Resumen de teoremas para el final de Matemática Discreta II

Agustin Curto, agucurto95@gmail.com

2016

Índice general

Capítulo 1

Parte A

1.1. La complejidad de EDMONS-KARP

<u>**Teorema:**</u> La complejidad de $\langle E - K \rangle$ con $n = |V|$ y $m = |E|$ es $\mathcal{O}(nm^2)$.

<u>**Prueba:**</u> Sean: $f_0, f_1, f_2, \ldots$ la sucesión de flujos creados por $\langle E - K \rangle$. Es decir, el paso k crea f_k.

Para cada k definimos funciones:

- $d_k(x) =$ "distancia" entre s y x en el paso k, en caso de existir, si no ∞.
- $b_k(x) =$ "distancia" entre x y t en el paso k, en caso de existir, si no ∞.

"Distancia": longitud del menor camino aumentante entre dos vértices.

Observaciones:

1. - $d_k(s) = 0$
   - $b_k(t) = 0$
2. Sabemos que las distancias de $\langle E - K \rangle$ no disminuyen en pasos sucesivos, como esto será útil para esta demostración llamaremos $\circledast$ a la demostración de:

$$d_k(x) \leq d_{k+1}(x)$$
$$b_k(x) \leq b_{k+1}(x)$$

Llamemos <u>*crítico*</u> a un lado disponible en el paso k pero no disponible en el paso *k+1*. Es decir, si xy es un lado $\Rightarrow$ xy se satura ó yx se vacía en el paso k.

Supongamos que al construir f_k el lado xy se vuelve crítico, el camino: $s \ldots$ x,y $\ldots$ t se usa para construir f_k.

$$\begin{aligned} d_k(t) &= d_k(x) + b_k(x) \\ &= d_k(x) + b_k(y) + 1 \end{aligned} \tag{1}$$

Para que xy pueda ser *crítico* nuevamente debe ser usado en la otra dirección (*i.e* yx). Sea j el paso posterior a k en el cual se usa el lado en la otra dirección, el camino $s \cdots$ y,x $\cdots$ t se usa para construir f_j.

$$\begin{aligned} d_j(t) &= d_j(x) + b_j(x) \\ &= d_j(y) + 1 + b_j(x) \end{aligned} \tag{2}$$

Entonces:

$$\text{De (1) y (2)} \Rightarrow \begin{cases} d_j(x) = d_j(y) + 1 & \star \\ d_k(y) = d_k(x) + 1 & \dagger \end{cases}$$

Luego:

$$\begin{aligned} d_j(t) &= d_j(x) + b_j(x) \\ &= d_j(y) + 1 + b_j(x) && \text{Por } \dagger \\ &\geq d_k(y) + 1 + b_k(x) && \text{Por } \circledast \\ &= d_k(x) + 1 + 1 + b_k(x) && \text{Por } \star \\ &= d_k(t) + 2 \\ \Rightarrow d_j(t) &\geq d_k(t) + 2 \end{aligned}$$

Por lo tanto cuando un lado se vuelve crítico recien puede volver a saturarse cuando la distancia de s a t haya aumentado en por lo menos 2. Puede existir $\mathcal{O}(n/t)$ tales aumentos, es decir:

$$\#\text{ Veces que un lado puede volverse crítico} = \mathcal{O}(n).$$

$$\begin{aligned} \therefore Complejidad(\langle E-K \rangle) &= (\#pasos) * Compl(1\ paso) \\ &= (\#\text{veces que un lado se vuelve crítico}) * (\#lados) * Compl(BFS) \\ &= \mathcal{O}(n) * \mathcal{O}(m) * \mathcal{O}(m) \\ &= \mathcal{O}(nm^2) \end{aligned}$$

1.2. Las distancias de Edmonds-Karp no disminuyen en pasos sucesivos

Teorema: Sean: $f_0, f_1, f_2, \ldots$ la sucesión de flujos creados por $\langle E-K \rangle$. Es decir, el paso k crea f_k.

Para cada k definimos funciones:

- $d_k(x) =$ "distancia" entre s y x en el paso k en caso de existir, si no ∞.
- $b_k(x) =$ "distancia" entre x y t en el paso k en caso de existir, si no ∞.

"Distancia": longitud del menor camino aumentante entre dos vértices.

Queremos probar que:

1. $d_k(x) \leq d_{k+1}(x)$

2. $b_k(x) \leq b_{k+1}(x)$

<u>Prueba:</u> Lo probaremos por inducción y solo para d_k ya que para b_k la prueba es análoga.

$$\text{HI: } H(i) = \{\forall_z : d_{k+1}(z) \leq i, \textit{ vale } d_k(z) \leq d_{k+1}(z)\}$$

1. Caso Base: $\boxed{\text{i} = 0}$ $\quad H(0) = \{\forall_z : d_{k+1}(z) \leq 0,\, d_k(z) \leq d_{k+1}(z)\}$
   Pero $d_{k+1}(z) \leq 0 \Rightarrow z = s$

$$\begin{aligned} d_k(z) &= d_k(s) \\ &= 0 \\ &\leq d_{k+1}(s) \\ &\leq d_{k+1}(z) \\ \Rightarrow d_k(z) &\leq d_{k+1}(z) \end{aligned}$$

2. Caso Inductivo: Supongamos ahora que vale H(i), veamos que vale H($)i$+*1*.
   Sea z con $d_{k+1}(z) \leq i$+*1*, si $d_{k+1}(z) \leq i$ vale H(i) para z.

$$\therefore\ d_{k+1}(z) \leq d_{k+1}(z)$$

   Supongamos que $\boxed{d_{k+1}(z) = i + 1}$
   Entonces existe un camino aumentante, relativo a f_k, de la forma: $s = z_0,\ z_1,\ \ldots\ z_i,\ z_{i+1} = z$.
   Sea $\boxed{x = z_i}$

   - <u>Caso 1:</u> Existe algun camino aumentante, relativo a f_{k-1} de la forma $s,\ \ldots\ x,\ z$. $\Rightarrow \boxed{d_k(x) \leq d_k(x) + 1}$

     Pues al haber un camino $\underbrace{s,\ \ldots\ x,}_{d_k(x)}\ z$, llamemosle A, de longitud $d_k(x) + 1$ entre s y z, sabemos que el minimo de todos los caminos de s a z seran $\leq$ A.
   - Caso 2: No existe un camino aumentante, relativo a f_{k-1}, pero si existe un camino aumentante relativo a f_k. Por lo tanto el lado xz no esta "disponible" en el paso k, ya que xz está saturado zx está vacío relativo a f_{k-1}. Para construir f_k usamos un camino de la forma $s,\ \ldots\ z,\ x$. Es decir:

     1) $f_{k-1}(xz) = C(xz)$ pero $f_k(xz) < C(xz),\ f_k$ devuelve flujo por xz ó
     2) $f_{k-1}(zx) = 0$ pero $f_k(zx) > 0,\ f_k$ manda flujo por zx.

