Interactive Proofs

Prove to me that "$x \in L$".

- You can think of $L \equiv$ THEOREMS

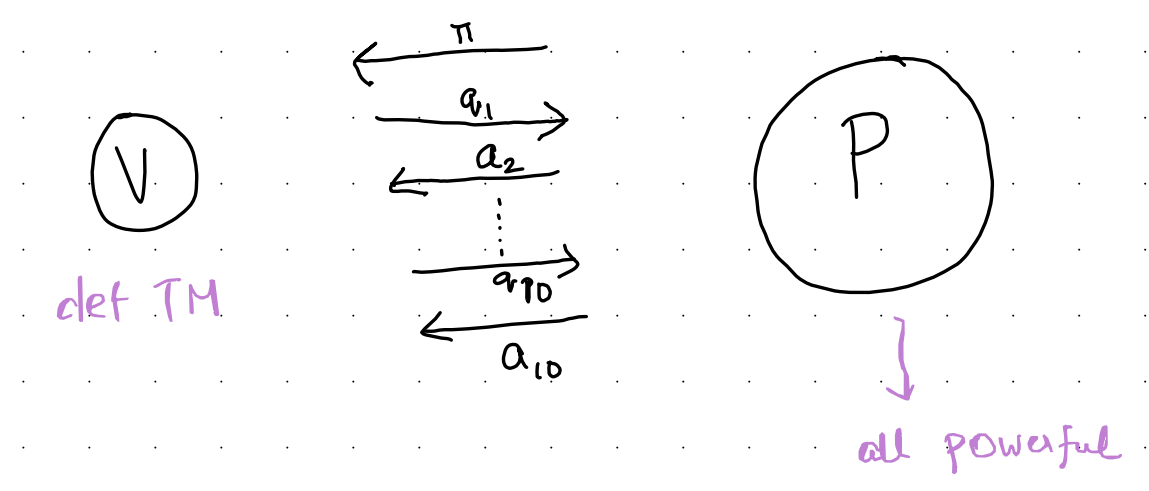
An NP-prover gave us a "certificate" or a "proof" [Π]

and

But what if → a condition we all can relate to. ☺ we don't understand the proof.

Perhaps access to interaction w/ prover helps ?

$x \in L$



All powerful prover eg:

det IP = NP

Perhaps randomness can help

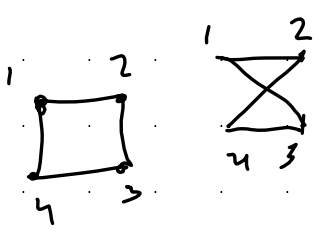
- Coke vs Pepsi

Model : - Verifier randomized
- Interaction w/ all powerful prover.

Example: Graph non-isomorphism.

$$GNI \equiv \{(G_0, G_1) \mid G_1 \ncong G_2\}$$

$\overline{GNI} \equiv GI \in NP$, $GNI \in coNP$.



$(G_0, G_1) \in GNI$

vertex, edges
Case deg different could be a proof, but.... coke vs pepsi not fanta.

1. $b \in_R \{0,1\}$
2. $\sigma \in_R S_n$ $\left(n = |V(G_0)| = |V(G_1)| \right)$
3. $H = \sigma(G_b)$ → H → P, ← $c \in \{0,1\}$
4. Accept: $b = c$.

