FD RELACIONES

Raúl Emilio Varela Perea

Universidad Nacional de Colombia
Facultad De Ciencias
Departamento De Matemáticas
Bogotá D.C.
2011

FD RELACIONES

Raúl Emilio Varela Perea

Trabajo final presentado como requisito parcial para optar al título de

Magister en Ciencias Matemáticas

Director:
Profesor Humberto Sarria Zapata

Universidad Nacional de Colombia
Facultad De Ciencias
Departamento De Matemáticas
Bogotá D.C.
2011

TÍTULO: FD RELACIONES

TITLE: FD RELATIONS

RESUMEN: En este trabajo se estudian las **relaciones de dependencia funcional** o **FD Relaciones**. Está basado en los resultados presentados en [2] y en [3]. Se presenta la conexión entre las FD relaciones, los operadores de clausura y algunos objetos definidos por operadores de clausura, a saber, las matroides y las topologías. Se estudia la conexión de las FD relaciones con los semiretículos y las funciones submodulares. Por último, se estudia una aplicación de las FD relaciones en la solución de problemas de Codificación en redes.

ABSTRACT: In this paper we study the **functional dependency relations** or **FD relations**. It is based on the results in [2] and [3]. It is showed the connexion between FD relations, the closure operators and some objects obtained from closure operators like matroids and topologies. It is studied also, the connexion between FD relations with semilattices and its connexion with submodular functions. At last, it is studied its application on the solutions of the Network Coding problems.

PALABRAS CLAVE: FD relación, operador de clausura, relación de dependencia funcional, topología, matroide, codificación en redes, función submodular, semiretículo, entropía.

KEY WORDS: FD relation, closure operator, functional dependency relation, topology, matroid, network coding, submodular function, semilattice, entropy.

DIRECTOR: Ph. D. Humberto Sarria Zapata

Índice general

Introducción **5**

1. Preliminares **8**

1.1. Representación gráfica de una FD relación finita 9

2. FD relaciones y operadores de clausura **11**

2.1. Operadores de Clausura 11

2.2. Matroides 13

2.2.1. Rango de una matroide y Operador de clausura de una matroide 14

2.3. Topologías 20

2.4. Conexión de Galois 23

3. FD relaciones y otras teorías **25**

3.1. Semiretículos 25

3.2. Funciones Submodulares 27

4. FD relaciones y códigos de red **36**

4.1. Conexión entre las FD relaciones y las soluciones de problemas de codificación en redes 40

Conclusiones **43**

A. Una introducción a Entropía **44**

Introducción

Sean N un conjunto arbitrario, $\{f_i\}_{i\in N}$ una colección de funciones con el mismo dominio y el mismo conjunto de llegada, y, $f_I = (f_i)_{i\in I}$ para cada $I \subseteq N$. Para un par de conjuntos $(I, J) \in 2^N \times 2^N$, puede existir una función que conecte f_I con f_J, es decir, una función $g(I, J)$ tal que $f_J = g(I, J) \circ f_I$. Informalmente hablando, diríamos que hay una cierta *dependencia funcional* en la pareja (I, J), o mejor, entre las familias de funciones indexadas por I y J. Evidentemente, existe tal dependencia funcional si el par (I, J) es tal que $J \subseteq I$. Ahora bien, si $f_J = g(I, J) \circ f_I$ y $f_K = g(J, K) \circ f_J$ entonces $f_K = g(J, K) \circ g(I, J) \circ f_I$; y, si $f_{J_\lambda} = g(I, J_\lambda) \circ f_I$ para cada $\lambda \in \Lambda$, entonces,

$$f_J = (g(I, J_\lambda))_{\lambda\in\Lambda} \circ f_I \text{ con } J = \bigcup_{\lambda\in\Lambda} J_\lambda.$$

Las afirmaciones anteriores permiten concluir que la dependencia funcional es transitiva y cerrada para la contenencia y para la unión de las segundas componentes.

El estudio de las propiedades de lo que hemos llamado dependencia funcional, se simplifica remitiendose al conjunto N de índices y definiendo un conjunto $\mathcal{N} \in 2^N \times 2^N$ así:

1. $(I, J) \in \mathcal{N}$ si $I \supseteq J$,
2. $(I, J), (J, K) \in \mathcal{N}$ implica $(I, K) \in \mathcal{N}$, y,
3. $(I, J_\lambda) \in \mathcal{N}$ para cada $\lambda \in \Lambda$ implica $(I, \bigcup_{\lambda\in\Lambda} J_\lambda) \in \mathcal{N}$.

A un conjunto $\mathcal{N}$ que satisfaga los axiomas anteriores, lo llamaremos **relación de dependencia funcional**, o simplemente, **FD relación**.

La noción de FD relación surgió del estudio de la Teoría de las Bases de Datos [1], sin embargo, su versatilidad es sorprendente. Hay una correspondencia bíunivoca entre las FD relaciones y los operadores de clausura [2]. Lo anterior implica que existe una conexión estrecha entre las FD relaciones y los objetos que son definidos por un operador de clausura, como por ejemplo las matroides y las topologías. Por otro lado, las matroides están relacionadas con la solución de problemas de Codificación en Redes ([3],[4],[5]), así, es de esperar que las FD relaciones también lo estén; de ahí que, en [3], se demuestre que las FD relaciones son estructuras adecuadas para capturar las dependencias e independencias que caracterizan los códigos de red.

Además, las FD relaciones son útiles para comprender las dependencias entre si de los elementos de una familia de funciones o los de un semiretículo inferior. También, es posible demostrar que toda función submodular (una generalización de función rango en matroides) define una FD relación, y, recíprocamente, toda FD relación finita define una función submodular que resulta ser una función de entropía [2].

El objetivo principal de este trabajo, es estudiar las propiedades de las FD relaciones, sus conexiones con los operadores de clausura, las topologías, las matroides, los semiretículos y las funciones submodulares; y, su aplicación a la solución de problemas de codificación de las redes de información.

El trabajo está organizado de la siguiente manera: En el capítulo 1 se presenta la definición base de todo el trabajo, a saber, la de FD relación. Se sugiere una forma de representar gráficamente las FD relaciones finitas, con el fin de visualizar mejor las dependencias entre sus elementos. Aunque [2] restringe su trabajo a FD relaciones finitas, en el presente documento se amplía el concepto al caso infinito. Hacerlo así, permitirá extender los resultados obtenidos en [2], y también permitirá explorar un nuevo campo de estudio, a saber, la conexión entre Topología y la Teoría de las FD relaciones.

En el capítulo 2, se probará que, dada una FD relación $\mathcal{N}$, es posible definir un operador clausura $c_{\mathcal{N}}$ a partir de ella, y, recíprocamente, dado un operador de clausura c, es posible definir una FD relación $\mathcal{N}_c$ a partir de él. Además, se probará que $\mathcal{N} = \mathcal{N}_{c_{\mathcal{N}}}$, $c = c_{\mathcal{N}_c}$ y que existe una conexión de Galois entre el conjunto de las FD relaciones sobre un soporte N y los operadores de clausura sobre N [2]. Se explorará cómo, algunos objetos definidos por operadores de clausura se pueden ver como FD relaciones, a saber, las matroides y las topologías.

En el capítulo 3, se presentan las conexiones, descritas en [2], entre las FD relaciones y los semiretículos, y entre las FD relaciones y las funciones submodulares. Se demostrará que toda función submodular define una FD relación, y que toda FD relación finita define una función submodular.

En el capítulo 4, se demuestra el resultado citado en [3], que describe el estrecho vínculo entre FD relaciones y las redes de información. Para tal efecto, se definen los conceptos de grafo dirigido acíclico y código de red.

Los aportes del presente documento son los siguientes:

- La extensión de la definición de las FD relaciones al caso infinito.
- La demostración, vía operadores de clausura, de que toda topología define una FD relación, y, los axiomas adicionales inducidos por una topología sobre la FD relación asociada.
- Los axiomas adicionales inducidos por una matroide sobre la FD relación asociada.
- La construcción de una función submodular a partir de una FD relación.
- Una demostración alternativa del resultado enunciado en [3], que vincula las FD relaciones con la solución de los problemas de codificación en redes.
- Una conexión de Galois entre el conjunto de las FD relaciones y el de los operadores de clausura definidos sobre N, alternativa a la presentada en [2].

Capítulo 1

Preliminares

En este capítulo se presenta la definición de FD relación. Se sugiere una forma de representar gráficamente las FD relaciones finitas, con el fin de visualizar mejor las dependencias entre sus elementos. Aunque [2] restringe su trabajo a FD relaciones finitas, en el presente documento se amplía el concepto al caso infinito. Hacerlo así, permitirá extender los resultados obtenidos en [2], y también permitirá explorar un nuevo campo de estudio, a saber, la conexión entre Topología y la Teoría de las FD relaciones.

Definición 1.1. *Sea N un conjunto arbitrario. Diremos que $\mathcal{N} \subseteq 2^N \times 2^N$ es una FD-relación sobre N, si satisface que:*

(FD1) $N \supseteq I \supseteq J$ *implica* $(I, J) \in \mathcal{N}$,

(FD2) $(I, J), (J, K) \in \mathcal{N}$ *implica* $(I, K) \in \mathcal{N}$,

(FD3) $(I, J_\lambda) \in \mathcal{N}$ *para todo* $\lambda \in \Lambda$ *implica* $(I, \bigcup_{\lambda \in \Lambda} J_\lambda) \in \mathcal{N}$.

Llamaremos al conjunto N de la definición el conjunto soporte de la FD relación.

Veamos un ejemplo de FD relación sobre un soporte de dos elementos, pero antes convengamos en notar el conjunto $\{a_1, a_2, ..., a_n\}$ en la forma $a_1 a_2 ... a_n$.

Ejemplo 1.2. *Sea $N = ab$. Es fácil verificar que los siguientes conjuntos son FD relaciones.*

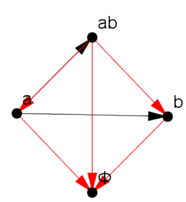
$$\mathcal{N} = \{(ab, ab), (a, a), (b, b), (\emptyset, \emptyset), (ab, \emptyset), (ab, a), (ab, b), (a, \emptyset), (b, \emptyset)\}$$
$$\mathcal{M} = \{(ab, ab), (a, a), (b, b), (\emptyset, \emptyset), (ab, \emptyset), (ab, a), (ab, b), (a, \emptyset), (b, \emptyset), (a, b), (a, ab)\}$$

*Nótese que, por la propiedad **(FD1)**, toda FD relación sobre un soporte de dos elementos contiene a $\mathcal{N}$, es decir, $\mathcal{N}$ es la más pequeña FD relación que se puede definir sobre un soporte de dos elementos. Obsérvese además que, si a $\mathcal{N}$ le adherimos la pareja (a, b), entonces para obtener una nueva FD relación $\mathcal{M}$, es obligatoria la presencia de (a, ab) por la propiedad **(FD3)**; ahora bien, otra forma de obtener $\mathcal{M}$ a través de $\mathcal{N}$ es pegar la pareja (a, ab) y luego, por **(FD2)**, la pareja (a, b).*

Nota: La existencia de la FD relación más pequeña definida sobre un soporte N, está garantizada por el hecho de que el conjunto de todas las parejas en donde la segunda componente es un subconjunto de la primera es una FD relación contenida en cualquier otra. Notaremos tal FD relación por $\mathcal{N}_{|N|}$.

