

Feb 22, 2008 - Interactive Proof System

Lecture note of EECS 395 Winter 2008 (Prof. Fortnow) taken by Bach Ha

Graph Isomorphism

- Given $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ and $|V_1| = |V_2| = n$.
- They are isomorphic if there is a permutation $\pi : V_1 \rightarrow V_2$ such that for all (u, v) , $(u, v) \in E_1 \Leftrightarrow (\pi(u), \pi(v)) \in E_2$
- GI = $\{(G_1, G_2) \mid G_1 \approx G_2\}$ – This problem is easier
- GNI = $\{(G_1, G_2) \mid G_1 \not\approx G_2\}$ – Harder

Interactive Proof Systems

- Two players: Prover and Verifier
- Prover: All knowing
- Verifier: Probabilistic Polynomial Time
- Verifier doesn't trust Prover and keeps challenge Prover

GNI

- V picks $i \in 1, 2$, and let $G = \pi(G_i)$
- V gives P the value G
- P gives V back the value $j \in \{1, 2\}$
- V accepts if $i = j$
- Note:
 - If $G_1 \not\approx G_2$ then for all σ, π then $\sigma(G_1) \not\approx \pi(G_2)$. Hence P can always figure out given $\pi(G_i)$. And V always accepts.
 - If $G_1 \approx G_2$, then best P can do is to choose at random, hence V will reject half the time.

Interactive Proof Class

- IP - Interactive Proof Class.
- $L \in \text{IP}$ if there is a P and V : V is a probabilistic poly time TM and P is arbitrary (infinite power). 2 machines share same input and communication tape, not coin or work tape.
- If $x \in L \Rightarrow \Pr(P \rightarrow V(x) \text{ accepts}) \geq 2/3$
- If $x \notin L \Rightarrow \forall P' : \Pr(P' \rightarrow V(x) \text{ accepts}) \leq 1/3$
- $\text{IP} = \text{PSPACE}$ (will prove later)

MA, AM

- MA and AM are public coin models: Prover can see Verifier's coin (meaning you can see all computational process)
- MA : a game in 2 rounds: Prover sends the message and the Verifier checks it with the randomize algorithm
- It is called Publishable proof
- MA = Merlin and Arthur.
- AM: a game in 2 rounds: Verifier sends random coin and Prover sends the response.
- Goldwasser-Sipser: $K(a)$ -rounds private coin-protocol can be simulated by $k(n)$ round public coin-protocol.

Linear Random Function

- Let A be a random $k \times b$ 0-1 matrix. and V be in random 0-1 matrix
- $H : \Sigma^k \rightarrow \Sigma^b$
- $H(x) : Ax + v$ is a linear random function