18.404/6.840 Lecture 25

Last time:

- Schwartz-Zippel Theorem
- $EQ_{\mathrm{ROBP}} \in$ BPP

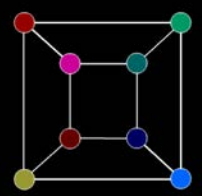
Today: (Sipser §10.4)

- Interactive Proof Systems
- The class IP
- Graph isomorphism problem
- coNP $\subseteq$ IP (part 1)

Interactive Proofs – Introduction

Illustration: Graph isomorphism testing

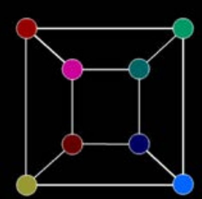
Defn: Undirected graphs G and H are isomorphic if they are identical except for a permutation (rearrangement) of the nodes.



Interactive Proofs – Introduction

Illustration: Graph isomorphism testing

Defn: Undirected graphs G and H are <u>isomorphic</u> if they are identical except for a permutation (rearrangement) of the nodes.



Defn: $ISO = \{\langle G, H \rangle \mid G$ and H are isomorphic graphs$\}$

$ISO \in$ NP

$ISO \in$ P ?

ISO is NP-complete ?

$\overline{ISO} \in$ NP ?

$ISO \in$ NP therefore a Prover can convince a poly-time Verifier that G and H are isomorphic (if true).

Even though $\overline{ISO} \in$ NP is unknown,

a Prover can still convince a poly-time Verifier that G and H are <u>not</u> isomorphic (if true).

Requires *interaction* and a *probabilistic* Verifier.

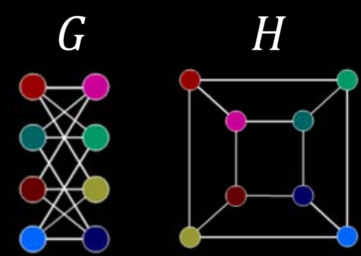
Interactive Proofs – informal model

Probabilistic
polynomial time TM

Professor = Verifier (V)

Unlimited
computation

Graduate Students = Prover (P)



Professor wants to know if graphs G and H are isomorphic.
- He asks his Students to figure out the answer.
- But he doesn't trust their answer. He must be convinced.

If the Students claim that G and H are isomorphic,
they can give the isomorphism and convince him.

But what if they claim that G and H are <u>not</u> isomorphic?
- The Professor randomly and secretly picks G or H and permutes it, then sends the result to the Students.
- If Students can identify which graph the Professor picked reliably (repeat this 100 times), then he's convinced.

Interactive Proofs – formal model

Two interacting parties
Verifier (V): Probabilistic polynomial time TM
Prover (P): Unlimited computational power

Both P and V see input w.
They exchange a polynomial number of polynomial-size messages.
Then V *accepts* or *rejects*.

Defn: Pr[(V ↔ P) accepts w] = probability that V accepts when V interacts with P, given input w.

Defn: IP $= \{A|$ for some V and P (This P is an "honest" prover)
$w \in A \rightarrow$ Pr [(V ↔ P) accepts w] $\geq {}^2\!/_3$
$w \notin A \rightarrow$ for any prover $\tilde{\mathrm{P}}$ Pr [(V ↔ $\tilde{\mathrm{P}}$) accepts w] $\leq {}^1\!/_3$

Think of $\tilde{\mathrm{P}}$ as a "crooked" prover trying to make V accept when it shouldn't.
An amplification lemma can improve the error probability from ${}^1\!/_3$ to ${}^1\!/_{2^{\mathrm{poly}\,(n)}}$

$\overline{ISO} \in$ IP

Theorem: $\overline{ISO} \in$ IP

Proof: Protocol for V and (the honest) P on input $\langle G, H \rangle$

1) Repeat twice:
2) V→P Randomly choose G or H and permute to get K, then send K
3) P→V Compare K with G and H. Send "G" or "H" (V's choice in step 2)
4) V *accepts* if P was correct both times. Otherwise V *rejects*.

Check-in 25.1

Suppose we change the model to allow the Prover access to the Verifier's random choices. Now consider the same protocol as described above. What language does it describe?

