Matemáticas y sus aplicaciones 18, Textos Científicos, Fomento Editorial de la Benemérita Universidad Autónoma de Puebla, ISBN: 978-607-525-858-4

Capítulo 1

Matroides: algunas definiciones equivalentes

Mireya Díaz López, Carlos Alberto López Andrade, Carlos Guillén Galván
FCFM, BUAP

Resumen

La teoría de matroides surgió en los años 30's del siglo XX. Hassler Whitney desarrolló una noción de independencia y rango en el contexto de la teoría de grafos y observó similitudes con los conceptos de independencia lineal y dimensión de álgebra lineal. Después de identificar las propiedades de independencia abstracta, Whitney introdujo el concepto de matroide en 1935 en [6] y se inspiró en la palabra matriz para crearlo. Otros matemáticos contemporáneos de Whitney también contribuyeron al nacimiento de la teoría de matroides. En 1937, B. L. van der Waerden, en la segunda edición de *Moderne Algebra*, estableció tres propiedades fundamentales que son comunes a la dependencia algebraica y lineal, descubriendo con ello el concepto de matroide de manera independiente a Whitney. En este capítulo se estudiarán los conceptos fundamentales de la teoría de matroides y se establecerán las equivalencias entre algunas de las definiciones de matroide.

1 Introducción

Una importante característica de los matroides es que pueden definirse de muchas formas diferentes pero equivalentes. Desde su artículo fundador, Whitney estableció cuatro definiciones equivalentes de matroides. Esto podría parecer molesto, pero es una de las principales cualidades que posee esta teoría, ya que puede preferirse una definición sobre otra, dependiendo del problema que quiera abordarse.

En las secciones siguientes se enunciarán algunas de las principales y más útiles definiciones de matroide. Se tomará como primera definición aquella

que abstrae las propiedades que satisface un conjunto de vectores linealmente independiente. Esta definición, por tanto, proviene del álgebra lineal. Posteriormente, se definirán nuevos conceptos y se demostrarán algunas de las propiedades que dichos conceptos satisfacen. A continuación se destacarán aquellas propiedades que serán suficientes para dar una definición alternativa del concepto de matroide y se probará la equivalencia de las definiciones. El desarrollo de esta teoría estará acompañada de algunos ejemplos y observaciones. Para el desarrollo de este capítulo de libro se tomaron [2] y [3] como principales referencias. A lo largo de este capítulo $[n]$ denotará el conjunto de números naturales menores o iguales a n, es decir, $\{1, 2, \ldots, n\}$.

2 Definición por conjuntos independientes

Sea V un espacio vectorial. Los subconjuntos linealmente independientes de V cumplen las siguientes propiedades:

a) Todo subconjunto de un conjunto linealmente independiente también es linealmente independiente.

b) Si I y J son conjuntos linealmente independientes tales que $|I| < |J|$, entonces existe $x \in J \setminus I$ tal que $I \cup \{x\}$ es linealmente independiente.

A continuación se presenta una definición de conjunto independiente en grafos que permitirá establecer una importante conexión con la independencia lineal en álgebra lineal.

Definición 2.1. Sea G un grafo finito no dirigido, no necesariamente simple, con conjunto de aristas E y conjunto de vértices V. Un conjunto $S \subseteq E$ es *independiente* si no contiene ciclos y es dependiente en otro caso.

Nótese que ésta no es la definición clásica de independencia de la teoría de grafos, la cual dice que un conjunto de vértices en un grafo es independiente si ninguno de sus vértices es adyacente a otro. Sin embargo, esta nueva definición es útil pues resulta que las propiedades a) y b) también se cumplen para los conjuntos de aristas independientes:

A) Todo subconjunto de un conjunto acíclico de aristas es acíclico.

B) Si I y J son dos conjuntos de aristas acíclicos y $|I| < |J|$, entonces existe $e \in J \setminus I$ tal que $I \cup \{e\}$ es acíclico.

Anteriormente se mencionó que Whitney y van der Waerden se basaron en las propiedades que cumplen los conjuntos linealmente independientes en álgebra lineal y teoría de grafos para definir el concepto de matroide. Dichas propiedades son justamente los incisos a), b), y A), B), respectivamente. La primera definición que se dará en este capítulo va en este sentido y se eligió porque está basada en resultados conocidos, y por ello puede resultar más familiar para la mayoría de los lectores.

Definición 2.2 (Por conjuntos independientes)**.** Un *matroide* M es un par ordenado $(E, \mathcal{I})$ que consiste de un conjunto finito E y una familia $\mathcal{I}$ de subconjuntos de E que satisface las tres condiciones siguientes:

(I1) (No trivialidad) $\mathcal{I} \neq \emptyset$.

(I2) (Cerrado bajo subconjuntos) Si $I \in \mathcal{I}$ y $J \subseteq I$, entonces $J \in \mathcal{I}$.

(I3) (Aumento de independencia) Si $I, J \in \mathcal{I}$ y $|I| < |J|$, entonces existe un elemento $e \in J \setminus I$ tal que $I \cup \{e\} \in \mathcal{I}$.

En este caso es usual referirse a M como matroide sobre E. Los elementos de $\mathcal{I}$ son los *conjuntos independientes* de M y E es el *conjunto subyacente* de M. Cuando es necesario se denota a $\mathcal{I}$ con $\mathcal{I}(M)$ y a E con $E(M)$. Un subconjunto de E que no pertenece a $\mathcal{I}$ se llama *conjunto dependiente*.

Puede darse una definición de matroide muy similar a la Definición 2.2 con ligeras modificaciones a las propiedades (I1) e (I3), que puede resultar más práctica al momento de verificar si un par ordenado es un matroide. Esto se establece en el siguiente teorema.

Teorema 2.3. *Sean E un conjunto finito e $\mathcal{I}$ una familia de subconjuntos de E. Entonces $\mathcal{I}$ es la familia de conjuntos independientes de un matroide si y sólo si satisfacen las tres condiciones siguientes:*

(J1) $\emptyset \in \mathcal{I}$.

(J2) Si $I \in \mathcal{I}$ *y* $J \subseteq I$, *entonces* $J \in \mathcal{I}$.

(J3) Si $I, J \in \mathcal{I}$ son tales que $|J| = |I| + 1$, entonces existe un elemento $x \in J \setminus I$ que cumple que $I \cup \{x\} \in \mathcal{I}$.

Demostración. Sea $M = (E, \mathcal{I})$ un matroide. Veamos que $\mathcal{I}$ verifica las propiedades (J1) y (J3). Dado que $\mathcal{I}$ satisface la condición (I1), $\mathcal{I} \neq \emptyset$. Así, existe un conjunto independiente, al que llamamos X. Como también se cumple (I2) y tenemos que $\emptyset \subseteq X$, concluimos que $\emptyset \in \mathcal{I}$, es decir, se satisface (J1). La condición (J3) es un caso particular de (I3) y por lo tanto, se verifica. Para la suficiencia supongamos que E es un conjunto finito y que $\mathcal{I}$ es una familia de subconjuntos de E que satisface las propiedades (J1), (J2) y (J3). Veamos que $M = (E, \mathcal{I})$ es un matroide. Por (J1), $\emptyset \in \mathcal{I}$, entonces se verifica (I1). Ahora, sean $I, J \in \mathcal{I}$ con $|I| < |J|$. Como I y J son conjuntos finitos, entonces existe $I_1 \subseteq J$ tal que $|I_1| = |I| + 1$. Por (J2), $I_1 \in \mathcal{I}$, luego por (J3) existe $x \in I_1 \setminus I$ tal que $I \cup \{x\} \in \mathcal{I}$. Más aún, $x \in J \setminus I$. Por lo tanto, M es un matroide. □

La equivalencia entre los conjuntos de propiedades (I1), (I2), (I3) y (J1), (J2), (J3) no puede establecerse probando de manera independiente que las parejas (I1), (J1) e (I3), (J3) son proposiciones equivalentes. Para verificar esto sea $E = \{a, b, c\}$, $\mathcal{I} = \{\{a\}, \{b\}, \{a, b, c\}\}$. La condición (J3) se satisface (no existe una pareja de elementos I, J de $\mathcal{I}$ que satisfagan $|J| = |I| + 1$). Sin embargo, (I3) no se satisface, pues los conjuntos $\{a\}$ y $\{a, b, c\}$ cumplen que $|\{a\}| < |\{a, b, c\}|$ y no existe un elemento $x \in \{a, b, c\} \setminus \{a\} = \{b, c\}$ tal que $\{a\} \cup \{x\} \in \mathcal{I}$.

A continuación se muestran dos ejemplos de matroides. Es importante tenerlos presentes porque son básicos para comprender los conceptos y resultados que se darán en las secciones posteriores.

Ejemplo 2.4. Sean V un espacio vectorial sobre un campo $\mathbb{F}$ y E un subconjunto finito de V. Defínase $\mathcal{I}$ como la colección de subconjuntos de E que son linealmente independientes sobre $\mathbb{F}$. Como $\emptyset$ es un conjunto linealmente independiente entonces $\emptyset \in \mathcal{I}$. Además, $\mathcal{I}$ satisface las propiedades a) y b) mencionadas anteriormente. Por lo tanto, $M = (E, \mathcal{I})$ es un matroide y se llama *matroide vector* o *matroide representable* y se dice que M es *representable sobre* $\mathbb{F}$. Este es uno de los ejemplos que motivaron la definición de matroide.

Ejemplo 2.5. Sean n y k enteros no negativos tales que $k \leq n$. Sea E un conjunto de cardinalidad n. Tómese $\mathcal{I}$ como la familia de todos los subconjuntos de E que tienen una cardinalidad menor o igual a k. Como $\emptyset \subseteq E$ y

$|\emptyset| = 0 \leq k$, entonces $\emptyset \in \mathcal{I}$. Ahora, supóngase que $I \in \mathcal{I}$ y $J \subseteq I$. Entonces $|I| \leq k$, $|J| \leq |I|$, y por tanto $|J| \leq k$, de donde $J \in \mathcal{I}$. Finalmente, sean $I, J \in \mathcal{I}$ tales que $|I| < |J|$. Como $|I| < |J|$, entonces existe un elemento $x \in J \setminus I$ y se tiene que $|I \cup \{x\}| \leq |J|$. Dado que $J \in \mathcal{I}$, verifica que $|J| \leq k$ y por ello $|I \cup \{x\}| \leq |J| \leq k$. Por consiguiente $I \cup \{x\} \in \mathcal{I}$. Así que M es un matroide. M se llama el *matroide uniforme* de rango k sobre un conjunto de n elementos y se denota por $U_{k,n}$. El matroide $U_{n,n}$ se llama *matroide libre*. Nótese que en el matroide libre todos los subconjuntos de E son independientes, es decir, $\mathcal{I} = \mathcal{P}(E)$.

Es igual de importante saber identificar lo que sí es un matroide de aquello que no lo es. Es por ello que en el siguiente ejemplo se presenta una familia de conjuntos que no satisface la condición (I3) y por tanto no es un matroide.

Ejemplo 2.6. Sean $E = \{a, b, c, d\}$, $\mathcal{I} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{c, d\}\}$. Se puede ver claramente que $\mathcal{I}$ satisface las propiedades (I1) e (I2), sin embargo, no cumple con (I3). Para comprobar esto, tómese los conjuntos $\{a\}$ y $\{c, d\}$ de la familia $\mathcal{I}$. Puede verse que no existe elemento x en $\{c, d\} \setminus \{a\}$ tal que $\{a\} \cup \{x\} \in \mathcal{I}$, ya que ni $\{a, c\}$ ni $\{a, d\}$ son elementos de $\mathcal{I}$. Por lo tanto, $\mathcal{I}$ no es una familia de conjuntos independientes.

3 Definición por bases

Sea $M = (E, \mathcal{I})$ un matroide. Para conocer por completo a M es necesario poder identificar todos sus conjuntos independientes. Si M posee una gran cantidad de conjuntos independientes dar una lista exhaustiva de todos ellos podría resultar una tarea complicada. Sin embargo, existe una manera de facilitar este trabajo. Sea I un conjunto independiente de M. Si no existe un conjunto independiente que contenga propiamente a I entonces I es un conjunto independiente maximal. En otro caso, supóngase que $I_1 \in \mathcal{I}$ es tal que $I \subsetneq I_1$. Si no existe un conjunto independiente que contenga propiamente a I_1 entonces I_1 es independiente maximal. De lo contrario existe un conjunto independiente I_2 diferente a I_1 que lo contiene. Podemos continuar este proceso, pero no de manera indefinida, pues como E es finito también lo es su conjunto potencia. Así que después de un número finito de pasos hallaremos un conjunto independiente que contiene a I y que no está contenido

propiamente en otro conjunto independiente, es decir, independiente maximal. De aquí concluimos que todo conjunto independiente está contenido en un conjunto independiente maximal. Además, todo subconjunto de un conjunto independiente es independiente por (I2). Así que una manera efectiva de enlistar todos los conjuntos independientes es proporcionar una lista de los conjuntos independientes maximales. De aquí la importancia de definir el siguiente concepto.

Definición 3.1. Sea $M = (E, \mathcal{I})$ un matroide. B es una *base* del matroide M si B es un conjunto independiente maximal. Se denotará el conjunto de las bases de M por $\mathcal{B}$.

Enseguida se enunciarán algunas de las propiedades más importantes que satisface el conjunto de bases de un matroide. Dichas propiedades permitirán dar una definición de matroide partiendo de este nuevo concepto. Para probarlas se empleará el siguiente lema.

