Não Isomorfismo de Grafos e a classe AM

Nicollas Sdroievski

24 de Junho de 2019

1 Introdução

O problema de não-isomorfismo de grafos é o problema de testar se dois grafos **não** são isomorfos, ou seja, de garantir que **não** existe isomorfismo entre os dois. Mais formalmente

$$\text{GNI} = \{(G_0, G_1) \mid \forall \pi \in S_n, \pi(G_0) \neq G_1\}.$$

Onde ambos G_0 e G_1 são grafos com n vértices e S_n representa o grupo das permutações em n elementos. Nesse caso, dizemos que $G_0 \ncong G_1$. Definimos o conjunto dos grafos isomorfos a G como $I_G = \{G' \mid G' \cong G\}$.

Um problema relacionado é o problema de automorfismo de grafos. A entrada é um único grafo G, e queremos saber se existe uma permutação não-identidade π tal que $\pi(G) = G$. Toda permutação, incluindo a identidade, que obedece à essa condição é chamada de *automorfismo* de G. O conjunto de todos os automorfismos de G é um subgrupo de S_n, que denotamos por $\text{Aut}(G)$.

Como consequência do Teorema Órbita-Estabilizador, mas que também pode ser provada para esse caso específico, temos a seguinte identidade, que será útil na nossa análise.

$$|I_G| = \frac{|S_n|}{|\text{Aut(G)}|} = \frac{n!}{|\text{Aut}(G)|}$$

2 GNI e AM

Queremos mostrar que existe um protocolo para GNI no qual V envia apenas uma mensagem, composta por bits aleatórios, e P responde. Após isso,

V pode apenas realizar uma computação determinística baseada nos bits aleatórios e na resposta de P para decidir se aceita ou não.

Para desenvolver esse protocolo, primeiro pensamos no problema de maneira diferente. Assuma que os grafos G_0 e G_1 são rígidos, ou seja, possuem apenas um automorfismo trivial. Defina o conjunto $S = \{H \mid H \cong G_0 \text{ ou } H \cong G_1\}$, nesse caso, usando a identidade da seção anterior:

$$\text{Se } G_0 \cong G_1 \text{ então } |S| = n! \tag{1}$$
$$\text{Se } G_0 \ncong G_1 \text{ então } |S| = 2n! \tag{2}$$

Como pode ser que ambos G_0 e G_1 possuam automorfismos não-triviais, modificamos um pouco a definição de S.

$$S = \{(H, \pi) \mid H \cong G_0 \text{ ou } H \cong G_1 \text{ e } \pi \in \mathrm{Aut}(H)\}.$$

Perceba que,

$$\text{Se } G_0 \cong G_1 \text{ então } |S| = |I_{G_0}||\mathrm{Aut}(G_0)| = n! \tag{3}$$
$$\text{Se } G_0 \ncong G_1 \text{ então } |S| = |I_{G_0}||\mathrm{Aut}(G_0)| + |I_{G_1}||\mathrm{Aut}(G_1)| = 2n! \tag{4}$$

Logo tudo que precisamos é de um protocolo no qual P tenta convencer V de que $|S| = 2n!$.V deve aceitar com alta probabilidade caso $|S| = 2n!$ e rejeitar com alta probabilidade caso $|S| = n!$.

3 O protocolo Goldwasser-Sipser

Veremos agora um protocolo que, de maneira genérica, permite a P provar que o tamanho de um determinado conjunto é pelo menos um valor K, sendo que se o tamanho desse conjunto for menor ou igual a $K/2$, V rejeita com alta probabilidade. Esse protocolo usa como ferramenta funções *hash* independentes dois-a-dois (*pairwise independent*).

Definição 1. *(Funções hash independentes dois-a-dois) Seja $\mathcal{H}_{n,k}$ uma coleção de funções de $\{0,1\}^n$ para $\{0,1\}^k$. Dizemos que $\mathcal{H}_{n,k}$ é independente dois-a-dois se para todo par $x \neq x' \in \{0,1\}^n$ e para todo $y, y' \in \{0,1\}^k$, temos*

$$\Pr_{h \in_R \mathcal{H}_{n,k}}[h(x) = y \wedge h(x') = y'] = \frac{1}{2^k}\frac{1}{2^k} = \frac{1}{2^{2k}}.$$

Teorema 1. *Existem coleções $\mathcal{H}_{n,k}$ de funções hash independentes dois-a-dois eficientes (computáveis em tempo polinomial em n e k).*

Veremos agora o protocolo e então o analisaremos.

