DD2445 COMPLEXITY THEORY: LECTURE 19

RECAP

ACC^0 Constant-depth circuits (poly-size) with also MOD-gates

$$MOD_m(x) = \begin{cases} 0 & \text{if } \sum_i x_i \equiv 0 \pmod m \\ 1 & \text{otherwise} \end{cases}$$

Focus on $ACC^0(3)$ – only MOD_3-gates

THEOREM $\quad PARITY \notin ACC^0(3)$

Razborov-Smolensky method of approximations

(1) Show circuits in $ACC^0(3)$ well approximated by low-degree $\mathbb{F}_3$-polynomials

(2) Show PARITY can't be approximated in this way

Did (1) last time:

COROLLARY 8 For any circuit C over $\{\vee, 1, \neg, MOD_3\}$ of size s and depth d there exist $\mathbb{F}_3$-polynomial p of degree $\leq (2k)^d$ such that and for all $k \in \mathbb{N}^+$

$$\Pr_{x \sim \{0,1\}^n}\left[C(x) \neq p(x)\right] \leq s/3^k$$

Challenge: Exact representation of $\vee$ and $\wedge$ requires high degree

Solution: Random linear sum (squared) $\left(\sum_{i=1}^{t} v_i x_i\right)^2$

for $v \sim \mathbb{F}_3^t$ approximates with probability $2/3$

– amplify to get error $1/3^k$ in degree $2k$.

"local"

LEMMA 9

There exists a constant $\delta > 0$ such that for n large enough it holds for all $\mathbb{F}_3$-polynomials p of degree $\leq \sqrt{n}$ that

$$P_{x \in \{0,1\}^n}\left[p(x) \neq PARITY(x) \right] \geq \delta$$

p and PARITY disagree on δ-fraction of inputs

Proof Let p be such a polynomial

Now switch from $p : \{0,1\}^n \to \mathbb{F}_3$

to $\tilde{p} : \{-1, 1\}^n \to \mathbb{F}_3$

Recall $\mathbb{F}_3 = \{-1, 0, 1\}$

identify $-1 = true$ $\quad +1 = false$

$$\{0,1\} \underset{y \mapsto y-1}{\overset{x \mapsto x+1}{\rightleftarrows}} \{1, -1\}$$

$$\widetilde{PARITY}(y) = \prod_{i=1}^{n} y_i \qquad y \in \{\pm 1\}^n$$

If p approximates PARITY well, then

$$\tilde{p}(y) = 1 + p(y_1 - 1, y_2 - 1, \ldots, y_n - 1)$$

approximates $\widetilde{PARITY}$ equally well

And degree doesn't increase

LEMMA 10 Suppose for $\tilde{T} \subseteq \{\pm 1\}^n$ $\exists$ degree-d polynomial $\tilde{p}$ s.t. $\forall y \in \tilde{T}$ $\widetilde{PARITY}(y) = \tilde{p}(y)$. Then for all $\tilde{f} : \{\pm 1\}^n \to \mathbb{F}_3$ there is a degree-$(n/2 + d)$ polynomial $\tilde{p}_f$ such that

$$\forall y \in \tilde{T} \quad \tilde{f}(y) = \tilde{p}_f(y).$$

Proof The monomials $\prod_{i \in S} y_i$, $S \subseteq [n]$, form a basis for $\{\{\pm 1\}^n \to \mathbb{F}_3\}$

In particular, they span this space (*), so any $\tilde{f}$ can be written as

$$\tilde{f}(y) = \sum_{S \subseteq [n]} c_S \prod_{i \in S} x_i \qquad c_S \in \mathbb{F}_3 \quad (\dagger)$$

