

Matroides Asociadas a Redes

Christian Nolasco Serna

Universidad Nacional de Colombia
Facultad De Ciencias
Departamento De Matemáticas
Bogotá D.C.
Año 2013

Matroides Asociadas a Redes

Christian Nolasco Serna

Trabajo final presentado como requisito parcial para optar al título de:
Magister en Ciencias Matemáticas

Director:
Humberto Sarria Zapata

Universidad Nacional de Colombia
Facultad De Ciencias
Departamento De Matemáticas
Bogotá D.C.
Año 2013

TÍTULO: Matroides Asociadas a Redes.

TITLE: Matroids Associated to Networks.

RESUMEN: En este trabajo, se estudian las relaciones entre la Teoría de matroides y la Teoría de codificación de redes. Se define el matroide red sobre la estructura de los caminos independientes de un digrafo, el cual resulta ser representable [3]. Se establece la igualdad entre el matroide red y el matroide inducido por los códigos genéricos ([3] y [5]). Se establece la relación entre las redes matroidales y los códigos lineales escalares ([4]).

ABSTRACT: In this paper we study the relations between Matroid theory and Network Coding Theory. Through the structure of edge-disjoint paths, a single-source network is associated with a network matroid, which turns out to be representable([3]). A linear network code on an acyclic network assigns a coding vector to every edge. The linear independence among coding vectors naturally induces a matroid. It is shown that the induced matroid is the network matroid if the linear network code is generic([3] and [5]). We study matroidal networks and the relationship with scalar-lineary codes.

PALABRAS CLAVE: Matroide red, red matroidal, códigos lineales escalares, códigos genéricos.

KEY WORDS: Network matroid, matroidal networks, generic code, scalar-linear code.

DIRECTOR: Profesor Ph D. Humberto Sarria Zapata

Contenido

1. Introducción	3
2. Preliminares	5
2.1. Redes Lineales	5
2.2. Matroides	8
3. Redes Matroidales y Soluciones Lineales Escalares	15
3.1. Códigos de red globales	15
3.2. Redes escalares solubles	18
4. Códigos lineales y redes genéricas	21
4.1. El matroide red	21
4.2. Códigos lineales y redes genéricas	26
4.3. La representación matricial del matroide red	34
5. Conclusiones	40
6. Bibliografía	42

,

1 Introducción

La Teoría de Codificación de Redes [6] estudia las diferentes formas algebraicas en que se puede representar la información con el fin de que sea transmitida de manera eficiente a través de una red. La Teoría de Matroides es una rama de las matemáticas, fundada en 1935 por Whitney [1], que generaliza la noción de independencia presente en el Álgebra Lineal, la Teoría de Grafos y otras ramas de la Matemática. Con el estudio de las relaciones de dependencia en la Teoría de redes, se ha encontrado un método para conseguir redes desde matroides [7], mostrándose algunas conexiones entre estos conceptos.

Este trabajo tiene como objetivo estudiar algunas relaciones entre la Teoría de Codificación de Redes de Información y la Teoría de Matroides. En particular se estudian los diferentes tipos de matroides que se pueden definir a partir de una red fija y las relaciones entre éstos. También se establece la relación entre los códigos lineales escalares y el matroide red. Se estudian las redes matroidales y los códigos lineales escalares. Estos temas están basados en [3], [4] y [5].

El trabajo está organizado de la siguiente manera: en el capítulo 2, se presentan los preliminares de la Teoría de Redes y de la Teoría de Matroides. En esta parte se destaca el concepto de código de red, el cual permite definir el concepto de red soluble. Además, se introducen los matroides vectoriales, transversales y duales.

En el capítulo 3, se establece la primera relación entre matroides y redes, con el fin de estudiar la solubilidad de redes lineales escalares. En primer lugar, se definen los códigos globales con el objetivo de mostrar su equivalencia con los códigos lineales. Luego, al definir la red matroidal, se establece el siguiente teorema [4]:

“Una red tiene una solución lineal escalar, si y sólo si, la red es matroidal con matroide representable sobre un cuerpo finito.”

Para la demostración del anterior resultado, se construye un código global que corresponde a la solución lineal buscada.

En el último capítulo, se construye el matroide red a partir de la estructura de los caminos independientes de la red [3]. Este matroide tiene como soporte las aristas de la red y resulta ser un matroide representable. Utilizando la noción de independencia lineal de los vectores de arista, asignados a un digrafo acíclico, se introducen los códigos de red genéricos con la finalidad de mostrar que el matroide inducido es isomorfo al matroide red [3].

2 Preliminares

En este capítulo, se exponen las ideas básicas de la Teoría de Codificación de Redes y la Teoría de Matroides necesarias para el desarrollo del trabajo. Se supone que se trabaja con redes de información cuyo grafo es dirigido y con un conjunto finito de mensajes.

2.1. Redes Lineales

Definición 2.1.1 1. Un **grafo dirigido** o **digrafo** es un par ordenado $G = (V, E)$, donde V es un conjunto finito no vacío y $E \subseteq V \times V$.

2. Los elementos del conjunto V se llaman los **nodos** del digrafo y los elementos de E las **aristas** del digrafo. Si $(u, v) \in E$, se utiliza la notación uv para las aristas del digrafo.

3. Sea $e = uv \in E$, se dice que u es la **cola** de e y v es la **cabeza** de e . En adelante, se utiliza la notación $u = \pi_1(e)$ y $v = \pi_2(e)$.

4. Un **Camino** P sobre un digrafo G , es un conjunto $\{v_0v_1, \dots, v_{k-1}v_k\} \subseteq E$, tal que $v_{i-1} \neq v_i$, para $i = 1, \dots, k$. También, se nota el camino P como $v_0e_1e_2, \dots, e_kv_k$, donde $e_i = v_{i-1}v_i$, $i = 1, \dots, k$.

5. Un **ciclo** sobre un digrafo G , es un camino $v_0e_1e_2, \dots, e_kv_k$, donde v_1, \dots, v_{k-1} son nodos distintos y $v_0 = v_k$.

6. Se dice que un digrafo G es **cíclico**, si posee un ciclo. En otro caso, se dice que G es **acíclico**.

7. Para cada $u \in V$ se definen:

$$\Gamma_I(u) := \{e \in E : \pi_2(e) = u\}$$

$$\Gamma_O(u) := \{e \in E : \pi_1(e) = u\}$$

Definición 2.1.2 1. Sea $G = (V, E)$ un digrafo. Una **red** sobre G , es una quintupla $N_G = (G, \mu, \mathcal{A}, S, R)$, donde :

- (i) μ es un conjunto no vacío que se llama el conjunto de mensajes.
- (ii) \mathcal{A} es un alfabeto de por lo menos dos elementos.
- (iii) $S : V \rightarrow 2^\mu$ es la función fuente.
- (iv) $R : V \rightarrow 2^\mu$ es la función de la demanda.

2. Un nodo $v \in V$, es un **nodo fuente**, si $S(v) \neq \emptyset$. El conjunto de los nodos fuente se nota por S_μ .

3. Un nodo $v \in V$, es un **nodo receptor**, si $R(v) \neq \emptyset$. El conjunto de los nodos receptores se nota por R_μ .

Notación: Las redes se notan por N_G .

A continuación se formaliza la acción sobre una red, mediante funciones que se asocian a cada arista.

Definición 2.1.3 1. Sean, N_G una red, k, n números enteros positivos y F un cuerpo, tal que $|F| > |\mathcal{A}|$. Un **código de red** (k, n) sobre N_G , es un conjunto de funciones f_{uv} y $f_{t,m}$ definidas como:

- (i) $f_{uv} : (F^k)^{\alpha(u)} \rightarrow F^n$, para $uv \in E$, $u \in S_\mu$.
- (ii) $f_{uv} : (F^n)^{\beta(u)} \rightarrow F^n$, para $uv \in E$, $u \notin S_\mu$.
- (iii) $f_{t,m} : (F^n)^{\beta(t)} \rightarrow F^k$, para todo $t \in R_\mu$ y $m \in R(t)$.

2. Los números $\alpha(u)$, $\beta(u)$ y $\gamma(u)$ se definen como:

- (i) $\alpha(u) := |S(u)|$, $u \in S_\mu$.
- (ii) $\beta(u) := |\Gamma_I(u)|$, $u \notin S_\mu$.
- (iii) $\gamma(u) := |R(u)|$, $u \in R_\mu$.

3. Los números k y n reciben el nombre de la **dimensión de la fuente y la arista**,

respectivamente.

4. Si las funciones f_{uv} y f_t son lineales, se dice que el código de red (k, n) es **lineal** y se nota $LN_G(k, n)$. Si $k = n = 1$, se dice que el código de red (k, n) es **lineal escalar**.

Notación: En adelante, los códigos de red (k, n) sobre la red N_G se notan por $NC_G(k, n)$.

Ejemplo 2.1.4 Considere el digrafo de la figura 1. Se define sobre este digrafo, una red N_G y un código de red LN_G , de la siguiente forma:

$$F = Z_2, k = n = 1$$

$$S(1) = \{0, 1\}, R(6) = R(7) = \{0, 1\}$$

$$f_{e_1}(x, y) = f_{e_3}(x) = f_{e_4}(x) = f_{e_8}(x) = f_{e_9}(x) = x$$

$$f_{e_2}(x, y) = y$$

$$f_{e_6}(x, y) = x + y$$

$$f_6(x, y) = (x, x + y), f_7(x, y) = (x + y, y)$$

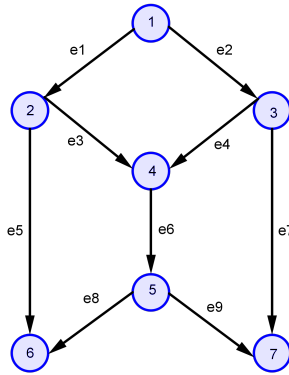


Figura 1

Definición 2.1.5 1. Sea $NC_G(k, n)$ un código de red sobre N_G . Una **función de símbolo**, es una función $a : \mu \rightarrow F^k$.

2. Un **símbolo de arista**, es cualquier valor de una función $\chi : E \rightarrow F^n$, definido recursivamente como:

- (i) $\chi(uv) = f_{uv}(a(m_1), \dots, a(m_{\alpha(u)}))$, donde $u \in S_\mu$ y $S(u) = \{m_1, \dots, m_{\alpha(u)}\}$.
(ii) $\chi(uv) = f_{uv}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(u)}))$, $u \notin S_\mu$ y $e_{\alpha+1}, \dots, e_{\alpha+\beta(u)} \in \Gamma_I(u)$.

Observación: El símbolo de arista $\chi(uv)$ de la anterior definición depende de la asignación sobre los mensajes.

Definición 2.1.6 Sea N_G una red. Un código de red $NC_G(k, n)$ es una **solución** para N_G , si para cada función de símbolo $a : \mu \rightarrow F^k$ y su correspondiente símbolo de arista $\chi : E \rightarrow F^n$, se tiene:

$$f_{t,m}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(t)})) = a(m),$$

para todo $t \in R_\mu$ y $m \in R(t)$.

Notación: $\mu = \{m_1, \dots, m_{|\mu|}\}$.

El código de red del ejemplo 2.1.4, es una solución para la red definida en el mismo ejemplo.

2.2. Matroides

La Teoría de Matroides es el estudio abstracto del concepto de dependencia. En la sección se introducen ejemplos de matroides y se estudia el concepto de dualidad.

Definición 2.2.1 1. Un **matroide** \mathcal{M} es un par ordenado (S, \mathcal{I}) , que consiste de un conjunto S y una colección \mathcal{I} de subconjuntos de S , tal que:

(M1) $\emptyset \in \mathcal{I}$.

(M2) Si $I \in \mathcal{I}$ e $I' \subseteq I$, entonces $I' \in \mathcal{I}$.

(M3) Si I_1 e I_2 pertenecen a \mathcal{I} , y $|I_1| < |I_2|$, entonces existe un elemento $x \in I_2 - I_1$, tal que $I_1 \cup \{x\} \in \mathcal{I}$.

2. El conjunto S se llama el **soporte** del matroide \mathcal{M} .

3. Un subconjunto X de S es un **conjunto independiente**, si $X \in \mathcal{I}$. En caso contrario, se dice que X es un **conjunto dependiente**.
4. Una **base** \mathcal{B} para un matroide \mathcal{M} es un conjunto maximal independiente.
5. Un **circuito** \mathcal{C} para un matroide \mathcal{M} es un conjunto minimal dependiente.
6. El **rango** de \mathcal{M} es una función $r_{\mathcal{M}} : 2^S \rightarrow Z^+$, tal que para todo $X \subseteq S$, $r_{\mathcal{M}}(X)$ es la cardinalidad máxima de un conjunto independiente contenido en X .
7. Dos matroides $\mathcal{M}_1 = (S_1, \mathcal{I}_1)$ y $\mathcal{M}_2 = (S_2, \mathcal{I}_2)$ son **isomorfos**, si existe una biyección $\Psi : S_1 \rightarrow S_2$, tal que para todo $X \subseteq S_1$, $X \in \mathcal{I}_1$,si y sólo si, $\Psi(X) \in \mathcal{I}_2$.

