



CS 579: Computational Complexity. Lecture 8

Interactive Proofs.

Alexandra Kolla

Today

- Adding randomness and interaction to NP.
- The class IP and its variants.
- IP for Graph non-Isomorphism.
- Private coins vs. public coins.

Characterization of NP, million-th time

- L is an NP language if there is a poly time algorithm $V(.,.)$ and a polynomial p s.t.

$x \in L \Leftrightarrow \exists y, |y| \leq p(|x|)$ and $V(x, y)$ accepts

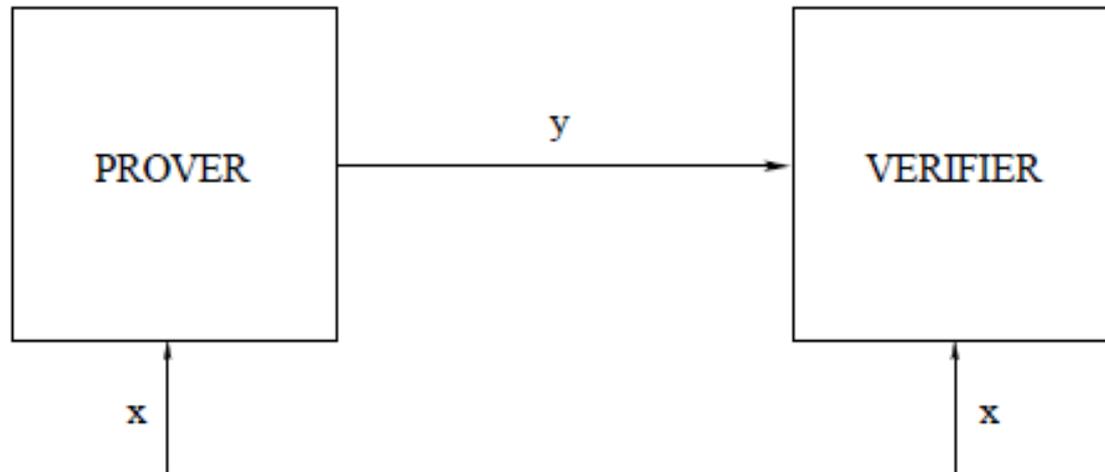
- Alternatively,

$x \in L \Rightarrow \exists y, |y| \leq p(|x|)$ and $V(x, y)$ accepts

$x \notin L \Rightarrow \forall y, |y| \leq p(|x|)$ $V(x, y)$ rejects

Completeness and soundness resp.

Prover /Verifier view of NP



Prover/verifier characterization of NP

- L is an NP language if there is a prover P and a poly time verifier (algorithm) $V(.,.)$ p s.t.

$x \in L \Rightarrow P$ has strategy to convince V .

$x \notin L \Rightarrow P$ has no strategy to convince V .

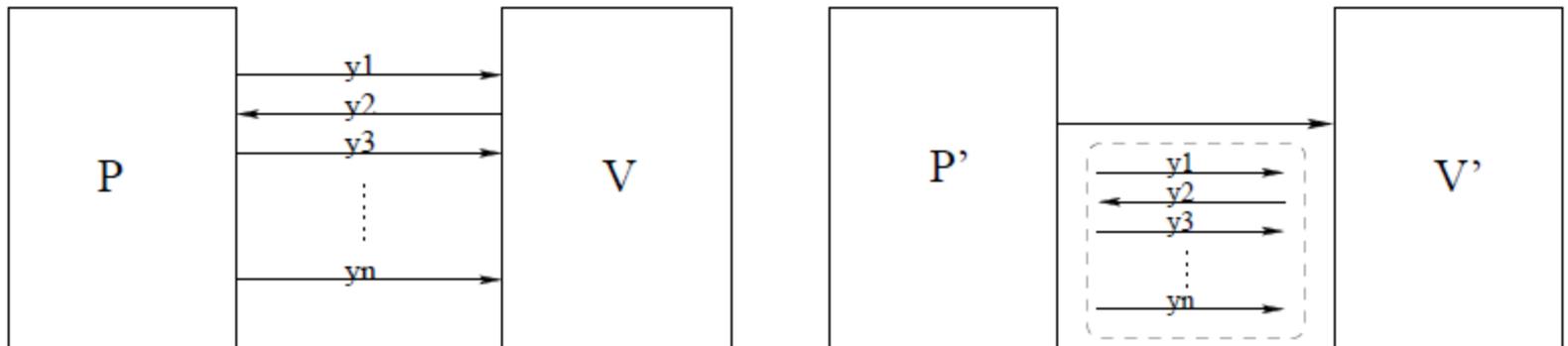
- Strategy means the certificate of proof is polynomially small.
- Later will generalize to interaction where there is a sequence of messages exchanged and strategy means a function from the sequence of messages seen to the next message the prover sends.

The class IP

- We will define the class IP with two more ingredients
- Randomness: V could be a randomized machine
- Interaction: unlike above where there is only one “round” of communication, verifier may ask several questions to prover based on the messages already seen.
- Both of the above are required.

NP + interaction

- **Theorem.** NP+interaction = NP



NP + randomness

- **Definition.** L is in MA if there exists a probabilistic polynomial time machine V such that:

$$x \in L \Rightarrow \exists y \Pr[V(x, y) \text{ accepts}] \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \forall y \Pr[V(x, y) \text{ accepts}] \leq \frac{1}{3}$$

- It is conjectured that MA=NP.
- It is known that if $\text{coNP} \subseteq \text{MA}$ the polynomial hierarchy collapses.
- **Definition.** NP+randomness =MA

The class IP

- **Definition.** A language L is in $IP(r(\cdot))$ iff there is a probabilistic polynomial time verifier V such that:

$x \in L \Rightarrow$

$\exists P \Pr[V \text{ interacting with } P \text{ accepts}] \geq \frac{2}{3}$

$x \notin L \Rightarrow$

$\forall P \Pr[V \text{ interacting with } P \text{ accepts}] \leq \frac{1}{3}$

V also uses at most $r(|x|)$ rounds of interaction.

Public coins and the class AM

- **Definition.** A language L is in $AM(r(.))$ iff L is in $IP(r(.))$ and at each round the verifier sends a random message, that is a message that is completely random and independent of the previous communication.

Public coins vs. private coins

Theorem 1. $IP(r(n)) \subseteq AM(r(n)+2)$

Theorem 2. For all $r > 1$, $AM(2r(n)) \subseteq AM(r(n))$

Corollary 3. $AM(O(1)) \subseteq AM(2)$

Theorem 4. $IP(O(1)) = AM(O(1)) = AM(2)$

Public coins vs. private coins

Theorem 5. $IP(\text{poly}(n)) = PSPACE$ (next time).

Theorem 6. If $\text{co NP} \subseteq IP(O(1))$ then the polynomial hierarchy collapses.

IP for Graph non-Isomorphism

- We will next see and IP with constant number of rounds for GNI:
- By previous results, it is also in AM(2).
- **Theorem.** $\text{GNI} \in \text{AM}(2)$.
- We show that next from scratch. Similar proof goes for theorem 4.

IP for Graph non-Isomorphism

- **Theorem.** If GI is NP-complete then the polynomial hierarchy collapses (to the second level).