Computational Complexity: Lecture 31.

Agenda: An explicit unconditional lower bound

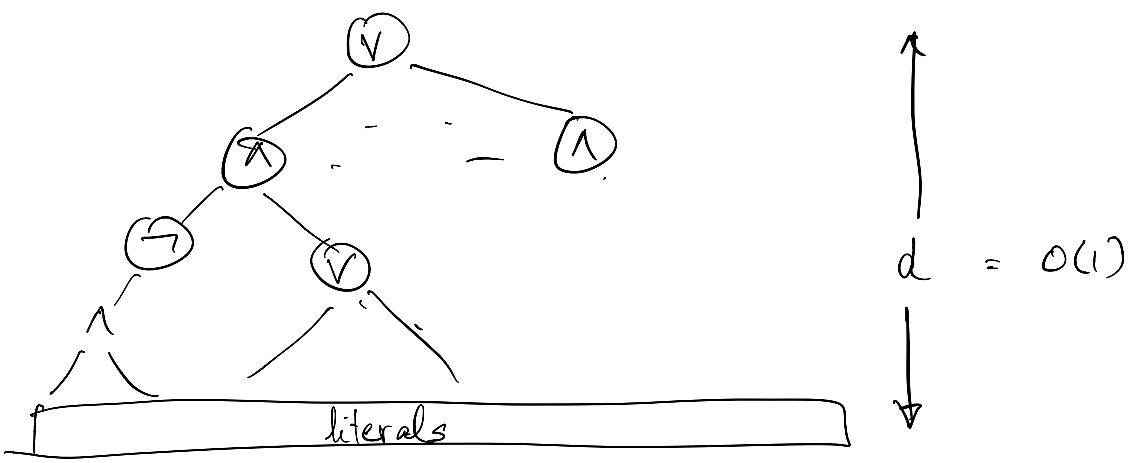
(albeit for a really simple model).

The Holy Grail: Prove SAT takes superpoly ~~time~~ size. $NP \not\subseteq P/poly$. $P \neq NP$

(If you believe in this...)

Can we prove lowerbounds for simpler models?

Very very restricted circuits: constant depth circuits.



AC^0 circuits: $\{C_i\}$

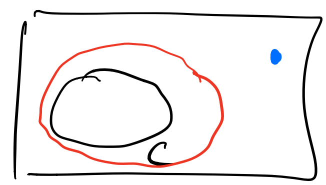
- Gates are $\wedge, \vee, \neg$
- $\text{depth}(C_i) = O(1)$
- fan-in of gates are arbitrary.

$L \subseteq \{0,1\}^n$ is in AC^0 if there is a poly size AC^0 ckt family computing it.

Qn: Can we at least prove lower bounds for these things?
(ie) Can we find $f: \{0,1\}^* \to \{0,1\}$ that requires large const. depth circuits?

How do you prove such lower bounds?

- Identify a weakness for the model.
- Quantify this weakness.
- Find a function that does not share this weakness.



Some weakness for AC^0:

- If you set a few vars to random values, the circuit seems to simplify a lot. (random restriction)
- Pick $x \in_R \{0,1\}^n$ and pick $i \in [n]$
  $$f(x) \approx f(x^{\oplus i}) \qquad \text{(influence)}$$

Candidate hard fn: PARITY

Razborov: "Any AC^0 fn looks like a low degree polynomial"
(it is not spikey)

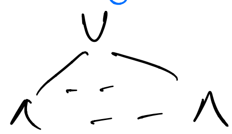
PARITY is not so.

[Ajtai, Furst-Saxe-Sipser, . . . Razborov, Smolensky, . . ., Håstad]

Thm: Any AC^0 circuit family computing PARITY must
[Håstad] have size $s \geq \exp_2\left(\Omega\left(n^{1/d-1}\right)\right)$

What is the "right" answer?