La siguiente definición introduce el primer ejemplo de matroide, el cual fué la motivación de Whitney para comenzar a estudiar el tema.

Definición 2.2.2 1. Sea A una matriz de tamaño $n \times m$ sobre un cuerpo F . Un **matroide vectorial** asociado con A , es un par $\mathcal{M}(A) = (S_A, \mathcal{I}_A)$ tal que:

- (i) $S_A = \{1, \dots, m\}$ está en correspondencia biunívoca con las columnas de A .
- (ii) $\mathcal{I}_A = \{X \subseteq S_A : \text{Las columnas de la matriz } A \text{ correspondientes a los elementos de } X \text{ son vectores independientes en } F^n\}$.

2. Un matroide \mathcal{M} es F -**representable**, si existe una matriz A definida sobre F , tal que $\mathcal{M}(A)$ es isomorfo a \mathcal{M} .

Ejemplo 2.2.3 Sea A la matriz,

$$\begin{array}{ccccc} a_1 & a_2 & a_3 & a_4 & a_5 \\ \left[\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{array} \right] \end{array}$$

definida sobre el cuerpo Z_2 . Entonces, $S_A = \{a_1, a_2, a_3, a_4, a_5\}$ e $\mathcal{I}_A = \{\emptyset, \{a_1\}, \{a_2\}, \{a_4\}, \{a_5\}, \{a_1, a_2\}, \{a_1, a_5\}, \{a_2, a_4\}, \{a_2, a_5\}, \{a_4, a_5\}\}$. Los dependientes de este matroide son: $\{\{a_3\}, \{a_1, a_3\}, \{a_1, a_4\}, \{a_2, a_3\}, \{a_3, a_4\}, \{a_3, a_5\}\} \cup \{X \subseteq S_A : 3 \leq |X|\}$.

La siguiente definición introduce otro ejemplo de un matroide. Éstos van a jugar un papel importante en la representación del matroide red.

Definición 2.2.4 1. Sea S un conjunto finito. Una familia $\{A_i | i = 1, \dots, n\}$ es una **sucesión** sobre S , si para cada $i \in \{1, 2, \dots, n\}$, $A_i \subseteq S$. En adelante, se nota las sucesiones como $(A_j : j \in J)$.

2. Un subconjunto $T \subseteq S$ es un **transversal** de la sucesión $(A_j : j \in J)$, si existe una biyección $\Psi : J \rightarrow T$, tal que $\Psi(j) \in A_j$, para todo $j \in J$.

3. Un subconjunto $X \subseteq S$ es un **transversal parcial** de la sucesión $(A_j : j \in J)$, si existe $K \subseteq J$, tal que X es un transversal de la sucesión $(A_j : j \in K)$.

4. Sea $\mathcal{A} = (A_j : j \in J)$ una sucesión de subconjuntos del conjunto finito S . El grafo $\Delta[\mathcal{A}] = (V, E)$, definido como:

$$(i) V = S \cup J.$$

$$(ii) E = \{xj : x \in S, j \in J, \text{ y } x \in A_j\},$$

es el **grafo bipartito** asociado con \mathcal{A}

5. Una **correspondencia** en el grafo bipartito $\Delta[\mathcal{A}]$, es un conjunto de aristas $\{e_1, \dots, e_n\}$, donde cualquiera de ellas no compartan sus puntos extremos.

Ejemplo 2.2.5 Sean, $S = \{x_1, x_2, \dots, x_6\}$, $A_1 = \{x_1, x_2, x_6\}$, $A_2 = \{x_3, x_4, x_5, x_6\}$, $A_3 = \{x_2, x_3\}$ y $A_4 = \{x_2, x_4, x_6\}$. Entonces, para $\mathcal{A} = (A_1, A_2, A_3, A_4)$, el grafo bipartito $\Delta[\mathcal{A}]$ es el siguiente:

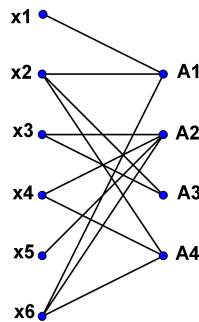


Figura 2

El conjunto $\{x_1, x_2, x_3, x_4\}$ es un transversal parcial de \mathcal{A} , ya que $\{x_11, x_42, x_33, x_24\}$ es una correspondencia en $\Delta[\mathcal{A}]$. Análogamente, $\{x_61, x_23, x_42, \}$ es una correspondencia

en $\Delta[\mathcal{A}]$, ya que $\{x_6, x_2, x_4\}$ es un transversal parcial de \mathcal{A} .

La siguiente proposición establece una relación entre el grafo bipartito $\Delta[\mathcal{A}]$ y los transversales parciales de $\mathcal{A} = (A_j : j \in J)$.

Proposición 2.2.6 Un subconjunto $X \subseteq S$ es un transversal parcial de la sucesión $\mathcal{A} = (A_j : j \in J)$, si y sólo si, existe una correspondencia $\{e_1, \dots, e_m\}$ en el grafo bipartito $\Delta[\mathcal{A}]$, donde $\pi_1(e_i) \in X$, para todo $i \in \{1, \dots, m\}$.

Demostración. \Rightarrow) : Sea X un transversal parcial de la sucesión $\mathcal{A} = (A_j : j \in J)$. Entonces, existen $K \subseteq J$ y una biyección $\Psi : K \rightarrow X$ tal que, $\Psi(k) \in A_k$, para todo $k \in K$. En adelante, se nota $\Psi(k)$ como x_k . Sea $\{x_k k | k \in K\}$ un conjunto de aristas en el grafo bipartito $\Delta[\mathcal{A}]$, estas establecen una correspondencia, ya que $x_{k_i} \neq x_{k_j}$, siempre y cuando $k_i \neq k_j$.

\Leftarrow) : Sea $\{e_1, \dots, e_n\}$ una correspondencia en el grafo bipartito $\Delta[\mathcal{A}]$, donde $\pi_1(e_i) \in X$, para todo $i \in \{1, \dots, n\}$. Sean, $K = \{\pi_2(e_1), \dots, \pi_2(e_n)\} \subseteq J$ y $\Psi : K \rightarrow X$, con $\Psi(\pi_2(e_i)) = \pi_1(e_i)$. La función Ψ es una biyección, ya que por la definición de correspondencia, $\pi_1(e_i) \neq \pi_1(e_j)$ y $\pi_2(e_i) \neq \pi_2(e_j)$, donde $i, j \in \{1, 2, \dots, n\}$. Entonces, se tiene que X es un transversal parcial de la sucesión $\mathcal{A} = (A_j : j \in J)$.

Teorema 2.2.7[1] Sean, S un conjunto finito, $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ una familia de subconjuntos de S e \mathcal{I} el conjunto de los transversales parciales de \mathcal{A} . Entonces, $\mathcal{M} = (S, \mathcal{I})$ es un matroide, el cual recibe el nombre del **matroide transversal**.

Demostración. El conjunto \emptyset es un transversal parcial de \mathcal{A} al tomar $K = \emptyset$, de aquí (M1) se satisface. Si I es un transversal parcial de \mathcal{A} e $I' \subseteq I$, entonces I' es también un transversal parcial de \mathcal{A} , en consecuencia (M2) se satisface. Supongamos que existen transversales parciales I_1 e I_2 de \mathcal{A} , tales que $|I_1| < |I_2|$. Entonces, existen correspondencias W_1 y W_2 en el grafo bipartito $\Delta[\mathcal{A}]$. Se pintan las aristas de $W_1 - W_2$, $W_2 - W_1$ y $W_1 \cap W_2$ de rojo, azul y púrpura respectivamente. Sea W el subgrafo de $\Delta[\mathcal{A}]$ inducido por las aristas que son rojas o azules. Ya que $|I_1| = |W_1|$ y $|I_2| = |W_2|$, existen más aristas azules que rojas en W . Cada ciclo en W tiene longitud par, por lo tanto tiene el mismo número de aristas rojas que azules. Como W tiene más aristas azules que rojas, debe existir una componente, en un camino impar P , cuya primera y última arista sean azules. Organizando los vértices del camino, se tiene que $P = \{v_1, \dots, v_{2k}\}$, sin pérdida de generalidad, $v_1 \in S$. Entonces, v_1 pertenece a una arista azul que no es

roja, así $v_1 \in I_2 - I_1$. Además, $\{v_2, \dots, v_{2k}\} \subseteq J$ y $\{v_3, \dots, v_{2k-1}\} \subseteq I_1 \cap I_2$. Intercambiando los colores sobre P dejando el resto igual en $\Delta[\mathcal{A}]$, existe una arista roja más que antes. De esta manera, $I_1 \cup v_1$ forman un transversal parcial de \mathcal{A} . En consecuencia, (M3) se satisface.

El matroide generado a partir de los transversales parciales de \mathcal{A} se nota por $M[\mathcal{A}]$. Si \mathcal{M} es un matroide cualquiera, $\mathcal{M} \cong M[\mathcal{A}]$, para alguna familia \mathcal{A} de conjuntos, entonces M se llama el **matroide transversal** y \mathcal{A} es la representación de \mathcal{M} .

En lo que sigue, se introduce el concepto de dualidad en el contexto de la Teoría de matroides.

Lema 2.2.8[1] Si B_1 y B_2 son bases de un matroide $\mathcal{M} = (S, \mathcal{I})$, entonces $|B_1| = |B_2|$.

Demostración. Supongase que $|B_1| < |B_2|$. Entonces, como B_1 y B_2 son conjuntos independientes en \mathcal{M} , por (M3), existe un elemento e de $B_2 - B_1$, tal que $B_1 \cup e \in \mathcal{I}$. Lo anterior contradice la maximalidad de B_1 . Por lo tanto $|B_1| \geq |B_2|$. Similarmente $|B_2| \geq |B_1|$.

Notación: En adelante, \mathcal{B} nota el conjunto de las bases del matroide $\mathcal{M} = (S, \mathcal{I})$.

Como una consecuencia directa de la propiedad (M1), se tiene que: (B1) \mathcal{B} es no vacío.

Lema 2.2.9[1] El conjunto \mathcal{B} satisface la siguiente condición: (B2) Si B_1 y B_2 son miembros de \mathcal{B} y $x \in B_1 - B_2$, entonces existe un elemento $y \in B_2 - B_1$, tal que $(B_1 - x) \cup y \in \mathcal{B}$.

Demostración. Los conjuntos $B_1 - x$ y B_2 son conjuntos independientes. Además, $|B_1 - x| < |B_2|$. Por la propiedad (M3), existe un elemento de y de $B_2 - (B_1 - x)$, tal que $(B_1 - x) \cup y \in \mathcal{I}$. Por lo tanto, $y \in B_2 - B_1$. Como $(B_1 - x) \cup y$ es un conjunto independiente, esta contenido en un conjunto maximal B'_1 . Además, $|B_1| = |(B_1 - x) \cup y|$. Entonces, $(B_1 - x) \cup y = B'_1$

Teorema 2.2.10[1] Sea S un conjunto y \mathcal{B} el conjunto de subconjuntos de S que

satisfacen las condiciones (B1) y (B2). La colección \mathcal{I} de los subconjuntos de S que están contenidos en algún elemento de \mathcal{B} , forman los independientes de un matroide sobre S .

Demostración. Como \mathcal{B} satisface la condición (B1), entonces $\emptyset \in \mathcal{I}$. Así, se tiene (M1). Sea $I \in \mathcal{I}$, entonces existe un conjunto $B \in \mathcal{B}$, tal que $I \subseteq B$. Por lo tanto, si $I' \subseteq I$, entonces $I' \subseteq B$. En consecuencia se tiene (M2). Se supone que existen conjuntos I_1 e I_2 en \mathcal{I} , donde $|I_1| < |I_2|$, tales que para todo $e \in I_2 - I_1$, $I_1 \cup e \notin \mathcal{I}$. Por definición existen B_1 y $B_2 \in \mathcal{B}$, donde $I_1 \subseteq B_1$ y $I_2 \subseteq B_2$. Además, se asume que el conjunto B_2 cumple con la condición de minimalidad para $|B_2 - (I_2 \cup B_1)|$. Por las elecciones de I_1 e I_2 , $I_2 - B_1 = I_2 - I_1$ (1). Ahora se supone que $B_2 - (I_2 \cup B_1)$ es no vacío. Entonces es posible elegir un elemento x en el conjunto y un elemento y en $B_1 - B_2$, tal que por (B2), $(B_2 - x) \cup y \in \mathcal{B}$. Como $|B_2 - (I_2 \cup B_1)| < |B_2 - (I_2 \cup B_1)|$, entonces se contradice la elección de B_2 . El conjunto $B_2 - (I_2 \cup B_1)$ es vacío y $B_2 - B_1 = I_2 - B_1$. Por el numeral (1), $B_2 - B_1 = I_2 - I_1$. (2). Ahora se supone que $B_1 - (I_1 \cup B_2)$ es no vacío. Entonces es posible elegir un elemento x en el conjunto y un elemento y en $B_2 - B_1$, tal que por (B2), $(B_1 - x) \cup y \in \mathcal{B}$. Ahora $I_1 \cup y \subseteq (B_1 - x) \cup y$, entonces $I_1 \cup y \in \mathcal{I}$. Como $y \in B_2 - B_1$, se tiene por el numeral (2), que $y \in I_2 - I_1$, lo cual contradice la hipótesis inicial. El conjunto $B_1 - (I_1 \cup B_2)$ es vacío y $B_1 - B_2 = I_1 - B_2$. Como el último conjunto está contenido en $I_1 - I_2$, se sigue que $B_1 - B_2 \subseteq I_1 - I_2$ (3). Ya que $|B_1| = |B_2|$, $|B_1 - B_2| = |B_2 - B_1|$. Por los numerales (2) y (3), $|I_1 - I_2| \geq |I_2 - I_1|$, entonces $|I_1| \geq |I_2|$. Lo anterior genera una contradicción con la hipótesis inicial. En consecuencia se cumple (M3).

