(Circuit) Lower bounds

- It is believed that $NP \neq P$.

  One way to prove that could be to show a stronger result: $SAT \notin P/poly$.

  It is a more algebraic question.

- This approach was tried in the 70/80s & lower bounds for special circuit models were obtained.

  Probabilistic methods were used!

Definition: • $\underline{AC^0} := \{L \subseteq \{0,1\}^* \mid \exists$ poly(n)-sized, $O(1)$-depth boolean circuits for $L\}$.

• **Modular gate** $\underline{mod_m}$: $\{0,1\}^n \longrightarrow \{0,1\}$;

$(x_1, \dots, x_n) \longmapsto \begin{cases} 1, \text{ if } \sum x_i \not\equiv 0 \pmod m, \\ 0, \text{ else.} \end{cases}$

• $\underline{AC^0 \text{ with counters}}$, $\underline{ACC^0[m]} := \{L \subseteq \{0,1\}^* \mid$ $\exists$ poly(n)-sized, $O(1)$-depth boolean circuit family, using mod_m gates, solving $L\}$.

– We would suspect $mod_2 \notin AC^0$, and in general, $mod_p \notin ACC^0[q]$ for distinct primes p, q.

Theorem (Razborov '87, Smolensky '87): For primes $p \neq q$, $mod_p \notin ACC^0[q]$.

Proof:

• Idea - "Approximate" an $ACC^0[q]$ circuit by

a polynomial over $\mathbb{F}_q$.

- We will exhibit the proof for $p=2, q=3$.

Lemma 1: Let C be a depth-d $ACC^0[3]$ circuit on n inputs and size-s.

There is a polynomial in $\mathbb{F}_3[\bar{x}]$ of deg $\leq (2\ell)^d$ which agrees with $C(\bar{x})$ on $\geq \left(1-\frac{s}{2^\ell}\right)$ fraction of the inputs.

allows us to make deg $\ll n$.

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

$\Rightarrow$ If mod_2 has a size-s $ACC^0[3]$ circuit then, by Lemma 1 for $\ell := \frac{1}{2} n^{1/2d}$, $\exists$ polynomial of deg $\leq \sqrt{n}$ agreeing with mod_2 on $\geq \left(1-\frac{s}{2^\ell}\right)$ fraction of the inputs.

Now, by Lemma 2, $1-\frac{s}{2^\ell} < 0.99$

$\Rightarrow \quad s > 0.01 \times 2^{\frac{1}{2} n^{1/2d}}$.

$\Rightarrow \mathrm{mod}_2 \notin \mathrm{ACC}^0[3]$. ($\Rightarrow$ parity $\notin AC^0$.)

- In fact, any depth d smaller than $\frac{\lg n}{(2+\varepsilon)\lg\lg n}$ will not work!

Proof of Lemma 1:

- We construct an approximator polynomial, in $\mathbb{F}_3[\bar{x}]$, for C by induction.
- Let g be a node in C at height h.
- We define a polynomial $\tilde{g} \in \mathbb{F}_3[x_1, \ldots, x_n]$ of deg $\leq (2\ell)^h$ s.t. $\tilde{g}(\bar{x}) = g(\bar{x})$ for "most" $(x_1, \ldots, x_n) \in \{0,1\}^n$:

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

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

· Obviously, $\deg(\tilde{g}) \leq (2\ell)^{h-1} < (2\ell)^h$.

Further, $\tilde{g}$ does not introduce any new error.

2) g is a mod_3 gate: Say, $g = \mathrm{mod}_3(f_1, \ldots, f_k)$.
By induction, $\exists$ approx. polys. $\tilde{f}_1, \ldots, \tilde{f}_k$ of $\deg \leq (2\ell)^{h-1}$.

Define $\tilde{g} := (\tilde{f}_1 + \ldots + \tilde{f}_k)^2$.

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

3) g is an OR gate: Say, $g = \bigvee_{i=1}^{k} f_i$.
A naive choice for $\tilde{g}$ could be $1 - \prod_{i=1}^{k} (1 - \tilde{f}_i)$. But, it increases the degree k times (which could be $\approx s$).

It is here that we will use the power of random choice & approximation.

Pick a random set $S \subseteq [k]$ and consider $\mathrm{mod}_3 (f_i \mid i \in S)$.

▷ $\forall \bar{x} \in \{0,1\}^n$, $\Pr_{\emptyset \neq S \subseteq [k]} \left[\bigvee_{i=1}^{k} f_i = \mathrm{mod}_3(f_i \mid i \in S) \right] \geq 1/2.$

Pf:

- If $f_i(\bar{x}) = \text{false}$, $\forall i \in [k]$, then obviously the probability is 1.
- For other $\bar{x}$'s, consider the linear form $L := \sum_{i=1}^{k} f_i(\bar{x}) \cdot y_i$, which is a nonzero element of $\mathbb{F}_3[y_1, \cdots, y_k]$.

