Journal homepage http://revistas.unitru.edu.pe/index.php/SSMM

SELECCIONES MATEMÁTICAS
Universidad Nacional de Trujillo
ISSN: 2411-1783 (Online)
2019; Vol.06(2): 264 - 274.

Problemas de Programación Lineal en Redes de Información y Operadores de Clausura usando Particiones.

Linear Programming Problems in Network Coding and Closure Operators via Partitions.

Victor Peña-Macias* and Humberto Sarria†

Received, Jul. 21, 2019 *Accepted, Set. 24, 2019*

How to cite this article:
Peña, V., Sarria, H. *Problemas de Programación Lineal en Redes de Información y Operadores de Clausura usando Particiones*. Selecciones Matemáticas. 2019; 6(2):264-274. http://dx.doi.org/10.17268/sel.mat.2019.02.12

Resumen

Una red de información es un grafo dirigido acíclico en el cual ciertos nodos llamados fuentes tienen mensajes que desean transmitir a otros nodos llamados receptores a través de la combinación de mensajes en nodos intermedios. El problema de solubilidad consiste en encontrar una colección adecuada de funciones que permita combinar los mensajes en los nodos intermedios para que puedan ser decodificados donde son requeridos. En esta trabajo se estudia el problema de solubilidad fraccional de una red a través de una extensión del problema de solubilidad de un operador de clausura definido por Gadouleau en el 2013. Se definen problemas de programación lineal mediante dicha conexión con operadores de clausura para estudiar la capacidad de una red; usando algunas desigualdades de la información y desigualdades rango lineales dependientes de la característica se obtienen cotas superiores sobre la capacidad lineal de algunas redes y operadores de clausura sobre un cuerpo dado.

Palabras clave. Grafo dirigido, código de red, operador de clausura, matroide representable, desigualdad rango lineal.

Abstract

A network is an acyclic directed graph in which there are sources that have some messages and want to transmit to receivers through the combination of messages in intermediate nodes. The goal is to find a collection of functions that allow to combine messages in order to satisfy the demand of the receivers. In this paper, we study the fractional solvability problem of a network using an extension of the solvability problem in closure operators given by Gadouleau in 2013. We define linear programming problems via the desired extension in order to study capacities; using some information inequalities and characteristic-dependent linear rank inequalities, we obtain upper bounds on linear capacity of some networks and closure operators over some fields.

Keywords. Directed graph, network code, closure operator, representable matroid, linear rank inequality.

1. Introducción. La Teoría de Codificación en Redes, conocida en inglés como *Network Coding*, es una rama de la Teoría de la Información, introducida por Ahlswede et al. en [1], que estudia el problema de flujo de información a través de una red. Una red es un grafo dirigido acíclico en el cual ciertos nodos llamados fuentes tienen ciertos mensajes que están siendo demandados por otros nodos llamados receptores. El problema de la solubilidad de la red, consiste en encontrar una manera eficiente de codificar los mensajes para que puedan ser "combinados" en los nodos intermedios con el fin de que puedan ser decodificados en los nodos receptores donde son requeridos. La colección de funciones que interviene en la codificación se denomina código de la red.

*Departamento de Matemáticas, Facultad de Ciencias, Universidad Nacional de Colombia. (vbpenam@unal.edu.co).
†Departamento de Matemáticas, Facultad de Ciencias, Universidad Nacional de Colombia. (hsarriaz@unal.edu.co).

Es conocido que es suficiente trabajar con redes que tienen la misma cantidad de fuentes y receptores, cada uno demandando mensajes de una fuente distinta, estas redes se llaman redes de uniemisión múltiple. Cuando una red es de uniemisión múltiple, un código de red se puede escribir en términos de particiones, y las relaciones que se deben cumplir entre las funciones se ponen en términos de refinamientos de particiones. Determinar un código de red, o una colección de particiones como la mencionada, puede llegar a ser en general muy complejo, aún si la red tiene una solución. Con el fin de encontrar formas alternativas de estudiar este problema, en [10], Gadouleau conecta la solubilidad de una red con un problema sobre operadores de clausura; introduce un problema que consiste en determinar una colección de particiones cuyos refinamientos se comportan "bien" respecto al operador. Este problema se llama "Solubilidad del Operador de Clausura". Con este procedimiento se logra conectar la solubilidad escalar de los operadores de clausura con la solubilidad escalar de las redes de información. Incluso se conecta con ciertos matroides muy importantes en esquemas de repartición de secretos en Criptología [3, 17, 18].

En este trabajo, se extiende el concepto de solubilidad de un operador de clausura de Gadouleau [10] a lo que se ha denominado la solubilidad fraccional de un operador de clausura. Dicha extensión permite conectar la solubilidad fraccional de una red de información con el problema de solubilidad fraccional del operador de clausura asociado a la red. Permite introducir una serie de problemas de programación lineal asociados al operador cuyas soluciones son cotas superiores de la capacidad de solubilidad fraccional de este operador. Los problemas son estudiados sobre algunos tipos de matroides y redes de información, evaluando sus capacidades sobre algunos alfabetos y cuerpos finitos. Además, con ayuda de algunas de las desigualdades rango lineales dependientes de característica introducidas en [15] y [8] se determinan cotas superiores de algunas capacidades lineales.

2. Particiones y entropía. Un conjunto finito $\mathcal{A}$ con al menos dos elementos, se llama *alfabeto*. Una partición del conjunto $\mathcal{A}^t$, $t \in \mathbb{N}$, se nota como $\bar{f}$. Sus bloques se notan por $P_i\left(\bar{f}\right)$. El *refinamiento común* de dos particiones $\bar{f}$ y $\bar{g}$, es la partición $\bar{f} \wedge \bar{g}$ dada por $\left\{P_i\left(\bar{f}\right) \cap P_j\left(\bar{g}\right) : P_i\left(\bar{f}\right) \cap P_j\left(\bar{g}\right) \neq \phi\right\}$. La colección de particiones de $\mathcal{A}^t$ con la operación refinamiento común es un semiretículo acotado, donde $E_{\mathcal{A}^t}$, la partición de $|\mathcal{A}|^t$-bloques, es el mínimo; y $\{\mathcal{A}^t\}$, la partición de un solo bloque, es el máximo. Naturalmente, se tiene un orden parcial en el cual $\bar{f} \leq \bar{g}$ si $\bar{f} \wedge \bar{g} = \bar{f}$. Para cualquier $X \subseteq [m] := \{1, \ldots, m\}$, el refinamiento común de toda partición $\bar{f}_v$, con $v \in X$, es $\bar{f}_X := \bigwedge_{v \in X} \bar{f}_v$. Observe que $\bar{f}_\emptyset := \{\mathcal{A}^t\}$; $\bar{f}_{X \cup Y} = \bar{f}_X \wedge \bar{f}_Y$; $\bar{f}_{X \cup Y} \leq \bar{f}_{X \cap Y}$; $\bar{f}_Y \leq \bar{f}_X$, si $X \subseteq Y$.

La *entropía* de $\bar{f}$ se define como:

$$\mathrm{H}\left(\bar{f}\right) := -\sum_i \frac{\left|P_i\left(\bar{f}\right)\right|}{|\mathcal{A}|^t} \log_{|\mathcal{A}|} \frac{\left|P_i\left(\bar{f}\right)\right|}{|\mathcal{A}|^t}.$$

Ciertamente una partición de $\mathcal{A}^t$ define una variable aleatoria $X_{\bar{f}}$ sobre $\bar{f}$ con distribución de probabilidad

$$\mathrm{p}\left(X_{\bar{f}} = i\text{-bloque}\right) = \frac{\left|P_i\left(\bar{f}\right)\right|}{|\mathcal{A}|^t}.$$

La variable aleatoria conjunta $\left(X_{\bar{f}}, X_{\bar{g}}\right)$ es dada por $X_{\bar{f} \wedge \bar{g}}$. Puesto que la diferencia entre la entropía de una partición y la entropía de su variable aleatoria es un cambio de base en el logaritmo (en Teoría de la Información se toma de base 2), se puede deducir que cualquier desigualdad de la información es una desigualdad válida para entropías de particiones.