Over set $\tilde{T}$ can rewrite $\tilde{f}$ as

$$\tilde{f}(y) = \sum_{S : |S| \leq n/2} c_S \prod_{i \in S} y_i \qquad (\neq)$$

$$+ \sum_{S : |S| > n/2} c_S \tilde{p}(y) \prod_{i \notin S} y_i$$

This will be polynomial $\tilde{p}_f$.
Degree $\leq n/2 + d$ by assumption

Why does this work? For $S \subseteq [n]$, $|S| \leq n/2$ have same terms in $(\dagger)$ and $(\neq)$.
For $|S| > n/2$ it holds for $y \in \tilde{T}$ that

$$c_S \tilde{p}(y) \prod_{i \notin S} y_i = c_S \prod_{i \in [n]} y_i \cdot \prod_{i \notin S} y_i$$

$$= c_S \prod_{i \in S} y_i \cdot \prod_{i \notin S} y_i^2$$

$$= c_S \prod_{i \in S} y_i$$

$\square$

Back to proof of Lemma 10...

(*) $I_\alpha(y) = \begin{cases} 1 & \text{if } y = \alpha \\ 0 & \text{o/w} \end{cases}$

DETOUR MA XI 1/2

for $\alpha \in \{\pm 1\}^n$ span $\{\{\pm 1\}^n \to \mathbb{F}_3\}$

Can write

$$I_\alpha(y) = \prod_{i=1}^{n} I_{\alpha_i}(y_i)$$

for

$$I_{\alpha_i}(y_i) = 1 - (y_i - \alpha_i)^2 = \begin{cases} 1 & \text{if } y_i = \alpha_i \\ 0 & \text{o/w} \end{cases}$$

So polynomials can represent all functions $\{\{\pm 1\}^n \to \mathbb{F}_3\}$

And since evaluated over $\{\pm 1\}$, w.l.o.g. multilinear.

So multilinear polynomials in $\mathbb{F}_3[y_1, \ldots, y_n]$ can represent any function $f: \{\pm 1\}^n \to \mathbb{F}_3$.

And, as discussed last time, this representation is unique.

Say that $p : \{0,1\}^n \to \mathbb{F}_3$ agrees with PARITY on $T \subseteq \{0,1\}^n$ of degree $\leq \sqrt{n}$

Then $\tilde{p}$ agrees with PARITY on corresponding set $\tilde{T} \subseteq \{\pm 1\}^n$

By Lem 10, Every $\tilde{f} : \{\pm 1\}^n \to \mathbb{F}_3$ has $(n/2 + \sqrt{n})$-degree polynomial agreeing with $\tilde{f}$ on $\tilde{T}$.

Restrict attention to $\tilde{T}$ and do some counting

distinct functions when restricted to $\tilde{T}$

$$= \left| \left\{ \tilde{T} \to \mathbb{F}_3 \right\} \right| = \boxed{3^{|\tilde{T}|}} \qquad (*)$$

Every such function must be approximated by distinct (multilinear) polynomial of degree $\frac{n}{2} + \sqrt{n}$

How many such polynomials are there?

CLAIM 11 # multilinear monomials of degree $\leq \frac{n}{2} + \sqrt{n}$ in n variables =

$$= \left| \left\{ S \subseteq [n] : |S| \leq n/2 + \sqrt{n} \right\} \right|$$

$$= \sum_{i=0}^{n/2+\sqrt{n}} \binom{n}{i} \leq \boxed{(1-\delta)2^n}$$

for some $\delta > 0$ if n is large enough

[Arora-Barak say we can take $\delta = \frac{1}{50}$.

This is just a calculation, so we skip it.]

