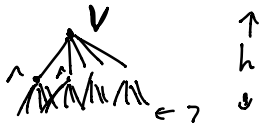
parity $\notin$ AC_0



Step 1: If $f \in AC_0$ then f can be "approximated" by a low-deg poly.

Step 2: Parity cannot be approximated by low-deg poly.

Step 1:

FACT: If $X \in \mathbb{F}_p$ $\quad X^{p-1} = \begin{cases} 1 & \text{if } X \neq 0 \\ 0 & \text{o.w.} \end{cases}$

$2^2 = 1 \mod 3$
$1^2 = 1 \mod 3$
$0^2 = 0 \mod 3$

Pick $S_1, \dots, S_\ell \subseteq \{1, \dots, k\}$

$$g_1 \vee g_2 \vee \cdots \vee g_k = 1 - \prod_{i=1}^{k} \left(1 - \left(\sum_{j \in S_i} g_j\right)^2\right)$$

with prob. $1 - 2^{-\ell}$ over choice of $S_1, \dots, S_\ell$.

$$g_1 \wedge \cdots \wedge g_k = \prod_{i=1}^{k} \left(1 - \left[\sum_{j \in S_i} (1 - g_j)\right]^2\right)$$

Set $\ell = (\log n)^2$

- Get poly f, $\deg f \leq (2\ell)^h \leq (2 \log n)^{2h}$.

$$\Pr[f(x_1, \dots, x_n) = \text{output of circuit}] \geq 1 - s \cdot 2^{-\ell}$$

$$\geq 0.99.$$

$\Rightarrow \exists f$, $\deg f \leq (2 \log n)^{2h}$,

$$\Pr_{x_1,\ldots,x_n}[f(x_1,\ldots,x_n) = \text{output}] \geq 0.99.$$

Step 2: Suppose f computes the parity.

$y_1,\ldots,y_n \in \{\pm 1\}$

$$y_1 \cdots y_n \overset{(1)}{\equiv}_{\bmod 3} f(y_1^{-1}, y_2^{-1}, \ldots, y_n^{-1}) + 1$$

$$1 = (-1)(1)(-1) = f(1,0,1)+1 = 1$$
$$-1 = (1)(1)(-1) = f(0,0,1)+1 = -1$$
$$-1-1 = -2 = 1 \bmod 3.$$

Let $T \subseteq \{+1,-1\}^n$ where (1) holds.

Step 1 implies $|T| \geq (0.99)\cdot 2^n$.

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

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

Claim:
Every function $g : T \to \mathbb{F}_3$
is a degree n polynomial. (with no x_i^2 terms)

Pf: For $a \in T$,

$$1_a = \prod_{i=1}^{n} \prod_{\substack{z_i \in \mathbb{F}_3 \\ z_i \neq a_i}} \frac{(x_i - z_i)}{(a_i - z_i)}$$

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

when $x_i \in \{\pm 1\}$ $x_i^2 = 1$

Claim: If $\deg f = d$, every function $g : \Gamma \to \mathbb{F}_2$ can be written as a poly of degree $\frac{n}{2} + d$.

Pf: $g = x_1 x_2 \cdots x_n + 2 \cdot x_1 x_2 \cdots x_{n-1} + \cdots$

$= f(x_1 - 1, \cdots, x_{n-1} - 1) + 1 + 2(x_1 \cdots x_n) \cdot x_n + \cdots$

$= f(\cdots) + 1 + 2(f(\cdots) + 1) \cdot x_n + \cdots$

$|S| > n/2$

$\prod_{i \in S} x_i = (x_1 \cdots x_n) \cdot \prod_{i \in S^c} x_i$

$$= (f(\cdots)+1) \prod_{i \in S^c} x_i$$

deg d ; deg $\le n/2$

of $g : T \to \mathbb{F}_3$

$$\le \#\text{ poly of deg } n/2 + d$$

$$= 3^{\sum_{i=0}^{n/2+d} \binom{n}{i}}$$

So,

$$|T| \le \sum_{i=0}^{n/2+d} \binom{n}{i}$$

$$= \frac{2^n}{2} + \sum_{i=n/2}^{n/2+d} \binom{n}{i}$$

$$\le \frac{2^n}{2} + O\left(d \cdot \left(\frac{2^n}{\sqrt{n}}\right)\right)$$

$$= 2^n \left(\frac{1}{2} + \Theta\left(\frac{d}{\sqrt{n}}\right) \right)$$

X ——————— X

Interactive Proofs

$f \in NP$ if $\exists V$

$f(x) = 1 \iff \exists w$ s.t $V(x,w) = 1$

Randomized Verifier (x) — Prover (x)

$m_1 \leftarrow$

$m_2 \rightarrow$

$m_3 \leftarrow$

$\vdots$

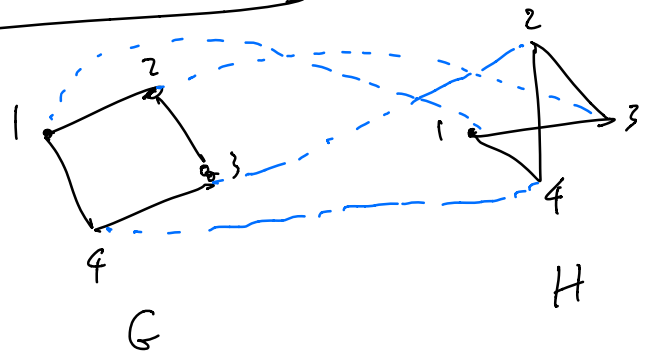
$V(x,w) = 1$

1. Completeness: if $f(x) = 1$, $\exists P$ s.t $\Pr[V^P(x) = 1] \geq 2/3$.
2. Soundness: if $f(x) = 0$, $\forall P$ $\Pr[V^P(x) = 0] \geq 2/3$.

Thm: $IP = PSPACE$.

$NP \subseteq IP = PSPACE$

Graph (non)-Isomorphism



$$Iso(G,H) = \begin{cases} 1 & \text{if } G, H \text{ are isomorphic} \\ 0 & \text{o.w} \end{cases}$$

$$\text{non } Iso(G,H) = \begin{cases} 0 & \text{if } G, H \text{ are isomorphic.} \\ 1 & \text{o.w.} \end{cases}$$

Thm: Graph non-iso $\in IP$

Verifier

1. $A = \begin{cases} G & \text{w.p } 1/2 \\ H & \text{w.p } 1/2 \end{cases}$
2. Randomly permute vertices of A to obtain B
3. Send B to prover.
4. Prover responds with Q
5. Accept if $Q = A$.