Protocolo 1 *Goldwasser-Sipser Set Lower Bound Protocol*

Pré-requisitos: $S \subseteq \{0,1\}^m$ é um conjunto tal que é possível certificar que strings pertencem a S. Ambos P e V conhecem o valor K. O objetivo de P é convencer V de que $|S| \geq K$ e V deve rejeitar com alta probabilidade se $|S| \leq K/2$. Seja k um inteiro tal que $2^{k-2} \leq K \leq 2^{k-1}$.

1: V: Seleciona de maneira aleatória e uniforme uma função h de $\mathcal{H}_{m,k}$ e um elemento $y \in \{0,1\}^k$. Envia h e y para P.
2: P: Encontra $x \in S$ tal que $h(x) = y$. Envia x para V junto de um certificado de que $x \in S$.
3: V: Aceita se e somente se $h(x) = y$ e o certificado enviado por P garante que $x \in S$.

Perceba no protocolo V desafia P ao pedir que este encontre uma pré-imagem em S de um elemento aleatório $y \in \{0,1\}^k$. Como P é arbitrariamente poderoso, se existir esse valor de x, então P pode encontrá-lo. Dessa maneira, basta analisar os casos em que esse valor existe ou não. Além disso, certamente encontrar esse valor deve ser mais fácil quando S é grande, portanto esperamos que a probabilidade de que V aceite seja maior quando $|S| \geq K$ e menor quando $|S| \leq K/2$. Analisamos essa probabilidade através das duas afirmações a seguir. Para ambas, defina $p = K/2^k$.

Afirmação 1. *Caso $|S| \leq K/2$, então*

$$\Pr_{h \in_R \mathcal{H}_{n,k}, y \in_R \{0,1\}^k}[\exists x \in S \mid h(x) = y] \leq \frac{p}{2}.$$

Demonstração. No melhor caso, cada elemento de x mapeia para um elemento diferente de $\{0,1\}^k$, dessa maneira temos

$$\Pr_{h \in_R \mathcal{H}_{n,k}, y \in_R \{0,1\}^k}[\exists x \in S \mid h(x) = y] \leq \frac{|S|}{2^k} \leq \frac{K}{2^{k+1}} = \frac{p}{2}.$$

□

Afirmação 2. *Caso* $|S| \geq K$ *com* $|S| \leq 2^{k-1}$*, então*

$$\Pr_{h \in_R \mathcal{H}_{n,k}, y \in_R \{0,1\}^k}[\exists x \in S \mid h(x) = y] \geq \frac{3p}{4}.$$

Demonstração. Mostraremos algo um pouco mais forte: que para qualquer y, temos

$$\Pr_{h \in_R \mathcal{H}_{n,k}}[\exists x \in S \mid h(x) = y] \geq \frac{3p}{4}.$$

Para cada $x \in S$, defina E_x como o evento em que $h(x) = y$, Nesse caso, $\Pr[\exists x \in S \mid h(x) = y] = \Pr[\bigcup_{x \in S} E_x]$, pelo Princípio da Inclusão-Exclusão, temos que essa probabilidade é pelo menos:

$$\sum_{x \in S} \Pr[E_x] - \frac{1}{2} \sum_{x \neq x' \in S} [E_x \cap E_{x'}]$$

Como $\Pr[E_x] = 1/2^k$ e $\Pr[E_x \cap E_{x'}] = 1/2^{2k}$, temos:

$$\begin{aligned}
\Pr_{h \in_R \mathcal{H}_{n,k}}[\exists x \in S \mid h(x) = y] &\geq \frac{|S|}{2^k} - \frac{1}{2}\frac{|S|^2}{2^{2k}} \\
&= \left(1 - \frac{|S|}{2^{k+1}}\right)\frac{|S|}{2^k} \\
&\geq \left(1 - \frac{2^{k-1}}{2^{k+1}}\right)\frac{|S|}{2^k} \\
&\geq \frac{3}{4}p.
\end{aligned}$$

□

Esse salto de $p/2$ para $3p/4$ na probabilidade de aceitação de V é suficiente para que, ao repetir o protocolo uma quantidade constante de vezes, as probabilidades de aceitação sejam maior ou igual a $2/3$ no caso $|S| \geq K$ e menor ou igual a $1/3$ no caso $|S| \leq K/2$. Podemos executar o protocolo uma quantidade constante de vezes em paralelo, assim continuamos com apenas duas mensagens trocadas entre P e V.

4 Exercícios

Prove as seguintes afirmações.

1. Fixando G_0 e G_1, o problema de decidir se um par (H, π) pertence a S é verificável em tempo polinomial.

2. Dado n em unário, é possível calcular o valor $2n!$ em binário em tempo polinomial. **Dica:** use os fatos de que $n!$ é tempo-construtível e $\log(n!) = O(n \log n)$.

3. GNI $\in \mathsf{AM}$.