Interactive Proofs

Lecture 19

$$NP := \{L \mid \exists \text{ DTM } M_L, \exists w \; M_L(x,w) = 1\}$$

w "is a proof"

$$x \in L \iff (\exists w_{|w| \le \text{poly}(|x|)}) \; M_L(x,w) = 1$$

$$x \notin L \iff \forall w \; M_L(x,w) = 0$$

how to get w?

IPs : Two algorithms, interactive TMs, (P, V)

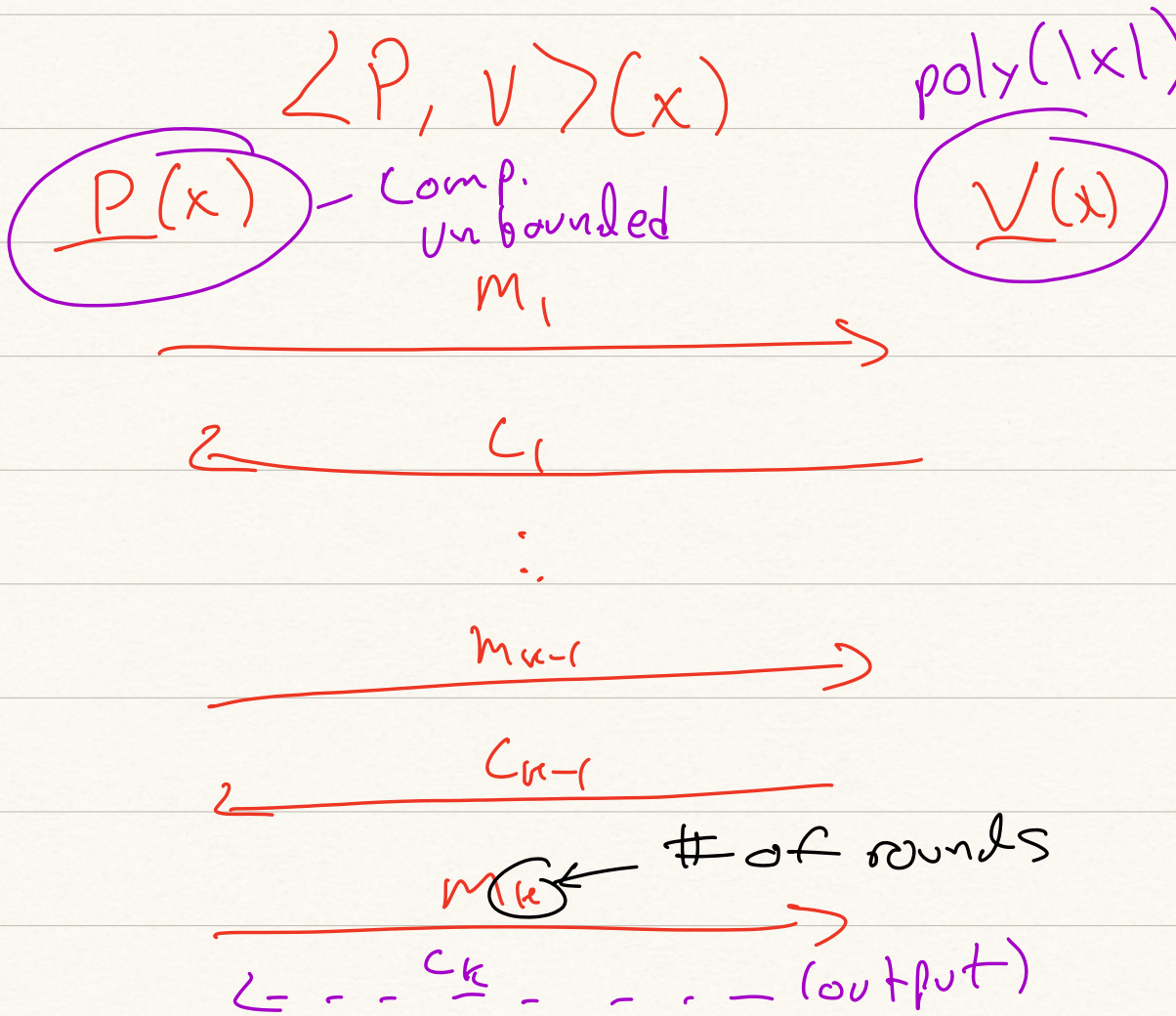
$L \in NP$ (other classes)

Q: $x \in L$?