By Claim 11, # multilinear polynomials of degree $\leq n/2 + \sqrt{n}$ is

$$\leq 3^{(1-\delta)2^n} \qquad (**)$$

since polynomial fully specified by choice of coefficients in $\mathbb{F}_3$ for monomials.
Combining (*) and (**) we get

$$3^{|\tilde{T}|} \leq 3^{(1-\delta)2^n}$$

$$|\tilde{T}| \leq (1-\delta)2^n$$

So $\tilde{p}$ and $\widetilde{\text{PARITY}}$ disagree on $\geq \delta$-fraction of inputs; hence, so do p and PARITY. Lemma 9 follows ▨

Now we are ready to prove PARITY $\notin$ ACC^0(3)

(1) For all $C \in$ ACC^0(3) of size s and depth d there is degree $(2k)^d$-polynomial p s.t.

$$\Pr_{x \sim \{0,1\}^n}\left[C(x) \neq p(x)\right] \leq s/3^k$$

(2) There exists $\delta > 0$ such that if C computes PARITY, then for all polynomials of degree $\leq \sqrt{n}$ it holds that

$$\Pr_{x \sim \{0,1\}^n}\left[C(x) \neq p(x)\right] \geq \delta.$$

Choose k so that [as large as possible] | MA XIV

$(2k)^d \leq \sqrt{n}$, meaning

$k := n^{1/2d} / 2^{\#\#\#}$

① and ② now yields

$$\delta \leq \Pr_x[C(x) \neq p(x)] \leq s / 3^k$$

or

$$s \geq \delta \cdot 3^k = \delta \cdot 3^{n^{1/2d}/2^{\#\#\#}}$$

$$= \exp(\Omega(n^\gamma))$$

for some $\gamma > 0$ when $d = O(1)$.
This concludes the proof ∎

What about ACC^0 in general?
(i.e., not just MOD_3 gates but also other moduli)

Brings us right to the frontier of circuit complexity. Consistent with state-of-the-art that $NP \subseteq ACC^0(2,3) = ACC^0(6)$?

Break-through result:

THEOREM [Williams '10]
$NEXP \not\subseteq ACC^0$

MONOTONE CIRCUITS

Circuit is monotone if no NOT-gates (only AND- and OR-gates)

For $x, y \in \{0,1\}^n$, write $x \leq y$ if for all $i \in [n]$ $x_i \leq y_i$

A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is MONOTONE if $\boxed{x \leq y \Rightarrow f(x) \leq f(y)}$

$\Updownarrow$

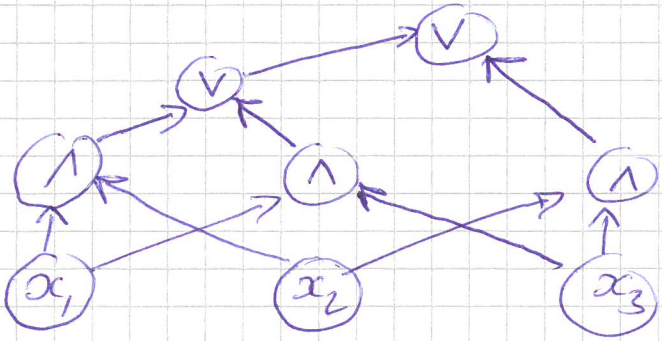
flipping any bit in input from 0 to 1 can never flip function from 1 to 0

FACTS 1

- Every monotone circuit computes a monotone function
- Every monotone function can be computed by a monotone circuit (Why?)

Ex 2 $MAJ(x_1, x_2, x_3)$ = majority value among bits

$$MAJ(x_1, x_2, x_3) = \begin{cases} 1 & \text{if } x_1 + x_2 + x_3 \geq 2 \\ 0 & \text{o/w} \end{cases}$$



Ex 3 $\boxed{CLIQUE_{k,n}}$

Input: $\binom{n}{2}$ bits = indicator bits for edges in graph on n vertices
$\Downarrow$
specification of graph G

Output: 1 if $\exists$ k-clique in G
0 o/w

clearly monotone — adding more edges can never remove clique.

clique NP-complete $\Rightarrow$ should be hard for general circuits (unless $NP \subseteq P/poly$)

Can prove lower bound for monotone circuits:

THEOREM 4 [Razborov '85, Andreev '85, Alon-Boppana '87]
There exists a constant $\varepsilon > 0$ such that for every $k \leq n^{1/4}$ there is no monotone circuit of size less than $2^{\varepsilon\sqrt{k}}$ that computes $CLIQUE_{k,n}$

No depth restrictions or anything...