En este documento se trabaja con familias de m particiones sobre una potencia $\mathcal{A}^t$ tal que cada una de ellas tiene a lo sumo $|\mathcal{A}|^n$-bloques, para algún n fijo, éstas son notadas como una tupla $\bar{\mathcal{F}} := \left(\bar{f}_v\right)_{v \in [m]}$. La razón de tomar cada partición con a lo sumo $|\mathcal{A}|^n$ bloques, es porque ésta se puede ver como la partición de preimágenes de una función $f : \mathcal{A}^t \to \mathcal{A}^n$, esto es, $\bar{f} = \left\{f^{-1}(x) : x \in f\left(\mathcal{A}^t\right)\right\}$. Esta partición se llama *kernel* de f, y se nota como $\ker(f) := \bar{f}$.

La entropía de $\bar{f}_X$ se nota

$$\mathrm{H}_{\bar{\mathcal{F}}}(X) := \mathrm{H}\left(\bar{f}_X\right),$$

el subíndice $\bar{\mathcal{F}}$ se omite cuando no hay confusión. Esto define una función $\mathrm{H} : 2^{[m]} \to \mathbb{R}$ que satisface las siguientes desigualdades:

- $0 \leq \mathrm{H}(v) \leq \log_{|\mathcal{A}|} \left|\bar{f}_v\right| \leq t$. Se cumple la igualdad en el medio si, y sólo si, $\bar{f}_v$ posee bloques uniformes.
- $\mathrm{H}(X) \leq n\,|X|$.
- $\mathrm{H}(X) \leq \mathrm{H}(Y)$ si $X \subseteq Y$ (*no decreciente*).
- $\mathrm{H}(X \cup Y) + \mathrm{H}(X \cap Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$ (*submodularidad*).

Es bien conocida la relación entre la dimensión de sumas de espacios vectoriales y cierta clase de variables aleatorias asociadas a ellos. Nótese que la diferencia entre la dimensión de un espacio vectorial y la entropía de su variable aleatoria, es un cambio de base del logaritmo [19]. Las desigualdades satisfechas por estas dimensiones son conocidas como *desigualdades rango lineales*.Toda desigualdad de la información es una desigualdad rango lineal [19]. Cuando la veracidad de la desigualdad depende de la característica del cuerpo en donde están definidos los espacios vectoriales, éstas se conocen como *desigualdades rango lineales dependientes de la característica* [8, 15, entre otros]. A continuación se presentan dos de ellas; para simplificar la escritura, se usa la notación $A_{[i]} = \{A_1, \ldots, A_i\}$ y $A_X = \{A_i : i \in X\}$.

Teorema 1. *[15, ejemplo 2: n=7, t=2] Para cualesquiera A_1, A_2, A_3, B_1, B_2, B_3, C subespacios de un espacio vectorial de dimensión finita V sobre un cuerpo escalar finito $\mathbb{F}$. Se verifica:*

(a) Si la característica de $\mathbb{F}$ es 2,

$$\mathrm{H}\left(B_{[3]}\right) \leq 2\mathrm{I}\left(A_{[3]}; C\right) + 3\left(\mathrm{H}\left(C \mid A_{[3]}\right) + \sum_{i=1}^{3} \mathrm{I}\left(A_{[3]-i}; C\right)\right)$$

$$+ \sum_{i=1}^{3} \left(\mathrm{H}\left(B_i \mid A_{[3]-i}\right) + \mathrm{H}\left(B_i \mid A_i, C\right) + \mathrm{I}\left(A_{[i]}; A_{[3]-[i]}\right) + \mathrm{I}\left(A_{[i-1]}; A_i\right)\right).$$

(b) Si la característica de $\mathbb{F}$ es distinta de 2,

$$\mathrm{H}\left(C\right) \leq \frac{1}{3}\mathrm{H}\left(B_{[3]}\right) + \mathrm{H}\left(C \mid A_{[3]}\right) + \sum_{i=1}^{3} \mathrm{I}\left(A_{[3]-i}; C\right)$$

$$+ \sum_{i=1}^{3} \left(\mathrm{H}\left(B_i \mid A_{[3]-i}\right) + \mathrm{H}\left(C \mid A_i, B_i\right) + \mathrm{I}\left(A_{[i]}; A_{[3]-[i]}\right) + \mathrm{I}\left(A_{[i-1]}; A_i\right)\right).$$

Las desigualdades en general no se cumplen sobre cuerpos de cualquier otra característica diferente a la mencionada.

Cuando cada miembro de $\bar{\mathcal{F}}$ es el kernel de una transformación lineal sobre un cuerpo finito $\mathbb{F}$ (i.e. la partición dada por el espacio vectorial cociente del dominio de la función con su núcleo), H define una función conocida como polimatroide lineal. Es conocido que los polimatroides lineales satisfacen todas las desigualdades rango lineales [**?**, capítulo 3]. En particular, un polimatroide lineal sobre $\mathbb{F}$, satisface toda desigualdad rango lineal dependiente de la característica valida sobre $\mathbb{F}$. Por lo tanto, las desigualdades del Teorema 1 se cumplen cuando $\bar{\mathcal{F}}$ está definido por 7 particiones en la que cada una es el kernel de una transformación lineal sobre un cuerpo de característica 2, y sobre un cuerpo de característica distinta de 2, respectivamente.

2.1. Redes de información. Un *dígrafo* es un par $D := ([m], E)$, donde $E \subseteq [m]^2$. Los elementos de $[m]$ se llaman *nodos* del dígrafo; los pares de E se llaman *aristas* y se denotan por $e = uv$, donde u y v son nodos. Defina $v^- := \{u \in [m] : uv \in E(D)\}$, y para cada $X \subseteq [m]$, $X^- := \bigcup_{v \in X} v^-$. De forma análoga, se define $v^+ := \{u \in [m] : vu \in E(D)\}$ y $X^+ := \bigcup_{v \in X} v^+$. Un nodo v se dice *intermedio*, si $v^-, v^+ \neq \emptyset$; un nodo s se dice *fuente*, si $s^- = \emptyset$; un nodo t se dice *receptor*, si $t^+ = \emptyset$. Un *camino* de u a v, es una sucesión de vértices $v_1, ..., v_k$ tales que $v_i v_{i+1} \in E$, donde $i = 1, ..., k-1$, $v_1 = u$ y $v_k = v$. Un *ciclo* es un camino, tal que $v_1 = v_k$. Un dígrafo es *acíclico*, si no tiene ciclos. Un dígrafo acíclico posee al menos una fuente y un receptor; el conjunto de fuentes se nota como S, y el conjunto de receptores se nota como T.

Definición 1. *Una* red*, es un par $\mathcal{N} = (D, \tau)$, donde $D = ([m], E)$ es un dígrafo acíclico y $\tau : T \to S$ es una función sobreyectiva, llamada función de demanda.*

Una red $\mathcal{N}$ es una *red de uniemisión múltiple*, si su función de demanda es biyectiva. En tal caso, $\tau(t_i) = s_i$, para $i = 1, \ldots, r := |S|$, y se escribe $\mathcal{N} = (D, S, T)$. Es conocido que estudiar la solubilidad de un red cualquiera, es equivalente a estudiar la solubilidad de una red de uniemisión múltiple asociada [9]. Por consiguiente, a menos que se diga lo contrario, se asume que todas las redes son de uniemisión múltiple.

Definición 2. *Un (k, n)-código de red de $\mathcal{N}$ sobre un alfabeto $\mathcal{A}$ es una colección de funciones $\mathcal{F} = (f_v)_{v \in [m]}$ de la forma $f_s : \mathcal{A}^{|S|k} \to \mathcal{A}^k$, si $v = s \in S$; $f_v : \mathrm{Im} f_{v^-} \subseteq \mathcal{A}^{|v^-|} \to \mathcal{A}^n$, donde $\mathrm{Im} f_{v^-} := \mathrm{Im} f_{v_1} \times \cdots \times \mathrm{Im} f_{v_l}$, $v^- = \{v_1, ..., v_l\}$, si $v \in [m] - S - T$; $f_t : \mathrm{Im} f_{t^-} \to \mathcal{A}^k$, si $v = t \in T$.*

Un *mensaje* es un elemento de $\mathcal{A}^k$. Se toma una tupla de mensajes $x \in \mathcal{A}^{|S|k}$. A cada nodo fuente, se le asocia una componente de $\mathcal{A}^{|S|k}$, de modo que si $S = \{s_1, ..., s_{|S|}\}$, cada tupla de mensajes se escribe como $x = (x_{s_1}, ..., x_{s_{|S|}}) := (x_1, ..., x_{|S|})$, donde cada x_i es el mensaje de s_i. Las funciones f_t, $t \in T$ se denominan funciones de decodificación. Un (k, n)-código de red es lineal, si cada una de sus funciones es una función lineal.

