INFR11102: Computational Complexity 21/11/2019

Lecture 19: Graph Isomorphisms

Lecturer: Heng Guo

1 An Arthur-Merlin protocol for GNI

Last time we gave a simple interactive protocol for GNI with private coins. We will show that it can also be achieved using only public coins.

Theorem 1. GNI $\in$ AM.

We will take a more quantitative approach. For any graph G with n vertices, let $\mathrm{aut}(G) = \{\pi \mid \pi(G) = G\}$ be its automorphism group. Let $\mathrm{iso}(G) = \{\pi(G) \mid \pi \in S_n\}$ be the set of graphs isomorphic to G. Consider the set $\{(G, \pi) \mid \pi \in S_n\}$. Clearly $\pi(G) \in \mathrm{iso}(G)$, and each one appears exactly $|\mathrm{aut}(G)|$ times. Namely,

$$n! = |\{(G, \pi) \mid \pi \in S_n\}| = |\mathrm{aut}(G)| \cdot |\mathrm{iso}(G)| \,.$$

Now, for G_1 and G_2, define

$$S := \{(G', \sigma) \mid \sigma \in \mathrm{aut}(G'), G' \cong G_1 \text{ or } G' \cong G_2\}.$$

Thus, if $G_1 \cong G_2$, then $|S| = n!$, and otherwise $|S| = 2n!$.

To distinguish these two cases, once again we will use pairwise independent hash family. Let $\mathcal{H}$ be such a family from S to T where T is some arbitrary set of size $4n!$. Fix a particular element $\alpha \in T$. Our protocol is the following:

1. Arthur picks a random function $H \in \mathcal{H}$ and present it to Merlin;
2. Merlin returns an element $(G', \sigma) \in S$ and a permutation τ;
3. Arthur accepts if (1) $\tau(G') = G_1$ or G_2; (2) $\sigma(G') = G'$; and (3) $H(G', \sigma) = \alpha$.

Note that the last verification step can be done easily in deterministic polynomial time. Conditions (1) and (2) verify that (G', σ) is indeed a element of S, and (3) asserts a fact whose probability to happen distinguishes the two scenarios of S.

If $|S| = n!$, then by the definition of pairwise independent hash function,

$$\Pr_{H \in \mathcal{H}}[\exists s \in S,\ H(s) = \alpha] \le \frac{|S|}{|T|} = \frac{1}{4}.$$

Otherwise $|S| = 2n!$, then by inclusion-exclusion,

$$\begin{aligned}\Pr_{H\in\mathcal{H}}[\exists s \in S,\ H(s) = \alpha] &\geq \sum_{s\in S} \Pr_{H\in\mathcal{H}}[H(s) = \alpha] - \sum_{s,s'\in S} \Pr_{H\in\mathcal{H}}[H(s) = H(s') = \alpha] \\ &= \frac{|S|}{|T|} - \binom{|S|}{2} \cdot \frac{1}{|T|^2} \\ &\geq \frac{1}{2} - \frac{|S|^2}{2\,|T|^2} = \frac{1}{2} - \frac{1}{8} = \frac{3}{8}.\end{aligned}$$

Thus, we have created a constant gap in the accepting probability between the two cases. We can employ the standard "repeat and vote" trick to amplify such a gap. Details of the amplification are omitted.

2 Evidence against NP-completeness of graph isomorphisms

Recall the graph isomorphism (GI) problem. Since there was no efficient algorithm, it is natural to wonder whether the problem is NP-complete. However, this is also unlikely to be the case, unless the polynomial hierarchy collapses.

Theorem 2. *If* GI *is* NP*-complete, then* $\Sigma_2^p = \Pi_2^p$.

Proof. It is sufficient to show that if GI is NP-complete, then $\Sigma_2^p \subseteq \Pi_2^p$.

Consider the QBF_2 problem, which is complete for Σ_2^p and whose input are formulas of the following form:

$$\psi = \exists x \forall y\ \varphi(x, y).$$

Since by assumption, GI is NP-complete, GNI is coNP-complete. Thus, there is a reduction $R(\cdot)$ such that fixing x, $\psi'(x) := \forall y\ \varphi(x, y)$ is valid if and only if $R(\psi'(x)) \in$ GNI.

