BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

POSGRADO EN CIENCIAS MATEMÁTICAS

ALGUNAS CASI CARACTERIZACIONES DE ESTRUCTURAS DE ACCESO IDEALES MEDIANTE MATROIDES

TESIS QUE PARA OBTENER EL GRADO DE

MAESTRA EN CIENCIAS MATEMÁTICAS

PRESENTA:

MIREYA DÍAZ LÓPEZ

DIRECTOR DE TESIS:

DR. CARLOS ALBERTO LÓPEZ ANDRADE

PUEBLA, PUE., DICIEMBRE 2023

DR. SEVERINO MUÑOZ AGUIRRE
SECRETARIO DE INVESTIGACIÓN Y
ESTUDIOS DE POSGRADO, FCFM-BUAP
P R E S E N T E:

Por este medio le informo que la C:

MIREYA DÍAZ LÓPEZ

estudiante de la Maestría en Ciencias (Matemáticas), ha cumplido con las indicaciones que el Jurado le señaló en el Coloquio que se realizó el día 27 de noviembre de 2023, con la tesis titulada:

Algunas casi caracterizaciones de estructuras de acceso ideales mediante matroides

Por lo que se le autoriza a proceder con los trámites y realizar el examen de grado en la fecha que se le asigne.

A T E N T A M E N T E.
H. Puebla de Z. a 27 de noviembre de 2023

DR. RAÚL ESCOBEDO CONDE
COORDINADOR DEL POSGRADO
EN MATEMÁTICAS.

D*REC/mtrv

Facultad
de Ciencias
Físico Matemáticas

Av. San Claudio y 18 sur, edif. FM1
Ciudad Universitaria, Col. San
Manuel, Puebla, Pue. C.P. 72570
(222) 229 55 00 Ext. 7550 y 7552

A mi familia pequeña: Armando y mi pequeño Andrés.
A mi familia grande: mis papás, Eloy y Elisa, y mis hermanas, Karla y Daniela.

Agradecimientos

Quiero agradecer a Dios por permitirme llegar a este punto de mi vida llena de tantas bendiciones.

Para mi esposo, Armando Ortega Xique, sólo tengo palabras de amor y agradecimiento. Mi amor, gracias por ser así. Eres la persona más maravillosa que ha llegado a mi vida y por eso la vida a tu lado me resulta tan bella. Me has enseñado las cosas más bonitas de este mundo a lo largo de estos 11 años juntos. Estás lleno de bondad y ternura. Crees en mí más que nadie en el mundo y te agradezco por convencerme de que puedo lograr cosas que a mí me parecen imposibles. Eres el mejor esposo del mundo, gracias por amarme tanto. Gracias también por esforzarte tanto por nuestra familia. Juntos hemos formado la mejor pareja, y sé que ahora con bebé formaremos el mejor equipo. Te amo tanto.

Quiero agradecer a mi bebé que está en camino, mi pequeño Andrés. Durante estos 5 meses que has estado dentro de mí has sido el bebé más tranquilo del mundo y me permitiste terminar este trabajo sin mayor dificultad. Te doy gracias por ello y por haber llegado a nuestras vidas en el mejor momento. Espero que algún día leas esto y sepas que te amamos desde el día en que supimos de tu existencia y que vamos a dar nuestro mejor esfuerzo para ser los padres que necesitas. Ojalá te sientas orgulloso de nosotros. Te amamos, mi pequeño Andrés.

A mis papás, Eloy Díaz Ramos y María Elisa López Soriano quiero darles las gracias por todo el apoyo que siempre me han dado. Durante toda mi vida siempre se han esforzado enormemente por darme las herramientas para salir adelante y ahora, durante el tiempo que cursé la maestría, continué recibiendo su apoyo incondicional en muchos aspectos. Este trabajo y el título de maestría que recibiré se los dedico como una muestra de agradecimiento por todo lo que han hecho por mí. Gracias por todo su amor. A mis hermanas Karla y Daniela quiero agradecerles por creer en mí y tenerme en tan buen concepto. Me motiva cada vez que me dicen que puedo lograr algo o que me admiran por conseguir algo que me propuse. Gracias por sus palabras de apoyo y gracias por ser mis eternas amigas. Espero que todos ustedes se sientan orgullosos de mí. Les agradezco también por compartir con nosotros esta

etapa de nuestras vidas. Los amo.

A mi mejor amiga, Arely Maldonado Azcona. Amiga, muchas gracias por todo lo bueno que tu amistad ha traído a mi vida. Te agradezco por todos esos momentos que pasamos en el ámbito académico y fuera de él. Gracias por seguir siendo mi amiga a pesar del tiempo y la distancia y gracias por vivir junto a mí esta etapa tan bonita de mi vida. Te quiero mucho.

A mi asesor, Dr. Carlos Alberto López Andrade, quiero darle las gracias por aceptarme nuevamente como su tesista. Gracias por motivarme a creer en mí y a ir más allá de lo que yo creo que puedo lograr. Gracias por el tiempo invertido a la dirección de mi tesis y a los cursos que nos impartió durante la maestría.