En la literatura existen varias definiciones de código de red [1, 5, 10, 16]. En algunos documentos se asignan las funciones del código a nodos fuentes, a cada arista y a los nodos receptores. En este documento, se ha preferido tomar el modelo de asignar una función a cada nodo de la red, de modo que cada nodo transmite el mismo mensaje a cada una de sus aristas de salida; en este modelo se dice que la red está en *circuito de representación* [16]. Elegir este modelo no ofrece ninguna diferencia significativa respecto al otro mas que simplificar la escritura. La función asignada a cada fuente es simplemente un formalismo que se debe introducir para conectar con particiones [10]; el mensaje que desea transmitir una fuente debe ser visto como el mensaje que se obtiene de esta función. Lo que obliga la restricción $k \leq n$, porque cada fuente debe transmitir su mensaje completo. En la literatura, las redes "interesantes" cumplen esta condición. Por [5, Lema II.1], una condición suficiente para garantizar su cumplimiento, consiste en considerar redes en las cuales existe al menos una fuente y un receptor que son conectados por un único camino; por ejemplo, la red de la figura 2.1. En adelante todas las redes cumplen esta condición, y por consiguiente $k \leq n$.

El hecho de que el dominio de la función asignada a cada vértice dependa de las imágenes de las funciones asignadas a sus vértices de entrada aclara la idea de lo que es transmitir o combinar información a lo largo de la red. La siguiente definición auxiliar captura esta idea.

Definición 3. *El* código acumulativo *de un (k, n)-código de red $\mathcal{F}$, es una colección de funciones $\mathcal{F}^* = (f_v^*)_{v\in[m]}$ de la forma $f_s^* := f_s$, si $v = s \in S$; $f_v^*(x) := f_v\left(f_{v^-}^*(x)\right) := f_v\left((f_w^*(x))_{w\in v^-}\right)$ para cada $x \in \mathcal{A}^{|S|k}$, si $v \in [m] - S$.*

Cada f_v^* se define de manera inductiva a partir de cada nodo de v^-, por ejemplo, para cada $v^- \subseteq S$ definimos f_v^*. Luego pasamos a los f_u^* tales que cada función correspondiente a cada nodo de u^- ya está definida. Se aplica éste proceso hasta finalizar con los nodos receptores. De este modo, el mensaje que transmite un nodo v se obtiene calculando f_v^* para determinada tupla de mensajes x.

Definición 4. *Un (k, n)-código de red es una* solución fraccional *de $\mathcal{N}$ sobre $\mathcal{A}$, si para cualquier tupla de mensajes $x = (x_1, ..., x_{|S|}) \in \mathcal{A}^{|S|k}$, existe un $y \in \mathcal{A}^{|S|k}$ tal que $f_{\tau(t)}^*(y) = f_t^*(y) = x_{\tau(t)}$, $\forall t \in T$.*

Observaciones:

- Cuando existe tal solución con $k = n = 1$, se dice que la red es *soluble* sobre $\mathcal{A}$. Si la solución es lineal, se dice que la red es linealmente soluble sobre $\mathcal{A}$ (que en este caso es un cuerpo finito).
- Si la red tiene una solución fraccional, a partir de ésta siempre se puede construir una solución tal que $f_S^* = \mathrm{id}_{\mathcal{A}^{rk}}$, o lo que es lo mismo $x = y$ en la definición 4.
- En la práctica, dado un vector mensaje x, cada s desea enviar el mensaje x_s a un t tal que $\tau(t) = s$. Con el fin de que t recupere el mensaje requerido, una solución debe permitir tomar un y' tal que $f_s^*(y') = x_s$ y $f_t^*(y') = x_s$. Esto se debe cumplir simultáneamente para todo s, en una solución siempre es posible, pues debe existir un y (necesariamente único) tal que $f_s^*(y) = f_t^*(y) = x_s$, para cualquier t.
- Cuando $\mathcal{N}$ es de uniemisión múltiple, un código es una solución, si para todo $x = (x_1, ..., x_r) \in \mathcal{A}^r$, existe un $y \in \mathcal{A}^r$ tal que $f_{t_i}^*(y) = x_i$ para cualquier $i = 1, ..., r$. En otras palabras, f_S^* es biyectiva y $f_T^* = f_S^*$.

La capacidad de $\mathcal{N}$ relativa a una clase de códigos $\mathcal{D}$ sobre $\mathcal{A}$ es dada por

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathcal{N}) := \sup\left\{\frac{k}{n} : \text{existe una } (k, n)\text{-solución fraccional en } \mathcal{D} \text{ sobre } \mathcal{A}\right\}.$$

La clase $\mathcal{D}$ usualmente se toma como la clase de todos los códigos sobre un alfabeto, en tal caso la capacidad se nota por $\mathrm{C}^{\mathcal{A}}(\mathcal{N})$; si se toma sobre cualquier alfabeto se omite el superíndice. Cuando los códigos son lineales se nota como $\mathrm{C}_{\text{lineal}}(\mathcal{N})$; y se coloca el superíndice $\mathbb{F}$ si se quiere especificar el cuerpo finito. Se verifica que

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathcal{N}) \leq \mathrm{C}_{\mathcal{D}}(\mathcal{N}) \leq \mathrm{C}(\mathcal{N}) \leq 1.$$

Calcular la capacidad de una red, en general es muy complejo. Las desigualdades de la información juegan un papel importante para su cálculo [5, 6]. El problema de solubilidad de una red consiste en encontrar soluciones con tasas eficientes, en el sentido que $\frac{k}{n}$ coincida o sea lo más próximo a la capacidad de la red en cuestión. De igual modo las desigualdades rango lineales son importantes para el problema de solubilidad lineal de una red.

En adelante, todas las redes son redes de uniemisión múltiple. Se asume que los nodos de la red están ordenados de tal manera que los r primeros nodos corresponden a fuentes y los r últimos corresponden a receptores, y por simplicidad cada receptor t_i, se nota como s_i'.

A continuación, se escribe la solubilidad de la red en términos de particiones:

Proposición 1. *Tome $\mathcal{F} = (f_v)_{v\in[m]}$ una (k, n)-solución fraccional de $\mathcal{N}$, y defina $\bar{f}_v := \ker(f_v^*)$ para cada v. Entonces,*

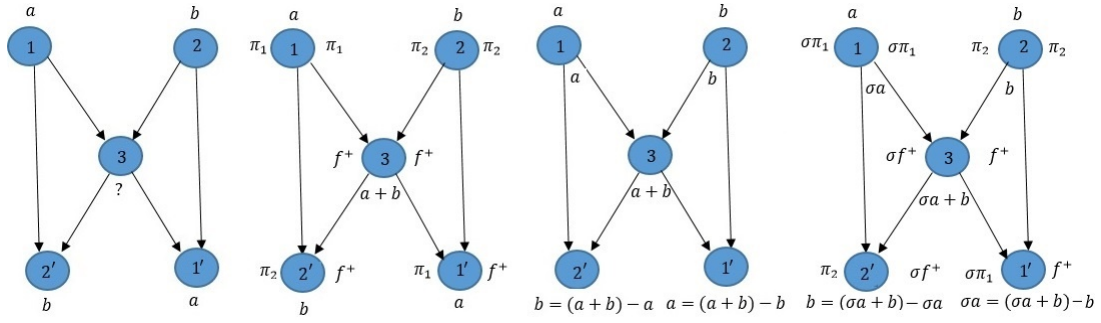

FIGURA 2.1. *De izquierda a derecha: la red Mariposa; código de red y código acumulativo; flujo de información de una solución; solución no lineal alternativa.*

(i) $\bar{f}_v$ *posee a lo sumo* $|\mathcal{A}|^n$*-bloques, para cada* v.
(ii) $\bar{f}_{s_i} = \bar{f}_{t_i}$, *para cada* $i = 1$.
(iii) $\bar{f}_{v^-} \leq \bar{f}_v$ *para cada* $v \in [m] - S$.
(iv) $\bar{f}_T = E_{\mathcal{A}^{rk}}$.