Would have $NP \neq P/poly$ if w.l.o.g. best circuit for monotone function is monotone circuit. Or at least suffer at most polynomial blow-up.
NOT TRUE! Shown by Razborov.

Consider first special kind of subfunctions / subcircuits

For $S \subseteq [n]$, let $C_S : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be

$$C_S(G) = \begin{cases} 1 & \text{if } S \text{ forms clique in } G \\ 0 & \text{o/w} \end{cases}$$

CLIQUE INDICATOR of S

$$CLIQUE_{k,n} = \bigvee_{\substack{S \subseteq [n] \\ |S| = k}} C_S$$

$\binom{n}{k} \leq n^k$ clique indicators

Show $CLIQUE_{k,n}$ cannot be computed by OR of $< n^{\sqrt{k}/20}$ clique indicators

Idea: Create distributions of yes-instances Y and no-instances N. Show that circuit cannot tell apart random samples from the two distributions.

Distribution Y: Choose $K \subseteq [n]$, $|K| = k$ at random. Output graph with

$V = [n]$

$E = \{(u,v) \mid u \neq v,\ u,v \in K\}$

clique on K and no other edges

Distribution N: Choose function $c : [n] \to [k-1]$ at random. Output graph with all edges (u,v) for $c(u) \neq c(v)$ (i.e., complete $(k-1)$-partite graph)

$V = [n]$

$E = \{(u,v) \mid c(u) \neq c(v)\}$

$$\Pr_{G \sim \mathcal{Y}}\left[CLIQUE_{k,n}(G) = 1 \right] = 1$$

$$\Pr_{G \sim \mathcal{N}}\left[CLIQUE_{k,n}(G) = 0 \right] = 1$$

But OR of at least $n^{\sqrt{k}/20}$ clique indicators needed

LEMMA 5 Pick n sufficiently large and let $k \leq n^{1/4}$ and $S \subseteq [n]$. Then either

$$\Pr_{G \sim \mathcal{N}}\left[C_S(G) = 1 \right] \geq 0.99 \quad \frac{99}{100}$$

or

$$\Pr_{G \sim \mathcal{Y}}\left[C_S(G) = 1 \right] \leq \frac{1}{100} n^{-\sqrt{k}/20}.$$

Proof By case analysis over $|S|$.

Let $\ell = \sqrt{k-1}/10$

Case 1: $|S| \leq \ell$

By the birthday paradox bound,

$\Pr[c : [S] \to [k-1] \text{ one-to-one}] \geq 99/100$

But if c one-to-one on S we get ℓ-clique

Hence, $\Pr[C_S(\mathcal{N}) = 1] \geq 99/100$ in this case

BIRTHDAY PARADOX

MC V

Choose ℓ random numbers $a_1, \ldots, a_\ell$ uniformly and independently in $[m]$

What is the expected number of collisions? (Pairs $i<j$ such that $a_i \leq a_j$) Let

$$Y_{ij} = \begin{cases} 1 & \text{if } a_i = a_j \\ 0 & \text{o/w} \end{cases}$$

$$\mathbb{E}[Y_{ij}] = 1/m$$

$$\#\text{ collisions} = \sum_{i<j} Y_{ij}$$

$$\mathbb{E}\left[\sum_{i<j} Y_{ij}\right] = \sum_{i<j} \mathbb{E}[Y_{ij}] = \boxed{\binom{\ell}{2}\frac{1}{m}}$$

If $\ell \approx \sqrt{2m}$ expect to see collision

In class of 27 students, expect to see 2 with the same birthday

If $\ell = \sqrt{m}/K$, then $\Pr[\text{collision}] \leq \frac{1}{K^2}$

Expect to see

$$\binom{\ell}{2}\frac{1}{m} \leq \frac{\ell^2}{m} = \frac{1}{K^2} \quad \text{collision}$$

