9. The Graph Isomorphism Problem

One of the few problem with an unclear complexity status.

Problem: Graph Isomorphism (GI)
Input: undirected graphs $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$
Question: Is there a bijective mapping $\varphi: V_1 \to V_2$ s.t. for all $u, v \in V_1$,

$$\{u, v\} \in E_1 \iff \{\varphi(u), \varphi(v)\} \in E_2$$

GNI denotes Graph Non-Isomorphism, i.e., $GNI = \overline{GI}$

We want to show that GI is not $\leq_m^p$-complete for NP under certain complexity-theoretical assumptions.

Define for graph $G = (V, E)$ the set of automorphisms of G:

$$Aut(G) =_{df} \{\varphi: V \to V \mid \varphi \text{ bijective}, \varphi(G) = G\},$$

where $\varphi(G) = (\varphi(V), \varphi(E))$.

Define for graphs G_1, G_2:

$$\mu(G_1, G_2) =_{df} \{(H, \varphi, i) \mid H \cong G_1 \vee H \cong G_2;\ \varphi \in Aut(G_i)\}$$

Lemma 1.

Let G_1, G_2 be undirected graphs.

(1.) $G_1 \cong G_2 \Rightarrow \mu(G_1, G_2) = 2n!$

(2.) $G_1 \ncong G_2 \Rightarrow \mu(G_1, G_2) \geq 4n!$

Proof: (1.) If $G_1 \cong G_2$ then $\|Aut(G_1)\| = \|Aut(G_2)\|$. So,

$$\mu(G_1, G_2) = \frac{n!}{\|Aut(G_1)\|} \cdot \left(\|Aut(G_1)\| + \|Aut(G_2)\|\right) = 2n!$$

(2.) If $G_1 \ncong G_2$ then all graphs H isomorphic to G_1 are not isom. to G_2 and vice versa. Thus,

$$\mu(G_1, G_2) = \left(\frac{n!}{\|Aut(G_1)\|} + \frac{n!}{\|Aut(G_2)\|}\right)\left(\|Aut(G_1)\| \cdot \|Aut(G_2)\|\right)$$

$$= n! \frac{\left(\|Aut(G_1)\| + \|Aut(G_2)\|\right)^2}{\|Aut(G_1)\| \cdot \|Aut(G_2)\|} \geq 4\, n!$$

Random hash functions:

$h : \{0,1\}^\ell \to \{0,1\}^m$ given by random matrix $A \in \{0,1\}^{\ell \times m}$ is defined for $x = x_1 \ldots x_\ell \in \{0,1\}^\ell$, $j \in \{1, \ldots, m\}$

$$h(x_1 \ldots x_\ell)_j = \bigoplus_{i=1}^{\ell} (a_{ij} \wedge x_i)$$

Lemma 2.

Let $X \subseteq \{0,1\}^t$.

(1.) If $\|X\| \leq 2^{m-1}$ then for randomly drawn hash functions $h_1, \ldots, h_{m+q-1} : \{0,1\}^\ell \to \{0,1\}^m$,

$$\text{prob}\left[h_i(x) = h_i(y) \text{ for } x \neq y \in X, 1 \leq i \leq m+q-1 \right] \leq \frac{1}{2^q}$$

(2.) If $\|X\| \geq (m+q-1)2^m$ then

$$\text{prob}\left[h_i(x) = h_i(y) \text{ for } x \neq y, 1 \leq i \leq m+q-1 \right] = 1.$$

Proof: (1) Note that for random hash function $h : \{0,1\}^\ell \to \{0,1\}^m$, and $x \neq y$: $\text{prob}[h(x)_j = h(y)_j] = \frac{1}{2}$ (by induction on ℓ).

Hence, $\text{prob}[h(x) = h(y)] = \frac{1}{2^m}$ for $x, y \in \{0,1\}^m$.

Hence, $\text{prob}[h(x) = h(y) \text{ for some } y \in X \setminus \{x\}] \leq \|X\| \cdot \frac{1}{2^m} \leq \frac{1}{2}$ for some $x \in X$

Hence, $\text{prob}[h_i(x) = h_i(y) \text{ for some } y \in X \setminus \{x\}, \text{all } i \in \{1, \ldots, m+q-1\}]$

$$\leq \frac{1}{2^{m+q-1}}$$

Hence, $\text{prob}[h_i(x) = h_i(y) \text{ for some } x \neq y \in X, \text{all } i \in \{1, \ldots, m+q-1\}]$

$$\leq \|X\| \cdot \frac{1}{2^{m+q-1}} \leq \frac{1}{2^q}$$

(2.) If $h : X \to \{0,1\}^m$ is injective then $\|X\| \leq 2^m$. If $\|X\| \geq (m+q-1)2^m > 2^m$ then a collision must occur (by pidgeonhole principle)

Random hash functions:

$h: \{0,1\}^\ell \to \{0,1\}^m$ given by random matrix $A \in \{0,1\}^{\ell \times m}$

defined for $x = x_1 \dots x_\ell \in \{0,1\}^\ell$, $j \in \{1, \dots, m\}$

$$h(x_1 \dots x_\ell)_j =_{def} \bigoplus_{i=1}^{m} (a_{ij} \wedge x_i)$$

Lemma 2.

Let $X \subseteq \{0,1\}^\ell$. Let $h_1, \dots, h_{m+q-1} : \{0,1\}^\ell \to \{0,1\}^m$ be randomly drawn hash functions (i.i.d.).