Demostración: (i), (ii) y (iv) son evidentes. Para probar (iii), considere $x_{v^-} \in f^*_{v^-}\left(\mathcal{A}^{rk}\right)$. Tome $y \in f^{*-1}_{v^-}(x_{v^-})$, se tiene que $f^*_{v^-}(y) = x_{v^-}$, entonces $f^*_v(y) = f_v\left(f^*_{v^-}(y)\right) = f_v(x_{v^-})$. Defina $x_v := f_v(x_{v^-})$, se tiene que $y \in f^{*-1}_v(x_v)$, es decir, $f^{*-1}_{v^-}(x_{v^-}) \subseteq f^{*-1}_v(x_v)$. Se sigue $\bar{f}_{v^-} \leq \bar{f}_v$. □

La siguiente afirmación está asociada a la proposición anterior; nótese que se han agregado una condiciones con el fin de obtener un resultado recíproco".

Proposición 2. *Sea* $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v\in[m]}$ *una colección de particiones sobre* $\mathcal{A}^{rk}$ *tal que*

(i) *cada* $\bar{f}_v$ *posee a lo sumo* $|\mathcal{A}|^n$*-bloques.*
(ii) $\bar{f}_{s_i} = \bar{f}_{t_i}$ *para cada* $i = 1, ..., r$.
(iii) $\bar{f}_{v^-} \leq \bar{f}_v$ *para cada* $v \in [m] - S$.
(iv) $\bar{f}_T = E_{\mathcal{A}^{rk}}$.

Sea $\mathcal{F}^* = (f^*_v)_{v\in[m]}$ *cualquier colección de funciones de* $\mathcal{A}^{rk}$ *en* $\mathcal{A}^n$, *tales que* $ker\,(f^*_v) = \bar{f}_v$, $\ker\left(f^*_{t_i}\right) = \bar{f}_{t_i}$, $f^*_{s_i} = f^*_{t_i}$ *para todo* $v \in [m] - S$, $i = 1, ..., r$. *Entonces, existe una* (k, n)*-solución fraccional* $\mathcal{F} = (f_v)_{v\in[m]}$ *de* $\mathcal{N}$ *sobre* $\mathcal{A}$ *cuyo código acumulativo coincide con* $\mathcal{F}^*$.

Demostración: La condición (i) permite definir cada f^*_v como una función de $\mathcal{A}^{rk}$ en $\mathcal{A}^n$. Para cada $v \in [m] - S$, la condición (iii) dice que $\ker\left(f^*_{v^-}\right) \leq \ker\left(f^*_v\right)$, esto es, dado $x_{v^-} \in f^*_{v^-}\left(\mathcal{A}^{rk}\right)$, existe un único $x_v \in f^*_v\left(\mathcal{A}^{rk}\right)$ tal que $f^{*-1}_{v^-}(x_{v^-}) \subseteq f^*_v(x_v)$. Para cada $v \in [m] - S$, defina $f_v(x_{v^-}) := x_v$, note que f_v es una función definida de $\mathrm{Im} f_{v^-} \subseteq \mathcal{A}^{|v^-|}$ en $\mathcal{A}^n$ que satisface $f^*_v(x) = f_v\left(f^*_{v^-}(x)\right)$ para cada $x \in \mathcal{A}^{rk}$. Haciendo $f_s := f^*_s$ para cada $s \in S$; resulta que el código de acumulación de $\mathcal{F} = (f_v)_{v\in[m]}$ es $\mathcal{F}^* = (f^*_v)_{v\in[m]}$. Las condiciones (ii) y (iv) dicen que f^*_S es biyectiva. Por lo tanto, $\mathcal{F}$ es una (k, n)-solución fraccional de $\mathcal{N}$ sobre $\mathcal{A}$. □

ejemplo 1. *En la figura 2.1 (izquierda) se presenta una red conocida como la red Mariposa. Seguido se presenta una solución en un alfabeto* $\mathbb{Z}_2$ *con su código acumulativo, donde* f^+ *simboliza la suma,* π_i *simboliza la* i*-proyección sobre* $\mathbb{Z}_2^2$. *Los códigos de* $\mathcal{F}$ *se presentan a la derecha de cada nodo; los códigos de* $\mathcal{F}^*$ *se presentan a la izquierda; y en la parte de abajo de cada nodo, el mensaje que ellos transmiten. En la tercera imagen se presenta el flujo de información de la red. En la figura de la derecha se presenta una solución no lineal alternativa, donde* σ *es una permutación de* $\mathbb{Z}_2$. *Uno puede verificar que estas soluciones producen la misma colección de particiones:* $\bar{f}_1 := \{\{(0,0),(0,1)\},\{(1,0),(1,1)\}\}$, $\bar{f}_2 := \{\{(0,0),(1,0)\},\{(0,1),(1,1)\}\}$ *y* $\bar{f}_3 := \{\{(0,0),(1,1)\},\{(0,1),(1,0)\}\}$. *Para más detalles véase [14].*

2.2. Operadores de clausura. Los operadores de clausura abundan en la literatura, aparecen en Álgebra como la subestructura generada de un subconjunto de una estructura algebraica (sea grupo, anillo, espacio vectorial, etc); Topología como el operador de clausura topológica; entre otras ramas de las matemáticas [4]. Un *operador de clausura sobre* m elementos es una aplicación $\mathrm{cl} : 2^{[m]} \to 2^{[m]}$ tal que para cualesquier par de conjuntos $X, Y \subseteq [m]$ se satisfacen las siguientes propiedades:

- $X \subseteq \mathrm{cl}(X)$.
- Si $X \subseteq Y$, entonces $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$
- $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.

El *rango* de cl es

$$r_{\mathrm{cl}} := min\{|X| : \mathrm{cl}(X) = [m]\},$$

para evitar confusión se escribe simplemente r. Una base de cl es un subconjunto de tamaño r cuya clausura es $[m]$.

Definición 5. *Una (k,n)-solución de particiones (o solución fraccional de particiones) de cl sobre un alfabeto $\mathcal{A}$, es una familia $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v\in[m]}$ de particiones de $\mathcal{A}^{rk}$, con a lo sumo $|\mathcal{A}|^n$-bloques cada una, tal que $\bar{f}_{\mathrm{cl}(X)} = \bar{f}_X$, para todo $X \subseteq [m]$ y $\bar{f}_{[m]} = E_{\mathcal{A}^{rk}}$.*

No es difícil ver que $k \leq n$. En caso de que exista una solución con $k = n = 1$, se dice que cl es un operador de clausura *soluble* sobre $\mathcal{A}$, [10]. La capacidad de cl relativa a una clase de particiones $\mathcal{D}$ sobre $\mathcal{A}$ está dada por

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathrm{cl}) := \sup\left\{\frac{k}{n} : \text{existe una } (k,n)\text{-solución de particiones en } \mathcal{D} \text{ sobre } \mathcal{A}\right\}.$$

La clase $\mathcal{D}$ usualmente se toma como la clase de todos las particiones sobre una potencia de $\mathcal{A}$, en tal caso la capacidad se nota por $\mathrm{C}^{\mathcal{A}}(\mathrm{cl})$; y si se toma sobre cualquier alfabeto se omite el superíndice. La clase $\mathcal{D}$ también se puede tomar como la clase de todos los kernel de transformaciones lineales sobre un cuerpo finito $\mathbb{F}$, en cuyo caso se nota $\mathrm{C}_{\text{lineal}}^{\mathbb{F}}(\mathrm{cl})$. Algunas desigualdades que consideran la capacidad son:

$$\mathrm{C}_{\mathcal{D}}^{\mathcal{A}}(\mathrm{cl}) \leq \mathrm{C}_{\mathcal{D}}(\mathrm{cl}) \leq \mathrm{C}(\mathrm{cl}) \leq 1.$$

La función de entropía de una solución satisface:

- $\mathrm{H}(v) \leq n$, para cada v.
- $\mathrm{H}(X) = \mathrm{H}(\mathrm{cl}(X))$, para cada X.
- $\mathrm{H}(V) = rk$.

ejemplo 2. *Considere el operador de clausura sobre 3 elementos dado por $U_{2,3}(X) = X$, si $|X| \leq 2$ y $U_{2,3}(X) = [3]$ de otro modo. Tome $\mathcal{A} = \{0,1\}$. Tome como $\bar{\mathcal{F}}$ las tres particiones dadas en el ejemplo 1. Resulta que $\bar{f}_{1,2} = \bar{f}_{U_{2,3}(1,2)} = \bar{f}_{1,3} = \bar{f}_{U_{2,3}(1,3)} = \bar{f}_{2,3} = \bar{f}_{U_{2,3}(2,3)} = \bar{f}_{1,2,3} = E_{\mathcal{A}^2}$, así $\bar{\mathcal{F}}$ es una $(1,1)$-solución de particiones de $U_{2,3}$ sobre $\mathcal{A}$. Luego $U_{2,3}$ es soluble.*

Dentro de la colección de operadores de clausura sobre m se puede definir una relación de orden parcial, dada por: $\mathrm{cl}_1 \leq \mathrm{cl}_2$ si, y sólo si, $\mathrm{cl}_1(X) \subseteq \mathrm{cl}_2(X)$ para cualquier subconjunto X. A continuación, se presenta otra versión de la proposición 2 de [10], cuya prueba es sencilla.

