05/11/21 : Randomized Computation

- fair coin toss

Probabilistic Turing Machines

Defn:- A probabilistic Turing machine (PTM) is a TM with two transition functions δ_0, δ_1.

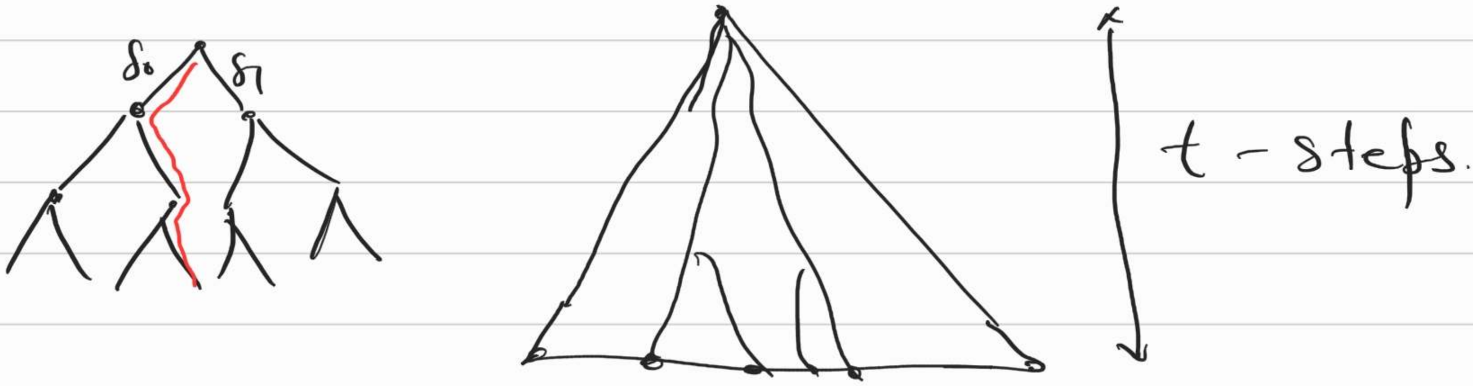
On an input x, the PTM in each step chooses to apply one of these transitions with prob. $1/2$.

These random choices are independent of each step.

For $T : \mathbb{N} \to \mathbb{N}$, we say that M runs in $T(n)$-time if for any input x, M halts on x within $T(|x|)$ steps regardless of the random choices.

x

M runs on x



$$\# \text{ computation paths} = 2^t$$

$$Pr[M(x) = 1] = \frac{\# \text{ accepting computation path}}{2^t}$$

$$Pr[M(x) = 0] = \frac{\# \text{ rejecting computation path}}{2^t}$$

We say that

M accepts x if $Pr[M(x)=1] \geq \frac{2}{3}$

M rejects x if $Pr[M(x)=0] \geq \frac{2}{3}$

Defn:- BPTIME($T(n)$): We say that a PTM M decides a language $L \subseteq \{0,1\}^*$ in Time $T(n)$ if for every $x \in \{0,1\}^*$, M halts in $T(|x|)$-time and

1) if $x \in L$, $Pr[M(x)=1] \geq 2/3$

2) if $x \notin L$, $\Pr[M(x)=0] \geq 2/3$

or, in other words, $\Pr[M(x)=1] \leq \frac{1}{3}$

<u>BPP</u> $:= \bigcup_{c>0} \text{BPTIME}(n^c)$

Bounded error Probabilistic Polynomial Time.

<u>Alternative Defn</u>:- DTM M, input x,

random string $r(x) \in \{0,1\}^{p(|x|)}$

(1) $x \in L \Rightarrow \Pr_{r \in \{0,1\}^{p(|x|)}}[M(x,r)=1] \geq 2/3$

(2) $x \notin L \Rightarrow \Pr_{r \in \{0,1\}^{p(|x|)}}[M(x,r)=0] \geq 2/3$.

<u>Primality testing</u>:

Given a number N, test whether N is prime or not.

<u>Input size</u>: $\log N$.

[AKS'04] - Primality testing $\in P$.

for every number N and $0 \le M < N$

$$QR(M) \pmod N = \begin{cases} 0 & \text{if } \gcd(M,N) \neq 1 \\ +1 & \text{if } M = A^2 \pmod N \\ & \text{and } \gcd(A,N) = 1 \\ -1 & \text{otherwise.} \end{cases}$$

Facts: (i) For every odd prime P and $M < P$

$$QR(M) \pmod P = M^{\frac{P-1}{2}} \pmod P$$

(ii) For an odd integer N, and $M < N$

Jacobi Symbol $\left(\frac{N}{M}\right) = \prod_{i=1}^{K} QR(M) \pmod{P_i}$

when $N = \prod_{i=1}^{K} P_i$.