$\langle P, V \rangle(x)$

$P(x)$ – comp. unbounded

$V(x)$ poly($|x|$)



$m_i = P(x, (m_j, c_j)_{j=1}^{i-1})$

$c_i = V(x, (m_j, c_j)_{j=1}^{i-1}, m_i)$

Output $V(x, (m_j, c_j)_{j=1}^{k-1}, m_k)$

$* \quad \langle P(y), V(z) \rangle(x)$

y: private; z: private; x: common/public input

Natural Questions:

1. randomized P / V?
2. what is accepting/rejecting proof?
3. who sends first/last

message?

(4) Proof size?

Deterministic IPs

- V is deterministic
- P also det, comp. unbounded
  - → V runs in poly(|x|) time

Def: We say L is in the class $dIP[k]$ if $\exists$ a k-round ($2k+1$ message) IP (P, V) such that $\langle P, V \rangle(x)$ has $k(|x|)$ rounds and the following hold:

① (completeness) If $x \in L$, then $\langle P, V \rangle(x) = 1$

② (soundness) If $x \notin L$, then for any P^*, $\langle P^*, V \rangle(x) = 0$.

in k rounds.

$$dIP = \bigcup_{c \geq 0} dIP[n^c]$$

Thm. $dIP = IP$

Proof: ① $NP \subseteq dIP$.

If $L \in NP$, $\exists$ DTM M_L running in poly-time such that

$x \in L \leftrightarrow \exists w \; M_L(x, w) = 1$

$x \notin L \leftrightarrow \forall w \; M_L(x, w) = 0$

$\hookrightarrow$ poly($|x|$)

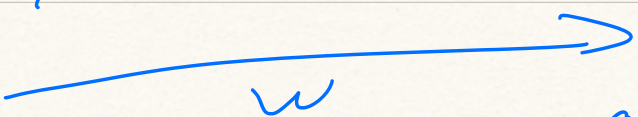
dIP for L:

$\langle P, V \rangle(x)$

P V

- compute w s.t.

$M_L(x, w) = 1$



w

↑

$|w| = poly(|x|)$

Output

$M_L(x, w)$.

② $dIP \subseteq NP$

Let $L \in dIP$. Then, $\exists$ k-round dIP (P, V) s.t.

$x \in L \Rightarrow \langle P, V \rangle(x) = 1$

$x \notin L \Rightarrow \forall P^*, \langle P^*, V \rangle(x) = 0.$

NP verifier M_L s.t.

$x \in L \iff \exists w \; M_L(x, w) = 1$

- What does $\langle P, V \rangle(x)$ look like?

$V(x, (m_i, c_i)_{i=1}^{k}, m_k) = b$

w

poly-time machine

poly-length certificate

IP: random Verifiers

Def. $IP[k]$ is the set of all languages L w/ a k-round IP (P, V), where

- P is deterministic, comp. unbounded
- V is a probabilistic polynomial time (PPT) algorithm
  - ↳ strict poly-time

such that

(1) (completeness) $x \in L \Rightarrow$

$$\Pr_V [\langle P, V \rangle(x) = 1] \geq 2/3$$

↑ arbitrarily close to 1

(2) (Soundness) $x \notin L \Rightarrow \forall P^*$

$$\Pr_V [\langle P^*, V \rangle(x) = 1] \leq 1/3$$

↑ arbitrarily close to 0

Def: $IP := \bigcup_{c \geq 0} IP[n^c]$.

Note: V in IP def. does not reveal its random choices! (doesn't have to)

↳ private-coin

Lemma: IP is the same class in completeness holds $\geq 1-2^{-n^s}$ & soundness $\leq 2^{-n^s}$, for fixed constant $s > 0$

Proof Sketch: Given (P, V), construct (P', V') which just sequentially runs (P, V) some # m times, and V' outputs majority answer. Set $m = O(n^s)$. □

Notes about IP

(1) Private coins are not necessary. we'll see later.