Lema 2.2.11.[1] El conjunto \mathcal{B} de las bases de un matroide $\mathcal{M} = (S, \mathcal{I})$ satisface la siguiente condición: (B3) Si B_1 y B_2 son miembros de \mathcal{B} y $x \in B_2 - B_1$, entonces existe un elemento y de $B_1 - B_2$, tal que $(B_1 - y) \cup x \in \mathcal{B}$.

Demostración. El conjunto $B_1 \cup x$ contiene un único circuito, $\mathcal{C}(x, B_1)$. Como $\mathcal{C}(x, B_1)$ es dependiente y B_2 es independiente, $\mathcal{C}(x, B_1) - B_2$ es no vacío. Sea y un elemento en este conjunto, donde $y \in B_1 - B_2$. El conjunto $(B_1 - y) \cup x$ no contiene a $\mathcal{C}(x, B_1)$, por lo tanto, es un conjunto independiente. Finalmente, $(B_1 - y) \cup x$ tiene los mismos elementos de B_1 .

El siguiente teorema permite caracterizar el dual de un matroide.

Teorema 2.2.12[1] Sea $\mathcal{M} = (S, \mathcal{I})$ un matroide y $\mathcal{B}^* = \{S - B : B \in \mathcal{B}\}$. Entonces, \mathcal{B}^* es el conjunto de bases de un matroide sobre S .

Demostración. Como \mathcal{B} es no vacío, entonces B^* no lo es. Así, (B1) se satisface. Se supone que B_1^* y B_2^* son miembros de B^* y $x \in B_1^* - B_2^*$. Sean, $B_1 = S - B_1^*$ y $B_2 = S - B_2^*$, entonces $B_1^* - B_2^* = B_2 - B_1$. Por la propiedad (B3), como $x \in B_2 - B_1$, entonces existe un elemento y de $B_1 - B_2$, tal que $(B_1 - y) \cup x \in \mathcal{B}$. Pero, $y \in B_2^* - B_1^*$ y $S - ((B_1 - y) \cup x) \in \mathcal{B}^*$. Por otro lado, $S - ((B_1 - y) \cup x) = ((S - B_1) - x) \cup y = (B_1^* - x) \cup y$. Entonces, B^* satisface (B2).

El matroide del teorema anterior cuyo soporte es S y tiene conjunto de bases B^* es el **dual** de $\mathcal{M} = (S, \mathcal{I})$ y se nota por $\mathcal{M}^* = (S, \mathcal{I}^*)$.

Ejemplo 2.2.13 Sea $\mathcal{M} = (S, \mathcal{I})$, donde $S = \{1, 2, 3\}$ e $\mathcal{I} = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\}$. El conjunto $\{2, 3\}$ es la base del matroide \mathcal{M} . Utilizando el teorema anterior, el conjunto $\{1\}$ es una base para el matroide dual con soporte $S = \{1, 2, 3\}$ e $\mathcal{I}^* = \{\{1\}, \emptyset\}$.

3 Redes Matroidales y Soluciones Lineales Escalares

En este capítulo, se establece la relación entre los códigos de red lineales escalares y las redes matroidales asociadas a matroides representables. Las definiciones y los teoremas centrales del capítulo son tomados de la referencia [4].

3.1. Códigos de red globales

En la sección, se definen los códigos de red globales y se demuestra su equivalencia con los códigos de red lineales definidos sobre un digrafo.

Definición 3.1.1 Sean, N_G una red, k, n números enteros positivos y F un cuerpo tal que $|F| > |\mathcal{A}|$. Un **código de red lineal global** $GN_G(k, n)$ sobre N_G , es un conjunto de funciones $\Phi_{msg}, \Phi_{arista}$, definidas como sigue:

(i) $\Phi_{msg} : \mu \rightarrow (F^{k \times k})^{|\mu|}$, tal que para cada mensaje m_i , $\Phi_{msg}(m_i) := (M_1^{(m_i)}, \dots, M_{|\mu|}^{(m_i)})^T$, donde $M_i^{(m_i)}$ es una matriz de tamaño $k \times k$ sobre F .

(ii) $\Phi_{arista} : E \rightarrow (F^{n \times k})^{|\mu|}$, tal que para cada arista e , $\Phi_{arista}(e) := (M_1^{(e)}, \dots, M_{|\mu|}^{(e)})^T$, donde $M_i^{(e)}$ es una matriz de tamaño $n \times k$ sobre F .

La siguiente definición permite asegurar que los vectores de matrices que se asignan en cada arista, se representan como combinación lineal (los escalares son matrices) de los vectores de matrices que ingresan. La representación junto con la notación empleada, dependenden del nodo donde se trabaje.

Definición 3.1.2 Sean, N_G una red, k, n números enteros positivos y F un cuerpo, tal que $|F| > |\mathcal{A}|$. Un código de red lineal global $GN_G(k, n)$, es una **solución** para la red N_G , si las siguientes condiciones se cumplen:

(i) Para cada $m_i \in \mu$, $\Phi_{msg}(m_i) = (0, \dots, 0, I^{k \times k}, 0, \dots, 0)^T$, donde la matriz identidad $I^{k \times k}$ está en la posición i -ésima .

(ii) Para cada nodo $u \in S_\mu$ y cada arista $e \in \Gamma_O(u)$, si $\Phi_{arista}(e) := (M_1^{(e)}, \dots, M_{|\mu|}^{(e)})^T$, existen matrices $C_1^{(e)}, \dots, C_{\alpha(u)}^{(e)}$ de tamaño $n \times k$ sobre F , tales que:

$$M_i^{(e)} = \sum_{j=1}^{\alpha(u)} C_j^{(e)} M_i^{(j)}, (i = 1, \dots, |\mu|), \text{ donde } S(u) = \{m_1, \dots, m_{\alpha(u)}\} \text{ y } \Phi_{msg}(m_j) = (M_1^{(j)}, \dots, M_{|\mu|}^{(j)})^T, 1 \leq j \leq \alpha(u) .$$

(iii) Sea $u \in V$, tal que $u \notin S_\mu$ y $u \notin R_\mu$. Si $e \in \Gamma_O(u)$, y $\Phi_{arista}(e) := (M_1^{(e)}, \dots, M_{|\mu|}^{(e)})^T$, entonces existen matrices $C_{\alpha+1}^{(e)}, \dots, C_{\alpha+\beta(u)}^{(e)}$ de tamaño $n \times n$ sobre F , tales que:

$$M_i^{(e)} = \sum_{j=\alpha+1}^{\beta(u)} C_j^{(e)} M_i^{(e_j)}, (i = 1, \dots, |\mu|), \text{ donde } \Phi_{arista}(e_j) = (M_1^{(e_j)}, \dots, M_{|\mu|}^{(e_j)})^T, j = \alpha + 1, \dots, \alpha + \beta(u).$$

(iv) Para cada nodo $t \in R_\mu$ y $m \in R(t)$, si $\Phi_{msg}(m_i) := (M_1^{(m_i)}, \dots, M_{|\mu|}^{(m_i)})^T$ entonces existen matrices $C_{\alpha+1}^{(m_i)}, \dots, C_{\alpha+\beta(t)}^{(m_i)}$ de tamaño $k \times n$ sobre F , tales que:

$$M_i^{(m_i)} = \sum_{j=1}^{\beta(t)} C_{\alpha+j}^{(m_i)} M_i^{(e_j)}, (i = 1, \dots, |\mu|) \text{ donde } \Phi_{arista}(e_j) = (M_1^{(e_j)}, \dots, M_{|\mu|}^{(e_j)})^T, j = \alpha + 1, \dots, \alpha + \beta(t).$$

Teorema 3.1.3[4] Sea N_G una red. Entonces, N_G tiene una solución lineal $LN_G(k, n)$, si y sólo si, tiene una solución lineal global $GN_G(k, n)$.

Demostración. \Rightarrow) Sea $a : \mu \rightarrow F^k$ una función de símbolo de los mensajes de la red N_G con su correspondiente símbolo de arista $\chi : E \rightarrow F^n$. Por hipótesis, $LN_G(k, n)$ es un código de red lineal, entonces sus funciones de arista f_{uv} y $f_{t,m}$ se definen como:

i) Para $u \in S_\mu$, $f_{uv}(a(m_1), \dots, a(m_{\alpha(u)})) = \sum_{j=1}^{\alpha(u)} C_j^{(m_j)} a(m_j)$, donde $S(u) = \{m_1, \dots, m_{\alpha(u)}\}$ y $C_1^{(m_1)}, \dots, C_{\alpha(u)}^{(m_{\alpha(u)})}$ son matrices de tamaño $n \times k$ sobre F .

ii) Para $u \notin S_\mu$, $f_{uv}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(u)})) = \sum_{j=\alpha+1}^{\alpha+\beta(u)} C_j^{(e_j)} \chi(e_j)$, donde $C_{\alpha+1}^{(e_{\alpha+1})}, \dots, C_{\alpha+\beta(u)}^{(e_{\alpha+\beta(u)})}$ son matrices de tamaño $n \times n$ sobre F .

iii) Para todo $t \in R_\mu$ y $m_i \in R(t)$, $f_{t,m_i}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(t)})) = \sum_{j=\alpha+1}^{\alpha+\beta(t)} C_j^{(e_j)} \chi(e_j)$, donde $C_{\alpha+1}^{(e_{\alpha+1})}, \dots, C_{\alpha+\beta(t)}^{(e_{\alpha+\beta(t)})}$ son matrices de tamaño $k \times n$ sobre F .

Utilizando las definiciones de los numerales, *i*), *ii*) y *iii*), se construye un código lineal global $GN_G(k, n)$, de la siguiente forma:

iv) Para cada mensaje m , $\Phi_{msg}(m) = (0, 0, \dots, 0, I^{k \times k}, \dots, 0)^T$, donde $I^{k \times k}$ es la matriz identidad de tamaño $k \times k$.

v) Sean, $u \in S_\mu$ y $\Phi_{msg}(m_j) = (M_1^{(m_j)}, \dots, M_{|\mu|}^{(m_j)})$ para $j = 1, \dots, \alpha(u)$. Utilizando el numeral *i*), $\Phi_{arista}(uv) = (M_1^{(uv)}, \dots, M_{|\mu|}^{(uv)})^T$, donde $M_i^{(uv)} = \sum_{j=1}^{\alpha(u)} C_j^{(m_j)} M_i^{(m_j)}$.

vi) Sean, $u \notin S_\mu$ y $\Gamma_I(u) = \{e_{\alpha+1}, \dots, e_{\alpha+\beta(u)}\}$ el conjunto de aristas que llegan a u , tales que $\Phi_{arista}(e_j) = (M_1^{(e_j)}, \dots, M_{|\mu|}^{(e_j)})^T$ para $j = \alpha + 1, \dots, \alpha + \beta(u)$. Utilizando el numeral *ii*), $\Phi_{arista}(uv) = (M_1^{(uv)}, \dots, M_{|\mu|}^{(uv)})^T$, donde $M_i^{(uv)} = \sum_{j=\alpha+1}^{\beta(u)} C_j^{(e_j)} M_i^{(e_j)}$

El código lineal global $GN_G(k, n)$ cumple las primeras condiciones de la definición 3.1.2, en virtud de las condiciones, *iv*), *v*) y *vi*). Para verificar la última condición de la definición 3.1.2, sean, $t \in R_\mu$ y $m \in R(t)$. Como el código lineal $LN_G(k, n)$ es una solución para la red N_G , por la definición 2.1.6 y el numeral *iii*) se tiene:

$$vii) \quad f_{t, m_i}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(t)})) = \sum_{j=\alpha+1}^{\alpha+\beta(u)} C_j^{(e_j)} \chi(e_j) = a(m_i)$$

Sean, $\Phi_{arista}(e_j) = (M_1^{(e_j)}, \dots, M_{|\mu|}^{(e_j)})^T$ para $j = \alpha + 1, \dots, \alpha + \beta(t)$. Utilizando el numeral *vii*), $[\Phi_{msg}]_i = \sum_{j=\alpha+1}^{\alpha+\beta(t)} C_j^{(e_j)} M_i^{(e_j)}$ para todo i . Por lo tanto, GN_G es una solución de la red N_G .