(iii) For every odd composite N

no of M's $\in [1, N-1]$ s.t. $\gcd(N,M) = 1$ and

$\left(\frac{N}{M}\right) = M^{\frac{N-1}{2}} \pmod N$ is at most half. $\left(\le \frac{N}{2}\right)$

1) choose u.a.r. a number $M \le N-1$.

2) if $\gcd(M,N) > 1$ then reject.

3) if $\left(\frac{N}{M}\right) \neq M^{\frac{N-1}{2}} \pmod N$ then reject.

4) otherwise accept.

— Polynomial Identity test

Problem :- Given a multivariate polynomial $P(x_1, .., x_n)$. Test whether this polynomial is identically zero.

Identically zero : on every input this polynomial evaluates to zero.

$$P(x_1,..,x_n) = \sum_{(e_1,..,e_n) \geq 0} C_{(e_1,..,e_n)} \prod_{i=1}^{n} x_i^{e_i}$$

Coeffecient of a monomial.

$$Q(x_1, x_2, x_3, x_4) = 2x_1 + 3x_2^2 x_1 + 4 x_1^2 x_2 + 10 x_1 x_2 x_3 + 15 x_1^2 x_3 x_4 + 10$$

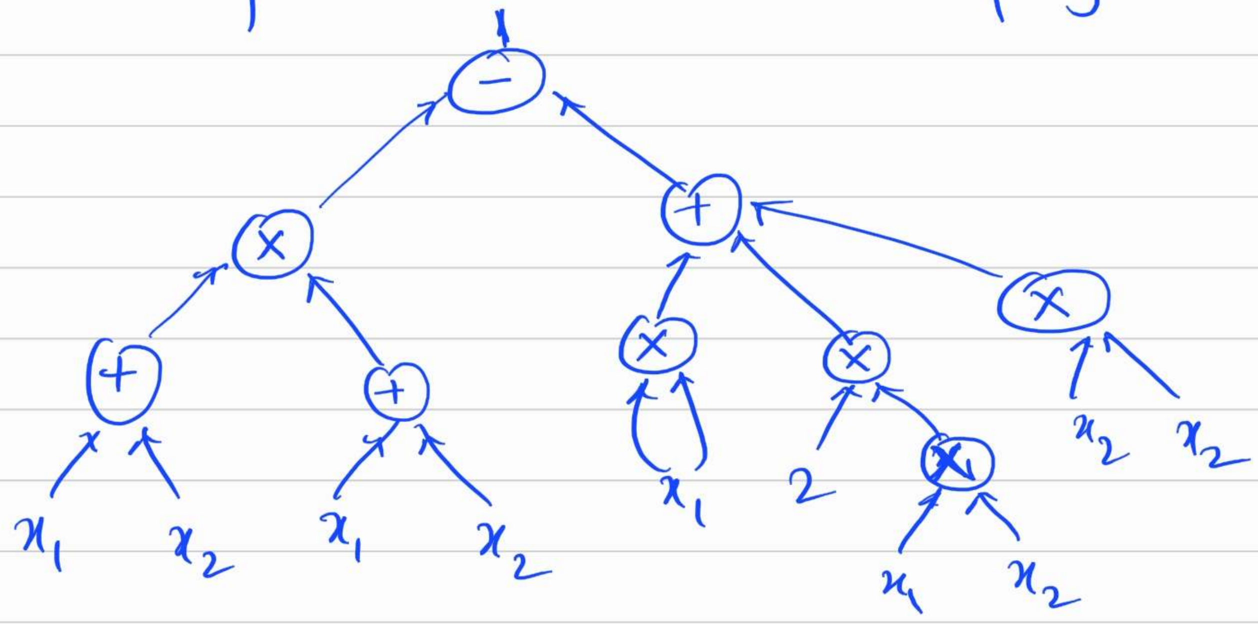
if every variable has deg $\leq d$. and no. of vars $\leq n$.

$(e_1, .., e_n)$ = defines a monomial.

$(d+1)^n$ = # monomial. potentially it can have.

if a polynomial evaluates to zero on every input then every coefficient in this polynomial equals 0.

In other words $Q(x_1, \ldots, x_n)$ is identically zero if it is a zero polynomial.



