# Polynomial Identity testing

Given $P$ and $Q$: test if $P = Q$ (i.e., test if $P - Q = 0$).

## Polynomial zeroes lemma: (Demillo-Lipton-Schwartz-Zippel)

Let $P$ be a $n$-variate non-zero polynomial of degree $d$. Let $S$ be a finite subset of $\mathbb{R}$. Let $\bar{a}$ be sampled randomly as follows - $\forall i \in [n]$ $a_i$ is chosen independently and uniformly at random. Then,

$$\Pr_{\bar{a}}[P(a_1, \ldots, a_n) = 0] \leq \frac{d}{|S|}.$$

# of zeroes $\leq d \cdot |S|^{n-1}$.

Proof: Induction on $n$.

Base case $n = 1$: $P$ is a univariate polynomial and thus has at most $d$ roots in $\mathbb{R}$.

$$\Rightarrow \Pr_{a}[P(a) = 0] \leq \frac{d}{|S|}.$$

Induction step: Let us express $P$ as follows.

$$P(x_1, \ldots, x_n) = \sum_{i=0}^{k} P_i(x_1, \ldots, x_{n-1}) \cdot x_n^i. \quad // \; k \leq d.$$

$$= P_k(x_1, \ldots, x_{n-1}) \cdot x^k + Q(x_1, \ldots, x_{n-1}, x_n).$$

As mentioned in the statement, $\bar{a} = (a_1, \ldots, a_n)$ be s.t each $a_i$ is chosen independently and uniformly at random.

$$\Pr_{\bar{a}}[P(a_1,\dots,a_n)=0] = \Pr[P(a_1,\dots,a_n)=0 \mid P_k(a_1,\dots,a_{n-1})=0]\cdot\Pr[P_k(a_1,\dots,a_{n-1})=0]$$
$$+ \Pr[P(a_1,\dots,a_n)=0 \mid P_k(a_1,\dots,a_{n-1})\neq 0]\cdot\Pr[P_k(a_1,\dots,a_{n-1})\neq 0]$$

Observation: If $P_k$ is $\neq 0$ at $(a_1,\dots,a_{n-1})$ then $P(a_1,\dots,a_{n-1},x_n)$ is a univariate polynomial in $x_n$ of degree $k$.

Thus, $\Pr_{\bar{a}}[P(a_1,\dots,a_n)=0 \mid P_k(a_1,\dots,a_{n-1})\neq 0] \leq \frac{k}{|S|}$.

Also, $\Pr_{\bar{a}}[P(\bar{a})=0] \leq \Pr[P(\bar{a})=0 \mid P_k(a_1,\dots,a_{n-1})\neq 0]\cdot 1$

$$+ 1\cdot\Pr[P_k(a_1,\dots,a_{n-1})=0].$$

Note: $P_k$ is a polynomial of degree at most $d-k$.

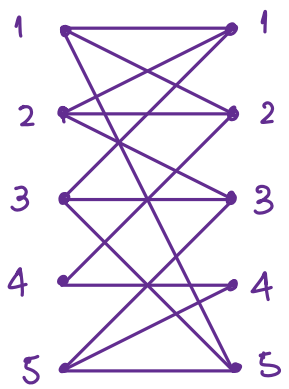
→ From induction hypothesis, this is at most $\frac{d-k}{|S|}$.

$$\Rightarrow \Pr_{\bar{a}}[P(\bar{a})=0] \leq \frac{k}{|S|} + \frac{d-k}{|S|} = \frac{d}{|S|}.$$

Remarkable that this bound does not depend on $n$.

## Bipartite graph perfect matching

$G=(L,R,E)$




Question: Given a bipartite graph, is there a perfect matching in it?

Various sequential algos are known for matching.

Can we parallelize this?

PIT: If $P \neq 0$ then $\exists \bar{a}$ w.h.p s.t $P(\bar{a}) \neq 0$.

Edmond's matrix: $X_G$.