\Leftarrow) : Supongamos que el código de red lineal global $GN_G(k, n)$ es una solución para la red N_G . Sean, $a : \mu \rightarrow F^k$ una función de símbolo con sus correspondientes símbolo de arista s y $LN_G(k, n)$ un código de red lineal con funciones de aristas dadas por :

i) Para $u \in S_\mu$, $f_{uv}(a(m_1), \dots, a(m_\alpha(u))) = \sum_{j=1}^{\alpha(u)} C_j^{(m_j)} a(m_j)$, ya que al aplicar la definición 3.1.2 al código de red $GN_G(k, n)$, $C_1^{(m_1)}, \dots, C_{\alpha(u)}^{(m_\alpha(u))}$ existen.

ii) Para $u \notin S_\mu$, $f_{uv}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(u)})) = \sum_{j=\alpha+1}^{\alpha+\beta(u)} C_j^{(e_j)} \chi(e_j)$, donde las matrices $C_{\alpha+1}^{(e_{\alpha+1})}, \dots, C_{\alpha+\beta(u)}^{(e_{\alpha+\beta(u)})}$ existen al aplicar parte *iii*) de la definición 3.1.2 al código de red $GN_G(k, n)$.

iii) Para cada $t \in R_\mu$ y $m_i \in R(t)$, $f_{t, m_i}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(t)})) = \sum_{j=\alpha+1}^{\alpha+\beta(t)} C_j^{(e_j)} \chi(e_j)$,

donde las matrices $C_{\alpha+1}^{(e_{\alpha+1})}, \dots, C_{\alpha+\beta(t)}^{(e_{\alpha+\beta(t)})}$ existen al aplicar parte (iv) de la definición 3.1.2 al código de red $GN_G(k, n)$.

Por el numeral (iii) y la última parte de la definición 3.1.2, $f_{t, m_i}(\chi(e_{\alpha+1}), \dots, \chi(e_{\alpha+\beta(t)})) = a(m_i)$. Por lo tanto, el código de red $LN_G(k, n)$ es una solución lineal para la red N_G .

3.2. Redes escalares solubles

En la sección, se establece la relación entre las redes matroidales representables y las soluciones lineales escalares definidas sobre un digrafo.

Definición 3.2.1 Sean, N_G una red y $\mathcal{M} = (S, \mathcal{I})$ un matroide con función de rango $r_{\mathcal{M}}$. La red N_G es una **red matroidal** asociada con \mathcal{M} , si existe una función $f_{\mathcal{M}} : \mu \cup E \rightarrow S$, tal que:

(RM1) $f_{\mathcal{M}}$ es una función uno a uno sobre μ .

(RM2) $f_{\mathcal{M}}(\mu) \in \mathcal{I}$.

(RM3) $r_{\mathcal{M}}(f_{\mathcal{M}}(\Gamma_I(u))) = r_{\mathcal{M}}(f_{\mathcal{M}}(\Gamma_I(u) \cup \Gamma_O(u)))$, para todo $u \in V$.

Lema 3.2.2 [4] Sean, A una matriz de tamaño $n \times m$ definida sobre un cuerpo finito F y $\mathcal{M}(A)$ un matroide representable sobre A . Entonces, existe una matriz A' definida sobre un cuerpo finito F' , tales que $|F'| > |F|$ y $\mathcal{M}(A)$ es isomorfa a $\mathcal{M}(A')$.

Demostración. Sea F' un cuerpo que contiene a F como subcuerpo. Es posible considerar la matriz A sobre F' , así se escoge $A = A'$. En lo que sigue, se demuestra que cualquier conjunto de vectores columna de A es independiente sobre F , si y sólo si, lo son sobre F' .

\Rightarrow) : Sea $\{v_1, \dots, v_k\}$ un conjunto independiente sobre F . Es posible extender el anterior conjunto a una base \mathcal{B} para F^n . Los vectores del conjunto \mathcal{B} forman una matriz con determinante no nulo sobre F . Como F es un subcuerpo de F' , el conjunto \mathcal{B} forma una matriz con determinante no nulo sobre F' . Por lo tanto, el conjunto \mathcal{B} es un independiente sobre F' , en particular el conjunto $\{v_1, \dots, v_k\}$ es independiente sobre F' .

\Leftarrow) : Sea $\{v_1, \dots, v_k\}$ un conjunto dependiente sobre F . Entonces, existe algún escalar no nulo $a_i \in F$, tal que $a_1 v_1 + \dots + a_k v_k = 0$. Como F es un subcuerpo de F' , $a_i \in F'$ para todo $i = 1, \dots, k$. Por lo tanto, el conjunto $\{v_1, \dots, v_k\}$ es dependiente sobre F' .

Teorema 3.2.3 [4] Una red N_G es matroidal, con matroide representable sobre un cuerpo finito, si y sólo si, la red N_G admite una solución lineal escalar.

Demostración. \Rightarrow) : Sea N_G una red matroidal, donde el matroide que la representa es $\mathcal{M}(A) = (S, \mathcal{I})$, donde A una matriz de tamaño $n \times m$ definida sobre un cuerpo finito F . Utilizando el lema anterior, es posible asumir que $|F| \geq |\mathcal{A}|$. Sin pérdida de generalidad, se supone que las filas de la matriz A son linealmente independientes. Como la red es matroidal, existe una función $f_{\mathcal{M}} : \mu \cup E \rightarrow S$, donde $f_{\mathcal{M}}(\mu) = \{i_1, \dots, i_{|\mu|}\}$ es un conjunto linealmente independiente de columnas en F^n , que se puede extender a una base \mathcal{B} para F^n . Al efectuar cambios elementales en la matriz A , esta es equivalente a matriz $[I_n | A']$, donde el conjunto $\{i_1, \dots, i_{|\mu|}\}$ corresponde a las primeras $|\mu|$ columnas de A y A' es una matriz de tamaño $n \times (m - n)$. Nótese que el matroide representado por A y la matriz $[I_n | A']$, es el mismo salvo isomorfismo. Además, si $|\mu| < n$ se introducen $n - \mu$ mensajes mudos generados por nodos separados a la red original. Se define un código lineal global sobre N_G , como:

$$i) \text{ Para cada mensaje } m_i, \Phi_{msg}(m_i) = A_{f(m_i)}.$$

$$ii) \text{ Para cada arista } e, \Phi_{arista}(e) = A_{f(e)}.$$

El código global anterior es una solución lineal escalar para la red, ya que, para cada $m_i \in \mu$, $\Phi_{msg}(m_i) = A_{f(m_i)} = (0, \dots, 1, 0, \dots, 0)$ y para cada $u \in S_\mu$ y cada arista $e \in \Gamma_O(u)$, $r(f(\Gamma_I(u))) = r(f(\Gamma_I(u) \cup \Gamma_O(u)))$, ya que la red N_G es matroidal. Lo cual es equivalente a decir que, si $\Phi_{arista}(e) = A_{f_e}$, entonces A_{f_e} es una combinación lineal del conjunto $\{A_{f_{m_i}} : m_i \in \Gamma_1(u)\}$. Para cada nodo $u \in V$, tal que $u \notin S_\mu$ y $u \notin R_\mu$, se tiene que, $\Phi_{arista}(e) = A_{f_e}$ es una combinación lineal del conjunto $\{A_{f_{e'}} : e' \in \Gamma_I(u)\}$, donde $r(f(\Gamma_I(u))) = r(f(\Gamma_I(u) \cup \Gamma_O(u)))$ y $e \in \Gamma_O(u)$. Para cada nodo $t \in R_\mu$ y $m_i \in R(t)$, $\Phi_{msg}(m_i) = A_{f_{m_i}}$ es una combinación lineal del conjunto $\{A_{f_{e'}} : e' \in \Gamma_I(t)\}$, donde $r(f(\Gamma_I(t))) = r(f(\Gamma_I(t) \cup \Gamma_O(t)))$.

\Leftarrow) : Sean, N_G una red con una solución lineal escalar, e_1, \dots, e_l las aristas de la red y $m_1, \dots, m_{|\mu|}$ sus mensajes. La información que se codifica en cada arista es de la forma $c_1^i m_1 + \dots + c_{|\mu|}^i m_{|\mu|}$, donde $c_j^i \in F$, para $1 \leq i \leq l$.

Sea C una matriz de tamaño $|\mu| \times (|\mu| + l)$, donde la i -ésima columna C_i es:

$$\begin{pmatrix} c_1^i \\ \cdot \\ \cdot \\ \cdot \\ c_{|\mu|}^i \end{pmatrix}$$

El matroide que representa a la red es $\mathcal{M}(C) = (S, \mathcal{I})$ y la función $f_{\mathcal{M}} : \mu \times E \rightarrow S$ se define como:

- i)* $f_{\mathcal{M}}(m_i) = (0, \dots, 1, 0, \dots, 0)$, donde $m_i \in S_{\mu}$ e $i = 1, \dots, |\mu|$.
- ii)* $f_{\mathcal{M}}(e_i) = C_i$, donde C_i es la correspondiente columna de la matriz C e $i = 1, \dots, |\mu| + l$.

La función $f_{\mathcal{M}}$ es uno a uno, por lo tanto se cumple (RM1). El conjunto $f_{\mathcal{M}}(\mu)$ forma un conjunto lineal independiente de vectores, por lo tanto se cumple (RM2). Como la red es lineal, $\Gamma_O(u) \subseteq \langle \Gamma_I(u) \rangle$, de lo cual se tiene $r(f(\Gamma_I(u))) = r(f(\Gamma_I(u) \cup \Gamma_O(u)))$. Por lo tanto, (RM3) se satisface.

4 Códigos lineales y redes genéricas

La Teoría de Matroides generaliza la noción de independencia lineal, por lo tanto, es natural preguntarse, si existe un matroide que refleje la estructura de caminos independientes en un digrafo. En este capítulo, se define el matroide red sobre un digrafo con un único nodo fuente, la estructura del matroide red depende de la topología del digrafo. Luego, se definen los códigos de red genéricos, que reflejan la relación entre independencia de vectores e independencia de caminos. Se establece la relación entre el matroide inducido asociado a los códigos genéricos y el matroide red. Por último, se encuentra una representación del matroide red utilizando el matroide transversal asociado al digrafo. Este capítulo está basado en [3] y [5].

4.1. El matroide red

Definición 4.1.1 1. Sea $G_s = (V, E, s)$ un digrafo con un único nodo fuente s . Para cada $X \subseteq E$, el **flujo máximo**, $\max f(X)$, es el número máximo de caminos independientes, que inician en s y terminan en alguna arista de X .

2. Sea $G = (V, E)$ un digrafo. El grafo $G_d = (V_d, E_d)$, donde $V_d = E$ y $E_d = \{(e, e') | \pi_1(e) = \pi_2(e')\}$, se denomina el **dual** de G .

Ejemplo 4.1.2 El siguiente grafo representa el grafo dual del ejemplo 2.1.4.

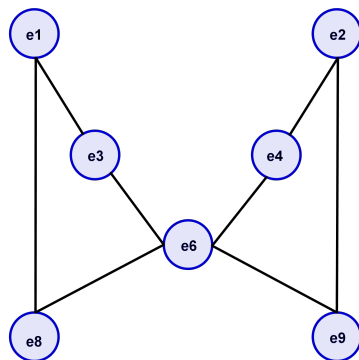


Figura 3

Lema 4.1.3 Sean, $G_s = (V, E, s)$ un digrafo, $G_d = (V_d, E_d)$ su dual y X un subconjunto no vacío de E . Entonces, $\max f(X) = |X|$, si y sólo si, existen $|X|$ caminos independientes por nodos en G_d , que inician en algún elemento de $\Gamma_O(s)$ y terminan en algún elemento de X .

Demostración. \Rightarrow) :Sea X un subconjunto no vacío de aristas del digrafo G_s , tal que $\max f(X) = |X|$. Entonces, existe una colección de caminos maximal independientes $\mathbf{P}_X = \{P_1, \dots, P_{|X|}\}$, donde para cada $i = 1, \dots, |X|$, $P_i = sv_1^i e_2^i \dots e_n^i$ y $e_n^i \in X$. Sea $\mathbf{P}'_X = \{P'_i = (sv_1^i, e_2^i)(e_2^i, e_3^i) \dots (e_{n-1}^i, e_n^i) | i = 1, \dots, |X|\}$, una colección de caminos en G_d . Ya que los caminos de la colección \mathbf{P}_X son independientes, ningún par de caminos de la colección \mathbf{P}'_X tienen aristas en común. Por lo tanto, ellos son independientes. Además, los nodos $sv_1^1, sv_1^2, \dots, sv_1^{|X|}$ son distintos en G_d , dado que los caminos de la colección \mathbf{P}_X son independientes. En conclusión, \mathbf{P}'_X es una colección de caminos independientes por nodos en G_d , tal que $|\mathbf{P}'_X| = |X|$.