A mis sinodales, Dr. Iván Fernando Vilchis Montalvo, Dr. Carlos Guillén Galván y Dr. Henry Ricardo Chimal Dzul quiero agradecerles por el tiempo invertido a la revisión de mi trabajo, y especialmente quiero agradecer a la Dra. Sonia Navarro Flores por revisar mi trabajo y realizarme valiosas sugerencias, aun cuando le compartí el documento a una fecha muy cercana a la celebración del coloquio.

Finalmente quiero agradecer a CONAHCYT por el apoyo económico brindado, gracias al cual pude dedicarme de tiempo completo a mis estudios de maestría.

Índice general

Introducción x

1. Matroides 1

1.1. Conceptos básicos . . . 1

1.1.1. Conjuntos independientes . . . 1

1.1.2. Bases . . . 2

1.1.3. Circuitos . . . 3

1.1.4. Rango . . . 8

1.2. Isomorfismos de matroides . . . 10

1.3. Representación geométrica de un matroide . . . 12

1.4. Algunos matroides importantes . . . 17

1.4.1. Matroide de Fano . . . 17

1.4.2. Matroide de Vamos . . . 18

1.4.3. Matroides de Pappus . . . 19

1.5. Matroides de caminos reticulares . . . 23

1.5.1. Matroides transversales . . . 23

1.5.2. Matroides de caminos reticulares . . . 30

1.5.3. Un corolario de Bonin y de Mier que no se verifica . . . 41

2. Esquemas de compartición de secretos y matroides 43

2.1. Introducción . . . 43

2.2. Esquemas de compartición de secretos . . . 45

2.3. Esquemas de compartición de secretos ideales . . . 52

2.4. Esquemas de compartición de secretos ideales conexos . . . 53

2.5. Una casi-caracterización de esquemas ideales conexos mediante matroides . . . 60

3. Estructuras de acceso y matroides 67

3.1. Estructuras de acceso inducidas por matroides . . . 68

3.2. Estructura de acceso no ideal inducida por un matroide 72
3.3. Estructura de acceso ideal inducida por un matroide no representable 79
3.3.1. Códigos casi afines 79
3.3.2. El matroide de un código casi afín 81

4. Dos ejemplos de estructuras de acceso ideales **83**
4.1. Estructuras de acceso universalmente ideales 83
4.1.1. Esquemas lineales 84
4.1.2. Una caracterización de estructuras de acceso 2-ideales y 3-ideales mediante matroides representables 87
4.1.3. Una caracterización de estructuras de acceso universalmente ideales mediante matroides representables 91
4.2. Estructuras de acceso jerárquicas ideales 95
4.2.1. Una caracterización de estructuras de acceso jerárquicas ideales mediante matroides de caminos reticulares 97

Conclusiones **99**

Notación **103**

Referencias bibliográficas **105**

Índice Alfabético **105**

Índice de figuras

1.1. Representación geométrica de un matroide de rango 2 12
1.2. Elementos no permitidos en la representación geométrica de un matroide. . . 13
1.3. Simplificación de elementos en la representación geométrica de un matroide . 13
1.5. Representación geométrica de un matroide de rango 4. 16
1.6. Matroide de Fano F_7. 17
1.7. Matroide de Vamos $\mathcal{V}$. 18
1.8. Matroide de Pappus. 20
1.9. Matroide de non-Pappus. 20
1.10. Gráfica asociada a una familia de conjuntos 25
1.11. Emparejamientos en una gráfica 27
1.16. Caminos reticulares hacia $(6, 5)$. 31
1.17. Caminos reticulares hacia $(3, 2)$. 32
1.18. Presentación de caminos reticulares de un matroide. 34
1.19. Caminos reticulares asociados a distintos conjuntos. 35
1.20. Caminos reticulares asociados a bases. 37
1.21. Presentación de un matroide de caminos reticulares que no verifica un corolario de Bonin y de Mier 42
1.22. Presentación de un matroide de caminos reticulares que no verifica un corolario de Bonin y de Mier 42

3.4. Matroide de non-Pappus correspondiente a un código casi afín 82

Introducción

Un esquema de compartición de secretos perfecto con estructura de acceso Γ es un método que un distribuidor puede usar para repartir fragmentos de un secreto en privado a cada elemento de un conjunto de participantes P de manera que un subconjunto de P puede conocer el secreto si y sólo si el subconjunto pertenece a Γ. Los elementos de Γ se llaman conjuntos autorizados y si todo elemento de P pertenece a un conjunto autorizado minimal decimos que la estructura de acceso es conexa y que el esquema es conexo. Los esquemas ideales son aquellos en los cuales el conjunto de fragmentos para cada participante coincide con el conjunto de secretos. Una estructura de acceso Γ es ideal si existe un esquema de compartición de secretos ideal con estructura de acceso Γ. Las estructuras de acceso ideales son interesantes porque tienen los esquemas de compartición de secretos más eficientes [2].

