Last time:
- Interactive Proofs (IP)
- Graph Non-Isomorphism ∈ IP

**Def:** A problem $L \in IP$ if there exists a randomized polytime verifier $V$ such that:

1. For all $x \in \{0,1\}^*$, if $x \in L$ then there exists a prover $P$ such that $\Pr_P \left[ V^p(x) \text{ accepts} \right] = 1$.
2. For all $x \notin L$, for all provers $P$, $\Pr_P \left[ V^p(x) \text{ accepts} \right] \leq \frac{1}{3}$.

Here, $V^p(x)$ means:

$V$ and $P$ have poly($n$)-many rounds of communication, at the end of which $V$ makes a decision (to accept or reject).
\[ y^+ \rightarrow V \text{ makes the decision (based on } x, y_1, z_1, \ldots, y_t) \]

**Thm:** \( \text{PSPACE} = \text{IP} \)

\[ \text{MIP} = \text{multiple provers IP} \]

\[ P_1 \xleftarrow{X} V \xrightarrow{X} P_2 \]

\( V \text{ makes the decision} \)

**Thm:** \( \text{NEXP} = \text{MIP} \) (with 2 provers).

Nondeterministic Exponential Time \( (\text{exponential-time version of NP}) \)

**PCP Theorem**
PCP Theorem: \( \text{NP} = \text{PCP} \)

\[ \forall L \in \text{NP} \exists \text{ verifier } V \text{ such that} \]
- \( V \) is randomized polytime algo
- \( V \) reads a constant number of symbols in a given "proof"

and such that, \( \forall x \in \{0,1\}^n \)
- \( x \in L \Rightarrow \exists \pi \in \{0,1\}^n, \text{poly}(n), \Pr[ V \pi(x) \text{ accepts} ] \geq \frac{2}{3} \)
- \( x \notin L \Rightarrow \forall \pi \in \{0,1\}^n, \text{poly}(n), \Pr[ V \pi(x) \text{ accepts} ] \leq \frac{1}{3} \).

PCP Theorem has applications to Hardness of Approximation.

For many \( \text{NP} \)-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**

\[ \text{Time}(T(n)) \nRightarrow \text{Time}(t(n)) \]

\[ \& \text{Space}(T(n)) \nRightarrow \text{Space}(t(n)) \]

E.g., In

\[ \text{Time}(n^3) \nRightarrow \text{Time}(n^2) \]

\[ \text{Space}(n^2) \nRightarrow \text{Space}(n^{1.5}) \]

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 strict

Proof: Otherwise, \( L = PSPACE \), but, by Space Hierarchy Theorem,
\[ L = \text{Space} \left( \log n \right) \neq \text{Space} \left( n \right) \subseteq PSPACE. \]

---

**Course Review**

**Computability & Logic**

- Finite Automata \( \Delta FA \equiv NFA \equiv \text{Reg. Express.} \)
  - Pumping Lemma

- Turing machines \( TM \equiv \text{“algorithm”} \)
  - \( k \)-tape, \( k \)-head, etc.
  - \( \Delta TM \equiv NTM \equiv \text{semi-decidable lang.} \)
  - decidable \( \neq \text{semi-decidable} \)
  - lower bounds: diagonalization + reductions
  - self-reference: Recursion Theorem,
    - Gödel's Incompleteness
  - application: Kolmogorov complexity
Complexity

"scale down": decidable $\rightarrow$ P
semi-decidable $\rightarrow$ NP

$P = NP$ ???

- NP-completeness (tons of natural NP-complete problems)

- Space: $\text{NPSPACE} = \text{PSPACE}$
  $\text{NL} = \text{coNL}$

- Randomized Computation: $\text{RP}, \text{BPP}, \text{ZPP}$
- Interactive Proofs: $\text{IP}, \text{PCP Theorem}$

- lower bounds: Time/Space Hierarchy