(a) $\{\langle G, H \rangle |\ G \neq H\}$

(b) $\{\langle G, H \rangle |\ G$ and H are not isomorphic $\}$

(c) $\{\langle G, H \rangle |\ G$ and H are any two graphs $\}$

(d) $\emptyset$

Check-in 25.1

Facts about IP – Checkin 25.2

Which of the following is true?
Check all that apply

a) NP $\subseteq$ IP

b) BPP $\subseteq$ IP

c) IP $\subseteq$ PSPACE

Surprising Theorem: PSPACE $\subseteq$ IP so IP = PSPACE

We will prove only a weaker statement: coNP $\subseteq$ IP

$\#SAT$ problem

Defn: $\#SAT = \{\langle \phi, k \rangle |$ Boolean formula ϕ has exactly k satisfying assignments$\}$

Let $\#\phi =$ the number of satisfying assignments of Boolean formula ϕ.
So $\#SAT = \{\langle \phi, k \rangle |\ k = \#\phi\}$

Defn: Language B is <u>NP-hard</u> if $A \leq_\mathrm{P} B$ for every $A \in$ NP.
(Note: B is NP-complete if B is NP-hard and $B \in$ NP.)

Theorem: $\#SAT$ is coNP-hard

Proof: Show $\overline{SAT} \leq_P \#SAT$

$$f(\langle \phi \rangle) = \langle \phi, 0 \rangle$$

To show coNP $\subseteq$ IP we will show $\#SAT \in$ IP

$\#SAT \in$ IP – notation

$\#SAT = \{\langle \phi, k\rangle |$ Boolean formula ϕ has exactly k satisfying assignments$\}$

Theorem: $\#SAT \in$ IP

Proof: First some notation. Assume ϕ has m variables $x_1, \ldots, x_m$.

Let $\phi(0)$ be ϕ with $x_1 = 0$ (0 substituted for x_1) 0 = FALSE and 1 = TRUE.
Let $\phi(01)$ be ϕ with $x_1 = 0$ and $x_2 = 1$.
Let $\phi(a_1 \ldots a_i)$ be ϕ with $x_1 = a_1, \ldots, x_i = a_i$ for $a_1, \ldots, a_i \in \{0,1\}$.
Call $a_1, \ldots, a_i$ presets. The remaining $x_{i+1}, \ldots, x_m$ stay as unset variables.

Let $\#\phi$ = the number of satisfying assignments of ϕ.
Let $\#\phi(0)$ = the number of satisfying assignments of $\phi(0)$.
Let $\#\phi(a_1 \ldots a_i)$ = the number of satisfying assignments of $\phi(a_1 \ldots a_i)$

Equivalently: $$\#\phi(a_1 \ldots a_i) = \sum_{\substack{a_{i+1}, \ldots, a_m \\ \in \{0,1\}}} \phi(a_1 \ldots a_m)$$

Check-in 25.3

If $\#\phi = 9$ and $\#\phi(0) = 6$ then what do we know?

a) $\#\phi(1) = 3$
b) $\#\phi(1) = 15$
c) $\#\phi(00) \leq 5$
d) none of these

1. $\#\phi(a_1 \ldots a_i) = \#\phi(a_1 \ldots a_i 0) + \#\phi(a_1 \ldots a_i 1)$
2. $\#\phi(a_1 \ldots a_m) = \phi(a_1 \ldots a_m)$

Check-in 25.3

$\#SAT \in$ IP – 1st attempt

Theorem: $\#SAT \in$ IP

Proof: Protocol for V and (the honest) P on input $\langle \phi, k \rangle$

0) P sends $\#\phi$; V checks $k = \#\phi$

1) P sends $\#\phi(0), \#\phi(1)$; V checks $\#\phi = \#\phi(0) + \#\phi(1)$

2) P sends $\#\phi(00), \#\phi(01), \#\phi(10), \#\phi(11)$; V checks $\#\phi(0) = \#\phi(00) + \#\phi(01)$

$\#\phi(1) = \#\phi(10) + \#\phi(11)$

$\vdots$

m) P sends $\#\phi(\overbrace{0 \cdots 0}^{m}), \ldots, \#\phi(1 \cdots 1)$; V checks $\#\phi(\overbrace{0 \cdots 0}^{m-1}) = \#\phi(\overbrace{0 \cdots 00}^{m-1}) + \#\phi(0 \cdots 01)$