$i,j \in [n]$: $X_{ij} = \begin{cases} x_{ij} & \text{if } \exists \text{ an edge } (i,j) \text{ s.t } i \in L \text{ and } j \in R; \\ 0 & \text{otherwise.} \end{cases}$

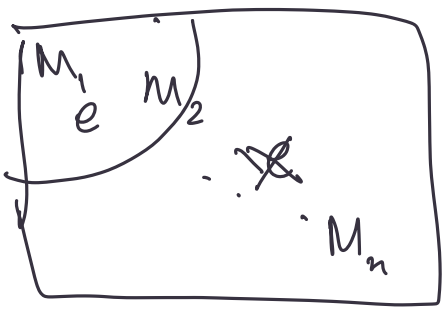
**Theorem:** Graph G has a PM iff $Det(X_G) \neq 0$ $\Rightarrow \exists A$ w.h.p s.t $Det(A) \neq 0$.

Proof sketch: Recall that $Det(X) = \sum_{\sigma \in S_n} sgn(\sigma) \cdot \prod_{i=1}^{n} x_{i\sigma(i)}$.

($\Rightarrow$) PM implies existance of a permutation for which each $x_{i\sigma(i)} \neq 0$. Thus $Det(X_G) \neq 0$. Note that monomials are distinct.

($\Leftarrow$) Non-zero det implies existence of a non-zero monomial. $\Rightarrow$ A permutation between the nodes.

## Algorithm for PM: (Sequential)




- $M \leftarrow \{\}$
- For each edge in E:

  Test if $G' = (L, R, E \setminus \{e\})$ has a PM.

  If "NO":

  $M \leftarrow M \cup \{e\}$.

  $E \leftarrow E \setminus \{e\}$.

- Return M.

Error

Running time = $m \cdot$ time (Det comput)
$= m \cdot O(n^3)$.

- Algorithm "refines"/"cuts down" the space of matchings to one.
- For different order of edges we could end up w/ different M

Theorem [Galil-Pan '85]: Let $A$ be a $n \times n$ matrix. Then $\text{Det}(A)$, $\text{adj}(A)$ and $A^{-1}$ can all be computed in $O(\log^2 n)$ time over $O(n^{3.5})$ processors.

$O(m \cdot \log^2 n)$ parallel.

## Parallel algorithm for PM:

Theorem [Mulmuley-Vazirani-Vazirani]: There is a randomized algorithm that finds a PM in $O(\log^2 n)$ time using $O(n^{3.5})$ processors w.p $\geq \frac{1}{2}$.

Key idea: Assign weights to the edges "randomly" and show that there is a unique PM of min weight (if a PM exists).

## Isolation lemma:

Let $S$ be any finite subset of $\mathbb{R}$. Let $T_1, \ldots, T_k$ be some subsets of $[m]$. For each $i \in [m]$, assign a weight $wt(i)$ independently and uniformly at random from $S$. Let weight of $T_j$ (for $j \in [k]$) $= \sum_{i \in T_j} wt(i)$. Then,

$$\Pr[\exists j \text{ s.t } T_j \text{ has unique min wt}] \geq 1 - \frac{m}{|S|}.$$

Proof: Suppose $T_j$ and $T_{j'}$ attain minimum wt.

Then $\sum_{i \in T_j} wt(i) = \sum_{i' \in T_{j'}} wt(i')$. Let $e \in T_j$ and not $T_{j'}$.

$$wt(e) + \sum_{\substack{i \in T_j \\ i \neq e}} wt(i) = \sum_{i' \in T_{j'}} wt(i').$$

We will now show that this happens w/ prob $\leq \frac{1}{|S|}$.

Let $E_i$ be an event s.t

b+wt(i) $\min_j \{ wt(T_j) \mid i \in T_j \} = \min_{j'} \{ wt(T_{j'}) \mid i \notin T_{j'} \}$. ← a

Suppose $\bigcap_{i=1}^{m} \bar{E}_i$ occurs then $\exists$ unique min wt $T_j$.

$$Pr\left[\bigcap_{i=1}^{m} \bar{E}_i\right] = 1 - Pr\left[\bigcup_{i=1}^{m} E_i\right] \geq 1 - \sum_{i=1}^{m} Pr[E_i]$$