Completeness: $G_1 \ncong G_0$ then "honest" prover P

$$Pr\left[(V \leftrightarrow P)(G_0, G_1) = acc\right] = 1$$

Soundness: $G_0 \cong G_1$

$\forall$ prover P^*

$$Pr\left[(V \leftrightarrow P^*) = acc\right] = 1/2.$$

Formal defn

Recall NP $\quad V \xleftarrow[\Pi]{x \in L} P$

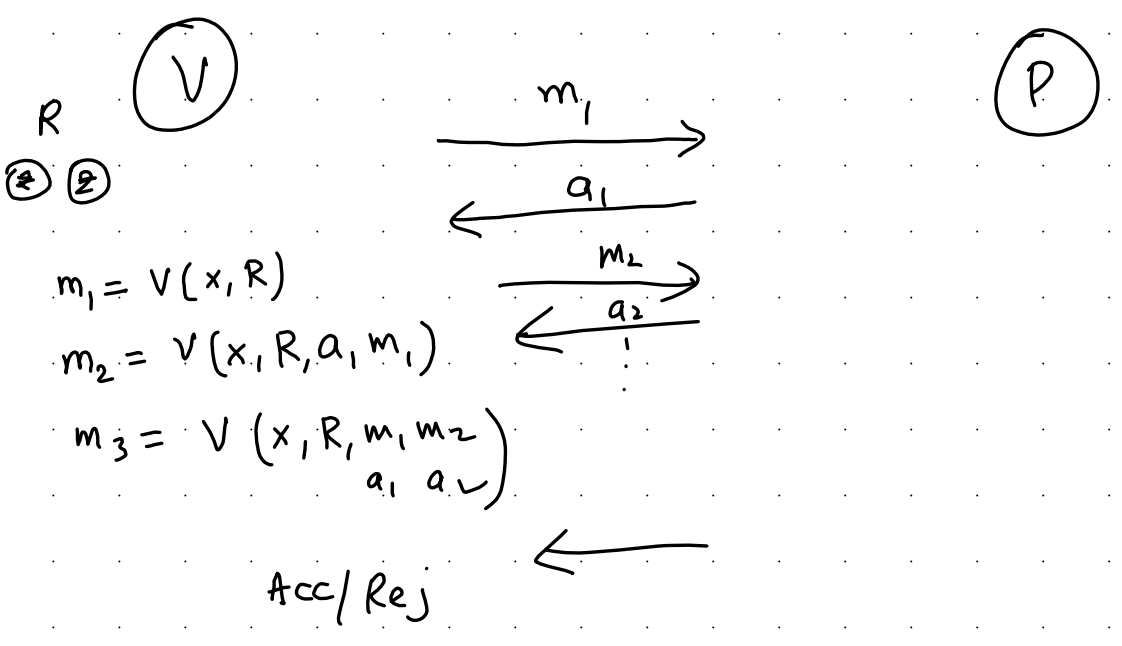
V is a det TM. $\quad V(x, r) \equiv acc/rej$

$L \in NP$ if $\exists\, V$ s.t. $\forall\, x \in L$

$\exists\, \Pi$ s.t $V(x, \Pi) = L(x)$.

1) Efficiency: V is poly-time det.
2) (perfect) Complete: $x \in L \Rightarrow \exists\, \Pi,\ V(x,\Pi) = acc$
3) (perfect) Soundness: $x \notin L \Rightarrow \forall\, \Pi,\ V(x,\Pi) = rej$

Input: x (original input)
R (randomness)



original motivation was cryptographic
- prove "$x \in L$" w/o revealing any bit of x.

Remarks (Hand wavy)

1. Error in the defⁿ can be reduced to e^{-m} by repⁿ $O(m)$
   - Repⁿ + Chernoff bounds
   [Can also do with parald repⁿ, complicated]

2. Randomized prover doesn't help.

3. Private vs Public coin

GNI excercise

4. Perfect Completeness. $2/3 \to 1$

5. Perfect Soundnes $Q//. \quad 1/3 \to 0$

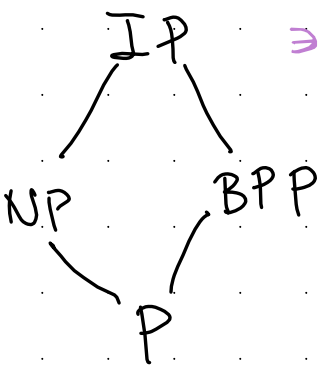
Possibly No. Can make the verifier deterministic by sending the random coins that cause the verifies to accept in yes case.

Proof system determined by Verifier

$$\max_{\text{Prover strategy}} \{ Pr[V \leftrightarrow P \text{ acc on } x] \}$$

V is fixed, write down every message a verifier can do, also Pspace using poly(|x|) space → Game

$\Rightarrow$ IP $\subseteq$ PSPACE



$\ni$ GNI

Parameteric IP protocols

$L \in IP$

- # rounds , k-round protocol

  $L \in IP[k]$, $IP = IP[poly(n)]$

- story-time

  #SAT, UNSAT $\in$ IP ?

#SAT $\equiv$ #P $\equiv$ Computing Permanent

Toda's thm: $PH \subseteq P^{\#P}$.