$\vdots$

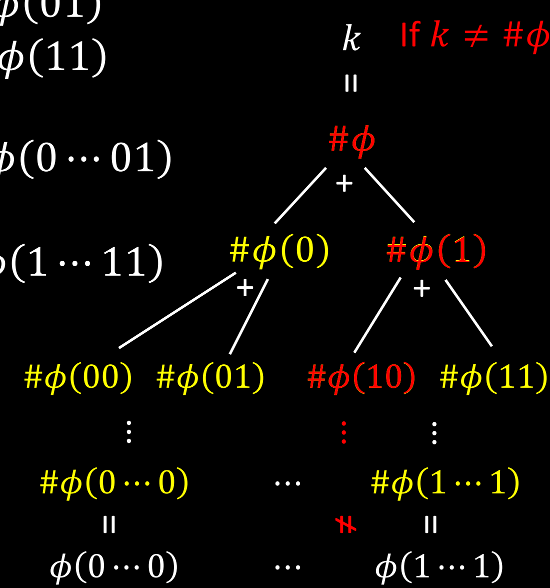
V checks $\#\phi(1 \cdots 1) = \#\phi(1 \cdots 10) + \#\phi(1 \cdots 11)$

$m+1$) V checks $\#\phi(\overbrace{0 \cdots 0}^{m}) = \phi(0 \cdots 0)$

$\vdots$

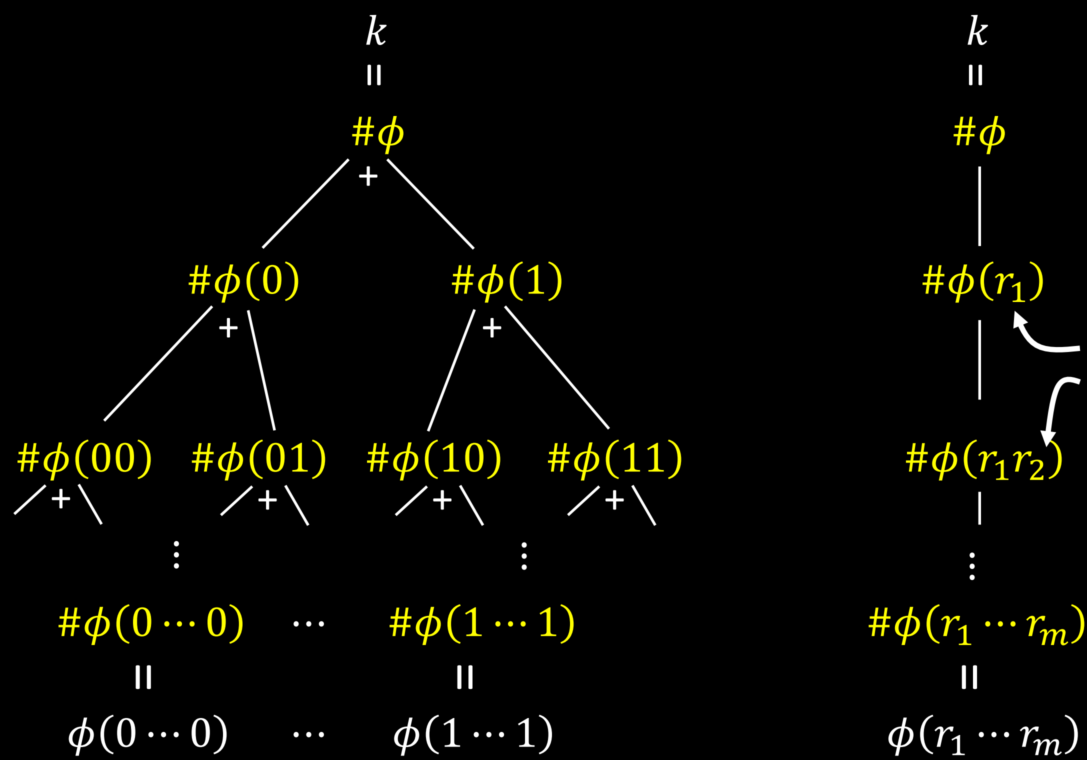
$\#\phi(1 \cdots 1) = \phi(1 \cdots 1)$

V *accepts* if all checks are correct. Otherwise V *rejects*.



Problem: Exponential. How to fix?

Idea for fixing $\#SAT \in$ IP protocol



Non-Boolean assignments to the variables of ϕ

To be continued…

Quick review of today

1. Introduced the interactive proof system model
2. Defined the class IP
3. Showed $\overline{ISO} \in$ IP
4. Started showing $\#SAT \in$ IP to prove that coNP $\subseteq$ IP