Last time, we showed that GNI $\in$ AM and AM $=$ AM$_1$ where AM$_1$ is the one-sided error version. Let $P(x) := R(\psi'(x))$. Thus, by appropriate amplification, there is a poly-time TM M such that

$$\begin{aligned}P(x) \in \text{GNI} &\Rightarrow \Pr_r[\exists z\ M(P(x), r, z) = 1] = 1; \\ P(x) \notin \text{GNI} &\Rightarrow \Pr_r[\exists z\ M(P(x), r, z) = 1] \leq 2^{-n-1},\end{aligned}$$

where $n = |x|$ and both r and z all have length bounded by a polynomial in n.

We claim that

$$\psi \text{ is valid} \Leftrightarrow \forall r \exists x \exists z\ M(P(x), r, z) = 1. \tag{1}$$

This implies the theorem. To verify (1), we have two cases:

1. If ψ is valid, then $\exists x$ such that $P(x) \in$ GNI which implies that

$$\exists x \forall r \exists z, M(P(x), r, z) = 1.$$

   This implies that $\forall r \exists x \exists z$, $M(R(\psi'(x)), r, z) = 1$.

2. If ψ is not valid, then $\forall x$, $P(x) \notin$ GNI. Thus,

$$\forall x \Pr_r[\exists z\ M(P(x), r, z) = 1] \leq 2^{-n-1},$$

   which implies, via the union bound,

$$\begin{aligned} \Pr_r[\exists x \exists z\ M(P(x), r, z) = 1] &\leq \sum_{x \in \{0,1\}^n} \Pr_r[\exists z\ M(P(x), r, z) = 1] \\ &\leq 2^n \cdot 2^{-n-1} = 1/2 < 1. \end{aligned}$$

   In other words, $\Pr_r[\forall x \forall z\ M(P(x), r, z) = 0] > 0$. The probabilistic method implies that

$$\begin{aligned} &\exists r \forall x \forall z\ M(P(x), r, z) = 0 \\ \Leftrightarrow\ &\neg\left(\forall r \exists x \exists z\ M(P(x), r, z) = 1\right). \end{aligned}$$

□

If we look more carefully at the proof of Theorem 2, the only crucial property of GNI we used is that GNI $\in$ $\mathtt{AM}$.

Corollary 3. *If* $\mathtt{coNP} \subseteq \mathtt{AM}$, *then* $\Sigma_2^p = \Pi_2^p$.

Recall that $\mathtt{NP} \subseteq \mathtt{AM} \subseteq \Pi_2^p$. Corollary 3 implies that $\mathtt{AM}$ sits in an interesting position at the complexity landscape.

3 Counting graph isomorphisms

We have seen that some decision problems in $\mathtt{P}$ have $\#\mathtt{P}$-complete counting counterparts. One natural question is that whether the counting version of GI is easy or hard.

Name: #GI

Input: Two graphs G_1 and G_2.

Output: How many permutations are there to make G_1 identical to G_2?

Clearly #GI is no easier than GI. Next we show that they actually have the same complexity.

Theorem 4. $\#\mathrm{GI} \leq_t \mathrm{GI}$.

To show Theorem 4, we need an intermediate problem. Recall that $\mathrm{aut}(G)$ is the automorphism group of a graph G.

Name: #Aut

Input: A graph G.

Output: $|\text{aut}(G)|$

Lemma 5. #Aut $\leq_t$ GI.

Proof. Let $G = (V, E)$ be a graph with $|V| = n$. Consider a particular vertex $v \in V$. Let $C_v(G) := \{\pi(v) \mid \pi \in \text{aut}(G)\}$ be the set of vertices that v can map to via an automorphism, and let $S_v(G) := \{\pi \mid \pi \in \text{aut}(G) \text{ and } \pi(v) = v\}$ be the set of automorphisms fixing v. Basic group theory implies that $|aut(G)| = |C_v(G)|\,|S_v(G)|$. One way to understand this fact is by choosing a π_u for each $u \in C_v(G)$ such that $\pi_u \in \text{aut}(G)$ and $\pi_u(v) = u$. Every $\pi \in \text{aut}(G)$ can be uniquely decomposed into $\pi_u \circ \sigma$ where $\sigma \in S_v$. The claim follows.