Arithmetic ckts. / Algebraic ckts.

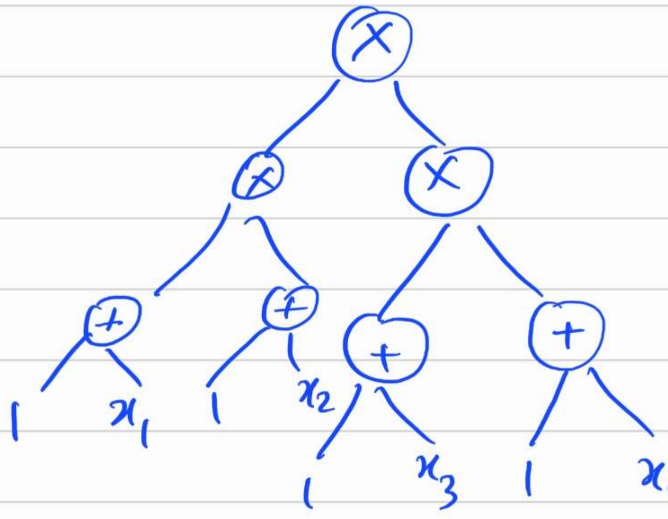
$$(x_1+x_2)^2 - x_1^2 - x_2^2 - 2x_1x_2 \equiv 0$$

Given an algebraic ckt of size s.

what is the maximum deg of the polynomial it computes?

$\deg \leq 2^s$.

degree can potentially double.



$(1+x_1)(1+x_2)(1+x_3)(1+x_4)$.

$\#$ monomials $\leq 2^4$.

$\prod_{i=1}^{n}(1+x_i)$: $\#$ monomials $\leq \underline{\underline{2^n}}$

$2n$ gate. $\prod_{i=1}^{n}(1+x_i) - x_1 x_2 \cdots x_n$

Fact :- Let $P(x_1, \ldots, x_m)$ be a non-zero polynomial of total degree $\leq d$.

Let F be a set of constants.

Then if $a_1, \ldots, a_m$ are chosen uniformly at random (with replacement) from F

then $\Pr_{a_1, \ldots, a_m}[P(a_1, \ldots, a_m) = 0] \leq \dfrac{d}{|F|}$

(Schwartz - Zipple - De Millo - Lipton Lemma)

returning to PIT problem

$\deg \leq 2^s$

$|F| \geq f = 2^{s+1}$

algo :- choose a random input $(a_1, \ldots, a_m)$ from F

Step 2: Evaluate the ckt at $(a_1, \ldots, a_m)$.

Step 3:- if $C(a_1, \ldots, a_m) \neq 0$ then reject.

Step 4:- Otherwise accept.

what is the prob. of failure?

Suppose C is identically zero

$\llcorner$ Alway accept.

Suppose C is not identically zero.

Prob. that you accept $\leq \frac{d}{|F|}$

$$\leq \frac{2^s}{2^{s+1}}$$

$$\leq \frac{1}{2}$$

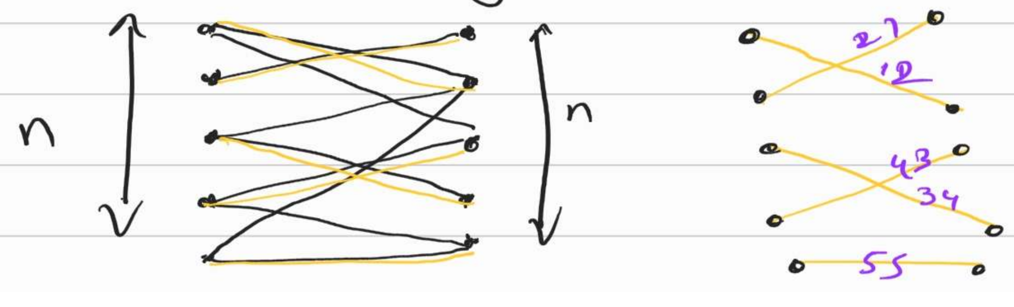
Is PIT $\in$ IP ? (OPEN).

$L := \{ P(x_1, \ldots x_m) \mid P(x_1, \ldots, x_m)$ is identically zero $\}$

Does $L \in$ co NP ? ✓

Does $\bar{L} \in$ NP ? ✓

— Perfect Matching in Bipartite graphs

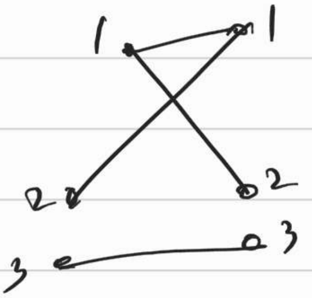


Perfecting Matching is a set of edges M s.t. every vertex in the graph has degree exactly 1 in M.

