

La jerarquía polinomial relativizada

Vamos a definir una jerarquía que intenta formalizar las ideas mostradas en las transparencias anteriores.

La jerarquía polinomial relativizada

Vamos a definir una jerarquía que intenta formalizar las ideas mostradas en las transparencias anteriores.

Para definir esta jerarquía primero tenemos que definir la relativización de la jerarquía polinomial a un lenguaje L .

La jerarquía polinomial relativizada

Notación

Dado un lenguaje L :

$$\begin{aligned}\Sigma_0^P(L) &= PTIME^L \\ \Sigma_{n+1}^P(L) &= NP^{\Sigma_n^P(L)}\end{aligned}$$

La jerarquía polinomial relativizada

Notación

Dado un lenguaje L :

$$\begin{aligned}\Sigma_0^P(L) &= PTIME^L \\ \Sigma_{n+1}^P(L) &= NP^{\Sigma_n^P(L)}\end{aligned}$$

Ejemplo

Tenemos que $\Sigma_1^P(L) = NP^L$ y $\Sigma_2^P(L) = NP^{(NP^L)}$

► ¿Por qué?

La jerarquía baja para NP

Definición (Low hierarchy)

Para cada $n \geq 0$:

$$L_n^P = \{L \in NP \mid \Sigma_n^P(L) = \Sigma_n^P\}$$

La jerarquía baja para NP

Definición (Low hierarchy)

Para cada $n \geq 0$:

$$L_n^P = \{L \in NP \mid \Sigma_n^P(L) = \Sigma_n^P\}$$

Nótese que en la definición anterior se incluye la condición $L \in NP$ para asegurar que la jerarquía esta dentro de NP

Algunas propiedades básicas de la jerarquía baja

Proposición

1. Para todo $n \geq 0$: $L_n^P \subseteq NP$
2. Para todo $n \geq 0$: $L_n^P \subseteq L_{n+1}^P$
3. $L_0^P = PTIME$
4. $L_1^P = NP \cap co-NP$

Algunas propiedades básicas de la jerarquía baja

Proposición

1. Para todo $n \geq 0$: $L_n^P \subseteq NP$
2. Para todo $n \geq 0$: $L_n^P \subseteq L_{n+1}^P$
3. $L_0^P = PTIME$
4. $L_1^P = NP \cap co-NP$

Ejercicio

Demuestre la proposición.

Una propiedad fundamental de la jerarquía baja

Teorema (Schöning)

Sea $L \in L_n^P$ para $n \geq 1$. Si L es NP-completo, entonces $\Sigma_n^P = \Pi_n^P$

Una propiedad fundamental de la jerarquía baja

Teorema (Schöning)

Sea $L \in L_n^P$ para $n \geq 1$. Si L es NP-completo, entonces $\Sigma_n^P = \Pi_n^P$

Ejercicio

Demuestre el teorema.

Un resultado fundamental sobre isomorfismos de grafos

Teorema (Schöning)

$$GRAPH-ISO \in L_2^P$$

Un resultado fundamental sobre isomorfismos de grafos

Teorema (Schöning)

$$GRAPH-ISO \in L_2^P$$

Este resultado es una de las razones para creer que GRAPH-ISO no es un problema NP-completo:

Corolario

Si GRAPH-ISO es NP-completo, entonces $\Sigma_2^P = \Pi_2^P$

Un resultado fundamental sobre isomorfismos de grafos

Teorema (Schöning)

$$\text{GRAPH-ISO} \in L_2^P$$

Este resultado es una de las razones para creer que GRAPH-ISO no es un problema NP-completo:

Corolario

Si GRAPH-ISO es NP-completo, entonces $\Sigma_2^P = \Pi_2^P$

En el resto de esta sección vamos a ver la demostración de este resultado.

