E0 224 Computational Complexity Theory	**Indian Institute of Science, Bangalore**
Fall 2014	**Department of Computer Science and Automation**

Lecture 22: Oct 29, 2014

Lecturer: Chandan Saha `<chandan@csa.iisc.ernet.in>` *Scribe: Pawan Kumar*

22.1 Interactive proof for graph non-isomorphism

In this lecture we will show that the language GNI is in class IP. Two graphs G_1 and G_2 are isomorphic if there is a permutation π of the labels of the nodes of G_1 such that $\pi(G_1) = G_2$, where $\pi(G_1)$ is the labeled graph obtained by applying π on its vertex labels.

Definition 22.1. $GNI = \{< G_1, G_2 >: G_1 \ncong G_2 \ i.e.\ G_1 \ and \ G_2 \ are \ nonisomorphic\}$

Definition 22.2. $GI = \{< G_1, G_2 >: G_1 \cong G_2 \ i.e.\ G_1 \ and \ G_2 \ are \ isomorphic\}$

Claim: $GI \in NP$

Proof. The certificate is the description of permutation π. One can apply the permutation π on the vertices of G_1 and check whether $\pi(G_1) = G_2$ in polynomial time. □

Interactive protocol for GNI
Input: Adjacency matrices of G_1 and G_2. (w.l.o.g. let n be the no. of vertices in $G_1 \& G_2$)
V: Verifier picks $i \in_R \{1, 2\}$ and a random $\pi \in S_n$, where set S_n contains all permutations of first n natural numbers. Computes $H = \pi(G_i)$, sends H to prover.
P: Prover sends $j \in \{1, 2\}$ to V after seeing H.
V: If $i = j$ then accept else reject.

observation: If $(G_1, G_2) \in GNI$ then $\exists P$ s.t.
$$Pr\left[Out_V < V, P > (G_1, G_2) = 1\right] = 1$$
If $(G_1, G_2) \notin GNI$ then $\forall P$
$$Pr\left[Out_V < V, P > (G_1, G_2) = 1\right] \leq \frac{1}{2}$$

Remark

- It appears the fact that verifier is keeping it's random coins secret is crucial.
- Class IP was defined in a work by Goldwasser, Micali, Rackoff in 1985.
- Laszlo Babai defined the classes AM(& MA) using public coins.

Definition 22.3. ***Class AM[k] (Arthur-Merlin) :*** *For any $k \in \mathbb{N}$, AM[k] is a subclass of IP[k], where the verifier only sends random strings to the prover and it is not allowed to use any other random bits that has not been revealed to the prover. Class AM[2] is also denoted by AM.*

Definition 22.4. ***Class MA (Merlin-Arthur) :*** *It is the class of languages with a two round public-coin interactive proof with the prover sending first message.*

Lemma : For every k>0, $AM[k] = AM$

Recall: BP.NP = $\{L : L \leq_R 3 - SAT\}$
Lemma : AM = BP.NP

Proof. $\Rightarrow$ **AM** $\subseteq$ **BP.NP :** Suppose L $\in$ AM, we need to show that L $\in$ BP.NP. Let $x \in$ L, for fixed input x V picks a random string r and send r to P. Upon receiving r prover sends $a = g(x, r)$ to verifier. Now V runs polytime algorithm say $f(x, r, a)$. If $x \in$L then

$$\exists P \; s.t. \; Pr_r \left[Out_V < V, P > (x, a, r) = 1\right] \geq \frac{2}{3}$$

If x $\notin$ L then

$$\forall P \; Pr_r \left[Out_V < V, P > (x, a, r) = 1\right] \leq \frac{1}{3}$$

Note that for any strings x, r the execution between verifier and prover can be interpreted as non-deterministic computation such that V on input (x, r) has access to some witness a (provided by P), which is checked by the polytime V. That is the language $L' = \{(x, r) : \exists \; a \; s.t. \; V(x, r, a) = 1\}$ is in NP, and therefore there exist a formula $\phi_{x,r}$ such that $(x, r) \in L' \Leftrightarrow \phi_{x,r} \in 3 - SAT$. Observe that $Out_V < V, P > (x, a, r) = 1$ if & only if $(x, r) \in L' \iff \phi_{x,r} \in 3 - SAT$. Hence

$$x \in L \Rightarrow Pr_r \left[\phi_{x,r} \in 3 - SAT\right] \geq \frac{2}{3}$$
$$x \notin L \Rightarrow Pr_r \left[\phi_{x,r} \in 3 - SAT\right] \leq \frac{1}{3}$$

