Lecture 29

Friday, August 2, 2019 11:10 AM

Last time:
- Interactive Proofs (IP)
- Graph Non-Isomorphism $\in$ IP

Def: $L \in IP$ if $\exists$ randomized, poly time verifier V s.t.

$\forall x \in \{0,1\}^n$,

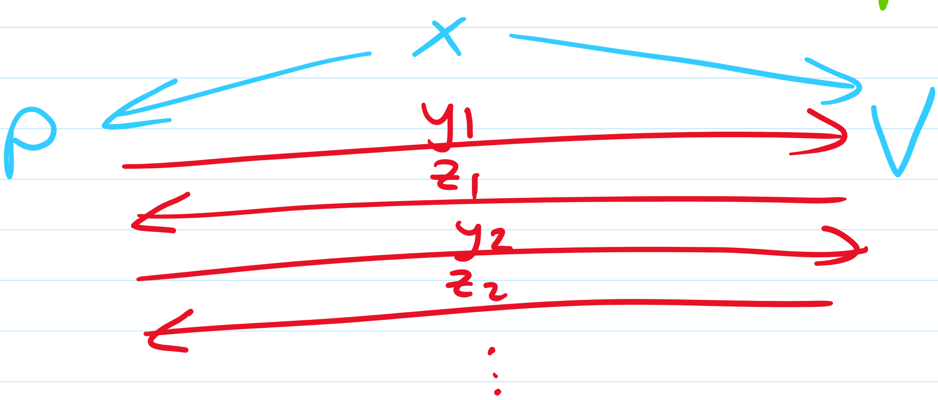
(1) $x \in L \Rightarrow \exists$ prover P s.t.

$$\Pr[V^P(x) \text{ accepts}] = 1$$

(2) $x \notin L \Rightarrow \forall$ prover P

$$\Pr[V^P(x) \text{ accepts}] \leq \frac{1}{3}$$

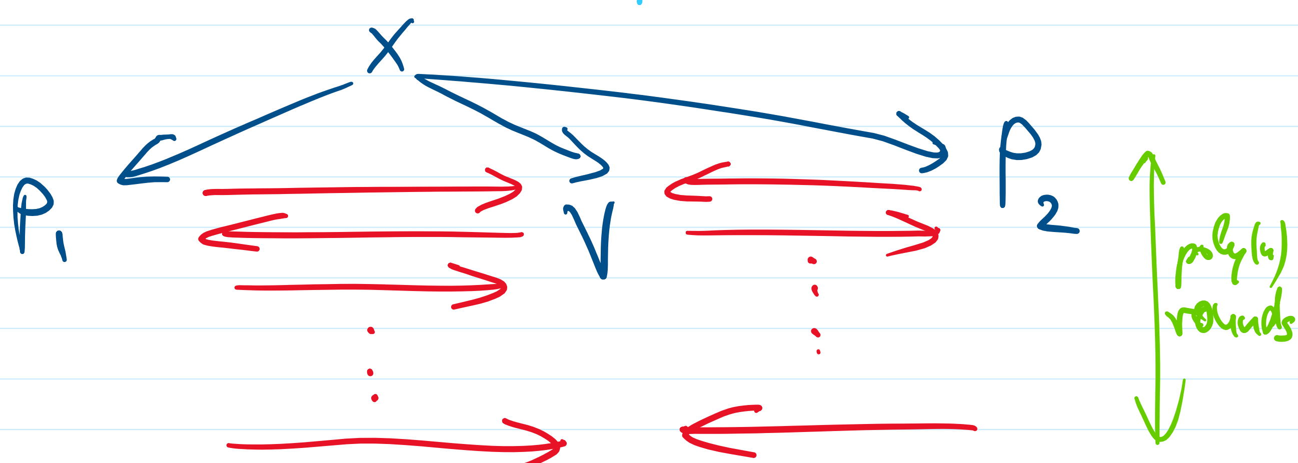
Here, $V^P(x)$ means: V & P have poly(n)-many rounds of communication, at the end of which V makes a decision (to accept or reject).



