Tenemos los ingredientes necesarios para la demostración

Teorema

$\overline{\textit{GRAPH-ISO}} \in \textit{AM}$

Tenemos los ingredientes necesarios para la demostración

Teorema

$\overline{\textit{GRAPH-ISO}} \in \textit{AM}$

Corolario

$\textit{GRAPH-ISO} \in \textit{co-AM}$

Tenemos los ingredientes necesarios . . .

El teorema anterior se demuestra estableciendo el siguiente resultado:

Teorema (Schöning)

Existe una MT probabilística no determinista M tal que $t_M(n)$ es $O(n^k)$ y para cada par (G_1, G_2) de grafos:

- *Si G_1 no es isomorfo a G_2, entonces* $\mathbf{Pr}_s(M(G_1, G_2, s)\ \textit{acepte}) = 1$
- *Si G_1 es isomorfo a G_2, entonces* $\mathbf{Pr}_s(M(G_1, G_2, s)\ \textit{acepte}) \leq \frac{1}{4}$

Demostración del teorema: notación inicial

Antes de definir la MT probabilística no determinista M, vamos a discutir algunas nociones y herramientas útiles para la demostración.

Suponga que G_1 y G_2 son dos grafos con $m > 0$ nodos cada uno.

- Recuerde que $\text{num}(G_1, G_2)$ fue definido como:

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

Para utilizar las herramientas desarrolladas primero tenemos que representar cada $(H, i, f) \in \text{num}(G_1, G_2)$ como un string en $\{0, 1\}^\ell$

- ¿Cuál es el valor de ℓ?

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \mathsf{num}(G_1, G_2)$?

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \text{num}(G_1, G_2)$?

- Podemos representar H usando su matriz de adyacencia, para lo cual necesitamos m^2 bits

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \text{num}(G_1, G_2)$?

- Podemos representar H usando su matriz de adyacencia, para lo cual necesitamos m^2 bits
- Para almacenar el valor de i necesitamos un bit

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \text{num}(G_1, G_2)$?

- Podemos representar H usando su matriz de adyacencia, para lo cual necesitamos m^2 bits
- Para almacenar el valor de i necesitamos un bit
- Podemos almacenar la biyección f como una lista de m números $a_1 \ldots a_m$ tal que $f(i) = a_i$

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \text{num}(G_1, G_2)$?

- Podemos representar H usando su matriz de adyacencia, para lo cual necesitamos m^2 bits
- Para almacenar el valor de i necesitamos un bit
- Podemos almacenar la biyección f como una lista de m números $a_1 \ldots a_m$ tal que $f(i) = a_i$
  - Dado que cada $a_i \leq m$, basta con utilizar $1 + \lfloor \log_2(m) \rfloor$ bits para almacenar a_i

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \text{num}(G_1, G_2)$?

- Podemos representar H usando su matriz de adyacencia, para lo cual necesitamos m^2 bits
- Para almacenar el valor de i necesitamos un bit
- Podemos almacenar la biyección f como una lista de m números $a_1 \ldots a_m$ tal que $f(i) = a_i$
  - Dado que cada $a_i \leq m$, basta con utilizar $1 + \lfloor \log_2(m) \rfloor$ bits para almacenar a_i
  - Por lo tanto necesitamos $m(1 + \lfloor \log_2(m) \rfloor)$ bits para almacenar la lista $a_1 \ldots a_m$

Demostración del teorema: notación inicial

¿Cuántos bits necesitamos para representar una tupla $(H, i, f) \in \text{num}(G_1, G_2)$?

