# Un protocolo interactivo para conteo

Defina el siguiente lenguaje:

$$\begin{aligned}\text{COUNT-CNF-SAT}^{\leq} \ = \ \{(\varphi, k) \mid \varphi \text{ es una fórmula en CNF y}\\ \text{el número de valuaciones que satisface a } \varphi \text{ es menor o igual a } k\}\end{aligned}$$

# Un protocolo interactivo para conteo

Defina el siguiente lenguaje:

$$\text{COUNT-CNF-SAT}^{\leq} \;=\; \{(\varphi, k) \mid \varphi \text{ es una fórmula en CNF y el número de valuaciones que satisface a } \varphi \text{ es menor o igual a } k\}$$

Y además considere la siguiente función que recibe como entrada a una fórmula $\varphi$ en CNF:

$$\#\text{CNF-SAT}(\varphi) \quad = \quad |\{\sigma \mid \sigma(\varphi) = 1\}|$$

# Un protocolo interactivo para conteo

Defina el siguiente lenguaje:

$$\begin{aligned}\text{COUNT-CNF-SAT}^{\leq} \;=\; \{(\varphi, k) \mid \varphi \text{ es una fórmula en CNF y} \\ \text{el número de valuaciones que satisface a } \varphi \text{ es menor o igual a } k\}\end{aligned}$$

Y además considere la siguiente función que recibe como entrada a una fórmula $\varphi$ en CNF:

$$\#\text{CNF-SAT}(\varphi) \;=\; |\{\sigma \mid \sigma(\varphi) = 1\}|$$

COUNT-CNF-SAT$^{\leq}$ y #CNF-SAT son polinomialmente equivalentes

- Si uno de los problemas se puede solucionar en tiempo polinomial, entonces el otro problema también

# Un protocolo interactivo para conteo

**Teorema**

$\mathit{COUNT\text{-}CNF\text{-}SAT}^{\leq} \in \mathit{IP}[2n]$

# Un protocolo interactivo para conteo

**Teorema**

$\mathit{COUNT\text{-}CNF\text{-}SAT}^{\leq} \in \mathit{IP}[2n]$

**Ejercicio**

Demuestre el teorema

# La probabilidad de que el verificador sea engañado

En los protocolos aleatorizados anteriores, la probabilidad de que **V** sea engañado puede ser reducida a

$$\left(\frac{1}{4}\right)^{\ell}$$

para una constante $\ell$ arbitraria

# La probabilidad de que el verificador sea engañado

En los protocolos aleatorizados anteriores, la probabilidad de que **V** sea engañado puede ser reducida a

$$\left(\frac{1}{4}\right)^{\ell}$$

para una constante $\ell$ arbitraria

Vamos a mostrar que esto se puede generalizar a cualquier lenguaje en IP

# Un lema de amplificación para IP

**Lema**

*Suponga que $\ell > 0$ y $L \in IP$. Entonces existe un verificador* **V** *que funciona en tiempo polinomial (MT aleatorizada de tiempo polinomial) tal que para cada $w \in \Sigma^*$:*

- *Si $w \in L$, entonces existe demostrador* **D** *tal que*

$$\Pr((\mathbf{V}, \mathbf{D}) \text{ acepte } w) \quad \geq \quad 1 - \left(\frac{1}{4}\right)^{\ell}$$

- *Si $w \notin L$, entonces para todo demostrador* **D'** *se tiene que*

$$\Pr((\mathbf{V}, \mathbf{D'}) \text{ acepte } w) \quad \leq \quad \left(\frac{1}{4}\right)^{\ell}$$

# Un lema de amplificación para IP

**Lema**

*Suponga que $\ell > 0$ y $L \in IP$. Entonces existe un verificador* **V** *que funciona en tiempo polinomial (MT aleatorizada de tiempo polinomial) tal que para cada $w \in \Sigma^*$:*

