Michael Forbes
miforbes@illinois.edu

CS 579: Computational Complexity Lecture 21

today: constant depth formulas
- context
- random restrictions
- polynomial approximations

last time: $NP \not\subseteq P \Leftarrow NP \not\subseteq P/poly$

thm [Subbotovskaya]: F size ℓ formula $\Rightarrow \rho$ set $n-1$ vars $\underbrace{|F|_\rho| \le \ell/n^{1.5}}_{<1 \Rightarrow}$ $F|_\rho$ constant

F = parity $\Rightarrow \underbrace{|F|_\rho| \ge 1}_{F|_\rho \text{ nonconstant}}$

Q: better lbs for restricted formulas?

def: $\underset{\text{alternating}}{AC^i} = \{ F_n : \{0,1\}^n \to \{0,1\}$ size$(F) \le$ poly(n) depth$(F) \le O(\lg n)^i \}$
unbounded fan in

AC^0 $\le O(1)$

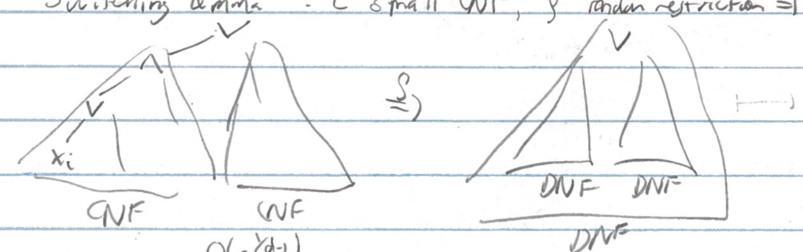
"simplest" nontrivial ckt class

Rmk: $AC^0 \subseteq \underbrace{NC^1}_{=\text{formulas}} \subseteq AC^1 \subseteq NC^2 \subseteq \cdots \subseteq NC = AC$

thm [Håstad]: $\oplus_n$ requires $2^{\Omega(n^{\frac{1}{d-1}})}$ size depth d AC^0 formulas

Sketch: F_n size s depth d AC^0 formula $\Rightarrow$ restriction ρ on $\sim(\log s)^{d-1}$ variables $F|_\rho$ constant

uses "Switching lemma": C small CNF, ρ random restriction $\Rightarrow C|_\rho$ has small DNF whp [[technical]]



Rmk: hw: parity has $2^{O(n^{1/d-1})}$ size depth d AC^0

Q: is this interesting?
- "can't" improve lb as
- not many interesting functions in AC^0

def: $MOD_m : \{0,1\}^n \to \{0,1\}$ $MOD_m(x_1, \ldots, x_n) = \begin{cases} 0 & \sum x_i = 0 \pmod m \\ 1 & \text{else} \end{cases}$

$AC^0[m] = AC^0$ w/ MOD_m gates

fact: interesting functions in $AC^0[2]$

Thm [Razborov Smolensky] $p \ne q$ prime $(= \Theta(1))$. MOD_p requires $2^{n^{\Omega(1/d)}}$-size $AC^0[q]$ formulas

today: $p = 2$, $q = 3$

idea: F small $AC^0[3]$ formula $\Rightarrow F$ is "approximately" a low degree poly over $\mathbb{F}_3$
MOD_2 is not

hw: $f : \{0,1\}^n \to \{0,1\}$ exist $p \in \mathbb{F}_3[x_1, \ldots, x_n]$ st
- $\deg_{x_i} p \le 1$ all i
- $f(\bar{x}) = p(\bar{x})$ all $x \in \{0,1\}^n$

$\Big\}$ p is unique

Michael Forbes
mforbes@illinois.edu
2018-04-04.2 ⟵ 2018-04-04.1
⟶ 2018-04-04.3
CS 579

$$\Rightarrow \quad OR(x_1,\dots,x_n) = \overbrace{1-(1-x_1)\cdots(1-x_n)}^{\deg n \text{ [maximal]}} \quad \underline{\text{uniquely}}$$

<u>idea</u>: get low degree by using <u>randomness</u>

<u>Key lemma</u>: exist poly $p(\bar{x},\bar{r}) \in \mathbb{F}_3[x_1,\dots,x_n,r_1,\dots,r_n]$ $\underbrace{\deg 2 \text{ in } \bar{x}}$, st
any $\bar{x}\in\{0,1\}^n$, $\Pr_{\bar{\alpha}\leftarrow\mathbb{F}_3^n}[p(\bar{x},\bar{\alpha}) \neq OR(\bar{x})] \le 1/3$ — don't care about dependence on $\bar{r}$

<u>Pf</u>: <u>ideas</u>: - $y \mapsto y^2$ [reduce back down to boolean]
$0 \to 0$
$1 \to 1$
$-1=2 \to 1$

- $\bar{x}\neq\bar{0} \Rightarrow \langle\bar{\alpha},\bar{x}\rangle = \sum \alpha_i x_i$ is uniformly distributed over $\mathbb{F}_3$

