Gráficas : teoría, aplicaciones e interacciones : I

J. Ramírez Alfonsín

Université Montpellier 2, Francia

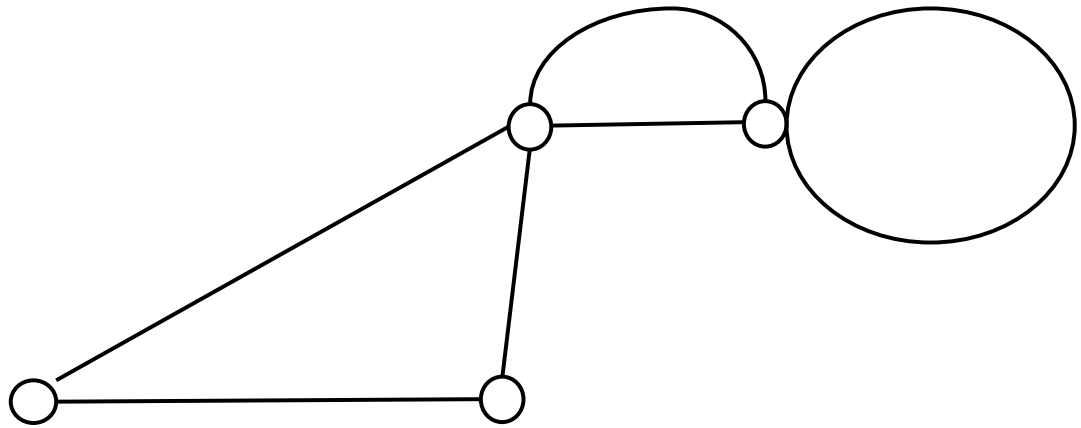
Facultad de Ciencias, UNAM, México
21 de Enero de 2013

Definiciones

- Una gráfica $G = (V, E)$ esta definida como una pareja de conjuntos finitos $V(G) \neq \emptyset$ y el conjunto $E(G)$ (que puede ser vacío) de parejas de elementos de $V(G)$ (distintos o no).
- $V(G)$ es llamado el conjunto de vértices de G et $E(G)$ el conjunto de aristas de G.

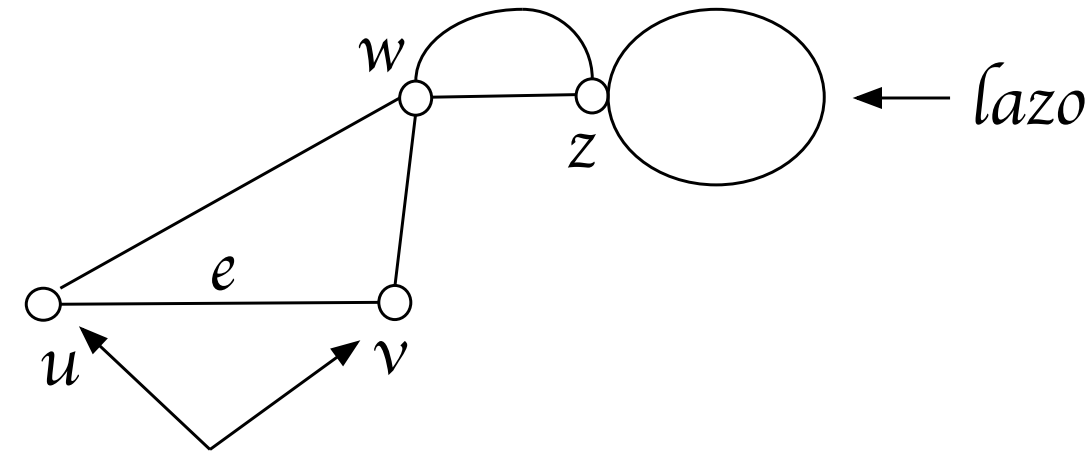
Definiciones

- Una gráfica $G = (V, E)$ esta definida como una pareja de conjuntos finitos $V(G) \neq \emptyset$ y el conjunto $E(G)$ (que puede ser vacío) de parejas de elementos de $V(G)$ (distintos o no).
- $V(G)$ es llamado el conjunto de vértices de G et $E(G)$ el conjunto de aristas de G.



- Sea $e = \{u, v\}$ una arista de G. Diremos que u y v son los extremos de e y que u y v son vecinos o adyacentes en G.
También diremos que e es incidente a u y v.
Si $u = v$ entonces e es llamado une lazo.
- Las aristas multiples son las aristas avec los mismo extremos.
- Una gráfica es simple si no tiene ni lazos ni aristas multiples.

- Sea $e = \{u, v\}$ una arista de G. Diremos que u y v son los extremos de e y que u y v son vecinos o adyacentes en G.
También diremos que e es incidente a u y v.
Si $u = v$ entonces e es llamado une lazo.
- Las aristas multiples son las aristas avec los mismo extremos.
- Una gráfica es simple si no tiene ni lazos ni aristas multiples.