- Podemos representar H usando su matriz de adyacencia, para lo cual necesitamos m^2 bits
- Para almacenar el valor de i necesitamos un bit
- Podemos almacenar la biyección f como una lista de m números $a_1 \dots a_m$ tal que $f(i) = a_i$
  - Dado que cada $a_i \leq m$, basta con utilizar $1 + \lfloor \log_2(m) \rfloor$ bits para almacenar a_i
  - Por lo tanto necesitamos $m(1 + \lfloor \log_2(m) \rfloor)$ bits para almacenar la lista $a_1 \dots a_m$

Suponemos entonces que $\ell = m^2 + 1 + m(1 + \lfloor \log_2(m) \rfloor)$

Demostración del teorema: notación inicial

Desde ahora en adelante consideramos a cada elemento de $\mathsf{num}(G_1, G_2)$ como un string de ℓ bits

- Tenemos que $\mathsf{num}(G_1, G_2) \subseteq \{0,1\}^{\ell}$

Demostración del teorema: notación inicial

Desde ahora en adelante consideramos a cada elemento de $\text{num}(G_1, G_2)$ como un string de ℓ bits

- Tenemos que $\text{num}(G_1, G_2) \subseteq \{0,1\}^{\ell}$

Defina $X(G_1, G_2)$ como $\text{num}(G_1, G_2)^m$

- Cada elemento de $\text{num}(G_1, G_2)^m$ es de la forma $w_1 w_2 \cdots w_m$, donde para cada $i \in \{1, \ldots, m\}$ se tiene que w_i es un string en $\text{num}(G_1, G_2)$

Demostración del teorema: notación inicial

Desde ahora en adelante consideramos a cada elemento de $\text{num}(G_1, G_2)$ como un string de ℓ bits

- Tenemos que $\text{num}(G_1, G_2) \subseteq \{0,1\}^{\ell}$

Defina $X(G_1, G_2)$ como $\text{num}(G_1, G_2)^m$

- Cada elemento de $\text{num}(G_1, G_2)^m$ es de la forma $w_1 w_2 \cdots w_m$, donde para cada $i \in \{1, \ldots, m\}$ se tiene que w_i es un string en $\text{num}(G_1, G_2)$

Tenemos que:

Demostración del teorema: notación inicial

Desde ahora en adelante consideramos a cada elemento de $\text{num}(G_1, G_2)$ como un string de ℓ bits

- Tenemos que $\text{num}(G_1, G_2) \subseteq \{0,1\}^{\ell}$

Defina $X(G_1, G_2)$ como $\text{num}(G_1, G_2)^m$

- Cada elemento de $\text{num}(G_1, G_2)^m$ es de la forma $w_1 w_2 \cdots w_m$, donde para cada $i \in \{1, \ldots, m\}$ se tiene que w_i es un string en $\text{num}(G_1, G_2)$

Tenemos que:

- $X(G_1, G_2) \subseteq \{0,1\}^{\ell \cdot m}$

Demostración del teorema: notación inicial

Desde ahora en adelante consideramos a cada elemento de $\text{num}(G_1, G_2)$ como un string de ℓ bits

- Tenemos que $\text{num}(G_1, G_2) \subseteq \{0,1\}^{\ell}$

Defina $X(G_1, G_2)$ como $\text{num}(G_1, G_2)^m$

- Cada elemento de $\text{num}(G_1, G_2)^m$ es de la forma $w_1 w_2 \cdots w_m$, donde para cada $i \in \{1, \ldots, m\}$ se tiene que w_i es un string en $\text{num}(G_1, G_2)$

Tenemos que:

- $X(G_1, G_2) \subseteq \{0,1\}^{\ell \cdot m}$
- Si G_1 no es isomorfo a G_2, entonces $|X(G_1, G_2)| \geq (4 \cdot m!)^m$

Demostración del teorema: notación inicial

Desde ahora en adelante consideramos a cada elemento de $\text{num}(G_1, G_2)$ como un string de ℓ bits

- Tenemos que $\text{num}(G_1, G_2) \subseteq \{0,1\}^{\ell}$

Defina $X(G_1, G_2)$ como $\text{num}(G_1, G_2)^m$

- Cada elemento de $\text{num}(G_1, G_2)^m$ es de la forma $w_1 w_2 \cdots w_m$, donde para cada $i \in \{1, \ldots, m\}$ se tiene que w_i es un string en $\text{num}(G_1, G_2)$

Tenemos que:

- $X(G_1, G_2) \subseteq \{0,1\}^{\ell \cdot m}$
- Si G_1 no es isomorfo a G_2, entonces $|X(G_1, G_2)| \geq (4 \cdot m!)^m$
- Si G_1 es isomorfo a G_2, entonces $|X(G_1, G_2)| = (2 \cdot m!)^m$

Demostración del teorema: notación inicial

Finalmente defina $n = 1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil$

Demostración del teorema: notación inicial

Finalmente defina $n = 1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil$

Tenemos que:

$$\begin{aligned} 1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil &= 1 + \lceil m \cdot (1 + \log_2(m!)) \rceil \\ &\leq 1 + \lceil m \cdot (1 + \log_2(m^m)) \rceil \\ &= 1 + \lceil m \cdot (1 + m \log_2(m)) \rceil \\ &\leq 1 + \lceil m \cdot (1 + m^2) \rceil \\ &= 1 + m + m^3 \end{aligned}$$

Demostración del teorema: notación inicial

Finalmente defina $n = 1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil$

Tenemos que:

$$\begin{aligned} 1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil &= 1 + \lceil m \cdot (1 + \log_2(m!)) \rceil \\ &\leq 1 + \lceil m \cdot (1 + \log_2(m^m)) \rceil \\ &= 1 + \lceil m \cdot (1 + m \log_2(m)) \rceil \\ &\leq 1 + \lceil m \cdot (1 + m^2) \rceil \\ &= 1 + m + m^3 \end{aligned}$$

Concluimos que $n + 1 = 2 + \lceil m \cdot \log_2(2 \cdot m!) \rceil < 2^{m-2}$ para todo $m \geq 14$

- Vamos a utilizar esta propiedad en la siguiente lámina

Demostración del teorema: notación inicial

Suponga que G_1 no es isomorfo a G_2 y que $m \geq 14$

- Tenemos que $2^{m-2} > (n+1)$

Demostración del teorema: notación inicial

Suponga que G_1 no es isomorfo a G_2 y que $m \geq 14$

- Tenemos que $2^{m-2} > (n+1)$

Concluimos que $|X(G_1, G_2)| > (n+1)2^n$, puesto que:

$$\begin{aligned}
|X(G_1, G_2)| &\geq (4 \cdot m!)^m \\
&= 2^{\log_2((4\cdot m!)^m)} \\
&= 2^{m \cdot \log_2(4\cdot m!)} \\
&= 2^{m + m\cdot\log_2(2\cdot m!)} \\
&= 2^{m-1+(1+m\cdot\log_2(2\cdot m!))} \\
&\geq 2^{m-1+\lceil m\cdot\log_2(2\cdot m!)\rceil} \\
&= 2^{m-2+n} \\
&= 2^{m-2} \cdot 2^n \\
&> (n+1)2^n
\end{aligned}$$

Demostración del teorema: notación inicial

Si G_1 es isomorfo a G_2 tenemos que $|X(G_1, G_2)| \leq 2^{n-1}$, puesto que:

$$\begin{aligned}
|X(G_1, G_2)| &= (2 \cdot m!)^m \\
&= 2^{\log_2((2 \cdot m!)^m)} \\
&= 2^{m \cdot \log_2(2 \cdot m!)} \\
&\leq 2^{\lceil m \cdot \log_2(2 \cdot m!) \rceil} \\
&= 2^{1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil - 1} \\
&= 2^{n-1}
\end{aligned}$$

Demostración del teorema: notación inicial

En la demostración vamos a considerar funciones de hash aleatorias $h \in \mathcal{H}(\ell \cdot m, n)$

Estas funciones están dadas por matrices Booleanas A de $n \times (\ell \cdot m)$

- Los elementos son de A son escogidos con distribución uniforme y de manera independiente

Necesitamos $(\ell \cdot m \cdot n)$ bits para representar A

Demostración del teorema: notación inicial

Necesitamos entonces $(\ell \cdot m \cdot n)$ bits para representar una función de hash aleatoria $h : \{0,1\}^{\ell \cdot m} \to \{0,1\}^n$

Demostración del teorema: notación inicial

Necesitamos entonces $(\ell \cdot m \cdot n)$ bits para representar una función de hash aleatoria $h : \{0,1\}^{\ell \cdot m} \to \{0,1\}^n$