La demostración de $\text{GRAPH-ISO} \in L_2^P$

La demostración tiene tres partes:

La demostración de $\text{GRAPH-ISO} \in L_2^P$

La demostración tiene tres partes:

1. Vamos a definir una clase de complejidad AM que extiende NP en el mismo sentido que BPP extiende a PTIME

La demostración de $\text{GRAPH-ISO} \in L_2^P$

La demostración tiene tres partes:

1. Vamos a definir una clase de complejidad AM que extiende NP en el mismo sentido que BPP extiende a PTIME
2. Vamos a demostrar que $\overline{\text{GRAPH-ISO}} \in \text{AM}$
 - ▶ De lo cual concluimos que $\text{GRAPH-ISO} \in \text{co-AM}$

La demostración de $\text{GRAPH-ISO} \in L_2^P$

La demostración tiene tres partes:

1. Vamos a definir una clase de complejidad AM que extiende NP en el mismo sentido que BPP extiende a PTIME
2. Vamos a demostrar que $\overline{\text{GRAPH-ISO}} \in \text{AM}$
 - ▶ De lo cual concluimos que $\text{GRAPH-ISO} \in \text{co-AM}$
3. Finalmente vamos a demostrar que $\text{NP} \cap \text{co-AM} \subseteq L_2^P$
 - ▶ De lo cual concluimos que $\text{GRAPH-ISO} \in L_2^P$

Extendiendo la definición de BPP

Recuerde que un lenguaje L sobre un alfabeto Σ está en BPP si existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

- ▶ Si $w \in L$, entonces $\Pr_s(M(w, s) \text{ acepta}) \geq \frac{3}{4}$
- ▶ Si $w \notin L$, entonces $\Pr_s(M(w, s) \text{ acepta}) \leq \frac{1}{4}$

Extendiendo la definición de BPP

Recuerde que un lenguaje L sobre un alfabeto Σ está en BPP si existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

- ▶ Si $w \in L$, entonces $\Pr_s(M(w, s) \text{ acepta}) \geq \frac{3}{4}$
- ▶ Si $w \notin L$, entonces $\Pr_s(M(w, s) \text{ acepta}) \leq \frac{1}{4}$

Podemos extender la definición permitiendo a M ser no determinista

- ▶ $M(w, s)$ acepta si y sólo si existe una ejecución de M con entrada (w, s) que se detiene en un estado final

La clase de complejidad AM (Arthur-Merlin)

Definición

Sea L un lenguaje sobre un alfabeto Σ . Entonces L está en AM si existe una MT probabilística **no determinista** M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

- ▶ Si $w \in L$, entonces $\Pr_s(M(w, s) \text{ acepta}) \geq \frac{3}{4}$
- ▶ Si $w \notin L$, entonces $\Pr_s(M(w, s) \text{ acepta}) \leq \frac{1}{4}$

Algunas propiedades básicas de AM

Tenemos que $BPP \subseteq AM$ y $NP \subseteq AM$

► ¿Por qué?

Algunas propiedades básicas de AM

Tenemos que $BPP \subseteq AM$ y $NP \subseteq AM$

► ¿Por qué?

En un problema abierto si $AM = co-AM$

Algunas propiedades básicas de AM

Tenemos que $BPP \subseteq AM$ y $NP \subseteq AM$

► ¿Por qué?

En un problema abierto si $AM = co-AM$

En las siguientes transparencias vamos a demostrar que
 $\overline{GRAPH-ISO} \in AM$

Algunas propiedades básicas de AM

Tenemos que $BPP \subseteq AM$ y $NP \subseteq AM$

- ▶ ¿Por qué?

En un problema abierto si $AM = co-AM$

En las siguientes transparencias vamos a demostrar que
 $\overline{GRAPH-ISO} \in AM$

- ▶ Nótese que $GRAPH-ISO \in AM$ puesto que $GRAPH-ISO \in NP$

Un poco de notación para grafos

Sin pérdida de generalidad, suponemos desde ahora en adelante que si un grafo $G = (N, A)$ tiene n nodos, entonces $N = \{1, \dots, n\}$

- ▶ Tenemos entonces 2^{n^2} grafos con n nodos

Un poco de notación para grafos

Sin pérdida de generalidad, suponemos desde ahora en adelante que si un grafo $G = (N, A)$ tiene n nodos, entonces $N = \{1, \dots, n\}$