- *Si $w \in L$, entonces existe demostrador* **D** *tal que*

$$\Pr((\mathbf{V}, \mathbf{D}) \text{ acepte } w) \quad \geq \quad 1 - \left(\frac{1}{4}\right)^{\ell}$$

- *Si $w \notin L$, entonces para todo demostrador* **D'** *se tiene que*

$$\Pr((\mathbf{V}, \mathbf{D'}) \text{ acepte } w) \quad \leq \quad \left(\frac{1}{4}\right)^{\ell}$$

**Ejercicio**

Demuestre el lema

# ¿Cuál es el poder de IP?

Ya sabemos que NP $\subseteq$ IP y co-NP $\subseteq$ IP

- ¿Por que se tiene que NP $\subseteq$ IP?

# ¿Cuál es el poder de IP?

Ya sabemos que NP $\subseteq$ IP y co-NP $\subseteq$ IP

- ¿Por que se tiene que NP $\subseteq$ IP?

Además tenemos que BPP $\subseteq$ IP

# ¿Cuál es el poder de IP?

Ya sabemos que NP $\subseteq$ IP y co-NP $\subseteq$ IP

- ¿Por que se tiene que NP $\subseteq$ IP?

Además tenemos que BPP $\subseteq$ IP

- ¿Cómo se demuestra esto?

# ¿Cuál es el poder de IP?

¿Hay problemas en cada nivel de la jerarquía polinomial en IP? ¿Es cierto que PSPACE $\subseteq$ IP? ¿En qué clase está contenido IP?

# ¿Cuál es el poder de IP?

¿Hay problemas en cada nivel de la jerarquía polinomial en IP? ¿Es cierto que PSPACE $\subseteq$ IP? ¿En qué clase está contenido IP?

Vamos a empezar por dar una cota superior en el poder de IP

# ¿Cuál es el poder de IP?

¿Hay problemas en cada nivel de la jerarquía polinomial en IP? ¿Es cierto que PSPACE $\subseteq$ IP? ¿En qué clase está contenido IP?

Vamos a empezar por dar una cota superior en el poder de IP

Después vamos a caracterizar qué se puede resolver en IP, y qué rol juega la aleatoriedad en esto

# ¿Cuál es el poder de IP?

¿Hay problemas en cada nivel de la jerarquía polinomial en IP? ¿Es cierto que PSPACE $\subseteq$ IP? ¿En qué clase está contenido IP?

Vamos a empezar por dar una cota superior en el poder de IP

Después vamos a caracterizar qué se puede resolver en IP, y qué rol juega la aleatoriedad en esto

- En particular, nos interesa entender qué rol juega el que los bit aleatorios sean privados o conocidos por **D**

# ¿Cuál es el poder de IP?

¿Hay problemas en cada nivel de la jerarquía polinomial en IP? ¿Es cierto que PSPACE $\subseteq$ IP? ¿En qué clase está contenido IP?

Vamos a empezar por dar una cota superior en el poder de IP

Después vamos a caracterizar qué se puede resolver en IP, y qué rol juega la aleatoriedad en esto

- En particular, nos interesa entender qué rol juega el que los bit aleatorios sean privados o conocidos por **D**
- En esta estudio vamos a definir una clase que naturalmente generaliza a NP y BPP, y que juega un rol fundamental en este curso

# Una cota superior en el poder de IP

**Teorema**

$IP \subseteq PSPACE$

# Una cota superior en el poder de IP

**Teorema**

$IP \subseteq PSPACE$

**Ejercicio**

Demuestre el teorema

- Para hacer esto, piense primero como demuestra directamente que BPP $\subseteq$ PSPACE, sin utilizar el teorema de Gács-Sipser-Lautemann

# Extendiendo la definición de BPP

Recuerde que un lenguaje $L$ sobre un alfabeto $\Sigma$ 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 $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \geq \frac{3}{4}$
- Si $w \notin L$, entonces $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \leq \frac{1}{4}$

# Extendiendo la definición de BPP

Recuerde que un lenguaje $L$ sobre un alfabeto $\Sigma$ 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 $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \geq \frac{3}{4}$
- Si $w \notin L$, entonces $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \leq \frac{1}{4}$

