CS221 LECTURE 12

2/29/20

TODAY

(1) PARITY $\notin AC^0$ [Razborov-Smolensky]

(2) Start TODA's Thm: $PH \subseteq P^{\#P}$

Reminder from last lecture

AC^0 = functions computable by poly-size, $O(1)$-depth circuits with ∞-AND, ∞-OR, NOT gates.

$\oplus(x_1 \cdots x_n) = \sum x_i \mod 2$

Thm: Parity $\notin AC^0$. Specifically if C is a depth d, size S circuit that computes parity, then $S \geq 2^{n^{1/2d}}$.

Razborov's "Method of Approximation".

- function is "simple" if it can be "approximated" by "low-degree" polynomial. (over $\mathbb{F}_3$).
- Parity is not simple.
- AC^0 is simple.

Defn: f is simple if $\exists S \subseteq \{0,1\}^n$, $|S| \geq \frac{3}{4} \cdot 2^n$ & ~~$\neq$~~.

polynomial $p(\ )$ of degree $o(\sqrt{n})$ ~~polylog~~ s.t.

$\forall\, a \in S \quad f(a) = p(a)$.

Lemma 1: depth d, size s, circuits with $s = o\left(2^{n^{1/2d}}\right)$ are simp

Lemma 2: Parity is not simple.

Proof of Lemma 1:

key idea: $\boxed{\forall x \quad \Pr_{\alpha}\left[\left(\sum \alpha_i x_i\right)^2 = \underbrace{OR(x_1 \ldots x_n)}_{\text{need to extend to all } AC^0}\right] \geq \underbrace{\frac{1}{2}}_{\text{need to boost to } \frac{3}{4}} \cdot \quad - \quad (*)}$

[Exercise: Prove (*)]

boosting: $\forall x \quad \Pr_{\alpha^{(1)} \ldots \alpha^{(\ell)}}\left[OR(x_1 \ldots x_n) \neq \underbrace{OR\left(\langle \alpha^{(1)}, x\rangle^2, \ldots \langle \alpha^{(\ell)}, x\rangle^2\right)}_{\deg 2\ell \text{ poly in } x.}\right] \leq 2^{-\ell}$

[will use $\ell = o(n^{1/2d})$]

$OR \Rightarrow AC^0$: replace every gate!

$\Pr_{\ldots}\left[C(x_1 \ldots x_n) \neq \text{comp. of poly}(x_1 \ldots x_n)\right] \leq s \cdot 2^{-\ell}$

- degree of resulting polynomial $= \ell^{2d} = o(\sqrt{n})$ [if $\ell = o(n^{1/2d})$]
- if $S \leq 2^{o(n^{1/2d})}$ then get that C is <u>simple</u>

<u>Lemma 2:</u> Parity is not simple.

Proof: linear algebra argument: Assume parity simple.

- will use $\text{parity}(\bar{x}_1, \ldots \bar{x}_n) = \prod_{i=1}^{n} \bar{x}_i$.
- Consider space of functions $\mathcal{F} = \{f : S \to \mathbb{F}_3\}$

So $\bar{x}_i \in \{-1, 1\}$
$S \subseteq \{-1, 1\}^n$
$|S| \geq \frac{3}{4} \cdot 2^n$.

- $\dim(\mathcal{F}) = |S| \geqslant \frac{3}{4} \cdot 2^n$
- consider monomial $M = \prod_{i \in T} \bar{x}_i$.

Claim $\deg(M) \leq \frac{n}{2} + o(\sqrt{n})$ [on S]

Proof: either $|T| \leq \frac{n}{2}$ & we are done

or $$\prod_{i \in T} \bar{x}_i = \underbrace{\prod_{i=1}^{n} \bar{x}_i}_{} \cdot \prod_{i \notin T} \bar{x}_i$$

$$= p(\,) \cdot \underbrace{\prod_{i \notin T} x_i}_{\leq o(\sqrt{n}) + \leq \frac{n}{2}}$$

$\deg \frac{n}{2} + o(\sqrt{n})$. ⊠

- $\Rightarrow$ all functions from $S \to \mathbb{F}_3$ generated by monomials of deg $\leq \underbrace{\frac{n}{2} + o(\sqrt{n})}_{\frac{n}{2}+o(\sqrt{n})}$.