Proposición 3. *Sean cl_1, cl_2 operadores de clausura de rango r sobre m elementos. Si $\mathrm{cl}_1 \leq \mathrm{cl}_2$, y cl_2 tiene una (k,n)-solución fraccional de particiones sobre un alfabeto $\mathcal{A}$, entonces cl_1 tiene la misma solución fraccional de particiones sobre $\mathcal{A}$.*

2.3. Problemas de programación lineal. En esta sección, se define un problema de programación lineal asociado a un operador de clausura con el fin de calcular cotas superiores sobre la capacidad del operador.

Problema 1. *Dado un operador de clausura cl sobre m elementos. Maximizar $z_{[m]}$ sujeto a que la tupla $(z_X)_{X\subseteq[m]}$ cumpla:*

(i) $z_v \leq \frac{1}{r}$ *para cada v.*
(ii) $z_X = z_{\mathrm{cl}(X)}$ *para cada X.*
(iii) $z_X \leq z_Y$, *si $X \subseteq Y$.*
(iv) $z_{X\cup Y} + z_{X\cap Y} \leq z_X + z_Y$.
(v) *Desigualdades adicionales validas sobre $\mathcal{A}$.*
La solución optima del problema se denota por $\mathrm{B}_{(v)}(\mathrm{cl})$.

Se tiene que $\mathrm{B}_{(\mathrm{v})}(\mathrm{cl}) \leq 1$, por ser $z_{[m]} = z_B \leq \sum_{b\in B} z_b \leq \frac{|B|}{r} = 1$, donde B es una base de cl.

Cuando $\bar{\mathcal{F}}$ es una (k,n)-solución de particiones de cl y (v) no define una desigualdad, se puede verificar que $z_X = \frac{1}{rn}\mathrm{H}(X)$ cumple todas las condiciones del problema descrito. De modo que $z_{[m]} = \frac{k}{n}$, por lo que $\mathrm{B}(\mathrm{cl})$ es una cota superior sobre la capacidad de cl.

Antes de continuar, conviene usar la siguiente notación:

- $z_{X|Y} = z_{X\cup Y} - z_Y$;
- $z_{X;Y} = z_X + z_Y - z_{X\cup Y}$.

Las desigualdades del Teorema 1 pueden escribirse de las siguientes formas:

$$z_{B_{[3]}} \leq 2z_{A_{[3]};C} + 3\left(z_{C|A_{[3]}} + \sum_{i=1}^{3} z_{A_{[3]-i};C}\right) + \sum_{i=1}^{3}\left(z_{B_i|A_{[3]-i}} + z_{B_i|A_i,C} + z_{A_{[i]};A_{[3]-[i]}} + z_{A_{[i-1]};A_i}\right); \tag{2.1}$$

$$z_C \leq \frac{1}{3}z_{B_{[3]}} + z_{C|A_{[3]}} + \sum_{i=1}^{3}\left(z_{A_{[3]-i};C} + z_{B_i|A_{[3]-i}} + z_{C|A_i,B_i} + z_{A_{[i]};A_{[3]-[i]}} + z_{A_{[i-1]};A_i}\right). \tag{2.2}$$

Estas restricciones pueden ser añadidas al numeral (v) del problema 1. Al añadir la primera restricción, se obtiene un problema de programación lineal en el cual la solución optima, denotada por

$$\mathrm{B}_{\text{lineal}}^{\text{char}(\mathbb{F})=2}(\mathrm{cl}),$$

es una cota superior de $\mathrm{C}_{\text{lineal}}^{\text{char}(\mathbb{F})=2}(\mathrm{cl})$. De forma análoga, al añadir la segunda restricción,

$$\mathrm{B}_{\text{lineal}}^{\text{char}(\mathbb{F})\neq 2}(\mathrm{cl}),$$

es una cota superior de $\mathrm{C}_{\text{lineal}}^{\text{char}(\mathbb{F})\neq 2}(\mathrm{cl})$.

Nótese que más desigualdades o restricciones pueden ser añadidas a los problemas de programación lineal con el fin de mejorar las cotas superiores que producen.

2.4. Matroides. La teoría de matroides fue creada para capturar la noción de independencia lineal de un espacio vectorial [13]. Un *matroide* es un operador de clausura que satisface la siguiente propiedad:

- para cualesquier $u, v \in [m]$ y $X \subseteq [m]$, si $u \in \mathrm{cl}(X \cup v) - \mathrm{cl}(X)$, entonces $v \in \mathrm{cl}(X \cup u)$.

Una forma alternativa de definir un matroide consiste en tomar un par ordenado $\mathcal{M} = ([m], \mathcal{I})$, donde $\mathcal{I}$ es una colección de subconjuntos de $[m]$, de modo que satisfaga las siguientes propiedades:

- $\emptyset \in \mathcal{I}$.
- Si $I \in \mathcal{I}$, $J \subseteq I$, entonces $J \in \mathcal{I}$.
- Si $I, J \in \mathcal{I}$, $|J| + 1 = |I|$, entonces existe un $v \in I - J$, tal que $J \cup v \in \mathcal{I}$.

Un subconjunto X es *independiente*, si $X \in \mathcal{I}$. De otro modo, se dice que X es un conjunto *dependiente*. Una *base* $\mathcal{B}$ de $\mathcal{M}$ es un conjunto independiente maximal de $\mathcal{M}$. Un *circuito* $\mathcal{C}$, es un conjunto dependiente minimal de $\mathcal{M}$. La función rango de un matroide $\mathcal{M}$, es la aplicación $r_{\mathcal{M}} : 2^{[m]} \to \mathbb{N}$, definida por la igualdad $r_{\mathcal{M}}(X) = |\mathcal{B}_X|$, donde $\mathcal{B}_X$ es el conjunto independiente más grande contenido en X. El operador de clausura que define un matroide en términos de su función rango es

$$\mathrm{cl}_{\mathcal{M}}(X) := \{v : r_{\mathcal{M}}(X) = r_{\mathcal{M}}(X \cup v)\}.$$

Un matroide se puede caracterizar en términos de bases, circuitos, operadores de clausura y otros objetos [13].

Sea A una matriz de $n \times m$ sobre un campo $\mathbb{F}$. El *matroide vectorial* asociado a A, es el par $\mathcal{M}(A) = ([m], \mathcal{I})$, donde cada elemento de $[m]$ le corresponde una única columna de A e $\mathcal{I} := \{X : \text{las columnas de la matriz } A, \text{ correspondientes a los elementos de } X, \text{ son vectores linealmente independientes en } \mathbb{F}^n\}$. Un matroide $\mathcal{M}$, se dice *representable* o *l-representable*, si se puede escribir como un matroide vectorial (isomorfismo de matroides).

Por simplicidad los conceptos de ml-representación (rep. multilineal), p-representación (rep. con particiones), ss-representación (rep. con matriz de repartición de secretos) son omitidos, y pueden consultarse en [11, 13, 17, 18, 20]. Particularmente se recomienda [14, Capítulo 2]. Las siguientes relaciones son conocidas:

$$\text{l-rep.} \subsetneq \text{ml-rep.} \subseteq \text{p-rep.} = \text{ss-rep.} \subsetneq \text{matroides} \subsetneq \text{operadores de clausura.}$$

Es un problema abierto determinar si la clase de ml-representables coincide con la de ss-representables [20].