- Tenemos entonces 2^{n^2} grafos con n nodos

Notación

Dado un grafo $G = (N, A)$ y una biyección $f : N \rightarrow N$, definimos $f(G)$ como un grafo (N, A') tal que para cada $(a, b) \in N \times N$:

$$(a, b) \in A \text{ si y sólo si } (f(a), f(b)) \in A'$$

Un poco de notación para grafos

Sin pérdida de generalidad, suponemos desde ahora en adelante que si un grafo $G = (N, A)$ tiene n nodos, entonces $N = \{1, \dots, n\}$

- Tenemos entonces 2^{n^2} grafos con n nodos

Notación

Dado un grafo $G = (N, A)$ y una biyección $f : N \rightarrow N$, definimos $f(G)$ como un grafo (N, A') tal que para cada $(a, b) \in N \times N$:

$$(a, b) \in A \text{ si y sólo si } (f(a), f(b)) \in A'$$

Nótese que G y $f(G)$ son grafos isomorfos en la definición anterior.

- De hecho f es un isomorfismo de G en $f(G)$

Los automorfismos de un grafo

Definición

Dado un grafo $G = (N, A)$ y una biyección $f : N \rightarrow N$, decimos que f es un automorfismo para G si $f(G) = G$

El conjunto de los automorfismos de un grafo G es denotado como $\text{Aut}(G)$

- Nótese que si G tiene n nodos, entonces $|\text{Aut}(G)| \leq n!$

Los automorfismos de un grafo

Definición

Dado un grafo $G = (N, A)$ y una biyección $f : N \rightarrow N$, decimos que f es un automorfismo para G si $f(G) = G$

El conjunto de los automorfismos de un grafo G es denotado como $\text{Aut}(G)$

- Nótese que si G tiene n nodos, entonces $|\text{Aut}(G)| \leq n!$

Ejercicio

Sea n un número natural arbitrario.

1. Construya un grafo G_1 con n nodos tal que $|\text{Aut}(G_1)| = n!$
2. Construya un grafo G_2 con n nodos tal que $|\text{Aut}(G_2)| = 1$

Contando el número de grafos isomorfos a un grafo

Considere el siguiente grafo $G = (N, A)$:



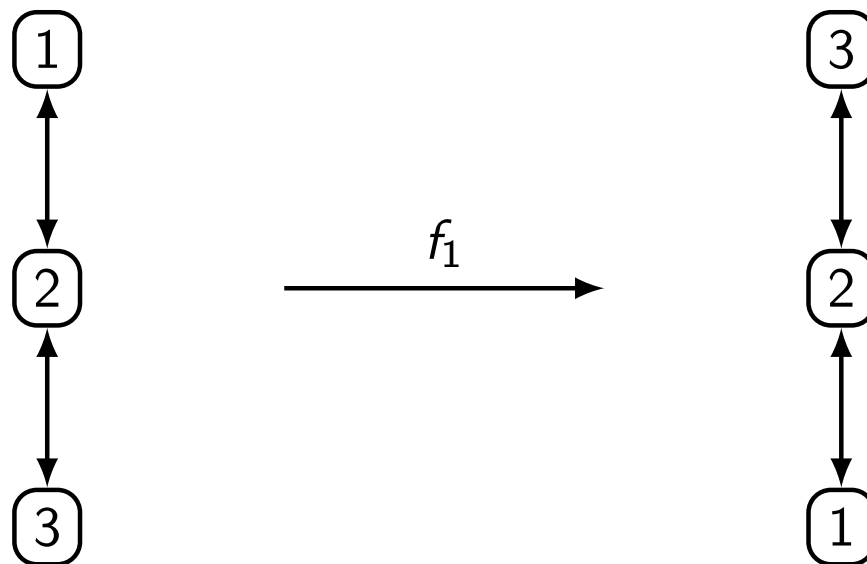
En este caso tenemos que $N = \{1, 2, 3\}$ y $A = \{(1, 2), (2, 1), (2, 3), (3, 2)\}$