1.1. Representación gráfica de una FD relación finita

Representaremos la pareja (I, J) como una flecha que parte desde el punto I y llega al punto J. La FD relación $\mathcal{N}_{|N|}$ será representada por un grafo rojo. Así, graficamente, la FD relación $\mathcal{M}$ del ejemplo 1.2 es:



Ejemplo 1.3. *Consideremos FD relaciones con soporte $N = \{a, b, c\}$. Nos preguntamos cúal es la más pequeña que contiene (b, c). Si colocamos la flecha negra $b \to c$, entonces, por **(FD2)**, aparece $ab \to c$. Las demás flechas negras son producto de la propiedad **(FD3)** aplicada sucesivas veces (ver figura 1.1).*

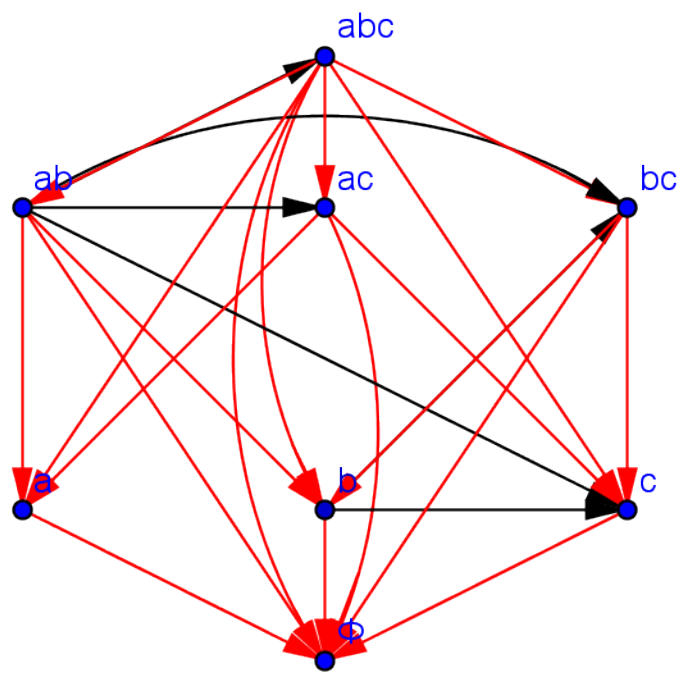


Figura 1.1: Figura del ejemplo 1.3

Capítulo 2

FD relaciones y operadores de clausura

Los operadores de clausura son bien conocidos, por ejemplo, el operador adherencia de una topología. Lo que no es conocido es su estrecha conexión con las FD relaciones. Se probará que, dada una FD relación $\mathcal{N}$, es posible definir un operador clausura $c_{\mathcal{N}}$ a partir de ella, y, recíprocamente, dado un operador de clausura c, es posible definir una FD relación $\mathcal{N}_c$ a partir de él. Además, se probará que $\mathcal{N} = \mathcal{N}_{c_{\mathcal{N}}}$, que $c = c_{\mathcal{N}_c}$ y que hay una conexión de Galois entre el conjunto de las FD relaciones sobre un soporte N y los operadores de clausura sobre N.

Algunos objetos definidos por operadores de clausura son las matroides [6] y las topologías. Lo anterior implica que existen algunas FD relaciones especiales que definen y son definidas por matroides, y otras, que definen y son definidas por topologías. Se darán condiciones suficientes y necesarias sobre tales FD relaciones. Dichas condiciones son novedades de este documento.

2.1. Operadores de Clausura

Nos proponemos en esta sección, mostrar que las FD relaciones y los operadores de clausura están vinculados de manera biunívoca.

Definición 2.1. *Diremos que el operador $c : 2^N \longrightarrow 2^N$ es de clausura sobre N si, dados $I, J \subseteq N$:*

(CL1) $I \subseteq c(I)$,

(CL2) $I \subseteq J$ implica $c(I) \subseteq c(J)$,

(CL3) $c(I) = c(c(I))$.

Proposición 2.2. *Sea $\mathcal{N} \subseteq 2^N \times 2^N$ una FD relación. El operador $c_{\mathcal{N}}$: $2^N \longrightarrow 2^N$*

$$c_{\mathcal{N}}(I) = \bigcup_{(I,J)\in\mathcal{N}} J$$

es de clausura.

Prueba.

1. Es claro que $(I, I) \in \mathcal{N}$. Luego $I \subseteq c_{\mathcal{N}}(I)$.
2. Sean $I \subseteq J \subseteq N$ y $x \in c_{\mathcal{N}}(I)$. Entonces $(I, x) \in \mathcal{N}$ y $(J, I) \in \mathcal{N}$. Luego, $(J, x) \in \mathcal{N}$. Por lo tanto $x \in c_{\mathcal{N}}(J)$.
3. Nótese que $(I, c_{\mathcal{N}}(I)) \in \mathcal{N}$ por **(FD3)**. Sea $x \in c_{\mathcal{N}}(c_{\mathcal{N}}(I))$. Entonces $(c_{\mathcal{N}}(I), x) \in \mathcal{N}$. Luego $(I, x) \in \mathcal{N}$. Por lo tanto $x \in c_{\mathcal{N}}(I)$. La otra contenencia es consecuencia inmediata de **(CL1)** y **(CL2)**.

□

Proposición 2.3. *Sea c un operador de clausura sobre N. Entonces*

$$\mathcal{N}_c = \{(I, J) \in 2^N \times 2^N : J \subseteq c(I)\}$$

es una FD relación.

Prueba.

1. Sean $N \supseteq I \supseteq J$. Entonces, $J \subseteq c(I)$ y $(I, J) \in \mathcal{N}_c$.
2. Sean $J \subseteq c(I)$ y $K \subseteq c(J)$, pot lo tanto, $K \subseteq c(J) \subseteq c(c(I)) \subseteq c(I)$, de donde $(I, K) \in \mathcal{N}_c$.
3. Para cada λ en un conjunto arbitrario Λ, sea $J_\lambda \subseteq c(I)$. Se concluye que $\bigcup_{\lambda\in\Lambda} J_\lambda \subseteq c(I)$.

□

Proposición 2.4.

1. *Si $\mathcal{N}$ es una FD relación, entonces, $\mathcal{N} = \mathcal{N}_{c_{\mathcal{N}}}$.*
2. *Si c es un operador de clausura, entonces, $c = c_{\mathcal{N}_c}$.*

Demostración. Sea $\mathcal{N}$ una FD relación con soporte N. Entonces, $(I, J) \in \mathcal{N}$, si y sólo si, $J \subseteq c_{\mathcal{N}}(I)$, si y sólo si, $(I, J) \in \mathcal{N}_{c_{\mathcal{N}}}$.

Ahora, sea c un operador de clausura. Entonces, $x \in c(I)$, si y sólo si, $(I, x) \in \mathcal{N}_c$, si y sólo si, $x \in c_{\mathcal{N}_c}(I)$. □

Las proposiciones anteriores garantizan que cada operador clausura se puede definir vía una FD relación y viceversa, de manera biunívoca. Esto permite ver los objetos definidos a través de operadores de clausura como FD relaciones. Nos proponemos mostrar la afirmación anterior en el caso de las matroides, y después, en el caso de las topologías.

2.2. Matroides

Las matroides surgen en el esfuerzo de generalizar los conceptos de dependencia e independencia que se tiene en espacios vectoriales. Cada uno de estos interesantes objetos, posee, además, su propia función rango. En [3] y [5] se demuestra su utilidad para la resolución de problemas de codificación de redes. Se incluyen en este trabajo por su conexión con las FD relaciones, vía los operadores de clausura. Para una revisión detallada de Teoría de Matroides, véase [6].

Definición 2.5. *Una matroide M consiste en un par $(E, \mathcal{I})$ donde E es un conjunto finito e $\mathcal{I}$ es una colección de subconjuntos de E que satisface los siguientes axiomas:*

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

(M2) *Si $A \in \mathcal{I}$ y $B \subseteq A$, entonces $B \in \mathcal{I}$.*

(M3) *Si $A, B \in \mathcal{I}$ y $|B| < |A|$, entonces existe $a \in A - B$ tal que $B \cup a \in \mathcal{I}$.*

Diremos que M es una matroide sobre E.

Ejemplo 2.6. *Algunas colecciones de independientes que se pueden obtener sobre el conjunto $E = \{a, b, c\}$ son:*

1. $\mathcal{I} = \{\emptyset, \{a\}\}$.
2. $\mathcal{J} = \{\emptyset, \{a\}, \{b\}\}$.
3. $\mathcal{K} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}$.

Así, $M = (E, \mathcal{I})$, $N = (E, \mathcal{J})$ y $L = (E, \mathcal{K})$ son matroides.

Definición 2.7. *Los elementos de $\mathcal{I}$ son los conjuntos independientes de M, y E es su conjunto base. Un subconjunto de E que no pertenezca a $\mathcal{I}$ es un conjunto dependiente. Un elemento $\mathcal{C} \in \mathcal{I}$ es un circuito, si es dependiente y cualquiera de sus subconjuntos propios es independiente. Un elemento $B \in \mathcal{I}$ es una base, si es maximal independiente, es decir, si no existe un elemento en $\mathcal{I}$ que lo contenga propiamente.*

A continuación listamos algunas proposiciones que serán útiles en lo que sigue.

Proposición 2.8. *Todas las bases de una matroide tienen la misma cantidad de elementos.*

Demostración. Sean A y B bases de M. Supongamos que $|B| < |A|$. Entonces, por **(M3)**, existe $x \in A - B$ tal que $B \cup x \in \mathcal{I}$. Pero eso es imposible porque B es maximal independiente. $\square$

Proposición 2.9. *Sean $M = (S, \mathcal{I})$ una matroide e $\mathcal{I}|X := \{I \subseteq X : I \in \mathcal{I}\}$. Entonces, $M|X := (X, \mathcal{I}|X)$ es una matroide sobre X.*

Demostración.

1. $\emptyset \subseteq X$ y $\emptyset \in \mathcal{I}$, luego $\emptyset \in \mathcal{I}|X$.
2. Si $A \in \mathcal{I}|X$ y $B \subseteq A$, entonces $A \in \mathcal{I}$, luego $B \in \mathcal{I}$; y dado que $B \subseteq X$, se sigue que $B \in \mathcal{I}|X$.
3. Supongamos que $A, B \in \mathcal{I}|X$ tales que $|B| < |A|$. Existe $a \in A - B$ tal que $B \cup a \in \mathcal{I}$. Pero $B \cup a \subseteq A \cup B \subseteq X$, luego $B \cup a \in \mathcal{I}|X$.

$\square$

Proposición 2.10. *Todo independiente está contenido en una base.*

Demostración. Sea $I \in \mathcal{I}$ que no es una base. Entonces, existe un independiente I_1 tal que $I_1 \supset I$. Si I_1 no es base, existe I_2 independiente tal que $I_2 \supset I_1$. Si I_2 no es base se repite el argumento, y así sucesivamente. Nótese que debe existir $k \in \mathbb{N}$ tal que I_k sea base puesto que los conjuntos I_n son crecientes por contenencia y están contenidos en E que es finito. $\square$

2.2.1. Rango de una matroide y Operador de clausura de una matroide

La función rango de una matroide, generaliza el concepto de rango en espacios vectoriales de dimensión finita. Esta función resulta ser submodular.

Vía la función rango, definiremos el operador de clausura de una matroide. Este operador satisface el axioma adicional **(CL4)**, e induce una propiedad adicional, sobre la FD relación asociada a él.

Definición 2.11. *Una función $r_M : 2^E \longrightarrow \mathbb{N}$ es la función rango de la matroide M, si para cada $X \subseteq E$, $r_M(X)$ es el tamaño del independiente más grande contenido en X.*

Las proposiciones 2.8 y 2.9 garantizan la buena definición de r_M.

Proposición 2.12. *La función r_M satisface los siguientes axiomas:*

(R1) $0 \leq r_M(X) \leq |X|$ *para todo* $X \subseteq E$.

(R2) *Si* $X \subseteq Y$ *entonces* $r_M(X) \leq r_M(Y)$.

(R3) *Si* $X, Y \subseteq E$, *entonces,*

$$r_M(X \cup Y) + r_M(X \cap Y) \leq r_M(X) + r_M(Y),$$

es decir, r_M es submodular.

Demostración. Las propiedades **(R1)** y **(R2)** se deducen directamente de la definición.

Sea $B_{X\cap Y}$ una base para $X \cap Y$. Entonces, $B_{X\cap Y}$ es un independiente de $M|(X \cup Y)$. Además, $B_{X\cap Y}$ está contenido en una base $B_{X\cup Y}$ de esta matroide (proposición 2.10). Ahora bien, $B_{X\cup Y} \cap X$ y $B_{X\cup Y} \cap Y$ son independientes en $M|X$ y $M|Y$, respectivamente. Así,

$$|B_{X\cup Y} \cap X| \leq r_M(X) \quad \text{y} \quad |B_{X\cup Y} \cap Y| \leq r_M(Y).$$

Luego,

$$\begin{aligned}
r_M(X) + r_M(Y) &\geq |B_{X\cup Y} \cap X| + |B_{X\cup Y} \cap Y| \\
&= |(B_{X\cup Y} \cap X) \cup (B_{X\cup Y} \cap Y)| \\
&\qquad\qquad + |(B_{X\cup Y} \cap X) \cap (B_{X\cup Y} \cap Y)| \\
&= |B_{X\cup Y} \cap (X \cup Y)| + |B_{X\cup Y} \cap X \cap Y| \\
&= |B_{X\cup Y}| + |B_{X\cap Y}| \\
&= r_M(X \cup Y) + r_M(X \cap Y),
\end{aligned}$$

y queda demostrado **(R3)**. □

Construyamos el operador de clausura asociado a una matroide. Necesitaremos los siguientes lemas.

