(Circuit) Lower Bounds

- It's believed that $NP \neq P$.
  One way to prove it could be to show a stronger result: $SAT \notin P/poly$.
  It's a more "algebraic" question.

- This approach was tried in the 70/80s & lower bounds, for special circuit models, were proved.
  Probabilistic methods were used!

Defn: • $AC^0 := \{ L \subseteq \{0,1\}^* \mid \exists$ poly(n)-size, $O(1)$-depth boolean circuits solving $L \}$.

• **Modular gate** $mod_m : \{0,1\}^m \to \{0,1\}$

$(x_1, \dots, x_m) \mapsto \begin{cases} 1, & \text{if } \sum x_i \not\equiv 0 \bmod m \\ 0, & \text{else} \end{cases}$

• AC^0 **with Counters**, $ACC^0[m] := \{ L \subseteq \{0,1\}^* \mid$ $\exists$ poly(n)-size, $O(1)$-depth boolean circuits, using mod_m-gate, solving $L \}$

Qn: $AC^0 \overset{?}{=} ACC^0[2]$ ($ACC^0[1]$)? $mod_2 \notin AC^0$?

(parity)

↖ sensitive to each of the n-bits.

- In general, we suspect $\mathrm{mod}_m \notin \mathrm{ACC}^0[m']$ for coprime m, m'.

Theorem [Razborov '87, Smolensky '87]: For primes $p \neq q$, $\mathrm{mod}_p \notin \mathrm{ACC}^0[q]$.

Pf: • **Idea:** "Approximate" an $\mathrm{ACC}^0[q]$ circuit by a polynomial over $\mathbb{F}_q$.

• We'll exhibit the proof for $p=2$ & $q=3$.

Lemma 1: Let $C(\bar{x})$ be a depth-d $\mathrm{ACC}^0[3]$ circuit on n inputs & size-s. Then, $\exists$ polynomial in $\mathbb{F}_3[\bar{x}]$ of deg $\leq (2t)^d$ which agrees with $C(\bar{x})$ on $\geq (1 - \frac{s}{2^t})$-

fraction of the inputs $\bar{x} \in \{0,1\}^n$.

<u>Lemma 2:</u> No polynomial, in $\mathbb{F}_3[\bar{x}]$, of deg $\leq \sqrt{n}$ can agree with mod_2 on ≥ 0.99 fraction of inputs.

- If mod_2 has size-s $ACC^0[3]$ circuit, then by Lemma-1 for $\ell := \lfloor \frac{1}{2} n^{1/2d} \rfloor$, $\exists$ polynomial, of deg $\leq (2\ell)^d \leq \sqrt{n}$, agreeing with mod_2 on $\geq \left(1 - \frac{s}{2^\ell}\right)$ fraction of inputs.
- By Lemma 2, $1 - s/2^\ell < 0.99 \Rightarrow s > 0.01 \times 2^\ell > 2^{n^{1/2d}/3}$
  $\Rightarrow mod_2 \notin ACC^0[3] \Rightarrow$ parity $\notin AC^0$. $\square$

- Remark: In fact, any depth-d smaller than $o(\lg n/\lg\lg n)$ will work.

("small-oh")

$\therefore$ $n^{1/d} = \omega(\lg n)$ iff $\frac{1}{d}\lg n = \omega(\lg\lg n)$ iff $d = o(\lg n/\lg\lg n)$.

- Proof of Lemma 1:
  - We construct an approximator, in $\mathbb{F}_3[\bar{x}]$, for circuit C by induction on size.
  - Let g be a gate in C at height h.
  - Define approximator $\tilde{g}$ of deg $\leq (2e)^h$ s.t. $\tilde{g}(\bar{x}) = g(\bar{x})$ for "most" $\bar{x} \in \{0,1\}^n$.

1) g is NOT gate: Say, $g = \neg f$ for some gate f at height $(h-1)$. By induction hypothesis f has an approximator $\tilde{f}$, of deg $\leq (2\ell)^{h-1}$.

Define $\tilde{g} := 1 - \tilde{f}$

- Obviously, deg $\tilde{g} \leq (2\ell)^{h-1} < (2\ell)^h$ &
  $\tilde{g}$ doesn't introduce new errors.

2) g is mod_3 gate: Say, $g = mod_3(f_1, \ldots, f_k)$. By induction, $\exists$ approximators $\tilde{f}_1, \ldots, \tilde{f}_k$ of deg $\leq (2\ell)^{h-1}$.

Define $\tilde{g} := \left(\sum_{i \in [k]} \tilde{f}_i\right)^2$.

$\Rightarrow$ deg $\tilde{g} \leq 2 \cdot (2\ell)^{h-1} \leq (2\ell)^h$ & $\tilde{g}$'s definition introduces no new error.

3) <u>g is OR gate</u>: Say, $g = \bigvee_{i\in[k]} f_i$.

• Naive arithmetization gives $\tilde{g} := 1 - \prod_{i=1}^{k}(1-\tilde{f}_i)$. But, it increases the deg k times; too much.

Here, we need to use probability & approximation.

Pick a <u>random</u> set $S \subseteq [k]$ & consider $\underline{\mathrm{mod}_3}(f_i \mid i\in S)$.