El operador de clausura del ejemplo 2 es conocido como el matroide uniforme de rango 2 sobre 3 elementos. El siguiente ejemplo presenta un operador de clausura soluble que no es un matroide.

ejemplo 3. *Tomando* $m = 4$*, defina* cl *así:* $\mathrm{cl}(X) = X$*, si* $X \in \{\emptyset, 1, 2, 3, 4, 12, 34\}$ *y* $\mathrm{cl}(X) = [4]$*, de otro modo. Se verifica que* cl *es un operador de clausura sobre* 4 *elementos; de rango* 2*, pues* 13 *es una base.* cl *no es el operador de clausura de un matroide porque* $2 \in \mathrm{cl}(13) - \mathrm{cl}(1)$ *pero* $3 \notin \mathrm{cl}(12)$*. Sean,* $\mathcal{A}$ *cualquier alfabeto, y* $\bar{\pi}_1$, $\bar{\pi}_2$ *los kernel de las proyecciones canónicas sobre* $\mathcal{A}^2$*. Defina* $\bar{\mathcal{F}} = \left(\bar{f}_1, \bar{f}_2, \bar{f}_3, \bar{f}_4\right)$ *donde* $\bar{f}_1 = \bar{f}_2 = \bar{\pi}_1$ *y* $\bar{f}_3 = \bar{f}_4 = \bar{\pi}_2$*. Se puede verificar que* $\bar{\mathcal{F}}$ *es una* $(1, 1)$*-solución de* cl *sobre* $\mathcal{A}$ *.*

El siguiente teorema permite ver el concepto de operador de clausura soluble como una extensión natural del concepto de matroide de repartición de secretos.

Teorema 2. *[10, Teorema 2]* $\mathrm{cl}_{\mathcal{M}}$ *es soluble sobre* $\mathcal{A}$ *si, y sólo si,* $\mathcal{M}$ *es un matroide ss-representable sobre* $\mathcal{A}$*.*

El concepto de (k, n)-solución de un operador de clausura extiende el concepto de operador de clausura soluble. En lo siguiente, se definen problemas de programación lineal para calcular cotas sobre capacidades de un operador y demostrar que existen cuerpos en donde un operador de clausura nunca será soluble linealmente. En la sección posterior, se presentará un ejemplo (usando la conocida red Fano) en donde la capacidad lineal de un operador de clausura sobre un cuerpo finito es $\frac{4}{5}$, y además, se alcanza mediante una solución de particiones. Mostrando así, que la definición de solución de particiones no es trivial, sobre alfabetos en donde un operador no es soluble.

$$\begin{array}{c} A_1\ A_2\ A_3\ B_1\ B_2\ B_3\ C \\ \left(\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \end{array}$$

FIGURA 2.2. *Matriz de representación del matroide Fano si* $\operatorname{char}(\mathbb{F}) = 2$*; y del matroide non-Fano si* $\operatorname{char}(\mathbb{F}) \neq 2$.

Corolario 1. *Si* $\mathcal{M}$ *es un matroide ss-representable sobre* $\mathcal{A}$*, entonces* $\mathrm{C}^{\mathcal{A}}(\mathcal{M}) = \mathrm{B}^{\mathcal{A}}(\mathcal{M}) = 1$*. La capacidad del operador se alcanza mediante una ss-representación sobre* $\mathcal{A}$*.*

ejemplo 4. *En la figura 2.2 aparece una matriz con entradas en un cuerpo finito* $\mathbb{F}$*. Dicha matriz corresponde a la representación del matroide Fano cuando la característica de* $\mathbb{F}$ *es* 2*; y corresponde a la representación del matroide non-Fano cuando la característica es distinta de* 2*, [13]. El conjunto de soporte de dichos matroides es un conjunto de* 7 *elementos (a cada elemento le corresponde una columna de la matriz), que por conveniencia al usar el Teorema 1, se nota como* $V := \{A_1, A_2, A_3, B_1, B_2, B_3, C\}$*. En virtud del corolario anterior, cada uno de estos matroides tiene capacidad lineal* 1 *en los cuerpos en donde son representables. Es decir,*

$$\mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})\neq 2}(\textit{non-Fano}) = \mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})=2}(\textit{Fano}) = \mathrm{C}(\textit{non-Fano}) = \mathrm{C}(\textit{Fano}) = 1.$$

Uno se puede preguntar por el valor de $\mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})=2}(\textit{non-Fano})$ *y* $\mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})\neq 2}(\textit{Fano})$*. El valor exacto de estas capacidades no pudo ser calculado, pero usando los problemas de programación lineal previamente definidos, es posible encontrar algunas cotas superiores. Para calcular una cota superior de* $\mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})=2}(\textit{non-Fano})$*, se calcula una cota superior de* $\mathrm{B}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})=2}(\textit{non-Fano})$*, la solución del problema de programación del matroide non-Fano sobre cuerpos de característica* 2*. Las siguientes restricciones se obtienen de las condiciones impuestas al problema de programación lineal:*

$z_{B_{[3]}} = z_V$*;* $z_{A_{[3]};C} = z_C \leq \frac{1}{3}$*;* $z_{C|A_{[3]}} = z_{B_i|A_{[3]-i}} = z_{B_i|A_i,C} = 0$*;*
$z_{A_{[3]-i};C} = z_{A_{[3]-i}} + z_C - z_V \leq 1 - z_V$*;*
$z_{A_{[i]};A_{[3]-[i]}} + z_{A_{[i-1]};A_i} = z_{A_{[3]-[i]}} - z_V + z_{A_{[i-1]}} + z_{A_i} \leq \frac{3-i}{3} + \frac{i}{3} - z_V = 1 - z_V$*.*
Reemplazando cada una de estas restricciones en la restricción (2.1) y simplificando, se sigue que

$$z_V \leq \frac{2}{3} + 4\sum_{i=1}^{3}(1 - z_V).$$

Luego, $z_V \leq \frac{38}{39}$*. Por lo tanto,*

$$\mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})=2}(\textit{non-Fano}) \leq \mathrm{B}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})=2}(\textit{non-Fano}) \leq \frac{38}{39}.$$

De igual modo, se calcula una cota superior de $\mathrm{C}_{\textit{lineal}}^{\textit{char}(\mathbb{F})\neq 2}(\textit{Fano})$*. Las siguientes restricciones se obtienen de las condiciones impuestas al problema de programación del matroide Fano sobre cuerpos de característica distinta de* 2*:*

$z_{B_{[3]}} \leq \frac{2}{3}$*;* $z_{A_{[3]};C} = z_C \leq \frac{1}{3}$*;* $z_{C|A_{[3]}} = z_{B_i|A_{[3]-i}} = z_{B_i|A_i,C} = 0$*;*
$z_{A_{[3]-i};C} = z_{A_{[3]-i}} + z_C - z_V \leq 1 - z_V$*;*
$z_{A_{[i]};A_{[3]-[i]}} + z_{A_{[i-1]};A_i} = z_{A_{[3]-[i]}} - z_V + z_{A_{[i-1]}} + z_{A_i} \leq \frac{3-i}{3} + \frac{i}{3} - z_V = 1 - z_V$*.*
Reemplazando cada una de estas restricciones en la restricción (2.2) y simplificando, se sigue que

$$z_C \leq \frac{1}{3}z_{B_{[3]}} + \sum_{i=1}^{3}\left(z_{A_{[3]-i}} + z_C - z_V + 1 - z_V\right).$$

De modo que $6z_V \leq \frac{2}{9} + \frac{2}{3} + 5$*. Es decir,* $z_V \leq \frac{53}{54}$*. Por lo tanto,*

$$\mathrm{C}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})\neq 2}(\textit{Fano}) \leq \mathrm{B}_{\text{lineal}}^{\operatorname{char}(\mathbb{F})\neq 2}(\textit{Fano}) \leq \frac{53}{54}.$$

2.5. Operador de clausura de una red. En un dígrafo $D = ([m], E)$, para cada $X \subseteq [m]$, defina inductivamente,

$$\mathrm{c}_D^0(X) := X,$$

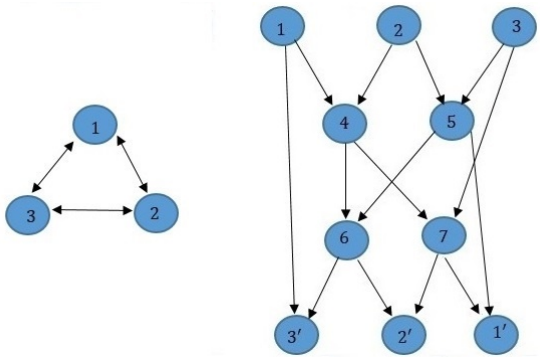

FIGURA 2.3. *El D*-dígrafo de la red Mariposa y la Red Fano.*

$$\mathrm{c}_D^1(X) := X \cup \left\{ v \in [m] \mid v^- \subseteq X \right\},$$

$$\mathrm{c}_D^i(X) := \mathrm{c}_D^1\left(c_D^{i-1}(X)\right) \text{ para } 1 < i \leq m.$$

El conjunto $\mathrm{cl}_D(X) := \mathrm{c}_D^m(X)$ se conoce como la *D-clausura de* X. La aplicación $\mathrm{cl}_D : 2^{[m]} \to 2^{[m]}$ que asigna a cada $X \subseteq [m]$, $cl_D(X)$, es un operador de clausura sobre m elementos, llamado el operador *D-clausura* [10].

