Lecture 6

- Random bits for Interactive Proofs

    - IP public vs. private coins
    - IP protocol for lower bounding a set size

Interactive Proofs

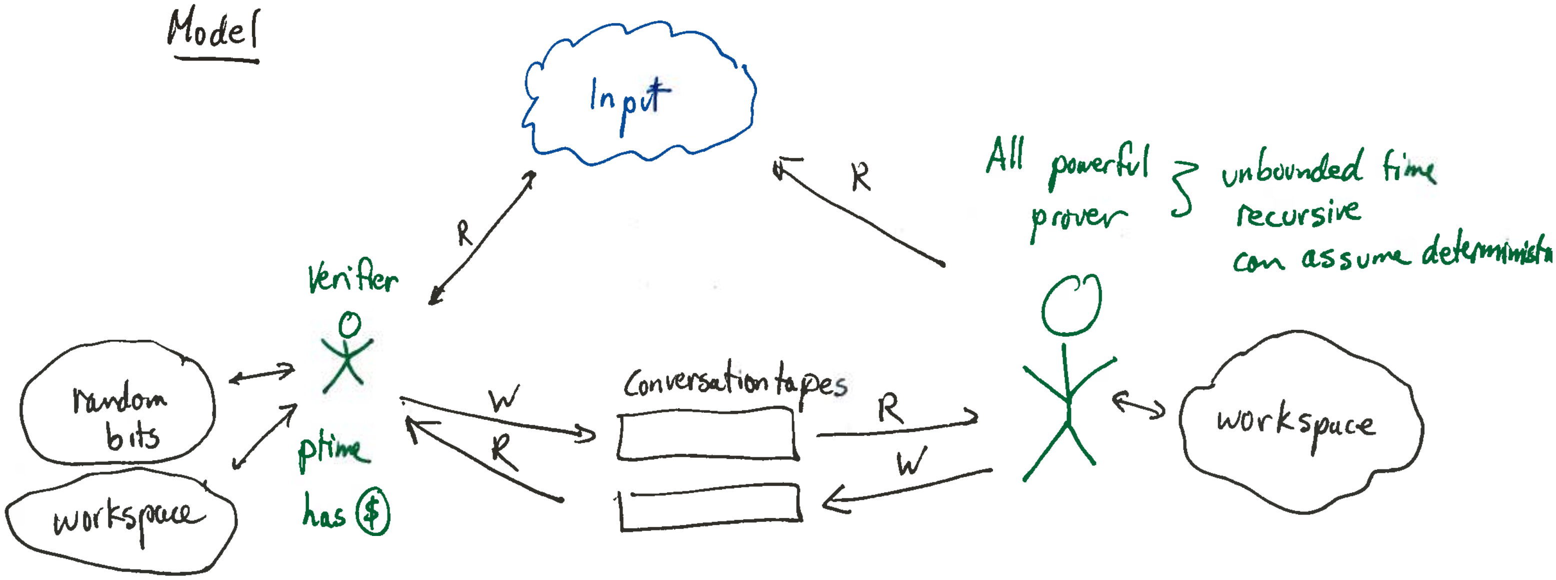
NP = all decision problems for which "Yes" answers can be verified in ptime by a deterministic TM ("verifier")

IP:

generalization of NP:

- short proofs ⇒ short interactive proofs "conversations that convince"

Model



def "Interactive Proof Systems" (IPS) [Goldwasser Micali Rackoff]

for language L is protocol s.t.

- if V, P follow protocol & $x \in L$ then $\Pr_{V\text{'s coins}}[V \text{ accepts } x] \geq \frac{2}{3}$
- if V follows protocol & $x \notin L$ then (no matter what P does) $\Pr_{V\text{'s coins}}[V \text{ rejects } x] \geq 2/3$

what if require that P follow protocol?

for crypto settings, useless!

def $IP = \{L \mid L \text{ has } IPS\}$

Note: Clearly $NP \subseteq IP$

turns out that $IP = PSPACE$!

Graph Isomorphism (GI)

Input G, H

Output is $G \cong H$? (ie $\exists\ \pi$ s.t. $(u,v) \in E_G$ iff $(\pi(u), \pi(v)) \in E_H$?)

NOTE: $GI \in NP \Rightarrow GI \in IP$

GI not known to be in P (though is now known to be in quasi-P [Babai])

Graph Non-Isomorphism (GNI)

Input G, H

Output is $G \ncong H$?