<u>hence</u>: $p(\bar{x},\bar{\alpha}) = (\sum x_i\alpha_i)^2$

$OR(\bar{x})=0 \Rightarrow \bar{x}=0 \Rightarrow p(\bar{0},\bar{\alpha}) = (0)^2 = 0$
$=1 \Rightarrow \neq \Rightarrow \sum x_i\alpha_i$ uniform over $\mathbb{F}_3$
$\Rightarrow (\sum x_i\alpha_i)^2 = 0$ w/p $1/3$
$=1$ w/p $2/3$ ∎

[need smaller error]

<u>Cor</u>: exist poly $p_k \in \mathbb{F}_3[\bar{x},\bar{r}]$ (don't care how many) $\deg 2k$ in $\bar{x}$ st
any $\bar{x}\in\{0,1\}^n$ $\Pr_{\bar{\alpha}\leftarrow\mathbb{F}_3^{|\bar{r}|}}[p_k(\bar{x},\bar{\alpha}) \neq OR(\bar{x})] \le 1/3^k$

<u>Pf</u>: $p_k = OR(p(\bar{x},\bar{\alpha}_1),\dots,p(\bar{x},\bar{\alpha}_k))$, $\bar{\alpha}_1,\dots,\bar{\alpha}_k \leftarrow \mathbb{F}_3^n$ iid
$\bar{x}=0 \Rightarrow$ all $0 \Rightarrow$ $=0$
$\bar{x}\neq 0 \Rightarrow$ all i $\Pr[p(\bar{x},\bar{\alpha}_i)=0] \le 1/3$
$\Pr[\text{all } i \text{ ''}] \le 1/3^k$
$\Pr[p_k = 0] \le 1/3^k$

do brute force: $p_k = 1-\prod_{i=1}^{k}(1-\underbrace{p(\bar{x},\bar{r}_k)}_{\deg 2})$] $\deg 2k$.

<u>Cor</u>: F $AC^0[3]$ size s depth d formula, exist polynomial $P\in\mathbb{F}_3[\bar{x},\bar{r}]$
st - $\deg_{\bar{x}} P(\bar{x},\bar{r}) \le \text{poly}(s/\varepsilon)^d$
- any $\bar{x}\in\{0,1\}$ $\Pr_{\bar{\alpha}\leftarrow\mathbb{F}_3^{|\bar{r}|}}[P(\bar{x},\bar{\alpha}) = F(\bar{x})] \le \varepsilon$

<u>Pf</u>. by induction:
x_i: $P = x_i$
$F = \neg G$: $G \approx Q(\bar{x},\bar{r})$
$P := 1-Q(\bar{x},\bar{r})$ — deg unchanged, error unchanged

Michael Forbes
miforbes@illinois.edu
2018-04-04.2 → 2018-04-04.3
2018-04-04.4 ←
CS579

better: take each gate to have error $\le \varepsilon$, then all s gates get total error $s\varepsilon$
OR: don't use $k\varepsilon \le s\varepsilon$ at each step, this gives $\le s\varepsilon$

$F = MOD_3(G_1, \ldots, G_k)$

$\quad \wr \qquad \wr$

$\quad Q_1 \qquad Q_k \qquad p := (Q_1 + \cdots + Q_k)^2$ ← multiplicative increase in degree

if $\underline{\text{all } i}$ $\quad G_i(\bar{x}) = Q_i(\bar{x}, \bar{r}_i) \Rightarrow p(\bar{x}, \bar{r}) = F(\bar{x})$

↳ happens except w/p $\quad k \cdot \varepsilon \le s \cdot \varepsilon$ ← multiplicative increase in error

$F = OR(G_1, \ldots, G_k)$

$\quad \wr \qquad \wr$

$\quad Q_1 \qquad Q_k \qquad p := \widetilde{OR}_\ell(Q_1 \ldots Q_k)$ ← deg $2\ell \cdot \max_i \deg Q_i$

if $\underline{\text{all } i}$ $\quad G_i(\bar{x}) = Q_i(\bar{x}, \bar{r}_i) \Rightarrow F = p$ except w/p $\underbrace{1/3^\ell}_{\varepsilon}$

↳ happens ~~except~~ w/p $\quad k \cdot \varepsilon \le s \cdot \varepsilon$

take: $\ell = \log_3 1/\varepsilon$

$\Rightarrow$ any x $\quad F = p$ except w/p $(s+1) \cdot \varepsilon$

$\left[\begin{array}{ll} \underline{\text{each step}}: & \text{degree increases by } O(\lg 1/\varepsilon) \\ \text{error} & O(s \cdot \varepsilon) \end{array}\right] \Rightarrow$ degree $O(\lg 1/\varepsilon)^d$, error $\underbrace{O(s\varepsilon)^d}_{\text{want } = \delta}$

$O(s\varepsilon)^d = \delta \Rightarrow \varepsilon^d = \delta / s^d \quad \varepsilon = \delta^{1/d}/s$

$\Rightarrow$ degree $O(\lg s/\delta^{1/d})^d = O(\lg s/\delta)^d$

error δ.