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 $\Sigma$. 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 $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \geq \frac{3}{4}$*
- *Si $w \notin L$, entonces $\mathbf{Pr}_s(M(w, s) \text{ acepte}) \leq \frac{1}{4}$*

# 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
$\overline{\text{GRAPH-ISO}} \in$ 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 $\overline{\text{GRAPH-ISO}} \in$ AM

- Note que GRAPH-ISO $\in$ AM puesto que GRAPH-ISO $\in$ NP

# ¿Cuál es la relación entre IP y AM?

Definimos la clase AM[$k$] como IP[$k$] pero con una restricción adicional:

> Cada vez que **V** envía una pregunta a **D** tiene que enviarle adicionalmente los bits aleatorios usados

# ¿Cuál es la relación entre IP y AM?

Definimos la clase AM[$k$] como IP[$k$] pero con una restricción adicional:

> Cada vez que **V** envía una pregunta a **D** tiene que enviarle adicionalmente los bits aleatorios usados

Hablamos entonces de protocolos con bits aleatorios públicos

# ¿Cuál es la relación entre IP y AM?

Definimos la clase AM[$k$] como IP[$k$] pero con una restricción adicional:

> Cada vez que **V** envía una pregunta a **D** tiene que enviarle adicionalmente los bits aleatorios usados

Hablamos entonces de protocolos con bits aleatorios públicos

- Note que **D** conoce los bits aleatorios usados por **V**, no conoce los que **V** podría usar en el futuro

# ¿Cuál es la relación entre IP y AM?

Definimos la clase AM[$k$] como IP[$k$] pero con una restricción adicional:

> Cada vez que **V** envía una pregunta a **D** tiene que enviarle adicionalmente los bits aleatorios usados

Hablamos entonces de protocolos con bits aleatorios públicos

- Note que **D** conoce los bits aleatorios usados por **V**, no conoce los que **V** podría usar en el futuro

Definimos aquí de manera distinta a las clases AM y AM[$k$]

# ¿Cuál es la relación entre IP y AM?

Definimos la clase AM[$k$] como IP[$k$] pero con una restricción adicional:

> Cada vez que **V** envía una pregunta a **D** tiene que enviarle adicionalmente los bits aleatorios usados

Hablamos entonces de protocolos con bits aleatorios públicos

- Note que **D** conoce los bits aleatorios usados por **V**, no conoce los que **V** podría usar en el futuro

Definimos aquí de manera distinta a las clases AM y AM[$k$]

- Pero vamos a ver que están estrechamente relacionadas

# ¿Cuál es la relación entre IP y AM?

**Teorema**

$AM = AM[2]$

**Ejercicio**

Demuestre el teorema.

# ¿Cuál es la relación entre IP y AM?

La clase AM fue definida originalmente en términos de protocolos de demostración interactivos con bit aleatorios públicos

- Fue definida originalmente como AM[2]

# ¿Cuál es la relación entre IP y AM?

La clase AM fue definida originalmente en términos de protocolos de demostración interactivos con bit aleatorios públicos

- Fue definida originalmente como AM[2]

La definición de AM como una clase que naturalmente extiende a NP y BPP nos da un punto de vista alternativo

# ¿Cuál es la relación entre IP y AM?

La clase AM fue definida originalmente en términos de protocolos de demostración interactivos con bit aleatorios públicos

- Fue definida originalmente como AM[2]

La definición de AM como una clase que naturalmente extiende a NP y BPP nos da un punto de vista alternativo

- Este punto de vista es útil en la demostración de que $\overline{\text{GRAPH-ISO}} \in \text{AM}$

# $\overline{\text{GRAPH-ISO}} \in \text{AM}$

**Teorema**

$\overline{\mathit{GRAPH\text{-}ISO}} \in \mathit{AM}[2]$

# $\overline{\text{GRAPH-ISO}} \in \text{AM}$

**Teorema**

$\overline{\textit{GRAPH-ISO}} \in \textit{AM}[2]$

Dado que $\text{AM} = \text{AM}[2]$, no es claro que $\overline{\text{GRAPH-ISO}} \in \text{AM}$