Public coin IP protocol for computing Perm

$$A = (a_{ij})_{\substack{i=1 \\ j=1}}^{n} \qquad a_{ij} \in \mathbb{F}$$

$|\mathbb{F}| > n^{10}$ large enough.

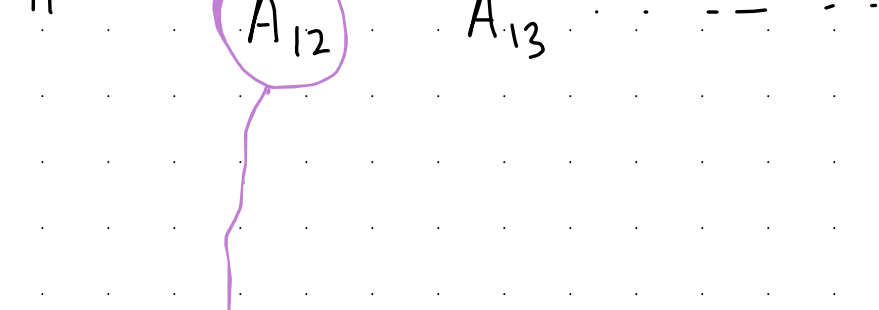
$$\text{Perm} = \{(\mathbb{F}, n, A, \alpha) \mid \mathbb{F},\ A \in \mathbb{F}^{n \times n},\ \text{perm}_{\mathbb{F}}(A) = \alpha\}$$

$$\sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{i=1}^{n} a_{1,i}\, \text{Perm}(A_{\underline{1},i})$$

where $A_{\underline{1},i}$



Candidate IP protocol



1. Check if $\alpha = \sum_{i=1}^{n} a_{1,i}\alpha_i$

$\alpha_1, \ldots, \alpha_n$ ←

$\alpha_1\ \alpha_2 \cdots \alpha_n$

$\alpha_i = \text{Perm}(A_{1,i})$

$i \in_R [n]$

$(A_{1,i}, \alpha_i)$ →

Reduced the problem to a $(n-1) \times (n-1)$ setting.

Efficient

Completeness

Soundness

Suppose $\text{Perm}(A) \neq \alpha$

Prover can cheat on just one of the path

prob that verifier catches $= \frac{1}{n!}$

[We will show that we can fix this protocol]

i.e. Modify $\frac{1}{2} \leftarrow \frac{1}{n!}$ or any constant.

Idea: Interpolate the n $(n-1) \times (n-1)$ matrix A_{ij}'s to obtain a single matrix $A(x)$.

s.t. $A(i) = A_{1,i} \quad \forall\ i \in [n]$

and ask prover to give $A(x)$.

Infact, define $A^{(i,j)}(x) \leftarrow$ unique poly deg $\leq n$

s.t. $A^{(i,j)}(k) = A_{i,k}^{(i,j)}$

TQBF?

Interactive Proof for Permanent.

Recall, $\text{Perm} \equiv \#\text{SAT} \in IP$

$\Rightarrow P^{\#P} \subseteq IP$ (Toda's thm)

UI

PH

Fact: Interpolation (univariate) $\in P$ $\deg < d$ d-points.

Idea: Interpolate the n $(n-1)\times(n-1)$ matrices $A_{i,j}$'s to obtain

Notation: $A^{(i,j)}(x) \equiv$ unique poly of deg $\leq n$ s.t. $A^{(i,j)}(k) = A^{(i,j)}_{1,k}$

Want $A^{i,j}_{1,k}$ as matrices, not just its permanent

$$A(x) = \left[A^{(i,j)}(x)\right]_{i,j \in [n-1]}$$

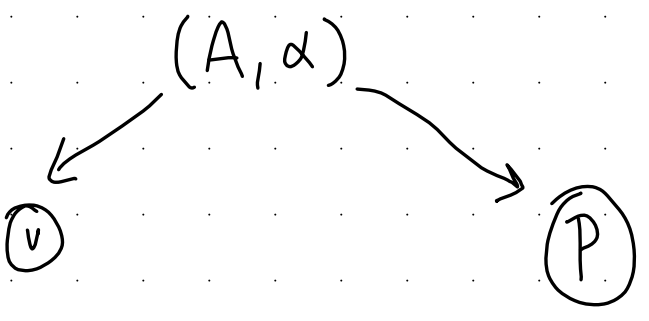
a matrix filled with deg $\leq n$ polynomial.

