- +10 min
- vector space method
- p vs p
- k vs l

Michael Forbes
miforbes@illinois.edu

2019-04-16-4 ⇒ 2019-04-18.1
2019-04-18.2 ⇐ cs579

cs 579 Computational Complexity : Lecture 26

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

thm [Subbotovskaya]: F size ℓ formula $\Rightarrow \exists \rho$ restricting $n-1$ vars w/ $|F|_\rho| \leq \rho n^{1.5}$

F = parity $\Rightarrow |F|_\rho| \geq 1 \Rightarrow \ell \geq n^{1.5}$

($F|_\rho$ nonconstant; under simplification; not too far from best known)

today: constant depth formulas - random restrictions
- polynomial approximations

Q: better lbs for restricted formulas?

def: (non uniform) $AC^i = \{ f_n : \{0,1\}^n \to \{0,1\}$ (alternating) exists circuit C_n computing f_n - $size(C_n) \leq poly(n)$ - $depth(C_n) \in O(\lg^i n)$ - C_n has unbounded fan-in AND, OR, NOT

AC^0 = constant depth unbounded fan-in

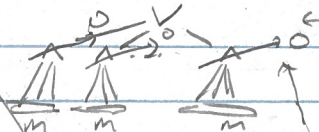
eg: $OR_n, AND_n \in AC^0$

rmk: $AC^0 \subseteq NC^1 \subseteq AC^1 \subseteq NC^2 \subseteq \cdots \subseteq NC = AC$

(turn unbounded fan-in AND, OR into fan-in 2 formula; formulas)

thm [Hastad]: $\oplus_n$ requires $2^{\Omega(n^{\frac{1}{d-1}})}$ size depth d unbounded fan-in formulas.

↳ idea: unbounded fan-in AND, OR simplify a lot under random restriction

eg 

all gates simplify if formula is small

$\Rightarrow F|_\rho$ constant but ρ sets $< n$ bits

whp as many gates have $\Rightarrow F \neq \rho$

rmk: - parity has $2^{O(n^{\frac{1}{d-1}})}$ size depth d unbounded fan-in formulas

- hence is essentially tight
- open: better lbs against AC^0
- not "too many" interesting functions in AC^0 (but still very restrictive; how to make more interesting?)

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

$AC^0[m] = AC^0$ formulas that also use unbounded fan-in MOD_m gates

Thm [Razborov, Smolensky]: $p \neq q$ prime $(= \Theta(1))$. MOD_q requires $2^{n^{\Omega(\gamma_d)}}$ size $AC^0[p]$ formulas

today: $p = 3, q = 2$

Rmk: - interesting functions exist in $AC^0[p]$

- not known to be tight $2^{O(n^{\frac{1}{d-1}})}$ vs $2^{n^{\Omega(\gamma_d)}}$

Michael Forbes
miforbes@illinois.edu
2019-04-16-2 ← 2019-04-18-1
os 57 → 2019-04-16-3

idea: F small $AC^0[3]$ formula $\Rightarrow$ F is "approximately" a low degree polynomial over $\mathbb{F}_3$

but: MOD$_2$ is not ↗

Fact: $f: \{0,1\}^n \to \{0,1\}$. exists $p \in \mathbb{F}_3[x_1, \dots, x_n]$ s.t.
- $\deg_{x_i} p \le 1$ all i ← multilinear
- $\forall x \in \{0,1\}^n \quad f(x) = p(x)$

} p unique

$\Rightarrow$ $OR(x_1, \dots, x_n) = 1 - (1-x_1)\cdots(1-x_n)$ uniquely

idea: can get lower degree using randomness ← degree n ← "large"

key lemma: exist poly $p(x, r) \in \mathbb{F}_3[x_1, \dots, x_n, r_1, \dots, r_m]$ $\deg_x p \le 2$ s.t.
$\forall x \in \{0,1\}^n$ $\Pr_{\alpha \leftarrow \mathbb{F}_3^m}[p(x,\alpha) \neq OR(x)] \le 1/3$
‖ probabilistic poly ‖ ‖ $2 \le n$ ‖
↖ don't care about r here

