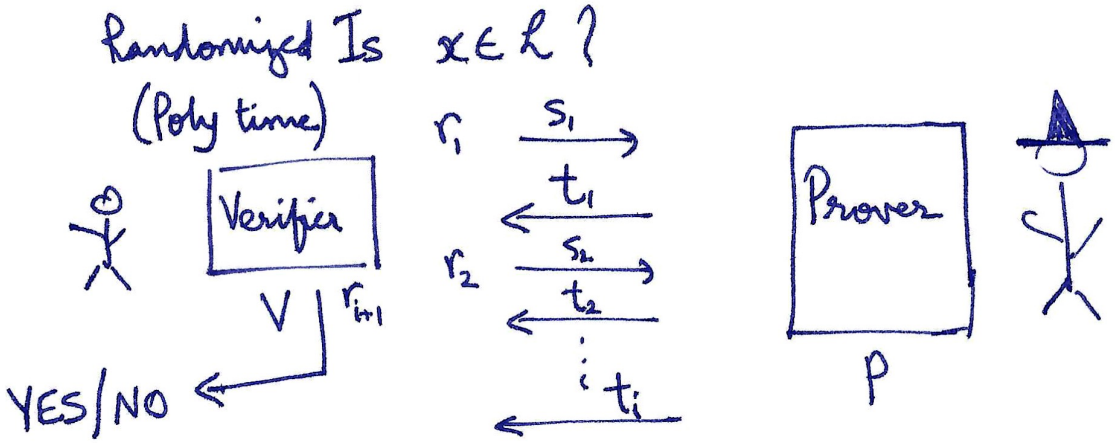
Interactive Proof Systems



Def: A k-round interactive protocol is defined by a set of functions: $(V_1, V_2 \cdots, V_{k/2}, P_1, P_2 \cdots, P_{k/2}, D)$

where V_i takes as arguments $x, r_1, r_2 \cdots, r_i$ and the outputs of $P_1, P_2 \cdots, P_{i-1}$. P_i takes as arguments x, and the outputs of $V_1, V_2 \cdots, V_i$.

The last function D takes as arguments $x, r_1, r_2 \cdots r_{k/2}$, $r_{k/2+1}$ and the outputs of $P_1, P_2 \cdots, P_{k/2}$, D outputs YES/NO.

$s_1 = V_1(x, r_1)$ $\quad t_1 = P_1(x, s_1)$ $\quad \text{out}_{V,P}(x)$

$s_2 = V_2(x, r_1, r_2, t_1)$ $\quad t_2 = P_2(x, s_1, s_2)$

$\vdots$

$D(x, r_1, r_2 \cdots, r_{k/2+1}, t_1, t_2 \cdots, t_{k/2}) \to \{0,1\}$

(If k is odd, prover starts.)

All V_i's are poly-time computable. All messages are polynomial in size | P_i's arbitrary

NP is a 1-round deterministic protocol decided by

Def: **The class $\mathbb{IP}(k)$:** $\mathcal{L} \in \mathbb{IP}(k)$ if there exists a prob. poly time verifier V s.t.

$$x \in \mathcal{L} \Rightarrow \exists \text{ Prover } P \quad \Pr_{r_1 \cdots r_{k/2}}[\text{out}_{V,P}(x, \vec{r}) = 1] \geq 2/3$$

(Completeness)

$$x \notin \mathcal{L} \Rightarrow \forall \text{ Provers } P \quad \Pr_{\vec{r}}[\text{out}_{V,P}(x, \vec{r}) = 1] \leq 1/3$$

(Soundness)

When $x \in \mathcal{L}$, the corresponding prover is called the Honest Prover.

$$\mathbb{IP} = \bigcup_{c \in \mathbb{N}} \mathbb{IP}(n^c)$$

Soundness and determinism:

Suppose soundness prob = 0 (perfect soundness)

$x \in \mathcal{L} \Rightarrow \exists$ Prover P $\exists \vec{r}$ s.t. $\text{out}_{V,P}(x, \vec{r}) = 1$

$x \notin \mathcal{L} \Rightarrow \forall$ Prover P $\forall \vec{r}$ $\text{out}_{V,P}(x, \vec{r}) = 0$

Then $\mathbb{IP}$ becomes NP.

$\mathbb{IP}(1)$

$x \in \mathcal{L} \Rightarrow \exists$ prover message t_1 $\Pr_{r_1}[V(x,t,r_1) \text{ accepts}] \geq 2/3$

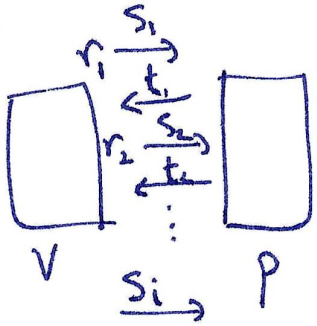
$x \notin \mathcal{L} \Rightarrow \forall\, t_1$ $\Pr_{r_1}[V(x,t,r_1) \text{ accepts}] \leq 1/3$

Clm: $\mathbb{IP} \subseteq \mathbb{PSPACE}$

Proof (sketch): We cannot enumerate over all provers.