Hence, $L \in BP.NP$
$\Leftarrow$ **BP.NP** $\subseteq$ **AM :** Suppose L$\in$ BP.NP, we need to show that L $\in$ AM. Since L $\in$ BP.NP there is a polytime algorithm f for constructing a formula $\phi_{x,r} = f(x, r)$ such that for every string x

$$x \in L \Rightarrow Pr_r \left[\phi_{x,r} \in 3 - SAT\right] \geq \frac{2}{3}$$
$$x \notin L \Rightarrow Pr_r \left[\phi_{x,r} \in 3 - SAT\right] \leq \frac{1}{3}$$

The 2-round protocol for deciding L is as follows: The verifier sends to the prover a random string r, and the prover replies with a satisfying assignment for $\phi_{x,r}$. At the end, the verifier checks that indeed the assignment is satisfying for $\phi_{x,r}$. □

Theorem 22.5. *(Goldwasser-Sipser) For every* $k : \mathbb{N} \rightarrow \mathbb{N}$*, with* $k(n)$ *computable in polytime, IP[k]*$\subseteq$ *AM[k+2]*

We'll now show an AM protocol for GNI.

Claim : Define the following set for two graphs G_1 and G_2. $S = \{(H, \pi) : H \cong G_1 or H \cong G_2 \; and \; \pi \in auto(H) \; \}$ where π is an automorphism of H.

Case 1: If $G_1 \cong G_2$ then $|S| = n!$
Case 2: If $G_1 \ncong G_2$ then $|S| = 2n!$

Proof. For an n-vertex graph consider the multiset $all(G) = \{\pi_1(G), ..., \pi_{n!}(G)\}$ of all permuted version of G. This is indeed a multi-set since it is possible that $\pi_i(G) = \pi_j(G)$ even when $\pi_i \neq \pi_j$. Let $auto(G) = \{\pi | \pi(G) = G\}$ be the automorphisms of G. Let $iso(G)$ be the set $\{\pi(G)|\pi \ is\ a\ permutation\}$. We claim that for any n-vertex graph G we have:

$$|auto(G)|\,.\,|iso(G)| = n!$$

The reason is that our original set $all(G)$ has exactly n! elements in it, but each graph in $iso(G)$ appears exactly $auto(G)$ times in $all(G)$ (because $|auto(G)| = |auto(\pi(G))|$ for any permutation π) Note that if $G_1 \cong G_2$ then H isomorphic to $G_1 \Leftrightarrow$ it is isomorphic to G_2; also the number of automorphisms of any such H is exactly $|auto(G_1)|$. So the size of S is exactly $|auto(G_1)|\,.\,|iso(G_1)| = n!$. On the other hand, if $G_1 \ncong G_2$ then the graphs isomorphic to G_1 are distinct from those graphs isomorphic to G_2. So the size of S in this case is

$$|auto(G_1)|\,.\,|iso(G_1)| + |auto(G_2)|\,.\,|iso(G_2)| = 2n!$$

□

Definition 22.6. ***Pairwise independent hash functions:*** *Let $\mathbb{H}_{m,q}$ be a collection of functions from $\{0,1\}^m$ to $\{0,1\}^q$. $\mathbb{H}_{m,q}$ is pairwise independent if $\forall x, x' \in \{0,1\}^m$ with $x \neq x'$ and $\forall y, y' \in \{0,1\}^q$,* $\underset{h \in_R \mathbb{H}_{m,q}}{Pr} \{h(x) = y \ \ and \ \ h(x') = y'\} = \frac{1}{2^{2q}}$.