$\xrightarrow{\quad y_t \quad}$ V makes the decision (based on $x, y_1, z_1, \dots, y_t$)

Thm: PSPACE = IP

MIP = multiple provers IP

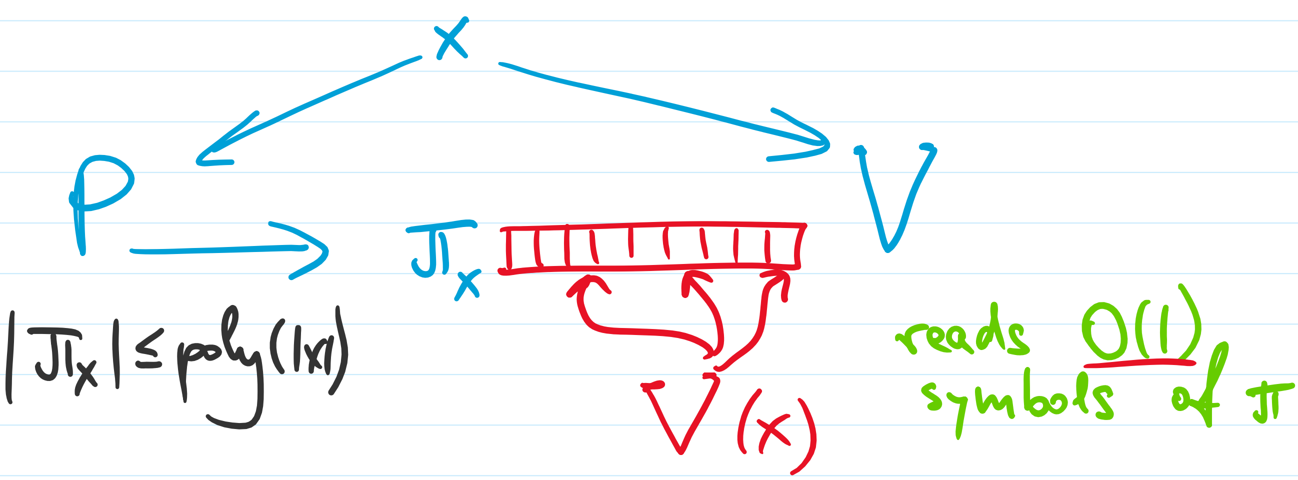


V makes the decision

Thm: NEXP = MIP (with 2 provers).

Nondeterministic
Exponential
Time (exponential-time version of NP)

PCP Theorem



PCP Theorem: $NP = PCP$.

$\forall L \in NP$ $\exists$ verifier V such that

- V is randomized polytime algo
- V reads a constant number of symbols in a given "proof"

and such that, $\forall x \in \{0,1\}^n$

- $x \in L \Rightarrow \exists \pi \in \{0,1\}^{poly(n)}$,

$$\Pr\left[V^{\pi}(x) \text{ accepts}\right] \geq \frac{2}{3}$$

- $x \notin L \Rightarrow \forall \pi \in \{0,1\}^{poly(n)}$, $\Pr[V^{\pi}(x) \text{ accepts}] \leq \frac{1}{3}$.

PCP Theorem has applications to Hardness of Approximation.

For many NP-hard optimization problems,

For many NP-hard optimization problems, not only are they NP-hard to solve optimally, but also NP-hard to solve approximately (to some factor of approximation).

Time / Space Hierarchy Theorems

Thm: $\forall$ "nice" functions $t(n) \ll T(n)$

$$\mathrm{Time}(T(n)) \supsetneq \mathrm{Time}(t(n))$$

& $$\mathrm{Space}(T(n)) \supsetneq \mathrm{Space}(t(n))$$

E.g., In

$$\mathrm{Time}(n^3) \supsetneq \mathrm{Time}(n^2)$$

$$\mathrm{Space}(n^2) \supsetneq \mathrm{Space}(n^{1.5})$$

Time/Space Hierarchy Theorems are proved using Diagonalization arguments.

Application:

$$L \subseteq NL \subseteq P \subseteq NP \subseteq PSPACE$$

$L \subseteq NL \subseteq P \subseteq NP \subseteq PSPACE$

at least one inclusion must be <u>strict</u>

<u>Proof</u>: Otherwise, $L = PSPACE$,
but, by Space Hierarchy Theorem,
$L = Space(\log n) \subsetneq Space(n) \subseteq PSPACE$.

Course Review

Computability & Logic

- Finite Automata — DFA ≡ NFA ≡ Reg. Express., Pumping Lemma
- Turing machines — TM ≡ "algorithm"
  - k-tape, k-head, etc.
  - DTM ≡ NTM ≡ semi-decidable lang.
  - decidable $\subsetneq$ semi-decidable
  - lower bounds: diagonalization + reductions
  - self-reference: Recursion Theorem, Gödel's Incompleteness
  - application: Kolmogorov complexity

Complexity

"scale down": decidable $\longrightarrow$ P

semi-decidable $\longrightarrow$ NP

P = NP ???

- NP-completeness (tons of natural NP-complete problems)
- Space: NPSPACE = PSPACE

  NL = coNL
- Randomized Computation: RP, BPP, ZPP
- Interactive Proofs: IP, PCP Theorem
- lower bounds: Time/Space Hierarchy