Problem :- Given a bipartite graph
Does it have a perfect matching?

$$\begin{array}{cc} & \begin{matrix} 1 & 2 & \cdots & \cdots & n \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ \vdots \\ n \end{matrix} & \begin{bmatrix} & & & & \\ & & & & \\ & & & 1/0 & \\ & & & & \\ & & & & \end{bmatrix} \end{array}$$

depending if there is an edge from i-th vertex on left to jth vertex on the right.



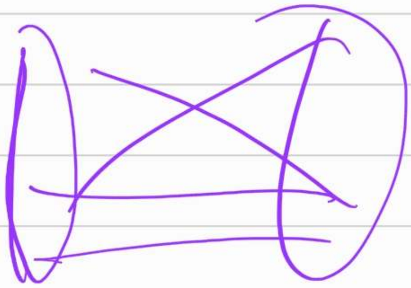
$$\begin{array}{cc} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array} \longrightarrow \begin{bmatrix} x_{11} & x_{12} & 0 \\ x_{21} & 0 & 0 \\ 0 & 0 & x_{33} \end{bmatrix}$$

$$\det\left(\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{bmatrix}\right)$$

$$:= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i\sigma(i)}$$

when $\sigma \in S_n$ is a permutation of $\{1, \dots, n\}$

and $\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if its even permutation} \\ -1 & \text{if its odd permut.} \end{cases}$



← Bipartite graph

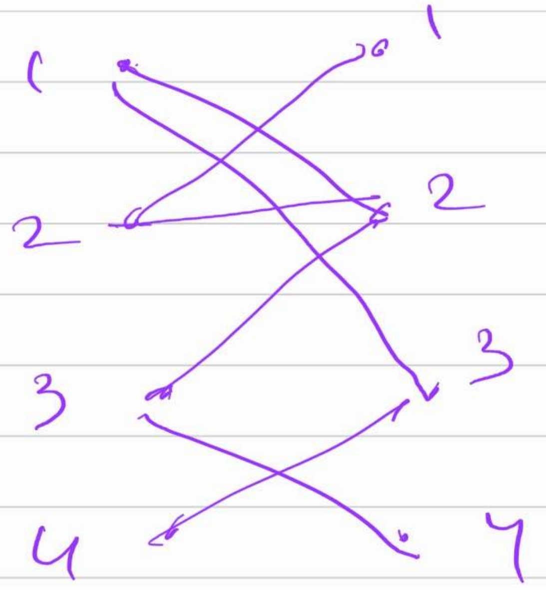
↓

[Adjacency matrix] → [Symbolic adjacency matrix]

$\begin{cases} 1 \rightarrow \text{distinct variables} \\ 0 \rightarrow 0 \end{cases}$

↓

determinant of this matrix

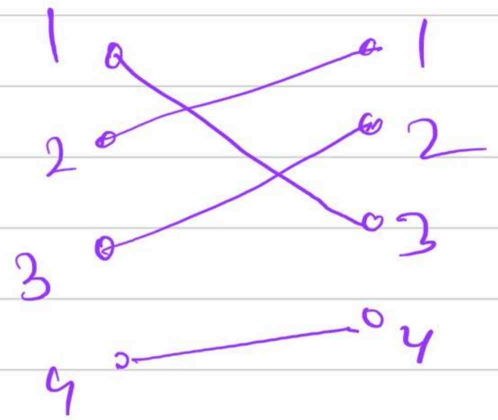


$$\begin{bmatrix} 0 & x_{12} & x_{13} & 0 \\ x_{21} & x_{22} & 0 & 0 \\ 0 & x_{32} & 0 & x_{34} \\ 0 & 0 & x_{43} & 0 \end{bmatrix}$$

$$\det(X) = \sum_{\sigma \in S_4} (\pm 1) \cdot \prod_{i=1}^{4} x_{i\sigma(i)}$$

different permutation will not cancel out.

permutation $\Longleftrightarrow$ perfect matching



$\det(X) \neq 0$

iff the bipartite graph has a perfect matching.

$\deg = n$.

just evalvate $\det(X)$ on a set of $2n$ integers.

if it outputs $\neq 0$ then perfect matching exist.

if it outputs $= 0$ then

(possibly perfect matching does n't exist).