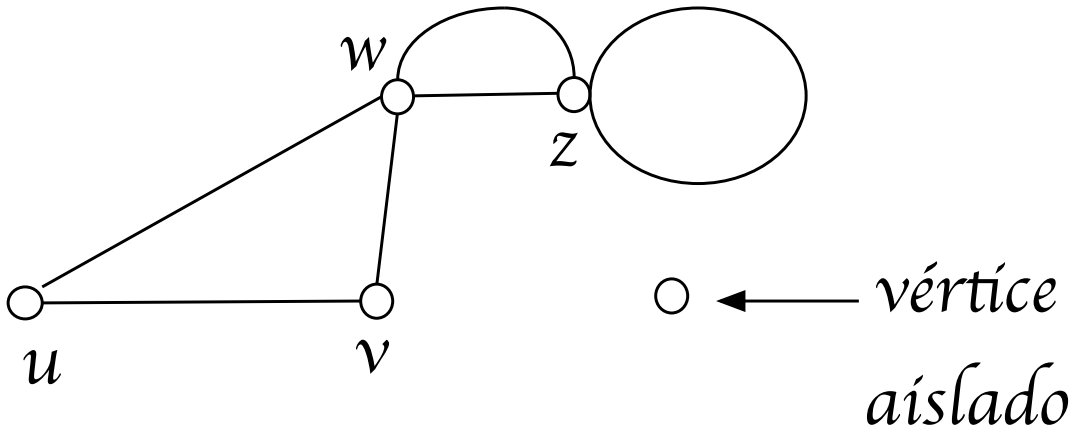


extremos de e

- El orden de una gráfica es el número de sus vértices.
- El grado de un vértice v, $d(v)$, es el número de aristas incidentes a v (contamos dos veces por cada lazo). Si $d(v) = 0$, decimos que v es un vértice aislado.
- El grado minimum de G es $\delta(G) = \min\{d(v)|v \in V(G)\}$ y el grado maximum de G es $\Delta(G) = \max\{d(v)|v \in V(G)\}$.

- El orden de una gráfica es el número de sus vértices.
- El grado de un vértice v, $d(v)$, es el número de aristas incidentes a v (contamos dos veces por cada lazo). Si $d(v) = 0$, decimos que v es un vértice aislado.
- El grado minimum de G es $\delta(G) = \min\{d(v)|v \in V(G)\}$ y el grado maximum de G es $\Delta(G) = \max\{d(v)|v \in V(G)\}$.

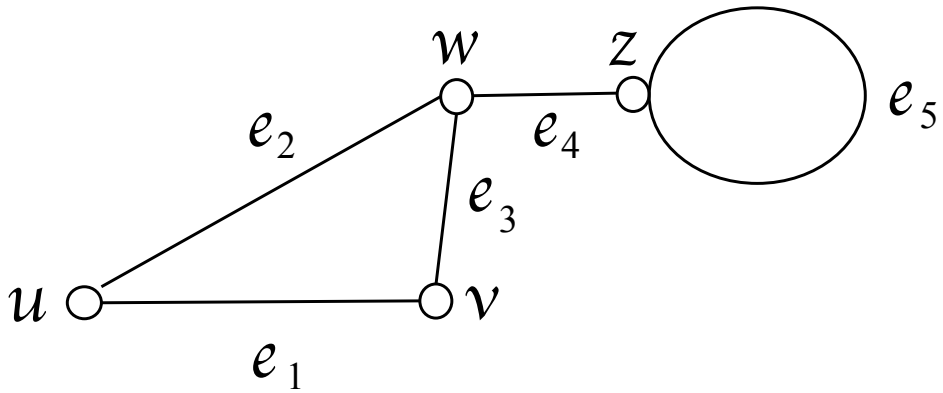
$d(u) = 2,\ d(w) = 4,\ \delta(G) = 0,\ \Delta(G) = 4$



Sea $G = (V, E)$ una gráfica con $V(G) = \{v_1, \ldots, v_n\}$ y $E(G) = \{e_1, \ldots, e_m\}$. La matriz de incidencia de G es una matriz de tamaño $n \times m$ en donde la entrada $a_{i,j} = 1$ si el vértice v_i es un extremo de la arista e_j y $a_{i,j} = 0$ en el caso contrario.

Sea $G = (V, E)$ una gráfica con $V(G) = \{v_1, \ldots, v_n\}$ y $E(G) = \{e_1, \ldots, e_m\}$. La matriz de incidencia de G es una matriz de tamaño $n \times m$ en donde la entrada $a_{i,j} = 1$ si el vértice v_i es un extremo de la arista e_j y $a_{i,j} = 0$ en el caso contrario.

