=\{j;x_j=1\}$.

➔ zu berechnen: $\Pr[\exists i:|S_i\cap T|=1]$

Fallunterscheidung:

Fall 1: $\forall i\in\{0,...,m\}:|S_i\cap T|>1$.

Wahrscheinlichkeit dafür ist:

$$\Pr[\forall i:|T\cap S_i|>1]\leq\Pr[\forall i:|T\cap S_i|\geq 1]$$
$$\leq\Pr[|T\cap S_n|\geq 1]\leq n*(\tfrac{1}{2})^{\log n+2}$$
$$=n*\tfrac{1}{4n}=\tfrac{1}{4}$$

Fall 2: $\exists i\in\{0,...,m\}:|S_i\cap T|\leq 1$

Sei $i_0:=\min\{i;|T\cap S_i|\leq 1\}$

d.h. $k=|T\cap S_{i_o-1}|>1$;

$|T\cap S_{i_0}|\leq 1$

$$\Pr[|T\cap S_{i_0}|=1\,|\,|T\cap S_{i_0-1}|=k\wedge|T\cap S_{i_0}|\leq 1]$$
$$=\frac{k*2^{-k}}{2^{-k}+k*2^{-k}}=\frac{k}{k+1}\geq\frac{2}{3}$$

also folgt: $\Pr[\exists i:|T\cap S_i|=1]\geq\frac{3}{4}*\frac{2}{3}=\frac{1}{2}$

Insgesamt: Schaltkreis C der Größe s und Tiefe d wird approximiert mit Fehlerwahrscheinlichkeit ∂ durch ein Polynom:

- approximiere jedes Gatter durch Polynom mit Fehler $\frac{\partial}{s}$
- Grad $O((\log(\frac{s}{d})\log n)^d)$, also polylogarithmisch in n, falls $s(n)$ ein Polynom und ∂, s konstant. Für große n ist der Grad < $\sqrt{n}/2$.

➔ Es gibt Polynom p von polylogarithmischem Grad (insb. Grad < $\sqrt{n}/2$) mit $C(x_1,...,x_n)=p(x_1,...,x_n)$ für mindestens $0{,}9^n*2^n$ der möglichen 2^n Inputs.

Ziel 2: Es gibt kein Polynom q() kleinen Grades mit $q(\vec{x}) = parity(\vec{x})$ für viele $\vec{x} \in \{0,1\}$.

Lineartransformation: $y = 1 - 2x$ liefert Darstellung mit “true“ = -1, “false“ = +1.
(bislang: “true“ = 1, “false“ = 0)

In dieser Darstellung ist $parity(y_1,...,y_n) = \prod_{i=1}^{n} y_i$.

Ziel 2’: (nächste Stunde)
Es gibt kein Polynom $q(y_1,...,y_n)$ vom Grad < $\sqrt{n}/2$ mit

$q(y_1,...,y_n) = \prod_{i=1}^{n} y_i$ für $0,9^n * 2^n$ der $(y_1,...,y_n) \in \{1,-1\}^n$.