Lema 2.13. *Si* $X \subseteq E$ *y* $x \in E$, *entonces,* $r(X) \leq r(X \cup x) \leq r(X) + 1$.

Demostración. Sea B_X una base para X. Entonces, debe darse una de dos posibilidades: B_X es una base de $X \cup x$ o $B_X \cup x$ lo es. Así $r(X \cup x)$ es $r(X)$ o es $r(X) + 1$. □

Lema 2.14. *Sean $X, Y \subseteq E$ tales que para todo $y \in Y - X$, $r_M(X \cup y) = r_M(X)$, entonces $r_M(X \cup Y) = r_M(X)$.*

Demostración. Sea $Y - X = \{y_1, ..., y_k\}$. Razonemos por inducción sobre k. Si $k = 1$, el resultado es inmedianto. Asumamos que el enunciado es cierto para $k = n$ y sea $k = n + 1$. Entonces, por **(R3)**,

$$\begin{aligned} r_M(X) + r_M(X) &= r_M(X \cup \{y_1, ..., y_n\}) + r_M(X \cup y_{n+1}) \\ &\geq r_M((X \cup \{y_1, ..., y_n\}) \cup (X \cup y_{n+1})) \\ &\qquad + r_M((X \cup \{y_1, ..., y_n\}) \cap (X \cup y_{n+1})) \\ &= r_M(X \cup \{y_1, ..., y_{n+1}\}) + r_M(X) \\ &\geq r_M(X) + r_M(X). \end{aligned}$$

Luego,

$$r_M(X \cup \{y_1, ..., y_{n+1}\}) = r_M(X).$$

$\square$

Definición 2.15. *El operador de clausura de una matroide M es una función $c_M : 2^E \longrightarrow 2^E$ tal que*

$$c_M = \{x \in E : r_M(X \cup x) = r_M(X)\}.$$

Proposición 2.16. *La función c_M no sólo satisface **(CL1)-(CL3)**, sino también el axioma adicional:*

(CL4) *Si $X \subseteq E, x \in E$, y, $y \in c_M(X \cup x) - c_M(X)$, entonces $x \in c_M(X \cup y)$.*

Demostración. **(CL1)** se satisface directamente de la definición. Ahora, para probar **(CL2)**, supongamos que $X \subseteq Y$ y $x \in c_M(X) - X$. Entonces, $r(X \cup x) = r(X)$. Así, si B_X es una base de X, entonces, B_X es una base de $X \cup x$. Entonces, $Y \cup x$ tiene una base $B_{Y \cup x}$ que contiene B_X y no contiene x. Como $B_{Y \cup x}$ debe ser también una base de Y, se sigue que

$$r(Y \cup x) = |B_{Y \cup x}| = r(Y),$$

y así, $x \in c_M(Y)$.

Para probar **(CL3)**, obsérvese primero que, por **(CL1)**, $c_M(X) \subseteq c_M(c_M(X))$. Ahora, para la otra contenencia, sea $x \in c_M(c_M(X))$. Entonces,

$$r(c_M(X) \cup x) = r(c_M(X)).$$

Pero, para todo $y \in c_M(X) - X$, $r(X \cup y) = r(X)$. Luego, por el lema 2.14,

$$r(X) = r(X \cup (c_M(X) - X)) = r(c_M(X)).$$

Así,

$$r(c_M(X) \cup x) = r(X).$$

Pero, por **(R2)**,

$$r(c_M(X) \cup x) \geq r(X \cup x) \geq r(X),$$

por lo que,

$$r(X \cup x) = r(X).$$

Ahora probaremos **(CL4)**. Supongamos que $y \in c_M(X \cup x) - c_M(X)$. Entonces

$$r(X \cup x \cup y) = r(X \cup x) \quad \text{y} \quad r(X \cup y) \neq r(X).$$

Por la última desigualdad del lema 2.13, deducimos que $r(X \cup y) = r(X) + 1$. Así,

$$r(X) + 1 = r(X \cup y) \leq r(X \cup y \cup x) = r(X \cup x) \leq r(X) + 1.$$

Entonces, $x \in c_M(X \cup y)$. □

El propósito de las proposiciones siguientes, es demostrar que la asociación del operador de clausura con su respectiva matroide es biunívoca.

Lema 2.17. *Sean c un operador de clausura que satisface **(CL4)**, $X \subseteq E$ y $x \in E$. Si $X \in \mathcal{I}$ pero $X \cup x \notin \mathcal{I}$, entonces $x \in c(X)$.*

Demostración. Como $X \cup x \notin \mathcal{I}$, hay un elemento $y \in X \cup x$ tal que $y \in c((X \cup x) - y)$. Si $y = x$, entonces el lema se satisface. Si $y \notin x$, se concluye que,

$$(X \cup x) - y = (X - y) \cup x \quad \text{y} \quad y \in c((X - y) \cup x) - c(X - y).$$

Así, por **(CL4)**, $x \in c((X - y) \cup y) = c(X)$. □

Proposición 2.18. *Sean c un operador de clausura que satisface **(CL4)** e*

$$\mathcal{I} = \{X \subseteq E : x \notin c(X - x) \text{ para todo } x \in X\}.$$

*Entonces, $(E, \mathcal{I})$ es una matroide, es decir, todo operador de clausura c que satisfaga **(CL4)** es el operador de clausura de alguna matroide.*

Demostración. Evidentemente $\emptyset \in \mathcal{I}$. Ahora, supongamos que $I \in \mathcal{I}$ y que $I' \subseteq I$. Si $x \in I'$, entonces, $x \in I$ por lo que $x \notin c(I - x)$. Por **(CL2)**, $c(I - x) \supseteq c(I' - x)$, así, $x \notin c(I' - x)$, de donde $I' \in \mathcal{I}$. Se satisface pues **(M2)**.

Ahora, supongamos que para $I_1, I_2 \in \mathcal{I}$, se tiene que $|I_1| < |I_2|$ pero no se satisface **(M3)**. Supongamos también que, entre las intersecciones de pares de conjuntos que cumplen la afirmación anterior, $|I_1 \cap I_2|$ es maximal. Escojamos $y \in I_2 - I_1$ y consideremos $I_2 - y$. Asumamos que $I_1 \subseteq c(I_2 - y)$. Luego, por **(CL2)** y **(CL3)**, $c(I_1) \subseteq c(I_2 - y)$. Como $y \notin c(I_2 - y)$, entonces, $y \notin c(I_1)$. De modo que, por la contrarecíproca del lema 2.17, $I_1 \cup y \in \mathcal{I}$, por lo que se satisface **(M3)** para I_1 e I_2; lo cual es una contradicción. Así, $I_1 \nsubseteq c(I_2 - y)$, es decir, existe $t \in I_1$ tal que $t \notin c(I_2 - y)$. Evidentemente $t \in I_1 - I_2$. De nuevo, por el lema 2.17, $(I_2 - y) \cup t \in \mathcal{I}$. Como

$$|I_1 \cap ((I_2 - y) \cup t)| > |I_1 \cap I_2|,$$

(M3) se satisface para el par I_1 e $(I_2 - y) \cup t$, es decir, existe $x \in (I_2 - y) \cup t$ tal que $I_1 \cup x \in \mathcal{I}$. Pero $x \in I_2 - I_1$, luego *(M3)* se satisface para I_1 e I_2; lo que es absurdo. □

Proposición 2.19. *Sea M la matroide obtenida a partir del operador de clausura c según la proposición anterior. Entonces $c = c_M$.*

Demostración. Supongamos primero que $x \in c_M(X) - X$. Entonces,

$$r_M(X \cup x) = r_M(X).$$

Sea B una base de X. Entonces $B \in \mathcal{I}$ y $B \cup x \notin \mathcal{I}$, así, por el lema 2.17, $x \in c(B)$. Pero, por **(CL2)**, $c(B) \subseteq c(X)$. Luego $x \in c(X)$ y así $c_M(X) \subseteq c(X)$.

Supongamos ahora que $x \in c(X) - X$. Sea B una base para X. Se sigue que $B \cup y \notin \mathcal{I}$ para todo $y \in X - B$, así, por el lema 2.17, $X \subseteq c(B)$. Luego, $c(X) \subseteq c(B)$ y $x \in c(B)$. Así, $B \cup x \notin \mathcal{I}$, por lo que B es una base para $X \cup x$, y,

$$r_M(X \cup x) = |B| = r_M(X).$$

De lo anterior, se deduce que $x \in c_M(X)$. Concluimos que $c(X) \subseteq c_M(X)$. □

Tal como vimos en la sección 2.1, toda FD relación $\mathcal{N}$ define un operador de clausura c y viceversa. Así pues, lo que la proposición 2.16 afirma es que toda matroide define una FD relación a partir de su operador clausura que en últimas depende de la función rango de la matroide. Ahora bien, esa FD relación debería satisfacer algún axioma más, auspiciado por **(CL4)**. Lo anterior nos lleva a la siguiente pregunta: ¿Cómo se refleja la propiedad **(CL4)** en las FD relaciones obtenidas a partir de matroides? La siguiente proposición se ocupa en responder esta pregunta.

Proposición 2.20. *La FD relación $\mathcal{N}$ con soporte E obtenida a partir del operador clausura de una matroide satisface el axioma adicional:*

(FD4) *Sean $x, y \in E$, $I \subseteq E$. Si $(I \cup x, y) \in \mathcal{N}$ y $(I, y) \notin \mathcal{N}$, entonces, $(I \cup y, x) \in \mathcal{N}$.*

*Además, si una FD relación $\mathcal{N}$ satisface **(FD4)**, entonces, el operador de clausura $c_{\mathcal{N}}$ generado a partir de $\mathcal{N}$ satisface **(CL4)**, es decir, $c_{\mathcal{N}}$ es el operador clausura de una matroide.*

Demostración. Sea $\mathcal{N}$ una FD relación obtenida a partir del operador clausura de una matroide. Supongamos que

$$(I \cup x, y) \in \mathcal{N} \text{ y } (I, y) \notin \mathcal{N}.$$

Entonces,

$$y \in c_M(I \cup x), \text{ y }, y \notin c_M(I).$$

Luego, por **(CL4)**, $x \in c_M(I \cup y)$. Así, existe H tal que

$$(I \cup y, H) \in \mathcal{N} \text{ y } (H, x) \in \mathcal{N},$$

luego

$$(I \cup y, x) \in \mathcal{N}.$$

Ahora, supongamos que $\mathcal{N}$ satisface **(FD4)**. Sea $y \in c_{\mathcal{N}}(I \cup x) - c_{\mathcal{N}}(I)$. Entonces existe J tal que

$$y \in J \text{ y } (I \cup x, J) \in \mathcal{N},$$

por lo que,

$$(I \cup x, y) \in \mathcal{N}.$$

Además, como

$$y \notin c_{\mathcal{N}}(I),$$

entonces,

$$(I, y) \notin \mathcal{N}.$$

Luego, por **(FD4)**, $(I \cup y, x) \in \mathcal{N}$. Concluimos que $x \in c_{\mathcal{N}}(I \cup y)$. $\square$

Proposición 2.21. *Una FD relación satisface el axioma* ***(FD4)****, si y sólo si, satisface el axioma:*

(FD4)' *Sean* $x \in E$*,* $I, J \subseteq E$*. Si* $(I \cup x, J) \in \mathcal{N}$ *y* $(I, J) \notin \mathcal{N}$*, entonces* $(I \cup J, x) \in \mathcal{N}$*.*

Demostración. Supongamos que $\mathcal{N}$ satisface **(FD4)**. Sean $x \in E$, $I, J \subseteq E$, tales que $(I \cup x, J) \in \mathcal{N}$ y $(I, J) \notin \mathcal{N}$. Entonces, existe $y \in J - I$ tal que $(I, y) \notin \mathcal{N}$, porque de lo contrario, $(I, y) \in \mathcal{N}$ para todo $y \in J - I$, y, por **(FD3)**, $(I, J) \in \mathcal{N}$; lo que es absurdo. Además, es claro que $(I \cup x, y) \in \mathcal{N}$. Luego, por **(FD4)**, $(I \cup y, x) \in \mathcal{N}$. Pero como $(I \cup J, I \cup y) \in \mathcal{N}$, entonces $(I \cup J, x) \in \mathcal{N}$.