Lema 3.2. *Sea M un matroide. Si $B_1, B_2 \in \mathcal{B}$, entonces $|B_1| = |B_2|$.*

Demostración. Supongamos que B_1 y B_2 son bases de M tales que $|B_1| \neq |B_2|$. Sin pérdida de generalidad supongamos que $|B_1| < |B_2|$. Ya que B_1 y B_2 son conjuntos independientes, por (I3) existe $e \in B_2 \setminus B_1$ tal que $B_1 \cup \{e\} \in \mathcal{I}$, de modo que $B_1 \cup \{e\}$ es un conjunto independiente que contiene propiamente a B_1, lo cual contradice que B_1 sea base. Por lo tanto, B_1 y B_2 tienen la misma cardinalidad. □

Concluimos entonces que cualesquiera dos bases de un matroide M tienen la misma cardinalidad.

Teorema 3.3. *El conjunto de bases $\mathcal{B}$ de un matroide M verifica las siguientes propiedades:*

(B1) (No trivialidad) $\mathcal{B} \neq \emptyset$.

(B2) (Familia Sperner o clutter) Si $B_1, B_2 \in \mathcal{B}$ y $B_1 \subseteq B_2$, entonces $B_1 = B_2$.

(B3) (Intercambio débil en bases) Si $B_1, B_2 \in \mathcal{B}$ y $x \in B_1 \setminus B_2$, entonces existe un elemento $y \in B_2 \setminus B_1$ tal que $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Demostración. Sabemos que $\emptyset$ es un conjunto independiente. Entonces existe un conjunto independiente maximal B que lo contiene. Por la definición de $\mathcal{B}$, $B \in \mathcal{B}$ y por lo tanto (B1) se cumple. Tomemos $B_1, B_2 \in \mathcal{B}$ tales que $B_1 \subseteq B_2$. Si suponemos que $B_1 \subsetneq B_2$ entonces $|B_1| < |B_2|$, lo cual no puede ocurrir por el Lema 3.2. Entonces $B_1 = B_2$. Para probar que se cumple (B3), sean $B_1, B_2 \in \mathcal{B}$ y $x \in B_1 \setminus B_2$. Como $B_1 \setminus \{x\} \subseteq B_1$ y $B_1 \in \mathcal{I}$, por (I2) tenemos que $B_1 \setminus \{x\} \in \mathcal{I}$. Por el Lema 3.2, $|B_1| = |B_2|$, luego $|B_1 \setminus \{x\}| < |B_2|$. Por (I3) existe un elemento $y \in B_2 \setminus (B_1 \setminus \{x\})$ tal que $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{I}$. Queremos probar que $(B_1 \setminus \{x\}) \cup \{y\}$ es una base, así que sólo falta probar que es conjunto independiente maximal. Tenemos que $|(B_1 \setminus \{x\}) \cup \{y\}| = |B_1|$. Si suponemos que $(B_1 \setminus \{x\}) \cup \{y\} \notin \mathcal{B}$, debe existir $B_3 \in \mathcal{B}$ tal que $(B_1 \setminus \{x\}) \cup \{y\} \subsetneq B_3$ y por tanto $|B_1| = |(B_1 \setminus \{x\}) \cup \{y\}| < |B_3|$, lo cual contradice el Lema 3.2. Concluimos que $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$, por lo que (B3) se verifica. □

La propiedad (B2) manifiesta que $\mathcal{B}$ es una familia Sperner o clutter, es decir, que los conjuntos de dicha familia no se contienen entre sí. La propiedad (B3) expresa que dadas dos bases B_1 y B_2, para un elemento $x \in B_1 \setminus B_2$ existe un elemento en la otra diferencia de conjuntos $y \in B_2 \setminus B_1$ tal que x puede "intercambiarse" por y para obtener nuevamente una base, es decir, $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ (de ahí el nombre de propiedad de intercambio débil en bases). Aplicando la propiedad (B3) al elemento y se tiene que existe $z \in B_1 \setminus B_2$ tal que $(B_2 \setminus \{y\}) \cup \{z\} \in \mathcal{B}$. Sin embargo, dicha propiedad no afirma algo acerca del conjunto $(B_2 \setminus \{y\}) \cup \{x\}$. El Teorema 3.4 es una versión más fuerte de la propiedad de intercambio débil en bases, pues asegura que siempre es posible que se dé un intercambio doble, es decir, que para cada elemento de $B_1 \setminus B_2$ es posible encontrar un elemento en $B_2 \setminus B_1$ de tal forma que pueden intercambiarse (el primero por el segundo y el segundo por el primero) para obtener dos bases. En muchas ocasiones bastará con tener la primera versión de esta propiedad, pero se menciona a continuación ya que será de utilidad más adelante.

Teorema 3.4. *([2, pág. 91]) Sea M un matroide. $\mathcal{B}$ satisface la siguiente propiedad:*

(B3) Si $B_1, B_2 \in \mathcal{B}$ y $x \in B_1 \setminus B_2$, entonces existe un elemento $y \in B_2 \setminus B_1$ de tal manera que $(B_1 \setminus \{x\}) \cup \{y\}, (B_2 \setminus \{y\}) \cup \{x\} \in \mathcal{B}$.*

La propiedad (B3*) se conoce como propiedad de *Intercambio Fuerte en Bases*.

Como pudo apreciarse, el Lema 3.2 fue crucial en la demostración del Teorema 3.3. En el Teorema 3.5 se verá que dicho lema puede emplearse para formular una nueva caracterización de matroide. Para ello identificaremos a la propiedad enunciada en el Lema 3.2 como (B2*).

Teorema 3.5. *Sean E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E. La familia $\mathcal{B}$ satisface (B1), (B2) y (B3) si y sólo si satisface (B1), (B2*) y (B3).*

Demostración. Sea $\mathcal{B}$ una familia que cumple (B1), (B2) y (B3) y sean $B_1, B_2 \in \mathcal{B}$, $B_1 \neq B_2$. Supongamos que $|B_1| < |B_2|$. B_1 y B_2 pueden escribirse como las siguientes uniones disjuntas: $B_1 = (B_1 \setminus B_2) \cup (B_1 \cap B_2)$, $B_2 = (B_2 \setminus B_1) \cup (B_1 \cap B_2)$. Como $|B_1| < |B_2|$, entonces debe ocurrir que $|B_1 \setminus B_2| < |B_2 \setminus B_1|$. Si $B_1 \setminus B_2 = \emptyset$, entonces $B_1 \subseteq B_2$, y por (B2), $B_1 = B_2$, lo cual es una contradicción. Así que $B_1 \setminus B_2 \neq \emptyset$. Sea $n = |B_1 \setminus B_2|$. Tomemos $x_1 \in B_1 \setminus B_2$. Por (B3) existe $y_1 \in B_2 \setminus B_1$ tal que $B_3 = (B_1 \setminus \{x_1\}) \cup \{y_1\} \in \mathcal{B}$. Sea $x_2 \in B_3 \setminus B_2$, entonces $x_2 \in (B_1 \setminus B_2) \setminus \{x_1\}$. Por (B3) existe $y_2 \in B_2 \setminus B_3$ tal que $B_4 = (B_3 \setminus \{x_2\}) \cup \{y_2\} \in \mathcal{B}$. Se tiene que:

$$\begin{aligned} B_2 \setminus B_3 &= B_2 \cap \big[(B_1 \setminus \{x_1\}) \cup \{y_1\}\big]^C = B_2 \cap \big[(B_1 \cap \{x_1\}^C)^C \cap \{y_1\}^C\big] \\ &= B_2 \cap \big[(B_1^C \cup \{x_1\}) \cap \{y_1\}^C\big] = \big[(B_2 \cap B_1^C) \cup (B_2 \cap \{x_1\})\big] \cap \{y_1\}^C \\ &= (B_2 \setminus B_1) \setminus \{y_1\} \end{aligned}$$

esto es, $B_2 \setminus B_3 = (B_2 \setminus B_1) \setminus \{y_1\}$, por lo que $y_2 \in (B_2 \setminus B_1) \setminus \{y_1\}$. Nótese que x_1, x_2, y_1 y y_2 son todos diferentes entre sí. Por eso y por los conjuntos en los cuales se tomaron tales elementos se tiene que

$$B_4 = \big[[(B_1 \setminus \{x_1\}) \cup \{y_1\}] \setminus \{x_2\}\big] \cup \{y_2\} = (B_1 \setminus \{x_1, x_2\}) \cup \{y_1, y_2\}.$$

Tomemos $x_3 \in B_4 \setminus B_2$, entonces $x_3 \in (B_1 \setminus B_2) \setminus \{x_1, x_2\}$. Por (B3) existe $y_3 \in B_2 \setminus B_4$ tal que $B_5 = (B_4 \setminus \{x_3\}) \cup \{y_3\} \in \mathcal{B}$. Puede verse que $B_2 \setminus B_4 = (B_2 \setminus B_1) \setminus \{y_1, y_2\}$. Además,

$$B_5 = \big[[(B_1 \setminus \{x_1, x_2\}) \cup \{y_1, y_2\}] \setminus \{x_3\}\big] \cup \{y_3\} = (B_1 \setminus \{x_1, x_2, x_3\}) \cup \{y_1, y_2, y_3\}.$$

Realizando este proceso n veces encontramos $x_1, x_2, \ldots, x_n \in B_1 \setminus B_2$ todos diferentes entre sí y $y_1, y_2, \ldots, y_n \in B_2 \setminus B_1$ también diferentes entre sí tales

que $B_{n+2} = (B_1 \setminus \{x_1, x_2, \ldots, x_n\}) \cup \{y_1, y_2, \ldots, y_n\} \in \mathcal{B}$. Recordemos que $|B_1 \setminus B_2| = n$, entonces ocurre que $B_1 \setminus B_2 = \{x_1, x_2, \ldots, x_n\}$, y como $B_1 = (B_1 \setminus B_2) \cup (B_1 \cap B_2)$, entonces $B_1 \setminus \{x_1, x_2, \ldots, x_n\} = B_1 \setminus (B_1 \setminus B_2) = B_1 \cap B_2$, lo cual implica que $B_{n+2} = (B_1 \cap B_2) \cup \{y_1, y_2, \ldots, y_n\} \subseteq B_2$ y por (B2) se concluye que $B_{n+2} = B_2$, pero $|B_{n+2}| = |B_1|$ y estamos suponiendo que $|B_1| < |B_2|$, entonces $|B_{n+2}| < |B_2|$, lo cual es una contradicción. Similarmente se prueba que no puede ocurrir que $|B_1| > |B_2|$. Entonces $|B_1| = |B_2|$, es decir, (B2*) es verdadera.

Para demostrar la suficiencia supongamos que $\mathcal{B}$ es una familia de subconjuntos de un conjunto finito E que satisface las propiedades (B1), (B2*) y (B3). Veamos que también satisface la propiedad (B2). Para ello sean $B_1, B_2 \in \mathcal{B}$ tales que $B_1 \subseteq B_2$. No puede ocurrir que $B_1 \subsetneq B_2$, ya que por (B2*), $|B_1| = |B_2|$. Entonces la igualdad de los conjuntos se verifica y por lo tanto, (B2) se cumple. □

Hasta este momento se ha abordado la manera mediante la cual pueden conocerse las bases de un matroide considerando sus conjuntos independientes, y las propiedades que dichas bases cumplen. Es de interés saber si puede construirse un matroide a partir de una familia $\mathcal{B}$ que cumple (B1), (B2) y (B3). La respuesta es sí. Esto se logra formando a partir de $\mathcal{B}$ una familia $\mathcal{I}$ de lo que serán los conjuntos independientes y demostrando que dicha familia satisface las propiedades (I1), (I2) e (I3). El punto clave de esta construcción es saber cómo definir la familia $\mathcal{I}$. Las bases se definieron como los conjuntos independientes maximales, luego todo conjunto independiente está contenido en una base y cualquier subconjunto de una base es un conjunto independiente, así que de manera natural $\mathcal{I}$ se toma como el conjunto de todos los subconjuntos de los elementos de $\mathcal{B}$. Esto se aborda en el Teorema 3.6.

Teorema 3.6. *Sean E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E que satisface (B1), (B2) y (B3). Se define el conjunto $\mathcal{I} = \{I \subseteq E \mid \exists B \in \mathcal{B} : I \subseteq B\}$. Entonces $M = (E, \mathcal{I})$ es un matroide que tiene a $\mathcal{B}$ como su colección de bases.*

Demostración. Por (B1), $\mathcal{B} \neq \emptyset$, entonces existe $B \in \mathcal{B}$. Como $B \subseteq B$, entonces $B \in \mathcal{I}$, esto es, (I1) es verdadera. Ahora, sea $I \in \mathcal{I}$. Entonces existe $B \in \mathcal{B}$ tal que $I \subseteq B$. Luego, si $J \subseteq I$, por transitividad de la contención de conjuntos tenemos que $J \subseteq B$, y por tanto $J \in \mathcal{I}$. Entonces (I2) se cumple.