Protocol: Goldwasser-Sipser Set Lower Bound Protocol

Notations: Let $S \subseteq \{0,1\}^m$ be a set such that membership in S can be certified efficiently. The prover's goal is to convince the verifier that $|S| \geq K$ and if $|S| \leq \frac{K}{2}$ then verifier will reject with high probability, where $K = 2n!$ and q be such that $2^{q-2} < K \leq 2^{q-1}$

V: Verifier picks a random $h \in \mathbb{H}_{m,q} = \mathbb{H}$(say), picks $y \in_R \{0,1\}^q$ and sends h , y to prover P.

P: Prover returns an $x \in \{0,1\}^m$ and a z (an honest prover returns an x in S s.t. $h(x) = y$ if such an x exists and z certifies that $x \in S$).

V: If $h(x) = y$ and z certifies that $x \in S$ then accept; otherwise reject.

Theorem 22.7. *GNI ∈ AM*

Proof. We need to show that there exists a 2-round protocol s.t.

if $< G_1, G_2 > \in GNI$ i.e. $G_1 \ncong G_2$ then probability of acceptance is high.

if $< G_1, G_2 > \notin GNI$ i.e. $G_1 \cong G_2$ then probability of acceptance is low.

The protocol is defined above. By using the above claim we compute the acceptance probability in two cases:

Case 1: If $|S| = n! = \frac{K}{2}$

$$\underset{\substack{h \in_R \mathbb{H} \\ y \in_R \{0,1\}^q}}{Pr} \{\exists x \in S, s.t.\ h(x) = y\} \leq \frac{n!}{2^q} = \frac{K}{2^{q+1}} \tag{22.1}$$

Case 2: If $|S| = 2n! = K$

$$\underset{\substack{h \in_R \mathbb{H} \\ y \in_R \{0,1\}^q}}{Pr} \{\exists x \in S, s.t.\ h(x) = y\} \geq ? \tag{22.2}$$

Now we fix y arbitrarily and compute the probability $\underset{h \in_R \mathbb{H}}{Pr} \{\exists x \in S, s.t.\ h(x) = y\}$

Let E_x be the event that $h(x) = y$, according to inclusion exclusion principle

$$Pr\left\{\bigvee_x E_x\right\} \geq \sum_x Pr\{E_x\} - \frac{1}{2}\sum_{x \neq x'} Pr\{E_x \cap E_{x'}\} \tag{22.3}$$

$$Pr\{E_x\} = \frac{1}{2^q} \tag{22.4}$$

$$Pr\{E_x \cap E_{x'}\} = \frac{1}{2^{2q}}(\text{as } h \text{ is picked from } \mathbb{H}_{m,q}) \tag{22.5}$$

$$\underset{h \in_R \mathbb{H}}{Pr}\{\exists x \in S, s.t.\ h(x) = y\} \geq \sum_{x \in S} \frac{1}{2^q} - \frac{1}{2}\sum_{x \neq x'} \frac{1}{2^{2q}} \tag{22.6}$$

Now put the value of equation 22.6 in equation 22.2

$$\begin{aligned}
\underset{h \in_R \mathbb{H}}{Pr}\{\exists x \in S, s.t.\ h(x) = y\} &\geq \sum_{x \in S} \frac{1}{2^q} - \frac{1}{2}\sum_{x \neq x'} \frac{1}{2^{2q}} \\
&\geq \frac{|S|}{2^q} - \frac{|S|^2}{2.2^{2q}} \\
&= \frac{K}{2^q} - \frac{K^2}{2.2^{2q}} \\
&= \frac{K}{2^q}(1 - \frac{K}{2^{q+1}}) \\
&\geq \frac{K}{2^q}(1 - \frac{2^{q-1}}{2^{q+1}}) \\
&= \frac{3}{4}\frac{K}{2^q}
\end{aligned}$$

□

Lemma: Let $p = \frac{|S|}{2^q}$ then

$$\frac{3}{4}p \leq \underset{\substack{h \in_R \mathbb{H} \\ y \in_R \{0,1\}^q}}{Pr}\{\exists x, h(x) = y\} \leq p$$

Note: If we repeat the lower bound protocol independently M times, where M is in $poly(|x|)$, we can tightly bound the probability of acceptance by using Chernoff bound.