Pf: idea: - $y \mapsto y^2$ ‖ $\mathbb{F}_3 \to \{0,1\}$ ‖
$0 \mapsto 0$
$1 \mapsto 1$
$-1 = 2 \mapsto 1$

- $x \neq 0^n \Rightarrow$ $\langle x, \alpha \rangle = \sum x_i \alpha_i$ is uniformly random ← as in pairwise indep

hence - $p(x, \alpha) = (\sum x_i \alpha_i)^2$ ← degree 2

$OR(x) = 0 \Rightarrow x = 0^n \Rightarrow \forall \alpha\ p(0, \alpha) = (0)^2 = 0 \Rightarrow \Pr[p \neq OR] = 0$ ‖ one sided error ‖

$1 \Rightarrow \neq \Rightarrow \sum x_i \alpha_i$ uniform over $\mathbb{F}_3$

$\Rightarrow (\sum x_i \alpha_i)^2 = 0$ w.p. $1/3$

‖ need small error ‖ $\Rightarrow \Pr[p \neq OR] = 1/3 = 1$ w.p. $2/3$ ∎

Cor: exists poly $p_k \in \mathbb{F}_3[x_1, \dots, x_n, r_{11}, \dots, r_{mk}]$ $\deg_x p \le 2k$ s.t.
$\forall x \in \{0,1\}^n$ $\Pr_{\alpha \leftarrow \mathbb{F}_3^{n \cdot k}}[p_k(x, \alpha) \neq OR(x)] \le 1/3^k$

‖ k times ‖

Pf: $p_k := OR(p(x, \alpha_1), \dots, p(x, \alpha_k))$ $\alpha_1, \dots, \alpha_k \in \mathbb{F}_3^n$ rand, indep

- $x = 0 \to$ all $0 \Rightarrow = 0$
- $\neq 0 \Rightarrow$ all i: $\Pr[p(x, \alpha_i) = 0] \le 1/3$
  $\Rightarrow$ $\Pr$[all $= 0$] $\le 1/3^k$ ‖ k independent ‖
  $\Rightarrow \Pr[p_k(x, \alpha) = 0] \le 1/3^k$

as poly: $p_k = 1 - \prod_{i=1}^{k} (1 - p(x, \alpha_i))$ deg $2k$
(deg 2)

Michael Forbes
Mirabel Reid Williamson
2019-04-15.1 → 2019-04-15.4 ← 2019-04-15.3
CS 579

$\forall \varepsilon > 0$

Cor: $F \in AC^0[3]$ size s depth d formula, exists poly $p \in \mathbb{F}_3[x_1, \dots, x_n]$, s.t.
- $\deg_x p \le O(\lg(s/\varepsilon))^d$
- $\forall x \in \{0,1\}^n$ $\Pr_{\alpha \leftarrow \mathbb{F}_3^{|x|}}[p(x,\alpha) \neq F(x)] \le \varepsilon$

Pf: by induction:

$F = x_i$: $p = x_i$

$F = \neg G$: $G = Q(x,r)$, $P := 1 - Q(x,r)$ ← degree, error unchanged

$F = MOD_3(G_1, \dots, G_k) \Rightarrow P := (Q_1 + \cdots + Q_k)^2$

(Q_i s.l. Q_k; ↑ degree multiplies by 2)

if all: $G_i(x) = Q_i(x, r_i) \Rightarrow P(x, r) = F(x)$ ← no error added

$F = OR(G_1, \dots, G_k)$ (Q_i s.l. Q_i) $P := \widetilde{OR}_\ell(Q_1, \dots, Q_k)$ ← $\deg \le 2\ell \cdot \max \deg Q_i$

if all: $G_i(x) = Q_i(x, r_i) \Rightarrow P(x,r) = F(x)$ except w.p. $\le 1/3^\ell$

