$\boxed{\text{PSPACE} = \text{IP}}$ ... $\boxed{\text{PERM} \in \text{IP}}$

$$\det(M) = \sum_{\sigma} \text{sign}(\sigma) \prod_{i=1}^{n} M_{i,\sigma(i)}$$ Can compute in time $O(n^3)$

$$\text{perm}(M) = \sum_{\sigma} \prod_{i=1}^{n} M_{i,\sigma(i)}$$ best alg is exp. time

#P : set of functions $f$ s.t $\exists$ poly $p(n)$, polytime machine $M$ with
$$f(x) = \left|\{y \in \{0,1\}^{p(|x|)} : M(x,y) = 1\}\right|$$

Thm: $\forall f \in \#P$ $\exists$ poly time $g, h$ s.t
$$f(x) = h(\text{PERM}(g(x))).$$

FACT: Given $a_0, b_0, a_1, b_1, \ldots, a_d, b_d$ where $a_0, \ldots, a_d$ are distinct $\exists$ unique deg $\le d$ polynomial $f(X)$ s.t $\forall i$ $f(a_i) = b_i$.
$$f(X) = \sum_{i=0}^{d} b_i \frac{\prod_{j \ne i} (X - a_j)}{\prod_{j \ne i} (a_i - a_j)}$$
$$f(a_{i'}) = b_{i'}.$$

Alg
1. Sample $X$
2. Compute $f(1), \ldots, f(n+1)$
⋮

$M$: $n \times n$ matrix, $p \geq 3n$, prime

Suppose we can compute $\text{PERM}(M)$ correctly on $1 - \frac{1}{3(n+1)}$ fraction of all matrices with entries from $\mathbb{F}_p$.

Consider $f(t) = \text{PERM}(M + tX)$ ($X$: random matrix)

degree of $f(t) \le n$.

$f(0) = \text{PERM}(M)$.

Compute $f(1), f(2), \ldots, f(n+1)$. ($\text{PERM}(M+X)$)

Prob that all comp. are correct
$$\geq 1 - \frac{n+1}{3(n+1)} \geq 2/3.$$

Algorithm

$M$
$$A_{i,j} = \begin{cases} -\sqrt{M_{ij}} & \text{with prob } 1/2 \\ +\sqrt{M_{ij}} & \text{with prob } 1/2 \end{cases}$$

Output $\det(A)^2$

Claim: $\mathbb{E}[\det(A)^2] = \text{perm}(M)$.

Pf:
$$\mathbb{E}\left[\left(\sum_{\sigma} \text{sign}(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)}\right)^2\right]$$
$$= \mathbb{E}\left[\sum_{\sigma,\sigma'} \text{sign}(\sigma) \cdot \text{sign}(\sigma') \prod_{i=1}^{n} A_{i\sigma(i)} \cdot A_{i,\sigma'(i)}\right]$$
$$= \mathbb{E}\left[\sum_{\sigma=\sigma'} \text{sign}(\sigma)^2 \prod_{i=1}^{n} A_{i\sigma(i)}^2\right] + \mathbb{E}\left[\sum_{\sigma \ne \sigma'} \cdots\right]$$
$$= \text{perm}(M) + \sum_{\sigma \ne \sigma'} \text{sign}(\sigma)\,\text{sign}(\sigma')\, \underbrace{\mathbb{E}\left[\prod_{i=1}^{n} A_{i,\sigma(i)} A_{i,\sigma'(i)}\right]}$$

if $\sigma \neq \sigma' \Rightarrow \exists j$ s.t $\sigma(j) \neq \sigma'(j)$

$$\mathbb{E}[\Pi] = \underbrace{\mathbb{E}[A_{j,\sigma(j)}]\,\mathbb{E}[A_{j,\sigma'(j)}]}_{0} \cdot \mathbb{E}\Big[\prod_{i \neq j} \cdots\Big]$$

$= \text{perm}(M)$.

---

**IP** : interactive proofs.

$f \in IP$ means

$\exists$ verifier with oracle access to $P$

s.t

If $f(x) = 1$ $\exists P$ s.t $\Pr[V^P(x) = 1] \geq 2/3$ — completeness

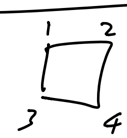
If $f(x) = 0$ $\forall P$ $\Pr[V^P(x) = 1] \leq 1/3$ — soundness.

---

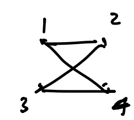
Graph non-isomorphism (GNI)

Input : $G, H$ graphs

Are they isomorphic?




isomorphic




__OPEN:__ Is $GNI \in NP$ ?

__$GNI \in IP$__

__Verifier__

1. Pick a random permutation $\sigma : [n] \to [n]$.
2. set $F = \begin{cases} G & \text{w.p } 1/2 \\ H & \text{w.p } 1/2 \end{cases}$
3. Send $\sigma(F)$ to prover
4. Prover says $F = G$ or $F = H$
5. Verifier accepts if prover is right.

$\boxed{\text{PERM} \in IP}$ Next time.