     Como $\langle E - K \rangle$ funciona con BFS, ese camino usado pra construir f_k debe ser de longitud mínima. Es decir: $\quad d_k(x) = d_k(z) + 1$

$$\begin{aligned} d_k(z) &= d_k(x) - 1 \\ &\leq d_k(x) + 1 \end{aligned}$$

   <u>Conclusión:</u> En cualquiera de los dos casos tenemos:

$$\boxed{d_k(x) \leq d_k(x) + 1}$$

Ahora bien: $\quad d_{k+1}(x) = d_{k+1}(z_i) = i \quad \Rightarrow \quad$ vale H(i) para x.
$\therefore d_k(z) \leq d_{k+1}(x)$

$$\begin{aligned} d_{k+1}(x) &= d_{k+1}(z_i) \\ &= i \\ &\Rightarrow \text{H}(i) \text{ vale para x.} \\ \therefore\ d_k(z) &\leq d_{k+1}(x) \end{aligned}$$

Por lo tanto:

$$\begin{aligned} d_k(z) &\leq d_k(x) + 1 \\ &\leq d_{k+1}(x) + 1 \\ &= i + 1 \\ &= d_{k+1}(z) \\ &\Rightarrow \text{H}(i\textit{+1}) \text{ vale.} \end{aligned}$$

1.3. La complejidad de DINIC

Teorema: La complejidad del algoritmo de Dinic es $\mathcal{O}(n^2m)$.
Prueba: Como Dinic es un algoritmo que trabaja con networks auxiliares y vimos que la distancia entre s y t en networks auxiliares consecutivos aumenta y puede ir a lo sumo entre 1 y $n-1$ entonces hay a lo sumo $\mathcal{O}(n)$ networks auxiliares.

Complejidad(Dinic)= $\mathcal{O}(n)*$ Compl(Hallar un flujo bloqueante en un NA con Dinic)

Para probar que la complejidad de Dinic es $\mathcal{O}(n^2m)$ debemos probar que complejidad del paso bloqueante es $\mathcal{O}(nm)$.
Sea:

- A = Avanzar()
- R = Retroceder()
- I = Incrementar_Flujo + Inicialización ($\mathcal{O}(1)$)

Una corrida de Dinic luce como:

AA ... AIAAARA ... AIAARAAARR ... IA ...

Dividamos la corrida en subpalabras del tipo:

$* \ \underbrace{AA\ \ldots\ A}_{Todas A's} I$

$* \ \underbrace{AA\ \ldots\ A}_{Todas A's} R$

Nota: el número de A's puede ser 0.
Debemos determinar:

1. Cual es la complejidad de cada subpalabra.

2. Cuantas palabras hay de cada tipo.

Complejidad de cada subpalabra
Recordemos que:

$$\text{A:}\left[\begin{array}{l} P[i+1] = \text{algún elemento de } \Gamma^+(P[i]) \\ i = i+1 \end{array}\right.$$

$$\Rightarrow \text{A es } \mathcal{O}(1)$$

$$\text{R:}\left[\begin{array}{l} P[i+1] = \text{borrar } P[i-1]P[i] \text{ del NA} \\ i = i-1 \end{array}\right.$$

$$\Rightarrow \text{R es } \mathcal{O}(1)$$

$$\text{I:}\left[\ P[i+1] = \text{recorre 2 veces, un camino de longitud } d = d(t)\right.$$

$$\Rightarrow \text{I es } \mathcal{O}(d)$$

Por lo tanto:

$$\begin{aligned} Compl(\underbrace{A\ \dots\ A}_{j\ veces}R) &= \underbrace{\mathcal{O}(1) +\ \dots\ \mathcal{O}(1)}_{j\ veces} + \mathcal{O}(1) \\ &= \mathcal{O}(j) + \mathcal{O}(1) \\ &= \mathcal{O}(j) \end{aligned}$$

Pero como cada A hace $i = i+1$ y tenemos $0 \leq i \leq d \ \Rightarrow\ j \leq d$.

$$\therefore\ Compl(A\ \dots\ AR) = \mathcal{O}(d)$$

Similarmente:

$$\begin{aligned} Compl(A\ \dots\ AI) &= \underbrace{\mathcal{O}(1) +\ \dots\ \mathcal{O}(1)}_{\leq d\ veces} + \mathcal{O}(1) \\ &= \mathcal{O}(d) + \mathcal{O}(1) \\ &= \mathcal{O}(d) \end{aligned}$$

Cantidad de subpalabras

- R tiene la instrucción "**borrar lado**". Como los lados borrados quedan borrados hay a lo sumo m R's, es decir:

$$\therefore\ \#(A\ \dots\ AR's) \leq m$$

- I tiene también línes de la forma:

  Lo que está dentro del **if** se cumple al menos una vez, es decir:

$$\therefore\ \#(A\ \dots\ AI's) \leq m$$

  Este análisis muestra que:

$$\therefore\ \#(A\ \dots\ AR's) + \#(A\ \dots\ AI's) \leq m$$

  Por lo tanto hay $\leq m$ palabras, cada una de complejidad $\mathcal{O}(d)$.

$$\begin{aligned} \therefore\ Compl(Paso\ Bloqueante) &= \mathcal{O}(m) + \mathcal{O}(md) \\ &= \mathcal{O}(mn) \end{aligned}$$

  ya que $d \leq n$.

1.4. La complejidad de WAVE

Teorema: La complejidad del algoritmo de Wave es $\mathcal{O}(n^3)$.

Prueba: Como Wave es un algoritmo que trabaja con networks auxiliares y vimos que la distancia entre s y t en networks auxiliares consecutivos aumenta y puede ir a lo sumo entre 1 y $n-1$ entonces hay a lo sumo $\mathcal{O}(n)$ networks auxiliares.

$$\text{Complejidad(Wave)} = \mathcal{O}(n) * \text{Compl(Hallar un flujo bloqueante en un NA con Wave)}$$

Para probar que la complejidad de Wave es $\mathcal{O}(n^3)$ debemos probar que complejidad del paso bloqueante es $\mathcal{O}(n^2)$. El paso bloqueante de Wave consiste en una serie de:

- Olas hacia adelante: Sucesión de **forwrdbalance** (FB)
- Olas hacia atrás: Sucesión de **backwardbalance** (BB)

Cada FB y BB es una sucesión de "**buscar vecinos**"y "**procesar**"el lado resultante. Estos "procesamientos" son complicados pero $\mathcal{O}(1)$.

$$\therefore\ Compl(Paso\ Bloqueante) = \#\text{"}procesamientos\text{" de lados}$$

Los "procesamientos" de lados los podemos dividir en dos categorías:

1. Aquellos procesamientos que saturan o vacian el lado. Denotaremos "T" al número de estos procesamientos.
2. Aquellos procesamientos que no saturan ni vacian el lado. Denotaremos "Q" al número de estos procesamientos.