En las proposiciones 1 y 2, aparecen pares de funciones y particiones repetidas, para cada t_i, con su respectivo s_i, esto sugiere una simplificación del dígrafo de la red, convirtiendo en uno solo cada par de tales nodos. Formalmente, se introduce el D*-dígrafo de D; este concepto ha sido usado en [16]. Una vez introducido, se presenta el teorema que conecta la solubilidad fraccional de las redes de información con la solubilidad de particiones de los operadores de clausura.

Definición 6. *El* D*-dígrafo *asociado de una red* $\mathcal{N}$*, es el dígrafo* $D^* = ([m-r], E^*)$*, donde* $uv \in E^*$*, si* $uv \in E$ *y* $v \neq t_i$ *para todo* i*; y* $us_i \in E^*$*, si* $ut_i \in E$ *para algún* i*.*

El enunciado y prueba del siguiente teorema es una reescrituración de la prueba del Teorema 1 de [10]. Se hace énfasis en que dicho teorema sigue siendo válido para (k, n)-soluciones. A continuación se presenta dicha prueba con más detalle.

Teorema 3. *Una red* $\mathcal{N} = (D, S, T)$ *tiene una* (k, n)*-solución fraccional sobre* $\mathcal{A}$ *si, y sólo si,* cl_{D^*} *tiene rango* r *y una* (k, n)*-solución de particiones sobre* $\mathcal{A}$*.*

Demostración: Teniendo en cuenta las proposiciones 1 y 2, la red $\mathcal{N}$ tiene una (k, n)-solución fraccional sobre $\mathcal{A}$ si, y sólo si, existe una colección de particiones de $\mathcal{A}^{rk}$, $\bar{\mathcal{F}} = \left(\bar{f}_v\right)_{v \in [m-r]}$, en a lo sumo $|\mathcal{A}|^n$-bloques cada una, tales que

(1) $\bar{f}_{v^-} \leq \bar{f}_v \; \forall v \in [m-r]$.
(2) $\bar{f}_T = \bar{f}_S = E_{\mathcal{A}^{rk}}$.

Estas condiciones pueden ser reescritas en términos de cl_{D^*}, como sigue:

(1') $\bar{f}_{\mathrm{cl}_{D^*}(X)} = \bar{f}_X \; \forall X \subseteq [m-r]$.
(2') cl_{D^*} tiene rango r y $\bar{f}_{[n-r]} = E_{\mathcal{A}^{rk}}$.

Se debe verificar que (1) es equivalente a (1'). Luego, se usa lo anterior para demostrar que (2) es equivalente a (2'):

(1) $\Leftrightarrow$(1'): puesto que $\bar{f}_{v^- \cup v} = \bar{f}_{v^-}$, para todo $v \in [m-r]$. Dado $X \subseteq [m-r]$, $v \in [m-r]$ tal que $v^- \subseteq X$, se tiene que $\bar{f}_{X \cup v^-} = \bar{f}_X$, así $\bar{f}_{X \cup v} = \bar{f}_{X \cup v^- \cup v} = \bar{f}_{X \cup v^-} = \bar{f}_X$, para cualquier v tal que $v^- \subseteq X$. Luego, $\bar{f}_{\mathrm{c}^1_{D^*}(X)} = \bar{f}_{X \cup \{v : v^- \subseteq X\}} = \bar{f}_X$. Continuando con este procedimiento hasta $\mathrm{c}^m_{D^*}$, se obtiene $\bar{f}_{\mathrm{cl}_{D^*}(X)} = \bar{f}_X$. Recíprocamente, suponga que $\bar{f}_{\mathrm{cl}_{D^*}(X)} = \bar{f}_X$, para todo X. En particular, para cada v, se tiene que $\bar{f}_{v^-} = \bar{f}_{\mathrm{cl}_{D^*}(v^-)} = \bar{f}_{\mathrm{cl}_{D^*}(v^-) \cup v} = \bar{f}_{v^- \cup v}$. En otras palabras, $\bar{f}_{v^-} \leq \bar{f}_v$.

(2) $\Leftrightarrow$(2'): Se puede comprobar que $\mathrm{cl}_{D^*}(S) = [m-r]$, de modo que $r_{\mathrm{cl}_{D^*}} \leq r$. De (1), $\bar{f}_{[m-r]} = \bar{f}_S = E_{\mathcal{A}^{rk}}$. Sin embargo, por definición, $\bar{f}_{[m-r]}$ puede tener a lo sumo $|\mathcal{A}|^{r_{\mathrm{cl}_{D^*}} k}$-bloques, es decir $r \leq r_{\mathrm{cl}_{D^*}}$. Se sigue que $r_{\mathrm{cl}_{D^*}} = r$. Recíprocamente, de (1') y usando que S es una base de cl_{D^*} se sigue que $\bar{f}_T = \bar{f}_S = \bar{f}_{\mathrm{cl}_{D^*}(S)} = \bar{f}_{[m-r]} = E_{\mathcal{A}^{rk}}$. □

Algoritmo 1. *(Una* red matroidal *) A partir de un matroide* $\mathcal{M} = ([m], \mathcal{I})$ *de rango* r*, se construye una red de uniemisión múltiple con* r *fuentes,* $\mathcal{N} = (D, S, T)$*, tal que* $cl^*_{D^*} \leq cl_{\mathcal{M}}$*. Aplicando el Teorema 3, el Teorema 2 y la Proposición 3, se obtiene que* $\mathcal{N}$ *es soluble sobre un alfabeto* $\mathcal{A}$*, si* $\mathcal{M}$ *es ss-representable sobre* $\mathcal{A}$*. La red* $\mathcal{N}$ *se construye de la siguiente forma:*

Paso ***1:*** *(fuentes) Elíjase una base cualquiera* $\mathcal{B} = \{s_1, ..., s_r\}$ *de* $\mathcal{M}$*. Cada* s_i *corresponde a un nodo fuente,* $i = 1, .., r$*. Así,* $S = \{s_1, ..., s_r\}$ *son las fuentes de la red.*

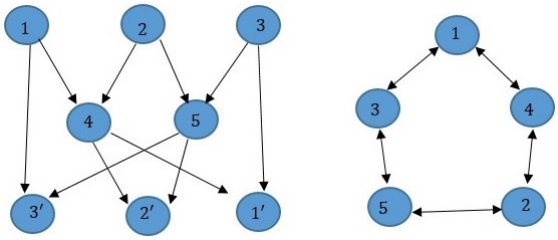

FIGURA 2.4. *Una red no soluble y su D*-dígrafo.*

Paso ***2:*** *(nodos intermedios) Para cada circuito* $\{v_0, ..., v_p\}$ *de* $\mathcal{M}$ *tal que los nodos* v_1, ..., v_p *ya están definidos, pero* v_0 *aún no lo está, defina un nodo nuevo* v_0, *y una colección de aristas* e_1, ..., e_p, *donde* $e_i := v_i v_0$, $i = 1, ..., p$.

Paso ***3:*** *(receptores) Elijase un circuito* $\{v_0, ..., v_p\}$ *de* $\mathcal{M}$, *tal que* v_i *está definido y* $v_0 = s_0 \in S$ *para* $i = 0, ..., p$. *Añada un nodo receptor* t_0 *y* p *aristas* e_1, ..., e_p *definidas por* $e_i := v_i t_0$, *si* $v_i \notin S$, *y* $e_i := v_i t_0$, *si* $v_i \in S$, *para* $i = 1, ..., p$. *Defina* $\tau(t_0) := s_0$. *Repita este paso* r*-veces tomando un nodo* v_0 *distinto en cada paso. Se obtiene un conjunto* $T = \{t_1, ..., t_r\}$ *de receptores de la red y una función demanda* τ.