Ahora, si suponemos que $\mathcal{N}$ satisface **(FD4)'**, basta hacer $J = \{y\}$ para comprobar que $\mathcal{N}$ satisface **(FD4)**. □

2.3. Topologías

No hace falta decir mucho para introducir las topologías, ampliamente conocidas en el mundo de las matemáticas. Son incluidas en este trabajo por su conexión con las FD relaciones, vía los operadores de clausura. En [2], el artículo base de este documento, no se hace mención de esta conexión; así, pues, en este trabajo se extendió el concepto de FD relación al caso infinito con el fin de establecer en qué forma una topología se puede ver como una FD relación.

Definición 2.22. *Una topología* τ *sobre un conjunto* X *arbitrario, es un subconjunto de* 2^X *que satisface:*

(T1) $X, \emptyset \in \tau$*,*

(T2) *si* $\{O_\lambda\}_{\lambda \in \Lambda} \subseteq \tau$*, entonces,* $\bigcup_{\lambda \in \Lambda} O_\lambda \in \tau$*, y,*

(T3) *si* $\{O_i\}_{i=1}^{n} \subseteq \tau$*, entonces,* $\bigcap_{i=1}^{n} O_i \in \tau$*.*

Definición 2.23. *Un conjunto* $O \in \tau$ *se llama abierto. Si* $A = O^c$*, entonces* A *es un cerrado. La adherencia de* $I \subseteq X$ *es el cerrado más pequeño que contiene a* I *y se nota por* $\overline{I}$*.*

Una topología se podría definir vía los conjuntos cerrados así:

Proposición 2.24. *τ es una topología sobre X, si y sólo si, el conjunto $\mathcal{C} = \{A : A = O^c$ para algún $O \in \tau\}$ satisface:*

1. $X, \emptyset \in \mathcal{C}$,
2. *si* $\{A_\lambda\}_{\lambda\in\Lambda} \subseteq \mathcal{C}$, *entonces,* $\bigcap\limits_{\lambda\in\Lambda} A_\lambda \in \mathcal{C}$, *y,*
3. *si* $\{A_i\}_{i=1}^n \subseteq \mathcal{C}$, *entonces,* $\bigcup\limits_{i=1}^{n} A_i \in \mathcal{C}$.

Demostración. Directa de la definición de topología. □

Proposición 2.25. *Sea τ una topología sobre X. El operador $c_\tau : 2^X \longrightarrow 2^X$ tal que $c_\tau(I) = \overline{I}$ es de clausura.*

Demostración. Por definición de clausura, $I \subseteq \overline{I}$ para todo $I \subseteq X$. Si $I \subseteq J \subseteq X$, entonces, $I \subseteq \overline{J}$, y como $\overline{I}$ es el cerrado más pequeño que contiene a I, entonces $\overline{I} \subseteq \overline{J}$. Por último, como $\overline{I}$ es cerrado, entonces $\overline{\overline{I}} = \overline{I}$. □

No todo operador de clausura es la adherencia de una topología. La siguiente proposición da condiciones necesarias y suficientes para que así sea.

Proposición 2.26. *Un operador de clausura c es la adherencia de una topología, si y sólo si,*

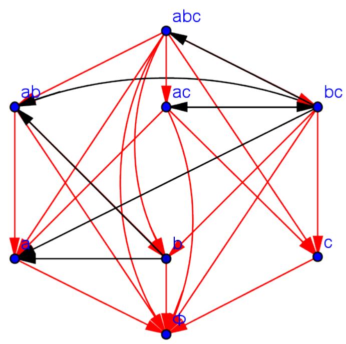
(CT1) $c(\emptyset) = \emptyset$, *y,*

(CT2) $c\left(\bigcup\limits_{k=1}^{n} I_k\right) = \bigcup\limits_{k=1}^{n} c(I_k)$.

Demostración. Ver [9]. □

Tenemos lo necesario para construir un ejemplo de una FD relación obtenida a partir de una topología.

Ejemplo 2.27. *Sea $N = \{a, b, c\}$, $\mathcal{C} = \{\emptyset, N, \{a\}, \{c\}, \{a, b\}, \{a, c\}\}$ el conjunto de los cerrados de una topología τ sobre N y sea c_τ el operador que asigna a cada subconjunto I de N el cerrado más pequeño que lo contenga. Siguiendo la construcción de la proposición 2.3, la FD relación asociada a c_τ es $\mathcal{N}_3 \cup \{(b, ab), (b, a), (bc, abc), (bc, ab), (bc, ac), (bc, a)\}$ (Ver figura).*



Tal como en el caso de las matroides, nos hacemos la siguiente pregunta: ¿Cómo se reflejan las propiedades **(CT1)-(CT2)** en las FD relaciones obtenidas a partir de topologías? La siguiente proposición se ocupa en responder esta pregunta.

Proposición 2.28. *La FD relación $\mathcal{N}$ con soporte X obtenida a partir del operador clausura de una topología τ sobre X satisface los axiomas adicionales:*

(FD5) *si $(\emptyset, J) \in \mathcal{N}$ para algún $J \subseteq X$, entonces $J = \emptyset$, y,*

(FD6) *si $(\bigcup_{k=1}^{n} I_k, J) \in \mathcal{N}$, entonces, existe una colección $\{J_k\}_{k=1,...,n}$ tal que, $J = \bigcup_{k=1}^{n} J_k$ con $(I_k, J_k) \in \mathcal{N}$ para todo $k = 1, ..., n$.*

*Además, si una FD relación $\mathcal{N}$ satisface **(FD5)-(FD6)**, entonces el operador de clausura $c_{\mathcal{N}}$ generado a partir de $\mathcal{N}$ satisface **(CT1)-(CT2)**, es decir, $c_{\mathcal{N}}$ es el operador clausura de una topología.*

Demostración. Sea $\mathcal{N}$ la FD relación con soporte X obtenida a partir de la topología τ. Veamos que $\mathcal{N}$ satisface **(FD5)-(FD6)**. Si $(\emptyset, J) \in \mathcal{N}$, entonces, $J \subseteq c_\tau(\emptyset) = \emptyset$, de donde $J = \emptyset$.

Ahora, si $(\bigcup_{k=1}^{n} I_k, J) \in \mathcal{N}$, entonces,

$$J \subseteq c_\tau(\bigcup_{k=1}^{n} I_k),$$

luego,

$$J \subseteq \bigcup_{k=1}^{n} c_\tau(I_k).$$

Pero esto implica que existen conjuntos J_k, $k = 1, ..., n$, tales que $J = \bigcup_{k=1}^{n} J_k$ y $J_k \subseteq c_\tau(I_k)$, es decir, $(I_k, J_k) \in \mathcal{N}$.

Supongamos ahora que $\mathcal{N}$ satisface **(FD5)-(FD6)**. Queremos ver que, $c_\mathcal{N}$ satisface **(CT1)-(CT2)**. **(CT1)** se cumple porque

$$c_\mathcal{N}(\emptyset) = \bigcup_{(\emptyset, J) \in \mathcal{N}} J = \emptyset.$$

Veamos que,

$$c_\mathcal{N}\left(\bigcup_{k=1}^{n} I_k\right) \subseteq \bigcup_{k=1}^{n} c_\mathcal{N}(I_k).$$

Si

$$x \in c_\mathcal{N}\left(\bigcup_{k=1}^{n} I_k\right),$$

entonces,

$$(\bigcup_{k=1}^{n} I_k, x) \in \mathcal{N}.$$

Así, por **(FD7)**, $(I_k, x) \in \mathcal{N}$ para algún $k = 1, ..., n$, de modo que $x \in c_\mathcal{N}(I_k)$. Concluimos que,

$$x \in \bigcup_{k=1}^{n} c_\mathcal{N}(I_k).$$

Por último, la contenencia

$$\bigcup_{k=1}^{n} c_\mathcal{N}(I_k) \subseteq c_\mathcal{N}\left(\bigcup_{k=1}^{n} I_k\right),$$

se satisface por ser $c_\mathcal{N}$ de clausura. □

2.4. Conexión de Galois

En la sección 2.1 se demostró que, dado un conjunto arbitrario N, hay una correspondecia biunívoca entre el conjunto $\mathbf{N}$ de las FD relaciones sobre N y el conjunto $\mathbf{C}$ de operadores de clausura sobre N. Dicho de otra forma, existe una biyección $\Phi : \mathbf{N} \longrightarrow \mathbf{C}$ tal que $\Phi(\mathcal{N}) = c_\mathcal{N}$ y $\Phi^{-1}(c) = \mathcal{N}_c$. Estas funciones resultan ser una conexión de Galois entre $\mathbf{N}$ y $\mathbf{C}$ dotados de ciertos ordenes, como lo veremos en esta sección. Cabe aclarar que, la conexión de Galois aquí presentada, difiere de la presentada en [2].

Definición 2.29. *Sean* $(X, \leq)$ *y* $(Y, \preceq)$ *dos conjuntos parcialmente ordenados. Una conexión de Galois entre* X *y* Y *es una pareja de funciones monótonas* $F : X \longrightarrow Y$ *y* $G : Y \longrightarrow X$ *tales que para todo* $x \in X$ *y* $y \in Y$*:*

$$F(x) \preceq y, \text{ si y sólo si, } G(y) \leq x.$$

Definición 2.30. *Sean* N *un conjunto arbitrario,* $\boldsymbol{N}$ *el conjunto de todas las FD relaciones sobre* N*, y,* $\boldsymbol{C}$ *el conjunto de todos los operadores de clausura sobre* N*. Entonces,* $(\boldsymbol{N}, \subseteq)$ *es el orden definido por contenencia, y,* $(\boldsymbol{C}, \leq)$ *es el orden definido así:*

$$c \leq k \text{ si } c(I) \subseteq k(I) \text{ para todo } I \in 2^N.$$

No es difícil verificar que $(\mathbf{C}, \leq)$ es, en efecto, un orden parcial.

Proposición 2.31. *Las funciones*

$$\Phi : (\boldsymbol{N}, \subseteq) \longrightarrow (\boldsymbol{C}, \leq),$$

y,

$$\Phi^{-1} : (\boldsymbol{C}, \leq) \longrightarrow (\boldsymbol{N}, \subseteq)$$

forman una conexión de Galois.

Demostración. Supongamos que, dados $\mathcal{N} \in \mathbf{N}$ y $c \in \mathbf{C}$, se satisface que,

$$\Phi^{-1}(c) = \mathcal{N}_c \subseteq \mathcal{N}.$$

Veamos que

$$c \leq \Phi(\mathcal{N}) = c_{\mathcal{N}},$$

es decir, veamos que,

$$c(I) \subseteq c_{\mathcal{N}}(I) \text{ para todo } I \in 2^N.$$

En efecto, dados $I \in 2^N$ y $x \in c(I)$, se tiene que $(I, x) \in \mathcal{N}_c$, luego, $(I, x) \in \mathcal{N}$, de donde $x \in c_{\mathcal{N}}(I)$.
Ahora, supongamos que

$$c \leq \Phi(\mathcal{N}) = c_{\mathcal{N}}.$$

Veamos que

$$\Phi^{-1}(c) = \mathcal{N}_c \subseteq \mathcal{N}.$$

Si $(I, J) \in \mathcal{N}_c$, es porque $J \subseteq c(I)$, entonces, $J \subseteq c_{\mathcal{N}}(I)$, pero esto significa que $(c_{\mathcal{N}}(I), J) \in \mathcal{N}$, así, dado que $(I, c_{\mathcal{N}}(I)) \in \mathcal{N}$, $(I, J) \in \mathcal{N}$. □

Capítulo 3

FD relaciones y otras teorías

Abordemos ahora la conexión entre FD Relaciones y otras teorías. No es necesario establecer dicha conexión vía los operadores de clausura (como en el caso de las matroides y las topologías), más bien, se utilizan métodos constructivos.