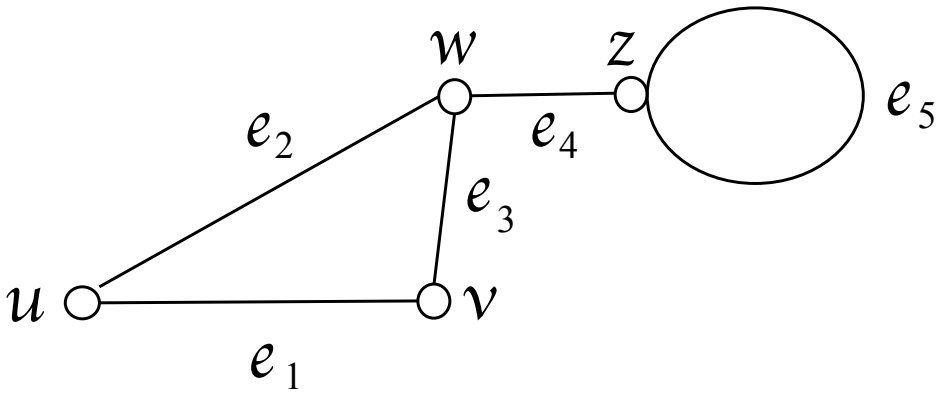
$$\begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array} \begin{array}{c} u \\ v \\ w \\ z \end{array}$$



Sea $G = (V, E)$ una gráfica con $V(G) = \{v_1, \ldots, v_n\}$ y $E(G) = \{e_1, \ldots, e_m\}$. La matriz de adyacencia de G es una matriz de tamaño $n \times n$ en donde la entrada $a_{i,j} = 1$ si el vértice v_i es adyacente al vértice v_j y $a_{i,j} = 0$ en el caso contrario.

Sea $G = (V, E)$ una gráfica con $V(G) = \{v_1, \ldots, v_n\}$ y $E(G) = \{e_1, \ldots, e_m\}$. La matriz de adyacencia de G es una matriz de tamaño $n \times n$ en donde la entrada $a_{i,j} = 1$ si el vértice v_i es adyacente al vértice v_j y $a_{i,j} = 0$ en el caso contrario.

$$\begin{array}{c} \begin{array}{cccc} u & v & w & x \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array} \begin{array}{c} u \\ v \\ w \\ z \end{array}$$

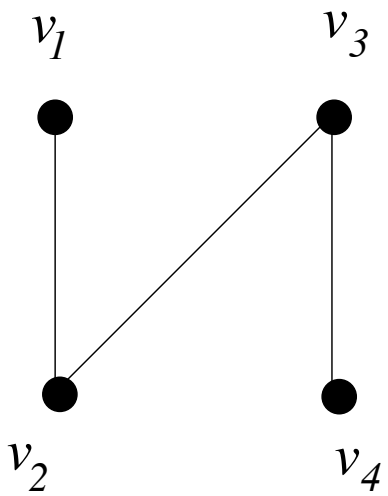


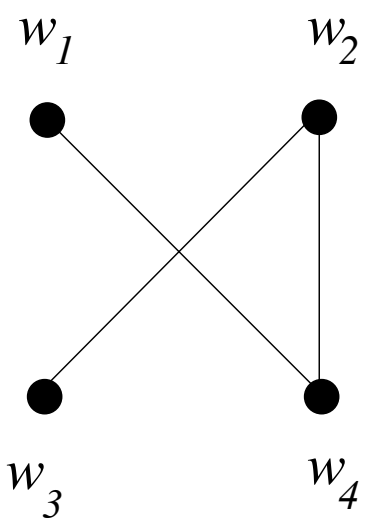
Isomorfismo

Dos gráficas G y H son isomorfas si existe una biyección $f : V(G) \longrightarrow V(H)$ tal que para todo par de vértices $u, v \in V(G)$ tenemos que u y v son adyacentes en G si y solamente si $f(u)$ y $f(v)$ son adyacentes en H.

Isomorfismo

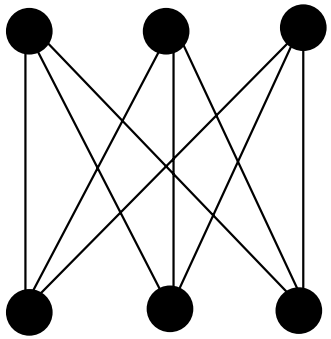
Dos gráficas G y H son isomorfas si existe una biyección $f : V(G) \longrightarrow V(H)$ tal que para todo par de vértices $u, v \in V(G)$ tenemos que u y v son adyacentes en G si y solamente si $f(u)$ y $f(v)$ son adyacentes en H.



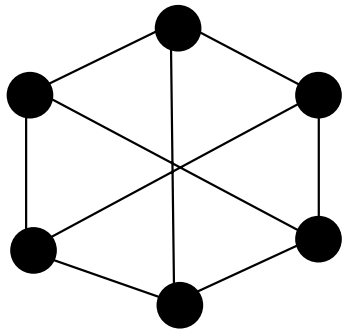


Isomorfismo

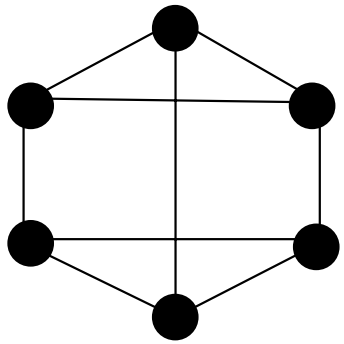
Dos gráficas G et H son isomorfas si existe una biyección $f : V(G) \longrightarrow V(H)$ tal que para todo par de vértices $u, v \in V(G)$ u y v son adyacentes en G si y solamente si $f(u)$ y $f(v)$ son adyacentes en H.