Note: GNI not known to be in P or NP

but is in IP! [Goldreich Micali Wigderson]

(and quasi-P [Babai])

IP Protocol for graph $\not\cong$:

<u>Input</u> G, H

<u>Protocol</u> Do $O(1)$ times:

- V computes G' : random permutation of G
  H' : " " " H

- V flips coin
  H: sends (G, G') to P
  T: sends (G, H') to P

- $P \to V$: $\cong / \not\cong$

-

V flip	"Correct" response	P response	V output
H	$\cong$	$\cong$	continue
H	$\cong$	$\not\cong$	fail + halt
T	$\not\cong$	$\cong$	fail + halt
T	$\not\cong$	$\not\cong$	continue

assuming that in fact $G \not\cong H$

not same as $\notin L$ unless V follows protocol

Output "ACCEPT"

Proof of correctness

- if $G \ncong H$, P can figure out coin toss & always answer correctly } here we use that P has unbounded time
- if $G \cong H$, {need to show that P can't fool V}
  - distribution of V's msgs are identical under H/T
  - since P deterministic wlog

    let $q \equiv$ fraction of random permutations π s.t. Prover $(G, \pi(G)) =$ "$\ncong$"

$$\Pr[\text{fail in round } i] = \frac{1}{2} \cdot q + \frac{1}{2}(1-q) = 1/2$$

prob V flips H & expect $\cong$

Prob V picks π s.t. P answers $\ncong$

prob V flips T & expect $\ncong$

Prob V picks π s.t. P answers $\cong$

Note V's random perm & coin flips must be hidden, or P could cheat!

Arthur - Merlin Games

V's random tape is public!

$\Rightarrow$ this protocol breaks

Can Graph $\not\cong$ have IPS with only public coins?

YES! [Goldwasser Sipser]

(important for complexity, crypto, interesting tool for checking delegated computations...)

How do they show this?

First, a notation:

$[A]$ = graphs $\cong$ to A

+ an assumption:

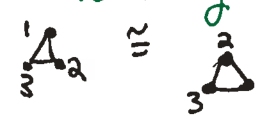
Cliques are bad!

Assume A, B graphs with no "nontrivial automorphisms"

i.e. not $\cong$ to self under relabeling

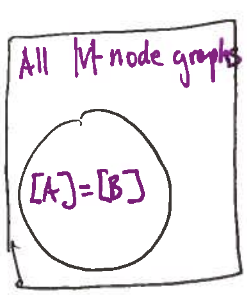
e.g. # distinct adjacency matrices

then $|[A]| = |[B]| = |V|!$

e.g. 

Why useful? let $U \leftarrow [A] \cup [B]$

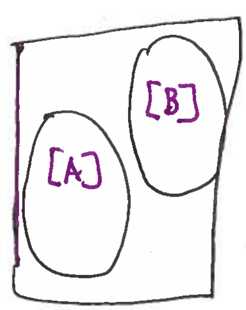
$A \cong B$



$|U| = |V|!$

"small"

$A \not\cong B$



$|U| = 2|V|!$

"big"

Goal: IP for proving a set is large

First Idea: Random Sampling?

Repeat **?** times:

$V \to P$: random $|V|$-node graph g

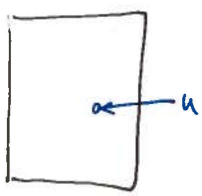
$P \to V$: if $g \in U$, a proof that it is a "success"

ie show $\cong$ to A or B

else nothing

Finally, V outputs $\dfrac{\#\text{successes}}{\text{total }\#\text{ loops}}$

- Adversarial P can't convince V that U is bigger
- How many loops needed? $\Omega\left(\dfrac{|U|}{\#\,|V|\text{-node graphs}}\right)$ just to hit one success

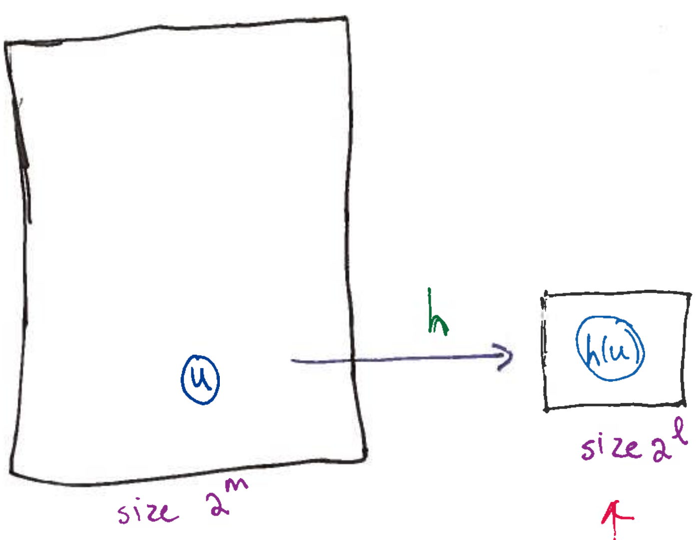


Problem: $|U|$ is very small compared to $\#$ $|V|$ node graphs

$\Rightarrow$ need many loops

$|h(U)| \leq |U|$ is obvious! but also not much smaller

Fix: Universal Hashing



m bits used to describe graph
$m \approx O(|V|^2)$
$\approx \Theta(n^2)$

Sample randomly here + estimate $\dfrac{|h(U)|}{2^\ell}$

(ℓ will be $\approx \Theta(\log |V|!) \approx \Theta(n \log n)$)

need:

1. $|h(U)| \approx |U|$

   $h(U)$ big iff $|U|$ big

2. $\dfrac{|h(U)|}{2^\ell}$ is $\dfrac{1}{\text{poly}(m)}$

   (in our case, constant)

3. h computable in poly time

Protocol:

given H, collection of p.i. fctns mapping $\{0,1\}^m \to \{0,1\}^\ell$

1. V picks $h \in_R H$
2. $V \to P$: h
3. $P \to V$: $x \in U$ s.t. $h(x) \in 0^\ell$
   with proof that $x \in U$
   (if possible)

idea

U big (i.e. $2|V|!$) : $h(U)$ usually hits 0^m so P can usually do it

U small (i.e. $|V|!$) : $h(U)$ usually doesn't hit 0^m so P usually can't do it

how?

map U to range of size $\approx 2V!$

if U big, it "fills" the range
& probably hits "0"

if U small, it only hits part of the range
$\Rightarrow$ less chance of hitting "0"

Recall H is p.i. $\overbrace{\text{if}}^{\text{family of hash fctns}}$ $\forall x,y \in \{0,1\}^m$ $\forall a,b \in \{0,1\}^\ell$

$$\Pr_{h \in H}[h(x)=a \;\&\; h(y)=b] = 2^{-2\ell}$$

Lemma H p.i., $U \subseteq \Sigma^m$ $\quad a = \frac{|U|}{2^\ell}$ ← would be fraction if h maps U 1-1

then $a - \frac{a^2}{2} \le \Pr_h[0^\ell \in h(U)] \le a$

Pf.

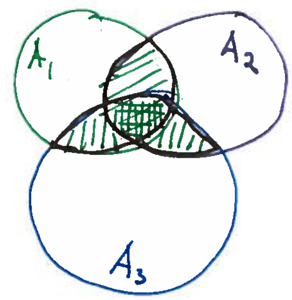
RHS:

$\forall x \quad \Pr_h[0^\ell = h(x)] = 2^{-\ell}$ (since $\mathcal{H}$ is p.i.)

so $\Pr_h[0^\ell \in h(U)] \le \sum_{x \in U} \Pr[0^\ell = h(x)] = \frac{|U|}{2^\ell} = a$

↑ union bnd

LHS: use inclusion-exclusion bnd:



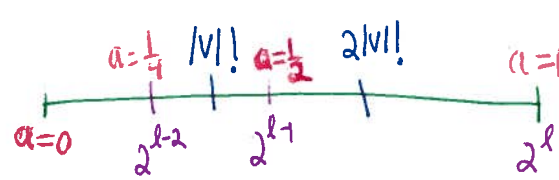
$$\Pr[\cup A_i] \ge \sum_i \Pr[A_i] - \sum_{i \ne j} \Pr[A_i \cap A_j]$$

$$\Pr_h[0^\ell \in h(U)] \ge \sum_{x \in U} \underbrace{\Pr[0^\ell \in h(x)]}_{2^{-\ell}} - \sum_{\substack{x,y \in U \\ x \ne y}} \underbrace{\Pr[0^\ell = h(x) = h(y)]}_{2^{-2\ell}}$$

$$= \frac{|U|}{2^\ell} - \binom{|U|}{2}\frac{1}{2^{2\ell}} \ge \frac{|U|}{2^\ell} - \frac{|U|^2}{2}\cdot\frac{1}{2^{2\ell}} \ge a - \frac{a^2}{2} \quad \blacksquare$$

Finishing up?

pick ℓ s.t. $2^{\ell-1} \le 2|V|! \le 2^\ell$



$\not\cong \;\Rightarrow\; |U| = 2|V|!$

$\frac{1}{2} \le a \le 1$

so $\Pr[V \text{ accepts}] \ge a - \frac{a^2}{2} \ge 3/8 = \alpha$

$\cong \;\Rightarrow\; |U| = |V|!$

$\frac{1}{4} \le a \le 1/2$

so $\Pr[V \text{ accepts}] \le 1/2 = \beta$

whoops!
need
$\alpha > \beta$
solution: HW

Idea for general Thm:

i.e. $IP_{\substack{\text{private}\\\text{coins}}} = IP_{\substack{\text{public}\\\text{coins}}}$

argue that l.b. protocol can be used to show that size of accepting region probability mass is large.

(need that can verify a conversation/random coin to be in accept region)