Así, en este capítulo, veremos que las FD relaciones son útiles para comprender las dependencias entre si de los elementos de un semiretículo inferior. También, demostraremos que toda función submodular (una generalización de función rango en matroides) define una FD relación, y, que toda FD relación finita define una función submodular que resulta ser una función de entropía [2].

3.1. Semiretículos

Un hecho interesante con respecto a las FD relaciones es su conexión con ciertos conjuntos parcialmente ordenados, entiéndase, los semiretículos.

Definición 3.1. *Un semiretículo inferior es un conjunto parcialmente ordenado en el que cada par de elementos tiene ínfimo, analogamente, un semiretículo superior es un conjunto parcialmente ordenado en el que cada par de elementos tiene supremo.*

La siguiente proposición muestra que todo semiretículo (inferior o superior) define una FD relación.

Proposición 3.2. *Sean $(Z, \wedge)$ un semiretículo inferior con elemento máximo 1 (o, pudiera ser también un semiretículo superior con mínimo), $z =$*

$(z_i)_{i\in N}$ un subconjunto de Z indexado por N finito y $z_I = \bigwedge_{i\in I} z_i$(tómese $z_\emptyset = 1$). Entonces, el conjunto $\mathcal{N} \subseteq 2^N \times 2^N$ definido de tal manera que

$$(I, J) \in \mathcal{N},\ \textit{si y sólo si},\ z_I \le z_J$$

es una FD relación.

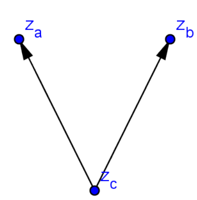
Prueba. 1. Si $I \supseteq J$ entonces $z_I \le z_J$.

2. Si $z_I \le z_J$ y $z_J \le z_K$, por transitividad, $z_I \le z_K$.

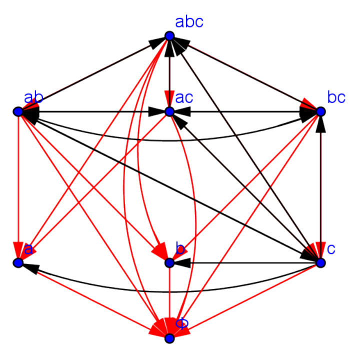
3. Si $z_I \le z_J$ y $z_I \le z_K$, se sigue que, $z_I \le z_{J\cup K}$ porque $z_I \le z_J \wedge z_K = z_{J\cup K}$.

□

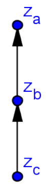
Ejemplo 3.3. *1. Considérese el semiretículo inferior de la figura*



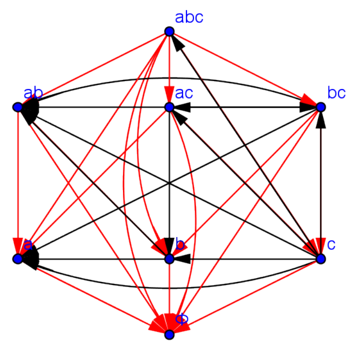
Según la construcción de la proposición anterior, la FD relación asociada al semiretículo inferior es



2. Ahora véase el semiretículo



La FD relación asociada es



3.2. Funciones Submodulares

Las funciones submodulares generalizan las funciones rango. Se demostrará que, dada una FD relación, se puede definir una función submudular y viceversa. Sin embargo, no existe una asociación biunívoca entre estos objetos. En la proposición 3.14, se construye una función submodular a partir de una FD relación finita; dicha función submodular resulta ser función de entropía.

Definición 3.4. *Diremos que la función $r : 2^N \longrightarrow \mathbb{R}$ es submodular sobre N, si*

$$r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y) \text{ para todo } X, Y \subseteq N,$$

y es no decreciente, si

$$r(X) \leq r(Y) \text{ cuando } X \subseteq Y \subseteq N.$$

Ejemplo 3.5. *La función dimensión de un subconjunto de un espacio vectorial es submodular no decreciente.*

En el capítulo anterior se introdujeron las nociones de matroide y de rango de una matroide. Estas no son más que generalizaciones de los conceptos de independencia lineal y de dimensión de espacio vectorial, respectivamente. Se probó que la función rango de una matroide es submodular. Se probó también que las matroides son casos particulares de FD relaciones. Así pues, es de esperar que haya en las FD relaciones una función de características similares a la función rango. Pero, ¿cómo definir tal función submodular?. Las proposiciones siguientes se incluyen con la idea de encontrar una función, no sólo no decreciente, sino también submodular asociada a una FD relación arbitraria finita. El plan es el siguiente:

1. A partir de un conjunto especial A, definir una FD relación $\mathcal{N}_A$ (proposición 3.6).
2. Construir una función submodular no decreciente r_A, asociada a la FD relación $\mathcal{N}_A$ (proposiciones 3.10,3.12, corolario 3.13).
3. Ver que toda FD relación finita se puede ver en la forma $\mathcal{N}_A$ (proposición 3.14).

Proposición 3.6. *Sea N un conjunto finito. Para cada $i \in N$, sean X_i un conjunto finito no vacío, $X_I = \prod_{i \in I} X_i$ para cada $I \subseteq N$ y $X = X_N$. Además, si $x = (x_i)_{i \in N}$, entonces x_I es la proyección canónica de $x \in X$ sobre X_I. Si $A \subseteq X$, entonces el conjunto $\mathcal{N}_A$ definido de tal manera que*

$$(I, J) \in \mathcal{N}_A, \text{ si y sólo si, } x_I = y_I \text{ implica } x_J = y_J \text{ para todo } x, y \in A$$

es una FD relación.

Prueba.

1. Si $I \supseteq J$ entonces $x_I = y_I$ implica $x_J = y_J$.
2. Si para todo $x, y \in A$, $x_I = y_I$ implica $x_J = y_J$, y, $x_J = y_J$ implica $x_K = y_K$, entonces, para todo $x, y \in A$ tal que $x_I = y_I$ se tiene que $x_K = y_K$.
3. Si para todo $x, y \in A$, $x_I = y_I$ implica $x_J = y_J$ y $x_K = y_K$, entonces también se tiene que $x_{J \cup K} = y_{J \cup K}$.

□

La clases de equivalencia definidas en la próxima proposición, son cruciales para la construcción de una función r_A asociada a $\mathcal{N}_A$, que resultará ser submodular no decreciente.

Proposición 3.7. $R_I^A =: \{(x,y) \in A \times A : x_I = y_I\}$ *es una relación de equivalencia. Si* $(I,J) \in \mathcal{N}_A$ *entonces* $R_I^A \subseteq R_J^A$*. Esto quiere decir que* A/R_I^A *es un refinamiento de* A/R_J^A*.*

Demostración. Por verificación directa, se ve que R_I^A es una relación de equivalencia. Si $(I,J) \in \mathcal{N}_A$, entonces para todo $x, y \in A$ se tiene que $x_I = y_I$ implica $x_J = y_J$. En otras palabras, $(x,y) \in R_I^A$ implica $(x,y) \in R_J^A$. Para ver que A/R_I^A es un refinamiento de A/R_J^A, nótese que si $y \in [x]_{R_I^A}$ entonces $y \in [x]_{R_J^A}$, luego toda clase de A/R_I^A está contenida en alguna clase de A/R_J^A. □

Proposición 3.8. *Para todo* $x \in A$

(a) $[x]_{R_{I\cup J}^A} = [x]_{R_I^A} \cap [x]_{R_J^A}$

(b) $[x]_{R_{I\cap J}^A} \supseteq [x]_{R_I^A} \cup [x]_{R_J^A}$

Demostración. (a) $[x]_{R_{I\cup J}^A} = \{y \in A : x_{I\cup J} = y_{I\cup J}\} = \{y \in A : x_I = y_I\} \cap \{y \in A : x_J = y_J\} = [x]_{R_I^A} \cap [x]_{R_J^A}$.

(b) $[x]_{R_{I\cap J}^A} = \{y \in A : x_{I\cap J} = y_{I\cap J}\} \supseteq \{y \in A : x_I = y_I\} \cap \{y \in A : x_J = y_J\} = [x]_{R_I^A} \cup [x]_{R_J^A}$.

□

Corolario 3.9. *(a) Para cada clase de equivalencia* F_i *(*G_j*) de la partición* A/R_I^A *(*A/R_J^A*), existe una única clase de equivalencia* H_k *de la partición* $A/R_{I\cap J}^A$ *que la contiene.*

(b) Toda clase de equivalencia E_l *de la partición* $A/R_{I\cup J}^A$ *es la intersección de una clase* F_i *con una clase* G_j*.*

Proposición 3.10. *Sean* N *finito y* A *como en la proposición 3.6. La función* $r_A : 2^N \longrightarrow \mathbb{R}$

$$r_A(I) = -\sum_{G \in A/R_I^A} \frac{|G|}{|A|} \ln \frac{|G|}{|A|}$$

es no decreciente.

Prueba. Veamos que r_A es no decreciente. Sean $I, J \subseteq N$ tales que $I \supseteq J$. Sea $G \in A/R_J^A$. Entonces, G es unión disyunta de clases de A/R_I^A porque A/R_I^A es un refinamiento de A/R_J^A. Luego,

$$|G| = \sum_{\substack{F \subseteq G \\ F \in A/R_I^A}} |F|.$$

Así,

$$\begin{aligned} r_A(J) = -\sum_{G \in A/R_J^A} \frac{|G|}{|A|} \ln \frac{|G|}{|A|} &= -\sum_{G \in A/R_J^A} \sum_{\substack{F \subseteq G \\ F \in A/R_I^A}} \frac{|F|}{|A|} \ln \frac{|G|}{|A|} \\ &= -\sum_{F \in A/R_I^A} \frac{|F|}{|A|} \ln \frac{|G_F|}{|A|}, \end{aligned}$$

donde G_F es la clase de A/R_J^A que contiene a F. Ahora bien,

$$1 \geq \frac{|G_F|}{|A|} \geq \frac{|F|}{|A|}$$

luego

$$\ln 1 \geq \ln \frac{|G_F|}{|A|} \geq \ln \frac{|F|}{|A|}$$

$$0 \geq \frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} \geq \frac{|F|}{|A|} \ln \frac{|F|}{|A|}$$

$$0 \leq -\frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} \leq -\frac{|F|}{|A|} \ln \frac{|F|}{|A|}$$

$$0 \leq r_A(J) = -\sum_{F \in A/R_I^A} \frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} \leq -\sum_{F \in A/R_I^A} \frac{|F|}{|A|} \ln \frac{|F|}{|A|} = r_A(I)$$

.

□

Demostraremos la submodularidad de r_A recurriendo a la noción de entropía (véase el apéndice A). Para empezar, retomemos los conjuntos y las clases de equivalencia definidos en las proposiciones 3.6 y 3.7. Notaremos con F_i a las clases de equivalencia de A/R_I^A, con G_j a las de A/R_J^A, con H_k a las de $A/R_{I\cap J}^A$ y con E_l a las de $A/R_{I\cup J}^A$. Supóngase que se quiere escoger un elemento de A al azar, y supóngase también que todos tienen la misma probabilidad de ser escogidos, es decir, que la probabilidad de escogencia de un elemento es $1/|A|$. Así, la probabilidad de escoger un elemento de la clase de equivalencia F_i es $|F_i|/|A|$.

Defínase el evento x_i como la escogencia de un elemento de la clase F_i, el evento y_j, como la escogencia de un elemento de la clase G_j y el evento z_k, como la escogencia de un elemento de la clase H_k, entonces

$$\begin{aligned} p(x_i) &= \frac{|F_i|}{|A|}, & p(y_j) &= \frac{|G_j|}{|A|}, \\ p(z_k) &= \frac{|H_k|}{|A|}, & p(x_i, z_k) &= \frac{|F_i \cap H_k|}{|A|}, \\ p(y_j, z_k) &= \frac{|G_j \cap H_k|}{|A|}, & p(x_i, y_j, z_k) &= \frac{|F_i \cap G_j \cap H_k|}{|A|}. \end{aligned}$$

Proposición 3.11. *(a) $p(x_i, z_k) = p(x_i)$, siempre que $F_i \subseteq H_k$.*

(b) $p(y_j, z_k) = p(y_j)$, siempre que $G_j \subseteq H_k$.