Case 1: If $|S| = \frac{K}{2}$ i.e. $G_1 \cong G_2$ and verifier accepts then this is bad event

$$Pr[\text{'Bad Event'}] = Pr[\text{'V accepts'}] \leq \frac{K}{2.2^q}$$

Case 2: If $|S| = K$ i.e. $G_1 \ncong G_2$ and verifier accepts then this is good event

$$Pr[\text{'Good Event'}] = Pr[\text{'V accepts'}] \geq \frac{3}{4}\frac{K}{2^q}$$

Remark: For single iteration
if case 1 then $Pr[\text{'V accepts'}] \leq \frac{K}{2.2^q}$
if case 2 then $Pr[\text{'V accepts'}] \geq \frac{3}{4}\frac{K}{2^q}$

Let X_i be the indicator random variable defined as below,

$$X_i = \begin{cases} 1 & \text{if V accepts in } i^{th} \text{ iteration} \\ 0 & \text{if V rejects in } i^{th} \text{ iteration} \end{cases}$$

Let $X = \sum_{i=1}^{M} X_i$,

$$Pr\left[X_i = 1\right] = Pr\left[\text{V accepts}\right]$$

$$\begin{aligned}\mathbb{E}\left[X\right] &= \mathbb{E}\left[\sum_{i=1}^{M} X_i\right] \\ &= \sum_{i=1}^{M} \mathbb{E}\left[X_i\right] \text{ (linearity of expectation as } X_i's \text{ are iids)} \\ &= \sum_{i=1}^{M} P(X_i = 1)\end{aligned}$$

For case 1 $\mathbb{E}\left[X\right] \leq \frac{1}{2}\frac{K}{2^q}M$
For case 2 $\mathbb{E}\left[X\right] \geq \frac{3}{4}\frac{K}{2^q}M$

If the expected value is close to $\frac{1}{2}\frac{K}{2^q}M$ then output $G_1 \cong G_2$, if expected value is close to $\frac{3}{4}\frac{K}{2^q}M$ then output $G_1 \ncong G_2$. We know that for case 1 expected value is less than equal to $\frac{1}{2}\frac{K}{2^q}M$ and the error probability is $Pr\left[X > (1+\delta)\mathbb{E}\left[X\right]\right]$. In case 2 expected value is greater than equal to $\frac{3}{4}\frac{K}{2^q}M$ and the error probability is $Pr\left[X < (1-\delta)\mathbb{E}\left[X\right]\right]$. We'll apply Chernoff bound to restrict these error probabilities as follows
For case 1

$$Pr\left[X > (1+\delta)\mathbb{E}\left[X\right]\right] \leq e^{-\frac{\mathbb{E}[X]\delta^2}{3}}$$

For case 2

$$Pr\left[X < (1-\delta)\mathbb{E}\left[X\right]\right] \leq e^{-\frac{\mathbb{E}[X]\delta^2}{2}}$$

We need to upper bound the error probability in both the cases.

Case 1: In this case $Pr\left[\text{Error}\right] = Pr\left[X > (1+\delta)\frac{1}{2}\frac{K}{2^q}M\right]$ and $\mathbb{E}\left[X\right] \leq \frac{1}{2}\frac{K}{2^q}M$
we can not directly apply the Chernoff bound because if $\mathbb{E}\left[X\right] = 0$ then $Pr\left[Error\right] \leq 1$ which is obvious and is of no use. Hence we'll apply the Markov's inequality. By Markov's inequality

$$Pr\left[\text{Error}\right] = Pr\left[X > (1+\delta)\frac{1}{2}\frac{K}{2^q}M\right] \leq \frac{\mathbb{E}\left[\mathbb{X}\right]}{(1+\delta)\frac{1}{2}\frac{K}{2^q}M}$$