Sean $I_1, I_2 \in \mathcal{I}$ tales que $|I_1| < |I_2|$ y supongamos que (I3) no se cumple, es decir, que para todo $x \in I_2 \setminus I_1$, $I_1 \cup \{x\} \notin \mathcal{I}$. Como $I_1, I_2 \in \mathcal{I}$, existen $B_1, B_2 \in \mathcal{B}$ tales que $I_1 \subseteq B_1$ e $I_2 \subseteq B_2$. Queremos analizar el conjunto

Figura 1: Diagrama de Venn de las relaciones entre B_1, B_2, I_1 e I_2.

coloreado de negro de la Figura 1, es decir, el conjunto $(I_2 \cap B_1) \setminus I_1$. Si $(I_2 \cap B_1) \setminus I_1 \neq \emptyset$, entonces existe $x \in (I_2 \cap B_1) \setminus I_1$, esto es, $x \in I_2 \setminus I_1$ y $x \in B_1$, por lo que $I_1 \cup \{x\} \subseteq B_1$, de donde $I_1 \cup \{x\} \in \mathcal{I}$, lo cual contradice nuestra suposición. Por lo tanto, $(I_2 \cap B_1) \setminus I_1 = \emptyset$, o expresado de otra forma, $I_2 \cap (B_1 \setminus I_1) = \emptyset$, y como $B_1 \cap I_2 = (I_2 \cap I_1) \cup (I_2 \cap (B_1 \setminus I_1))$ concluimos que $B_1 \cap I_2 = I_1 \cap I_2$. Por otro lado, puede existir más de un elemento en $\mathcal{B}$ que contenga a I_2. Tomaremos a B_2 de tal forma que $|B_2 \setminus (I_2 \cup B_1)|$ sea minimal (ver en la Figura 1 región coloreada de gris). Afirmamos que $B_2 \setminus (I_2 \cup B_1) = \emptyset$. Si existe $x \in B_2 \setminus (I_2 \cup B_1)$, en particular $x \in B_2 \setminus B_1$, luego aplicando la propiedad (B3) a B_2 y a B_1 (en ese orden), existe $y \in B_1 \setminus B_2$ tal que $B_3 = (B_2 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$. Veamos que $B_3 \setminus (I_2 \cup B_1) \subsetneq B_2 \setminus (I_2 \cup B_1)$.

$$
\begin{aligned}
B_3 \setminus (I_2 \cup B_1) &= [(B_2 \setminus \{x\}) \cup \{y\}] \setminus (I_2 \cup B_1) \\
&= [(B_2 \cap \{x\}^C) \cup \{y\}] \setminus (I_2 \cup B_1) \\
&= [(B_2 \cup \{y\}) \cap (\{x\}^C \cup \{y\})] \setminus (I_2 \cup B_1) \\
&= [(B_2 \cup \{y\}) \cap \{x\}^C] \setminus (I_2 \cup B_1) \\
&= [(B_2 \cup \{y\}) \cap \{x\}^C] \cap (I_2 \cup B_1)^C \qquad (1) \\
&= [(B_2 \cup \{y\}) \cap (I_2 \cup B_1)^C] \cap \{x\}^C \\
&= [(B_2 \cap (I_2 \cup B_1)^C) \cup (\{y\} \cap (I_2 \cup B_1)^C)] \cap \{x\}^C \\
&= [(B_2 \setminus (I_2 \cup B_1)) \cup (\{y\} \cap (I_2 \cup B_1)^C)] \cap \{x\}^C \\
&= [B_2 \setminus (I_2 \cup B_1)] \setminus \{x\} \subsetneq [B_2 \setminus (I_2 \cup B_1)]
\end{aligned}
$$

La última igualdad se consigue ya que $y \in B_1$ y la contención propia se da puesto que $x \in B_2 \setminus (I_2 \cup B_1)$. De aquí tenemos que $|B_3 \setminus (I_2 \cup B_1)| < |B_2 \setminus (I_2 \cup B_1)|$. Como $I_2 \subseteq B_2$ y $x \notin I_2$ entonces $I_2 \subseteq (B_2 \setminus \{x\}) \cup \{y\} = B_3$. Entonces B_3 es un elemento de $\mathcal{B}$ que contiene a I_2 y tal que $|B_3 \setminus (I_2 \cup B_1)| < |B_2 \setminus (I_2 \cup B_1)|$, lo cual contradice la elección de B_2. Concluimos entonces que $B_2 \setminus (I_2 \cup B_1) = \emptyset$. Usando un argumento similar, podemos elegir B_1 de tal forma que $B_1 \setminus (I_1 \cup B_2) = \emptyset$. Ahora bien, como $B_2 \setminus B_1 = (I_2 \setminus B_1) \cup [(B_2 \setminus$

$I_2) \setminus B_1] = (I_2 \setminus B_1) \cup [B_2 \setminus (I_2 \cup B_1)]$ y como $B_2 \setminus (I_2 \cup B_1) = \emptyset$, entonces $B_2 \setminus B_1 = I_2 \setminus B_1$. Previamente habíamos visto que $I_1 \cap I_2 = B_1 \cap I_2$, lo cual es equivalente a que $I_2 \setminus I_1 = I_2 \setminus B_1$, así que tenemos la siguiente igualdad:

$$B_2 \setminus B_1 = I_2 \setminus B_1 = I_2 \setminus I_1. \tag{2}$$

Puede demostrarse también que $B_1 \setminus B_2 = I_1 \setminus B_2$. Además, como $I_2 \subseteq B_2$, entonces $I_1 \setminus B_2 \subseteq I_1 \setminus I_2$. Por tanto, tenemos las siguientes contenciones de conjuntos:

$$B_1 \setminus B_2 = I_1 \setminus B_2 \subseteq I_1 \setminus I_2 \tag{3}$$

Como $\mathcal{B}$ cumple (B1), (B2) y (B3), por el Teorema 3.5 también satisface (B2*), así, $|B_1| = |B_2|$, y como $B_1 = (B_1 \cap B_2) \cup (B_1 \setminus B_2)$, $B_2 = (B_1 \cap B_2) \cup (B_2 \setminus B_1)$, y dichas uniones son disjuntas, entonces $|B_1 \setminus B_2| = |B_2 \setminus B_1|$. Por las relaciones establecidas en (2) y (3), resulta que

$$|I_2 \setminus I_1| \leq |I_1 \setminus I_2|. \tag{4}$$

Pero I_1 e I_2 son tales que $|I_1| < |I_2|$, y pueden escribirse como las uniones disjuntas $I_1 = (I_1 \cap I_2) \cup (I_1 \setminus I_2)$, $I_2 = (I_1 \cap I_2) \cup (I_2 \setminus I_1)$, entonces $|I_1 \setminus I_2| < |I_2 \setminus I_1|$, lo cual contradice (4). Por lo tanto, (I3) es verdadera. Así que en efecto $M = (E, \mathcal{I})$ es un matroide.

Sólo resta verificar que los elementos de la familia $\mathcal{B}$ son las bases de M. Sea $B \in \mathcal{B}$. Como $B \subseteq B$, entonces $B \in \mathcal{I}$, esto es, B es un conjunto independiente. Ahora supongamos que B' es un conjunto independiente tal que $B \subseteq B'$. Por (B2) tenemos que $B = B'$, es decir, el único conjunto independiente que contiene a B es él mismo, con lo cual queda probado que B es un conjunto independiente maximal. Para el sentido inverso, sea B una base de M. $B \in \mathcal{I}$, entonces existe $B' \in \mathcal{B}$ tal que $B \subseteq B'$. B' también es conjunto independiente, pero B es maximal, entonces ocurre que $B = B'$ y por consiguiente $B \in \mathcal{B}$. □

Los Teoremas 3.3 y 3.6 justifican la equivalencia entre la definición de matroide por conjuntos independientes (Definición 2.2) y la que se da a continuación.

Definición 3.7 (Por bases)**.** Un *matroide* M es un par ordenado $(E, \mathcal{B})$ donde E es un conjunto finito y $\mathcal{B}$ es una familia de subconjuntos de E que satisface las siguientes tres condiciones:

(B1) (No trivialidad) $\mathcal{B} \neq \emptyset$.

(B2) (Familia Sperner o clutter) Si $B_1, B_2 \in \mathcal{B}$ y $B_1 \subseteq B_2$, entonces $B_1 = B_2$.

(B3) (Intercambio débil en bases) Si $B_1, B_2 \in \mathcal{B}$ y $x \in B_1 \setminus B_2$, entonces existe un elemento $y \in B_2 \setminus B_1$ tal que $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

M se llama matroide sobre E y los elementos de $\mathcal{B}$ se llaman *bases* de M.

Esta definición surge de la idea de abstraer algunas de las propiedades que cumple la familia de bases de un espacio vectorial V de dimensión n. Dicha familia satisface (B1) porque todo espacio vectorial tiene una base; satisface (B2*) porque todas las bases de un espacio vectorial tienen el mismo número de elementos. A continuación se verá que también se verifica (B3). Sean $B_1 = \{v_1, v_2, \ldots, v_n\}$ y $B_2 = \{w_1, w_2, \ldots, w_n\}$ dos bases para V. Sin pérdida de generalidad supóngase que $v_1 \notin B_2$ y que para todo $i \in [n]$, $(B_1 \setminus \{v_1\}) \cup \{w_i\}$ no es una base para V. Entonces $(B_1 \setminus \{v_1\}) \cup \{w_i\}$ es linealmente dependiente, de manera que existen escalares $\alpha_1, \alpha_2, \ldots, \alpha_n$ no todos iguales a cero tales que:

$$\alpha_1 w_i + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0.$$

Note que α_1 debe ser distinto de cero, pues los vectores $v_2, \ldots, v_n$ son linealmente independientes, así que

$$w_i = -\frac{\alpha_2}{\alpha_1} v_2 - \cdots - \frac{\alpha_n}{\alpha_1} v_n.$$

Esto es, para todo $i \in [n]$, $w_i \in gen(\{v_2, \ldots, v_n\})$, por lo que,

$$gen(\{w_1, w_2, \ldots, w_n\}) \subseteq gen(\{v_2, \ldots, v_n\})$$

y como $gen(\{w_1, w_2, \ldots, w_n\}) = V$, luego $V = gen(\{v_2, \ldots, v_n\})$, pero esto contradice que la dimensión de V sea n. Entonces se cumple (B3).

Sin embargo, ésta no es la única manera de definir un matroide a partir de sus bases. El Teorema 3.5 presenta propiedades equivalentes que pueden emplearse para tal fin además de (B1), (B2) y (B3). El siguiente corolario expone una equivalencia más que es consecuencia inmediata de resultados anteriores, pero se enuncia ya que se empleará posteriormente.

Corolario 3.8. *Sea E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E que satisface las propiedades (B1), (B2*) y (B3*). Sea $\mathcal{I}$ la familia de subconjuntos de E que están contenidos en algún elemento de $\mathcal{B}$. Entonces $M = (E, \mathcal{I})$ es un matroide y $\mathcal{B}$ es su conjunto de bases. De manera inversa, si M es un matroide, entonces su familia de bases $\mathcal{B}$ satisface las propiedades (B1), (B2*) y (B3*).*

Demostración. Para la necesidad supongamos que $\mathcal{B}$ satisface las propiedades (B1), (B2*) y (B3*). Por ser un caso particular de (B3*), $\mathcal{B}$ cumple (B3). Por el Teorema 3.5, $\mathcal{B}$ satisface (B1), (B2) y (B3). La conclusión del corolario es inmediata por el Teorema 3.6.

Para la suficiencia, sea M un matroide. Por el Lema 3.2 y por los Teoremas 3.3 y 3.4, la familia de bases $\mathcal{B}$ satisface las propiedades (B1), (B2*) y (B3*). □

En los siguientes ejemplos se presentan las bases de cada uno de los matroides mencionados anteriormente.

Ejemplo 3.9. Sea $M = (E, \mathcal{I})$ un matroide representable. Una base de M es un conjunto de vectores de E linealmente independiente maximal, es decir, es una base para el generado de E en el sentido usual de álgebra lineal. En caso de que el generado de E sea igual al espacio vectorial V, entonces una base para M es una base para V.

Ejemplo 3.10. Sea $M = (E, \mathcal{I})$ el matroide uniforme de rango k sobre un conjunto de n elementos definido en el Ejemplo 2.5. Veamos que $\mathcal{B}$ es la familia de todos los subconjuntos de E de cardinalidad k. Sea $B \subseteq E$ de cardinalidad k. Claramente $B \in \mathcal{I}$. Ahora, supongamos que B' es un conjunto independiente tal que $B \subseteq B'$, entonces $k = |B| \leq |B'|$. Como $B' \in \mathcal{I}$, entonces $|B'| \leq k$. Concluimos pues que $|B'| = k$ y por tanto $B = B'$, con lo cual queda probado que B es una base. A la inversa, supongamos que B es una base de M y supongamos que $|B| \neq k$. Como B es un conjunto independiente ocurre que $|B| \leq k$, luego $|B| < k$. Como $B \subseteq E$ y $k \leq n = |E|$ entonces existe un subconjunto B_1 de E que contiene propiamente a B y cuya cardinalidad es igual k. Por sus características B_1 es elemento de $\mathcal{I}$, pero esto contradice que B sea un conjunto independiente maximal. Así, $|B| = k$.

4 Definición por circuitos

A continuación se enuncia un concepto que permitirá dar una definición más de matroide. Es el concepto dual de base, así que, si una base es un conjunto independiente maximal, el siguiente concepto se referirá a un conjunto dependiente minimal.

Definición 4.1. Sea $M = (E, \mathcal{I})$ un matroide. Un subconjunto C de E se llama *circuito* si es un conjunto dependiente minimal, es decir, si es dependiente pero todos sus subconjuntos propios son independientes. Se denota con $\mathcal{C}$ el conjunto de circuitos de M. En símbolos:

$$\mathcal{C} = \{C \subseteq E \mid C \notin \mathcal{I} \text{ y } \forall I \subsetneq C : I \in \mathcal{I}\}.$$

Nótese que a diferencia de las bases, los circuitos de un matroide pueden tener diferente cardinalidad entre ellos; un circuito podría ser un conjunto unitario cuyo único subconjunto propio independiente sea el conjunto vacío, o podría ser todo el conjunto subyacente del matroide.