(c) $p(x_i, y_j, z_k) = p(x_i, y_j)$, siempre que $F_i, G_j \subseteq H_k$.

Proposición 3.12. *Sean $X = \{x_1, ..., x_{|A/R_I^A|}\}$, $Y = \{y_1, ..., y_{|A/R_J^A|}\}$ y $Z = \{z_1, ..., z_{|A/R_{I\cap J}^A|}\}$. Entonces,*

(a) $H(X) = H(X, Z) = r_A(I)$

(b) $H(Y) = H(Y, Z) = r_A(J)$

(c) $H(Z) = r_A(I \cap J)$

(d) $H(X, Y) = H(X, Y, Z) = r_A(I \cup J)$

Demostración. Probemos *(a)*. Nótese que, por la proposición 3.8, para cualesquiera que sean F_i y H_k, se tiene que $F_i \subseteq H_k$ ó que $F_i \cap H_k = \emptyset$. Así, en la parte derecha de la igualdad

$$H(X, Z) = -\sum_{i,k} p(x_i, z_k) \ln p(x_i, z_k)$$

los únicos términos no nulos son aquellos para los cuales los subíndices i y k son tales que $F_i \subseteq H_k$. Además, como $p(x_i, z_k) = p(x_i)$ siempre que

$F_i \subseteq H_k$, y, como para todo i existe un único k tal que $F_i \subseteq H_k$ (corolario 3.9), entonces,

$$\begin{aligned} H(X,Z) &= -\sum_{i,k} p(x_i, z_k) \ln p(x_i, z_k) \\ &= -\sum_{i} p(x_i) \ln p(x_i) = H(X). \end{aligned}$$

Las igualdades *(b)* y *(d)* se demuestran de manera similar. Las igualdades $H(X) = r_A(I)$ y *(c)* se deducen directamente de las definiciones. $\square$

Corolario 3.13. *La función r_A es submodular.*

Hasta aquí, hemos obtenido funciones submodulares sólo para ciertas FD relaciones. En la siguiente proposición, nos proponemos mostrar que toda FD relación finita es, de hecho, del tipo $\mathcal{N}_A$.

Proposición 3.14. *Toda FD relación $\mathcal{N}$ con soporte N finito, define una función submodular $r_{\mathcal{N}}$.*

Demostración. La idea es encontrar un conjunto A contenido en algún producto cartesiano de conjuntos finitos de tal manera que la FD relación $\mathcal{N}_A$ obtenida según el procedimiento de la proposición 3.6 sea precisamente $\mathcal{N}$.

Si $\mathcal{N} = 2^N \times 2^N$, sean $X_i = \{1\}$ para cada $i \in N$, $X = \prod_{i \in N} X_i$ y $A = X$, así, $\mathcal{N} = \mathcal{N}_A$, y, por las proposiciones 3.15 y 3.16, la función submodular definida por $\mathcal{N}$ es constante.

Si $\mathcal{N}$ está contenido estrictamante en $2^N \times 2^N$, sean p el número de elementos de $2^N \times 2^N$ que no pertenecen a $\mathcal{N}$, $X_i = \{1, 2, ..., 2p\}$ para cada $i \in N$, y $X = \prod_{i \in N} X_i$.

Recuérdese que para cada $I \in 2^N$ se define la clausura de I como

$$c(I) = \bigcup_{(I,H) \in \mathcal{N}} H.$$

Sea $(I, J) \in 2^N \times 2^N$ tal que $(I, J) \notin \mathcal{N}$. Nótese que $J \nsubseteq c(I)$ porque, de lo contrario, $(c(I), J) \in \mathcal{N}$, y, como $(I, c(I)) \in \mathcal{N}$, entonces, $(I, J) \in \mathcal{N}$, lo cual es absurdo. Identifiquemos a cada pareja $(I, J) \notin \mathcal{N}$ con un único número natural $k = 1, ..., p$, y viceversa. Entonces, definimos $x^{(2k-1)}, x^{(2k)} \in X$ así:

$$x_i^{(2k-1)} = 2k - 1 \text{ para todo } i \in N,$$

$$x_i^{(2k)} = \begin{cases} 2k-1, & \text{si } i \in c(I), \\ 2k, & \text{en otro caso.} \end{cases}$$

Sea $A = \{x^{(n)} \in X : n = 1, ..., 2p\}$. Nótese que, si k es el natural con el que identificamos a $(I, J) \notin \mathcal{N}$, entonces $x_i^{(2k-1)} = x_i^{(2k)}$ para todo $i \in I$, pero existe $j \in J$ tal que $x_j^{(2k-1)} \neq x_j^{(2k)}$ porque $J \nsubseteq c(I)$. Así, $(I, J) \notin \mathcal{N}_A$.

Veamos ahora que si $(I, J) \in \mathcal{N}$ entonces $(I, J) \in \mathcal{N}_A$.

Sea $(I, J) \in \mathcal{N}$. Para cada $(I', J') \notin \mathcal{N}$ tal que $I \subseteq c(I)$, se tiene que $J \subseteq c(I')$. Así, si k es el natural con el que idenficamos a (I', J'), entonces $x_i^{(2k-1)} = x_i^{(2k)}$ para todo $i \in I \cup J$, es decir, $x_{I\cup J}^{(2k-1)} = x_{I\cup J}^{(2k)}$, por lo que $x_I^{(2k-1)} = x_I^{(2k)}$ implica $x_J^{(2k-1)} = x_J^{(2k)}$. Y para cada par $(I', J') \notin \mathcal{N}$ tal que $I \nsubseteq c(I')$, se tiene que $x_I^{(2k-1)} \neq x_I^{(2k)}$, donde k es el natural que corresponde a (I', J'). Concluimos que $(I, J) \in \mathcal{N}_A$. □

En la siguiente proposición demostraremos que toda función submodular define una FD relación.

Proposición 3.15. *Si r es una función submodular sobre un conjunto N arbitrario, entonces el conjunto*

$$\mathcal{N}_r = \{(I, J) \in 2^N \times 2^N : r(I) = r(I \cup J)\}$$

es una FD relación.

Prueba. 1. Si $I \supseteq J$, entonces $r(I) = r(I \cup J)$, luego $(I, J) \in \mathcal{N}$.

2. Si $(I, J) \in \mathcal{N}$ y $(J, K) \in \mathcal{N}$, entonces $r(I) = r(I \cup J)$ y $r(J) = r(J \cup K)$. Ahora, por la submodularidad y por el no decrecimiento de r, tenemos que,

   $$r(I \cup J) + r(J \cup K) \geq r(I \cup J \cup K) + r(J \cup (I \cap K)) \geq r(I \cup K) + r(J),$$

   luego $r(I) + r(J) \geq r(I \cup K) + r(J)$, de donde $r(I) = r(I \cup K)$.

3. Si $(I, J) \in \mathcal{N}$ y $(I, K) \in \mathcal{N}$, entonces $r(I) = r(I \cup J)$ y $r(I) = r(I \cup K)$. Además, como

   $$2r(I) = r(I \cup J) + r(I \cup K) \geq r(I \cup J \cup K) + r(I \cup (J \cap K)) \geq$$
   $$r(I \cup J \cup K) + r(I),$$

entonces $r(I) = r(I \cup J \cup K)$.

$\square$

Finalmente, veamos que, si una función submodular se obtiene a través de una FD relación finita $\mathcal{N}$, entonces, la FD relación obtenida a partir de dicha función submodular, es precisamente $\mathcal{N}$.

Proposición 3.16. *Sea A un conjunto como en la proposición 3.6. Entonces, $\mathcal{N}_{r_A} = \mathcal{N}_A$.*

Demostración. Veamos que $\mathcal{N}_A \subseteq \mathcal{N}_{r_A}$. Sea $(I, J) \in \mathcal{N}_A$. Entonces $(I, I \cup J) \in \mathcal{N}_A$. Esto significa que A/R_I^A es un refinamiento de $A/R_{I \cup J}^A$, así, por el mismo razonamiento con el que se demostró el no decrecimiento de r_A en la proposición 3.10, $r_A(I \cup J) \leq r_A(I)$, luego, $r_A(I \cup J) = r_A(I)$ y por lo tanto $(I, J) \in \mathcal{N}_{r_A}$.

Ahora, veamos que $\mathcal{N} \subseteq \mathcal{N}_A$. Sea $(I, J) \in \mathcal{N}_{r_A}$. Entonces, $r_A(I) = r_A(I \cup J)$, pero como $A/R_{I \cup J}^A$ es un refinamiento de A/R_I^A, se tiene que

$$r_A(I) = -\sum_{F \in A/R_{I \cup J}^A} \frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} = -\sum_{F \in A/R_{I \cup J}^A} \frac{|F|}{|A|} \ln \frac{|F|}{|A|} = r_A(I \cup J)$$

donde G_F es la clase de A/R_I^A que contiene a F. Nótese que aunque $-\frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} \leq -\frac{|F|}{|A|} \ln \frac{|F|}{|A|}$, no existen F y G_F tales que $-\frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} < -\frac{|F|}{|A|} \ln \frac{|F|}{|A|}$ porque, si existieran, $r_A(I) < r_A(I \cup J)$, lo cual es absurdo. Luego, para cada F y cada G_F,

$$-\frac{|F|}{|A|} \ln \frac{|G_F|}{|A|} = -\frac{|F|}{|A|} \ln \frac{|F|}{|A|}$$

$$\ln \frac{|G_F|}{|A|} = \ln \frac{|F|}{|A|}$$

$$\frac{|G_F|}{|A|} = \frac{|F|}{|A|}$$

$$|G_F| = |F|,$$

y, como $F \subseteq G_F$ y ambas son clases finitas, entonces $F = G_F$ para cada $F \in A/R_{I \cup J}^A$. Entonces, $A/R_I^A = A/R_{I \cup J}^A$, o lo que es lo mismo, $x_I = y_I$, si y sólo si, $x_{I \cup J} = y_{I \cup J}$, luego, $x_I = y_I$ implica $x_J = y_J$, y, por lo tanto, $(I, J) \in \mathcal{N}_A$. $\square$

Corolario 3.17. *Sea* $r_{\mathcal{N}}$ *la función submodular obtenida a partir de la FD relación finita* $\mathcal{N}$ *según la proposición 3.14. Entonces* $\mathcal{N}_{r_{\mathcal{N}}} = \mathcal{N}$*.*

Demostración. Sea A el conjunto tal que $\mathcal{N} = \mathcal{N}_A$ y $r_{\mathcal{N}} = r_A$. Entonces, por la proposición 3.16, $\mathcal{N} = \mathcal{N}_{r_A} = \mathcal{N}_{r_{\mathcal{N}}}$. $\square$

Capítulo 4

FD relaciones y códigos de red

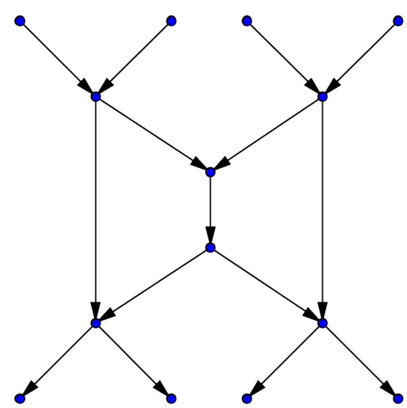
El problema de la codificación de redes consiste en encontrar modos eficientes de transmitir el flujo de información a través de los canales de una red, modelandola como un digrafo (un grafo cuyas aristas tienen dirección) e interpretando la información sobre algún alfabeto. A medida que la información va recorriendo las aristas, se transforma haciendo uso de ciertas funciones escogidas de tal forma que se permita la entrega de los datos enviados por ciertos nodos, denominados fuentes, hasta otros que demandan la información llamados receptores.

Vía las matroides, es posible encontrar la solución de algunos problemas de codificación de redes ([5],[3]), sin embargo, en [3], se demuestra que las FD relaciones resultan ser estructuras más adecuadas para capturar las dependencias e independencias en las redes de información.

No es el propósito de este trabajo el hacer un estudio detallado de la resolución de problemas de codificación redes (un estudio detallado de estos problemas se hace en [4]), más bien, se busca demostrar el resultado citado en [3] (aquí, proposición 4.8), que describe el estrecho vínculo entre FD relaciones y las redes de información que se trabajan en el artículo ya mencionado.