$F = AND$: convert to OR using de Morgan's law

each step: degree increases by $\le 2\ell$ over children $\Rightarrow$ degree $\le (2\ell)^d$ (depth d)

error: each gate works with probability $\ge 1 - 1/3^\ell$ conditioned on correct inputs

union bound over s gates $\Rightarrow$ error $\le s/3^\ell = \varepsilon$

$\Rightarrow$ pick $\ell = \log_3 s/\varepsilon = O(\lg s/\varepsilon)$

$\Rightarrow$ degree $\le O(\lg s/\varepsilon)^d$

∎ by averaging

Cor: $F \in AC^0[3]$ formula size s depth d. Any $\varepsilon > 0$ exists $p \in \mathbb{F}_3[x]$
- $\deg_x p \le O(\lg s/\varepsilon)^d$
- exists $S \subseteq \{0,1\}^n$ $|S| \ge (1-\varepsilon)2^n$ $\forall x \in S$ $p(x) = F(x)$ ∎

Pf: no $o(\sqrt{n})$ degree polynomial over $\mathbb{F}_3[x]$ computes MOD_2 on $n \ge 3/4 \cdot 2^n$ many inputs

Cor: MOD_2 requires $2^{n - \Omega(n^d)}$ size $AC^0[3]$ depth d formula.

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

$\Rightarrow s \ge 2^{n - \Omega(n^{1/2d})}$

Pf: suppose not. $S \subseteq \{0,1\}^n$ $|S| \ge 3/4\, 2^n$ $p(x)$ deg $o(\sqrt{n})$

idea: change basis $\{0,1\} \to \{\pm 1\}^* \subseteq \mathbb{F}_2$ $\quad p|_S = MOD_2|_S$

$x \mapsto (-1)^x$

$x \mapsto 1 - 2x$

hence $q(x) := 1 - 2 \cdot P\left(\frac{1-x_1}{2}, \dots, \frac{1-x_n}{2}\right)$

$MOD_2(x) \mapsto x_1 \cdots x_n$ ↑ deg q = deg P ?

Q: $x_1 \cdots x_n$ ≥ low degree over $T \subseteq \{\pm 1\}^n$?

idea: polynomial method

$V = \{ f : T \to \mathbb{F}_2 \}$ $\mathbb{F}_2$ vector space dimension $|T|$

↳ represented by polynomials in $\mathbb{F}_2[x]$ w/ ideg ≤ 2

on T, $x_i^2 = 1$ ⇒ ≤ 1

consider $f : T \to \mathbb{F}_2$ $f = \sum_{a \in \{0,1\}^n} \alpha_a x^a$

$MOD_2 : T \to \mathbb{F}_2$ $MOD_2 = x_1 \cdots x_n = q(x)$ ← deg $\le \sqrt{n}$

now consider x^a w/ deg $x^a > n/2$

$x^a \equiv x^a \cdot q(x) \cdot (x_1 \cdots x_n)$ $y^2 = 1$

$= \prod_i x_i^{(a_i+1) \pmod 2} \cdot q(x)$

$= 1 - a_i$

deg = n − deg x^a + deg $\le \sqrt{n}$

deg ≤ $n/2 + o(\sqrt{n})$]

hence - on T all monomials equiv to degree ≤ $n/2 + o(\sqrt{n})$ polynomial

⇒ $|T| = \dim V \le \dim \{ \text{poly deg} \le n/2 + o(\sqrt{n}) \} \le \sum_{k \le n/2 + o(\sqrt{n})} \binom{n}{k}$

$\le \frac{1}{2} \cdot 2^n + \sum_{\ell \le o(\sqrt{n})} \binom{n}{n/2 + \ell}$ ← Stirling

$\le \binom{n}{n/2} \le O\left(\frac{2^n}{\sqrt{n}}\right)$

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

$o(1) \cdot 2^n$

$< 3/4 \cdot 2^n$ ⇒ ⇐ ∎

Rmk: - drastically fails for $AC^0[m]$ w/ m composite [no large vector space]

- thm [Williams 13]: $NEXP \not\subseteq AC^0[m]$