Por lo tantos queremos acotar $T+Q$.

Complejidad de T:

- ¿Puede un lado xy saturado volver a saturarse?

  Para poder volver a saturarse primero tiene que vaciarse auque sea un poco, es decir, antes de poder volver a saturarlo "y" debe devolver flujo a "x" , pero para que en Wave "y" le devuelva flujo a "x" debe ocurrir que "y" este bloqueado (porque BB(y) solo se ejecuta si "y" está bloqueado), pero si "y" está bloqueado "x" no puede mandarle flujo nunca más.

  $$\therefore\ xy \text{ no puede resaturarse}$$

  Conclusión 1: Los lados se saturan solo una vez.

- ¿Puede un lado xy vaciado completamente volver a vaciarse?

  Para poder volver a vaciarse como está vacío completamente, primero hay que mandar flujo, pero si lo vacié "y" está bloqueado por lo que "x" no puede mandar flujo.

  $$\therefore\ xy \text{ no puede volver a vaciarse}$$

  Conclusión 2: Los lados se vacían completamente a lo sumo una vez.

  Las conclusiones (1) y (2) implican que $\boxed{T \leq 2\,m}$

Complejidad de Q:

En cada FB a lo sumo un lado no se satura y en cada BB a lo sumo un lado no se vacía completamente.

$\therefore$ Q $\leq$ # Total de FB's y BB's

- # FB's en cada ola hacia adelante es $\leq n$ (un FB por vértice)
- # BB's en cada ola hacia atrás es $\leq n$

  $\therefore$ Total de FB's y BB's $\leq 2\ n$ #Total de ciclos de "ola adelante $-$ ola hacia atrás"

Ahora bien, en cada ola hacia adelante, pueden o no, bloquearse algunos vértices. Si no se bloquea ningún vértice entonces todos los vértices ($\neq s,\ t$) quedan balaceados por lo que estamos en la última ola. Luego en toda ola que no sea la última se bloquea al menos un vértice ($\neq s,\ t$).

$$\therefore \ \#\text{Total de ciclos es} \leq (n-2)+1 = n-1$$
$$\Rightarrow \boxed{Q \ \leq 2n(n-1) = \mathcal{O}(n^2)}$$

$$\begin{aligned} \therefore\ T+Q &\leq 2m+\mathcal{O}(n^2) \\ &= \mathcal{O}(m)+\mathcal{O}(n^2) \\ &= \mathcal{O}(n^2) \end{aligned}$$

1.5. La distancia entre NA sucesivos aumenta

Teorema: Sea A un NA (network auxiliar) y sea A^* el siguiente NA. Sean d(x) y $d^*(x)$ las distancias de s a t en A y A^* respectivamente, entonces: $d(t) < d^*(t)$.

Prueba: Como A y A^* se construyen con BFS sabemos que $d(t) \leq d^*(t)$ pero queremos ver el $<$.

Sea:

$$s = x_0,\ x_1,\ \ldots\ t = x_r$$

un camino dirigido en A^*.

Ese camino $\boxed{\text{No existe}}$ en A ya que para pasar de A a A^* debemos bloquear todos los caminos dirigidos de A. Por lo tanto si ese camino estuviese en A, Dinic lo habría bloqueado y no estaría en A^*.

¿Cuáles son las razones posibles para que no esté en A?

1. Puede faltar un vértice, es decir $\exists\ i\ :\ x_i \nexists V(A)$ entonces:

$$\begin{aligned} d(t) &\leq d(x_i) \\ &\leq d^*(x_i) \\ &= i < r \\ &= d^*(t) \end{aligned}$$
$$\boxed{\therefore\ d(t) < d^*(t)}$$

2. Están todos los vértices pero falta una arista, es decir $\exists\ i\ :\ x_i x_{i+1} \nexists E(A)$.

a) $x_i x_{i+1}$ no está porque corresponde a un lado vacío o saturado en NA, es decir $x_i x_{i+1}$ no está en el recidual que dá origen a A pero si está en el residual que dá origen a A^*. Para que esto pase se tiene que haber usado el lado $x_{i+1} x_i$ en A. Luego podemos cocluir, por la prueba de $\langle E - K \rangle$ que:

$$d^*(t) \geq d(t) + 2 > d(t)$$

$$\boxed{\therefore\ d(t) < d^*(t)}$$

b) $x_i x_{i+1}$ si está en el residual pero: $\boxed{d(x_{i+1}) \neq d(x_i) + 1}$ (1)

Pero como $x_i x_{i+1}$ está en el residual entonces: $\boxed{d(x_{i+1}) \leq d(x_i) + 1}$ (2)

De (1) y (2) tenemos que: $\boxed{d(x_{i+1}) < d(x_i) + 1}$ $\circledast$
Entonces:

$$\begin{aligned}
d(t) &= d(x_{i+1}) + b(x_{i+1}) && \text{Por } \langle E - K \rangle \\
&\leq d(x_{i+1}) + b^*(x_{i+1}) && \text{Por } \langle E - K \rangle \\
&< d(x_i) + 1 + b^*(x_{i+1}) && \text{Por } \circledast \\
&\leq d^*(x_i) + 1 + b^*(x_{i+1}) && \text{Por } \langle E - K \rangle \\
&= d^*(x_{i+1}) + b^*(x_{i+1}) && \text{Por } (\dagger) \\
&= d^*(t)
\end{aligned}$$

$$\boxed{\therefore\ d(t) < d^*(t)}$$

($\dagger$): Ya que $s,\ x_1,\ \ldots\ x_r$

Capítulo 2

Parte B

2.1. 2-COLOR es polinomial

2.2. Teorema Max-Flow Min-Cut

<u>Teorema:</u>

a) Si f es flujo y S es corte $\Rightarrow$ V(f) $\leq$ Cap(S).

b) Si V(f) = Cap(S) $\Rightarrow$ f es maximal y S es minimal.

c) Si f es maximal $\Rightarrow \exists$ S con V(f) = Cap(S).

<u>Prueba:</u> Denotemos $\boxed{V(f) = f(S,\overline{S}) - f(\overline{S},S)}$ $(\star)$

a) $\boldsymbol{f}$ es flujo y S es corte $\Rightarrow$ V($\boldsymbol{f}$) $\leq$ Cap(S).

$$V(f) \overset{Por\ (\star)}{=} f(S,\overline{S}) \underbrace{- \underbrace{f(\overline{S},S)}_{\geq 0}}_{\leq 0}$$

$$\Rightarrow V(f) \leq f(S,\overline{S}) \leq Cap(S,\overline{S}) = \text{Cap(S)}$$

b) V($\boldsymbol{f}$) = Cap(S) $\Rightarrow$ $\boldsymbol{f}$ es maximal y S es minimal.

