Lecture 6

- Random bits for Interactive Proofs
- IP public vs. private coins
- IP protocol for lower bounding a set size
Interactive Proofs

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

\(\text{IP: generalization of NP:}\)

- short proofs \(\Rightarrow\) short interactive proofs
  "Conversations that convince"

**Model**

```
Input

Verifier

Random bits

Workspace

ptime has 0

W

R

Conversation tapes

R

W

All powerful provers \(\subseteq\) unbounded time recursive

Can assume deterministic
```

**Def** "Interactive Proof Systems" (IPS) 

- for language \(L\) is protocol st.
  - if \(V, P\) follow protocol \(\land x \in L\) then \(\Pr_{V, P} [V \text{ accepts } X] \geq \frac{2}{3}\)
  - if \(V\) follows protocol \(\land x \notin L\) then \(\Pr_{V, P} [V \text{ rejects } X] \geq \frac{2}{3}\)

↑ what if require that \(P\) follow protocol? Forcibly useless!
\[ \text{def } I_P = \{ L \mid L \text{ has IP} \} \]

**Note:** Clearly \( \text{NP} \subseteq I_P \)

It turns out that \( I_P = \text{PSPACE} \).

---

**Graph Isomorphism (GI)**

- **Input:** \( G, H \)
- **Output:** \( G \cong H \) (i.e., \( \exists \phi \text{ s.t. } (u, v) \in E_G \text{ if } (\phi(u), \phi(v)) \in E_H \) )

**Note:** \( GI \in \text{NP} \Rightarrow GI \in I_P \)

\( GI \) not known to be in \( P \) (though is now known to be in \( \text{quasi-P} \) [Babai]).

---

**Graph Non-Isomorphism (GNI)**

- **Input:** \( G, H \)
- **Output:** \( G \not\cong H \)?

**Note:** \( GNI \) not known to be in \( P \) or \( \text{NP} \)

but is in \( I_P \) [Gottreich, Mikul's, Wigderson].

(And \( \text{quasi-P} \) [Babai]).
IP Protocol for graph $G$:

**Input** $G,H$

**Protocol** 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 $P$

- $P \rightarrow V$: $\frac{1}{2}$

- $V$ flip $\frac{X}{Y}$ 

<table>
<thead>
<tr>
<th>$H$</th>
<th>$H'$</th>
<th>$T$</th>
<th>$T'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
<td>$\frac{1}{2}$</td>
</tr>
</tbody>
</table>

  **V output**

  - continue
  - fail + halt
  - fail + halt

  **Fact** $G \neq H$

  Output "ACCEPT"
Proof of correctness

- If \( G \neq H \), P can figure out coin toss and always answer correctly. Here we use that P has unbounded time.

- If \( G = H \), need to show that P cannot fool \( V_S \).

  . Distribution of \( V_S \)'s msgs are identical under \( H/T \).

  . Since P deterministic wlog,

  \[ \Pr \left[ \text{fail in round } i \right] = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot (1-q) = \frac{1}{2} \]

  Prob V picks \( H \)\)
  Prob V picks \( T \)\)
  Prob V answers \# \)

Note \( V_S \)'s random perm + coin flips must be hidden, or P could cheat!
Arthur-Merlin Games

Vs. random tape is public!

\[ \Rightarrow \text{this protocol breaks} \]

Can Graphs have 1PS 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:

\[
[A] = \text{graphs isomorphic to A}
\]

+ an assumption:

Assume \( A, B \) graphs with no "nontrivial automorphisms" e.g. distinct adjacency matrices

\[ [A] = [B] = |V|! \]

Why useful? Let \( U = [A] \cup [B] \)

\( A \cong B \) All \( n \)-node graphs

\( |A| = |B| \)

\( 1U| = |V|! \)

"Small"

\( |B| \)

\( 1U| = 2|V|! \)

"big"

Goal: IP for proving a set is large
First Idea: Random Sampling?