Contando el número de grafos isomorfos a un grafo

Considere la biyección $f_1(1) = 3$, $f_1(2) = 2$ y $f_1(3) = 1$:

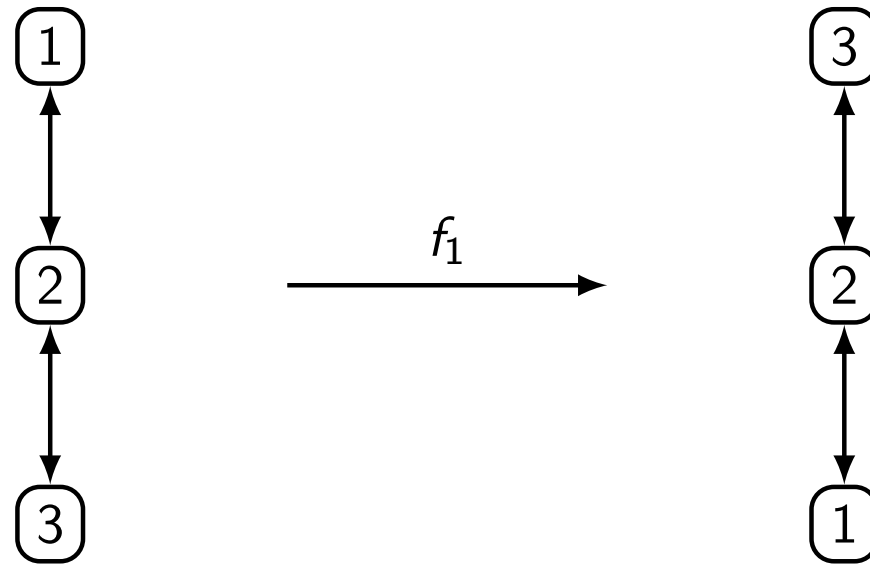
Contando el número de grafos isomorfos a un grafo

Considere la biyección $f_1(1) = 3$, $f_1(2) = 2$ y $f_1(3) = 1$:



Contando el número de grafos isomorfos a un grafo

Considere la biyección $f_1(1) = 3$, $f_1(2) = 2$ y $f_1(3) = 1$:



f_1 es un automorfismo para G ya que $f_1(G) = G$

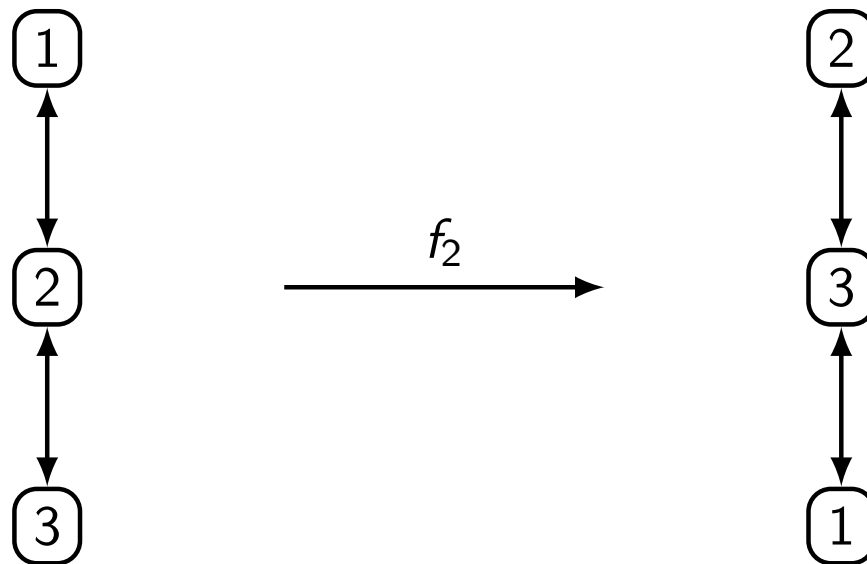
- En particular, si $f_1(G) = (N, A')$ entonces $A = A'$

