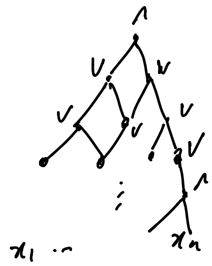
Next few lectures: Circuit Lowerbounds

OPEN

1. Show that SAT cannot be computed by
   - $O(n)$ size circuits.
   - $O(\log n)$ depth

Known

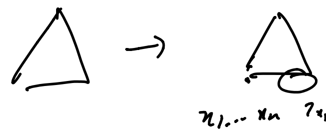
- Monotone
- Formulas
- ⋮
- Few alterations – today



alternations = # switches between ∨ and ∧ on every input – out put path.

Circuit has a alternations if ∀ path, c alternations.

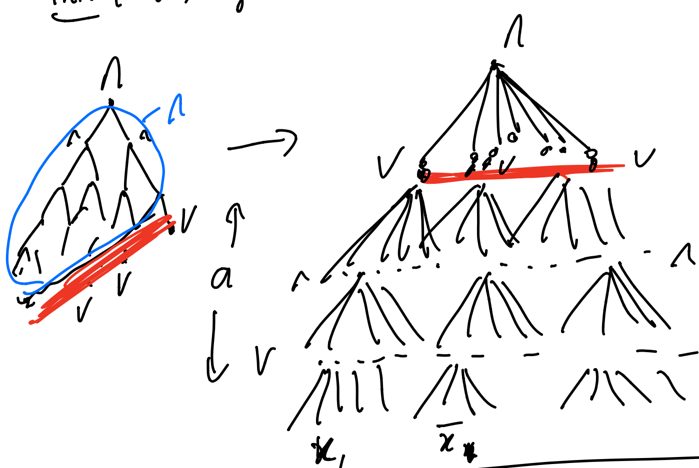
Claim:



Can make all negations at bottom

AC_0: poly sized circuits with $O(1)$ alternations.

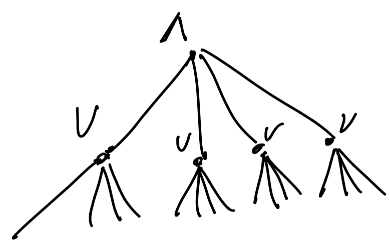
Thm [Hastad, Razborov, Smolensky] PARITY $\notin AC_0$



FACT: Every $f: \{0,1\}^n \to \{0,1\}$ can be computed by a SAT formula

$(x_1 \vee x_2 \vee \bar{x}_3 \vee x_4) \wedge (\vee \ \vee \vee \ ) \wedge (\ldots)$

size 2^n.



$$\text{PARITY}(x_1, \ldots, x_n) = \sum_i x_i \mod 2.$$

High level:

1. Small circuit for PARITY $\overset{\sim}{\longrightarrow}$ low-degree poly computing parity.
2. No such low degree poly can exist over $\mathbb{F}_3$.

Fix $\mathbb{F}_3$ as the field

① 

$$x_1 \vee x_2 \vee \dots \vee x_n \overset{\text{approx}}{\approx} 1 - \prod_{i=1}^{m} \left(1 - \left(\sum_{j \in S_i} x_j\right)^2\right) \quad \text{deg } 2m$$

Let $S_1, \dots, S_m \subseteq \{1, 2, \dots, n\}$ uniformly randomly

Claim: If $\bigvee_i x_i = 0 \Rightarrow \Pr\left[\sum_{j \in S_i} x_j = 0\right] = 1$ ①

If $\bigvee_i x_i = 1 \Rightarrow \Pr\left[\sum_{j \in S_i} x_j \neq 0\right] \geq 1/2$ ②

Pf: ① ✓

② Suppose $x_1 = 1$

$\forall\, T \subseteq \{2, \dots, n\}$

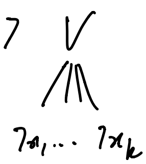
either $x_1 + \sum_{j \in T} x_j \neq 0$

or $\sum_{j \in T} x_j \neq 0$

Over $\mathbb{F}_3$ $\quad 2^2 = 1^2 = 1 \mod 3$.

Claim: $\Pr[\text{approx is correct}] \geq 1 - 2^{-m}$.

V ✓

$=$ $\neg$


$\neg x_1 = 1 - x_1$

Final degree:

$(2m)^a \approx O((\log n)^a)$

$\text{Prob}[\text{Approx is correct}]$

$\geq 1 - \underbrace{s}_{\#\text{gates}} \cdot 2^{-m}$

Set $m = 10 \log s = O(\log n)$ $\quad \geq 0.99$.

By averaging

$\exists$ a poly of deg $O(\log n)^a$ that computes PARITY on 99% of inputs $(0.99 \cdot 2^n)$

Let $x_1, \ldots x_n \in \{\pm 1\}^n$

$$x_1 \cdots x_n = 1 - 2 \cdot \text{PARITY}\left(\frac{1-x_1}{2}, \frac{1-x_2}{2}, \ldots, \frac{1-x_n}{2}\right) \tilde{\approx} f$$

$x_1 \to \frac{1-x_1}{2}$		PARITY $\to$	$1 - 2 \cdot$ PARITY
$1 \to 0$		$1 \to$	-1
$-1 \to 1$		$0 \to$	1

Let $T \subseteq \{\pm 1\}^n$ where

$x \in T \Rightarrow x_1 \cdots x_n = f(x_1, \ldots, x_n)$.

$|T| \geq (0.99)\, 2^n$

Count # functions $g : T \to \mathbb{F}_3$

$\geq 3^{|T|} = 3^{0.99 \cdot 2^n}$

On the other hand

Every such function can be computed by a deg. n polynomial

$$1_a(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{o.w} \end{cases}$$

$$1_a(x) = \frac{(x_1 - a_1 + 1)(x_1 - a_1 + 2)(x_2 - a_2 + 1)(x_2 - a_2 + 2) \cdots}{(1)(2)(1)(2) \cdots}$$

$$g(x) = \sum_{a \in T} g(a) \cdot 1_a(x)$$

$x_1 \cdots x_t$ if $t \leq n/2$ ✓

if $t \geq n/2$ $\quad x_1 \cdots x_t = x_1 \cdots x_n \cdot x_{t+1} \cdots x_n$

low degree $\quad \deg \le n/2$

$\deg \le n/2 + \mathrm{polylog}(n).$

$\# \text{ polys of such low deg} \le 3 \qquad \frac{2^n}{2} + \frac{\mathrm{polylog}(n)}{\sqrt{n}} \cdot 2^n$