Repeat \( \mathbb{E} \) times:

- \( V \to P \): random \( \mathcal{M} \)-node graph \( g \)
- \( P \to V \): if get \( U \), a proof that it is a "success"
  - i.e., show \( \cong \) to \( A \) or \( B \)
  - else nothing

Finally, \( V \) outputs \( \frac{\# \text{successes}}{\text{total \# loops}} \)

- Adversarial \( P \) can't convince \( V \) that \( U \) is bigger
- How many loops needed? \( \mathcal{O}(\frac{\#(\mathcal{M})}{\#(\mathcal{M}) \text{-node graphs}}) \)

Problem: \( |\mathcal{M}| \) is very small

\( \Rightarrow \) need many loops

Fix: Universal Hashing

\( m \) bits used to describe graph
\( m \approx O(\sqrt{\#(\mathcal{M})}) \)

- Need: \( |h(u)| \approx |u| \)
- \( h(u) \) big iff \( |u| \) big

\( \frac{|h(u)|}{2^e} \) is \( \frac{1}{\text{poly}(m)} \)

(in our case, constant)

- \( h \) computable in \( \text{poly time} \)
Protocol:

given $H$, collection of p.i. P ws mapping $\Sigma^m \rightarrow \Sigma^l$

1. $V$ picks $h \in H$
2. $V \rightarrow P: h$
3. $P \rightarrow V: x \in U$ st. $h(x) \in 0^l$

with proof that $x \in U$ (if possible)

Idea

- $u$ big (i.e. $2^{|U|}$): $h(u)$ usually hits $0^m$ so $P$ can usually do it
- $u$ small (i.e. $|U|$): $h(u)$ usually doesn't hit $0^m$ so $P$ usually can't do it

How?

- map $u$ to range of size $\approx 2^{|U|}$
- if $u$ big, it "fills" the range
- $h$ probably hits "0"
- if $u$ small, it only hits part of the range
  $\Rightarrow$ less chance of hitting "0"

Recall

$H$ is p.i. if \[
\forall x, y \in \Sigma^m \quad \forall a, b \in \Sigma^l
\]

\[
Pr_{h \leftarrow H}[h(x) = a \land h(y) = b] = 2^{-2l}
\]

Lemma

$H$ p.i., $u \in \Sigma^m$

\[
a = \frac{|U|}{2^l}
\]

Then

\[
a - \frac{a^2}{2} \leq Pr_{h}[a \in h(U)] \leq a
\]
pf.

RHS:

\[ \forall x \ \Pr[h(x) = 0^l] = 2^{-l} \quad \text{(since } k \text{ is p.a.)} \]

so \[ \Pr[h(u) = 0^l] \leq \sum_{x \in \mathbb{U}} \Pr[h(x) = 0^l] = \frac{|U|}{2^l} = a \]

\[ \uparrow \quad \text{union bnd} \]

LHS:

use inclusion-exclusion bnd:

\[ \Pr[\bigcup_{i} A_i] \geq \sum_{i} \Pr[A_i] - \sum_{i \neq j} \Pr[A_i \cap A_j] \]

\[ \Pr[h(u) = 0^l] \geq \sum_{x \in \mathbb{U}} \Pr[h(x) = 0^l] = \sum_{x \neq y} \Pr[h(x) = h(y)] \]

\[ = \frac{|U|}{2^l} - (\frac{|U|}{2}) \cdot \frac{1}{2^l} = \frac{|U|}{2^l} - \frac{|U|^2}{2^l} \cdot \frac{1}{2^l} \geq \frac{a - a^2}{2} \quad \blacksquare \]

Finishing up?

pick \ l \ s.t. \ 2^{l-1} \leq 2|V|! \leq 2^{l} \]

so \[ 1/2 \leq a \leq 1 \]

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

\[ \Rightarrow 1|V|! = |V|! \]

\[ \frac{1}{4} \leq a \leq \frac{1}{2} \]

\[ \text{so } \Pr[V \text{ accepts}] \leq \frac{1}{2} = \beta \]

\[ \alpha \neq a \quad |V|! \]

\[ \alpha = a = \frac{1}{2} = 2|V|! \]

Whoops!

need \ \alpha > \beta

solution: if w
Idea for general Thm:

i.e. $\text{IP}_{\text{private coins}} = \text{IP}_{\text{public coins}}$

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

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