- El protocolo que muestra que $\overline{\text{GRAPH-ISO}} \in \text{IP}$ no funciones si los bit aleatorios usados son públicos

# Un poco de notación para grafos

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

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

# Un poco de notación para grafos

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

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

**Notación**

*Dado un grafo $G = (N, A)$ y una biyección $f : N \to N$, 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 perdida de generalidad, suponemos desde ahora en adelante que si un grafo $G = (N, A)$ tiene $n$ nodos, entonces $N = \{1, \ldots, n\}$

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

**Notación**

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

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

Note 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 $f : N \to N$, decimos que $f$ es un automorfismo para $G$ si $f(G) = G$*

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

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

# Los automorfismos de un grafo

**Definición**

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

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

- Note 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 $G = (N, A)$:

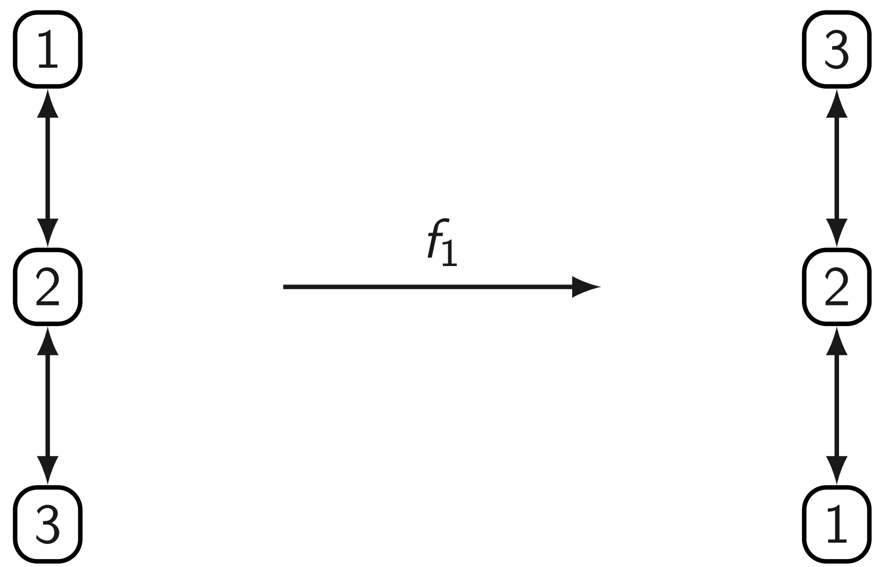

En este caso tenemos que $N = \{1, 2, 3\}$ y $A = \{(1, 2), (2, 1), (2, 3), (3, 2)\}$

# Contando el número de grafos isomorfos a un grafo

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

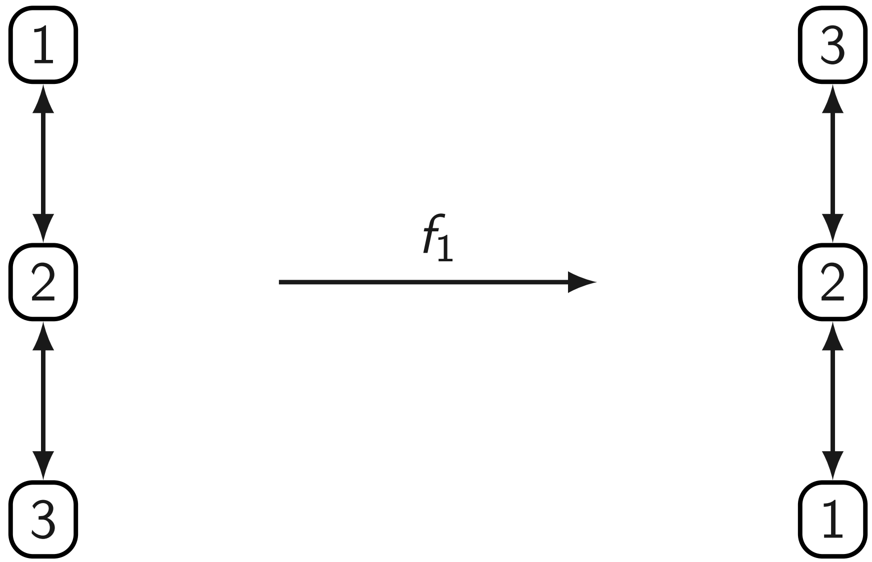
# Contando el número de grafos isomorfos a un grafo