\Leftarrow) : Supongamos que en G_d , existe una colección de caminos independientes por nodos $\mathbf{P}'_X = \{P'_i = (sv_1^i, e_2^i)(e_2^i, e_3^i) \dots (e_{n-1}^i, e_n^i) | i = 1, \dots, |X|\}$, tal que $|\mathbf{P}'_X| = |X|$ y $e_n^i \in X$, $i = 1, \dots, |X|$. Sea $\mathbf{P}_X = \{P_i = sv_1^i e_2^i \dots e_n^i | i = 1, \dots, |X|\}$, una colección de caminos en G . Ya que los caminos de la colección \mathbf{P}'_X son independientes, ninguno de los caminos de la colección \mathbf{P}_X tienen aristas en común. Por lo tanto, ellos son independientes. Además, la maximalidad de \mathbf{P}_X se tiene ya que $|\mathbf{P}'_X| = |X|$. Así, $\max f(X) = |X|$.

En la demostración de los axiomas de un matroide para el caso particular del matroide red, se necesita otro tipo de matroide definido sobre un digrafo, cuyo soporte

está formado por los vértices del digrafo. A continuación se introducen los elementos necesarios para definir este matroide.

Definición 4.1.4 1. Sean, $G = (V, E)$ un digrafo y $X, Y \subseteq V$. Se dice que X **está conectado con** Y si :

- (i) $|X| = |Y|$
- (ii) Existen $|X|$ -caminos independientes por aristas y nodos, tales que sus vértices iniciales están en X y sus vértices finales están en Y .

2. Sea $Z \subseteq V$. El conjunto X **está conectado sobre** Z , sí X está conectado a algún subconjunto de Z .

Notación: Sea $B_0 \subseteq V$ un conjunto fijo. El conjunto $L(G, B_0)$ representa la colección de subconjuntos de V conectados sobre B_0 .

Definición 4.1.5 Sea $G = (V, E)$ un digrafo. El **grafo bipartito** \hat{G} asignado a G , es el grafo cuyo conjunto de vértices es $V \cup \hat{V}$, donde $\hat{V} = \{\hat{v} : v \in V\}$ y cuyo conjunto de aristas es $\{v\hat{v} : v \in V\} \cup \{v\hat{u} : (u, v) \in E\}$

Lema 4.1.6 [1] Sean, X y Y subconjuntos de V . Entonces, X está conectado a Y en G , si y sólo si, $V - X$ está en correspondencia a $\hat{V} - \hat{Y}$ en \hat{G} .

Demostración. \Rightarrow): Por hipótesis existe un conjunto de caminos independientes por nodos y aristas, $\{P_x : x \in X\}$, que conecta X a Y . Sea $\Psi : (\hat{V} - \hat{Y}) \rightarrow (V - X)$, definida como:

$$\Psi(\hat{u}) = \begin{cases} v, & \text{Si } u \text{ está sobre uno de los caminos} \\ & \{P_x : x \in X\} \text{ y } v \text{ es el sucesor sobre este camino} \\ u, & \text{Si } u \in V - Y \text{ pero } u \text{ no está} \\ & \text{en ninguno de los caminos } \{P_x : x \in X\} \end{cases}$$

Como los caminos $\{P_x : x \in X\}$ son independientes por nodos y aristas, la función Ψ está bien definida y es uno a uno. Por lo tanto, el subconjunto de aristas $\{\Psi(\hat{u})u : \hat{u} \in \hat{V} - \hat{Y}\}$ en \hat{G} , forma una correspondencia de $\hat{V} - \hat{Y}$ a $V - X$.

\Leftarrow): Supongamos que existe una correspondencia entre $V - X$ y $\hat{V} - \hat{Y}$ en \hat{G} . Se pintan de rojo las aristas de la correspondencia y de azul las aristas de la forma $v\hat{v}$, donde $v \in V$. Si $x \in X \cap Y$, el camino P_x consiste de un único vértice x . Ahora se supone que

$x \in X - Y$, entonces x pertenece a una arista azul que no es roja. Sea P'_x el camino maximal de aristas azules o rojas comenzando en x . Se va a demostrar que P'_x deberá tener el último vértice en \hat{Y} , para ello se razona por contradicción. La primera arista de P'_x es azul, además las aristas de P'_x intercalan sus colores, ya que las aristas rojas forman una correspondencia como las azules. Si la última arista de P'_x es azul, esta arista es de la forma $v\hat{v}$. Como P'_x no tiene vértices en \hat{Y} , entonces $\hat{v} \notin \hat{Y}$. Por lo tanto, existe una arista roja que contiene a \hat{v} y puede ser parte del camino P'_x . Lo cual es contradictorio por la definición de P'_x . Si la última arista de P'_x es roja, esta arista es de la forma $v\hat{u}$. Como $v\hat{u} \neq v\hat{v}$, es posible adicionar la arista azul $v\hat{v}$ a P'_x , de nuevo se genera una contradicción con la elección de P'_x . Por lo tanto, P'_x incluye algún vértice en \hat{Y} . Sea \hat{y} el primer vértice de \hat{Y} en aparecer en P'_x . Como $y \notin \hat{V} - \hat{Y}$, \hat{y} no pertenece a ninguna arista roja. Así, P'_x termina en la arista azul $y\hat{y}$. El camino P'_x es el único camino maximal de aristas azules y rojas comenzando en x . Más aún, si $x = x_0$ y $\hat{y} = \hat{x}_n$, entonces P'_x es de la forma $x_0\hat{x}_0, \dots, x_n\hat{x}_n$. Sea $P_x = x_0x_1\dots x_n$. Si z_1 y z_2 son diferentes elementos de $X - Y$, entonces P'_{z_1} y P'_{z_2} son diferentes. Por lo tanto, $\{P_x : x \in X\}$ es un conjunto de caminos independientes por vértices y nodos que conectan X a Y , además $|X| = |Y|$.

Lema 4.1.7[1] Sea $\mathcal{A} = (A_1, A_2, \dots, A_m)$, una familia de subconjuntos de S y supongase que T es un transversal parcial maximal de \mathcal{A} , esto significa que T es un transversal de $\mathcal{A}' = (A_1, \dots, A_t)$, donde $t < m$. Entonces, cada transversal parcial maximal de \mathcal{A} es un transversal de \mathcal{A}' .

Demostración. Sean, $\Delta[\mathcal{A}]$ el grafo bipartito asociado con \mathcal{A} , $J = \{1, 2, \dots, m\}$ y $J' = \{1, 2, \dots, t\}$. Como T es un transversal parcial asociado con J' , es posible definir una correspondencia en $\Delta[\mathcal{A}]$, de T con J' . A continuación se colorean de azul las aristas de la anterior asignación. Supongamos que existe un transversal parcial maximal T_1 de \mathcal{A} que no es transversal de \mathcal{A}' . Por lo tanto, existe $v \in J - J'$, tal que v no hace parte de ninguna arista azul. Como T_1 es un transversal parcial de \mathcal{A} , existe $J'' \subset J$, tal que hay una correspondencia entre T_1 y J'' en $\Delta[\mathcal{A}]$. Luego se colorean de rojo la aristas de la anterior asignación. Sea P el camino de mayor longitud, que contiene aristas azules y rojas, comenzando con la arista roja e que contiene a v . Como las aristas azules y rojas conforman asignaciones en $\Delta[\mathcal{A}]$, P alterna los colores de las aristas entre rojas y azules. Sea f la última arista de P y supongase que es de color azul. Cambiando los colores sobre las aristas de P , se tiene que en el grafo bipartito $\Delta[\mathcal{A}]$, las aristas rojas son una asignación de T_1 en J con mas vertices de J' que la asignación original

de aristas rojas. Lo anterior genera una contradicción. Por lo anterior, la arista f es de color rojo. Esta consideración, genera un mayor número de aristas rojas que azules en P . Al cambiar los colores de las aristas de P , se tiene que las aristas azules del grafo $\Delta[\mathcal{A}]$ forman una asignación de cardinalidad $|T| + 1$. La anterior consideración genera una contradicción con la maximalidad de T . La arista f no es de color rojo ni azul, lo cual es contradictorio con la definición de P .

Teorema 4.1.8[1] (i) Sean, $G = (V, E)$ un digrafo y $B_0 \subseteq V$. Entonces, $L(G, B_0)$ es el conjunto de independientes del dual de algún matroide transversal definido sobre V . (ii) Inversamente, sean \mathcal{M} un matroide transversal sobre un conjunto V y \mathcal{M}^* su matroide dual, donde B_0 es una base cualquiera para \mathcal{M}^* . Entonces, existe un digrafo $G = (V, E)$ teniendo como vertices el conjunto V , tal que \mathcal{M}^* tiene a $L(G, B_0)$ como su conjunto de independientes.

Demostración. (i). Sea $G = (V, E)$ un digrafo y \hat{G} su grafo bipartito. Por el lema 4.1.6, B es un elemento maximal de $L(G, B_0)$, si y sólo si, $V - B$ esta en correspondencia a $\hat{V} - \hat{B}_0$ (1). Los subconjuntos de V que están en correspondencia a $\hat{V} - \hat{B}_0$ conforman la colección de las bases de un matroide transversal \mathcal{M} sobre V (2). Por los numerales (1) y (2), los elementos de la base del matroide dual \mathcal{M}^* son precisamente los elementos maximales de $L(G, B_0)$. Por lo tanto, $L(G, B_0)$ es el conjunto de independientes del matroide dual \mathcal{M}^* sobre V .

(ii). Sean, \mathcal{M} un matroide transversal sobre V y $V - B_0$ una base de \mathcal{M} . Por el lema 4.1.7, $\mathcal{M} = N[\mathcal{A}]$, para alguna familia \mathcal{A} de conjuntos, tal que $V - B_0$ es un transversal. Sea $\Delta[\mathcal{A}]$ el grafo bipartito asociado con \mathcal{A} , donde $\mathcal{A} = (A_j : j \in J)$. Sobre este grafo se puede definir una correspondencia de $V - B_0$ con J . Si $j \in J$ y j está relacionado a v en esta correspondencia, se renombra a j como \hat{v} . Por cada u en B_0 , se adiciona un nuevo vértice \hat{u} a $\Delta[\mathcal{A}]$, de manera tal que \hat{u} está conectado únicamente con u . El grafo resultante es de la forma \hat{G} para algún digrafo G . Por el lema 4.1.6, \mathcal{M}^* tiene a $L(G, B_0)$ como su conjunto de independientes.

El matroide $(V, L(G, B_0))$ recibe el nombre de **gamoide estricto**. En adelante el conjunto $L(G, B_0)$ se nota como \mathcal{I}_{B_0} .

Teorema 4.1.9[3] Sean, $G_s = (V, E, s)$ un digrafo e $\mathcal{I} = \{X \subseteq E | \max f(X) = |X|\}$. Entonces, (E, \mathcal{I}) es un matroide.

Demostración. Supongamos que $G_d = (V_d, E_d)$ es el grafo dual del digrafo G_s . Es posible definir el digrafo $G_d^R = (V_d, E_d^R)$, donde $E_d^R = \{(e_i, e_j) \in V_d \times V_d \mid (e_j, e_i) \in E_d\}$. Sean, $B_0 = \Gamma_O(s) \subseteq V_d$ y (V_d, \mathcal{I}_{B_0}) el correspondiente gamonoide estricto definido sobre G_d^R . Por el lema 4.1.3, un subconjunto $X \subseteq E$ es un elemento de \mathcal{I} , si y sólo si, X es un elemento de \mathcal{I}_{B_0} . Por lo tanto, (E, \mathcal{I}) es un matroide isomorfo al gamonoide estricto (V_d, \mathcal{I}_{B_0}) .

El matroide (E, \mathcal{I}) se conoce como el **matroide red**.

Ejemplo 4.1.10[3] En la figura 4, todos los conjuntos de aristas con dos elementos son independientes en el matroide red asociado al digrafo, exceptuando los conjuntos $\{e_4, e_5\}$, $\{e_4, e_6\}$, $\{e_5, e_6\}$, $\{e_7, e_8\}$, $\{e_7, e_9\}$ y $\{e_8, e_9\}$. Ningún conjunto de más de tres elementos es un independiente en el matroide red.

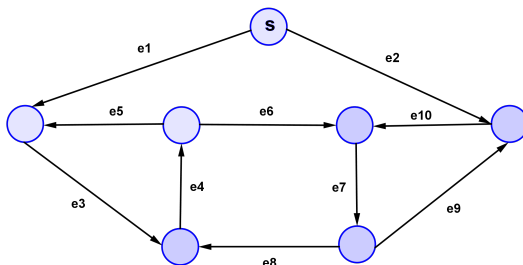


Figura 4

4.2. Códigos lineales y redes genéricas

En la sección 4.1, se define el matroide red utilizando los caminos independientes de un digrafo. En ésta sección, se relacionan los códigos de red lineales escalares con el matroide red, en particular se definen los códigos genéricos y se muestra la equivalencia entre el matroide inducido por ellos y el matroide red. Los digrafos en la sección son acíclicos.

Notación: $w \leq |\Gamma_0(s)|$

Definición 4.2.1 1. Sean, $G_s = (V, E, s)$ un digrafo y F un cuerpo. Un código de red **F-Lineal** sobre G_s , es un conjunto de vectores $f_e \in F^w$, tales que :

- (i) Los vectores f_e para $e \in \Gamma_O(s)$, pueden ser cualquier vector en F^w .
- (ii) Si $e \notin \Gamma_O(s)$, $f_e = \sum_{d \in \Gamma_I(\pi_1(e))} k_{d,e} f_d$, donde $k_{d,e} \in F$.