$\boxtimes$

$\underline{\text{Cor}}$: F $AC^0[3]$ formula size s depth d. any $\varepsilon > 0$ exist poly $p(x) \in \mathbb{F}_3[\bar{x}]$

- deg $\le O(\lg s/\varepsilon)^d$
- exist set $S \subseteq \{0,1\}^n$ $\quad |S| \ge (1-\varepsilon) 2^n$, $\forall x \in S \quad p(x) = F(x)$. $\square$

$\underline{\text{Prop}}$: no $o(\sqrt{n})$ degree poly over $\mathbb{F}_3[\bar{x}]$ can agree w/ MOD_2 on $\ge \frac{3}{4} 2^n$ inputs

$\underline{\text{Cor}}$: MOD_2 requires $2^{n^{\Omega(1/d)}}$ size $AC^0[3]$ depth d formulas

$\underline{\text{Pf}}$: set $\varepsilon = 1/5 \Rightarrow (1-\varepsilon) 2^n \ge 3/4\, 2^n$, s st $O(\lg s/\varepsilon)^d \le o(\sqrt{n})$

$\underline{\text{Pf}}$: Suppose not. $S \subseteq \{0,1\}^n$ $\quad |S| \ge 3/4 \cdot 2^n$ $\quad p(x)$ deg $\le o(\sqrt{n})$ $\quad p|_S = MOD|_S$

$\underline{\text{idea}}$: change basis $\{0,1\} \Rightarrow \{\pm 1\} \subseteq \mathbb{F}_3$ $\quad x \mapsto (-1)^x$, $\quad x \mapsto 1 - 2x$

consider $q(\bar{x}) = 1 - 2 \cdot p\left(\frac{1-x_1}{2}, \ldots, \frac{1-x_n}{2}\right)$ ← deg q = deg p

$MOD_2(\bar{x}) \mapsto x_1 \cdots x_n$

$\underline{Q}$: $x_1 \cdots x_n \approx$ low degree poly on $T \subseteq \{\pm 1\}^n$?

$\underline{\text{idea}}$: polynomial method.

$V := \{ f : T \to \mathbb{F}_3 \}$ $\mathbb{F}_3$ vector space, dimension $|T|$

$\underline{\text{rhm}}$: ↳ represented by polynomial in $\mathbb{F}_3[\bar{x}]$ w/ ideg ≤ 2

on T $\quad x_i^2 = 1 \qquad \Rightarrow \qquad \le 1$

consider $f : T \to \mathbb{F}_3$, $\quad f = \sum_{\bar{a} \in \{0,1\}^n} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$

$MOD_2 : T \to \mathbb{F}_3 \qquad MOD_2 = x_1 \cdots x_n$

$= q(\bar{x})$ ← deg $o(\sqrt{n})$

Michael Forbes
mforbes@illinois.edu
2018-04-04.4 ⇆ 2018-04-04.3
2018-04-09.1
cs579

now consider $\bar{x}^{\bar{a}}$ w/ $\deg \bar{x}^{\bar{a}} > n/2$

$$\bar{x}^{\bar{a}} \equiv \bar{x}^{\bar{a}} \cdot g(\bar{x}) \cdot (x_1 \cdots x_n)$$

$$= \underbrace{\prod x_i^{\overbrace{a_i+1}^{1-a_i} \pmod 2}}_{\deg = n - \deg \bar{x}^{\bar{a}}} \cdot \underbrace{g(x)}_{\text{degree } o(\sqrt{n})}$$

$\deg \leq \frac{n}{2} + o(\sqrt{n})$

hence: on T all monomials are equiv to deg $\frac{n}{2}+o(\sqrt{n})$ monomials polynomials

$$\Rightarrow \quad T = \dim V \leq \#\text{poly deg } \tfrac{n}{2}+o(\sqrt{n}) \text{ poly} \leq \sum_{k \leq n/2 + o(\sqrt{n})} \binom{n}{k}$$

$$\leq \frac{1}{2} \cdot 2^n + \sum_{0 \leq k \leq o(\sqrt{n})} \underbrace{\binom{n}{n/2+k}}_{\leq \binom{n}{n/2} \leq O\left(\frac{2^n}{\sqrt{n}}\right)}$$

Stirling

$$\leq \frac{1}{2} 2^n + o(\sqrt{n}) \cdot O\left(\frac{2^n}{\sqrt{n}}\right)$$

$$< \frac{3}{4} 2^n. \quad \boxtimes$$

Rmk: this "is" Valiant-Vazirani / Toda's thm
drastically fails for $AC^0[m]$, m composite
Thm [Williams 13]: $NEXP \not\subseteq AC^0[m]$.

union bound
lg p dependence
in deg