

Definiendo un testigo (probabilístico) para grafos no isomorfos

Dado un par de grafos (G_1, G_2) , queremos definir un conjunto $\text{num}(G_1, G_2)$ con las siguientes propiedades:

1. Cada elemento de $\text{num}(G_1, G_2)$ es de tamaño polinomial en el tamaño de (G_1, G_2)
2. Cada elemento de $\text{num}(G_1, G_2)$ tiene un testigo de tamaño polinomial de su pertenencia al conjunto
3. Para grafos con n nodos, la cantidad de elementos de $\text{num}(G_1, G_2)$ es necesariamente mayor si G_1 y G_2 no son isomorfos.

Definiendo un testigo (probabilístico) para grafos no isomorfos

Ejemplo

Podríamos intentar definir $\text{num}(G_1, G_2)$ de la siguiente forma:

$$\text{num}(G_1, G_2) = \{f \mid f \text{ es un isomorfismo de } G_1 \text{ a } G_2\}$$

Esta función satisface 1 y 2, pero no 3

Definiendo un testigo (probabilístico) para grafos no isomorfos

Vamos a considerar la siguiente definición del conjunto $\text{num}(G_1, G_2)$:

$$\text{num}(G_1, G_2) = \{(H, i, f) \mid H \text{ es un grafo isomorfo a } G_1 \text{ o } G_2, \\ i \in \{1, 2\} \text{ y } f \in \text{Aut}(G_i)\}$$

$\text{num}(G_1, G_2)$ satisface las condiciones 1 y 2

- ¿Cómo se demuestra que satisface la condición 2?

Vamos a demostrar que $\text{num}(G_1, G_2)$ además satisface la condición 3

El conjunto $\text{num}(G_1, G_2)$ nos ayuda a distinguir

Lema

Sean G_1 y G_2 dos grafos con n nodos cada uno. Si G_1 es isomorfo a G_2 , entonces se tiene que $|\text{num}(G_1, G_2)| = 2 \cdot n!$, si no se tiene que $|\text{num}(G_1, G_2)| \geq 4 \cdot n!$

¿Por qué en el lema sólo consideramos grafos con el mismo número de nodos?

- ¿Cómo manejamos el caso en el que los grafos tienen distinto número de nodos?

Demostración del lema

Primero suponemos que G_1 y G_2 son grafos isomorfos

- Recuerde que el número de grafos isomorfos a un grafo G con n nodos es $\frac{n!}{|\text{Aut}(G)|}$

Tenemos que:

$$\begin{aligned} |\text{num}(G_1, G_2)| &= |\{(H, i, f) \mid H \text{ es un grafo isomorfo a } G_1 \text{ o } G_2, \\ &\quad i \in \{1, 2\} \text{ y } f \in \text{Aut}(G_i)\}| \\ &= |\{H \mid H \text{ es un grafo isomorfo a } G_1 \text{ o } G_2\}| \cdot \\ &\quad (|\text{Aut}(G_1)| + |\text{Aut}(G_2)|) \\ &= |\{H \mid H \text{ es un grafo isomorfo a } G_1\}| \cdot 2|\text{Aut}(G_1)| \\ &= \frac{n!}{|\text{Aut}(G_1)|} \cdot 2|\text{Aut}(G_1)| \\ &= 2 \cdot n! \end{aligned}$$

Demostración del lema

Suponemos ahora que G_1 y G_2 no son grafos isomorfos

Tenemos que:

$$\begin{aligned} |\text{num}(G_1, G_2)| &= |\{(H, i, f) \mid H \text{ es un grafo isomorfo a } G_1 \text{ o } G_2, \\ &\quad i \in \{1, 2\} \text{ y } f \in \text{Aut}(G_i)\}| \\ &= (|\{H_1 \mid H_1 \text{ es un grafo isomorfo a } G_1\}| + \\ &\quad |\{H_2 \mid H_2 \text{ es un grafo isomorfo a } G_2\}|) \cdot \\ &\quad (|\text{Aut}(G_1)| + |\text{Aut}(G_2)|) \\ &= \left(\frac{n!}{|\text{Aut}(G_1)|} + \frac{n!}{|\text{Aut}(G_2)|} \right) \cdot (|\text{Aut}(G_1)| + |\text{Aut}(G_2)|) \\ &= n! \frac{(|\text{Aut}(G_1)| + |\text{Aut}(G_2)|)^2}{|\text{Aut}(G_1)| \cdot |\text{Aut}(G_2)|} \end{aligned}$$