En el siguiente teorema se establecen algunas de las propiedades que caracterizan a la familia de circuitos de un matroide.

Teorema 4.2. *Sea M un matroide. Su colección de circuitos $\mathcal{C}$ tiene las siguientes propiedades:*

(C1) (No trivialidad) $\emptyset \notin \mathcal{C}$.

(C2) (Clutter) Si C_1 y C_2 son elementos de $\mathcal{C}$ y $C_1 \subseteq C_2$, entonces $C_1 = C_2$.

(C3) (Eliminación de circuito) Si C_1 y C_2 son elementos distintos de $\mathcal{C}$ y $e \in C_1 \cap C_2$, entonces existe un elemento C_3 de $\mathcal{C}$ tal que $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

Demostración. Por (J1), $\emptyset$ es independiente, entonces (C1) se cumple. Sean C_1 y C_2 circuitos tales que $C_1 \subseteq C_2$ y supongamos que $C_1 \neq C_2$, es decir, que C_1 es subconjunto propio de C_2. Como C_2 es un conjunto dependiente minimal, C_1 debe ser independiente, lo cual contradice que C_1 sea un circuito. Por lo tanto, $C_1 = C_2$, esto es, se cumple (C2).

Probemos ahora que (C3) es cierta. Tomemos dos circuitos diferentes C_1 y C_2, y un elemento $e \in C_1 \cap C_2$. Supongamos que ningún subconjunto de $(C_1 \cup C_2) \setminus \{e\}$ es circuito, en particular tenemos que $(C_1 \cup C_2) \setminus \{e\}$ no es

un circuito. Entonces $(C_1 \cup C_2) \setminus \{e\}$ no es un conjunto dependiente o es un conjunto dependiente pero no minimal. Lo segundo no puede ocurrir, pues en caso de que sí, $(C_1 \cup C_2) \setminus \{e\}$ debería tener como subconjunto un conjunto dependiente minimal, es decir, algún circuito, lo cual contradice lo supuesto. Así que $(C_1 \cup C_2) \setminus \{e\}$ es independiente. Dado que $C_1 \neq C_2$, entonces $C_1 \nsubseteq C_2$ o $C_2 \nsubseteq C_1$. Sin pérdida de generalidad supongamos que ocurre lo segundo. Entonces existe un elemento de C_2 que no está en C_1, digamos $f \in C_2 \setminus C_1$. El conjunto $C_2 \setminus \{f\}$ es independiente pues C_2 es un circuito. Elijamos un subconjunto I de $C_1 \cup C_2$, independiente maximal que contenga a $C_2 \setminus \{f\}$ (existe porque $C_2 \setminus \{f\} \in \mathcal{I}$ y $C_2 \setminus \{f\} \subseteq C_1 \cup C_2$). Si $f \in I$, entonces $C_2 \subseteq I$, y tendríamos que C_2 es independiente, lo cual no es cierto, así que $f \notin I$. $C_1 \nsubseteq I$ pues C_1 es dependiente, así que existe $g \in C_1 \setminus I$. Como $f \notin C_1$ y $g \in C_1$, entonces $f \neq g$. Ya que f y g no son elementos de I se cumple que

$$|I| \leq |(C_1 \cup C_2) \setminus \{f, g\}| = |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) \setminus \{e\}|.$$

Como I y $(C_1 \cup C_2) \setminus \{e\}$ son conjuntos independientes tales que $|I| < |(C_1 \cup C_2) \setminus \{e\}|$, por (I3) existe $h \in \{(C_1 \cup C_2) \setminus \{e\}\} \setminus I$ tal que $I \cup \{h\} \in \mathcal{I}$. Dado que $I \subseteq C_1 \cup C_2$ y $h \in C_1 \cup C_2$, luego $I \cup \{h\} \subseteq C_1 \cup C_2$, y como $h \notin I$, $I \cup \{h\}$ es un subconjunto de $C_1 \cup C_2$ independiente de cardinalidad mayor que I que contiene a $C_2 \setminus \{f\}$, lo cual contradice la elección de I. Por lo tanto, la propiedad (C3) es verdadera. □

Existen dos tipos de conjuntos dependientes en un matroide: los minimales, que son los circuitos, y los que no son minimales, y por lo tanto, contienen un circuito. Entonces los conjuntos independientes son todos aquellos que no pertenecen a ninguna de esas dos clases de conjuntos, es decir, conjuntos que no son un circuito y que no contienen un circuito, en resumen, conjuntos que no contienen un circuito. Esta idea se emplea en el siguiente teorema que establece cómo puede construirse un matroide a partir de una familia de conjuntos que verifica las tres propiedades dadas en el Teorema 4.2.

Teorema 4.3. *Sean E un conjunto y $\mathcal{C}$ una familia de subconjuntos de E que satisface (C1), (C2) y (C3). Sea $\mathcal{I}$ la familia de subconjuntos de E tales que ninguno de sus subconjuntos es elemento de $\mathcal{C}$, es decir,*

$$\mathcal{I} = \{I \subseteq E \mid \forall C \in \mathcal{C}, C \nsubseteq I\}.$$

Entonces $(E, \mathcal{I})$ es un matroide que tiene a $\mathcal{C}$ como su colección de circuitos.

Demostración. El único subconjunto del conjunto $\emptyset$ es el conjunto $\emptyset$ y por (C1) $\emptyset \notin \mathcal{C}$, entonces $\emptyset$ no contiene algún elemento de $\mathcal{C}$. Por tanto $\emptyset \in \mathcal{I}$, así que (I1) es verdadera. Sean $I \in \mathcal{I}$ y $J \subseteq I$. Ninguno de los subconjuntos de I es elemento de $\mathcal{C}$, entonces todo subconjunto de J tampoco es elemento de $\mathcal{C}$, de donde J es elemento de $\mathcal{I}$ y, por lo tanto, (I2) se cumple.

Veamos por último que (I3) es verdadera. Sean $I_1, I_2 \in \mathcal{I}$ tales que $|I_1| < |I_2|$. Supongamos que para toda $x \in I_2 \setminus I_1$, $I_1 \cup \{x\} \notin \mathcal{I}$. Elijamos un elemento I_3 de $\mathcal{I}$ que esté contenido en $I_1 \cup I_2$, cuya cardinalidad sea mayor que la de I_1 (I_2 satisface tales condiciones) y tal que $|I_1 \setminus I_3|$ sea mínima. Si suponemos que $I_1 \setminus I_3 = \emptyset$, entonces $I_1 \subseteq I_3$ y como $|I_1| < |I_3|$, entonces existe $x \in I_3 \setminus I_1$, y dado que $I_3 \subseteq I_1 \cup I_2$, entonces $x \in I_2 \setminus I_1$ y como $I_1 \cup \{x\} \subseteq I_3$, por (I2) $I_1 \cup \{x\} \in \mathcal{I}$, lo cual contradice lo supuesto. Así pues, $I_1 \setminus I_3 \neq \emptyset$; elegimos un elemento e de $I_1 \setminus I_3$. Si suponemos que $I_3 \setminus I_1 = \emptyset$, entonces $I_3 \subseteq I_1$, lo cual no ocurre porque la cardinalidad de I_1 es menor que la cardinalidad de I_3. Por tanto, $I_3 \setminus I_1 \neq \emptyset$. Para cada elemento f de $I_3 \setminus I_1$, sea $T_f = (I_3 \cup \{e\}) \setminus \{f\}$. Por su definición, $T_f \subseteq I_1 \cup I_2$. Además, tomando en cuenta que $e \in I_1 \cap I_3^C$ y $f \notin I_1$ se cumple lo siguiente:

$$\begin{aligned} I_1 \setminus T_f &= I_1 \cap \left[(I_3 \cup \{e\}) \cap \{f\}^C\right]^C = I_1 \cap \left[(I_3 \cup \{e\})^C \cup \{f\}\right] \\ &= I_1 \cap \left[(I_3^C \cap \{e\}^C) \cup \{f\}\right] = \left[I_1 \cap (I_3^C \cap \{e\}^C)\right] \cup [I_1 \cap \{f\}] \\ &= \left[I_1 \cap (I_3^C \cap \{e\}^C)\right] \cup \emptyset = (I_1 \cap I_3^C) \setminus \{e\} \subsetneq I_1 \cap I_3^C = I_1 \setminus I_3. \end{aligned}$$

Por lo tanto, $|I_1 \setminus T_f| < |I_1 \setminus I_3|$. T_f es un subconjunto de $I_1 \cup I_2$ y tiene cardinalidad mayor que I_1 ($|T_f| = |I_3|$). Por la manera en la que elegimos a I_3, tenemos que $T_f \notin \mathcal{I}$, de donde T_f contiene un elemento C_f de $\mathcal{C}$. Dado que $f \notin T_f$, entonces $f \notin C_f$. También debe cumplirse que $e \in C_f$, en caso contrario $C_f \subseteq I_3$, lo cual contradice que $I_3 \in \mathcal{I}$. Si $C_f \cap (I_3 \setminus I_1) = \emptyset$, entonces $C_f \subseteq (I_3 \setminus I_1)^C = (I_3 \cap I_1^C)^C = I_3^C \cup I_1$, es decir, $C_f \subseteq I_1 \cup I_3^C$. Como C_f también es subconjunto de $(I_3 \cup \{e\}) \setminus \{f\}$ se cumple lo siguiente:

$$\begin{aligned} C_f &\subseteq (I_1 \cup I_3^C) \cap \left[(I_3 \cup \{e\}) \setminus \{f\}\right] \\ &= \left[I_1 \cap \left[(I_3 \cup \{e\}) \cap \{f\}^C\right]\right] \cup \left[I_3^C \cap \left[(I_3 \cup \{e\}) \cap \{f\}^C\right]\right] \end{aligned}$$

$$
\begin{aligned}
&= \Big[I_1 \cap \big[(I_3 \cap \{f\}^C) \cup (\{e\} \cap \{f\}^C)\big]\Big] \cup \\
&\quad \Big[I_3^C \cap \big[(I_3 \cap \{f\}^C) \cup (\{e\} \cap \{f\}^C)\big]\Big] \\
&= (I_1 \cap I_3 \cap \{f\}^C) \cup (I_1 \cap \{e\}) \cup (I_3^C \cap I_3 \cap \{f\}^C) \cup (I_3^C \cap \{e\}) \\
&= [(I_1 \cap I_3) \cap \{f\}^C] \cup \{e\} \\
&= [(I_1 \cap I_3) \cup \{e\}] \setminus \{f\} \\
&\subseteq I_1.
\end{aligned}
$$

Esto es, $C_f \subseteq I_1$, lo cual contradice que $I_1 \in \mathcal{I}$. Entonces existe un elemento g en $C_f \cap (I_3 \setminus I_1)$. Nótese que como $f \notin C_f$, entonces $g \neq f$. Como $g \in I_3 \setminus I_1$, existe su respectivo $C_g \in \mathcal{C}$. No puede ocurrir que $C_g = C_f$ ya que $g \in C_f$ y $g \notin C_g$. Entonces C_f y C_g son dos elementos distintos de $\mathcal{C}$ y $e \in C_f \cap C_g$. Por (C3) existe $C \in \mathcal{C}$ tal que $C \subseteq (C_f \cup C_g) \setminus \{e\}$. Como C_f y C_g son subconjuntos de $I_3 \cup \{e\}$, entonces $(C_f \cup C_g) \setminus \{e\} \subseteq I_3$, de donde $C \subseteq I_3$, lo cual contradice que $I_3 \in \mathcal{I}$. Entonces debe cumplirse (I3). Por lo tanto, $M = (E, \mathcal{I})$ es un matroide.

Ahora veamos que $\mathcal{C}$ es el conjunto de circuitos de M. Sea C un circuito de M, veamos que $C \in \mathcal{C}$. Como C es circuito, no es un conjunto independiente, así que por la definición de $\mathcal{I}$, C debe tener un subconjunto C' que es elemento de $\mathcal{C}$. Como C es circuito, todo subconjunto propio de C es independiente. Sea I un subconjunto propio de C. Para todo $C \in \mathcal{C}$ se cumple que $C \not\subseteq I$ y como $I \subseteq I$ entonces $I \notin \mathcal{C}$ y por lo tanto todo subconjunto propio de C no es elemento de $\mathcal{C}$, por consiguiente $C' = C$, es decir, $C \in \mathcal{C}$. Ahora, si $C \in \mathcal{C}$, como $C \subseteq C$, entonces $C \notin \mathcal{I}$, luego C es dependiente. Si suponemos que un subconjunto C' de C también es dependiente, entonces $C' \notin \mathcal{I}$, de donde existe $C'' \in \mathcal{C}$ tal que $C'' \subseteq C'$. En particular tenemos que $C'' \subseteq C$. Para C y C'' se cumple (C2) y por tanto concluimos que $C = C''$, más aún, $C' = C$ lo cual verifica que C es conjunto dependiente minimal, y por tanto C es circuito de M. □

Los Teoremas 4.2 y 4.3 justifican la siguiente definición.

Definición 4.4 (Por circuitos)**.** Un *matroide* M es un par ordenado $(E, \mathcal{C})$, donde E es un conjunto finito y $\mathcal{C}$ es un subconjunto de $\mathcal{P}(E)$ que verifica las siguientes tres propiedades:

(C1) (No trivialidad) $\emptyset \notin \mathcal{C}$.

(C2) (Familia Sperner o clutter) Si $C_1, C_2 \in \mathcal{C}$ son tales que $C_1 \subseteq C_2$, entonces $C_1 = C_2$.