Contando el número de grafos isomorfos a un grafo

Considere ahora la biyección $f_2(1) = 2$, $f_2(2) = 3$ y $f_2(3) = 1$:

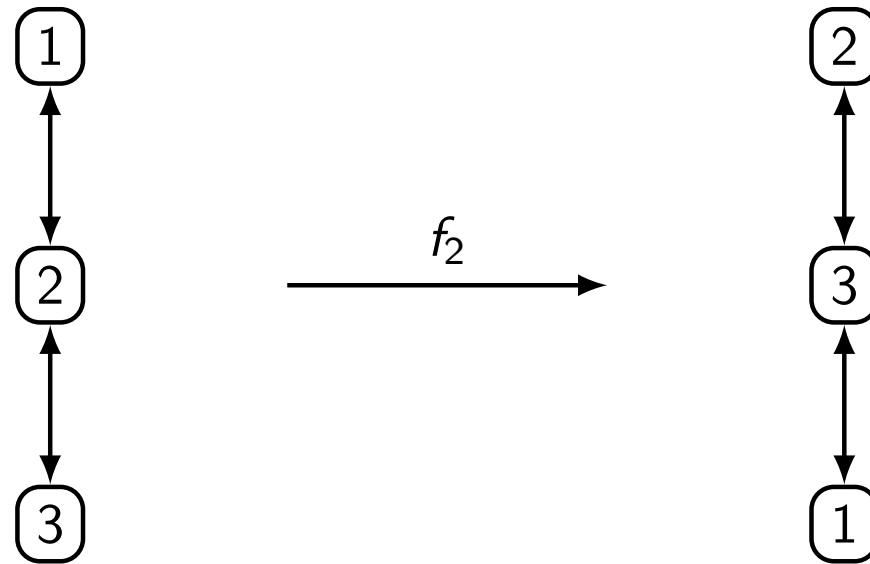
Contando el número de grafos isomorfos a un grafo

Considere ahora la biyección $f_2(1) = 2$, $f_2(2) = 3$ y $f_2(3) = 1$:



Contando el número de grafos isomorfos a un grafo

Considere ahora la biyección $f_2(1) = 2$, $f_2(2) = 3$ y $f_2(3) = 1$:

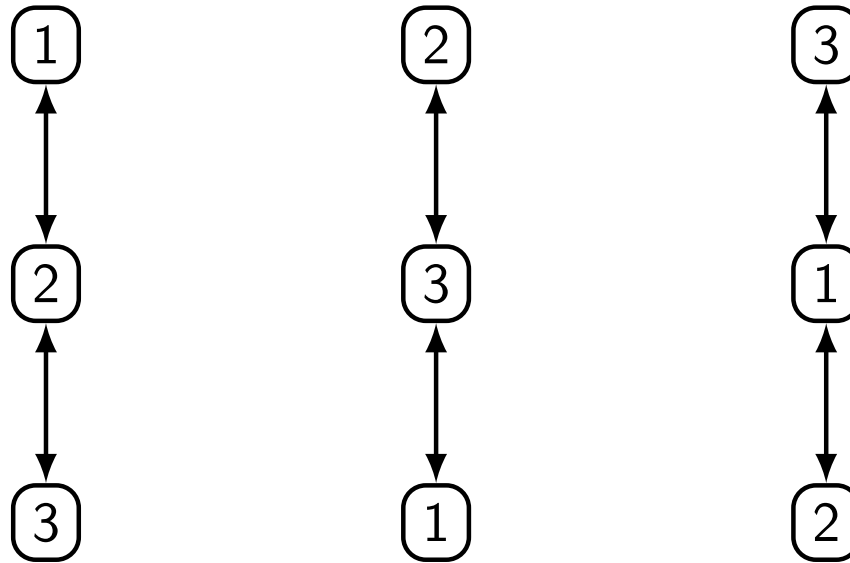


f_2 no es un automorfismo para G ya que $f_2(G) \neq G$

- En particular, el arco $(1, 2)$ está G pero no en $f_2(G)$

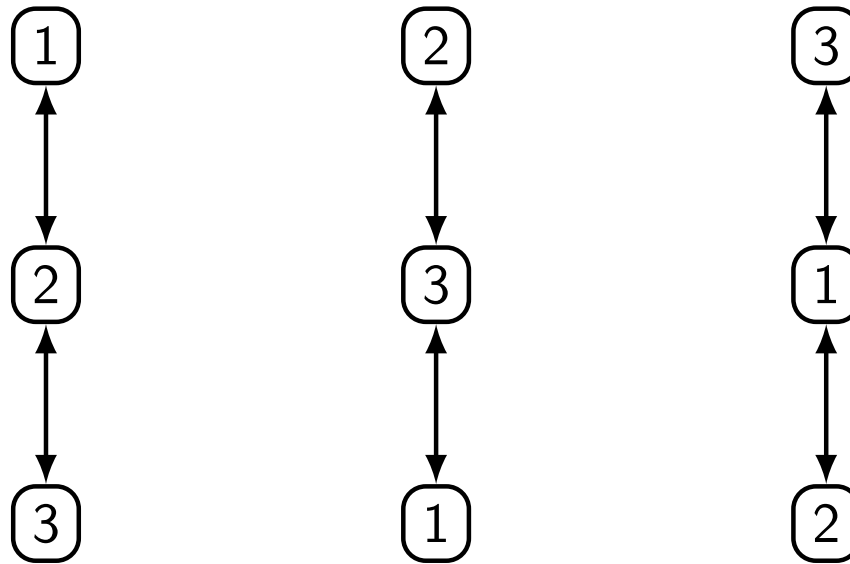
Contando el número de grafos isomorfos a un grafo

Para el caso de G tenemos seis biyecciones posibles que generan tres grafos distintos:



Contando el número de grafos isomorfos a un grafo

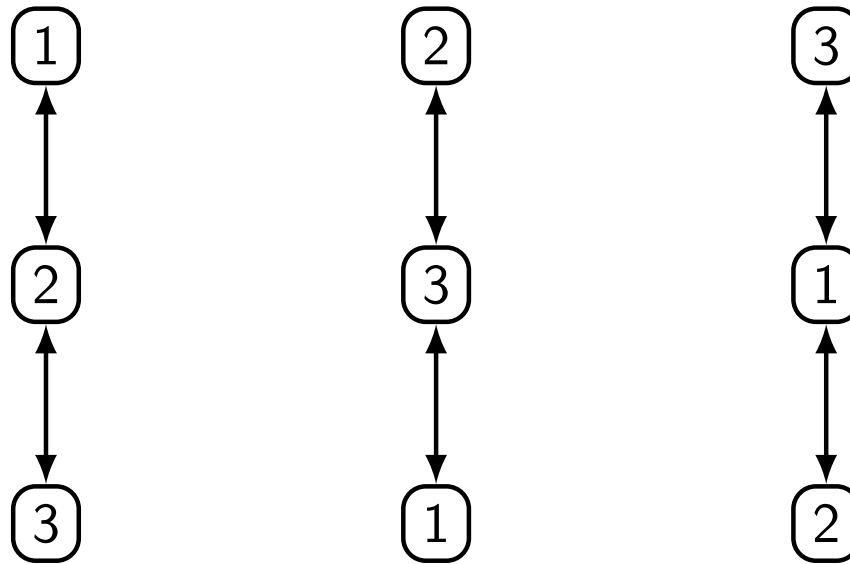
Para el caso de G tenemos seis biyecciones posibles que generan tres grafos distintos:



Tenemos entonces tres grafos distintos que son isomorfos a G

Contando el número de grafos isomorfos a un grafo

Para el caso de G tenemos seis biyecciones posibles que generan tres grafos distintos:



Tenemos entonces tres grafos distintos que son isomorfos a G

- Esto corresponde al número de biyecciones de tres elementos dividido por el número de automorfismo de G . ¿Tiene sentido esta interpretación? ¿Puede ser generalizada?