Supongamos que V(f) = Cap(S). Sea g un flujo cualquiera y T un corte cualquiera.

- $V(g) \overset{Por\ a)}{\leq} Cap(S) = V(f) \Rightarrow$ f es maximal.
- $Cap(T) \overset{Por\ a)}{\geq} V(f) = Cap(S) \Rightarrow$ S es minimal.

c) $\boldsymbol{f}$ es maximal $\Rightarrow \exists$ S con V($\boldsymbol{f}$) = Cap(S).

Sea $S = \{s\} \cup \{x\ :\ \exists$ camino aumentante realtivo a f entre s y $t\}$

¿$t \in S$?
<u>Si t estuviera en S:</u> existiría un camino aumentante entre s y t.
Por el teorema del camino aumentante podemos construir un flujo g tal que:

$$V(g) = V(f) + \epsilon \text{ para algun } \epsilon > 0$$
$$\therefore V(g) > V(f) \textbf{ Absurdo} \text{ pues } f \text{ es maximal.}$$

$\therefore t \notin S \Rightarrow S$ es corte.

Solo resta ver que: $V(f) = Cap(S)$

Por $(\star)$: $V(f) = \underbrace{f(S, \overline{S})}_{(1)} - \underbrace{f(\overline{S}, S)}_{(2)}$

Analicemos (1) y (2)

(1) $f(S, \overline{S}) = \sum_{\substack{x \in S \\ y \in \overline{S} \\ xy \in E}} f(\overrightarrow{xy})$

$x \in S \Rightarrow \exists$ camino aumentante $s, \ldots x$.

$y \in \overline{S} \Rightarrow \nexists$ camino aumentante entre s y y. En particular $s, \ldots x, \ldots y$ no es camino aumentante, por lo que no puede darse que $f(\overrightarrow{xy}) < Cap(\overrightarrow{xy})$.

$\Rightarrow f(\overrightarrow{xy}) = Cap(\overrightarrow{xy}) \qquad \forall x \in S, \forall y \in \overline{S} : \overrightarrow{xy} \in E.$

$\Rightarrow \boxed{f(S, \overline{S})} = \sum_{\substack{x \in S \\ y \in \overline{S} \\ xy \in E}} f(\overrightarrow{xy}) = \sum_{\substack{x \in S \\ y \in \overline{S} \\ xy \in E}} Cap(\overrightarrow{xy}) = Cap(S, \overline{S}) = \boxed{Cap(S)}$

(2) $f(\overline{S}, S) = \sum_{\substack{x \in \overline{S} \\ y \in S \\ xy \in E}} f(\overrightarrow{xy})$

$x \in \overline{S} \Rightarrow \nexists$ camino aumentante entre s y x.

$y \in S \Rightarrow \exists$ camino aumentante $s, \ldots y$.

En particular $s \ldots y, y \ldots x$ no es camino aumentante $\Rightarrow f(\overrightarrow{xy}) = 0 \; \forall x \in S, \forall y \in \overline{S} : \overrightarrow{xy} \in E$.

$\therefore \boxed{f(\overline{S}, S) = 0}$

Luego de (1) y (2)

$$\begin{aligned} V(f) &= f(S, \overline{S}) - f(\overline{S}, S) \\ &= Cap(S) - 0 \\ &= Cap(S) \end{aligned}$$

2.3. Complejidad del Hungaro es $\mathcal{O}(n^4)$

<u>**Teorema:**</u> La complejidad del algoritmo Húngaro es $\mathcal{O}(n^4)$.
<u>**Prueba:**</u>

1. La complejidad del matching inicial es $\mathcal{O}(n^2)$, ya que:

   Restar mínimo de cada fila:

   $$(\underbrace{\mathcal{O}(n)}_{calcular\ min} + \underbrace{\mathcal{O}(n)}_{restar\ min}) * \underbrace{n}_{\#filas} = \mathcal{O}(n^2)$$

   Idem para las columnas.

2. Llamemos **extender** el matching, a incrementar su número de filas en 1, es decir, agregar una fila más al matching.

$$\#\text{ extensiones de matching} = \mathcal{O}(n)$$

   Resta ver la complejidad de cada **extender**.

3. En cada extensión vamos a ir revisando filas y columnas, donde escanear una fila es $\mathcal{O}(n)$ y se realizan n escaneos, por lo que sería $\mathcal{O}(n^2)$ sin considerar que se debe realizar un cambio de matriz.

   Hacer un **cambio de matriz** es $\mathcal{O}(n^2)$, ya que:

   - Buscar $m = \min S \text{ x } \overline{\Gamma(S)} \to \mathcal{O}(n^2)$
   - Restar m de $S \to \mathcal{O}(n^2)$
   - Sumar m a $\Gamma(S) \to \mathcal{O}(n^2)$

   Luego la implementación NAIVE lanzaría nuevamente el algoritmo desde cero. La forma correcta es continuar con el matching que teniamos, ya que el mismo no se pierde.

   Si lo hacems así, ¿Cuántos **cambios de matriz** habrá antes de extender un matching nuevamente?

   Lema Interno: Luego de un **cambio de matriz**, se extiende el matching o bien se aumenta S.

   Prueba:

$$\begin{array}{cc} \left(\begin{array}{c|c} \text{A} & \text{A} \\ \hline \text{B} & \text{C} \end{array}\right) & \begin{array}{c} \overline{\text{S}} \\ \text{S} \end{array} \\ \begin{array}{cc} \Gamma(S) & \overline{\Gamma(S)} \end{array} & \end{array}$$

   Referencias:

   - A: puede haber ceros.
   - B: ceros del matching.
   - C: no hay ceros, no hay matching.

   Al restar $m = \min S \text{ x } \overline{\Gamma(S)}$ de las filas de S, habrá un nuevo cero en alguna fila i ($\in S$) y columna j ($\in \overline{\Gamma(S)}$) entonces la columna se etiquetará con i y se revisará. Tenemos dos resultados posible:

   a) j está libre (i.e no forma parte del matching) $\Rightarrow$ extendemos el matching.

   b) j forma parte de matching $\Rightarrow \exists$ fila k matcheada con j. En este caso, la fila k se etiquetará con j, por lo que el "nuevo" $S \geq S \cup \{k\}$.

   Entonces se termina con una extensión o se produce un nuevo S de cardinalidad, al menos $|S| + 1$.