Definición 4.1. *Sea $G = G(V, E)$ un grafo dirigido acíclico (es decir, que las aristas tienen dirección y no existen caminos de retorno a un vértice) con conjunto de vértices V y conjunto de aristas $E \subseteq V \times V$. El grado de entrada de un vértice u es el número de aristas que entran a u, o sea, el* *número de aristas cuya cabeza es u; y, el grado de salida de u es el número de aristas que salen de u, es decir, el número de aristas cuya cola es u. El conjunto de aristas cuya cabeza es u será denotado con $In(u)$; mientras que el conjunto de aristas cuya cola es u será denotado con $Out(u)$. Si u y v son la cola y la cabeza de e respectivamente, escribiremos $e(u,v)$. Para cada arista $e = e(u,v) \in E$, sean $In(e) = \{a \in E : a \in In(u)\}$ y $Out(e) = \{a \in E : a \in Out(v)\}$. El grado de entrada de e es $|In(e)|$ y el grado de salida $|Out(e)|$. Sean S el conjunto de vértices cuyo grado de entrada es cero y D el conjunto de vértices cuyo grado de salida es cero. Los nodos que son cola de alguna arista de S son nodos fuente y los nodos que son cabeza de alguna arista de D es un nodo terminal. Asumimos que los elementos de E están numerados y definimos $m = |E|, k = |S|$, y, $d = |D|$. Asumimos también que $S = \{e_1, ..., e_k\}$ y $D = \{e_{m-d+1}, ..., e_m\}$.*

Ejemplo 4.2. *Considérese el grafo,*



nótese que no existen caminos que retornen a un vértice.

En un grafo dirigido acíclico, los nodos y las aristas bien podrían representar una red de computadoras. Habría computadoras emisoras y computadoras receptoras que demandan cierta información de las primeras. Si la información es enviada en forma de mensajes codificados, entonces, dichos mensajes, son transformados y re-enviados por cada una de las computadoras de la red, de tal manera que las receptoras puedan decodificar la información que han solicitado.

Dicho lo anterior, es necesario, pues, escoger un alfabeto en el cual codificar los mensajes, y, definir funciones sobre cada una de las aristas del grafo de manera que se pueda garantizar la demanda de la red. Las siguientes definiciones formalizan las ideas descritas.

Definición 4.3. *Sean $G = G(V, E)$ tal como se definió anteriormente, Σ un alfabeto de cardinal q y $\delta : D \longrightarrow S$ una función sobreyectiva. Una red es un par $N(G(V, E), \delta)$. Asumimos que $e_i \in S$ carga un mensaje $x(e_i) = x_i \in \Sigma^n, n \in \mathbb{N}$. La función δ especifica que mensaje $x(\delta(e_j))$ es requerido por cada $e_j \in D$. Llamaremos a δ una función de demanda. Denotaremos por $\xi = (x_1, ..., x_k) \in \Sigma^{nk}$ a la concatenación de todos los mensajes cargados por las aristas de S.*

Definición 4.4. *Un código de red (n, q) para la red $N(G, \delta)$ es una colección de funciones*

$$\{f_e = (f_e^1, ..., f_e^n) : e \in E, f_e^i : \Sigma^{nk} \longrightarrow \Sigma\}$$

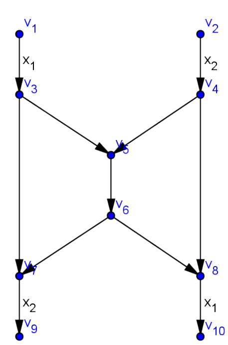
llamadas funciones de decodificación que satisfacen, para todo $\xi \in \Sigma^{nk}$, las siguientes condiciones:

(N1) $f_{e_i}(\xi) = x_i$ *para* $i = 1, ..., k$,

(N2) $f_{e_j}(\xi) = x(\delta(e_j))$ *para* $j = m - d + 1, ..., m$, *y,*

(N3) Para cada $e \in E - S$ existe una función $\phi_e : \Sigma^{|In(e)|n} \longrightarrow \Sigma^n$, a la que llamaremos función de decodificación local, tal que $f_e(\xi) = \phi_e(f_{c_1}(\xi), ..., f_{c_{|In(e)|}}(\xi))$ donde $c_i \in In(e)$ para $i = 1, ..., |In(e)|$.

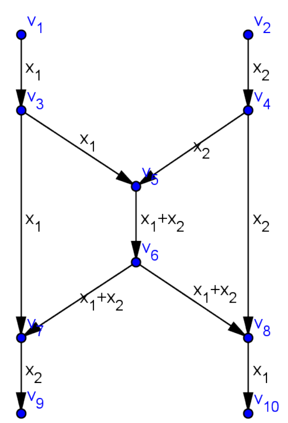
Ejemplo 4.5. *Considérese la red,*



Los rótulos sobre las aristas fuente y sobre las receptoras, representan los mensajes enviados y demandados, respecivamente. Nos proponemos encontrar un código de red. Tomemos $\Sigma = \mathbb{F}_2$ (en este ejemplo el alfabeto es *además una estructura algebraica, aunque esto no es necesario según nuestras definiciones) y* $n = 1$*. Entonces* $k = 2$ *y* $\xi = (x, y)$*. Así, un código de red es:*

- $f_{v_1v_3}(\xi) = x$;
- $f_{v_2v_4}(\xi) = y$;
- $f_{v_3v_5}(\xi) = \phi_{v_3v_5}(f_{v_1v_3}(\xi)) := f_{v_1v_3}(\xi) = x$;
- $f_{v_4v_5}(\xi) = \phi_{v_4v_5}(f_{v_2v_4}(\xi)) := f_{v_2,v_4}(\xi) = y$;
- $f_{v_5v_6}(\xi) = \phi_{v_5v_6}(f_{v_3v_5}(\xi), f_{v_4v_5}(\xi)) := f_{v_3v_5}(\xi) + f_{v_4v_5}(\xi) = x + y$;
- $f_{v_6v_7}(\xi) = \phi_{v_6v_7}(f_{v_5v_6}(\xi)) := f_{v_5v_6}(\xi) = x + y$;
- $f_{v_6v_8}(\xi) = \phi_{v_6v_8}(f_{v_5v_6}(\xi)) := f_{v_5v_6}(\xi) = x + y$;
- $f_{v_3v_7}(\xi) = \phi_{v_3v_7}(f_{v_1v_3}(\xi)) := f_{v_1v_3}(\xi) = x$;
- $f_{v_4v_8}(\xi) = \phi_{v_4v_8}(f_{v_2v_4}(\xi)) := f_{v_2,v_4}(\xi) = y$;
- $f_{v_7v_9}(\xi) = \phi_{v_7v_9}(f_{v_3v_7}(\xi), f_{v_6v_7}(\xi)) := f_{v_3v_7}(\xi) + f_{v_6v_7}(\xi) = 2x + y = y$;
- $f_{v_8v_{10}}(\xi) = \phi_{v_8v_{10}}(f_{v_6v_8}(\xi), f_{v_4v_8}(\xi)) := f_{v_6v_8}(\xi) + f_{v_4v_8}(\xi) = x + 2y = x$.

En la siguiente figura, se visualiza la red junto a su cóigo de red.



4.1. Conexión entre las FD relaciones y las soluciones de problemas de codificación en redes

La proposición 4.8 conecta los códigos de red con las FD relaciones [3]. Se procede construyendo una FD relación a partir del grafo de la red, y se demuestra que la red tiene solución, si y sólo si, la FD relación posee una representación funcional sobre los mismos conjuntos en los que están definidas las funciones del código de red.

Comenzamos definiendo el concepto de representación funcional de una FD relación.

Definición 4.6. *Sea $\{f_i\}_{i\in N}$ una colección de funciones de un conjunto no vacío B en un conjunto C, y para cada $I \subseteq N$ sea $f_I : B \longrightarrow \prod_{i\in I} C$ tal que $f_I(b) = (f_i(b))_{i\in N}$. Diremos que la colección $\{f_i\}_{i\in N}$ es una representación funcional de una FD relación $\mathcal{N}$, si*

$$\text{para todo } (I,J) \in \mathcal{N} \text{ existe una función } g_{I,J} : \prod_{i\in I} C \longrightarrow \prod_{j\in J} C \text{ tal que } f_J = g_{I,J} \circ f_I.$$

Sean $N(G(V,E),\delta)$ una red, V' el conjunto de nodos no conectados con una arista terminal y de grados de entrada y de salida positivos, y, V'' el conjunto de nodos que son cabeza de alguna arista terminal. Sea $\mathcal{N}_{N(G,\delta)}$ la menor FD relación que contenga al conjunto

$$M = \{(In(v), Out(v)) : v \in V'\} \cup \{(In(v), \delta(Out(v))) : v \in V''\}.$$

¿Cómo es $\mathcal{N}_{N(G,\delta)}$?. La siguiente proposición, del autor de este trabajo, nos da la respuesta.

Proposición 4.7. *Sean $N(G(V,E),\delta)$ una red,*
$E_I = \{J \subseteq E :$ si $e...e''$ es un camino tal que $e \in S$ y $e'' \in J$ entonces $e...e''$ comparte por lo menos una arista con $I\}$ y

$$\mathcal{L} = \{(I,J) \in 2^E \times 2^E : \text{ para algún } v \in V' \cup V'',\ I \supseteq In(v) \text{ y } J \in E_I\}.$$

Entonces

$$\mathcal{N}_{N(G,\delta)} = \mathcal{N}_{|E|} \cup \mathcal{L}.$$

Demostración. Veamos que $\mathcal{N}_{|E|} \cup \mathcal{L}$ es una FD relación.

1. El axioma **(FD1)** se satisface gracias a $\mathcal{N}_{|E|}$.

2. Para ver **(FD2)** debemos considerar casos.

   a) Si $(I, J) \in \mathcal{N}_{|E|}$ y $(J, K) \in \mathcal{L}$, entonces $I \supseteq J$ y $J \supseteq In(v)$ para algún $v \in V$; luego $I \supseteq In(v)$. De modo que $(I, K) \in \mathcal{L}$.

   b) Si $(I, J) \in \mathcal{L}$ y $(J, K) \in \mathcal{N}_{|E|}$, entonces $J \in E_I$ y $J \supseteq K$, de modo que $K \in E_I$, y así $(I, K) \in \mathcal{L}$.

   c) Ahora, sean $I, J, K \subseteq E$ y $v_1, v_2 \in V$ tales que $I \subseteq In(v_1)$, $J \subseteq In(v_2)$, $J \in E_I$ y $K \in E_J$. Entonces, todo camino que empieza en un nodo fuente y llega a K pasa por J, luego, pasa por I. Por lo tanto $(I, K) \in \mathcal{L}$

3. Verificar **(FD3)** es sencillo.

Veamos que $\mathcal{N}_{N(G,\delta)}$ es la FD relación más pequeña que contiene a M. Sean $(I, J) \in \mathcal{N}_{N(G,\delta)}$, $a \in J$ y C_a el conjunto de caminos que empieza en S y termina en a. Para cada $c \in C_a$, sea e_c la primera arista de c que pertenece a I; y, si $e \in c$, sea $grad_c(e)$ el número de aristas que hay entre e_c y e, inclusive e. Si $e \notin c$, $grad_c(e) = 0$. Sea $grad(e) = \max\limits_{c \in C_a} grad_c(e)$. Para cada $n \in \mathbb{N}$, sea $I_n = \{e \in E : grad(e) = n\}$. Veamos que, dada una FD relación $\mathcal{N} \supseteq M$, $(I, I_n) \in \mathcal{N}$ para todo $n \geq 1$. Nótese que $I_1 \neq \emptyset$. Nótese también que, si $e \in I_1$, entonces $In(e) \subseteq I$, luego $(I, e) \in \mathcal{N}$, de donde $(I, I_1) \in \mathcal{N}$. Supongamos ahora que $(I, I_n) \in \mathcal{N}$. Ahora, nótese que, si $e \in I_{n+1}$, entonces $In(e) \subseteq \bigcup\limits_{k=1,\ldots,n} I_k$, de donde $(I, e) \in \mathcal{N}$, y, $(I, I_{n+1}) \in \mathcal{N}$. Así, como $a \in I_m$ para algún m entonces $(I, a) \in \mathcal{N}$. Concluimos que $(I, J) \in \mathcal{N}$.