(C3) (Eliminación de circuito) Si C_1 y C_2 son dos elementos distintos de $\mathcal{C}$ y $e \in C_1 \cap C_2$, entonces existe $C_3 \in \mathcal{C}$ tal que $C_3 \subseteq (C_1 \cup C_1) \setminus \{e\}$.

M se llama matroide sobre E y los elementos de $\mathcal{C}$ se llaman *circuitos* de M.

Para finalizar este apartado, se presentan los circuitos de los matroides dados en los ejemplos que se trataron en las secciones anteriores.

Ejemplo 4.5. Sea M un matroide representable. Los circuitos de M son conjuntos de vectores linealmente dependientes, cuyos subconjuntos propios son todos linealmente independientes.

Ejemplo 4.6. Sea M el matroide uniforme de rango k sobre el conjunto E de n elementos. Claramente $\mathcal{C}$ es la familia de subconjuntos de E de cardinalidad $k+1$. En este ejemplo, todos los circuitos del matroide tienen la misma cardinalidad. Sin embargo, no siempre es así.

5 Definición por función rango

Sean $M = (E, \mathcal{I})$ un matroide y $A \subseteq E$. Como $\emptyset \subseteq A$ y $\emptyset$ es un conjunto independiente, entonces A tiene a un elemento de $\mathcal{I}$ como subconjunto. Puede compararse el tamaño de todos los conjuntos independientes que están contenidos en A. Como A es finito, entonces existe el máximo de dichas cardinalidades. Lo anterior garantiza que el siguiente concepto está bien definido.

Definición 5.1. Sean $M = (E, \mathcal{I})$ un matroide y $A \subseteq E$. El *rango* o la *dimensión* de A es la mayor de las cardinalidades de los conjuntos independientes que están contenidos en A y se denota por $r(A)$, es decir:

$$r(A) = \text{máx}\{|I| : I \in \mathcal{I} \text{ e } I \subseteq A\}.$$

$r(E)$ se llama el *rango del matroide* M, y se denota por $r(M)$.

En otras palabras, la función rango r asociada a un matroide es una función del conjunto potencia del conjunto subyacente del matroide al conjunto de los enteros no negativos que se define de la siguiente forma:

$$\begin{aligned} r\colon \mathcal{P}(E) &\to \mathbb{N} \cup \{0\} \\ A &\mapsto \text{máx}\{|I| : I \in \mathcal{I} \text{ e } I \subseteq A\}. \end{aligned}$$

Puede darse una definición de matroide en términos de la función rango. La manera de hacerlo se presenta en los teoremas siguientes. Para probarlos se necesita una generalización de la propiedad (J3) que se enuncia y se demuestra a continuación.

Lema 5.2. *Sea $M = (E, \mathcal{I})$ un matroide, y sean I y J dos conjuntos independientes tales que $|I| < |J|$, $n = |J| - |I|$. Entonces existen $x_1, x_2, \ldots, x_n \in J \setminus I$ tales que $I \cup \{x_1, x_2, \ldots, x_n\} \in \mathcal{I}$.*

Demostración. Sean $I, J \in \mathcal{I}$ tales que $|J| - |I| = n$, $n \geq 1$. Si $n = 1$, la proposición es cierta ya que es justamente (J3). Supongamos que el resultado es válido para cualquier pareja de conjuntos independientes tales que la diferencia de sus cardinalidades es igual a n. Si $|J| - |I| = n + 1$, elijamos $x \in J$. Por (I2), $J \setminus \{x\} \in \mathcal{I}$, además $|J \setminus \{x\}| - |I| = n$. Por la hipótesis de inducción existen $x_1, x_2, \ldots, x_n \in (J \setminus \{x\}) \setminus I$ tales que $I \cup \{x_1, x_2, \ldots, x_n\} \in \mathcal{I}$. Ahora, $I \cup \{x_1, x_2, \ldots, x_n\}$ y J son dos conjuntos independientes tales que $|J| = |I \cup \{x_1, x_2, \ldots, x_n\}| + 1$. Por (J3) tenemos que existe $x_{n+1} \in J \setminus (I \cup \{x_1, x_2, \ldots, x_n\})$ tal que $I \cup \{x_1, x_2, \ldots, x_n, x_{n+1}\} \in \mathcal{I}$, es decir, $x_1, x_2, \ldots, x_n, x_{n+1} \in J \setminus I$ son tales que $I \cup \{x_1, x_2, \ldots, x_n, x_{n+1}\} \in \mathcal{I}$, con lo cual el lema queda establecido. □

Teorema 5.3. *Sea $M = (E, \mathcal{I})$ un matroide. La función rango r de M satisface las siguientes propiedades para cualesquiera $A, B \subseteq E$:*

(r1) (Normalización) $0 \leq r(A) \leq |A|$;

(r2) (Creciente) Si $A \subseteq B$, entonces $r(A) \leq r(B)$;

(r3) (Semimodular) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Demostración. Como $r(A)$ es la cardinalidad de un subconjunto de A entonces trivialmente se cumple que $0 \leq r(A) \leq |A|$. Sean $A, B \subseteq E$ tales que $A \subseteq B$. Todo subconjunto de A también es subconjunto de B, así que

$$r(A) = \text{máx}\{|I| : I \in \mathcal{I} \text{ e } I \subseteq A\} \leq \text{máx}\{|J| : J \in \mathcal{I} \text{ y } J \subseteq B\} = r(B).$$

Esto prueba que (r2) se satisface. Sea I_1 un conjunto independiente contenido en $A \cap B$ tal que $r(A \cap B) = |I_1|$. Queremos encontrar un subconjunto I de $A \cup B$ que sea independiente, que satisfaga que $r(A \cup B) = |I|$ y que contenga a I_1. Lo haremos de la siguiente forma: como $A \cap B \subseteq A \cup B$, por (r2) ocurre que $r(A \cap B) = r(A \cup B)$ o $r(A \cap B) < r(A \cup B)$. Si ocurre lo primero, entonces I_1 es un subconjunto de $A \cup B$ que es independiente y que satisface que $r(A \cup B) = |I_1|$, así que elegimos $I = I_1$. Si ocurre lo segundo, sea I_2 un conjunto independiente contenido en $A \cup B$ tal que $r(A \cup B) = |I_2|$. Tenemos que $|I_1| < |I_2|$, sea $n = |I_2| - |I_1|$. Por el Lema 5.2, existen $x_1, x_2, \ldots, x_n \in I_2 \setminus I_1$ tales que $I_1 \cup \{x_1, x_2, \ldots, x_n\} \in \mathcal{I}$. En particular, $x_1, x_2, \ldots, x_n \in A \cup B$, por lo tanto, $I_1 \cup \{x_1, x_2, \ldots, x_n\}$ es un subconjunto independiente de $A \cup B$ de la misma cardinalidad que I_2, entonces $r(A \cup B) = |I_1 \cup \{x_1, x_2, \ldots, x_n\}|$, así que elegimos $I = I_1 \cup \{x_1, x_2, \ldots, x_n\}$. Podemos descomponer a I como la siguiente unión disjunta:

$$I = [I \cap (A \cap B)] \cup [I \cap (A \setminus B)] \cup [I \cap (B \setminus A)].$$

Definimos $I_A = I \cap (A \setminus B)$ e $I_B = I \cap (B \setminus A)$. Observemos que $I \cap (A \cap B) = (I_1 \cup \{x_1, x_2, \ldots, x_n\}) \cap (A \cap B)$. Si suponemos que para algún $i \in [n]$, $x_i \in A \cap B$, entonces $I_1 \cup \{x_i\} \subseteq A \cap B$. Dado que $I_1 \cup \{x_i\} \subsetneq I$, $I_1 \cup \{x_i\} \in \mathcal{I}$. Por consiguiente, $I_1 \cup \{x_i\}$ sería un subconjunto de $A \cap B$ de mayor cardinalidad que I_1, lo cual contradice que $r(A \cap B) = |I_1|$. Por lo tanto, $I \cap (A \cap B) = I_1$ y tenemos lo siguiente:

$$r(A \cup B) = |I| = |I_1| + |I_A| + |I_B|. \tag{5}$$

También la unión disjunta $I_1 \cup I_A$ es un conjunto independiente por ser subconjunto de I y además está contenido en A. Por lo tanto, $|I_1| + |I_A| \leq r(A)$. De manera análoga obtenemos que $|I_1| + |I_B| \leq r(B)$. Entonces $2|I_1| + |I_A| + |I_B| \leq r(A) + r(B)$. Pero recordemos que $|I_1| = r(A \cap B)$, entonces

$$|I_1| + |I_A| + |I_B| + r(A \cap B) \leq r(A) + r(B). \tag{6}$$

De (5) y (6) obtenemos la desigualdad esperada. Así que la función rango r de M satisface (r1), (r2) y (r3). □

Existe un conjunto de condiciones que son equivalentes a (r1), (r2) y (r3). En los siguientes teoremas se demuestra dicha equivalencia.

Teorema 5.4. *Sea r una función de valor entero con dominio el conjunto potencia de un conjunto finito E que satisface las propiedades (r1), (r2) y (r3). También r satisface lo siguiente:*

(r1) (Normalización local)* $r(\emptyset) = 0$.

(r2) (Incremento del rango en una unidad) Para todo* $A \subseteq E$ *y para todo* $x \in E$, *se tiene que*

$$r(A) \leq r(A \cup \{x\}) \leq r(A) + 1.$$

(r3) (Semimodularidad local) Para cualquier* $A \subseteq E$ *y cualesquiera* $x, y \notin A$, *si* $r(A) = r(A \cup \{x\}) = r(A \cup \{y\})$, *entonces*

$$r(A) = r(A \cup \{x, y\}).$$

Demostración. Por (r1) tenemos que $0 \leq r(\emptyset) \leq |\emptyset| = 0$, y, por lo tanto, $r(\emptyset) = 0$, esto es, (r1*) se cumple. Sean $A \subseteq E$ y $x \in E$. Como $A \subseteq A \cup \{x\}$, por (r2), $r(A) \leq r(A \cup \{x\})$. Ahora, por (r3) tenemos que $r(A \cup \{x\}) \leq r(A) + r(\{x\}) - r(A \cap \{x\})$. Como $|\{x\}| = 1$, por (r1) tenemos que $r(\{x\})$ es igual a 0 o a 1. Si $r(\{x\}) = 0$, entonces $r(A \cup \{x\}) \leq r(A) - r(A \cap \{x\})$. También por (r1) sabemos que el rango de cualquier subconjunto de E es mayor o igual que 0, así que $r(A) - r(A \cap \{x\}) \leq r(A) < r(A) + 1$. Si $r(\{x\}) = 1$, entonces $r(A \cup \{x\}) \leq r(A) + 1 - r(A \cap \{x\}) \leq r(A) + 1$. Podemos concluir entonces que (r2*) se satisface.

Sean $A \subseteq E$, $x, y \notin A$ tales que $r(A) = r(A \cup \{x\}) = r(A \cup \{y\})$. Si $x = y$ el resultado claramente es cierto, así que podemos suponer $x \neq y$. Aplicando la propiedad (r3) a los conjuntos $A \cup \{x\}$ y $A \cup \{y\}$, se tiene que

$$\begin{aligned} r\big((A \cup \{x\}) \cup (A \cup \{y\})\big) + r\big((A \cup \{x\}) \cap (A \cup \{y\})\big) &\leq r(A \cup \{x\}) + \\ &\quad r(A \cup \{y\}) \\ &= r(A) + r(A). \end{aligned}$$

Dado que $(A \cup \{x\}) \cap (A \cup \{y\}) = [(A \cup \{x\}) \cap A] \cup [(A \cup \{x\}) \cap \{y\}] = A \cup \emptyset = A$, ocurre que $r(A \cup \{x, y\}) + r(A) \leq r(A) + r(A)$, de donde $r(A \cup \{x, y\}) \leq r(A)$. Además, por (r2), $r(A) \leq r(A \cup \{x, y\})$. Concluimos que $r(A \cup \{x, y\}) = r(A)$, por lo que (r3*) es verdadera. □

A continuación se demostrará el recíproco del Teorema 5.4, es decir, que una función de valor entero r que satisface las propiedades (r1*), (r2*) y (r3*) también verifica (r1), (r2) y (r3). Primero se probará que se cumplen (r1) y (r2).

Teorema 5.5. *Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Entonces r satisface las propiedades (r1) y (r2).*

Demostración. Sea $A \subseteq E$. Probaremos que se cumple la condición (r1) por inducción sobre $|A|$. Si $|A| = 0$, por (r1*) tenemos que $r(\emptyset) = 0 = |\emptyset|$, así que (r1) es verdadera si $|A| = 0$. Supongamos que (r1) es cierta para todos los conjuntos de cardinalidad n y que A es un conjunto de cardinalidad $n + 1$. Sea $A' \subseteq A$ tal que $|A'| = n$ y sea x tal que $\{x\} = A \setminus A'$. Por hipótesis de inducción se tiene que

$$0 \leq r(A') \leq |A'|. \tag{7}$$

Por (r2*) obtenemos la siguiente desigualdad:

$$r(A') \leq r(A' \cup \{x\}) \leq r(A') + 1. \tag{8}$$

Así que por (7) y por (8) obtenemos que

$$0 \leq r(A') \leq r(A' \cup \{x\}) \leq r(A') + 1 \leq |A'| + 1 = |A|,$$

de donde, $0 \leq r(A' \cup \{x\}) \leq |A|$. Pero $A' \cup \{x\} = A$, así que $0 \leq r(A) \leq |A|$. Por lo tanto, la proposición (r1) es válida.