2. Sean, $G_s = (V, E, s)$ un digrafo y L un código de red **F-Lineal** sobre G_s . El **matroide inducido** por L , (E, \mathcal{I}_L) , se define como :

- (i) El soporte del matroide es el conjunto de las aristas del digrafo G_s .
- (ii) Los independientes del matroide son subconjuntos de aristas cuyos vectores asociados son linealmente independientes

3. Sea $G_s = (V, E, s)$ un digrafo. Un conjunto de aristas α de G es **independiente**, si cada arista de α pertenece a algún camino iniciando en s , y además dichos caminos son independientes. El conjunto de caminos independientes es el **flujo** asociado a α . Si e_i representa una arista, entonces $\pi_1(e_i) = t_i$.

4. Sea $G_s = (V, E, s)$ un digrafo. Un conjunto de aristas α es **regular**, si $\{f_e : e \in \alpha\}$ es un conjunto de vectores independientes.

5. Sean, $\{a, b, e_1, \dots, e_i\}$ cualquier conjunto de aristas, donde $0 \leq i$. Sí $\pi_2(a) = \pi_1(b)$ y $\alpha = \{a, e_1, \dots, e_i\}$ y $\beta = \{b, e_1, \dots, e_i\}$ son conjuntos independientes, entonces el conjunto α es el **soporte** del conjunto β . En adelante, $\alpha \rightarrow \beta$, significa que α es el soporte de β .

6. Sean, $G_s = (V, E, s)$ un digrafo y $T \subseteq V$, tal que $s \notin T$. Un **corte** entre el nodo s y T , es un conjunto $U \subseteq V$, tal que $s \in U$ y $t \notin U$, para todo $t \in T$.

7. El conjunto $E_U = \{e \in E : e \in \Gamma_O(i) \cap \Gamma_I(j) \text{ para } i \in U \text{ y } j \notin U\}$, es el conjunto de aristas que **cruzan** el corte.

8. Dados $T \subseteq V$ y $\tilde{E} \subseteq E$, se definen los conjuntos $V_T = \langle \{f_e : e \in \Gamma_I(t), t \in T\} \rangle$ y $V_{\tilde{E}} = \langle \{f_e : e \in \tilde{E}\} \rangle$.

Ejemplo 4.2.2 Sea, $f_{e_1} = f_{e_2} = f_{e_3} = f_{e_4} = f_{e_5} = (1, 0)$, un código lineal definido sobre el digrafo de la figura 5. El conjunto $\{e_3, e_4\}$ es independiente y no es regular. Los códigos genéricos serán definidos como códigos lineales, donde los conjuntos de aristas independientes sean regulares.

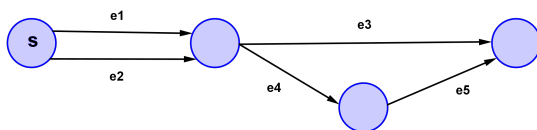


Figura 5

En adelante, se asume que $\Gamma_I(s)$ es una base de F^ω . Los vectores de la base de F^ω serán canales imaginarios que llegan al único nodo fuente s .

Lema 4.2.3 [5] Sean, $G_s = (V, E, s)$ un digrafo y $\{e_1, \dots, e_m\}$, $1 \leq m \leq \omega$, un conjunto de aristas cuyos vectores asociados son linealmente independientes. Entonces, $\{e_1, \dots, e_m\}$ es un conjunto independiente.

Demostración. Sea $\{e_1, \dots, e_m\}$ un conjunto de aristas cuyos vectores de arista f_{e_1}, \dots, f_{e_m} son linealmente independientes. Para cada arista e_i , $1 \leq i \leq m$, se adiciona una nueva arista e'_i , tal que $\pi_2(e_i) = \pi_1(e'_i)$, $\pi_2(e'_i) = t$ y $f_{e_i} = f_{e'_i}$. Sean, U cualquier corte entre s y t e $E_U = \{e \in E : e \in \Gamma_O(i) \cap \Gamma_I(j)\}$ el conjunto de aristas que cruzan el corte, donde $i \in U$ y $j \notin U$. Por la definición de código de red lineal y de E_U se tiene que $\langle f_{e'_i} : 1 \leq i \leq m \rangle \subseteq \langle f_e : e \in E_U \rangle$. Por lo tanto, $\dim(\langle f_{e'_i} : 1 \leq i \leq m \rangle) \leq \dim(\langle f_e : e \in E_U \rangle) \leq |E_U|$, en particular $\dim(\langle f_{e'_i} : 1 \leq i \leq m \rangle) \leq \min_U |E_U| = \text{Mincut}(s, t)$ (1). Sea $E_{U^*} = \{e'_i : 1 \leq i \leq m\}$ las aristas a travez de un corte U^* . Por la hipótesis y el numeral (1), $m = \dim(\langle f_{e'_i} : 1 \leq i \leq m \rangle) \leq \text{Mincut}(s, t) \leq |E_{U^*}| = m$. Por lo tanto, $\text{Maxflow}(s, t) = \text{Mincut}(s, t)$, entonces $\{e_1, \dots, e_m\}$ es un conjunto independiente

Una interesante situación es construir códigos de red lineales donde los conjuntos independientes de aristas tengan asociados vectores linealmente independientes. El siguiente lema responde a la anterior situación.

Lema 4.2.4 [5] Sean, $G_s = (V, E, s)$ un digrafo y K un cuerpo, donde $|K| = q$. Para cualquier colección de conjuntos independientes \mathcal{I} , existe un código de red lineal \mathbf{F} , definido sobre K , tal que cualquier conjunto independiente $I \in \mathcal{I}$ es regular, dado que $|I| \leq q$.

Demostración. Dado cualquier elemento $I \in \mathcal{I}$, es posible establecer un conjun-

to de caminos independientes por aristas, P_I , que inician en los canales imaginarios y terminan en los elementos de I . Nótese en primer lugar que para cada P_I , sus conjuntos de aristas iniciales son subconjuntos de $\Gamma_O(s)$, por lo tanto resultan ser regulares. Supongase que se van adicionando aristas de manera que cada P_I resulta ser regular hasta en cierto momento. Sea e la siguiente arista en ser procesada. La arista e induce los conjuntos independientes β_i , $1 \leq i \leq n$. Supongase que $\alpha_i \rightarrow \beta_i$, $1 \leq i \leq n$, donde los conjuntos independientes α_i son los obtenidos en el paso anterior. Se nota por $e_i = \alpha_i \setminus \beta_i$ y $\pi_1(e) = t$. Sea $V_t = \{f_e : \pi_2(e) = t\}$, nótese que $\dim(V_t \cap \langle f_e : e \in (\alpha_i \setminus e_i) \rangle) \leq \dim(V_t) - 1$ ya que α_i es un conjunto regular por hipótesis inductiva. Por lo tanto, $|V_t \setminus \cup_i \langle f_e : e \in (\alpha_i \setminus e_i) \rangle| > 0$, ya que $q > |I| \geq n$. Escogiendo cualquier vector del conjunto $V_t \setminus \langle f_e : e \in (\alpha_i \setminus e_i) \rangle$ para e se sigue manteniendo la regularidad.

El siguiente teorema introduce el concepto de códigos de red genéricos. Los primeros enunciados del teorema establecen relaciones algebraicas y los últimos relacionan los conceptos de independencia y regularidad de conjuntos de aristas.

Teorema 4.2.5 [5] Sean, $G_s = (V, E, s)$ un digrafo y L un código de red F -Lineal sobre G_s . Las siguientes condiciones son equivalentes:

(i) Para cualquier conjunto de vectores de arista $\{f_{e_1}, \dots, f_{e_m}\}$, si $\langle \Gamma_I(t_i) \rangle$ no está contenido en el conjunto $\langle f_{e_k} : k \neq i \rangle$, para $1 \leq i \leq m$, entonces $\{f_{e_1}, \dots, f_{e_m}\}$ son linealmente independientes.

(ii) Para cualquier conjunto de vectores de arista $\{f_{e_1}, \dots, f_{e_m}\}$, si $\langle \Gamma_I(t_m) \rangle$ no está contenido en el conjunto $\langle f_{e_k} : k \neq m \rangle$ y no existe un camino desde t_m a t_i , para $1 \leq i \leq m - 1$, entonces $f_{e_m} \notin \langle f_{e_1}, \dots, f_{e_{m-1}} \rangle$.

(iii) Para cualquier conjunto de vectores de arista $\{f_{e_1}, \dots, f_{e_m}\}$, si $f_{e_1}, \dots, f_{e_{m-1}}$ son linealmente independientes, $\langle \Gamma_I(t_m) \rangle$ no está contenido en el conjunto $\langle f_{e_1}, \dots, f_{e_{m-1}} \rangle$ y no existe un camino desde t_m a t_i , para $1 \leq i \leq m - 1$, entonces $f_{e_m} \notin \langle f_{e_1}, \dots, f_{e_{m-1}} \rangle$.

(iv) Cualquier conjunto independiente de aristas β , de a lo más ω aristas, es regular.

(v) Cualquier conjunto independiente de aristas α , con ω aristas, es regular.

Demostración. $(v) \Rightarrow (iv)$: Cualquier conjunto independiente de aristas β , de a lo más ω aristas, se puede extender a un conjunto α con ω aristas, ya que $w \leq |\Gamma_0(s)|$. El resultado se tiene por la hipótesis.

$(iv) \Rightarrow (iii)$: Sean, e_1, \dots, e_m un conjunto de aristas tales que $f_{e_1}, \dots, f_{e_{m-1}}$ son linealmente independientes. Por hipótesis, $\langle \Gamma_I(t_m) \rangle$ no está contenido en $\langle f_{e_1}, \dots, f_{e_{m-1}} \rangle$, entonces existe $e'_m \in \langle \Gamma_I(t_m) \rangle$, tal que $f_{e_1}, \dots, f_{e'_m}$ son linealmente independientes. Por el lema 4.2.3, existen P_1, \dots, P'_m caminos independientes, iniciando en s y terminando en las aristas e_1, \dots, e'_m . Por la hipótesis, no existe un camino desde t_m a t_i , para $1 \leq i \leq m-1$, entonces existe un camino $P_m = P'_m \cup e_m$, tal que P_1, \dots, P_m son caminos independientes. Así, e_1, \dots, e_m un conjunto independiente y por (iv) , f_{e_1}, \dots, f_{e_m} son linealmente independientes.

$(iii) \Rightarrow (ii)$: Sean, $\xi = \{e_1, \dots, e_{m-1}\}$ un conjunto de aristas y $e_m \notin \xi$ tal que $\langle \Gamma_I(t_m) \rangle$ no está contenido en el conjunto $\langle f_{e_k} : k \neq m \rangle$. El conjunto $\{f_{e_1}, \dots, f_{e_{m-1}}\}$ puede ser un conjunto de vectores linealmente dependientes. Por lo tanto, existe $\xi' \subseteq \xi$, tal que $\{f_e | e \in \xi'\}$ es un conjunto de vectores linealmente independientes y $\langle f_e | e \in \xi \rangle = \langle f_e | e \in \xi' \rangle$. Por hipótesis, se satisface (iii) , entonces $f_{e_m} \notin \langle f_e | e \in \xi' \rangle = \langle f_e | e \in \xi \rangle$.

$(ii) \Rightarrow (i)$: Sea, e_1, \dots, e_m un conjunto de aristas, se razona por inducción sobre la longitud del número de aristas.

Si $m = 2$ y (ii) no implica (i) , entonces debe existir un camino desde t_1 hasta t_2 , ya que de lo contrario, por (ii) , f_1 y f_2 serían vectores linealmente independientes y esto contradice la negación de (i) . Similarmente, debe existir un camino desde t_2 hasta t_1 . Entonces, el digrafo G debería ser cíclico, lo cual es contradictorio. Así, en el caso $m = 2$, $(ii) \Rightarrow (i)$. Supongase que $(ii) \Rightarrow (i)$, para $m \leq k$. Para $m = k + 1$, (ii) no implica (i) , sin pérdida de generalidad $f_{e_1} \in \langle f_{e_k} : k \neq 1 \rangle$ por la negación de i . Entonces, debe existir un camino desde t_1 hasta t_{i_1} , donde $1 \leq i_1 \leq k + 1$. Similarmente, debe existir un camino desde t_{i_2} hasta t_{i_3} y así sucesivamente, se produce un ciclo lo cual es contradictorio. Por lo tanto, para $m = k + 1$, (ii) implica (i) .