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 $f_1(G) = G$

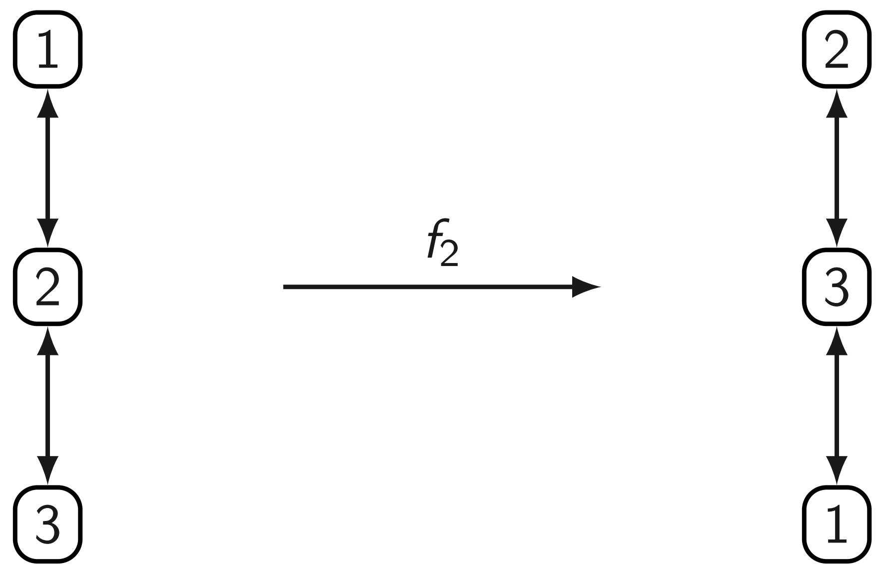
- En particular, si $f_1(G) = (N, A')$ entonces $A = A'$

# Contando el número de grafos isomorfos a un grafo

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

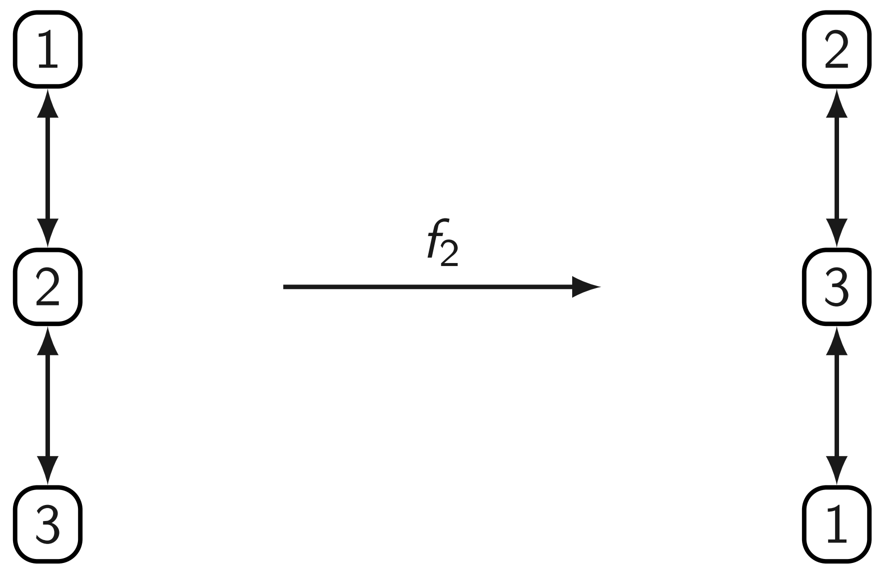
# Contando el número de grafos isomorfos a un grafo