El número de grafos isomorfos a un grafo

Recuerde que estamos supuniendo que si un grafo tiene n nodos, entonces sus nodos son $1, \dots, n$

El número de grafos isomorfos a un grafo

Recuerde que estamos supuniendo que si un grafo tiene n nodos, entonces sus nodos son $1, \dots, n$

Lema

Sea G es un grafo con n nodos. El número de grafos isomorfos a G es:

$$\frac{n!}{|Aut(G)|}$$

El número de grafos isomorfos a un grafo

Recuerde que estamos supuniendo que si un grafo tiene n nodos, entonces sus nodos son $1, \dots, n$

Lema

Sea G es un grafo con n nodos. El número de grafos isomorfos a G es:

$$\frac{n!}{|Aut(G)|}$$

Demostración: Sea $B = \{f : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid f \text{ es una biyección}\}$

Defina $\sim$ como la siguiente relación sobre B . Para cada $f_1, f_2 \in B$:

$$f_1 \sim f_2 \quad \text{si y sólo si} \quad f_1(G) = f_2(G)$$

Demostración del lema

$\sim$ es una relación de equivalencia sobre B

► ¿Por qué?

Demostración del lema

$\sim$ es una relación de equivalencia sobre B

► ¿Por qué?

Sea $[f]_{\sim}$ la clase de equivalencia de $f \in B$

Demostración del lema

$\sim$ es una relación de equivalencia sobre B

► ¿Por qué?

Sea $[f]_{\sim}$ la clase de equivalencia de $f \in B$

El número de clases de equivalencia de $\sim$ corresponde al número de grafos isomorfos a G

► ¿Por qué?

Demostración del lema

Vamos a demostrar las siguientes propiedades:

1. Si id es la función identidad sobre $\{1, \dots, n\}$: $[\text{id}]_{\sim} = \text{Aut}(G)$
2. Para cada $f_1, f_2 \in B$: $|[f_1]_{\sim}| = |[f_2]_{\sim}|$

Demostración del lema

Vamos a demostrar las siguientes propiedades:

1. Si id es la función identidad sobre $\{1, \dots, n\}$: $[\text{id}]_{\sim} = \text{Aut}(G)$
2. Para cada $f_1, f_2 \in B$: $|[f_1]_{\sim}| = |[f_2]_{\sim}|$

De esto concluimos que el número de clases de equivalencia de $\sim$ es $\frac{n!}{|\text{Aut}(G)|}$, que es lo que teníamos que demostrar.

► ¿Por qué?

Demostración del lema

En primer lugar tenemos que:

$$\begin{aligned} [\text{id}]_{\sim} &= \{f \in B \mid \text{id} \sim f\} \\ &= \{f \in B \mid \text{id}(G) = f(G)\} \\ &= \{f \in B \mid G = f(G)\} \\ &= \text{Aut}(G) \end{aligned}$$

Demostración del lema

Sean $f_1, f_2 \in B$

En segundo lugar tenemos que demostrar que $|[f_1]_{\sim}| = |[f_2]_{\sim}|$

Para hacer esto vamos a construir una biyección $\mathcal{T} : [f_1]_{\sim} \rightarrow [f_2]_{\sim}$

Demostración del lema

Sean $f_1, f_2 \in B$

En segundo lugar tenemos que demostrar que $|[f_1]_{\sim}| = |[f_2]_{\sim}|$

Para hacer esto vamos a construir una biyección $\mathcal{T} : [f_1]_{\sim} \rightarrow [f_2]_{\sim}$

Para cada $f \in [f_1]_{\sim}$, se define $\mathcal{T}(f)$ de la siguiente forma:

$$\mathcal{T}(f) = (f_2 \circ f_1^{-1} \circ f)$$

Demostración del lema

Primero tenemos que demostrar que $\mathcal{T}$ está bien definida.

- Vale decir, si $f \in [f_1]_{\sim}$, entonces $\mathcal{T}(f) \in [f_2]_{\sim}$

Demostración del lema

Primero tenemos que demostrar que $\mathcal{T}$ está bien definida.