$(i) \Rightarrow (v)$ Sea, $\alpha = \{e_1, \dots, e_\omega\}$ un conjunto independiente. Por lo tanto, existen ω caminos independientes P_1, \dots, P_ω , iniciando en s y terminando en los elementos de α , donde la última arista del camino P_i es e_i , $1 \leq i \leq \omega$. Se nota por l_i la longitud del camino P_i y sea $L = \sum_{i=1}^{\omega} l_i$. Sí $L = \omega$, entonces α es un conjunto regular de aristas,

ya que $\langle \Gamma_1(t_i) \rangle = \langle \Gamma_1(s) \rangle$ no está contenido en el conjunto $\langle f_{e_k} : k \neq i \rangle$, $1 \leq i \leq \omega$. Supongase que $K(\alpha)$, es un conjunto de vectores independientes, para todo α , donde $\omega \leq L \leq k$. Sean, $A = \{i : l_i > 1\}$ y $\alpha_i = \{e_1, \dots, e'_i, \dots, e_m\}$ para $i \in A$, donde $e'_i \in P_i$ y $\pi_1(e'_i) = \pi_2(e_i)$. Entonces, para α_i , $K(\alpha_i)$ es un conjunto de vectores independientes ya que $L = k$.

Definición 4.2.6 Sea $G_s = (V, E, s)$ un digrafo. Un código de red **F -Lineal** sobre G_s es **genérico**, si se satisface alguna de las condiciones del teorema anterior.

Ejemplo 4.2.7 El código $GF(3)$ -lineal L , definido sobre el digrafo de la figura 5, por,

$$\begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \\ \begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 2 & 1 \end{bmatrix} \end{array}$$

es un código de red genérico.

El siguiente teorema establece la relación entre el matroide red y los códigos genéricos.

Teorema 4.2.8 [3] Un código de red **F -Lineal** L sobre un digrafo G_s es genérico, si y sólo si, el matroide inducido sobre L es el matroide red del digrafo G_s .

Demostración. \Leftarrow) : Por la hipótesis, el matroide inducida por el código de red **F -Lineal** L es la misma matroide red, lo cual significa que $(E, \mathcal{I}) = (E, \mathcal{I}_L)$. Sea, $X = \{e_1, e_2, \dots, e_m\}$ un subconjunto de aristas, con $m \leq w$, tal que para todo j , el conjunto $\langle \Gamma_I(\pi_1(e_j)) \rangle$ no está contenido en $\langle \{f_{e_1}, \dots, f_{e_m}\} - \{f_{e_j}\} \rangle$. Por lo tanto, para e_j , $1 \leq j \leq m$, se tiene que:

$$\dim(\langle \{f_{e_k} : k \neq j\} \rangle) < \dim(\langle \Gamma_I(\pi_1(e_j)) \rangle \cup \langle \{f_{e_k} : k \neq j\} \rangle)$$

De lo cual, se concluye que:

$$r(\bigcup_{k \neq j} e_k) < r(\Gamma_I(\pi_1(e_j)) \cup (\bigcup_{k \neq j} e_k)),$$

donde r es el rango del matroide red (E, \mathcal{I}) . Sean, I_1 e I_2 , conjuntos maximales independientes contenidos en $(\bigcup_{k \neq j} e_k)$ y $(\Gamma_I(\pi_1(e_j)) \cup (\bigcup_{k \neq j} e_k))$ respectivamente. Como $|I_1| < |I_2|$, existe una arista $e \in I_2 - I_1 \subseteq \Gamma_I(\pi_1(e_j))$, tal que $I_1 \cup e$ es un conjunto

independiente. Por lo tanto, $r(X - e_j) = r(X) - 1(1)$. Razonando por contradicción, se asume que el conjunto X es dependiente, entonces cada subconjunto Y de X , de cardinal $m - 1$ es dependiente, de lo contrario por (1), $r(X) = m$, lo cual es contradictorio. Sean, $Y \subseteq X$, $|Y| = m - 1$, y I_X e I_Y conjuntos maximales independientes contenidos en X y Y . Como $r(Y) = r(X) - 1$, $|I_Y| < |I_X|$, entonces existe $e_i \in I_X - I_Y$, tal que $I_Y \cup e_i$ es independiente. Además, por la dependencia de Y , existe $e_j \in Y - I_Y$, tal que $r(Y - e_j) = r(Y)$. Al considerar $X - e_j$ como $(Y - e_j) \cup e_i$, se tiene que, $r(X - e_j) = r(Y) + 1 = r(X)$. Lo anterior genera una contradicción. Por lo tanto, el conjunto de aristas X es linealmente independiente.

\Rightarrow) : $i)(E, \mathcal{I}_L) \subseteq (E, \mathcal{I})$ Sea, X un conjunto independiente en el matroide inducido (E, \mathcal{I}_L) . Denotamos por C al conjunto mínimo de aristas que después de ser removidas del digrafo, no existen caminos desde s hasta cualquier arista en X . Como el digrafo es cíclico, $|X| = \dim(\langle f_e : e \in X \rangle) \leq \dim(\langle f_e : e \in C \rangle) \leq |C| = \max f(X) \leq |X|$. Entonces, X es conjunto independiente en la matroide red (E, \mathcal{I}) .

$ii)(E, \mathcal{I}) \subseteq (E, \mathcal{I}_L)$: Sean, \mathcal{B} la familia de las bases de la matroide red (E, \mathcal{I}) y $\mathcal{L} : \mathcal{B} \rightarrow N$ una función, donde $\mathcal{L}(B)$ es el mínimo número de aristas contenidas en los w -caminos independientes desde $\Gamma_O(s)$ hasta las aristas de B . Por medio de la función \mathcal{L} , $\mathcal{B} = \{B_1, \dots, B_{|\mathcal{B}|}\}$. Utilizando inducción sobre el cardinal de \mathcal{B} , se tendrá que $B_i \in \mathcal{I}_L$. En el caso $k = 1$, nótese que $B_1 = \Gamma_O(s)$. Como $\langle f_e : e \in \Gamma_I(s) \rangle = F^w$, entonces, B_1 satisface la condición i) del teorema 4.2.5, de donde $B_1 \in \mathcal{I}_L$. Sea, $B_{k+1} = \{e_1, \dots, e_w\}$ un elemento de \mathcal{B} que no satisface la condición i) del teorema 4.2.5. Entonces, debe existir una arista $e_j \in B_{k+1}$, donde:

$$\langle f_e : e \in \Gamma_I(\pi_1(e_j)) \rangle \subseteq \langle f_e : e \in B_{k+1} - e_j \rangle(1).$$

Ya que B_{k+1} es una base de la matroide red, existe por lo menos una arista e' en $\Gamma_I(\pi_1(e_j))$, de tal manera que $(B_{k+1} - e_j) \cup e'$ es una base de la matroide red.

Ya que $\mathcal{L}((B_{k+1} - e_j) \cup e') = \mathcal{L}(B_{k+1}) - 1$, por la hipótesis de inducción, $(B_{k+1} - e_j) \cup e'$ satisface la condición i) del teorema 4.2.5. Por lo tanto, $f_{e'} \notin \langle f_e : e \in B_{k+1} - e_j \rangle$, lo cual es contradictorio con el numeral (1). Así, $B_{k+1} \in \mathcal{I}_L$.

El siguiente teorema ofrece una caracterización de los códigos de red genéricos, en terminos de alguna representación del matroide red.

Teorema 4.2.9 [3] Sean, $G_s = (V, E, s)$ un digrafo y (E, \mathcal{I}) el matroide red sobre G_s . Cualquier F -representación para el matroide red induce un código de red genérico.

Demostración. Sea, $\mathcal{M}(A)$ una F -representación del matroide red (E, \mathcal{I}) . Para cada nodo $s' \neq s$ y cualquier arista $e \in \Gamma_O(s')$, por la definición de \mathcal{I} , se tiene que $\{\Gamma_I(s') \cup e\} \notin \mathcal{I}(1)$. Por la definición del matroide $\mathcal{M}(A)$, para cada $e \in E$, existe un vector columna $f_e \in A$, donde por el numeral (1), $f_e \in \langle f_d : d \in \Gamma_I(s') \rangle$. Por lo anterior, el conjunto $\{f_e : e \in E\}$ forma un código de red F -lineal sobre G_s , que es genérico por el teorema 4.2.8.

El siguiente teorema, permite establecer una cota para la información que ingresa a cualquier nodo en una red. Además, es el punto de partida para introducir otro tipo de códigos lineales, que son importantes en las aplicaciones. Para profundizar en esta dirección, se recomienda la lectura de la sección 19.3 de [8].

Teorema 4.2.10[8] Sean, L un código de red F -**Lineal** sobre G_s y $T \subseteq V$, tal que $s \notin T$. Entonces, $\dim(V_T) \leq \min\{w, \maxflow(T)\}$.

Demostración. Sea, U un corte entre s y T . Ya que L es un código de red F -**Lineal**, entonces $\dim(V_T) \leq \dim(V_{E_U}) \leq |E_U|$. Al aplicar el teorema de corte mínimo y flujo máximo (pg 423, [8]), al corte mínimo entre s y T , se tiene que $\dim(V_{E_U}) \leq \maxflow(T)$. Además, por la definición de L , V_T es combinación lineal de $V_s = F^w$. Por lo tanto, $\dim(V_T) \leq \dim(V_s) = w$.

La siguiente definición es una consecuencia del anterior teorema.

Definición 4.2.11 Sea, $G_s = (V, E, s)$ un digrafo. Un código de red F -**Lineal** es una **dispersión lineal**, si $\dim(V_T) = \min\{w, \maxflow(T)\}$, para todo $T \subseteq V$, donde $s \notin T$.

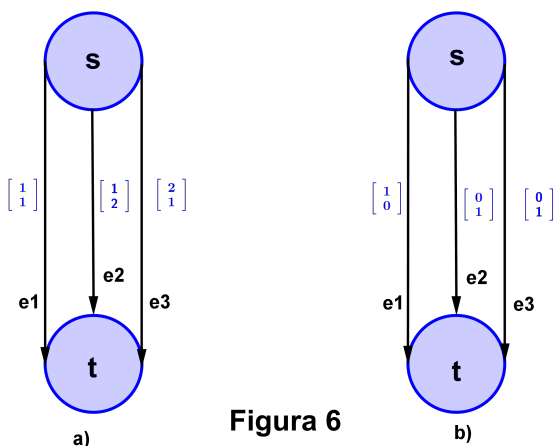
Teorema 4.2.12[5] Sean, $G_s = (V, E, s)$ un digrafo, L un código de red F -**Lineal** y $T \subseteq V$, donde $s \notin T$. El código lineal L es una dispersión lineal, si y sólo si, existe un conjunto regular independiente E_T , donde $E_T = \min(\maxflow(T), w)$ y $\pi_1(e) \in T$, para todo $e \in E_T$.

Demostración. \Rightarrow) : Supongase que $\maxflow(T) = \dim(V_T)$, entonces existe un conjunto de caminos independientes, $\{P_1, \dots, P_{|w_1|}\}$, partiendo de s y terminando en algunos nodos de T , donde $w_1 \leq w$. Sea, E_T el conjunto de las últimas aristas tomadas de cada uno de los caminos P_i , $i = 1, \dots, |w_1|$. Entonces, el conjunto E_T es regular e

independiente.

\Leftarrow) : Supongamos que existe E_T , tal que $|E_T| = \min(\text{maxflow}(T), w)$ y $\pi_1(e) \in T$. Entonces, $\min(\text{maxflow}(T), w) \leq \dim(V_T)$. Por otro lado, por el teorema 4.2.10, $\dim(V_T) \leq \min\{w, \text{maxflow}(T)\}$. Así, $\dim(V_T) = \min\{w, \text{maxflow}(T)\}$.

Ejemplo 4.2.13 La red a) de la figura 6, representa una dispersión lineal que es un código de red genérico. La red b) de la figura 6, representa una dispersión lineal, que no es un código de red genérico. El siguiente teorema establece la relación entre códigos de red genéricos y dispersiones lineales.



Teorema 4.2.14 [5] Sean, $G_s = (V, E, s)$ un digrafo y L un código de red F -Lineal. Si L es código de red genérico, entonces L es una dispersión lineal.

Demostración. Por la hipótesis, el código de red L es genérico, entonces todos los conjuntos independientes son regulares. En particular, los correspondientes conjuntos del teorema 4.2.12 son regulares. Por lo tanto, por la definición 4.2.11, el código L es una dispersión lineal.

4.3. La representación matricial del matroide red

En esta sección, se encuentra la relación entre matroides transversales y el matroide red asociado a un digrafo. Los resultados de la sección son tomados de la referencia [3].

Teorema 4.3.1[3] Sea S un conjunto finito y $\mathcal{A} = \{A_j | j \in J\}$ una familia de subconjuntos de S . El matroide transversal $\mathcal{M} = (S, \mathcal{I}_{\mathcal{A}})$, asociado a la familia \mathcal{A} , es isomorfo a algún matroide red.

Demostración. Sea, $\Delta[\mathcal{A}] = (V, E)$ el grafo bipartito asociado a \mathcal{A} , donde $V = S \cup J$ y $E = \{xj : x \in S, j \in J, \text{ y } x \in A_j\}$. Se define un digrafo (s', t', V', E') sobre $\Delta[\mathcal{A}]$, donde s' es un único nodo fuente, t' es un único nodo receptor, $V' = S \cup J \cup s' \cup t'$ y $E' = \{(s', u) : u \in J\} \cup E \cup \{(v, t') : v \in S\}$. Si el matroide red asociado al digrafo (s', t', V', E') se restringe al conjunto de aristas $\{(x, t') : x \in S\}$, se tiene que el matroide transversal $\mathcal{M} = (S, \mathcal{I}_{\mathcal{A}})$ es isomorfo a dicha restricción.