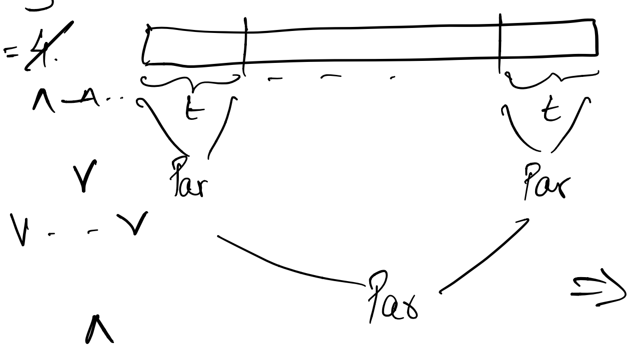
$d = 2$



DNF or CNF

2^{n-1}

$d = \cancel{4}\ 3$



$\frac{n}{t} 2^{t-1} + 2^{n/t - 1}$
$= 2^{O(\sqrt{n})}$

$\Rightarrow d = 3$. $2^{O(\sqrt{n})}$

In general, for depth d: $2^{O(n^{1/d-1})}$

$\Rightarrow$ Håstad's l.b is optimal.

– Switching lemma

This class: a weaker lower bound of $\exp\left(\Omega\left(n^{1/2(d-1)}\right)\right)$
by Razborov & Smolensky.

Roadmap:

(1) Show every "small" AC^0 is approximated by a low degree polynomial over $\mathbb{F}_3$.

(2) PARITY requires large degree even to approximate it.

$f: \{0,1\}^n \longrightarrow \{0,1\}$ $\qquad\qquad$ $\tilde{f}: \mathbb{F}_3^n \longrightarrow \mathbb{F}_3$

$\tilde{f}(x_1, \ldots, x_n)$

Candidate defn: $\tilde{f}$ ε-approximates f if

$$\Pr_{x \in \{0,1\}^n} [f(x) \neq \tilde{f}(x)] \leq \varepsilon.$$

not work.

Defn: (Randomised polynomials): $P(x, r)$ is a randomised deg d polynomial if $\forall\, r \in \{0,1\}^m$,

$$P(x, r) = p_r(x) \in \mathbb{F}_3[x_1, \ldots, x_n] \text{ of deg } d.$$

We will say $P(x, r)$ ε-approximates $f: \{0,1\}^n \to \{0,1\}$ if

$$\forall x: \quad \Pr_r [P(x, r) = f(x)] \geq 1 - \varepsilon.$$

Eg: $OR(x_1, \ldots, x_n)$ $\qquad\qquad$ $P(x, r) = 1$

Does this ε-approx OR? No!

Always errs on 0^n.

$$P(x, r_1, \ldots, r_n) = (x_1 r_1 + \cdots + x_n r_n)^2 \qquad r_i \in_R \mathbb{F}_3$$

$$x = 0^n \Rightarrow P(x, r) = 0 \qquad \forall r.$$

What if $x \neq 0^n$? $\Pr_r[r_1x_1+\dots+r_nx_n = 0 \bmod 3] \leq 1/3$.

$\Rightarrow \Pr_r[P(x,r)=1] \geq 2/3$

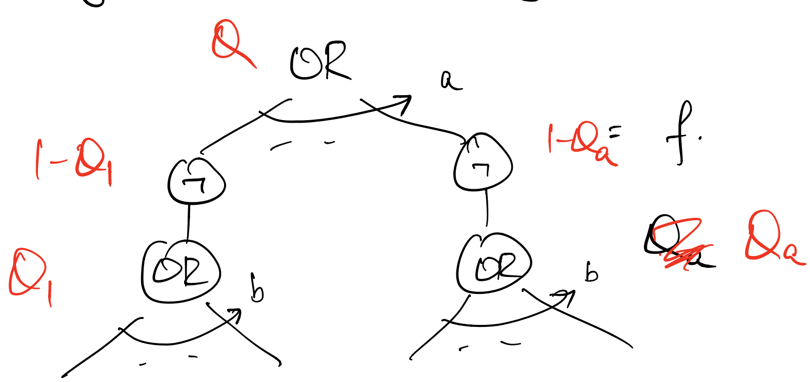
What about smaller ε?

$Q(x,r)$ $\quad 1-(1-P(x,r^{(1)}))\cdots(1-P(x,r^{(k)}))$

error $\leq \left(\frac{1}{3}\right)^k = \varepsilon \qquad k = O(\log \frac{1}{\varepsilon})$

degree $(Q) = O(\log \frac{1}{\varepsilon'})$

Eg:



$\tilde{Q} = Q(1-Q_1, \dots, 1-Q_a)$

What is the error here? Fix an input x.