- Vale decir, si $f \in [f_1]_{\sim}$, entonces $\mathcal{T}(f) \in [f_2]_{\sim}$

Si $f \in [f_1]_{\sim}$ tenemos que $f(G) = f_1(G)$. De esto concluimos que:

$$\begin{aligned} f_2(f_1^{-1}(f(G))) &= f_2(f_1^{-1}(f_1(G))) \\ &= f_2(G) \end{aligned}$$

Demostración del lema

Primero tenemos que demostrar que $\mathcal{T}$ está bien definida.

- Vale decir, si $f \in [f_1]_{\sim}$, entonces $\mathcal{T}(f) \in [f_2]_{\sim}$

Si $f \in [f_1]_{\sim}$ tenemos que $f(G) = f_1(G)$. De esto concluimos que:

$$\begin{aligned} f_2(f_1^{-1}(f(G))) &= f_2(f_1^{-1}(f_1(G))) \\ &= f_2(G) \end{aligned}$$

Tenemos entonces que $\mathcal{T}(f)(G) = f_2(G)$

- Vale decir $f_2 \sim \mathcal{T}(f)$, de lo que concluimos que $\mathcal{T}(f) \in [f_2]_{\sim}$

Demostración del lema

Vamos a demostrar ahora que $\mathcal{T}$ es una función 1-1

Demostración del lema

Vamos a demostrar ahora que $\mathcal{T}$ es una función 1-1

Utilizando la asociatividad de la composición de funciones obtenemos:

$$\begin{aligned}\mathcal{T}(f) = \mathcal{T}(g) &\Rightarrow (f_2 \circ f_1^{-1} \circ f) = (f_2 \circ f_1^{-1} \circ g) \\ &\Rightarrow (f_1 \circ f_2^{-1}) \circ (f_2 \circ f_1^{-1} \circ f) = (f_1 \circ f_2^{-1}) \circ (f_2 \circ f_1^{-1} \circ g) \\ &\Rightarrow (f_1 \circ (f_2^{-1} \circ f_2) \circ f_1^{-1} \circ f) = (f_1 \circ (f_2^{-1} \circ f_2) \circ f_1^{-1} \circ g) \\ &\Rightarrow (f_1 \circ \text{id} \circ f_1^{-1} \circ f) = (f_1 \circ \text{id} \circ f_1^{-1} \circ g) \\ &\Rightarrow ((f_1 \circ f_1^{-1}) \circ f) = ((f_1 \circ f_1^{-1}) \circ g) \\ &\Rightarrow (\text{id} \circ f) = (\text{id} \circ g) \\ &\Rightarrow f = g\end{aligned}$$

Demostración del lema

Finalmente vamos a demostrar que $\mathcal{T}$ es sobre.

Demostración del lema

Finalmente vamos a demostrar que $\mathcal{T}$ es sobre.

Sea $g \in [f_2]_{\sim}$ y defina f como $(f_1 \circ f_2^{-1} \circ g)$

Tenemos que $f \in [f_1]_{\sim}$ ya que:

$$\begin{aligned} f(G) &= (f_1 \circ f_2^{-1} \circ g)(G) \\ &= f_1(f_2^{-1}(g(G))) \\ &= f_1(f_2^{-1}(f_2(G))) \\ &= f_1(G) \end{aligned}$$

Demostración del lema

Además, tenemos que:

$$\begin{aligned}\mathcal{T}(f) &= (f_2 \circ f_1^{-1} \circ f) \\ &= (f_2 \circ f_1^{-1} \circ (f_1 \circ f_2^{-1} \circ g)) \\ &= (f_2 \circ (f_1^{-1} \circ f_1) \circ f_2^{-1} \circ g) \\ &= (f_2 \circ \text{id} \circ f_2^{-1} \circ g) \\ &= ((f_2 \circ f_2^{-1}) \circ g) \\ &= (\text{id} \circ g) \\ &= g\end{aligned}$$

Concluimos entonces que $\mathcal{T}(f) = g$