Demostración del lema

Para terminar la demostración usamos la siguiente observación:

Observación

Para cada $a, b \in \mathbb{R}$ se tiene que $(a + b)^2 \geq 4ab$, puesto que:

$$\begin{aligned}(a - b)^2 \geq 0 &\Rightarrow a^2 - 2ab + b^2 \geq 0 \\&\Rightarrow a^2 + b^2 \geq 2ab \\&\Rightarrow a^2 + 2ab + b^2 \geq 4ab \\&\Rightarrow (a + b)^2 \geq 4ab\end{aligned}$$

Concluimos que $\frac{(|\text{Aut}(G_1)| + |\text{Aut}(G_2)|)^2}{|\text{Aut}(G_1)| \cdot |\text{Aut}(G_2)|} \geq 4$, de lo que obtenemos que $|\text{num}(G_1, G_2)| \geq 4 \cdot n!$



Otro ingrediente necesario: Funciones de hash aleatorias

Sea $A = (a_{i,j})$ una matriz Booleana de $n \times m$ tal que cada uno de sus elementos es escogido de manera independiente y con distribución uniforme.

La matriz A define una función de hash aleatoria $h : \{0, 1\}^m \rightarrow \{0, 1\}^n$

Para cada $u \in \{0, 1\}^m$ se tiene que $h(u) = v$ con $v \in \{0, 1\}^n$, donde para $j \in \{1, \dots, n\}$:

$$\pi_j(v) = (a_{j,1} \wedge \pi_1(u)) \oplus (a_{j,2} \wedge \pi_2(u)) \oplus \dots \oplus (a_{j,m} \wedge \pi_m(u))$$

suponiendo que $\pi_k(w)$ es el k -ésimo símbolo en un string w

Una propiedad fundamental de las funciones de hash aleatorias¹

En las siguientes transparencias consideramos las funciones de hash aleatorias $h : \{0, 1\}^m \rightarrow \{0, 1\}^n$ dadas por matrices $A = (a_{i,j})$

Lema

Sean $u, v \in \{0, 1\}^m$ tales que $u \neq v$. Para cada $j \in \{1, \dots, n\}$ se tiene que:

$$Pr_h(\pi_j(h(u)) = \pi_j(h(v))) = \frac{1}{2}$$

¹ Esta sección fue preparada con la ayuda de Pedro Bahamondes

Demostración del lema

Sean $u, v \in \{0, 1\}^m$ tales que $u \neq v$, y sea $j \in \{1, \dots, n\}$

Sabemos que:

$$\begin{aligned}\pi_j(h(u)) &= (a_{j,1} \wedge \pi_1(u)) \oplus (a_{j,2} \wedge \pi_2(u)) \oplus \dots \oplus (a_{j,m} \wedge \pi_m(u)) \\ \pi_j(h(v)) &= (a_{j,1} \wedge \pi_1(v)) \oplus (a_{j,2} \wedge \pi_2(v)) \oplus \dots \oplus (a_{j,m} \wedge \pi_m(v))\end{aligned}$$

Además, dado que $u \neq v$ sabemos que existe $k \in \{1, \dots, m\}$ tal que $\pi_k(u) \neq \pi_k(v)$

Demostración del lema

Tenemos cuatro casos posible para los términos $(a_{j,k} \wedge \pi_k(u))$ y $(a_{j,k} \wedge \pi_k(v))$:

- ▶ Si $a_{j,k} = 1$, $\pi_k(u) = 0$ y $\pi_k(v) = 1$, tenemos que $(a_{j,k} \wedge \pi_k(u)) = 0$ y $(a_{j,k} \wedge \pi_k(v)) = 1$
- ▶ Si $a_{j,k} = 1$, $\pi_k(u) = 1$ y $\pi_k(v) = 0$, tenemos que $(a_{j,k} \wedge \pi_k(u)) = 1$ y $(a_{j,k} \wedge \pi_k(v)) = 0$
- ▶ Si $a_{j,k} = 0$, entonces $(a_{j,k} \wedge \pi_k(u)) = (a_{j,k} \wedge \pi_k(v)) = 0$ en las dos combinaciones de valores posibles para $(\pi_k(u), \pi_k(v))$