Next we will compute $|C_v(G)|$ and $|S_v(G)|$ separately. We go through every vertex $u \in V$ using the GI oracle to determine whether an automorphism exists mapping v to u. To do so, let H be a "rigid" graph with $n+1$ vertices such that $\text{aut}(H)$ contains only the identity.[1] Construct G_v by taking a copy of G and a copy of H, and then gluing $v \in G$ to an arbitrary vertex $w \in H$. Similarly, construct G_u by gluing u to w. We ask the GI oracle whether $G_v \cong G_u$. Since vertices in H must map to vertices in H (H has one more vertex than G), such an isomorphism exists if and only if v is mapped to u. Namely $G_v \cong G_u$ if and only if $u \in C_v(G)$.

We still need to count $|S_v(G)|$. The idea is to use self-reducibility. Namely we want to transform it into a smaller instance of #Aut itself. In fact, we claim that $|S_v(G)| = |\text{aut}(G_v)|$. The reason is the same as above, namely that all vertices in the copy of H can only map to vertices in H, and H has only one automorphism. Although G_v contains $2n$ vertices, $n+1$ of them can only map to themselves. Hence, the number of "free" vertices in G_v is $n-1$. Let $v_1 := v$, and to continue, we pick an arbitrary free vertex. Call it v_2, and we proceed to compute $|C_{v_2}(G_{v_1})|$. Namely, we attach a rigid graph H' of size $2n+1$ to v_2 to get G_{v_1,v_2} and go through all vertices in $V \setminus \{v_1, v_2\}$ to determine their membership in $C_{v_2}(G_{v_1})$ using the GI oracle. Then we recursively compute $S_{v_2}(G_{v_1})$.

This recursion can only go down n steps. In fact, we construct a sequence of graphs G_{v_1}, G_{v_1,v_2}, $\cdots$, $G_{v_1,\ldots,v_{n-1}}$, each one fixing one more vertex and having polynomial size. It can be verified that

$$|\text{aut}(G)| = |C_{v_1}(G)| \cdot |C_{v_2}(G_{v_1})| \cdot \cdots \cdot \left|C_{v_n}(G_{v_1,\ldots,v_{n-1}})\right|.$$

This finishes the proof. □

Now we are ready to prove Theorem 4.

Proof of Theorem 4. We first use the GI oracle to test whether $G_1 \cong G_2$. If not, then we return 0. Otherwise, we compute the number of automorphisms of G_1 using Lemma 5. We claim that this is also the number of isomorphisms from G_1 to G_2.

[1] Such graphs do exist!

To be more specific, let $\mathrm{iso}(G_1, G_2) := \{\pi \mid \pi(G_1) = G_2\}$. Our claim is that $|\mathrm{iso}(G_1, G_2)| = |\mathrm{aut}(G_1)|$ if $G_1 \cong G_2$. Fix an arbitrary permutation $\pi_0 \in \mathrm{iso}(G_1, G_2)$. For any $\sigma \in \mathrm{iso}(G_1)$, it is easy to see that $\pi_0 \circ \sigma(G_1) = \pi(G_1) = G_2$. Thus, $\pi_0 \circ \sigma \in \mathrm{iso}(G_1, G_2)$. It implies that $\pi_0 \circ \mathrm{aut}(G_1) \subseteq \mathrm{iso}(G_1, G_2)$.

On the other hand, for each $\pi' \in \mathrm{iso}(G_1, G_2)$, we have that $\pi_0^{-1} \circ \pi'(G_1) = \pi_0^{-1}(G_2) = G_1$. Thus, $\pi_0^{-1} \circ \pi' \in \mathrm{aut}(G_1)$, namely $\pi' = \pi_0 \circ \sigma$ for some $\sigma \in \mathrm{aut}(G_1)$. It implies that $\mathrm{iso}(G_1, G_2) \subseteq \pi_0 \circ \mathrm{aut}(G_1)$.

To summarize, we have that

$$\mathrm{iso}(G_1, G_2) = \pi_0 \circ \mathrm{aut}(G_1).$$

Taking the cardinality on the both sides yields the claim. $\square$

Remark (Bibliographic). Theorem 2 was first shown by Boppana, Håstad, and Zachos [BHZ87]. Relevant chapters are [AB09, Chapter 8.2].

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.

[BHZ87] Ravi B. Boppana, Johan Håstad, and Stathis Zachos. Does co-NP have short interactive proofs? *Inf. Process. Lett.*, 25(2):127–132, 1987.