   Fin Lema Interno

   Luego como $|S|$ solo puede crecer $\mathcal{O}(n)$ veces, tenemos que hay a lo sumo n **cambios de matriz** antes de extender el matching. Entonces:

$$\text{Complejidad(1 Extensión)} = \underbrace{\mathcal{O}(n)}_{\#CM} * \underbrace{\mathcal{O}(n^2)}_{Compl(CM)} + \underbrace{\mathcal{O}(n^2)}_{Busqueda\ n\ filas\ x\ n\ columnas}$$

$$\therefore \text{Complejidad(Húngaro)} = \underbrace{\mathcal{O}(n^2)}_{Matching\ inicial} + (\underbrace{\mathcal{O}(n)}_{\#extensiones} * \underbrace{\mathcal{O}(n^3)}_{Compl(extension)}) = \mathcal{O}(n^4)$$

2.4. Teorema de Hall

Teorema: Sea G = (X ∪ Y, E) grafo bipartito ⇒ ∃ matching completo de X a Y ⇔ $|S| \leq |\Gamma(S)|\ \forall S \subseteq X$.

Prueba:
⇒) Si M es matching completo de X a Y entonces oberservemos que M induce una función inyectiva de X a Y.

$$f(x) = \text{único y : xy} \in E(M).$$

1. Si $S \subseteq X \Rightarrow |S| \leq |\Gamma(S)|$
2. Además por definición de f, $f(x) \in \Gamma(x)$

$$\begin{aligned} \text{Si x} \in S &\Rightarrow f(x) \in \Gamma(S) \\ &\Rightarrow f(S) \subseteq \Gamma(S) \\ &\therefore |f(S)| \leq |\Gamma(S)| \end{aligned}$$

De 1 y 2 $\Rightarrow |S| \leq |\Gamma(S)|$.

⇐) Supongamos que no es cierto, entonces G es bipartito con $|S| \leq |\Gamma(S)|\ \forall S \subseteq X$ pero no tiene matching completo de X a Y. Esto equivalente a ver que: si ∄ un matching completo de X a Y $\Rightarrow \exists\ S \subseteq X : |S| > |\Gamma(S)|$.

Corramos el algoritmo para hallar matching. Al finalizar habrá filas sin matcher (las de s).

Sean:

- S_0 = filas sin matchear.
- $T_1 = \Gamma(S_0)$, es decir, las columnas etiquetadas por las filas de S_0. Todas las columnas de T_1 están matcheadas, pues si no, se podría agregar alguna alguna fila de S_0 al matching.
- S_1 = filas etiquetadas por las columnas de T_1.
- $T_2 = \Gamma(S_1) - T_1$, es decir, columnas etiquetadas por las filas de S_1.

En general:

- S_i = filas matcheadas con T_i.
- $T_{i+1} = \Gamma(S_i) - (T_1 \cup T_2 \cup \ldots T_i)$.

Como el algoritmo para sin hayar matching, entonces $\forall i\ T_i \neq \emptyset$, produce un S_i (i.e $S_i \neq \emptyset$).
$\therefore$ La única forma de parar es en un k, tal que $T_{k+1} = \emptyset$.

Observaciones:

1. $|S_j| = |T_j|$, pues S_j son las filas matcheadas con T_j.
2. Por construcción, los S_i y T_i son todos distintos.
3. $\Gamma(S_0 \cup S_1 \cup \ldots S_j) = T_1 \cup T_2 \cup \ldots T_{j+1}$
   Por inducción en j:
   - Caso Base: $j = 0$ vale, ya que $T_1 = \Gamma(S_0)$
   - Caso Inductivo: Supongamos que vale para j, veamos para *j+1*.

$$\begin{aligned}
T_1 \cup T_2 \ldots T_{j+2} &= T_1 \cup T_2 \cup \ldots T_{j+1} \cup \underbrace{(\Gamma(S_{i+1}) - (T_1 \cup T_2 \ldots T_{j+1}))}_{T_{j+1}} \\
&= T_1 \cup T_2 \cup \ldots T_{j+1} \cup (\Gamma(S_{i+1}) \\
&= \Gamma(S_0 \cup S_1 \cup \ldots S_j) \cup \Gamma(S_{i+1}) \qquad \text{Por H.I} \\
&= \Gamma(S_0 \cup S_1 \cup \ldots S_j \cup S_{j+1})
\end{aligned}$$

Sea $S = S_0 \cup S_1 \cup \ldots S_k$

$$\begin{aligned}
|\Gamma(S)| &= |\Gamma(S_0 \cup S_1 \cup \ldots S_k)| \\
&= |T_1 \cup T_2 \cup \ldots \underbrace{T_{k+1}}_{=\emptyset}| && \text{Por Obs 3} \\
&= |T_1 \cup T_2 \cup \ldots T_k| \\
&= |T_1| + |T_2| + \ldots |T_k| && \text{Por Obs 2} \\
&= |S_1| + |S_2| + \ldots |S_k| && \text{Por Obs 1} \\
&= |S| - |S_0| && \text{Por Obs 2} \\
&< |S| && \text{Pues } S_0 \neq \emptyset
\end{aligned}$$

Absurdo!

2.5. Teorema del matrimonio

Teorema: Todo grafo regular bipartito tiene un matching perfecto.
Prueba: Sea $G = (X \cup Y, E)$ bipartito regular, tal que $\forall W \subseteq V(G)$, definimos:

$$\begin{aligned}
E_W &= \{xy \in E(G) : x \in W \ o\ y \in W\} \\
&= \text{lados con un extremo en W}
\end{aligned}$$

Supongamos que $W \subseteq X$ (de igual forma para $W \subseteq Y$). Además, como G es regular, $\exists\ \Delta > 0 : d(z) = \Delta\ \ \forall z$.

$$
\begin{aligned}
|E_w| &= |\{xy \in E : x \in W\}| \\
&= \sum_{x \in w} |\{y : xy \in E\}| \\
&= \sum_{x \in w} \underbrace{d(x)}_{\Delta} \\
&= \Delta * |w|
\end{aligned}
$$

Es decir, a cada w le corresponden Δ lados distintos. En particular:

$$
\begin{aligned}
|E_x| &= \Delta * |x| \\
|E_y| &= \Delta * |y|
\end{aligned}
$$

pero $E_x = E = E_y$ pues G es bipartito.

Por lo tanto:

$|E_x| = |E_y| \Rightarrow \Delta * |x| = \Delta * |y| \Rightarrow |x| = |y|$ $\therefore$ Todo matching completo es perfecto.
Basta ver que existe un matching completo de X a Y, es decir, que se cumple la condición de Hall.