<u>Claim</u>: $\forall \bar{x}\in\{0,1\}^n \Pr_{\phi\neq S\subseteq[k]}\left[\bigvee_{i=1}^{k} f_i = \mathrm{mod}_3(f_i \mid i\in S)\right] \geq \frac{1}{2}$

<u>Pf</u>:

• If $\forall i$, $f_i(\bar{x}) = \text{False}/0$, then $\Pr_S[\text{—}] = 1$.

- Otherwise, consider the linear form $L := \sum_{i \in [k]} f_i(\bar{x}) \cdot y_i$.
  L is a nonzero element of $\mathbb{F}_3[y_1, \ldots, y_k]$.
- It's easy to see: $\Pr_{\bar{y} \in \{0,1\}^k} [L(\bar{y}) \neq 0] = 1/2$.

  (∵ On fixing all y_i's except one, the last one's value gets fixed.)
- In other words, $\Pr_{\phi \neq S \subseteq [k]} [\, 1 \equiv \sum_{i \in S} f_i(\bar{x}) \bmod 3 \,] \geq \frac{1}{2}$. □
- To boost the probability we ℓ subsets $S_1, \ldots, S_\ell \subseteq [k]$
  & consider polynomial $\tilde{g}' := \mathrm{OR}\left(\left(\sum_{i \in S_1} \tilde{f}_i\right)^2, \ldots, \left(\sum_{i \in S_\ell} \tilde{f}_i\right)^2 \right)$.

  using $\tilde{g}$-defn. as given before

▷ $\deg \tilde{g}' \leq \ell \cdot 2 \cdot (2\ell)^{h-1} = (2\ell)^h$

▷ $\forall \bar{x}$, $\Pr_{S_1,\dots,S_\ell \subseteq [k]} [\tilde{g}' \neq \bigvee_{i \in [k]} f_i] \leq 1/2^\ell$.

· We deduce, $\exists\, S_1,\dots,S_\ell \subseteq [k]$, $\Pr_{\bar{x} \in \{0,1\}^h} [\tilde{g}' \neq \bigvee_{i=1}^{k} f_i] \leq 1/2^\ell$.

· Let's fix $S_1,\dots,S_\ell$ like this & denote the corresponding $\tilde{g}'$ as the final approximator $\tilde{g}$.

▷ $\deg \tilde{g} \leq (2\ell)^h$ & introduces errors $\leq 2^{-\ell}$ fraction.

4) g is AND gate: Say, $g = \bigwedge_{i=1}^{k} f_i$. So, $(\neg g) = \bigvee_{i=1}^{k} (\neg f_i)$.

⇒ Reduce to cases 1 & 3.

▷ By induction, the above four cases convert a circuit $C(x_1, \ldots x_n)$ to a polynomial in $\mathbb{F}_3[\bar{x}]$ of deg $\leq (2\ell)^d$; which disagrees with C on $\leq 8/2^\ell$ fraction of inputs in $\{0,1\}^n$. □

<u>Proof of Lemma 2:</u> • Suppose $f \in \mathbb{F}_3[\bar{x}]$ agrees with $\mathrm{mod}_2(x_1, \ldots x_n)$ on $G' \subseteq \{0,1\}^n$, with deg $f \leq \sqrt{n}$.

• Transform f to g as: $g(\bar{y}) := 1 + f(y_1 - 1, \ldots y_n - 1) \bmod 3$.

▷ $g: \{-1, +1\}^n \longrightarrow \{-1, 1\}$ & $f: \{1, 0\}^n \longrightarrow \{1, 0\}$ are <u>isomorphic</u> functions. G' converts to <u>$G \subseteq \{-1,1\}^n$</u>.

▷ deg $g \leq \sqrt{n}$ & $g(\bar{y}) = y_i \cdots y_n$ on $\bar{y} \in G$.

$\Rightarrow$ Intuitively, the deg $= \sqrt{n}$ polynomial g shouldn't approximate $y_1 \cdots y_n$ well! We'll formalize this.

- More generally, consider F_G — the set of $u : G \to \mathbb{F}_3$.
  Any $u \in F_G$ has a multilinear representation
  $u =: \sum_{I \subseteq [n]} a_I \cdot \prod_{i \in I} y_i$. [$\because G \subseteq \{-1,1\}^n$, so we can use the identity $y_i^2 = 1$, $\forall i \in [n]$]
- Replace each (deg $> n/2$)-monomial $\prod_{i \in I} y_i$ by $g \cdot \prod_{i \notin I} y_i$.
  [$\because g \cdot \prod_{i \notin I} y_i = \prod_{i \in [n]} y_i \cdot \prod_{i \notin I} y_i = \prod_{i \in I} y_i$.]
  deg $< (\frac{n}{2} + \sqrt{n})$

▷ $\forall u \in F_G$, u has a representation of deg $< n/2 + \sqrt{n}$.

$\Rightarrow \quad |F_G| \leq 3^m$, where $m := \#\{I \subseteq [n] \mid |I| < n/2 + \sqrt{n}\}$

& $|F_G| = 3^{|G|}$

$= \sum_{i < \frac{n}{2} + \sqrt{n}} \binom{n}{i} < 0.99 \times 2^n$. (Exercise)

$\Rightarrow |G| \leq m < 0.99 \times 2^n$.

$\Rightarrow$ No polynomial of deg $\leq \sqrt{n}$ agrees with $\mod_2$ on 99% of the inputs. □

→ $ACC^0[q]$ has low-deg approximators,

→ $\mod_p$ " high-deg " !