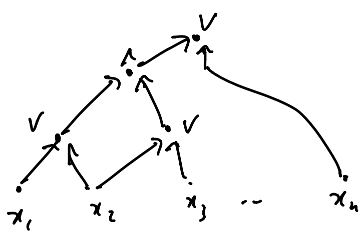
Schwartz-Zippel

If $f(x_1, \ldots, x_n)$ non-zero, has deg d, S

$$\Pr_{a_1, \ldots, a_n \in S} [f(a_1, \ldots, a_n) = 0] \le \frac{d}{|S|}.$$

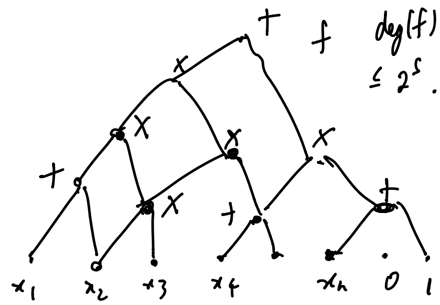
X ——————— X

Boolean Circuit



Arithmetic Circuit

Size = S



Identity testing

Given an arithmetic circuit of size computing $f(x_1, \ldots, x_n)$. Is $f \equiv 0$?

Algorithm: $S = \{1, 2, \ldots, 2^{2S}\}$

- Pick $a_1, \ldots, a_n \in S$ uniformly, prime $p \in \{1, 2, \ldots, 2^{S^2}\}$
- Evaluate $f(a_1, \ldots, a_n) \bmod p$.
- If $f(a_1, \ldots, a_n) = 0$ conclude $f \equiv 0$.

Claim: If $f \not\equiv 0$,

- $\Pr[f(a_1, \ldots, a_n) = 0] \le \frac{\deg(f)}{|S|} \le \frac{2^S}{2^{2S}} = 2^{-S}$. ✓
- $\Pr[f(a_1, \ldots, a_n) = 0 \bmod p] \le$ small.

FACT! Let $t(N)$ be the # of primes in $\{1, \ldots, N\}$. $\lim_{N \to \infty} \frac{t(N)}{N/\ln(N)} = 1$.

# of primes in $\{1, 2, \ldots, 2^{s^2}\}$

is $\sim \frac{2^{s^2}}{\ln(2^{s^2})} \geq \frac{2^{s^2}}{10 s^2}$

Proof of Correctness

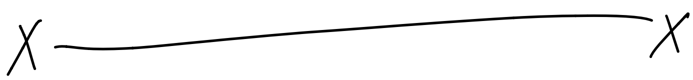
- $|f(a_1, \ldots, a_n)| \leq 2^{(2s)^s}$
- If t distinct primes divide $f(a_1, \ldots, a_n)$

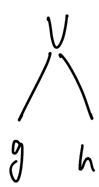
$\Rightarrow f(a_1, \ldots, a_n) \geq 2^t$

$\Rightarrow 2^{(2s)^s} \geq 2^t$

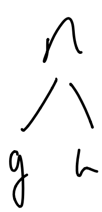
$\Rightarrow (2s)^s \geq t$

$$\Pr[\, f(a_1,\dots,a_n) = 0 \bmod p \mid f(a_1,\dots,a_n) \neq 0 \,] \le \frac{(2s)^s}{2^{s^2}/10s^2} \le 2^{O(s\log s) - s^2}.$$

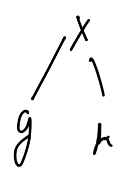




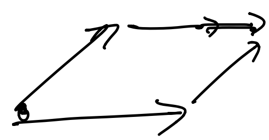
$\to \quad 1-(1-g)(1-h)$



$\to \quad g\cdot h$



$x_1^2 - x_1$



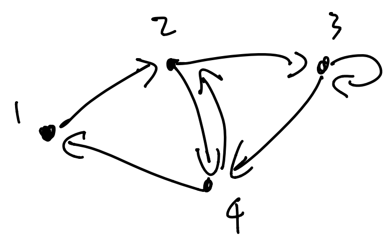
M: $n \times n$ matrix

$$\det(M) = \sum_{\pi} \operatorname{sign}(\pi) \prod_{i=1}^{n} M_{i,\pi(i)}. \quad \Big\} \text{ - can compute}$$

$$\operatorname{perm}(M) = \sum_{\pi} \prod_{i=1}^{n} M_{i,\pi(i)} \quad \Big\} \text{ no idea how to compute in less than } 2^n \text{ time.}$$

<u>Suppose</u> M is adjacency matrix of a graph

$\operatorname{perm}(M) = $ # cycle covers.



$(1\,2\,3\,4)$

$(1\,2\,4)\ (3)$

#P

$f : \{0,1\}^* \to \mathbb{Z}$ iff there is a polytime machine V and a poly p s.t $f(x) = |\{w \in \{0,1\}^{|p(n)|} : V(x,w) = 1\}|$

$\#3SAT(\phi)$: # satisfy assignments to ϕ.

<u>Thm</u>: Every $f \in \#P$ can be reduced to #3SAT in poly time

<u>Thm</u>: Every $f \in \#P$ can be reduced to perm in poly time.

HALT($\langle, x\rangle$)

$H(x) = \text{Halt}(y)$ where y is binary encoding of $|x|$.

$H(n)$ has poly sized circuits

$H(x) \notin EXP$.