G_1



G_2



G_3

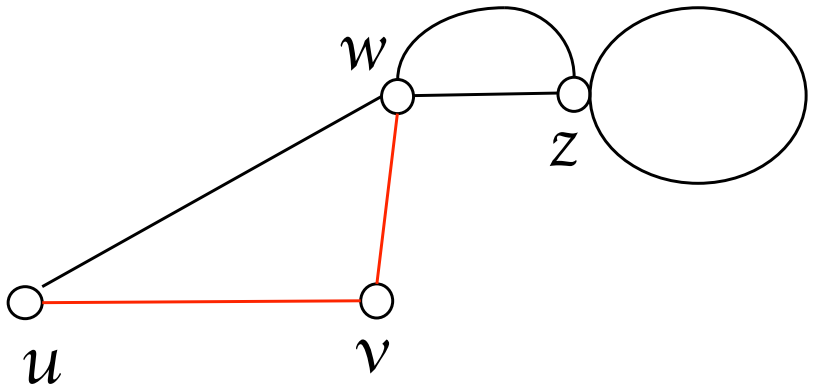
Subgráfica

- Una subgráfica de una gráfica $G = (V, E)$ es una gráfica $H = (V, E)$ con $V(H) \subseteq V(G)$ y $E(H) \subseteq E(G)$ tal que toda arista de $E(H)$ tiene sus extremos en $V(H)$.
- Una subgráfica generadora de G es una subgráfica H de G donde $V(H) = V(G)$.

Subgráfica

- Una subgráfica de una gráfica $G = (V, E)$ es una gráfica $H = (V, E)$ con $V(H) \subseteq V(G)$ y $E(H) \subseteq E(G)$ tal que toda arista de $E(H)$ tiene sus extremos en $V(H)$.
- Una subgráfica generadora de G es una subgráfica H de G donde $V(H) = V(G)$.

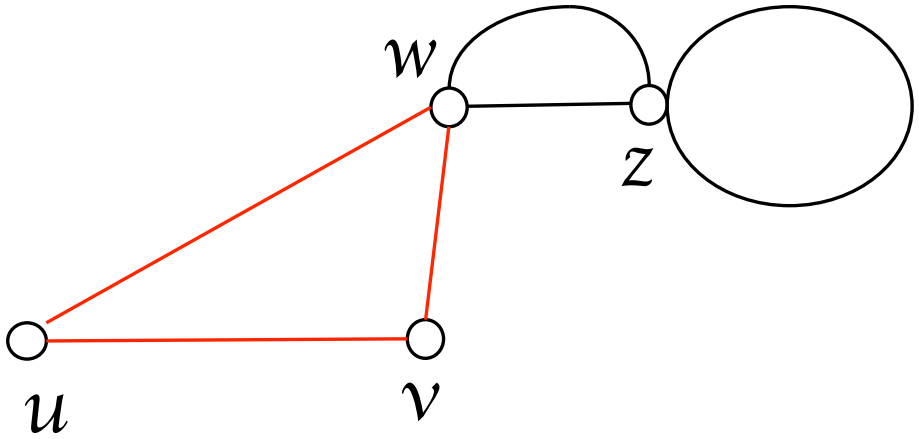
$V(H) = \{u, v, w\}, \ E(H) = \{(u, v), (v, w)\}$



- Una subgráfica inducida de G es una subgráfica H tal que $E(H)$ son todas las aristas de G cuyos extremos están en $V(H)$. Diremos que H es la subgráfica inducida por $V(H)$.

- Una subgráfica inducida de G es una subgráfica H tal que $E(H)$ son todas las aristas de G cuyos extremos están en $V(H)$. Diremos que H es la subgráfica inducida por $V(H)$.

$V(H) = \{u, v, w\},\ E(H) = \{(u, v), (v, w), (u, w)\}$



Grado

Teorema Sea G una gráfica simple. Entonces,

$$2|E(G)| = \sum_{v \in V(G)} d(v).$$

Grado

Teorema Sea G una gráfica simple. Entonces,

$$2|E(G)| = \sum_{v \in V(G)} d(v).$$

Teorema Sea G una gráfica simple. Entonces, el número de vértices de grado impar es par

Grado

Teorema Sea G una gráfica simple. Entonces,

$$2|E(G)| = \sum_{v \in V(G)} d(v).$$

Teorema Sea G una gráfica simple. Entonces, el número de vértices de grado impar es par

Demostración Utilizando teorema.

Problema sobre conocer personas

Problema ¿ Es cierto que en toda reunión de n personas siempre hay al menos dos que conocen el mismo número de personas ?