If $\mathbb{E}\left[X\right] \leq \frac{1}{3}\frac{1}{2}\frac{K}{2^q}M$ then Pr[Error] $\leq \frac{1}{3}$
Else i.e. ($\mathbb{E}\left[X\right] \geq \frac{1}{3}\frac{1}{2}\frac{K}{2^q}M$) we need to apply the chernoff bound

$$
\begin{aligned}
\mathbb{E}[X] &\leq \frac{1}{2}\frac{K}{2^q}M \\
&\Rightarrow (1+\delta)\mathbb{E}[X] \leq (1+\delta)\frac{1}{2}\frac{K}{2^q}M \\
&\Rightarrow \text{if } X > (1+\delta)\frac{1}{2}\frac{K}{2^q}M \text{ then } X > (1+\delta)\mathbb{E}[X] \\
&\Rightarrow Pr\left[X > (1+\delta)\frac{1}{2}\frac{K}{2^q}M\right] \leq Pr[X < (1+\delta)\mathbb{E}[X]] \\
&\leq e^{-\frac{\mathbb{E}[X]\delta^2}{3}} \text{(using chernoff bound)} \\
&= \frac{1}{e^{\frac{\mathbb{E}[X]\delta^2}{3}}} \\
&\leq \frac{1}{e^{\frac{1}{2}\frac{K}{2^q}M\frac{\delta^2}{9}}} \text{ as } \mathbb{E}[X] \geq \frac{1}{3}\frac{1}{2}\frac{K}{2^q}M
\end{aligned}
$$

Remark: By increasing the number of rounds i.e. M we can decrease the error probability. Error probability for this case say EP_1=$Pr[Error] \leq min(\frac{1}{3}, \frac{1}{e^{C_1 \cdot M}}) \leq \frac{1}{3}$, where $C_1 = \frac{1}{2}\frac{K}{2^q}\frac{\delta^2}{9}$ is constant.

Case 2: In this case $Pr[\text{Error}] = Pr\left[X < (1-\delta)\frac{3}{4}\frac{K}{2^q}M\right]$

$$
\begin{aligned}
\mathbb{E}[X] &\geq \frac{3}{4}\frac{K}{2^q}M \\
&\Rightarrow (1-\delta)\mathbb{E}[X] \geq (1-\delta)\frac{3}{4}\frac{K}{2^q}M \\
&\Rightarrow \text{if } X < (1-\delta)\frac{3}{4}\frac{K}{2^q}M \text{ then } X < (1-\delta)\mathbb{E}[X] \\
&\Rightarrow Pr\left[X < (1-\delta)\frac{3}{4}\frac{K}{2^q}M\right] \leq Pr[X < (1-\delta)\mathbb{E}[X]] \\
&\leq e^{-\frac{\mathbb{E}[X]\delta^2}{2}} \text{(using chernoff bound)} \\
&= \frac{1}{e^{\frac{\mathbb{E}[X]\delta^2}{2}}} \\
&\leq \frac{1}{e^{\frac{3}{4}\frac{K}{2^q}M\frac{\delta^2}{2}}}
\end{aligned}
$$

Remark: Error probability for this case say $EP_2 = Pr[\text{Error}] \leq \frac{1}{e^{C_2 \cdot M}}$, where $C_2 = \frac{3}{4}\frac{K}{2^q}\frac{\delta^2}{2}$ is constant. Hence the overall error probability $Pr[Error] = max(EP_1, EP_2) \leq \frac{1}{3}$

Choose a δ such that

$$
\begin{aligned}
(1+\delta)\frac{K}{2^{q+1}}M &< (1-\delta)\frac{3}{2}\frac{K}{2^{q+1}}M \\
(1+\delta) &< (1-\delta)\frac{3}{2} \\
\frac{(1+\delta)}{(1-\delta)} &< \frac{3}{2}
\end{aligned}
$$

For example, $\delta = \frac{1}{10}$ suffices.

Lemma: If GI is NP-Complete then PH collapses.

Proof. Let us assume GI $\in$ NP-Complete

$$\begin{aligned}
&\Rightarrow GNI \in Co-NPC \\
&\Rightarrow \overline{3-SAT} \leq_P GNI \\
&\Rightarrow \overline{3-SAT} \in BP.NP \;(as\ GNI \in AM = BP.NP) \\
&\Rightarrow \overline{3-SAT} \leq_R 3-SAT \\
&\Rightarrow Co-NP \subseteq BP.NP \subseteq NP_{/poly}
\end{aligned}$$

Note: Assignment Problem If Co-NP $\subseteq NP_{/poly}$ then PH collapses to $\sum_3^P$. (This is also known as Yap's theorem). □

References

[M1] S. ARORA and B. BARAK "Computational Complexity: A Mordern Approach," *Cambridge University Press*, 2009