Sean $A, B \subseteq E$ tales que $A \subseteq B$. Demostraremos que se cumple (r2) por inducción sobre $|B \setminus A|$. Si $|B \setminus A| = 0$, entonces $A = B$ y (r2) se satisface. Supongamos ahora que la afirmación se cumple para todas las parejas de conjuntos tales que uno es subconjunto del otro y tales que la cardinalidad de la diferencia del más grande con el más pequeño igual a n. Supongamos que $|B \setminus A| = n + 1$. Podemos elegir $x \in B \setminus A$ tal que $|B \setminus (A \cup \{x\})| = n$. Como $A \cup \{x\} \subseteq B$, podemos aplicar la hipótesis de inducción y obtenemos que $r(A \cup \{x\}) \leq r(B)$. Por (r2*), $r(A) \leq r(A \cup \{x\})$, así que $r(A) \leq r(B)$. Por lo tanto, (r2) se cumple. □

Demostrar que una función de valor entero que satisface (r1*), (r2*) y (r3*) verifica también (r3) es un tanto más complejo. En la prueba se hará uso de dos lemas; el primero se demuestra y del segundo se omite su demostración.

Lema 5.6. *Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Si $A \subseteq E$, y $x_1, x_2, \ldots, x_n \in E \setminus A$ son tales que $r(A) = r(A \cup \{x_1\}) = r(A \cup \{x_2\}) = \cdots = r(A \cup \{x_n\})$, entonces*

$$r(A \cup \{x_1, x_2, \ldots, x_n\}) = r(A).$$

Demostración. La demostración la haremos por inducción sobre n. Si $n = 1$, el resultado es trivialmente cierto. Supongamos que la afirmación es válida para algún n. Sean $x_1, x_2, \ldots, x_n, x_{n+1} \in E \setminus A$ tales que para cada $i \in [n+1]$, $r(A) = r(A \cup \{x_i\})$ y sin pérdida de generalidad supongamos que son todos diferentes entre sí. Podemos aplicar la hipótesis de inducción a los conjuntos $\{x_1, x_2, \ldots, x_{n-1}, x_n\}$ y $\{x_1, x_2, \ldots, x_{n-1}, x_{n+1}\}$, ya que ambos tienen n elementos, de donde obtenemos lo siguiente:

$$r(A) = r(A \cup \{x_1, x_2, \ldots, x_{n-1}, x_n\}) = r(A \cup \{x_1, x_2, \ldots, x_{n-1}, x_{n+1}\}). \quad (9)$$

Por el Teorema 5.5 (r2) se cumple, así que las siguientes desigualdades son ciertas:

$$\begin{aligned} r(A) = r(A \cup \{x_1\}) &\leq r(A \cup \{x_1, x_2, \ldots, x_{n-1}\}) \\ &\leq r(A \cup \{x_1, x_2, \ldots, x_{n-1}, x_n\}) \\ &= r(A), \end{aligned}$$

por lo cual $r(A \cup \{x_1, x_2, \ldots, x_{n-1}\}) = r(A)$. Por (9) se tiene que:

$$\begin{aligned} r(A \cup \{x_1, x_2, \ldots, x_{n-1}\}) &= r((A \cup \{x_1, x_2, \ldots, x_{n-1}\}) \cup \{x_n\}) \\ &= r((A \cup \{x_1, x_2, \ldots, x_{n-1}\}) \cup \{x_{n+1}\}). \end{aligned}$$

Por (r3*) aplicado al conjunto $A \cup \{x_1, x_2, \ldots, x_{n-1}\}$ concluimos que $r(A \cup \{x_1, x_2, \ldots, x_{n-1}\}) = r((A \cup \{x_1, x_2, \ldots, x_{n-1}\}) \cup \{x_n, x_{n+1}\})$, de aquí tenemos finalmente que $r(A \cup \{x_1, x_2, \ldots, x_n, x_{n+1}\}) = r(A)$. Así que el resultado es válido para toda n. □

La propiedad mencionada en el Lema 5.6 se identificará con (r3**).

Lema 5.7. *([2] Lema 2.47, pág. 69) Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Sean $A, B \subseteq E$ tales que $A \subseteq B$, y sea $x \in E$. Entonces*

$$r(A \cup \{x\}) - r(A) \geq r(B \cup \{x\}) - r(B).$$

Teorema 5.8. *Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Entonces r satisface la propiedad (r3).*

Demostración. Sean $A, B \subseteq E$. Si $|A \setminus B| = 0$, entonces $A \subseteq B$, y por lo tanto, $A \cup B = B$, $A \cap B = A$, de donde $r(A \cup B) + r(A \cap B) = r(B) + r(A)$ y el resultado se cumple. Supongamos que el resultado es cierto para cualquier pareja de conjuntos tales que la cardinalidad de su diferencia es igual a n. Supongamos que $|A \setminus B| = n + 1$. Podemos elegir $x \in A \setminus B$. Entonces $|(A \setminus \{x\}) \setminus B| = n$. Por la hipótesis de inducción tenemos que

$$r((A \setminus \{x\}) \cup B) + r((A \setminus \{x\}) \cap B) \leq r(A \setminus \{x\}) + r(B).$$

Como $A \setminus \{x\} \subseteq (A \setminus \{x\}) \cup B$, por el Lema 5.7 se verifica que

$$r((A \setminus \{x\}) \cup \{x\}) - r(A \setminus \{x\}) \geq r(((A \setminus x) \cup B) \cup \{x\}) - r((A \setminus x) \cup B),$$

de donde

$$r(A) - r(A \setminus \{x\}) \geq r(A \cup B) - r((A \setminus x) \cup B). \tag{10}$$

De (10) y de la hipótesis de inducción obtenemos las siguientes desigualdades:

$$r(A \cup B) - r(A) + r(A \setminus \{x\}) \leq r((A \setminus x) \cup B) \leq r(A \setminus \{x\}) + r(B) - r((A \setminus \{x\}) \cap B).$$

Como $x \notin B$, entonces $A \setminus \{x\} \cap B = A \cap B$. Por lo tanto,

$$r(A \cup B) - r(A) \leq r(B) - r(A \cap B),$$

de donde obtenemos la desigualdad $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$, es decir, (r3) es verdadera. □

Dada la colección de conjuntos independientes de un matroide, es posible encontrar el rango de todo subconjunto de E. Si se tiene el conjunto subyacente E de un matroide M y el rango de cada subconjunto de E, ¿cómo se encuentran los conjuntos independientes? El rango de un conjunto independiente es igual a su cardinalidad, y si un conjunto tiene rango igual a su cardinalidad, entonces éste debe ser independiente, ya que dicho conjunto es finito y por lo tanto, no puede tener un subconjunto independiente propio con su misma cardinalidad. Esto indica que los conjuntos independientes son los únicos conjuntos con la propiedad de que su rango coincide con su cardinalidad. Esta idea permite construir un matroide partiendo de una función que satisface las propiedades (r1), (r2) y (r3) como se explica en el siguiente teorema.

Teorema 5.9. *Sea E un conjunto finito con una función de valor entero r con dominio $\mathcal{P}(E)$ tal que satisface las propiedades (r1), (r2) y (r3). Definimos la familia*

$$\mathcal{I} = \{I \subseteq E \mid r(I) = |I|\}.$$

Entonces $M = (E, \mathcal{I})$ es un matroide que tiene a r como su función rango.

Demostración. A continuación probaremos que la familia $\mathcal{I}$ satisface (I1), (I2) e (I3).

Por (r1) tenemos que $0 \leq r(\emptyset) \leq |\emptyset|$, de donde $r(\emptyset) = 0 = |\emptyset|$, y por lo tanto, $\emptyset \in \mathcal{I}$, es decir, (I1) se cumple. Sean $I \in \mathcal{I}$ y $J \subseteq I$. Aplicando (r3) a los conjuntos $I \setminus J$ y J tenemos que $r\left((I \setminus J) \cup J\right) + r\left((I \setminus J) \cap J\right) \leq r(I \setminus J) + r(J)$, es decir, $r(I) + r(\emptyset) \leq r(I \setminus J) + r(J)$, y por (I1), $r(I) \leq r(I \setminus J) + r(J)$. Como $I \in \mathcal{I}$, entonces $r(I) = |I|$, así que

$$|I| \leq r(I \setminus J) + r(J). \tag{11}$$

Por (r1), $r(I \setminus J) \leq |I \setminus J|$ y $r(J) \leq |J|$, lo cual implica que

$$r(I \setminus J) + r(J) \leq |I \setminus J| + |J| = |I|. \tag{12}$$

De (11) y de (12) tenemos que $|I| \leq r(I \setminus J) + r(J) \leq |I|$, así que $r(I \setminus J) + r(J) = |I| = |I \setminus J| + |J|$, de donde $|I \setminus J| - r(I \setminus J) = r(J) - |J|$. Como $r(I \setminus J) \leq |I \setminus J|$ y $r(J) \leq |J|$, entonces $0 \leq |I \setminus J| - r(I \setminus J)$ y $r(J) - |J| \leq 0$, por lo que $0 \leq |I \setminus J| - r(I \setminus J) = r(J) - |J| \leq 0$, luego $0 = |I \setminus J| - r(I \setminus J) = r(J) - |J|$, por consiguiente, $r(I \setminus J) = |I \setminus J|$ y $r(J) = |J|$. Así queda demostrado que $J \in \mathcal{I}$, es decir, (I2) se satisface. Para probar (I3), sean $I, J \in \mathcal{I}$ tales que $|I| < |J|$. Como $I, J \in \mathcal{I}$, entonces $r(I) = |I|$ y $r(J) = |J|$. Sea $J \setminus I = \{x_1, x_2, \ldots, x_k\}$, para alguna $k \geq 1$. Supongamos que (I3) no se cumple, es decir, que para todo $i \in [k]$, $I \cup \{x_i\} \notin \mathcal{I}$, entonces $r(I \cup \{x_i\}) \neq |I \cup \{x_i\}| = |I| + 1$. Por (r1), $r(I \cup \{x_i\}) \leq |I \cup \{x_i\}| = |I| + 1$, entonces $r(I \cup \{x_i\}) < |I| + 1$. Por (r2), $r(I) \leq r(I \cup \{x_i\})$, así que $|I| \leq r(I \cup \{x_i\}) < |I| + 1$. Por lo tanto, para todo $i \in [k]$, $r(I \cup \{x_i\}) = |I|$. Si $|J \setminus I| = 1$, entonces $I \cup \{x_1\} = J$ y por lo anterior tenemos que $r(J) = r(I \cup \{x_1\}) = r(I) = |I| < |J| = r(J)$, lo cual es una contradicción. Entonces $|J \setminus I| > 1$, es decir, existe $k > 1$ tal que $J \setminus I = \{x_1, x_2, \ldots, x_k\}$. Como r verifica (r1), (r2) y (r3), por el Teorema 5.4 r cumple con (r1*), (r2*) y (r3*), luego por el Lema 5.6 se cumple (r3**), así que $r(I \cup \{x_1, x_2, \ldots, x_k\}) = |I|$, pero $I \cup \{x_1, x_2, \ldots, x_k\} = J$, entonces

$|J| = r(J) = |I| < |J|$, lo cual es una contradiccón. Por lo tanto, (I3) se satisface y en efecto $M = (E, \mathcal{I})$ es un matroide.

Por último, vamos a demostrar que en efecto r es la función rango de M. Sea s la función rango de M, es decir, la función que a cada subconjunto de E le asigna la mayor de las cardinalidades de los conjuntos independientes contenidos en él. Nuestro objetivo es comprobar que $r = s$. El dominio de ambas funciones es $\mathcal{P}(E)$, así que sólo falta verificar que su regla de correspondencia es la misma. Sean $A \subseteq E$ e $I \subseteq A$ un conjunto independiente tal que $s(A) = |I|$. Como $I \in \mathcal{I}$, cumple que $r(I) = |I|$, de manera que $s(A) = |I| = r(I)$. Además, por (r2) tenemos que $r(I) \leq r(A)$. Por lo tanto, para todo $A \in \mathcal{P}(E)$, $s(A) \leq r(A)$. Supongamos que la otra desigualdad no se cumple, es decir, que existe $A \in \mathcal{P}(E)$ tal que $s(A) < r(A)$. Sea $I \in \mathcal{I}$ subconjunto de A tal que $s(A) = |I|$, entonces $|I| < r(A)$ y para todo $x \in A \setminus I$, $I \cup \{x\} \notin \mathcal{I}$. Por (r2*), $|I| = r(I) \leq r(I \cup \{x\}) \leq r(I)+1 = |I|+1$, pero por la manera en la que se tomó I no puede ocurrir que $r(I \cup \{x\}) = |I|+1$, por lo que $r(I \cup \{x\}) = r(I)$. Como r verifica (r3**), obtenemos que $r(A) = r(I) = |I|$, lo cual contradice que $|I| < r(A)$. Concluimos entonces que para todo $A \in \mathcal{P}(E)$, $r(A) \leq s(A)$. Así que en efecto, r es la función rango de M. □

Los Teoremas 5.3 y 5.9 permiten establecer una cuarta definición de matroide.

Definición 5.10 (Por función rango)**.** Un *matroide* M es un par ordenado (E, r) donde E es un conjunto finito y r es una función de valor entero con dominio $\mathcal{P}(E)$ que cumple las siguientes propiedades para cualesquiera $A, B \subseteq E$:

(r1) (Normalización) $0 \leq r(A) \leq |A|$;

(r2) (Creciente) Si $A \subseteq B$, entonces $r(A) \leq r(B)$;

(r3) (Semimodular) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

En este contexto, M se llama un matroide sobre E. La función r se conoce como la *función rango* de M.