Problema sobre conocer personas

Problema ¿ Es cierto que en toda reunión de n personas siempre hay al menos dos que conocen el mismo número de personas ?

Respuesta SI

Problema sobre conocer personas

Problema ¿ Es cierto que en toda reunión de n personas siempre hay al menos dos que conocen el mismo número de personas ?

Respuesta SI

Traducir el problema en términos de gráficas y demostrar que en toda gráfica siempre hay al menos dos vértices que tienen el mismo grado.

Problema sobre una réunion

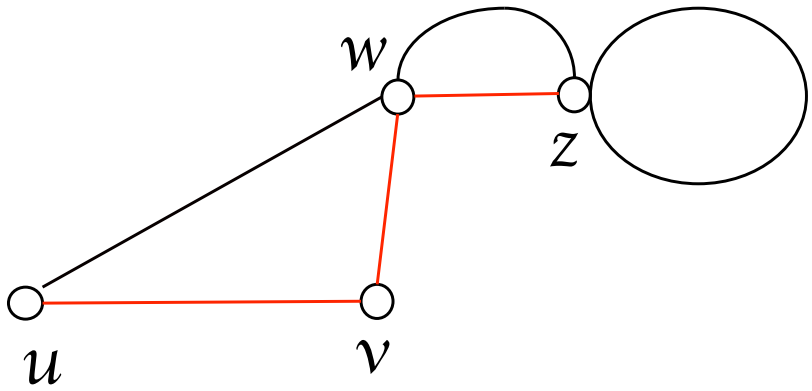
Problema El Señor y la Señora X invitaron 4 parejas a una reunión. Llegando a la reunión, cada invitado le da la mano o no a las personas que están ya presentes, pero dos miembros de la misma pareja no se dan la mano.

El Señor X le pregunta a cada persona presente cuantas veces dió la mano y obtiene 9 respuestas diferentes ¿Cuántas manos dio la Señora X ?

- Dados dos vértice u y v de G, Un uv-camino de longitud k de G es una sucesión de vértices $v_0, v_1, \ldots, v_k$ todos distintos tales que $u = v_0, v = v_k$ y v_{i-1} es adyacente a v_i para $i = 1, \ldots, k$.
- Un uv-camino es simple si todas las aristas utilizadas son diferentes.

- Dados dos vértice u y v de G, Un uv-camino de longitud k de G es una sucesión de vértices $v_0, v_1, \ldots, v_k$ todos distintos tales que $u = v_0, v = v_k$ y v_{i-1} es adyacente a v_i para $i = 1, \ldots, k$.
- Un uv-camino es simple si todas las aristas utilizadas son diferentes.

Un uz-camino

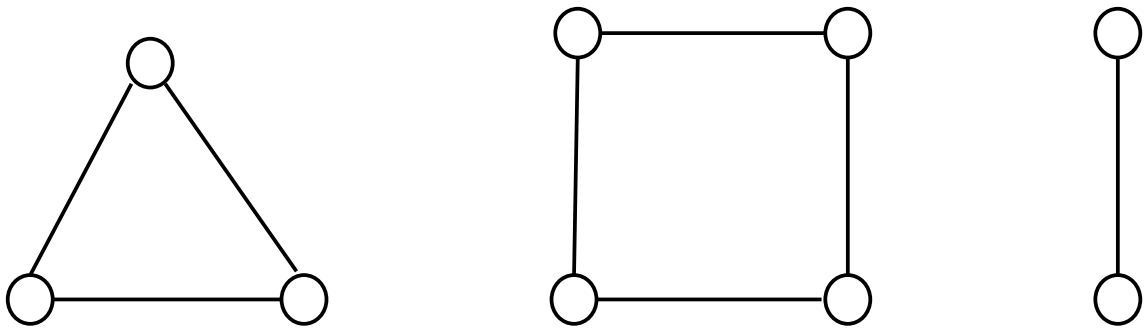


Conexidad

Una gráfica G es conexa si para todo par de vértices u y v de G existe un uv-camino en G.

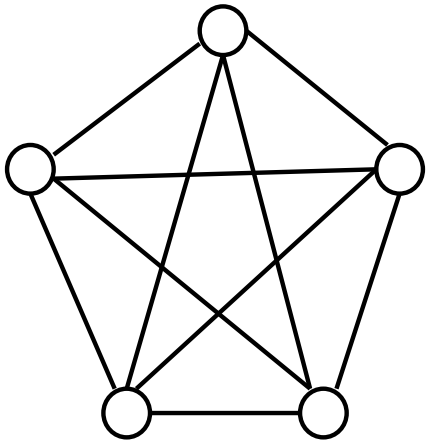
Conexidad

Una gráfica G es conexa si para todo par de vértices u y v de G existe un uv-camino en G.