Sea $S \subseteq X$:

$$
\text{Sea } \underbrace{xy}_{\substack{x \in X \\ y \in Y}} \in E_s \Rightarrow \exists \left\{ \begin{array}{c} x \in S \\ y \in \Gamma(x) \end{array} \right\} \Rightarrow y \in \Gamma(S) \Rightarrow xy \in E_{\Gamma(s)}
$$

Es decir, hemos probado que:

$$
\begin{aligned}
E_s &\subseteq E_{\Gamma(S)} \\
|E_S| &\leq |E_{\Gamma(S)}| \\
\Delta\,|S| &\leq \Delta\,|\Gamma(S)| \\
|S| &\leq \Gamma(S)
\end{aligned}
$$

2.6. Todo grafo bipartito es Δ coloreable

Teorema: Si G es bipartito $\Rightarrow \chi'(G) = \Delta$
Prueba:

Lema Interno: Todo grafo bipartito es subgrafo de un grafo bipartito regular con el mismo Δ, es decir:

$$
\text{G bipartito} \Rightarrow \exists \text{ H bipartito regular con G} \subseteq \text{H y } \Delta(G) = \Delta(H)
$$

Prueba: Sean:

- $G = (V = X \cup Y, E)$ grafo bipartito
- $G^\star = (V^\star, E^\star)$ una copia de G

- $E^\dagger = \{vv^\star : d_G < \Delta(G)\}$
- $\overline{G} = (\overline{V}, \overline{E})$ con:
  - $\overline{V} = V \cup V^\star$
  - $\overline{E} = E \cup E^\star \cup E^\dagger$

Propiedades de $\overline{G}$:

1. $\overline{G}$ es bipartito, sus partes son:
   - $X \cup Y^\star$
   - $X \cup Y$

   No existen lados entre $x \leftrightarrow x,\ y^\star \leftrightarrow y^\star,\ x \leftrightarrow y^\star$.

2. Sea v $\in$ V tal que $d_G(v) = \Delta = \Delta(G)$ entonces V no es parte de ningún lado de $E^\dagger$.
   $\Rightarrow d_{\overline{G}}(v) = d_{\overline{G}}(v^\star) = \Delta$

   Sea v $\in$ V tal que $d_G(v) < \Delta \Rightarrow$ forma parte de un nuevo lado.
   $\therefore d_{\overline{G}}(v) = d_{\overline{G}}(v^{\star)} = d_G(v) + 1$
   <u>Conclusión:</u> $\Delta(\overline{G}) = \Delta(G)\ y\ \delta(\overline{G}) = \delta(G) + 1$

   Repitiendo este proceso, $i.e\ G \to \overline{G} \to \overline{\overline{G}} \to \overline{\overline{\overline{G}}} \dots$ eventualmente llegaremos a un $G^\blacktriangle$ tal que $\delta(G^\blacktriangle) = \Delta\ \therefore$ regular.

Fin del Lema Interno

- Sea H bipartito regular con $G \subseteq H$ y $\Delta(G) = \Delta(H)$. Como H es bipartito regular $\Rightarrow \exists$ un matching perfecto en H, llamado M. Coloreemos todos los lados de M con `Color 1`.
- Sea $H_1 = H-$ los lados del matching M. Como M es matching perfecto, H_1 sigue siendo regular y $\Delta_{H_1}(x) = \Delta_H(x) - 1 = \Delta - 1$. Como H_1 es bipartito regular $\Rightarrow \exists$ un matching perfecto en H_1, llamado M_1. Coloreemos todos los lados de M_1 con `Color 2`.
- Sea $H_2 = H_1-$ los lados del matching M_1. Luego $\Delta_{H_2}(x) = \Delta_{H_1}(x) - 1 = \Delta - 2$.

  Siguiendo así $H_{\Delta-1}$ seguirá siendo regular con $\Delta_{H_{\Delta-1}}(x) = 1$. En total obtuvimos Δ matchings y Δ colores. $\therefore \chi'(H) = \Delta$

$$\Rightarrow \chi'(G) = \Delta \text{ pues } G \subseteq H.$$

2.7. Cota de Hamming

<u>**Teorema:**</u> Sea C un código de longitud n y sea $t = \lfloor \frac{\delta-1}{2} \rfloor$ la cantidad de errores que corrige, entonces:

$$|C| \leq \frac{2^n}{1 + n + \binom{n}{2} + \dots \binom{n}{t}}$$

<u>**Prueba:**</u> Sea $\boxed{A = \cup_{x\in C} B_t(x)}$

Como ya dijimos C corrigue t errores $\Rightarrow B_t(x) \cap B_t(y) \neq \emptyset\ \forall x, y \in C : x \neq y$.

$$\therefore \text{ La unión en A es disjunta y } \boxed{\#A = \sum_{x \in C} B_t(x)}$$

Sea $S_r(x) = \{y \in Z_2^n : d(x,y) = r\}$

$\therefore B_t(x) = \cup_{r=0}^{t} S_r(x)$ y la unión es disjunta $\Rightarrow \boxed{\#B_t(x) = \sum_{r=0}^{t} \#S_r(x)}$

¿Cuánto vale $S_r(x)$?

$$\begin{aligned} y \in S_r(x) & \Leftrightarrow d(x,y) = r \\ & \Leftrightarrow |x \oplus y| = r \text{ donde defino } (x \oplus y) = \epsilon \\ & \Leftarrow \exists \underbrace{\epsilon : |\epsilon| = r}_{\in S_r(0)} : y = x \oplus \epsilon \end{aligned}$$

$\therefore\ S_r(x) = x \oplus S_r(0) \Rightarrow \#S_r(x) = \#S_r(0)$

Luego

$$\begin{aligned} \#S_r(x) &= \#S_r(0) \\ &= \#\text{ vectores de longitud n con r unos} \\ &= \binom{n}{r} \end{aligned}$$

Por lo tanto

$$\begin{aligned} \#A &= \sum_{x \in C} \#B_t(x) \\ &= \sum_{x \in C} \sum_{r=0}^{t} \#S_r(x) \\ &= \sum_{x \in C} \sum_{r=0}^{t} \binom{n}{r} \\ &= \#C * \sum_{r=0}^{t} \binom{n}{r} \end{aligned}$$

Como $A \in Z_2^n \Rightarrow \#A \leq 2^n$, entonces:

$$\begin{aligned} & \sum_{r=0}^{t} \binom{n}{r} * \#C \leq 2^n \\ & \Rightarrow \#C \leq \frac{2^n}{\sum_{r=0}^{t} \binom{n}{r}} \end{aligned}$$

2.8. Teorema de la matriz de chequeo de códigos lineales

<u>Teorema:</u> Sea C un código lineal con matriz de chequeo H, entonces:

a) $\delta(C) = \text{mín}\,\{|x| : x \in C, x \neq 0\}$ (# columas LD de H).

b) Si H no tiene columnas 0, ni columnas repetidas, entonces $\delta \geq 3$ y corrigue al menos un error.