El algoritmo presenta una porción del método para construir redes matroidales de Dougherty et al. [6]. Es bien conocido que un matroide es l-representable si, y sólo si, está asociado a una red matroidal que es linealmente soluble. Este resultado es parcialmente extendido a matroides ss-representables; en este caso la red generada por el algoritmo es soluble. El método se basa en la siguiente propiedad: dados $X \subseteq [m]$, $v \in [m]$ tales que $v^- \subseteq X$, se verifica que $v \in cl_{\mathcal{M}}(X)$. Como consecuencia, $cl_{D^*}(X) \subseteq cl_{\mathcal{M}}(X)$ o $cl_{D^*} \leq cl_{\mathcal{M}}$. Lo que permite una aplicación directa de la Proposición 3.

ejemplo 5. *La red mariposa es soluble sobre cualquier alfabeto; su D*-dígrafo aparece en la figura 2.3 (izquierda), y se puede verificar que la clausura de éste, es el matroide uniforme* $U_{2,3}$, *que es soluble sobre cualquier alfabeto. Esta red se puede construir mediante el algoritmo 1 con* $U_{2,3}$ *[6]. Otra red que se puede construir mediante el algoritmo es la red Fano, figura 2.3 (derecha); desde el matroide Fano. La solubilidad de esta red fue completamente determinada en [5]. Si reescribimos dichos resultados, se tiene que* $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})=2}$ *(red Fano)* $= \mathrm{C}$ *(red Fano)* $= 1$, $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}$ *(red Fano)* $= \frac{4}{5}$, *y todas estas capacidades son alcanzadas por soluciones adecuadas. Uno puede usar el problema de programación lineal de la red Fano, añadiendo en (v) la desigualdad rango lineal dada en el Teorema 12 de [8], y obtener como cota superior de* $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}$ *(red Fano), el valor* $\frac{14}{15}$. *Lamentablemente este valor está muy lejos de* $\frac{4}{5}$, *lo que indica que se deben añadir más restricciones al problema de programación lineal o mejorar la técnica usada. Note que el operador de clausura asociado a la red Fano es menor estricto que el matroide Fano, usando la proposición 3, se tiene que una solución del matroide Fano, es una solución de la red Fano, de modo que* $\mathrm{C}_{\mathrm{lineal}}^{\mathrm{char}(\mathbb{F})\neq 2}$ *(Fano)* $\leq \frac{4}{5}$.

Un ejemplo de una red no soluble es el siguiente.

ejemplo 6. *La red de la figura 2.4 (izquierda) no es soluble para cualquier alfabeto que se considere. Del lado derecho aparece su D*-dígrafo. Note que su D*-clausura tiene rango* 3, *por lo que se tiene que verificar que ésta no es soluble sobre todo alfabeto* $\mathcal{A}$. *De hecho, se tiene que* $z_{[5]} \leq \frac{5}{6}$ *para toda función de codificación* $\mathcal{F}$ *sobre cualquier alfabeto* $\mathcal{A}$. *En efecto,* $z_{[5]} = z_{123} \leq z_{13} + z_2 \leq z_{13} + \frac{1}{3}$. *Por otro lado,* $z_{[5]} = z_{1345}$, *sumando miembro a miembro estas desigualdades, y luego aplicando submodularidad:* $2z_{[5]} \leq z_{13} + z_{1345} + \frac{1}{3} \leq z_{134} + z_{135} + \frac{1}{3} = z_{34} + z_{15} + \frac{1}{3} \leq \frac{5}{3}$. *Luego,* $\frac{5}{6}$ *es una cota superior de su capacidad. Se sigue en particular que la red y su operador no son solubles.*

Para finalizar se resumen algunos capacidades presentadas:

O. Clausura	$\mathrm{C}^{\mathrm{char}(\mathbb{F})=2}$	$\mathrm{B}^{\mathrm{char}(\mathbb{F})=2}$	$\mathrm{C}^{\mathrm{char}(\mathbb{F})\neq 2}$	$\mathrm{B}^{\mathrm{char}(\mathbb{F})\neq 2}$	C	B
$U_{2,3}$	1	1	1	1	1	1
Fano	1	1	$\leq \frac{4}{5}$	$\leq \frac{53}{54}$	1	1
non-Fano	$\leq \frac{38}{39}$	$\leq \frac{38}{39}$	1	1	1	1
red Fano	1	1	$\frac{4}{5}$	$\leq \frac{14}{15}$	1	1

3. Conclusión. En este documento, se introduce el problema de encontrar (k, n)- soluciones de particiones de un operador de clausura. Usando problemas de programación lineal, se determinan algunas cotas superiores sobre distintos tipos de capacidad en un operador de clausura; en particular, cuando el operador se ha definido mediante algunos matroides o redes de información conocidos. Se quiere hacer énfasis en que este problema es totalmente novedoso y muchas propiedades faltan por estudiarse. Incluso se deben estudiar posibles mejoras a los problemas de programación lineal con el fin de ajustar las cotas superiores que producen.

Agradecimientos. El primer autor agradece el soporte proporcionado por COLCIENCIAS y el segundo autor agradece el soporte proporcionado por la Universidad Nacional de Colombia.

ORCID and license
Victor Pèña Macias https://orcid.org/0000-0002-4020-015X,
Humberto Sarria Zapata https://orcid.org/0000-0003-3515-7676.

Referencias

[1] Ahlswede R., Cai N., Li S.-Y. R. & Yeung R. W., *Network information flow*, IEEE Trans. Inform. Theory, 2000; 46:1204-1216 .
[2] Blasiak A., Kleinberg R. & Lubetzky E., *Lexicographic products and the power of non-Linear Network Coding*, IEEE Symposium on Foundations of Computer Science, 2011; 609-618.
[3] Brickell E. F. & Davenport D. M., *On the classification of Ideal Secret Sharing*, J. of Cryptology, 1991; 4:123-134.
[4] Burris S. & Sankappanavar H. P., *A course in Universal Algebra*, Springer-Verlag 1981.
[5] Dougherty R., Freiling C. & Zeger K., *Insufficiency of linear coding in network information flow*, IEEE Transactions on Information Theory, 2005; 51(8):2745-2759.
[6] Dougherty R., Freiling C. & Zeger K., *Networks, Matroids, and non-Shannon Information Inequalities*, IEEE Trans. on Information Theory, 2007; 3(6):1949-1969.
[7] Dougherty R., Freiling C. & Zeger K., *Linear Rank Inequalities on five or more variables*, arXiv:0910.0284 (2010).
[8] Dougherty R., Freiling C. & Zeger K., *Achievable Rate Regions for Network Coding*, IEEE Transactions on Information Theory, 2015; 61(5): 2488-2509.
[9] Dougherty R. & Zeger K., *Non-reversibility and equivalent constructions of Multiple-Unicast Networks*, IEEE Transactions on Information Theory, 2006; 52(11):5067-5077
[10] Gadouleau M., *Closure solvability for Network Coding and Secret Sharing*, IEEE Trans. Inform. Theory, UK , 2013; 59(12):7858-7869.
[11] Matúš F., *Matroid representations by partitions, Discrete Math.*, 1999; 203:169-194.
[12] Mejía C., *On the theory of linear rank inequalities*, Tesis de Doctorado, Universidad Nacional de Colombia, Bogotá. Disponible en red, 2016.
[13] Oxley J. G., *Matroid Theory*, Oxford Graduate Text in Mathematics, Department of Mathematics, Louisiana State University, 1992.
[14] Peña V., *Conexiones entre codificación en red, operadores de clausura y matroides de secreto compartido*, Tesis de Maestría, Universidad Nacional de Colombia, Bogotá. Disponible en red, 2015.
[15] Peña V. & Sarria H., *How to find new Characteristic-Dependent Linear Rank Inequalities using binary matrices as a guide*, 2019; arXiv:1905.00003.
[16] Riis S. & Gadouleau M., *Graph-theoretical constructions for graph entropy and network coding based communications*, IEEE Transactions on Information Theory, 2011; 57(10):6703-6717.
[17] Seymour P. D., *On secret-sharing matroids*, Journal of Combinatorial Theory, 1992; B(56):69-73.
[18] Shamir A., *How to share a secret*, Communications of the ACM, 1979; 22(11):612-613.
[19] Shen A., Hammer D., Romashchenko A. E. & Vereshchagin N. K., *Inequalities for Shannon entropy and Kolmogorov complexity*, Journal of Computer and Systems Sciences, 2000; 60:442-464.
[20] Simonis J. & Ashikhmin A., *Almost affine codes*, Des. Codes Cryptogr. 1998; 14:179-197.