(2) Does P being probabilistic change IP? No!

(3) P can compute undecidable functions. However, can compute optimal $\hat{P}$ to maximize completeness, only using poly(|x|) space

$\Rightarrow IP \subseteq PSPACE$

(4) Completeness probability = 1 does not change IP.

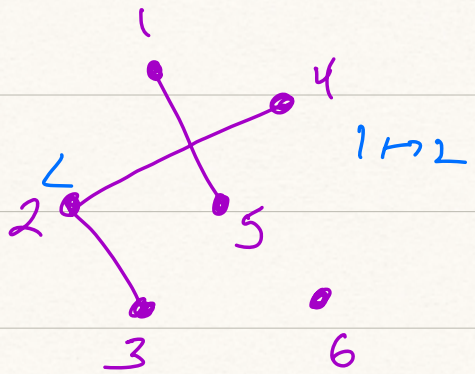
(5) Soundness error = 0 $\Rightarrow IP = dIP$

⑥ Above lemma can be done in parallel, SD protocol is still k-round.

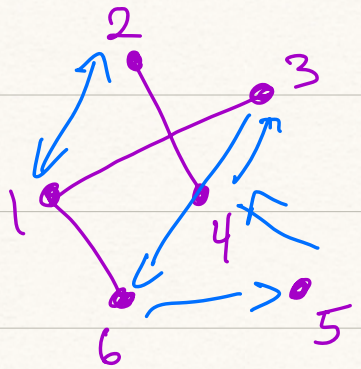
IP for Graph Non-Isomorphism

- G_0, G_1 are undirected, simple graphs, on n vertices
- G_0 is isomorphic to G_1, $G_0 \cong G_1$, if you can relabel the vertices in G_0 and obtain G_1
  → $\exists$ permutation π s.t.
  $\pi(G_0) = G_1$

Ex



G_0



G_1

$\pi(G_1) = G_1$

$\pi = (12)(3654)$

$1 \mapsto 2$ $\quad 3 \mapsto 6$

$2 \mapsto 1$ $\quad 6 \mapsto 5$

$5 \mapsto 4$

$4 \mapsto 3$

$GI := \{(G_0, G_1) : G_0 \cong G_1\}$

$GI \in NP$

Unknown if GI is NP-complete.

$$GNI := \{ (G_0, G_1) : G_0 \not\cong G_1 \}$$

$$GNI \in coNP$$

IP for GNI

Let (G_0, G_1) be graphs

$$\langle P, V \rangle (G_0, G_1)$$

P	V
	$b \xleftarrow{\$} \{0,1\}$
	$\sigma \xleftarrow{\$} P_n$ (All permutations over $[n]$)
$H = \sigma(G_b)$ ←	
	b' →
	Output

$b = b'$.

Analysis

① If $G_0 \not\cong G_1$, no σ exists s.t. $\sigma(G_0) = \sigma(G_1)$.

- P can compute σ via brute force, send correct b.

② If $G_0 \cong G_1$, then

$\exists\ \pi$ s.t. $\pi(G_0) = G_1$

$G_0 = \pi^{-1}(G_1)$

P can only guess correct bit and succeed w.p. $\leq \frac{1}{2}$.

GNI w/ public coins?

- Above IP seems to crucially rely on b, σ being hidden.
- Need to view GNI in quantitative, but equivalent, way.
- Let G_0, G_1 be n vertex graphs
- Define $S := \{ H \mid H \cong G_0 \text{ or } H \cong G_1 \}$

$\forall H$, easy to certify if $H \in S$

↳ just give Π s.t. $\Pi(H) = G_0$ or $\Pi(H) = G_1$.

- A graph G on n vertices can have at most $n!$ equivalent graphs.

- $\pi(G) \neq G$

- Pretend G_0, G_1 both have exactly $n!$ equivalent Graphs

① If $G_0 \cong G_1$, then $|S| = n!$

② If $G_0 \ncong G_1$, then $|S| = 2n!$