Prueba: Sean:

- w : mín # columnas LD de H.
- $e_i = 000\ldots \underbrace{1}_{i} 0\ldots 0$

a) $\boxed{w \geq \delta}$ *Sea* $v \in C, v \neq 0$ *y* $|v| = \delta \Rightarrow v$ tiene δ unos.

Es decir; $\exists j_1, j_2 \ldots j_\delta$ tal que:

$$v = e_{j_1} + e_{j_2} + \ldots e_{j_\delta}$$

Como $v \in C \Rightarrow v =$ NU(H) entonces $Hv^t = 0$.

$$\begin{aligned} \Rightarrow 0 = Hv^t &= H(e^t_{j_1} + e^t_{j_2} + \ldots e^t_{j_\delta}) \\ &= He^t_{j_1} + He^t_{j_2} + \ldots He^t_{j_\delta} \\ &= H^{j_1} + H^{j_2} + \ldots H^{j_\delta} \end{aligned}$$

$\therefore \{H^{j_1} + H^{j_2} + \ldots H^{j_\delta}\}$ es LD $\Rightarrow w \geq \delta$.

$\boxed{w \leq \delta}$ Sea ahora $\{H^{i_1} + H^{i_2} + \ldots H^{i_w}\}$ un conjunto LD, entonces $\exists$ constantes $c_w \in Z_2^n$ no todas nulas, tales que:

$$c_1 H^{i_1} + c_2 H^{i_2} + \ldots c_w H^{i_w} = 0$$

Sea $v = c_1 e_{i_1} + c_2 e_{i_2} + \ldots c_w e_{i_w},\ v \neq 0$ ya que dijimos que no todos los c_i eran nulos. Luego:

$$\begin{aligned} Hv^t &= H(c_1 e^t_{i_1} + c_2 e^t_{i_2} + \ldots c_w e^t_{i_w}) \\ &= Hc_1 e^t_{i_1} + Hc_2 e^t_{i_2} + \ldots Hc_w e^t_{i_w} \\ &= H^{e_{i_1}} + H^{e_{i_2}} + \ldots H^{e_{i_w}} \\ &= 0 \end{aligned}$$

$\Rightarrow v \in C$ *y* $|v| = w$. Como δ es la menor distancia, tenemos que $\delta \leq |v| = w$.

Por lo tanto vale $\boxed{w \leq \delta}$ y $\boxed{w \geq \delta} \Rightarrow \boxed{w = \delta}$.

b)

- Si H no tiene columnas ceros $\Rightarrow w \leq 2$.
- Si H no tiene columnas repetidas $\Rightarrow \nexists i, j : i \neq j$ y $H^i = H^j$. Como no puede pasar que $Hi = Hj$ tampoco $Hi + Hj = 0$, es decir, $Hi + Hj \neq 0 \forall i, j : i \neq j$ por lo que $\nexists$ conjuntos de columnas LD $\Rightarrow w \leq 3$.

  Luego $\delta \leq 3 \Rightarrow t = \lfloor \frac{\delta - 1}{2} \rfloor \leq 1$, es decir, C corrige al menos un error.

2.9. Teorema del polinomio generador de códigos cíclicos

Teorema: Sea C un código cíclico de dimensión k y longitud n y sea $g(x)$ su polinomio generador, entonces:

- C está formado por los múltiplos de $g(x)$ de grado menor a n.
- El grado de $g(x)$ es $n-k$.
- $g(x)$ divide a $1+x^n$

Prueba:
a) Sea $v(x) \in C$, dividamos v por g(x). Entonces $\exists$ q(x) y r(x) con $gr(r) < gr(g)$ tal que:

$$\begin{aligned} v(x) &= q(x)g(x) + r(x) \\ &\Rightarrow \boxed{q(x)g(x) = v(x) + r(x)} (1) \end{aligned}$$

.

Como $v \in C \Rightarrow gr(v) < n$ y $gr(r) \underbrace{<}_{g \in C} n$ con lo que concluimos que $\boxed{gr(v+r) < n}$ (2).

Luego de (1) y (2) deducimos: $\boxed{gr(q\ g) < n}$.

Recordemos que si $p \in C$ y $gr(p) < n$ entonces: $\boxed{p \mod (1+x^n) = p}$.

Por lo tanto $q(x)g(x) \mod (1+x^n) = q(x)g(x)$, es decir: $\boxed{q(x) \odot g(x) = q(x)g(x)}$ (A). Además como $g(x) \in C \Rightarrow \boxed{q(x) \odot g(x) \in C}$ (B).

De (A) y (B) resuta que $q(x)g(x) \in C \Rightarrow v(x) + r(x) \in C$. Además dijimos que $v(x) \in C$ y como C es lineal $\Rightarrow \boxed{r(x) \in C}$ (†). Llamemos $\boxed{gr(r) < gr(g)}$ ($\star$).

De (†) y ($\star$) deducimos $r = 0 \Rightarrow v(x) = q(x)g(x)$.

b) Recordemos que si $v(x) \in C \Rightarrow \exists \mu(x) : v(x) = \mu(x)g(x)$. Entonces para que $gr(\mu g) < n$ debe darse que $gr(\mu) + gr(g) < n$, es decir, $gr(\mu) < n - gr(g)$.

Sea

$$C = \{v(x) : \exists \mu(x), gr(\mu) < n - gr(g), v(x) = \mu(x)g(x)\}$$

Entonces existe una bitección entre C y el conjunto: $\{\mu(x) : gr(\mu) < n - gr(g)\}$.

$$\begin{aligned} \therefore\ |C| &= |\{\mu(x) : gr(\mu) < n - gr(g)\}| \\ 2^k &= 2^{n-gr(g)} \\ k &= n - gr(g) \\ gr(g) &= n - k \end{aligned}$$

c) Recordemos que si $g(x)$ es polinomio generador, la $ROT^k(g) = x^k \odot g(x)$. Como $g(x) \in C \Rightarrow ROT^k(g) \in C$. Además $x^k \odot g(x) = x^k g(x) \mod (1+x^n)$.
Sea $p(x)$ tal que:

$$\underbrace{x^k g(x)}_{gr=k+(n-k)} = \underbrace{p(x)(1+x^n)}_{gr=gr(p)+n} + \underbrace{x^k \odot g(x)}_{gr<n}$$

Luego para que la igualdad valga, debe valer que $gr(p) = 0$, es decir, $p = 1$. Entonces: $\boxed{x^k g(x) = (1 + x^n) + x^k \odot g(x)}$ (1), pero $x^k \odot g(x) \in C \Rightarrow \exists \mu(x) :$ $\boxed{x^k \odot g(x) = \mu(x) g(x)}$ (2)

De (1) y (2) :

$$\begin{aligned} x^k g(x) &= (1 + x^n) + \mu(x) g(x) \\ 1 + x^n &= x^k g(x) + \mu(x) g(x) \\ &= (x^k + \mu(x)) g(x) \\ &\therefore \; g | 1 + x^n \end{aligned}$$