But size of set $\leq \sum_{i=0}^{\frac{n}{2}+o(\sqrt{n})} \binom{n}{i}$

$$= 2^{n-1} + \sum_{i=\frac{n}{2}+1}^{\frac{n}{2}+o(\sqrt{n})} \binom{n}{i}$$

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

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

Contradiction ! (concludes parity $\notin AC^0$) $\times$

Tighter result [Håstad] : $S > 2^{n^{\frac{1}{d+1}}}$

Idea: • Use "random restrictions" [Furst-Saxe-Sipser]

- Randomly leave x_i variable w.p. p, set to 0 w.p. $\frac{1-p}{2}$ (ind. for each i) set to 1 w.p $\frac{1-p}{2}$.
- Converts $par_n \to par_{pn}$ [not much simpler]
- converts depth d ckt $\to$ depth $d-1$. [only slightly larger].

"Switching lemma"

[Done [Håstad] style - optimal!]

Rest of lecture: Overview of TODA's Thm

Thm: $\forall i \quad \Sigma_i^P \subseteq P^{\#P}$

Proof overview:

- Will setup a collection of operators on complexity classes
- Will show basic calculus.

Operators: co-, $\exists$, $\forall$, BP, $\oplus$

- $co\text{-}\mathcal{C} = \{co\text{-}L \mid L \in \mathcal{C}\}$

  $co\text{-}L = \{x \mid x \notin L\}$

- $\exists \cdot \mathcal{C} = \{\exists \cdot L \mid L \in \mathcal{C}\}$

  $\exists \cdot L = \{x \mid \exists y \text{ s.t. } (x,y) \in L\}$

- $\forall \cdot \mathcal{C} = \{\forall \cdot L \mid L \in \mathcal{C}\}$

- $\oplus \cdot \mathcal{C} = \{\oplus \cdot L \mid L \in \mathcal{C}\}$

  $\oplus \cdot L = \{x \mid \underset{y}{\oplus} L(x,y) = 1\}$

- $\mathrm{BP}\cdot\mathcal{C} = \bigcap_{\text{poly } p} \left\{ \mathrm{BP}_p \cdot L \mid L \in \mathcal{C} \right\}$

$$\left(\mathrm{BP}_p \cdot L\right)_Y = \left\{ x \mid \Pr_y\left[(x,y)\in L\right] \geq 1 - 2^{-p(n)} \right\}$$

$$\left(\mathrm{BP}_p \cdot L\right)_N = \left\{ x \mid \Pr_y\left[(x,y)\in L\right] \leq 2^{-p(n)} \right\}$$

Operator Calculus

- $\exists\cdot\exists\cdot\mathcal{C} = \exists\cdot\mathcal{C}$
- $\forall\cdot\forall\cdot\mathcal{C} = \forall\cdot\mathcal{C}$
- $\mathrm{co}\text{-}\exists\cdot\mathcal{C} = \forall\cdot\mathcal{C}$

} trivial

- $\mathrm{BP}\cdot\mathrm{BP}\cdot\mathcal{C} = \mathrm{BP}\cdot\mathcal{C}$
- $\oplus\cdot\oplus\cdot\mathcal{C} = \oplus\cdot\mathcal{C}$

} similarly

- $\mathrm{co}\cdot\mathrm{BP}\cdot\mathcal{C} = \mathrm{BP}\cdot\mathrm{co}\cdot\mathcal{C}$
- $\mathrm{co}\cdot\oplus\cdot\mathcal{C} = \oplus\cdot\mathrm{co}\cdot\mathcal{C}$

} simple

(so far nothing interesting)

Key: $\exists\cdot\mathcal{C} \subseteq \mathrm{BP}\cdot\oplus\cdot\mathcal{C}$

[Valiant-Vazirani ?
Razborov-Smolensky ?
will see ...]

Corollary: $\Sigma_i^P = \underbrace{\exists \cdot \forall \cdot \exists \cdots}_{i} \cdot P$

$\subseteq$ $\underbrace{BP \cdot \oplus P \cdot BP \cdot \oplus P \cdots BP \cdot \oplus P}_{i \text{ times}} \cdot P$

Half-Key: $\oplus P \cdot BP \cdot C \subseteq BP \cdot \oplus P \cdot C$ (switching lemma) ☺

Corollary': $\forall i \quad \Sigma_i^P \subseteq BP \cdot \oplus P \cdot P$

Lemma 2: $BP \cdot \oplus P \cdot P \subseteq P^{\#P}$

(non-trivial, different from all above, but less important)

Will see proofs of Key, Half-Key & Lemma 2 next lecture.