Consider ① $p(x) = \text{perm}(A(x))$ (i)

univariate of deg $< n(n-1)$

② $p(i) = \text{perm}(A(i)) = \text{perm}(A_{1,i})$

Modified IP for Perm



construct $A(x)$ s.t.

1) deg $< n$.

2) $A(i) = A_{1,i}$ $\forall\, i \in [n]$

3) Compute $p(x) = \text{perm}(A(x))$

If $n > 1$

① Checks $\alpha = \sum_{i=1}^{n} a_{1i}\, p(i)$

$p(x)$ ←

i.e. $n(n-1)$ $\mathbb{F}$ elements

Sample $\beta \in_R \mathbb{F}$ deg $p \leq n(n-1)$.

β →

Asking $(A(\beta), p(\beta)) \in \text{Perm}_{n-1}$

Efficiency: next message in poly $(|x|)$ time.

Completeness: $x \in L \Rightarrow \exists$ prover P

$\Pr_R[(V \leftrightarrow P)(x:R) = \text{accp}] \geq 2/3$

$x \notin L \Rightarrow$ $\forall$ prover $\tilde{P}$

$\Pr_R[(V \leftrightarrow \tilde{P})(x:R) = \text{acc}] \leq 1/3$

Soundness

Suppose $\text{Perm}(A) \neq \alpha$

Need to show for all provers $\tilde{P}$

$$\Pr\left[(V \leftrightarrow \tilde{P})(A, \alpha_i, \beta) = \text{accpt}\right] < 1/2$$

$\beta_1, \ldots, \beta_n$

Fix a prover $\tilde{P}$, let its first

Case 1: $p(x) \equiv \text{perm}(A(x))$

Case 2: $p(x) \not\equiv \text{perm}(A(x))$

C1: $\alpha \neq \sum a_{1i}\, \text{perm}(A_{1i})$

$= \sum a_{1i}\, \text{perm}(A(i))$

$= \sum a_{1i}\, p(i)$.

(verifier rejects)

C2: $p(x) \not\equiv \text{perm}(A(x))$

$\Pr_\beta[p(\beta) = \text{perm}(A(\beta))] \leq \frac{\deg}{|\mathbb{F}|}$

$|\mathbb{F}| > 2n^3$ $< \frac{1}{2n}$

$\Pr[\text{Prover not get caught}] \leq \frac{1}{2n} + \cdots + \frac{1}{2n}$

$\leq 1/2$.

$\Rightarrow$ Conclusion: $P^{\#P} \subseteq IP$

#SAT

Thm: $\#SAT_D = \{ (\varphi, k) \mid \#SAT(\varphi) = k \}$
↳ 3CNF

$\in IP.$

Can we have a direct attack on this.

$$\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$$

Total sum

$$S_0() = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \varphi(x_1 \cdots x_n)$$

Partial sum

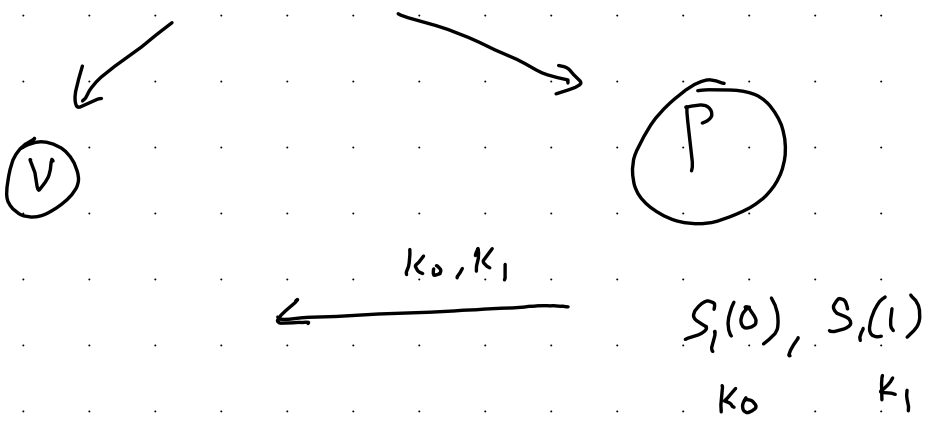
$$S_i(x_1, \cdots, x_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \varphi(x_1 \cdots x_n)$$