6 Representación gráfica de un matroide

En matemáticas es de gran ayuda poder representar gráficamente un concepto, pues en muchas ocasiones es más sencillo interpretar algunas de sus propiedades mediante un dibujo o diagrama que teniendo sólo texto. En el caso de matroides, igual que ocurre con sus definiciones, existen múltiples formas de representar un matroide. Esto depende en gran medida del rango del matroide que desee representarse. A continuación se presenta una manera de representar e interpretar gráficamente un matroide de rango 3.

Ejemplo 6.1. Las reglas para elaborar la representación gráfica de un matroide de rango 3 son las siguientes:

- Los puntos aislados que se colocan dentro de una nube representan un conjunto unitario dependiente. Cualquier otro punto representa un conjunto unitario independiente.
- Dos puntos que se colocan en la misma posición corresponden a un conjunto dependiente de dos elementos. Cualquier otro par de puntos en el que ninguno de los dos pertenezca a un conjunto unitario dependiente representa un conjunto independiente.
- Tres puntos colineales simbolizan un conjunto dependiente. Cualquier otro conjunto de tres puntos que no contenga un conjunto dependiente de cardinalidad uno o dos es considerado independiente.
- Cualquier conjunto de 4 o más puntos representa a un conjunto dependiente.

Figura 2: Representación de un matroide.

Sea M el matroide representado en la Figura 2. M tiene como conjunto subyacente a $E = \{a, b, c, d, e, f\}$. M tiene 20 conjuntos independientes y son los siguientes:

- Cardinalidad 0: $\emptyset$.
- Cardinalidad 1: $\{a\}, \{b\}$, $\{c\}$, $\{d\}$, $\{e\}$.

- Cardinalidad 2: $\{a, c\}$, $\{a, d\}$, $\{a, e\}$, $\{b, c\}$, $\{b, d\}$, $\{b, e\}$, $\{c, d\}$, $\{c, e\}$, $\{d, e\}$.
- Cardinalidad 3: $\{a, c, e\}$, $\{a, d, e\}$, $\{b, c, e\}$, $\{b, d, e\}$, $\{c, d, e\}$.

Las bases de M, son justamente todos los conjuntos independientes de cardinalidad 3.

Los conjuntos dependientes de M son los siguientes 44 conjuntos:

- Cardinalidad 1: $\{f\}$.
- Cardinalidad 2: $\{a, b\}$, $\{a, f\}$, $\{b, f\}$, $\{c, f\}$, $\{d, f\}$, $\{e, f\}$.
- Cardinalidad 3: $\{a, b, c\}$, $\{a, b, d\}$, $\{a, b, e\}$, $\{a, b, f\}$, $\{a, c, d\}$, $\{a, c, f\}$, $\{a, d, f\}$, $\{a, e, f\}$, $\{b, c, d\}$, $\{b, c, f\}$, $\{b, d, f\}$, $\{b, e, f\}$, $\{c, d, f\}$, $\{c, e, f\}$, $\{d, e, f\}$.
- Cardinalidad 4: $\{a, b, c, d\}$, $\{a, b, c, e\}$, $\{a, b, c, f\}$, $\{a, b, d, e\}$, $\{a, b, d, f\}$, $\{a, b, e, f\}$, $\{a, c, d, e\}$, $\{a, c, d, f\}$, $\{a, c, e, f\}$, $\{a, d, e, f\}$, $\{b, c, d, e\}$, $\{b, c, d, f\}$, $\{b, c, e, f\}$, $\{b, d, e, f\}$, $\{c, d, e, f\}$.
- Cardinalidad 5: $\{a, b, c, d, e\}$, $\{a, b, c, d, f\}$, $\{a, b, c, e, f\}$, $\{a, b, d, e, f\}$, $\{a, c, d, e, f\}$, $\{b, c, d, e, f\}$.
- Cardinalidad 6: $\{a, b, c, d, e, f\}$.

Los conjuntos dependientes minimales, o bien, los circuitos de M, son $\{f\}$, $\{a, b\}$, $\{a, c, d\}$, $\{b, c, d\}$. Vemos en este ejemplo circuitos que tienen distinta cardinalidad entre sí, como se había mencionado anteriormente.

A continuación se enlistan todos los subconjuntos de E agrupados según su rango.

- Rango 0: $\emptyset$, $\{f\}$.
- Rango 1: $\{a, b\}$, $\{a, f\}$, $\{b, f\}$, $\{c, f\}$, $\{d, f\}$, $\{e, f\}$ y todos los conjuntos independientes de cardinalidad 1.
- Rango 2: $\{a, b, c\}$, $\{a, b, d\}$, $\{a, b, e\}$, $\{a, c, d\}$, $\{a, c, f\}$, $\{a, d, f\}$, $\{a, e, f\}$, $\{b, c, d\}$, $\{b, c, f\}$, $\{b, d, f\}$, $\{b, e, f\}$, $\{c, d, f\}$, $\{c, e, f\}$, $\{d, e, f\}$, $\{a, b, c, d\}$, $\{a, b, c, f\}$, $\{a, b, d, f\}$, $\{a, b, e, f\}$, $\{a, c, d, f\}$, $\{b, c, d, f\}$, $\{a, b, c, d, f\}$ y los conjuntos independientes de cardinalidad 2.

- Rango 3: los conjuntos independientes de cardinalidad 3 y los conjuntos restantes.

7 Matroide representable sobre el campo $\mathbb{F}$ y matroide dual

Como es usual en matemáticas, después de definir un nuevo concepto y establecer algunas de las propiedades que cumple es de interés saber si pueden relacionarse entre sí objetos del mismo tipo, por ejemplo, dos espacios vectoriales, dos grupos o dos anillos. Se busca una función que preserve la operación u operaciones definidas y una estructura en la que por alguna razón sea más sencillo resolver determinado problema. En el caso de matroides lo que se desea es una función que preserve la independencia de los conjuntos.

Definición 7.1. Sean $M_1 = (E_1, \mathcal{I}_1)$ y $M_2 = (E_2, \mathcal{I}_2)$ matroides. Una función $\varphi\colon E_1 \to E_2$ es un *morfismo de matroides* si para cada $I \in \mathcal{I}_1$, $\varphi(I) \in \mathcal{I}_2$. La función φ se llama *isomorfismo de matroides* si φ es morfismo de matroides, φ es biyectiva y φ^{-1} es también un morfismo de matroides. Si existe un isomorfismo de matroides entre M_1 y M_2, decimos que M_1 y M_2 son *isomorfos*.

Recuérdese que uno de los objetivos principales de este trabajo es asociar un matroide a un código lineal. Se ha visto que ciertos resultados de la teoría de códigos pueden demostrarse con menos dificultad empleando resultados de la teoría de matroides. A un código lineal ya se le ha asignado su matriz generadora.

Lo que se hará a continuación es relacionar una matriz con un matroide.

Teorema 7.2. *Sea $E_G = [n]$ el conjunto de etiquetas de las columnas de una matriz G de tamaño $k \times n$ sobre un campo $\mathbb{F}$ y sea $\mathcal{I}_G$ la familia de subconjuntos I de E_G para los cuales el conjunto de columnas con etiquetas en I es linealmente independiente en el espacio vectorial $\mathbb{F}^k$. Entonces $(E_G, \mathcal{I}_G)$ es un matroide.*

Demostración. Demostraremos que $(E_G, \mathcal{I}_G)$ es un matroide mediante la caracterización de conjuntos independientes. La condición (I1) se satisface ya que el conjunto de columnas etiquetadas por $\emptyset$ es el conjunto $\emptyset$, que es linealmente independiente en $\mathbb{F}^k$. Sea $I \in \mathcal{I}_G$, entonces el conjunto de columnas etiquetadas por I es linealmente independiente en $\mathbb{F}^k$, así que si $J \subseteq I$, el

conjunto de columnas etiquetadas por J está contenido en el conjunto de columnas etiquetadas por I, y por ello también es linealmente independiente en $\mathbb{F}^k$. Por lo tanto, se cumple (I2). Para probar (I3), tomemos $I, J \in \mathcal{I}$, tales que $|I| < |J|$. Sea W el subespacio de $\mathbb{F}^k$ generado por los vectores columna etiquetados por $I \cup J$. Tenemos que $\dim W \geq |J|$. Supongamos que para todo elemento e de $J \setminus I$, el conjunto de vectores columna etiquetados por $I \cup \{e\}$ es linealmente dependiente. Sea $\{v_1, v_2, \ldots, v_k\}$ el conjunto de vectores etiquetados por I y $\{u_1, u_2, \ldots, u_l\}$ el conjunto de vectores correspondiente al conjunto $J \setminus I$. Entonces para cada $i \in \{1, 2, \ldots, l\}$ existen escalares $\lambda_1^{(i)}, \lambda_2^{(i)}, \ldots, \lambda_k^{(i)}, \lambda_{k+1}^{(i)}$ no todos iguales a 0, tales que

$$\lambda_1^{(i)} v_1 + \lambda_2^{(i)} v_2 + \cdots + \lambda_k^{(i)} v_k + \lambda_{k+1}^{(i)} u_i = 0,$$

en particular $\lambda_{k+1}^{(i)} \neq 0$, pues los vectores $v_1, v_2, \ldots, v_k$ son linealmente independientes, así que

$$u_i = -\frac{\lambda_1^{(i)}}{\lambda_{k+1}^{(i)}} v_1 - \frac{\lambda_2^{(i)}}{\lambda_{k+1}^{(i)}} v_2 - \cdots - \frac{\lambda_k^{(i)}}{\lambda_{k+1}^{(i)}} v_k,$$

es decir, cada uno de los elementos u_i puede escribirse como una combinación lineal de los elementos v_i. Entonces W es el subespacio generado por los vectores etiquetados por I, luego

$$|J| \leq \dim W = |I| < |J|$$

lo cual no puede ocurrir. Por lo tanto, (I3) se cumple. Entonces, $(E_G, \mathcal{I}_G)$ es un matroide. □

Definición 7.3. El matroide que se obtiene como en el Teorema 7.2 a partir de una matriz G se denota por $M[G]$ y se llama el *matroide vector* de G.

Nótese que el Teorema 7.2 es más general, ya que no se limita a matrices con entradas en un campo finito, sino que abarca incluso campos infinitos como es el caso del siguiente ejemplo.

Ejemplo 7.4. Sea G la matriz

1 2 3 4 5

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

sobre el campo de los números reales. Sean E_G e $\mathcal{I}_G$ como en el Teorema 7.2. Entonces $E_G = \{1,2,3,4,5\}$ e $\mathcal{I}_G = \{\emptyset, \{1\}, \{2\}, \{4\}, \{5\}, \{1,2\}, \{1,5\}, \{2,4\}, \{2,5\}, \{4,5\}\}$. La familia de bases de $M[G]$ es $\mathcal{B} = \{\{1,2\}, \{1,5\}, \{2,4\}, \{2,5\}, \{4,5\}\}$; la familia de conjuntos dependientes de este matroide es $\{\{3\}, \{1,3\}, \{1,4\}, \{2,3\}, \{3,4\}, \{3,5\}\} \cup \{X \subseteq E\colon |X| \geq 3\}$ y su familia de circuitos es $\{\{3\}, \{1,4\}, \{1,2,5\}, \{2,4,5\}\}$. Observe que $M[G]$ es un matroide de rango 2.

Definición 7.5. Un matroide M se llama *representable* sobre el campo $\mathbb{F}$ si existe una matriz G con entradas en $\mathbb{F}$ tal que M es isomorfo al matroide $M[G]$. G se llama *representación* para M sobre $\mathbb{F}$ o $\mathbb{F}-$*representación* para M. Un matroide es *representable* si tiene una representación sobre algún campo.

Sea C un código sobre $\mathbb{F}_q$ con matrices generadoras G_1 y G_2. ¿Es cierto que $(E_{G_1}, \mathcal{I}_{G_1}) = (E_{G_2}, \mathcal{I}_{G_2})$? La respuesta es afirmativa, pero para demostrar que en efecto es así, se presenta el siguiente teorema.