- It is easy to see that
$$\Pr_{\bar{y} \in \{0,1\}^k} [\, L(\bar{y}) \neq 0 \,] \geq 1/2.$$

(Fix all $\bar{y}$'s but one, say y_i. This has at least one boolean value that keeps $L(\bar{y}) \neq 0$.)

- As $\bar{y}$ taking 0/1 values is the same as picking S, we get the result. □

- To boost the probability we pick ℓ subsets $S_1, \ldots, S_\ell \subseteq [k]$ & consider the

polynomial $\tilde{g}' := OR\left(\left(\sum_{i\in S_1}\tilde{f}_i\right)^2, \ldots, \left(\sum_{i\in S_\ell}\tilde{f}_i\right)^2\right)$,

where we use the arithmetized OR.

- $\deg(\tilde{g}') \leq \ell \cdot 2 \cdot (2\ell)^{h-1} = (2\ell)^h$.
- Also, $\forall \bar{x}$, most $\tilde{g}'$ work:

$$\Pr_{S_1,\ldots,S_\ell \subseteq [k]}\left[\tilde{g}' \neq \bigvee_{i\in[k]}\tilde{f}_i\right] \leq 1/2^\ell .$$

$\Rightarrow \exists\, S_1,\ldots,S_\ell \subseteq [k]$,

$$\Pr_{\bar{x}\in\{0,1\}^n}\left[\tilde{g}' \neq \bigvee_{i\in[k]}\tilde{f}_i\right] \leq 2^{-\ell}.$$

- Let us fix this $(S_1,\ldots,S_\ell)$ & denote the corresponding $\tilde{g}'$ by $\tilde{g}$.
- $\tilde{g}$ has $\deg \leq (2\ell)^h$ & introduces error in at most $2^{-\ell}$ fraction.

4) g is an AND gate: Say, $g = \bigwedge_{i=1}^{k} f_i$.
By de Morgan's law, $\neg g = \bigvee_{i\in[k]} \neg f_i$.

$\Rightarrow$ it reduces to cases 3 & 1.

▷ The above four cases, via induction, 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 $\leq \frac{s}{2^\ell}$ fraction of inputs.

□

Proof of Lemma 2:

- Suppose f agrees with $\mod_2$ on $G' \subseteq \{0,1\}^n$, with $\deg(f) \leq \sqrt{n}$.
- Transform f to g as:

$$g(y_1,\ldots,y_n) := 1 + f(y_1-1,\ldots,y_n-1) \pmod 3.$$

$\Rightarrow$ f's 0/1 input is g's $\pm 1/-1$ input, and the same holds for the output.

- Also, $\deg(g) \leq \sqrt{n}$ & $g = y_1 \cdots y_n$ on $G \subseteq \{1,-1\}^n$, where G corresponds to G'.

- Intuitively, a degree $\sqrt{n}$ polynomial should agree with $y_1 \cdots y_n$ on "few" inputs.

We will formalize this now.

- Consider F_G the set of $u: G \to \mathbb{F}_3$.
  Any $u \in F_G$ has a multilinear representation $u = \sum_{I \subseteq [n]} a_I \cdot \prod_{i \in I} y_i$ (using $y_i^2 = 1$).

- Replace each deg $> \frac{n}{2}$ monomial $\prod_{i \in I} y_i$ by $g \cdot \prod_{i \notin I} y_i$, which is of degree $< \frac{n}{2} + \sqrt{n}$.
  (On G, $\prod_{i \in I} y_i = \prod_{i \in [n]} y_i \cdot \prod_{i \notin I} y_i = g \cdot \prod_{i \notin I} y_i$.)

$\Rightarrow \forall u \in F_G$, u has a representation in $\mathbb{F}_3[y_1, \ldots, y_n]$ of deg $< \frac{n}{2} + \sqrt{n}$.

$\Rightarrow 3^{|G|} = |F_G| \leq 3^m$,
where $m := \#\{I \subseteq [n] \mid |I| < \frac{n}{2} + \sqrt{n}\}$
$= \sum_{i < \frac{n}{2} + \sqrt{n}} \binom{n}{i} < 0.99 \times 2^n$.

$\Rightarrow |G| < 0.99 \times 2^n$

$\Rightarrow$ No polynomial of deg $\leq \sqrt{n}$ can agree with $\mod_2$ on $\geq 0.99 \times 2^n$ of the inputs. $\square$