Consider the collision predicate $Col(X)$ on X:

$$Col(X) =_{def} (\exists x \in X)(\forall i \in \{1, \dots, m+q-1\})(\exists y \in X)\left[x \neq y \wedge h_i(x) = h_i(y)\right]$$

(1.) If $\|X\| \leq 2^{m-1}$ then $prob[Col(X)] \leq \frac{1}{2^q}$

(2.) If $\|X\| \geq (m+q-1)\,2^m$ then $prob[Col(X)] = 1$.

Proof: 1) Note that for random hash function $h: \{0,1\}^\ell \to \{0,1\}^m$ and $x \neq y \in \{0,1\}^\ell$: $prob[h(x)_j = h(y)_j] = \frac{1}{2}$ (by ind. on ℓ)

we obtain

$$prob[h_i(x) = h_i(y)] = \frac{1}{2^m} \quad \text{for } x \neq y \in \{0,1\}^m,\ i \in \{1, \dots, m+q-1\}$$

$$\Rightarrow prob[h_i(x) = h_i(y) \text{ for some } y \in X] \leq \|X\| \cdot \frac{1}{2^m} \leq \frac{1}{2}$$

for $x \in \{0,1\}^m$, $i \in \{1, \dots, m+q-1\}$

$$\Rightarrow prob[h_i(x) = h_i(y) \text{ for all } i, \text{ some } y \in X] \leq \frac{1}{2^{m+q-1}} \quad \text{for } x \in \{0,1\}^m$$

$$\Rightarrow prob[Col(X)] \leq \|X\| \cdot \frac{1}{2^{m+q-1}} \leq \frac{1}{2^q}$$

(2) If $h: X \to \{0,1\}^m$ is injective then $\|X\| \leq 2^m$. If $\|X\| \geq (m+q-1)\,2^m > 2^m$ then $Col(X)$ is always true (by pidgeonhole principle). ∎

Theorem 3. Let q be a polynomial.

There exist a set $B \in NP$, polynomials p s.t. for every pair (G_1, G_2) of graphs on n vertices, the following is true:

(i) $G_1 \cong G_2 \Rightarrow \underset{|y|=p(n)}{\text{prob}}\left[(G_1, G_2, y) \in B\right] \leq \frac{1}{2^{q(n)}}$

(ii) $G_1 \ncong G_2 \Rightarrow \underset{|y|=p(|x|)}{\text{prob}}\left[(G_1, G_2, y) \in B\right] = 1.$

Proof: Define B as follows:

$B =_{def} \{ (G_1, G_2, y) \mid y$ is an encoding of $p(n)+q(n)-1$ hash functions on the set $X^k =_{def} \{ (H, \varphi, i) \mid (H \cong G_1 \vee H \cong G_2) \wedge \varphi \in Aut(G_i) \}^k$ and $col(X^k)$ is true $\}$

Note that $B \in NP$ for all p, k, q. Choose p so that $p(n) \geq 1 + \lfloor n \cdot \log(2n!) \rfloor$, $k = n$. We obtain

(i) $G_1 \ncong G_2 \Rightarrow \|X^n\| = \|X\|^n = (2n!)^n \leq 2^{p(n)-1}$

$\Rightarrow \underset{|y|=p(n)}{\text{prob}}\left[(G_1, G_2, y) \in B\right] \leq \frac{1}{2^{q(n)}}$ (Lemma 2)

(ii) $G_1 \cong G_2 \Rightarrow \|X^n\| = \|X\|^n \geq (4n!)^n \geq (p(n)+q(n)-1)\, 2^{p(n)}$

$\Rightarrow \underset{|y|=p(n)}{\text{prob}}\left[(G_1, G_2, y) \in B\right] = 1.$

∎

Corollary 4.

$GI \in coNP/poly$.

Theorem 5.

$$coNP \subseteq NP/poly \Rightarrow \Sigma_2^P = \Pi_3^P.$$

Proof: Let $L \in \Pi_3^P$, i.e., there ex. $B \in coNP$, poly. p s.t.

$$x \in L \Leftrightarrow (\forall^p y)(\exists^p z)[(x,y,z) \in B]$$

Since $coNP \subseteq NP/poly$, there ex. $A \in NP$, $h \in poly$ s.t.

$$x \in L \Leftrightarrow (\forall^p y)(\exists^p z)[(x,y,z,h(|xyz|)) \in A]$$

Define $A' =_{def} \{(x,y,\alpha) \mid (\exists^p z)[(x,y,z,\alpha) \in A]\} \in NP$.

We have to guarantee that $\alpha = h(|x|+2p(|x|))$.

Consider the set

$$H =_{def} \{\alpha \in R_{h+2p(n)} \mid (\forall x, |\alpha| = h+2p(n))[x \in B \Leftrightarrow (x,\alpha) \in A]\}$$

Then, $H \in \forall(coNP \wedge NP \vee NP \wedge coNP) = \Pi_2^P$.

We obtain:

$$x \in L \Leftrightarrow (\forall^p y)[(x,y,h(|x|+2p(|x|))) \in A']$$

$$\Leftrightarrow (\exists \alpha, |\alpha| = h(|x|+2p(|x|)))[\underbrace{\alpha \in H}_{\Pi_2} \wedge \underbrace{(\forall^p y)[(x,y,\alpha) \in A']}_{\forall \cdot NP}]$$

Thus, $L \in \Sigma_3^P$. ∎

Corollary 6.

If GI is $\leq_m^P$-complete for NP then polynomial hierarchy is finite.