But in poly space, we can compute the max. acceptance prob. of any prover. We will prove by induction over rounds. Suppose the max. size of random seeds, messages, and work space of verifier is $p(n)$.

Clm: Suppose we fix the first $2i-1$ rounds; fix $r_1, s_1, t_1, r_2, s_2, t_2 \dots, r_{si}, s_{si}$. Then, the t_i that maximizes the prob. of final acceptance can be computed in $O((k-2i)\,p(n))$ space.



Proof: Reverse Induction on i.

Algorithm writes down a choice for t_i. Then, it writes down r_{i+1}. s_{i+1} can be computed exactly. By induction, in $\leq c(k-2i-2)p(n)$ space, alg. can compute the largest acceptance prob. (for remaining protocol). By iterating over all r_{i+1}, it computes the largest acc. prob. for a choice of t_i. By trying all t_i, alg. computes best choice. ∎

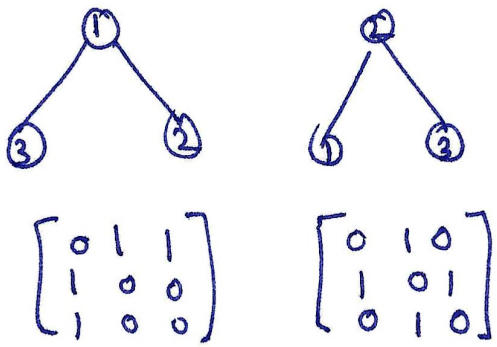
Total space $\leq \underbrace{3p(n)}_{t_i, r_{i+1}, s_i} + c(k-2i-2)p(n) \leq c(k-2i)p(n)$

$\blacksquare$

---

k is polynomial; hence total space is polynomial $\blacksquare$

A protocol



GI = graph isomorphism

$G_1 \cong G_2$

if $\exists$ permutation π of vertices

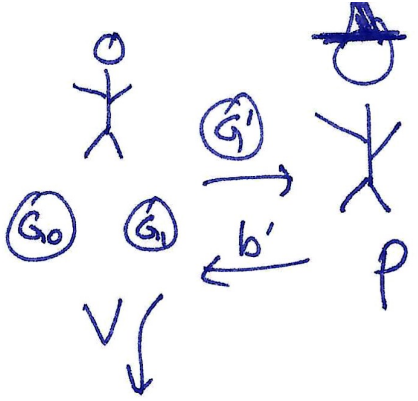
s.t. apply π to both rows & columns of adj. matrix of G_1 yields adj. matrix of G_2.

$GI \in NP$ not known to be in P or NP-complete.

[Babai 15] GI can be solved in $n^{\text{poly}(\log n)}$ time.

$GNI = \overline{GI} \longrightarrow \{\langle G_0, G_1\rangle \mid G_0 \not\cong G_1\}$

Thm: $GNI \in \Pi P(2)$

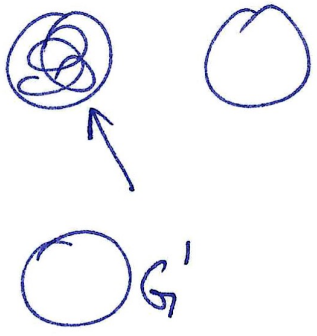


Proof:

Verifier (G_0, G_1)

1. Pick uar $b \in \{0,1\}$
2. Pick a uar permutation π
3. Generates a new graph (adj. matrix) by permuting vertices of G_b by π. Call this G'.
4. Send G' to Prover and asks "What was b?"

Prover sends its "guess" for b



Accept if ~~prover's output~~ guess is correct

Honest prover (G', G_0, G_1)

1. Checks if $G_0 \cong G_1$. If so, ~~abort~~ output 0.
2. Check if $G' \cong G_0$ or $G' \cong G_1$ (only one can hold)
3. Output b accordingly

Clm: If $G_0 \ncong G_1$, honest prover correctly outputs b (w. prob. 1).

Perfect completeness.

Clm: If $G_0 \cong G_1$, regardless of the prover, verifier accepts w.p. $1/2$.

Proof: Let $\mathcal{D}_b$ be the set of graphs isomorphic to G_b (labeled). $\mathcal{D}_0$ and $\mathcal{D}_1$ are identical! G' is chosen from $\mathcal{D}_b$, where b is uar bit. The message G' has the same distribution regardless of choice of b. No function can take a sample and distinguish $\mathcal{D}_0$ from $\mathcal{D}_1$. Hence prover is correct w.prob $1/2$. ∎