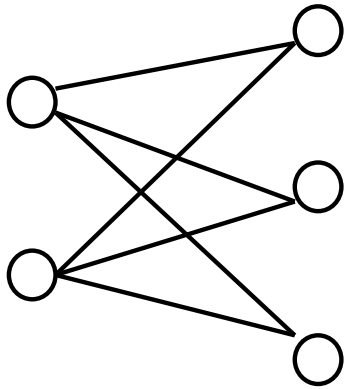


Una gráfica de orden n es llamada completa y denotada por K_n si todo par de vértices son adyacentes.
Una gráfica G es bipartita si existe una partición de $V(G) = V_1 \cup V_2$ tal cualquier arista de G tenga uno de sus extremos en V_1 y el otro en V_2. Si $|V_1| = n_1$ y $|V_2| = n_2$ entonces la gráfica es denotada por K_{n_1,n_2}.

Una gráfica de orden n es llamada completa y denotada por K_n si todo par de vértices son adyacentes.
Una gráfica G es bipartita si existe una partición de $V(G) = V_1 \cup V_2$ tal cualquier arista de G tenga uno de sus extremos en V_1 y el otro en V_2. Si $|V_1| = n_1$ y $|V_2| = n_2$ entonces la gráfica es denotada por K_{n_1,n_2}.



$\mathcal{K}_5$



$\mathcal{K}_{2,3}$

Coloración

Sea G una gráfica simple y sea $k \geq 1$ un entero.
- Una k-coloración de los vértices de G es une aplicación $g : V(G) \to \{1, \ldots, k\}$ tal que si u y v son dos vértices adyacentes, $g(u)$ es diferente de $g(v)$. Una gráfica es k-coloreable si admite una k-coloración.
- El entero mas pequeño k tal que G es k-coloreable es llamado número cromático de G, denotado por $\chi(G)$.

Algoritmo de coloración

Algoritmo Glotón

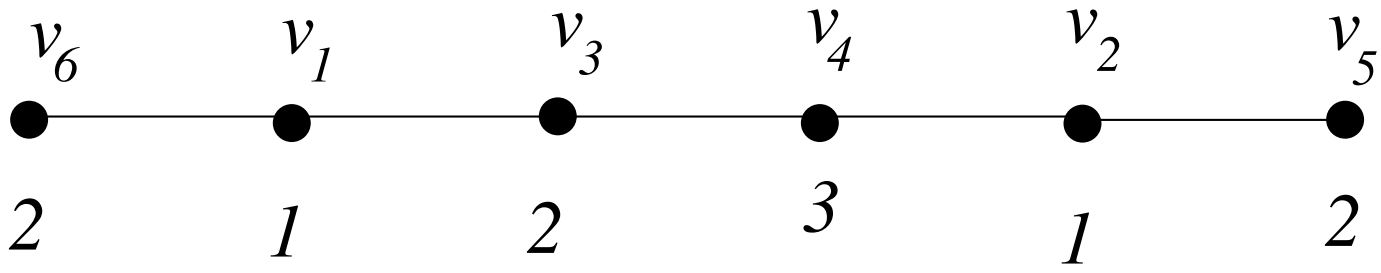
Datos de entrada : Una gráfica G y un entero positivo k
Salida : Une k-coloración de G (pero no garantizada)

- Ordonemos arbitrariamente los n vértices de G : $v_1, \ldots, v_n$.
- Le damos al vértice v_1 el color 1 y después coloreamos con el color 1 sucesivamente los vértices de la lista $v_2, \ldots, v_n$ que no son adyacentes a algún vértice ya coloreado.
- Si sobran vértices no coloreados, le damos el color 2 al primer vértice
de la lista no coloreado y empezamos el proceso
precedente hasta que ya ho haya colores.

Este algoritmo glotón puede dar una k-coloración de G con $k \geq \chi(G)$ pero no necesariamente $k = \chi(G)$.

Este algoritmo glotón puede dar una k-coloración de G con $k \geq \chi(G)$ pero no necesariamente $k = \chi(G)$.

Ejemplo : la numeración de los vértices de la siguiente gráfica da una 3-coloración sin embargo su número cromático es 2.



Teorema Una gráfica G es bipartita si y solamente si G es 2-coloreable.

Teorema Una gráfica G es bipartita si y solamente si G es 2-coloreable.

Teorema Sea G una gráfica con grado maximal $\Delta(G)$. Entonces $\chi(G) \leq \Delta(G) + 1$.

Teorema Una gráfica G es bipartita si y solamente si G es 2-coloreable.

Teorema Sea G una gráfica con grado maximal $\Delta(G)$. Entonces $\chi(G) \leq \Delta(G) + 1$.

Demostración Aplicando el algoritmo glotón.

Teorema Una gráfica G es bipartita si y solamente si G es 2-coloreable.

Teorema Sea G una gráfica con grado maximal $\Delta(G)$. Entonces $\chi(G) \leq \Delta(G) + 1$.

Demostración Aplicando el algoritmo glotón.

Observación $\chi(C_k) = \Delta(C_k) + 1$, k-impar y $\chi(K_n) = \Delta(K_n) + 1$.