Teorema 7.6. *Sea G una matriz de tamaño $k \times n$ con entradas en un campo $\mathbb{F}$. Sea G' una matriz que se obtiene realizando algunas de las operaciones elementales con los renglones de G (es decir, intercambio de renglones, multiplicación de un renglón por una constante diferente de cero o sumar un múltiplo de un renglón a otro renglón). Entonces $M[G] = M[G']$.*

Demostración. Sean $G = (g_{ij})$, $G' = (g'_{ij})$. Por la forma en la que se obtiene G', las matrices G y G' son del mismo tamaño, así que $E_G = E_{G'}$. Veamos que los conjuntos independientes de $M[G]$ pertenecen a $\mathcal{I}_{G'}$. Si $J = \{l_1, l_2, \ldots, l_r\} \in \mathcal{I}_G$, entonces los vectores columna con etiquetas en J son linealmente independientes, así que la única solución al sistema lineal homogéneo

$$\begin{aligned} \alpha_1 g_{1l_1} + \alpha_2 g_{1l_2} + \cdots + \alpha_r g_{1l_r} &= 0 \\ \alpha_1 g_{2l_1} + \alpha_2 g_{2l_2} + \cdots + \alpha_r g_{2l_r} &= 0 \\ &\vdots \\ \alpha_1 g_{kl_1} + \alpha_2 g_{kl_2} + \cdots + \alpha_r g_{kl_r} &= 0 \end{aligned} \tag{13}$$

es el vector $[\alpha_1, \alpha_2, \ldots, \alpha_r] = [0, 0, \ldots, 0]$. Queremos ver si los vectores columna de G' etiquetados por J también son linealmente independientes. Planteamos el siguiente sistema de ecuaciones:

$$\begin{aligned} \beta_1 g'_{1l_1} + \beta_2 g'_{1l_2} + \cdots + \beta_r g'_{1l_r} &= 0 \\ \beta_1 g'_{2l_1} + \beta_2 g'_{2l_2} + \cdots + \beta_r g'_{2l_r} &= 0 \\ &\vdots \\ \beta_1 g'_{kl_1} + \beta_2 g'_{kl_2} + \cdots + \beta_r g'_{kl_r} &= 0 \end{aligned} \tag{14}$$

La matriz de coeficientes asociada al sistema lineal homogéneo (14) es (g'_{ml_n}) de tamaño $k \times r$. Como G' se obtiene mediante operaciones elementales con los renglones de G, entonces existe una serie de operaciones elementales que al aplicarlas a la matriz G' se obtiene la matriz G, así que si aplican dichas operaciones a la matriz (g'_{ml_n}) se obtiene la matriz (g_{ml_n}) que es la matriz asociada al sistema (13). Por lo tanto, la única solución al sistema (14) es el vector $[\beta_1, \beta_2, \ldots, \beta_r] = [0, 0, \ldots, 0]$, entonces los vectores columna de G' etiquetados por J en efecto son linealmente independientes, por lo que $J \in \mathcal{I}_{G'}$. Análogamente se prueba que si $J \in \mathcal{I}_{G'}$ también $J \in \mathcal{I}_G$. En conclusión, $\mathcal{I}_G = \mathcal{I}_{G'}$ y con ello queda probado que $M[G] = M[G']$. □

Definición 7.7. Sea $M = (E, \mathcal{I})$ un matroide y $\mathcal{B}$ su familia de bases. Para cada $B \in \mathcal{B}$ se establece la notación $B^\perp = E \setminus B$. Definimos la familia $\mathcal{B}^\perp = \{B^\perp \mid B \in \mathcal{B}\}$. Sea $\mathcal{I}^\perp = \{I \subseteq E \mid \exists B \in \mathcal{B} : I \subseteq B^\perp\}$. $M^\perp = (E, \mathcal{I}^\perp)$ se llama *matroide dual* de M.

Teorema 7.8. *Sea M un matroide. Entonces $M^\perp$ es, en efecto, un matroide.*

Demostración. En esta prueba haremos uso del Corolario 3.8: usaremos el hecho de que M es matroide y por ello la familia $\mathcal{B}$ satisface (B1), (B2*) y (B3*), y por otro lado probaremos que la familia $\mathcal{B}^\perp$ satisface las propiedades (B1), (B2*) y (B3*) para demostrar que $M^\perp$ es un matroide.

La familia $\mathcal{B}$ satisface la propiedad (B1), así que existe $B \in \mathcal{B}$, de donde $B^\perp \in \mathcal{B}^\perp$, es decir, $\mathcal{B}^\perp \neq \emptyset$ y por tanto, $\mathcal{B}^\perp$ satisface la propiedad (B1). Ahora, sean ${B_1}^\perp, {B_2}^\perp \in \mathcal{B}^\perp$, donde $B_1, B_2 \in \mathcal{B}$. Por (B2*), $|B_1| = |B_2|$, de aquí obtenemos inmediatamente que $|E \setminus B_1| = |E \setminus B_2|$, es decir, $|{B_1}^\perp| = |{B_2}^\perp|$, así que $\mathcal{B}^\perp$ también satisface (B2*). Dado que $B_1^\perp \setminus B_2^\perp = (E \setminus B_1) \setminus (E \setminus B_2) = B_2 \setminus B_1$, si $x \in B_1^\perp \setminus B_2^\perp$, entonces $x \in B_2 \setminus B_1$. $\mathcal{B}$ verifica la propiedad (B3*), es decir, la propiedad de intercambio fuerte en bases, por lo que existe

$y \in B_1 \setminus B_2 = B_2^\perp \setminus B_1^\perp$ tal que $(B_1 \setminus \{y\}) \cup \{x\}$ y $(B_2 \setminus \{x\}) \cup \{y\}$ son bases del matroide M, entonces $E \setminus [(B_1 \setminus \{y\}) \cup \{x\}]$ y $E \setminus [(B_2 \setminus \{x\}) \cup \{y\}]$ son elementos de $B^\perp$. Se tiene que $E \setminus [(B_1 \setminus \{y\}) \cup \{x\}] = [E \setminus (B_1 \setminus \{y\})] \cap (E \setminus \{x\}) = [(E \setminus B_1) \cup \{y\}] \cap (E \setminus \{x\}) = [E \setminus (B_1 \cup \{x\})] \cup \{y\} = [(E \setminus B_1) \setminus \{x\}] \cup \{y\} = (B_1^\perp \setminus \{x\}) \cup \{y\}$, y de manera análoga puede mostrarse que $E \setminus [(B_2 \setminus \{x\}) \cup \{y\}] = (B_2^\perp \setminus \{y\}) \cup \{x\}$, por lo cual concluimos que $(B_1^\perp \setminus \{x\}) \cup \{y\}$ y $(B_2^\perp \setminus \{y\} \cup \{x\} \in \mathcal{B}^\perp$. Entonces $\mathcal{B}^\perp$ verifica (B3*). Por lo tanto, $M^\perp$ es un matroide. □

El siguiente teorema muestra una forma sencilla de calcular en el matroide dual el rango de un subconjunto a partir de la función rango del matroide original. Se denotará la función rango del matroide dual como $r^\perp$.

Teorema 7.9. *Sea $M = (E, \mathcal{I})$ un matroide y r su función rango. Para $A \subseteq E$ se cumple lo siguiente:*

$$r^\perp(A) = r(E \setminus A) + |A| - r(M).$$

Demostración. Veamos que $r^\perp(A) = \text{máx}\{|A \cap B^\perp| \colon B^\perp \in \mathcal{B}^\perp\}$. Por definición $r^\perp(A)$ es la cardinalidad del conjunto independiente más grande de $M^\perp$ que está contenido en A. Sea $I_A \subseteq A$ conjunto independiente tal que $r^\perp(A) = |I_A|$ y $B_1^\perp$ una base de $M^\perp$ tal que $I_A \subseteq B_1^\perp$, por lo tanto $I_A \subseteq A \cap B_1^\perp$. Además, existe una base B_1 del matroide M tal que $B_1^\perp = E \setminus B_1$. Si suponemos que $I_A \subsetneq A \cap B_1^\perp$, entonces existe $x \in A \cap B_1^\perp$ tal que $x \notin I_A$ y se cumple que $I_A \subsetneq I_A \cup \{x\} \subseteq A \cap B_1^\perp$. Como $I_A \cup \{x\} \subseteq B_1^\perp$ e $I_A \cup \{x\} \subseteq A$, $I_A \cup \{x\}$ es un conjunto independiente de $M^\perp$ que es subconjunto de A y cuya cardinalidad es mayor que I_A, lo cual es una contradicción. Por lo tanto, $I_A = A \cap B_1^\perp$. Finalmente, como todos los conjuntos de la forma $A \cap B^\perp$ son conjuntos independientes de $M^\perp$ que están contenidos en A e I_A es uno de tales conjuntos pero de cardinalidad máxima, entonces concluimos que $r^\perp(A) = |I_A| = \text{máx}\{|A \cap B^\perp| \colon B^\perp \in \mathcal{B}^\perp\}$. Entonces $B_1^\perp$ es un elemento de $\mathcal{B}^\perp$ cuya intersección con A es máxima, o equivalentemente, $B_1^\perp$ es un elemento de $\mathcal{B}^\perp$ cuya intersección con $E \setminus A$ es mínima, entonces la intersección de $B_1 = E \setminus B_1^\perp$ y $E \setminus A$ es máxima entre todos los complementos de las bases de $\mathcal{B}^\perp$ (que son las bases de M), así que por definición de rango del matroide M, $r(E \setminus A) = |(E \setminus A) \cap B_1|$. E se divide en los siguientes cuatro conjuntos ajenos entre sí: $A \setminus B_1^\perp$, $A \cap B_1^\perp$, $B_1^\perp \setminus A$ y $E \setminus (A \cup B_1^\perp) = (E \setminus A) \cap (E \setminus B_1^\perp) = (E \setminus A) \cap B_1$. Sean x_1, x_2, x_3

y x_4 las cardinalidades de dichos conjuntos, respectivamente. Tenemos que $x_2 = |A \cap B_1^{\perp}| = r^{\perp}(A)$ y $x_4 = |E \setminus (A \cup B_1^{\perp})| = |(E \setminus A) \cap B_1| = r(E \setminus A)$. Además, $x_3 + x_4 = |B_1^{\perp} \setminus A| + |E \setminus (A \cup B^{\perp})| = |E| - |A|$ y $x_2 + x_3 = |A \cap B_1^{\perp}| + |B_1^{\perp} \setminus A| = |B_1^{\perp}| = |E| - |B_1| = |E| - r(M)$, así que por el valor de x_3 en ambas igualdades tenemos que $|E| - |A| - x_4 = |E| - r(M) - x_2$, por lo que $x_2 = |A| + x_4 - r(M)$, y sustituyendo los valores ya conocidos de x_2 y x_4 concluimos finalmente que $r^{\perp}(A) = r(E \setminus A) + |A| - r(M)$. □

8 Conclusiones

En este trabajo se estudiaron los conceptos básicos de la teoría de matroides, poniendo especial atención al establecimiento de las equivalencias entre algunas de las definiciones del concepto de matroide. Tales equivalencias, explicadas a detalle en las secciones 2, 3, 4 y 5, pueden esquematizarse como se muestra en la Figura 3.

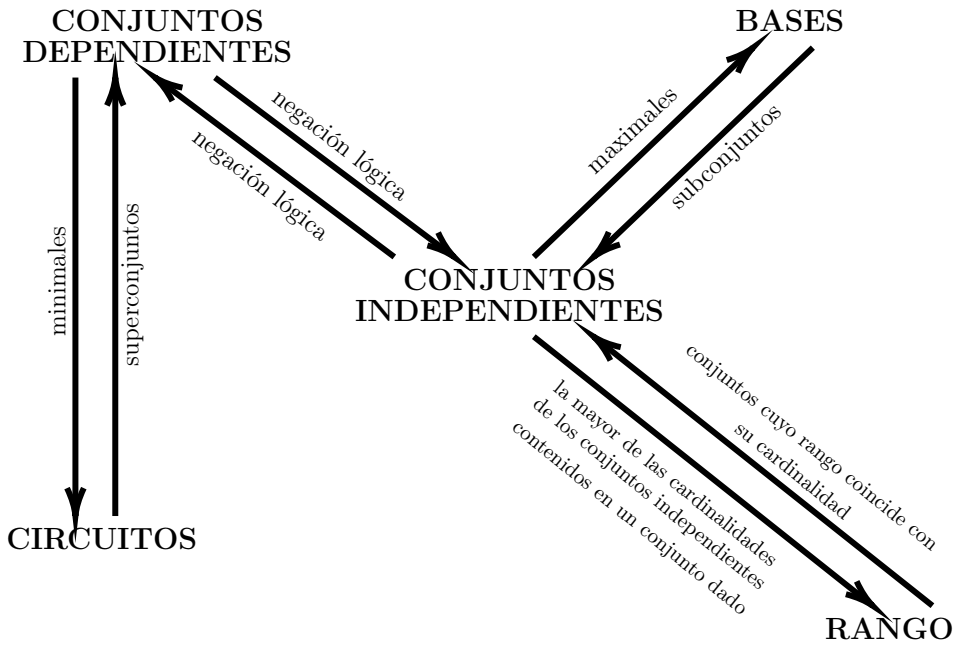

Figura 3: Equivalencias entre definiciones de matroide

Además se presentaron algunos ejemplos de los conceptos definidos y se abordó una manera de representar un matroide de manera gráfica. Esperamos que este material sea una herramienta útil para el lector que está por iniciarse en el estudio de alguna de las múltiples aplicaciones de esta rama de las matemáticas. Como ejemplos de estas aplicaciones invitamos al lector a consultar [4], donde encontrará una utilización de los matroides en el área de la Teoría de la Información ó [5], en el cual los matroides son ocupados para resolver problemas en el área de Cinemática de Robots ó [1], en donde se relacionan a los matroides con la Criptografía a través del esquema de compartición de secretos ideal.

Agradecimientos

Bibliografía

[1] Ernest F. Brickell and Daniel M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, J. Cryptology **4** (1991), 123–134

[2] Gary Gordon y Jennifer McNulty, *Matroids: A Geometric Introduction*, Cambridge University Press, 2012.

[3] James Oxley, *Matroid Theory*, Oxford University Press, 1992.

[4] S. El Rouayheb, A. Sprintson y C. Georghiades, *On the Index Coding Problem and Its Relation to Network Coding and Matroid Theory*, IEEE Transactions on Information Theory, **56(7)**, (2010), 3187-3195, doi: 10.1109/TIT.2010.2048502.

[5] J. Lenarčič, y B. Siciliano (Eds.), *Advances in Robot Kinematics 2020*, Vol. 15, Springer Nature, 2020.

[6] Hassler Whitney, *On the Abstract Properties of Linear Dependence*, American Journal of Mathematics **57** (1935), 63–87.

Facultad de Ciencias Físico Matemáticas, BUAP
Avenida San Claudio y 18 Sur, Colonia San Manuel,

Puebla, Pue. C.P. 72570

mireya.diaz.ljdb@gmail.com
carlos.lopezandrade@correo.buap.mx
cguillen@fcfm.buap.mx