Vale decir, necesitamos la siguiente cantidad de bits para representar h:

$$[m^2 + 1 + m(1 + \lfloor \log_2(m) \rfloor)] \cdot m \cdot [1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil]$$

Demostración del teorema: notación inicial

Necesitamos entonces $(\ell \cdot m \cdot n)$ bits para representar una función de hash aleatoria $h : \{0,1\}^{\ell \cdot m} \to \{0,1\}^n$

Vale decir, necesitamos la siguiente cantidad de bits para representar h:

$$[m^2 + 1 + m(1 + \lfloor \log_2(m) \rfloor)] \cdot m \cdot [1 + \lceil m \cdot \log_2(2 \cdot m!) \rceil]$$

El valor $(\ell \cdot m \cdot n)$ es polinomial en m, de lo cual concluimos que es polinomial en el tamaño de (G_1, G_2)

Demostración del teorema: la definición de M

Recuerde que la MT probabilística no determinista M está tratando de verificar si dos grafos G_1 y G_2 **no** son isomorfos.

M recibe como entrada una tupla de la forma $(G_1, G_2, h_1, \ldots, h_{n+1})$

- Cada h_i es una función de hash aleatoria de $\{0,1\}^{\ell \cdot m}$ en $\{0,1\}^n$
  - m es el número de nodos de G_1, ℓ y n son definidos como fue mostrado en las transparencias anteriores
- La tupla $(h_1, \ldots, h_{n+1})$ corresponde al string de bits aleatorios que recibe M

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2
3. Si $m < 14$ entonces vaya al paso 3.1, si no vaya al paso 4

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2
3. Si $m < 14$ entonces vaya al paso 3.1, si no vaya al paso 4
   - 3.1 Construya todas las posibles biyecciones $f : \{1, \ldots, m\} \to \{1, \ldots, m\}$

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2
3. Si $m < 14$ entonces vaya al paso 3.1, si no vaya al paso 4
   - 3.1 Construya todas las posibles biyecciones $f : \{1, \ldots, m\} \to \{1, \ldots, m\}$
   - 3.2 Si alguna de estas biyecciones f es un isomorfismo de G_1 en G_2 entonces retorne **no**. En caso contrario retorne **sí**

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2
3. Si $m < 14$ entonces vaya al paso 3.1, si no vaya al paso 4
   - 3.1 Construya todas las posibles biyecciones $f : \{1, \ldots, m\} \to \{1, \ldots, m\}$
   - 3.2 Si alguna de estas biyecciones f es un isomorfismo de G_1 en G_2 entonces retorne **no**. En caso contrario retorne **sí**
4. Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2, y $f_j \in \mathrm{Aut}(G_{i_j})$

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2
3. Si $m < 14$ entonces vaya al paso 3.1, si no vaya al paso 4
   - 3.1 Construya todas las posibles biyecciones $f : \{1, \ldots, m\} \to \{1, \ldots, m\}$
   - 3.2 Si alguna de estas biyecciones f es un isomorfismo de G_1 en G_2 entonces retorne **no**. En caso contrario retorne **sí**
4. Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2, y $f_j \in \mathrm{Aut}(G_{i_j})$
5. Sea $x = (H_1, i_1, f_1, \ldots, H_m, i_m, f_m)$

Demostración del teorema: la definición de M

Con entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ la MT M realiza los siguientes pasos:

1. Si G_1 y G_2 no tienen el mismo número de nodos entonces retorne **sí**, si no vaya al paso 2
2. Sea m el número de nodos de G_1 y G_2
3. Si $m < 14$ entonces vaya al paso 3.1, si no vaya al paso 4
   - 3.1 Construya todas las posibles biyecciones $f : \{1, \ldots, m\} \to \{1, \ldots, m\}$
   - 3.2 Si alguna de estas biyecciones f es un isomorfismo de G_1 en G_2 entonces retorne **no**. En caso contrario retorne **sí**
4. Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2, y $f_j \in \mathrm{Aut}(G_{i_j})$
5. Sea $x = (H_1, i_1, f_1, \ldots, H_m, i_m, f_m)$ $\boxed{x \in X(G_1, G_2)}$