1 collision = Factor K^2 more than expected

Markov $\Pr[X \geq K] \leq \frac{\mathbb{E}[X]}{K}$

$$\Pr[\text{collision}] \leq \frac{1/K^2}{1} = 1/K^2$$

Case 2: $|S| > \ell$

For $G \sim \gamma$ $C_S(G) = 1$ iff it holds for randomly sampled $K \subseteq [n]$, $|K| = k$, that $S \subseteq K$

$$\Pr_K[S \subseteq K] \leq \frac{\binom{n-\ell}{k-\ell}}{\binom{n}{k}} =$$

$$= \frac{(n-\ell)!}{(k-\ell)!(n-\ell-k+\ell)!} \cdot \frac{k!\,(n-k)!}{n!}$$

$$= \frac{k(k-1)\cdots(k-\ell+1)}{n(n-1)\cdots(n-\ell+1)}$$

$$\leq \frac{k^\ell}{(n-\ell+1)^\ell} \leq \left[\begin{array}{c}\ell \text{ small} \\ \text{compared to } k \text{ \& } n\end{array}\right]$$

$$\leq \left(\frac{2k}{n}\right)^\ell \qquad \left[\begin{array}{l} k \leq n^{1/4} \\ \ell \geq \sqrt{k-1}/10 \end{array}\right]$$

$$\leq \left(2\, n^{-3/4}\right)^{\frac{\sqrt{k-1}}{10}}$$

$$\leq \frac{1}{100}\, n^{-\sqrt{k}/20} \qquad \text{for } n \text{ large enough}$$

Lemma 5 follows ▨

This implies that OR of too few clique indicators fails dramatically to distinguish γ and $\mathcal{N}$

COROLLARY 6

Suppose that $C' = \bigvee_{i=1}^{m} C_{S_i}$ and suppose n is large enough and $k \le n^{1/4}$.

Then if # clique indicators $m \le n^{\sqrt{k}/20}$ it holds that not only does C' fail to compute $CLIQUE_{k,n}$ but C' errs on 99% of either Y or N.

Proof If some $C_{S_{i^*}}$ has $|S_{i^*}| \le \sqrt{k-1}/10$, then

$$\Pr_{G \sim N}\left[\bigvee_{i=1}^{m} C_{S_i}(G) = 1\right] \ge \Pr\left[C_{S_{i^*}}(G) = 1\right] \ge 99/100$$

So suppose all S_i have $|S_i| > \sqrt{k-1}/10$

Then

$$\Pr_{G \sim Y}\left[\bigvee_{i=1}^{m} C_{S_i}(G) = 1\right] \le \sum_{i=1}^{m} \Pr\left[C_{S_i}(G) \neq 1\right]$$

$$\le m \cdot n^{-\sqrt{k}/20}/100$$

$$\le 1/100. \qquad \square$$

Now prove:

Monotone, small circuit C for $CLIQUE_{k,n}$

$\Downarrow$

OR of somewhat small # clique indicators distinguish Y and N well (almost as well as C)

Here formally:

LEMMA 7 Let C monotone circuit of size $s \leq 2^{\sqrt{k}/2}$. Then there exists a collection $S_1, \ldots, S_m$; $S_i \subseteq [n]$, $m \leq n^{\sqrt{k}/20}$, such that

$$\Pr_{G \sim Y}\left[\bigwedge_{i=1}^{m} C_{S_i}(G) \geq C(G)\right] > 0.9$$

$$\Pr_{G \sim N}\left[\bigwedge_{i=1}^{m} C_{S_i}(G) \leq C(G)\right] > 0.9$$

But we know $\bigwedge_{i=1}^{m} C_{S_i}$ either far too pessimistic on instances in Y or far too optimistic on instances in N.

The same must then hold for G, which hence cannot be deciding $CLIQUE_{k,n}$