$$\forall i \quad S_i(x_1, \ldots, x_i) = S_{i+1}(x_1 \cdots x_i\ 0) + S_{i+1}(x_1 \ldots x_i\ 1)$$

$$S_n = \varphi(x_1 \cdots x_n)$$

Candidate IP

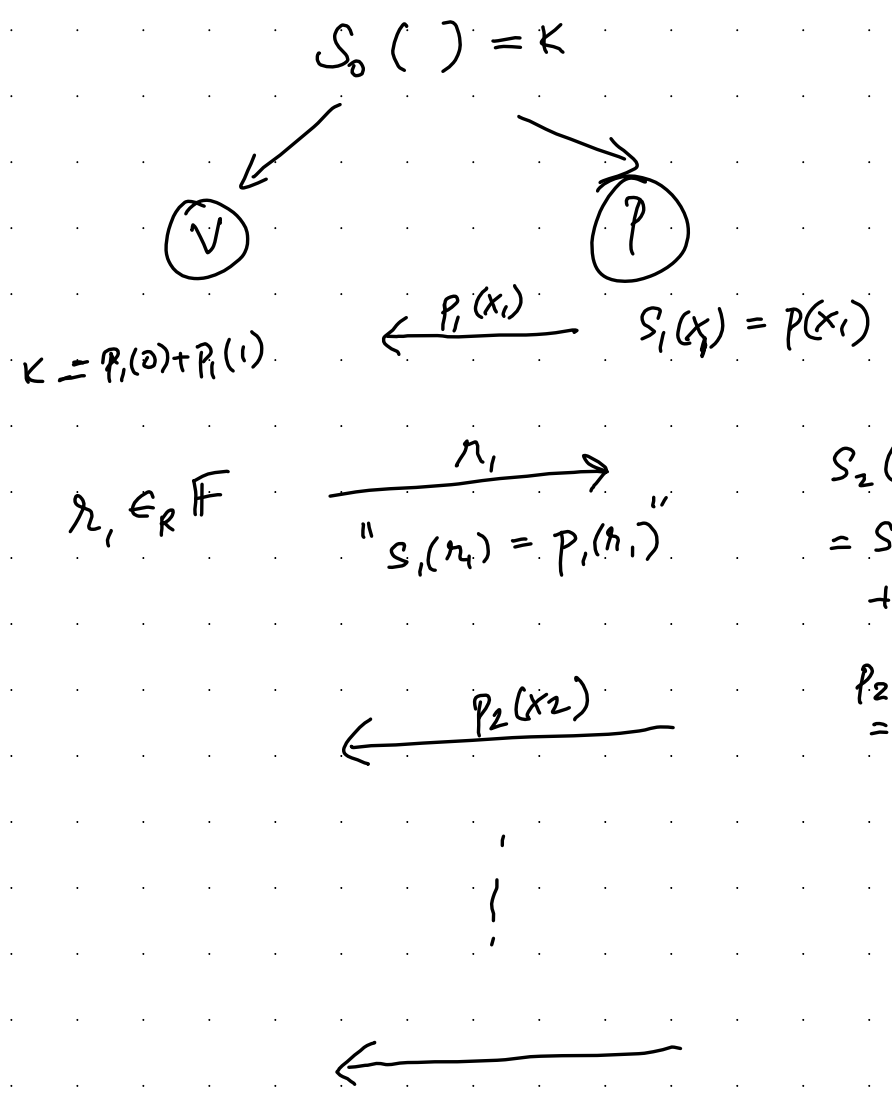
$$(\varphi, k) \equiv S_0 = k$$



Similar issue arise as in Perm before.

Arithmetization

Updated Protocol #SAT



$S(r_1, \ldots r_n) = P_\varphi(r_1, \ldots, r_n)$ → yes or no.

Crucial
▷ self-reducibility of SAT $\notin$ PERM

Soundness: $(\varphi, k) \notin \#SAT$,

$$\Pr_{r_1 \cdots r_n}\left[(V \leftrightarrow P^*)((\varphi, k), R) = acc\right] \geq \left(1 - \frac{d}{q}\right) \cdots \left(1 - \frac{d}{q}\right) \geq \left(1 - \frac{d}{q}\right)^n$$

d = max-degree