Demostración del teorema: la definición de M

6. Para $k = 1$ hasta $n + 1$ haga lo siguiente:

Demostración del teorema: la definición de M

6. Para $k = 1$ hasta $n + 1$ haga lo siguiente:

   6.1 Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2 y $f_j \in \mathrm{Aut}(G_{i_j})$

Demostración del teorema: la definición de M

6. Para $k = 1$ hasta $n + 1$ haga lo siguiente:

   6.1 Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2 y $f_j \in \mathrm{Aut}(G_{i_j})$

   6.2 Sea $y = (H_1, i_1, f_1, \ldots, H_m, i_m, f_m)$

Demostración del teorema: la definición de M

6. Para $k = 1$ hasta $n + 1$ haga lo siguiente:

   6.1 Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2 y $f_j \in \mathrm{Aut}(G_{i_j})$

   6.2 Sea $y = (H_1, i_1, f_1, \ldots, H_m, i_m, f_m)$ $\boxed{y \in X(G_1, G_2)}$

Demostración del teorema: la definición de M

6. Para $k = 1$ hasta $n + 1$ haga lo siguiente:

   6.1 Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2 y $f_j \in \mathrm{Aut}(G_{i_j})$

   6.2 Sea $y = (H_1, i_1, f_1, \ldots, H_m, i_m, f_m)$ $\boxed{y \in X(G_1, G_2)}$

   6.3 Si $x = y$ o $h_k(x) \neq h_k(y)$, entonces retorne **no**

Demostración del teorema: la definición de M

6. Para $k = 1$ hasta $n + 1$ haga lo siguiente:

   6.1 Adivine $(H_1, g_1, i_1, f_1, \ldots, H_m, g_m, i_m, f_m)$ tal que para cada $j \in \{1, \ldots, m\}$: g_j es un isomorfismo de H_j en G_1 o G_2 y $f_j \in \mathrm{Aut}(G_{i_j})$

   6.2 Sea $y = (H_1, i_1, f_1, \ldots, H_m, i_m, f_m)$ $\boxed{y \in X(G_1, G_2)}$

   6.3 Si $x = y$ o $h_k(x) \neq h_k(y)$, entonces retorne **no**

7. Retorne **sí**

Demostración del teorema: la probabilidad de error de M

La MT no determinista M funciona en tiempo polinomial.

Además, M acepta una entrada $(G_1, G_2, h_1, \ldots, h_{n+1})$ si y sólo si alguna de las siguientes condiciones se cumple:

- G_1 y G_2 no tienen el mismo número de nodos
- G_1 y G_2 tienen $m < 14$ nodos cada uno y no son isomorfos
- G_1 y G_2 tienen $m \geq 14$ nodos cada uno y

$$\exists x \in X(G_1, G_2)\, \forall k \in \{1, \ldots, n+1\} \\ \exists y \in X(G_1, G_2) : (x \neq y \wedge h_k(x) = h_k(y))$$

Demostración del teorema: la probabilidad de error de M

Usamos las condiciones de aceptación de M para establecer la probabilidad de error de esta máquina de Turing

Vale decir, dados dos grafos G_1 y G_2 queremos calcular la probabilidad:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(M(G_1, G_2, h_1, \ldots, h_{n+1}) \text{ acepte})$$

dependiendo de si G_1 y G_2 son o no son isomorfos.

Demostración del teorema: la probabilidad de error de M

Suponemos primero que G_1 y G_2 **no** son isomorfos.

Demostración del teorema: la probabilidad de error de M

Suponemos primero que G_1 y G_2 **no** son isomorfos.

Si G_1 y G_2 no tienen el mismo número de nodos, o si tienen el mismo número de nodos $m < 14$, entonces:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(M(G_1, G_2, h_1, \ldots, h_{n+1}) \text{ acepte}) \quad = \quad 1$$

De hecho en estos casos las funciones $h_1, \ldots, h_{n+1}$ no son tomadas en cuenta.