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 $f_2(3) = 1$:

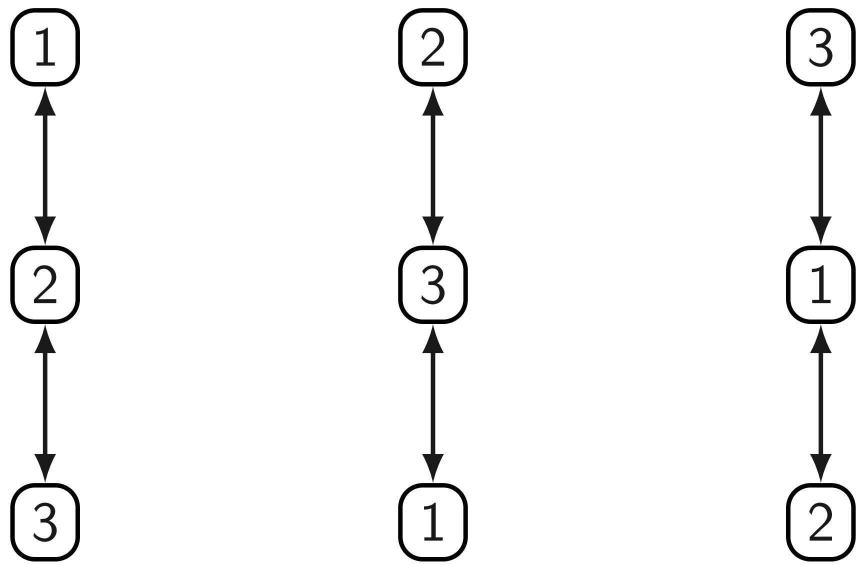



$f_2$ no es un automorfismo para $G$ ya que $f_2(G) \neq G$

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

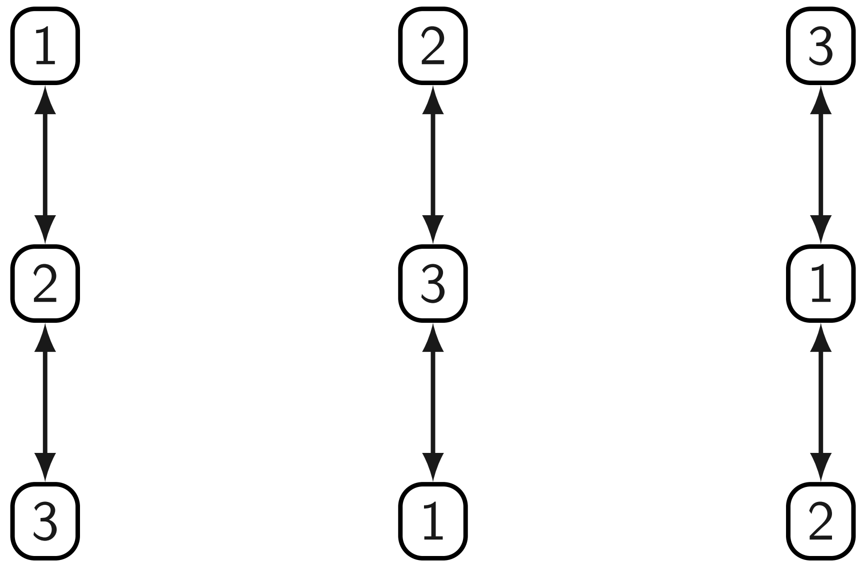
# Contando el número de grafos isomorfos a un grafo