Teorema Una gráfica G es bipartita si y solamente si G es 2-coloreable.

Teorema Sea G una gráfica con grado maximal $\Delta(G)$. Entonces $\chi(G) \leq \Delta(G) + 1$.

Demostración Aplicando el algoritmo glotón.

Observación $\chi(C_k) = \Delta(C_k) + 1$, k-impar y $\chi(K_n) = \Delta(K_n) + 1$.

Teorema (Brooks) Sea G una gráfica con grado maximal $\Delta(G)$ y diferente a C_k, k-impar y a la gráfica completa. Entonces, $\chi(G) \leq \Delta(G)$.

Dilema del espía

En una noche con mucha neblina un espía regresa al castillo después de haber cumplido su misión en el campo enemigo. Cuando estaba cerca de la entrada del castillo una voz tenue le pregunta : ¿cuál es la contraseña ? Pero, ¿es un amigo o enemigo el que le preguntó ? ¿Cómo puede el espía mostrar que él sabe la contraseña sin revelársela a un posible impostor ?

Dilema del espía

En una noche con mucha neblina un espía regresa al castillo después de haber cumplido su misión en el campo enemigo. Cuando estaba cerca de la entrada del castillo una voz tenue le pregunta : ¿cuál es la contraseña ? Pero, ¿es un amigo o enemigo el que le preguntó ? ¿Cómo puede el espía mostrar que él sabe la contraseña sin revelársela a un posible impostor ?

Un método que ha sido propuesto para el intercambio de claves en este contexto es la prueba de conocimiento cero.

Protocolo

- Un protocolo interactivo consiste en dos algoritmos : P (*probador*) y V (*verificador*) que leen una entrada en común w y después de hacer cálculos respectivos se comunican en forma alternada para determinar si w tiene una propiedad específica (w pertence a un conjunto L).

Protocolo

- Un protocolo interactivo consiste en dos algoritmos : P (*probador*) y V (*verificador*) que leen una entrada en común w y después de hacer cálculos respectivos se comunican en forma alternada para determinar si w tiene una propiedad específica (w pertence a un conjunto L).

- V es *probabilístico* (le es permitido hacer selecciones al azar) y tiene como datos de salida *aceptado* o *rechazado*.

Protocolo

- Un protocolo interactivo consiste en dos algoritmos : P (*probador*) y V (*verificador*) que leen una entrada en común w y después de hacer cálculos respectivos se comunican en forma alternada para determinar si w tiene una propiedad específica (w pertence a un conjunto L).

- V es *probabilístico* (le es permitido hacer selecciones al azar) y tiene como datos de salida *aceptado* o *rechazado*.

- Un auténtico P transmitirá partes del secreto y así V aceptará $w \in L$, pero la transmisión será inútil para verificadores falsos. Un probador impostor causaría que V rechazará w con una alta probabilidad.

Método con gráficas

Sea L un conjunto de gráficas 3-coloreable y C el conjunto de colores.

Método con gráficas

Sea L un conjunto de gráficas 3-coloreable y C el conjunto de colores.
Sea f una función de encripción, esto es $f(c_1, r) = c_1^e$ encripta el color c_1 mediante una cadena aleatoria de lanzamientos de monedas r dando el color encriptado c_1^e.

Método con gráficas

Sea L un conjunto de gráficas 3-coloreable y C el conjunto de colores.
Sea f una función de encripción, esto es $f(c_1, r) = c_1^e$ encripta el color c_1 mediante una cadena aleatoria de lanzamientos de monedas r dando el color encriptado c_1^e.
w representa una 3-coloración de una gráfica conexa G (con n vértices y m aristas). P y V conocen G y C pero sólo P conoce el secreto (una 3-coloración correcta de G).

Prueba interactiva de conocimiento cero para $w \in L$

(1) P aplica una permutación π al azar a los colores. P forma una cadenas r_i a partir de lanzamientos de monedas y calcula $f(\pi(c_i), r_i) = c_i^e$ y el color encriptado c_i^e es enviado a V.

Prueba interactiva de conocimiento cero para $w \in L$

(1) P aplica una permutación π al azar a los colores. P forma una cadenas r_i a partir de lanzamientos de monedas y calcula $f(\pi(c_i), r_i) = c_i^e$ y el color encriptado c_i^e es enviado a V.

---

(2) V guarda $c_1^e, \ldots, c_n^e$ y escoje al azar dos vértices adyacentes u y v y los envia a P.

Prueba interactiva de conocimiento cero para $w \in L$

(1) P aplica una permutación π al azar a los colores. P forma una cadenas r_i a partir de lanzamientos de monedas y calcula $f(\pi(c_i), r_i) = c_i^e$ y el color encriptado c_i^e es enviado a V.

---

(2) V guarda $c_1^e, \ldots, c_n^e$ y escoje al azar dos vértices adyacentes u y v y los envia a P.

---

(3) P checa que u y v son adyacentes (si no, P detecta un impostor). Si $(u, v) \in E(G)$ P manda los colores $\pi(c_u)$ y $\pi(c_v)$ y los valores r_u y r_v a V.