□

Proposición 4.8. *[3] La red $N(G(V, E), \delta)$ tiene un código de red (n, q) si y sólo si $\mathcal{N}_{N(G,\delta)}$ tiene una representación funcional con $|B| = q^{kn}$ y $|C| = q^n$.*

Demostración. Supongamos que $(I, J) \in \mathcal{N}_{N(G,\delta)}$ y que $N(G(V, E), \delta)$ tiene un código de red (n, q). Cualquier camino $e...e''$ con $e \in S$ y $e'' \in J$ debe pasar por I. Lo anterior implica que existe una función $\varphi_{e''} : \Sigma^{|I|n} \longrightarrow \Sigma^n$ tal que $f_{e''}(\xi) = \varphi_{e''}((f_e(\xi))_{e \in I})$. Sea $g_{I,J} : \Sigma^{|I|n} \longrightarrow \Sigma^{|J|n}$ tal que

$$g_{I,J} = (\varphi_{e''})_{e'' \in J}.$$

Entonces $f_J = g_{I,J} \circ f_I$, $B = \Sigma^{nk}$ y $C = \Sigma^n$.

Ahora, supongamos que existe una representación funcional para $\mathcal{N}_{N(G,\delta)}$ con $|B| = q^{nk}$ y $|C| = q^n$. Entonces, para todo par $(I, J) \in \mathcal{N}_{N(G,\delta)}$, existen funciones

$$\tilde{f}_I : B \longrightarrow C, \quad \tilde{f}_J : B \longrightarrow C \quad \text{y} \quad \tilde{g}_{I,J} : C^{|I|} \longrightarrow C^{|J|}$$

tales que $\tilde{f}_J = \tilde{g} \circ \tilde{f}_I$. Pero también existen biyecciones $h_1 : B \longrightarrow \Sigma^{nk}$ y $h_2 : C \longrightarrow \Sigma^n$; y así, existen funciones

$$f_I : h_1(B) \longrightarrow h_2(C), \quad f_J : h_1(B) \longrightarrow h_2(C) \text{ y},$$

$$g_{I,J} : (h_2(C))^{|I|} \longrightarrow (h_2(C))^{|J|}$$

tales que $f_J = g \circ f_I$. Como $(In(v), Out(v)) \in \mathcal{N}_{N(G,\delta)}$ para cada $v \in V'$ y $(In(v), \delta(Out(v))) \in \mathcal{N}_{N(G,\delta)}$ para cada $v \in V''$, tenemos pues, un código de red lineal. $\square$

Conclusiones

Para la realización de este trabajo, se han tomado como base [2] y [3]. Se han detallado minuciosamente los resultados de los artículos citados, concernientes a las propiedades de las FD relaciones y sus conexiones con los operadores de clausura, los problemas de Codificación en Redes y otros objetos.

No obstante, se han demostrado también resultados nuevos, entre los que destacamos aquellos que describen las topologías como casos particulares de FD relaciones, vía los operadores de clausura. Así, una cuestión que se podría abordar en futuras investigaciones, es cómo conectar la Topología con la Teoría de Codificación en Redes. La motivación para estudiar dicha relación está en que los problemas de Codificación en Redes están vinculados con las FD relaciones (capítulo 4), y, en que a través de las matroides, que como las topologías son casos particulares de FD relaciones, se hallan soluciones para algunos de tales problemas ([3],[5]).

Apéndice A

Una introducción a Entropía

Definición A.1. *Sean X, Y y Z variables aleatorias finitas con función de probabilidad dada por*

$$p(x_i, y_j, z_k) := Pr(X = x_i, Y = y_j, Z = z_k)$$

Definimos

$$\begin{aligned} p(x_i, y_j) &:= \sum_k p(x_i, y_j, z_k) & p(x_i, z_k) &:= \sum_j p(x_i, y_j, z_k) \\ p(y_j, z_k) &:= \sum_i p(x_i, y_j, z_k) & p(x_i) &:= \sum_{j,k} p(x_i, y_j, z_k) \\ p(y_j) &:= \sum_{i,k} p(x_i, y_j, z_k) & p(z_k) &:= \sum_{i,j} p(x_i, y_j, z_k). \end{aligned}$$

Nota: Obsérvese que

$$\begin{aligned} \sum_i p(x_i) = \sum_j p(y_j) = \sum_k p(z_k) = \sum_{i,j} p(x_i, y_j) \\ = \sum_{i,k} p(x_i, z_k) = \sum_{j,k} p(y_j, z_k) = \sum_{i,j,k} p(x_i, y_j, z_k) = 1. \end{aligned}$$

Definición A.2. *(a) La entropía de una variable X está dada por*

$$H(X) = -\sum_i p(x_i) \ln p(x_i)$$

Podemos extender la definición de entropía a dos variables X, Y así

$$H(X,Y) = -\sum_{i,j} p(x_i, y_j) \ln p(x_i, y_j)$$

y para tres variables X, Y, Z

$$H(X,Y,Z) = -\sum_{i,j,z} p(x_i, y_j, z_k) \ln p(x_i, y_j, z_k)$$

Definición A.3. *(a) Sean X, Y dos variables, la información mutua entre X y Y está dada por*

$$I(X \wedge Y) = \sum_{i,j} p(x_i, y_j) \ln \frac{p(x_i, y_j)}{p(x_i)p(y_j)}$$

(b) La información mutua de X y Y dada Z es

$$I(X \wedge Y|Z) = \sum_{i,j,k} p(x_i, y_j, z_k) \ln \frac{p(x_i, y_j|z_k)}{p(x_i|z_k)p(y_j|z_k)}$$

Lema A.4. *Para todo número real $x > 0$*

$$\ln y \leq \frac{1}{x}(y - x) + \ln x \tag{A.1}$$

para todo $y > 0$.

Demostración. Tómese la función

$$f(y) = \ln y - \frac{1}{x}(y - x) - \ln x$$

para $y > 0$. Entonces $f'(y) = \frac{1}{y} - \frac{1}{x}$ y $f''(y) = -\frac{1}{y^2}$. Luego f alcanza máximo en $y = x$, pero como $f(x) = 0$ entonces

$$\ln y - \frac{1}{x}(y - x) - \ln x \leq 0$$

$$\ln y \leq \frac{1}{x}(y - x) + \ln x$$

. □

Lema A.5. *Para todo real* $y > 0$

$$1 - \frac{1}{y} \leq \ln y \leq y - 1 \tag{A.2}$$

Demostración. Si en la desigualdad del lema anterior se toma $x = 1$, entonces queda demostrada la desigualdad de la derecha. Para demostrar la desigualdad de la izquierda, basta con cambiar y por $\frac{1}{y}$ en la desigualdad de la derecha. □

Proposición A.6. *(a)* $I(X \wedge Y|Z) = H(X,Z) + H(Y,Z) - H(Z) - H(X,Y,Z)$.

(b) $I(X \wedge Y|Z) \geq 0$.

Demostración. (a)

$$
\begin{aligned}
I(X \wedge Y|Z) &= \sum_{i,j,k} p(x_i, y_j, z_k) \ln \frac{p(x_i, y_j|z_k)}{p(x_i|z_k)p(y_j|z_k)} \\
&= \sum_{i,j,k} p(x_i, y_j, z_k) \ln \frac{p(x_i, y_j, z_k)p(z_k)}{p(x_i, z_k)p(y_j, z_k)} \\
&= \sum_{i,j,k} p(x_i, y_j, z_k)(\ln p(x_i, y_j, z_k) + \ln p(z_k) \\
&\qquad\qquad - \ln p(x_i, z_k) - \ln p(y_j, z_k)) \\
&= \sum_{i,j,k} p(x_i, y_j, z_k) \ln p(x_i, y_j, z_k) + \sum_{i,j,k} p(x_i, y_j, z_k) \ln p(z_k) \\
&\qquad\qquad - \sum_{i,j,k} p(x_i, y_j, z_k) \ln p(x_i, z_k) \\
&\qquad\qquad - \sum_{i,j,k} p(x_i, y_j, z_k) \ln p(y_j, z_k) \\
&= \sum_{i,j,k} p(x_i, y_j, z_k) \ln p(x_i, y_j, z_k) + \sum_{k} \ln p(z_k) \sum_{i,j} p(x_i, y_j, z_k) \\
&\qquad\qquad - \sum_{i,k} \ln p(x_i, z_k) \sum_{j} p(x_i, y_j, z_k) \\
&\qquad\qquad - \sum_{j,k} \ln p(y_j, z_k) \sum_{i} p(x_i, y_j, z_k) \\
&= \sum_{i,j,k} p(x_i, y_j, z_k) \ln p(x_i, y_j, z_k) + \sum_{k} p(z_k) \ln p(z_k) \\
&\qquad\qquad - \sum_{i,k} p(x_i, z_k) \ln p(x_i, z_k) - \sum_{j,k} p(y_j, z_k) \ln p(y_j, z_k) \\
&= -H(X, Y, Z) - H(Z) + H(X, Z) + H(Y, Z).
\end{aligned}
$$

(b)

$$
\begin{aligned}
I(X \wedge Y|Z) &= \sum_{i,j,k} p(x_i, y_j, z_k) \ln \frac{p(x_i, y_j|z_k)}{p(x_i|z_k)p(y_j|z_k)} \\
&= \sum_{i,j,k} p(z_k) p(x_i, y_j|z_k) \ln \frac{p(x_i, y_j|z_k)}{p(x_i|z_k)p(y_j|z_k)} \\
&= \sum_{k} p(z_k) \sum_{i,j} p(x_i, y_j|z_k) \ln \frac{p(x_i, y_j|z_k)}{p(x_i|z_k)p(y_j|z_k)} \\
&\geq \sum_{k} p(z_k) \sum_{i,j} p(x_i, y_j|z_k) \left(1 - \frac{p(x_i|z_k)p(y_j|z_k)}{p(x_i, y_j|z_k)}\right) \quad \text{por (A.2)} \\
&= \sum_{k} p(z_k) \sum_{i,j} (p(x_i, y_j|z_k) - p(x_i|z_k)p(y_j|z_k)) \\
&= \sum_{k} \sum_{i,j} \left(p(x_i, y_j, z_k) - \frac{p(x_i, z_k)p(y_j, z_k)}{p(z_k)}\right) \\
&= \sum_{k} \left(\sum_{i,j} p(x_i, y_j, z_k) - \sum_{i,j} \frac{p(x_i, z_k)p(y_j, z_k)}{p(z_k)}\right) \\
&= \sum_{k} \left(\sum_{i,j} p(x_i, y_j, z_k) - \sum_{i} \frac{p(x_i, z_k)}{p(z_k)} \sum_{j} p(y_j, z_k)\right) \\
&= \sum_{k} \left(\sum_{i,j} p(x_i, y_j, z_k) - \sum_{i} \frac{p(x_i, z_k)}{p(z_k)} p(z_k)\right) \\
&= \sum_{k} \left(\sum_{i,j} p(x_i, y_j, z_k) - p(z_k)\right) = \sum_{k} (p(z_k) - p(z_k)) = 0.
\end{aligned}
$$

□

Corolario A.7. $H(X, Z) + H(Y, Z) \geq H(X, Y, Z) + H(Z)$.

Bibliografía

[1] W. W. Armstrong, Dependency structures of database relationships, In: Proc. Information Processing 74 (North Holland, Amsterdam, 1974) 580-583.

[2] F. Matús, Abstract functional dependency structures, Institute of Information Theory and Automation, In: Theorethical Computer Science 81, (Praga, Checoslovaquia, 1991) 117-126.

[3] S. El Rouayheb, A. Sprintson y C. Georghiades, A New Construction Method for Networks from Matroids, Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843. Email: {salim, spalex, c-georghiades}@ece.tamu.edu (Seul, Corea, 2009).

[4] H. Sarria, An Introduction to Network Coding. Email: hsarriaz@unal.edu.co (2009).

[5] A. Kim y M. Médard, Scalar-linear Solvability of Matroidal Networks Associated with Representable Matroids, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA. Email: {tonyekim, medard}@mit.edu (2010).

[6] J. Oaxley, Matroid Theory, Oxford Graduate Text in Mathematics, Department of Mathematics, Louisiana State University (1992).

[7] R. Yeung, A First Course in Information Theory, Springer (2002)

[8] S. Fujishige, Submodular Functions and Optimization, Elsevier (2005).

[9] C. Neira, Notas de Topología. Universidad Nacional de Colombia.