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



# Contando el número de grafos isomorfos a un grafo

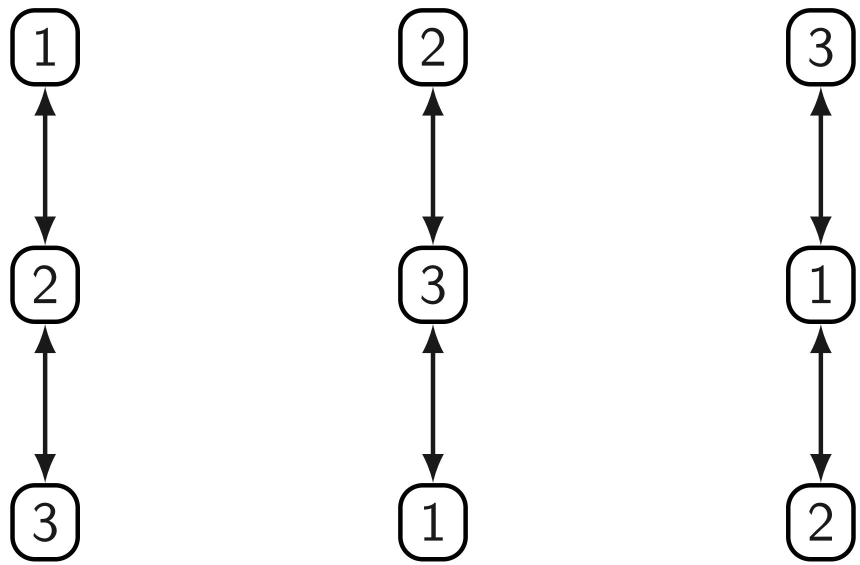
Para el caso de $G$ tenemos seis biyecciones posibles que generan tres grafos distintos:




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 suponiendo que si un grafo tiene $n$ nodos, entonces sus nodos son $1, \ldots, n$

# El número de grafos isomorfos a un grafo

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

**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 suponiendo que si un grafo tiene $n$ nodos, entonces sus nodos son $1, \ldots, n$

**Lema**

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

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

**Demostración:** Sea $B = \{f : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid f \text{ es una biyección}\}$

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 $\{1, \ldots, n\}$: $[\mathrm{id}]_\sim = \mathrm{Aut}(G)$
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 $\{1, \ldots, n\}$: $[\text{id}]_\sim = \text{Aut}(G)$
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:

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

# Demostración del lema

Sean $f_1, f_2 \in B$

# Demostración del lema

Sean $f_1, f_2 \in B$

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

# 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 $\mathcal{T} : [f_1]_\sim \to [f_2]_\sim$

# 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 $\mathcal{T} : [f_1]_\sim \to [f_2]_\sim$

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

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

# 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:

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

# 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 $(f_1 \circ f_2^{-1} \circ g)$

# 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:

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

# Demostración del lema

Además, tenemos que:

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

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

# 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:

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

# Definiendo un testigo (probabilístico) para grafos no isomorfos

Ejemplo

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

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

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 $\text{num}(G_1, G_2)$:

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

# Definiendo un testigo (probabilístico) para grafos no isomorfos

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

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

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

- ¿Cómo se demuestra que satisface la condición 2?

# Definiendo un testigo (probabilístico) para grafos no isomorfos

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

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

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

- ¿Cómo se demuestra que satisface la condición 2?

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

# El conjunto 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 $|num(G_1, G_2)| = 2 \cdot n!$, si no se tiene que $|num(G_1, G_2)| \geq 4 \cdot n!$*

# El conjunto 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 $|num(G_1, G_2)| = 2 \cdot n!$, si no se tiene que $|num(G_1, G_2)| \geq 4 \cdot n!$*

¿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 $\frac{n!}{|\mathrm{Aut}(G)|}$

# 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:

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

# Demostración del lema

Suponemos ahora que $G_1$ y $G_2$ no son grafos isomorfos

# Demostración del lema

Suponemos ahora que $G_1$ y $G_2$ no son grafos isomorfos

Tenemos que:

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

# 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:

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

# 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:

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

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