Prueba interactiva de conocimiento cero para $w \in L$

(1) P aplica una permutación π al azar a los colores. P forma una cadenas r_i a partir de lanzamientos de monedas y calcula $f(\pi(c_i), r_i) = c_i^e$ y el color encriptado c_i^e es enviado a V.

---

(2) V guarda $c_1^e, \ldots, c_n^e$ y escoje al azar dos vértices adyacentes u y v y los envia a P.

---

(3) P checa que u y v son adyacentes (si no, P detecta un impostor). Si $(u, v) \in E(G)$ P manda los colores $\pi(c_u)$ y $\pi(c_v)$ y los valores r_u y r_v a V.

---

(4) V calcula $c'_u = f(\pi(c_u), r_u)$ y $c'_v = f(\pi(c_v), r_v)$; V checa que $c'_u = c_u^e$ y $c'_v = c_v^e$, $\pi(c_u), \pi(c_v) \in C$ y $\pi(c_u) \neq \pi(c_v)$
si alguno de estos chequeos falla, entonces V se detiene y rechaza.

Prueba interactiva de conocimiento cero para $w \in L$

(1) P aplica una permutación π al azar a los colores. P forma una cadenas r_i a partir de lanzamientos de monedas y calcula $f(\pi(c_i), r_i) = c_i^e$ y el color encriptado c_i^e es enviado a V.

---

(2) V guarda $c_1^e, \ldots, c_n^e$ y escoje al azar dos vértices adyacentes u y v y los envia a P.

---

(3) P checa que u y v son adyacentes (si no, P detecta un impostor). Si $(u, v) \in E(G)$ P manda los colores $\pi(c_u)$ y $\pi(c_v)$ y los valores r_u y r_v a V.

---

(4) V calcula $c'_u = f(\pi(c_u), r_u)$ y $c'_v = f(\pi(c_v), r_v)$; V checa que $c'_u = c_u^e$ y $c'_v = c_v^e$, $\pi(c_u), \pi(c_v) \in C$ y $\pi(c_u) \neq \pi(c_v)$ si alguno de estos chequeos falla, entonces V se detiene y rechaza.

---

(5) Si le chequeo en (4) fué bueno entonces P y V empiezan nuevamente en el paso (1). Si m^2 interacciones de este protocolo es completado sin rechazo de V, entonces V se detiene y acepta w.

¿Porque funciona ?

- Si $w \in L$ entonces V acepta con probabilidad 1 después de m^2 iteraciones (ya que V nunca va a detectar una falla de P).

¿Porque funciona ?

- Si $w \in L$ entonces V acepta con probabilidad 1 después de m^2 iteraciones (ya que V nunca va a detectar una falla de P).
- Si $w \notin L$ entonces el P debe enviar una coloración inválida (vértices adyacentes con el mismo color o bien que use mas de tres colores), lo cual será detectado con probabilidad al menos de $1/m$ en una iteración.

¿Porque funciona ?

- Si $w \in L$ entonces V acepta con probabilidad 1 después de m^2 iteraciones (ya que V nunca va a detectar una falla de P).
- Si $w \notin L$ entonces el P debe enviar una coloración inválida (vértices adyacentes con el mismo color o bien que use mas de tres colores), lo cual será detectado con probabilidad al menos de $1/m$ en una iteración.

La probabilidad que V se detenga y acepte después de m^2 pruebas al azar (sin detectar fallas de P) es de a lo mas $(1 - 1/m)^{m^2}$
(dicha probabilidad es suficiente).

- El protocolo es muy astuto

- Una prueba de interacción sería suficiente que P simplemente mandara los colores de los vértices a V, los demás pasos son necesarios para asegurar el conocimiento cero.

- El protocolo es muy astuto

- Una prueba de interacción sería suficiente que P simplemente mandara los colores de los vértices a V, los demás pasos son necesarios para asegurar el conocimiento cero.
- V aprende que los vértices u y v tienen diferente color (lo cual no es más que lo que aprendería si simplemente supusiera que $w \in L$)

- El protocolo es muy astuto

- Una prueba de interacción sería suficiente que P simplemente mandara los colores de los vértices a V, los demás pasos son necesarios para asegurar el conocimiento cero.
- V aprende que los vértices u y v tienen diferente color (lo cual no es más que lo que aprendería si simplemente supusiera que $w \in L$)
- V no gana información adicional en cada etapa porque los colores son permutados al azar y encriptados.

- El protocolo es muy astuto

- Una prueba de interacción sería suficiente que P simplemente mandara los colores de los vértices a V, los demás pasos son necesarios para asegurar el conocimiento cero.
- V aprende que los vértices u y v tienen diferente color (lo cual no es más que lo que aprendería si simplemente supusiera que $w \in L$)
- V no gana información adicional en cada etapa porque los colores son permutados al azar y encriptados.
- Aún después de muchas pruebas V no tendrá idea de como es la 3-coloración de la gráfica.