Demostración del teorema: la probabilidad de error de M

Si G_1 y G_2 tienen el mismo número de nodos $m \geq 14$, entonces tenemos que $|X(G_1, G_2)| > (n+1)2^n$

Demostración del teorema: la probabilidad de error de M

Si G_1 y G_2 tienen el mismo número de nodos $m \geq 14$, entonces tenemos que $|X(G_1, G_2)| > (n+1)2^n$

Concluimos por el último lema demostrado que para cualquier secuencia h_1, ..., h_{n+1} de funciones de hash aleatorias en $\mathcal{H}(\ell \cdot m, n)$:

$$\exists x \in X(G_1, G_2) \forall k \in \{1, \ldots, n+1\} \\ \exists y \in X(G_1, G_2) : (x \neq y \wedge h_k(x) = h_k(y))$$

Demostración del teorema: la probabilidad de error de M

Si G_1 y G_2 tienen el mismo número de nodos $m \geq 14$, entonces tenemos que $|X(G_1, G_2)| > (n+1)2^n$

Concluimos por el último lema demostrado que para cualquier secuencia h_1, $\ldots$, h_{n+1} de funciones de hash aleatorias en $\mathcal{H}(\ell \cdot m, n)$:

$$\exists x \in X(G_1, G_2) \forall k \in \{1, \ldots, n+1\} \\ \exists y \in X(G_1, G_2) : (x \neq y \wedge h_k(x) = h_k(y))$$

Por lo tanto en este caso también tenemos que:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(M(G_1, G_2, h_1, \ldots, h_{n+1}) \text{ acepte}) \quad = \quad 1$$

Demostración del teorema: la probabilidad de error de M

Finalmente, consideramos el caso en que G_1 y G_2 son grafos isomorfos.

- Suponemos que G_1 y G_2 tienen el mismo número de nodos m

Demostración del teorema: la probabilidad de error de M

Finalmente, consideramos el caso en que G_1 y G_2 son grafos isomorfos.

- Suponemos que G_1 y G_2 tienen el mismo número de nodos m

Si $m < 14$ entonces la MT M no se puede equivocar al decidir si G_1 es isomorfo a G_2, y tenemos que:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(M(G_1, G_2, h_1, \ldots, h_{n+1}) \text{ acepte}) \quad = \quad 0$$

Demostración del teorema: la probabilidad de error de M

Finalmente, consideramos el caso en que G_1 y G_2 son grafos isomorfos.

- Suponemos que G_1 y G_2 tienen el mismo número de nodos m

Si $m < 14$ entonces la MT M no se puede equivocar al decidir si G_1 es isomorfo a G_2, y tenemos que:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(M(G_1, G_2, h_1, \ldots, h_{n+1}) \text{ acepte}) \quad = \quad 0$$

Suponemos entonces que $m \geq 14$

Demostración del teorema: la probabilidad de error de M

Tenemos que $|X(G_1, G_2)| \leq 2^{n-1}$

Demostración del teorema: la probabilidad de error de M

Tenemos que $|X(G_1, G_2)| \leq 2^{n-1}$

Concluimos por el último lema demostrado:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(\exists x \in X(G_1, G_2)\, \forall k \in \{1, \ldots, n+1\} \\ \exists y \in X(G_1, G_2) : (x \neq y \wedge h_k(x) = h_k(y))) \leq \frac{1}{4}$$

Demostración del teorema: la probabilidad de error de M

Tenemos que $|X(G_1, G_2)| \leq 2^{n-1}$

Concluimos por el último lema demostrado:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(\exists x \in X(G_1, G_2)\, \forall k \in \{1, \ldots, n+1\} \\ \exists y \in X(G_1, G_2) : (x \neq y \wedge h_k(x) = h_k(y))) \leq \frac{1}{4}$$

Por lo tanto:

$$\mathbf{Pr}_{h_1,\ldots,h_{n+1}}(M(G_1, G_2, h_1, \ldots, h_{n+1}) \text{ acepte}) \leq \frac{1}{4}$$

□