Capítulo 3

Parte C

3.1. 4-COLOR $\leq_p$ SAT

Sea G un grafo con vértices $v_1, v_2, \ldots v_n$, queremos construir (en tiempo polinomial) una expresión booleana B en CNF (*forma conjuntiva normal*), tal que:

$$\chi(G) \leq 4 \Leftrightarrow B\ es\ satisfacible$$

Sea n = #vértices de G, y sean las variables $x_{i,j}$ con $i = 1, 2, \ldots n$ y $j = 1, 2, 3, 4$
Sean

$$\begin{aligned} A_i &= x_{i,1} \vee x_{i,2} \vee x_{i,3} \vee x_{i,4} \\ A &= A_1 \wedge A_2 \wedge \ldots A_n \end{aligned}$$

Defino

$$Q_{i,j,k,l} = \overline{x_{i,j}} \vee \overline{x_{k,l}} \qquad i,k = 1 \ldots n \qquad j,l = 1,2,3,4 \tag{1}$$

$$D_i = Q_{i,i,1,2} \wedge Q_{i,i,1,3} \wedge Q_{i,i,1,4} \wedge Q_{i,i,2,3} \wedge Q_{i,i,2,4} \wedge Q_{i,i,3,4} \tag{2}$$

$$D = D_1 \wedge D_2 \ldots \wedge D_n \tag{3}$$

$$F_{i,k} = Q_{i,k,1,1} \wedge Q_{i,k,2,2} \wedge Q_{i,k,3,3} \wedge Q_{i,k,4,4} \tag{4}$$

$$F = \wedge_{\substack{i,k \\ v_i v_k \in E(G)}} F_{i,k} \tag{5}$$

$\boxed{\Rightarrow}$

Sea C un coloreo propio de G, con a lo sumo 4 colores. Debemos dar un asignamiento de valores a las variables $x_{i,j}$ que satisfagan B, es decir, un elemento $\overrightarrow{b} \in \mathbb{Z}_2^{4n}$ tal que $B(\overrightarrow{b}) = 1$.

Definimos

$$b_{i,j} \begin{cases} 1 \text{ si } C(v_i) = j \\ 0\ c.c \end{cases}$$

Debemos probar $B(\overrightarrow{b}) = 1$, es decir, (1) $A(\overrightarrow{b}) = 1$, (2) $D(\overrightarrow{b}) = 1$ y (3) $F(\overrightarrow{b}) = 1$.

(1) $\boxed{A(\overrightarrow{b}) = 1}$

Debemos ver que $A_i(\overrightarrow{b}) = 1 \; \forall i$, es decir, hay que probar:

$$b_{i,1} \vee b_{i,2} \vee b_{i,3} \vee b_{i,4} = 1$$

pero

$$C(v_i) \in \{1,2,3,4\} \Rightarrow \exists j \in \{1,2,3,4\} \text{ tal que } C(v_i) = j \Rightarrow b_{i,j} = 1$$

(2) $\boxed{D(\overrightarrow{b}) = 1}$

Debemos ver que $D_i(\overrightarrow{b}) = 1 \; \forall i$, es decir,

$$Q_{i,j,j,l}(\overrightarrow{b}) = 1 \; \forall i, j, l, j < l$$

es decir:

$$\overline{b_{i,j}} \vee \overline{b_{i,l}} = 1 \; \forall i, j, l, j < l$$

por el absurdo, supongamos que no:

$$\begin{aligned}
&\Rightarrow \; \exists i, j, l, j < l \; : \; \overline{b_{i,j}} \vee \overline{b_{i,l}} = 0 \\
&\Rightarrow \; \overline{b_{i,j}} = \overline{b_{i,l}} = 0 \\
&\Rightarrow \; b_{i,j} = b_{i,l} = 1 \\
&\Rightarrow \; C(v_i) = j, \; C(v_i) = l, \; pero \; j \neq l \text{ Absurdo!}
\end{aligned}$$

Luego, el absurdo vino de suponer que $\overline{b_{i,j}} \vee \overline{b_{i,l}} = 0$

$\therefore \overline{b_{i,j}} \vee \overline{b_{i,l}} = 1$

(3) $\boxed{F(\overrightarrow{b}) = 1}$

Por el absurdo, supongamos que no:

$$\begin{aligned}
&\Rightarrow \; \exists i, k \; : \; v_i v_k \in E(G) \text{ tal que } F_{i,k}(\overrightarrow{b}) = 0 \\
&\Rightarrow \; \exists j \; \in \{1,2,3,4\} : Q_{i,k,j,j}(\overrightarrow{b}) = 0 \\
&\Rightarrow \; \overline{b_{i,j}} \vee \overline{b_{k,j}} = 0 \\
&\Rightarrow \; \overline{b_{i,j}} = \overline{b_{k,j}} = 0 \\
&\Rightarrow \; b_{i,j} = b_{k,j} = 1 \\
&\Rightarrow \; C(v_i) = 1 \; y \; C(v_k) = 1 \\
&\Rightarrow \; C(v_i) = C(v_k) \; (= j) \text{ Absurdo!}
\end{aligned}$$

Pues, el coloreo C es propio y $v_i v_k \in E(G)$. El absurdo vino de suponer que $F(\overrightarrow{b}) = 0$

$\therefore F(\overrightarrow{b}) = 1$

$\boxed{\Leftarrow}$

Ahora sabemos que existe un $\overrightarrow{b}$ con $B(\overrightarrow{b}) = 1$ y debemos construir un coloreo propio, con al menos 4 colores.

$$B(\overrightarrow{b}) = 1 \Rightarrow \begin{cases} A(\overrightarrow{b}) = 1 \Rightarrow A_i(\overrightarrow{b}) = 1 \; \forall i \Rightarrow (1) \; \forall i \; \exists j : b_{i,j} = 1 \\ D(\overrightarrow{b}) = 1 \Rightarrow D_i(\overrightarrow{b}) = 1 \; \forall i \Rightarrow (2) \; \forall i \; \nexists j \neq l : b_{i,j} = 1 = b_{i,l} \\ F(\overrightarrow{b}) = 1 \Rightarrow \forall i, j \in E(G), C(v_i) \neq C(v_j) \Rightarrow \text{C es propio} \end{cases}$$

De (1) y (2) $\Rightarrow \boxed{\forall i \; \exists! j : b_{i,j} = 1}$

Luego, definimos:

$$C(v_i) = \text{unico j con } b_{i,j} = 1$$

3.2. 3-SAT es NP-Completo

3.3. 3-COLOR es NP-Completo

Bibliografía

[1] MAXIMILIANO ILLBELE, «Resumen de Discreta II, 16 de agosto de 2012», *FaMAF, UNC*.