For a fixed element $i$, let wts of all but $i$ are fixed. Let $a$ and $b$ be s.t

$$a = \min_j \{ wt(T_j) \mid i \notin T_j \}$$

$$b = \min_j \{ wt(T_j \setminus \{i\}) \mid i \in T_j \}$$

$\bar{E}_i$ ↓ ↓ $E_i$

$a = b + wt(i)$ ← random choice

$Pr[a = b + wt(i)] \leq \frac{1}{|S|}$ ✓

Thus, $Pr[E_i] \leq \frac{1}{|S|} \Rightarrow Pr\left[\bigcap_{i=1}^{m} \bar{E}_i\right] \geq 1 - \frac{m}{|S|}$

## Parallel algo of MVV :

Space of matchings $\longleftrightarrow$ Sets $T_1, \ldots, T_k$.

$m = |E|$.

- For each edge assign a weight $w$ independently and uniformly at random from $S$.

- Let the matrix $W$ be defined as follows.

$$W_{ij} = \begin{cases} 2^{wt(i,j)} & \text{if } \exists \text{ an edge } (i,j) \in E,\ i \in L \ \& \ j \in R; \\ 0 & \text{otherwise.} \end{cases}$$

$$\underline{Det}(W) = \sum_{\sigma \in S_n} sgn(\sigma) \cdot \prod_{i=1}^{n} W_{i\sigma(i)}$$

Each PM corresponds to a permutation.

$$= \sum_{\sigma \in S_n} sgn(\sigma) \cdot \prod_{\substack{i=1 \\ (i,\sigma(i)) \in E \ \forall i}}^{n} 2^{wt(i,\sigma(i))}$$

$M$ = space of matchings.

$$= \sum_{\substack{\sigma \in S_n \\ \sigma \in M}} sgn(\sigma) \cdot 2^{wt(M_\sigma)}$$

$\rightarrow$ $\exists \sigma$ s.t $M_\sigma$ attains min wt and $\forall \sigma' \neq \sigma$; $wt(M_{\sigma'}) > wt(M_\sigma)$

Observation: Wt of min matching is $r$ s.t $r$ is the max value s.t $2^r$ divides $Det(W)$.

$\rightarrow$ $Det(W) = sgn(M_1) \cdot 2^{wt(M_1)} + \cdots + sgn(M_t) \cdot 2^{wt(M_t)} = 2^{wt(M_0)} \left[ sgn(M_0) + rest \right]$

Lemma: Let $M_0$ be the unique min wt PM in $G$. Let $r = wt(M_0)$. Then

$(i,j) \in M_0$ iff $\dfrac{\det(W^{(i,j)}) \cdot 2^{wt(i,j)}}{2^r} = \dfrac{\det(w(i,j))}{2^{r - wt(i,j)}}$ is odd.

$W^{(i,j)}$ is obtained from $W$ by removing $i^{th}$ row and $j^{th}$ col.

## Algo:

$r = 2^r \mid \text{Det}(W)$.

1. Compute $\text{Det}(W)$ and obtain $r$.
2. For all edges $(i,j)$ in $E$ (in parallel):

   Compute $\dfrac{\text{Det}(W^{(i,j)}) \cdot 2^{wt(i,j)}}{2^r}$.

   If the result is odd then $(i,j) \in$ min wt matching.

$m \cdot n^{3.5}$ $(\log^2 n)$

## Proof of Lemma:

$M_1, \ldots, M_t$ be the PMs for graph $G$.

$$\text{Det}(W) = \text{sign}(M_1) \cdot 2^{wt(M_1)} + \cdots + \text{sign}(M_t) \cdot 2^{wt(M_t)}.$$

$$= 2^{wt(M_0)} \left[ \text{sgn}(M_0) + \sum_{\substack{M \neq M_0 \\ M \in \{M_1, \ldots, M_t\}}} \text{sgn}(M) \cdot 2^{wt(M) - wt(M_0)} \right]$$

Unique min wt guarantees that $wt(M) - wt(M_0) > 0$ $\forall M \neq M_0$.

$$\frac{\text{Det}(W)}{2^{wt(M_0)}} = \left[ \text{Sgn}(M_0) + \sum_{M \neq M_0} 2^{wt(M) - wt(M_0)} \cdot \text{Sgn}(M) \right].$$

is odd.