$\Pr_r[\tilde{Q}(x) \neq f(x)] \leq (a+1)\varepsilon' \leq \varepsilon$

$\Rightarrow$ each Q_i and Q have deg $O(\log \frac{a}{\varepsilon})$

$\Rightarrow$ deg $\tilde{Q} \leq O((\log \frac{a}{\varepsilon})^2)$

Corollary: If f is computed by a size s, depth d circuit, then there is a randomised poly $\mathcal{P}(x,r)$ of $\deg \leq O(\log^d s)$ that $1/4$-approximates f.

Pf:

Each $Q^{(i)}$ is an ε'-app where $\varepsilon' < \frac{1}{4s}$

$\Rightarrow \deg Q^{(i)} \leq O(\log s)$

$\deg \tilde{Q} = O((\log s)^d)$

$\square$

What's left to show:

Lemma: Any randomised poly $\mathcal{P}(x,r)$ that $1/4$-approximates PARITY has $\deg \geq \sqrt{n}/1000$ over $\mathbb{F}_3$.

Let's assume this and finish the theorem.

Suppose C is a depth d ckt computing PARITY_n.

- C can be $1/4$-app by a $O((\log s)^d)$-deg rand. poly.
- C cannot be $\frac{1}{4}$-approx by $\deg \leq \frac{\sqrt{n}}{1000}$

$$\Rightarrow C(\log s)^d \geq \frac{\sqrt{n}}{1000} \Rightarrow s \geq 2^{n^{1/2d} \cdot 1000 \cdot c} = 2^{\Omega(n^{1/2d})}$$

$\square$

Pf of lemma: In $\mathbb{F}_3$

We'll prove that for any $p(x)$ s.t

$$\Pr_x [p(x) = \text{PARITY}(x)] \geq \frac{3}{4} \quad (*)$$

$$\Rightarrow \deg(p) \geq \sqrt{n}/1000$$

(why is this enough?)

$$Q(x_1, .., x_n) = P\left(\frac{1-x_1}{2}, \ldots, \frac{1-x_n}{2}\right)$$

$$-1 \xrightarrow{\frac{1-x}{2}} 1$$

$$1 \to 0$$

$\deg Q = \deg(P)$ $\quad x \in \{-1,1\}^n$

$$(*) \Longrightarrow \Pr_{x \in \{-1,1\}^n}\left[Q(x) = \prod_{i=1}^n x_i\right] \geq \frac{3}{4}.$$

$A = \{x \in \{-1,1\}^n : Q(x) = \prod x_i\}$ $\quad |A| \geq \frac{3}{4} \cdot 2^n.$

Claim: Consider any $f(x_1, .., x_n) \in \mathbb{F}_3[\bar{x}]$. Then, there is a poly $g(x_1, .., x_n)$ of $\deg \leq \deg(Q) + n/2$.

s.t $f(x) = g(x) \;\; \forall \; x \in A$.

Pf: Monomial by monomial.

	f	g.
	x_i^2	1
$\lvert S\rvert \leq \frac{n}{2}$:	$\prod_{i \in S} x_i$	$\prod_{i \in S} x_i$

$|S| \geq \frac{n}{2}$ $\quad \prod_{i \in S} x_i = \prod_{i \notin S} x_i \cdot Q(x).$

$$\deg(g) \leq \frac{n}{2} + \deg(Q).$$

$\square$.

$\mathcal{F} = \{ f : A \to \mathbb{F}_3 \ : \ \text{a polynomial fn} \}.$

How many different functions are there? $3^{|A|}$

Vector space, of dim $|A|$

But claim above says $\mathcal{F}$ is "spanned" by sq. free monomial of deg $\leq \frac{n}{2} + \frac{\sqrt{n}}{1000} = r$

$$\Rightarrow 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r} \geq \frac{3}{4} \cdot 2^n.$$

$$\underbrace{\sum_{i=0}^{n/2} \binom{n}{i}}_{\frac{1}{2} \cdot 2^n} + \sum_{i=n/2+1}^{n/2 + \frac{\sqrt{n}}{1000}} \binom{n}{i}$$

$$\wedge|$$

$$\binom{n}{n/2} \cdot \frac{\sqrt{n}}{1000}$$

$$\frac{2^n}{\cancel{\sqrt{n}}} \cdot \frac{\cancel{\sqrt{n}}}{1000}$$

$\square$.