La figura 7, ilustra la construcción utilizada en la demostración del teorema 4.3.1.

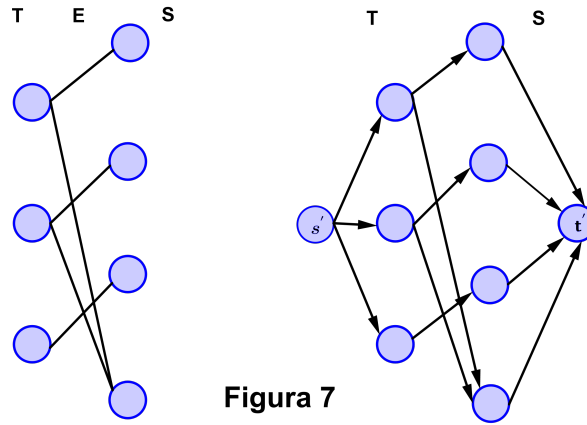


Figura 7

Definición 4.3.2 1. Sea, $G_s = (V, E, s)$ un digrafo. El **grafo bipartito** asociado a G_s , es una tripla (E, T_G, E') , donde:

- (i) $T_G = \{\hat{e}_{\omega+1}, \dots, \hat{e}_{|E|}\} = E - \Gamma_O(s)$.
- (ii) $E' = \{e_i, \hat{e}_i\} \cup \{\{e_i, \hat{e}_j\} : \pi_2(e_i) = \pi_1(e_j)\}$.

2. Sean, $G_s = (V, E, s)$ un digrafo y (E, T_G, E') su grafo bipartito asociado. El **matroide transversal inducido** por (E, T_G, E') , se define como:

- (i) El **soporte** es E .
- (ii) Para cada $\hat{e}_i \in T_G$, $i = \omega + 1, \dots, |E|$, se define $A_i \subseteq E$, tal que $e \in A_i$,

si y sólo si, $\{e, \hat{e}_i\} \in E'$. Los **independientes** se definen como los transversales parciales asociados a la sucesión $\{A_i | \hat{e}_i \in T_G\}$.

Ejemplo 4.3.3 La figura 8, representa un digrafo y su correspondiente grafo bipartito. El matroide transversal asociado, tiene como soporte al conjunto $S = \{e_1, e_2, e_3, e_4, e_5\}$ y como familia asociada, $A_{\hat{e}_3} = \{e_1, e_3, e_5\}$, $A_{\hat{e}_4} = \{e_4\}$ y $A_{\hat{e}_5} = \{e_2, e_5\}$.

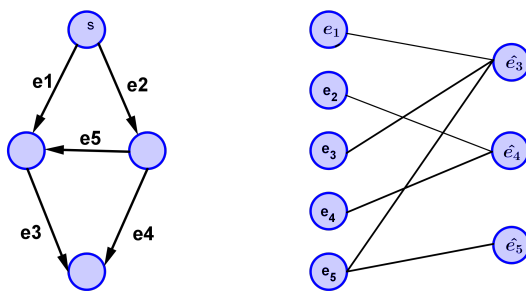


Figura 8

Lema 4.3.4 [3] Sean, $G_s = (V, E, s)$ un digrafo y (E, \mathcal{I}) el matroide red sobre G_s . Un subconjunto $B \subseteq E$ es una base para el matroide red (E, \mathcal{I}) , si y sólo si, en el grafo bipartito (E, T_G, E') , existe una correspondencia entre $E - B$ y T_G .

Demostración. \Rightarrow) : Sea, B una base del matroide red (E, \mathcal{I}) . Por lo tanto, existe un conjunto de caminos independientes por aristas $\{P_1, \dots, P_\omega\}$, donde cada camino P_i , inicia con aristas en $\Gamma_O(s)$ y termina con aristas en B . El siguiente conjunto,

$$M = \left\{ \bigcup_{i=1}^{\omega} \{e_i, \hat{e}_j\} \in E' : (e_i, e_j) \subseteq P_i \right\} \cup \left\{ \{e_k, \hat{e}_k\} \in E' | e_k \notin P_i, \forall i \in \{1, \dots, \omega\} \right\},$$

es una correspondencia de $E - B$ con T_G , ya que, cualquier arista en el digrafo G_s , está en algún camino P_i , $i = 1, \dots, \omega$, ó en ninguno de ellos.

\Leftarrow) : Sea, $B \subseteq E$, tal que el en grafo bipartito (E, T_G, E') , existe una correspondencia M entre $E - B$ y T_G . El siguiente algoritmo define los ω -caminos independientes por aristas desde $\Gamma_O(s) = \{e_1, \dots, e_\omega\}$ hasta las aristas en B .

Algoritmo

```

for  $1 \leq i \leq \omega$ 
{
     $c_i = e_i$ ;
     $P_i = (e_i)$ 
for  $i = 1$  hasta  $\omega$ 
{
    While  $c_i \notin B$ 
    { $P_i$  es un camino desde  $e_i$  hasta  $c_i$ ;
    Encuentre el nodo  $\hat{d}_i$  en  $T_G$ , tal que  $\{c_i, \hat{d}_i\} \in M$ ;
     $c_i = \hat{d}_i$ ;
    Unir camino  $c_i$  al camino  $P_i$ }}

```

Teorema 4.3.5 [3] Sean, $G_s = (V, E, s)$ un digrafo y (E, T_G, E') su grafo bipartito. Además, sea \mathcal{C} la colección de las bases de la matroide transversal inducida por (E, T_G, E') . Entonces, $\mathcal{I} = \{X | X \subseteq E - C, C \in \mathcal{C}\}$ forma el conjunto de los independientes del matroide red (E, \mathcal{I}) .

Demostración. El conjunto $E - \Gamma_O(s)$ es una base del matroide transversal inducido por (E, T_G, E') , entonces $|C| = |E - \Gamma_O(s)|$, para todo $C \in \mathcal{C}$. Lo anterior significa que, existe una correspondencia entre los elementos de \mathcal{C} y el conjunto T_G . Por el lema 4.3.4, cada conjunto de la forma $E - C$, $C \in \mathcal{C}$, es una base para la matroide red (E, \mathcal{I}) . Por lo tanto, cualquier conjunto independiente X del matroide red esta contenido en un conjunto de la forma $X \subseteq E - C$, para algún $C \in \mathcal{C}$.

El teorema 4.3.5 establece un método para construir el matroide red. En efecto, en primer lugar se construye el matroide transversal asociado al digrafo y luego se toma su dual.

Ejemplo 4.3.6 La figura 9, representa un digrafo y su dual. El matroide transversal asociado es: El soporte es $S = \{e_1, e_2, e_3, e_4, e_5\}$, el conjunto de independientes es $\mathcal{I} = \{\{e_1, e_2\}, \{e_1, e_4\}, \{e_1, e_5\}, \{e_3, e_2\}, \{e_3, e_4\}, \{e_3, e_5\}, \{e_3, e_1\}, \{e_5, e_2\}, \{e_4, e_5\}, \{e_1, e_2, e_5\}, \{e_1, e_4, e_5\}, \{e_1, e_2, e_3\}, \{e_3, e_4, e_5\}, \{e_1, e_3, e_5\}, \{e_1, e_4, e_3\}, \{e_3, e_2, e_5\}\}$

Por teorema 4.3.5, el matroide red es: El soporte es $S = \{e_1, e_2, e_3, e_4, e_5\}$ y una base para el matroide red es $\{\{e_3, e_4\}, \{e_1, e_2\}, \{e_2, e_3\}, \{e_2, e_4\}, \{e_4, e_5\}, \{e_2, e_5\}, \{e_4, e_1\}\}$

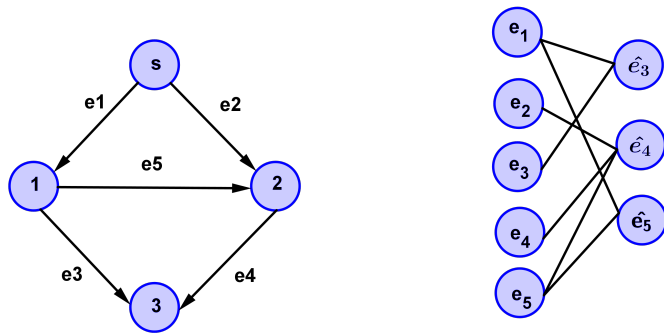


Figura 9

Teorema 4.3.7[3] Sean, $G_s = (V, E, s)$ un digrafo y (E, T_G, E') su grafo bipartito. Sean, $\Gamma_O(s) = \{e_1, \dots, e_\omega\}$ y $E = \{e_1, e_2, \dots, e_{|E|}\}$. Considerese una F -representación para la matroide transversal, inducida a partir del grafo bipartito (E, T_G, E') , en la forma:

$$(1) \left[\begin{array}{c|c} e_1 \dots e_\omega & e_{\omega+1} \dots e_{|E|} \\ \hline D & I_{|E|-\omega} \end{array} \right]$$

donde D es una matriz de tamaño $(|E| - \omega) \times \omega$. Entonces, la matriz,

$$(2) \left[\begin{array}{c|c} e_1 \dots e_\omega & e_{\omega+1} \dots e_{|E|} \\ \hline I_\omega & -D^T \end{array} \right]$$

es una F -representación del matroide red.

Demostración. El conjunto de aristas $\{e_{\omega+1} \dots e_{|E|}\}$, forman una base del matroide

transversal inducida a partir del grafo bipartito (E, T_G, E') . El matroide \mathcal{M} , inducido por el grafo bipartito, tiene una representación de la forma (1). Utilizando el teorema 4.3.5, el matroide red es el dual del matroide transversal inducido por grafo bipartito (E, T_G, E') . Por lo tanto, la representación (2) es una consecuencia del teorema 2.2.8 de la referencia [1].

5 Conclusiones

1. Este trabajo estudia las relaciones existentes, entre los diferentes tipos de matroides, que pueden definirse sobre una red de información y la Teoría de codificación de redes.
2. Un código de red lineal escalar es una solución para una red, si y sólo si, la red es matroidal con matroide representable sobre un cuerpo finito [4]. Este resultado muestra el aporte de los matroides vectoriales a la caracterización de las redes lineales escalares solubles.
3. La noción de matroide estricto es esencial para comprobar que el matroide red es efectivamente un matroide [3].
4. Los teoremas 4.3.1 y 4.3.5 establecen las relaciones entre el matroide red y los matroides transversales. En particular, se encontró una representación matricial del matroide red (Teorema 4.3.7).
5. En el teorema 4.2.8, se establece la relación entre los códigos de red genéricos y el matroide red. En efecto, el matroide vectorial asociada a los códigos de red genéricos coincide con el matroide red.

Las siguientes preguntas podrían generar nuevas investigaciones.

6. Dado un digrafo acíclico es posible construir un álgebra asociada a el [2,pg 41-51]. Si se definen códigos de red lineal escalares, tomando los vectores de arista en el álgebra correspondiente, cuáles problemas de red pueden resolverse con estos códigos?.
7. En [9], se introduce la noción de matroide n-lineal representable. Es posible decidir, si el matroide red es n-lineal representable?
8. El matroide red, se puede definir sobre cualquier digrafo sin restricciones impuestas

sobre él. Si se estudian digrafos cíclicos, que relación existe entre el matroide inducido por los códigos de red asociados al digrafo y el matroide red?

6 Bibliografía

- [1] J. Oxley, *Matroid Theory*. New York: Oxford Univ. Press, 1992
- [2] Ibrahim Assem, Daniel Simson, Andrzej Skowronski, *Elements of Representation Theory of Associative Algebras*. London: London Mathematical Society, Student Texts 65, 2006.
- [3] Qifu Sun, Siu Ho y Shuo-Yen Robert Li, "On Network Matroids and Linear Network Codes," *IEEE International Symposium on Information theory*, pp 1833-1837, Octubre 19. 2008
- [4] Anthony Kim y Muriel Médard, "Scalar-linear Solvability of Matroid Networks Associated with Representable Matroids," *Turbo Codes and Iterative Information Processing*, pp 452-456. 2010.
- [5] Min Tan, Raymond W. Yeung y Siu Ting Ho, "A Unified Framework For Linear Network Codes," *IEEE Trans. Inf Theory*, Vol 57, pp 416-423, Enero. 2011.
- [6] Raymond W. Yeung, "Network Coding: A Historical Perspective," *Proceedings on the IEEE*, vol.99, no. 3, pp 366-372, Marzo. 2011.
- [7] R. Dougherty, C. Freiling y K. Zeger, "Network Coding and Matroid Theory," *Proceedings on the IEEE*, vol.99, no. 3, pp 388-405, Marzo. 2011.
- [8] Raymond W. Yeung, *Information Theory and Network Coding*. New York: Springer Verlag, Mayo, 2011.
- [9] Rubiche C. Juan, "Conexiones entre Codificación de Redes y Codificación de Índices y la Teoría de Matroides," M.Cs. tesis, Universidad Nacional de Colombia, Bogotá, Junio, 2011.