IP = PSPACE

IP ⊆ PSPACE ✓

Today: TQBF ∈ IP.

① PERM ∈ IP

Prover wants to convince verifier that $\text{Perm}(M) = k \pmod p$ (M is $n \times n$)

$$\text{Perm}(M) = \sum_{\sigma} \prod_{i=1}^{n} M_{i\sigma(i)}$$

Protocol

1. Prover will send verifier prime p with $p > 2^{n^2}$. $>> n!$
2. Prover sends $h(X) \stackrel{?}{=} \text{Perm}(D(X))$. (supposed to be)
3. Verifier check $M_{11} \cdot h(1) + \cdots + M_{1n} \cdot h(n) = k \pmod p$
4. Verifier: pick $a \in \mathbb{F}_p$ randomly, recursively check $h(a) = \text{Perm}(D(a))$.

If $h(X) \neq \text{Perm}(D(X))$,

$$\Pr_a[h(a) \neq \text{Perm}(D(a))] \geq 1 - \frac{n^2}{p}$$

Analysis: Only way prover succeeds if $\text{Perm}(M) \neq k$ is if in some round $h(a) = \text{Perm}(D(a))$

$$\Pr[\text{success}] \leq \frac{n^2}{p} \cdot n$$

Thm: $\pi(t)$: number of primes $\leq t$

$$\lim_{t \to \infty} \frac{\pi(t)}{t/\ln(t)} = 1.$$

primes p $2^n \leq p \leq 2^{2n}$ is $\Omega(2^n/n)$.

$$\text{perm}(M) = M_{11} \cdot \text{Perm}(M^{1,1}) + M_{12} \cdot \text{Perm}(M^{1,2}) + \cdots + M_{1n} \text{Perm}(M^{1,n})$$

$M^{1,i}$: $n-1 \times n-1$ matrix obtained by deleting 1st row i^{th} column.

$D(X)$: $n-1 \times n-1$ matrix whose entries are degree n polys. s.t

$D(i) = M^{1,i}$.

FACT: If $h(X) \neq \text{Perm}(D(X))$ (deg n^2)

Can agree on at most n^2 inputs!

② 3-SAT $\in$ IP

$\exists x, \phi(x) = 1$

Claim: $\exists\ g_\phi$, $g_\phi(x) = \phi(x)$.

$(x \vee y \vee z) \wedge (\quad) \wedge \ldots$,

$\downarrow$

$(\quad)(\quad)(\quad)$

$\backslash \quad m \quad /$

x, y

$x \wedge y \Rightarrow xy$

$\neg x \rightarrow 1 - x$

$x \vee y \rightarrow 1 - (1-x)(1-y)$

$= x + y - xy$

$\exists x\ \phi(x) \iff \sum_x g_\phi(x) > 0$

Protocol to prove $\sum_x g_\phi(x) = k > 0$.

1. Prime p. $p > 2^n$. Prover sends k.
2. Prover sends $h(X) = \sum_{x_2, \ldots x_n} g_\phi(X, x_2, \ldots, x_n)$
3. Verifier checks $h(0) + h(1) = k \mod p$.
4. Verifier picks $a \in F_p$ at random

   recursively checks $h(a) = \sum_{x_2, \ldots x_n} g_\phi(a, x_2, \ldots, x_n)$

$\Pr[\text{prover succeeds in cheating}] \leq \frac{3m}{p} \cdot n$.

③ TQBF $\in$ IP

$\exists x_1 \forall x_2 \exists x_3 \cdots \forall x_n \ \phi(x_1, \cdots, x_n)$

$$\forall x \ \phi(x) = 1 \iff \prod_x g_{\phi(x)} = 1$$

$$\exists x_1 \forall x_2 \cdots \forall x_n \ \phi(x) \iff \sum_{x_1} \underbrace{\prod_{x_2} \cdots \prod_{x_n} g_{\phi(x)}}_{r} > 0$$

Two obstacles

1. r could be $\sim 2^{2^n}$
2. degree could be 2^n.

Solutions:

1. Consider all primes $0 \le p_1, p_2, \cdots, p_t \le 2^{n^2}$ (by prime number thm $t \ge 2^{n^2}/n^2$.)

   $\exists p_i$ s.t. $r \bmod p_i \neq 0$.

   if not $r \ge p_1 p_2 p_3 \cdots p_t \ge 2^t \ge 2^{2^n}$

2. Given $f(x_1, \cdots, x_{i-1}, X, x_{i+1}, \cdots, x_n)$

   define $L_i f = X \cdot f(x_1, \cdots, x_{i-1}, 1, x_{i+1}, x_n) + (1-X) \cdot f(x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots, x_n)$

Prover proves:

$$\sum_{x_1} L_1 \prod_{x_2} L_1 L_2 \sum_{x_3} L_1 L_2 L_3 \cdots \prod_{x_n} L_1 L_2 \cdots L_n \ g_\phi(x_1, \cdots, x_n) = k > 0 \pmod p$$

$$O_1 O_2 O_3 \cdots O_n \ g_\phi(x_1, \cdots, x_n)$$

O_1 is

Case 1: $O_1 = \sum_{x_1}$

- Prover sends $h(X) = O_2 \cdots O_n \ g_\phi(X, \cdots, x_n)$
- Ver. checks $h(0) + h(1) = k \bmod p$

- Ver rec. checks $h(a) = \theta_2 \cdots \theta_m g_\phi(a, x_2, \ldots, x_m)$

Case 2: $\theta_1 = \prod_{x_1}$

$(L_1) \sum_{x_2} \cdots \cdots g_\phi(a_1, x_2, \ldots, x_m) = k$

Case 3: $\theta_1 = L_1$ $\quad h(X) = \sum_{x_2 \cdots} g_\phi(X, x_2, \ldots, x_n)$

$\vdots$

Verifier checks

$a_1 h(0) + (1 - a_1) h(1) = k \mod p.$

$h(a) = \sum_{x_2 \cdots} g_\phi(a, x_2, \ldots, x_n).$

$\frac{1}{n^2}$ possible assignments eliminated)

$\left(1 - \frac{1}{n^2}\right)\left(1 - \frac{1}{n^2}\right) \cdots$

$\left(1 - \frac{1}{n^2}\right)^t \leq e^{-\frac{t}{n^2}}$