Por lo tanto:

$$\Pr_h((a_{j,k} \wedge \pi_k(u)) = (a_{j,k} \wedge \pi_k(v))) = \frac{1}{2}$$

dado que $a_{i,j}$ es escogido con distribución uniforme desde el conjunto $\{0, 1\}$

Demostración del lema

Defina los siguientes strings:

$$\begin{aligned}\pi_{j,-k}(h(u)) &= (a_{j,1} \wedge \pi_1(u)) \oplus \cdots \oplus (a_{j,k-1} \wedge \pi_{k-1}(u)) \oplus \\ &\quad (a_{j,k+1} \wedge \pi_{k+1}(u)) \oplus \cdots \oplus (a_{j,m} \wedge \pi_m(u)) \\ \pi_{j,-k}(h(v)) &= (a_{j,1} \wedge \pi_1(v)) \oplus \cdots \oplus (a_{j,k-1} \wedge \pi_{k-1}(v)) \oplus \\ &\quad (a_{j,k+1} \wedge \pi_{k+1}(v)) \oplus \cdots \oplus (a_{j,m} \wedge \pi_m(v))\end{aligned}$$

Podemos reescribir las definiciones de $\pi_j(h(u))$ y $\pi_j(h(v))$ de la siguiente forma:

$$\begin{aligned}\pi_j(h(u)) &= \pi_{j,-k}(h(u)) \oplus (a_{j,k} \wedge \pi_k(u)) \\ \pi_j(h(v)) &= \pi_{j,-k}(h(v)) \oplus (a_{j,k} \wedge \pi_k(v))\end{aligned}$$

Demostración del lema

Utilizando la notación anterior tenemos que:

$$\begin{aligned}\Pr_h(\pi_j(h(u)) = \pi_j(h(v))) &= \\ \Pr_h(\pi_j(h(u)) = \pi_j(h(v)) \mid \pi_{j,-k}(h(u)) = \pi_{j,-k}(h(v))) &\cdot \\ \Pr_h(\pi_{j,-k}(h(u)) = \pi_{j,-k}(h(v))) &+ \\ \Pr_h(\pi_j(h(u)) = \pi_j(h(v)) \mid \pi_{j,-k}(h(u)) \neq \pi_{j,-k}(h(v))) &\cdot \\ \Pr_h(\pi_{j,-k}(h(u)) \neq \pi_{j,-k}(h(v))) &\end{aligned}$$

Dado que $\Pr_h((a_{j,k} \wedge \pi_k(u)) = (a_{j,k} \wedge \pi_k(v))) = \frac{1}{2}$, concluimos que:

$$\begin{aligned}\Pr_h(\pi_j(h(u)) = \pi_j(h(v)) \mid \pi_{j,-k}(h(u)) = \pi_{j,-k}(h(v))) &= \frac{1}{2} \\ \Pr_h(\pi_j(h(u)) = \pi_j(h(v)) \mid \pi_{j,-k}(h(u)) \neq \pi_{j,-k}(h(v))) &= \frac{1}{2}\end{aligned}$$

Demostración del lema

Tenemos entonces que:

$$\begin{aligned}\Pr_h(\pi_j(h(u)) = \pi_j(h(v))) \\&= \frac{1}{2} \cdot \Pr_h(\pi_{j,-k}(h(u)) = \pi_{j,-k}(h(v))) + \frac{1}{2} \cdot \Pr_h(\pi_{j,-k}(h(u)) \neq \pi_{j,-k}(h(v))) \\&= \frac{1}{2} \cdot [\Pr_h(\pi_{j,-k}(h(u)) = \pi_{j,-k}(h(v))) + \Pr_h(\pi_{j,-k}(h(u)) \neq \pi_{j,-k}(h(v)))] \\&= \frac{1}{2} \cdot 1 \\&= \frac{1}{2}\end{aligned}$$