La caracterización exacta de las estructuras de acceso ideales es un problema abierto desde hace ya algún tiempo, y para resolver este problema han entrado en juego conceptos de combinatoria y teoría de la información. El resultado más importante con miras hacia la anhelada caracterización fue dado por Brickell y Davenport [8], quienes probaron que una condición necesaria para que una estructura de acceso conexa sea ideal es que sea inducida por un matroide. Brickell y Davenport también presentaron una condición suficiente para que una estructura de acceso conexa sea ideal: si una estructura de acceso conexa es inducida por un matroide representable sobre un campo finito, entonces es ideal [8]. Desafortunadamente, la condición necesaria no es suficiente pues hay ejemplos de estructuras de acceso inducidas por matroides que no son ideales, como es el caso de las estructuras de acceso inducidas por el matroide de Vamos [22], el cual no es representable sobre ningún campo, y la condición suficiente no es necesaria ya que existen estructuras de acceso ideales cuyo matroide apropiado no es representable sobre ningún campo [24]. Por esta razón hablamos de la existencia de una casi-caracterización de estructuras de acceso ideales conexas mediante matroides. El estudio de esta casi-caracterización y de sus implicaciones es el objetivo principal de este trabajo.

En el Capítulo 1 presentamos los conceptos básicos de la teoría de matroides: conjuntos

independientes, bases, circuitos y rango, y las definiciones del concepto de matroide que surgen para cada uno de dichos conceptos. Definimos los conceptos de isomorfismo de matroides y de matroide representable, explicamos la construcción de la representación geométrica de un matroide y establecemos algunos resultados que nos permiten discernir aquellos diagramas que representan un matroide de aquellos que no. Estos criterios nos permiten definir algunos matroides importantes simplemente mostrando su representación geométrica. Así exponemos los matroides de Fano, Vamos, Pappus y non-Pappus y comentamos algunas de sus características y propiedades. También en este capítulo definimos los matroides transversales y estudiamos una subclase de estos: los matroides de caminos reticulares. Presentamos algunos de los principales resultados acerca de este tipo de matroides y mediante dos contraejemplos exhibimos que dos afirmaciones acerca de matroides de caminos reticulares de [5] no se verifican, lo cual tendrá repercusiones posteriores.

En el Capítulo 2 exponemos las definiciones fundamentales de la teoría de esquemas de compartición de secretos desde un punto de vista algebraico: abordamos conceptos tales como estructura de acceso, conjuntos autorizados, esquema de distribución y esquema de compartición de secretos. Para estos últimos se definen la condiciones de regularidad, privacidad débil y fuerte, y las nociones de esquemas perfectos, ideales y conexos. La parte más importante de este capítulo es el análisis a profundidad de [8], que es la piedra angular de la teoría de caracterización de estructuras de acceso ideales conexas mediante matroides.

En el Capítulo 3 construimos estructuras de acceso a partir de matroides, nos enfocamos en la estructura creada a partir del matroide de Vamos, que no es representable sobre ningún campo, y probamos que esta estructura no es ideal, con lo cual queda probado que la condición necesaria para que una estructura conexa sea ideal no es suficiente. También estudiamos a los códigos casi afines y la manera en la cual podemos definir un matroide a partir de ellos. Vemos que el matroide de non-Pappus, que no es representable sobre ningún campo, está asociado a un código casi afín que corresponde a un esquema de compartición de secretos ideal, con lo cual verificamos que la condición suficiente para que una estructura de acceso conexa sea ideal no es necesaria.

Finalmente, en el Capítulo 4 hablamos sobre dos tipos de estructuras de acceso: las estructuras de acceso universalmente ideales y las estructuras de acceso jerárquicas. En el primer caso veremos que la casi-caracterización previamente mencionada se convierte, de hecho, en una caracterización. En el segundo caso comentaremos algunos de los resultados presentados por Mo [20] acerca de estructuras de acceso jerárquicas ideales, que por los resultados que no se verifican de [5] no necesariamente son correctos.

A lo largo de este documento encontraremos algunas proposiciones cuyo encabezado

aparece subrayado. Esto indica que el autor citado únicamente enunció el resultado, pero no presentó su demostración o la presentó de manera incompleta y para cumplir con los objetivos de este trabajo nosotros elaboramos o completamos la prueba. Si presentamos alguna proposición junto con su demostración sin citar algún autor significa que tanto el enunciado de la proposición como su demostración fueron elaborados por nosotros.

Capítulo 1

Matroides

En este capítulo presentamos teoría básica de matroides que nos será útil en el desarrollo de este trabajo. Sugerimos al lector consultar especialmente [10], ya que en dicho trabajo se hace un análisis minucioso de la mayoría de los conceptos y teoremas mencionados a continuación, por esta razón, se enuncian sin demostración. También recomendamos consultar [14], [21] y [28] para un estudio más profundo de esta área de las matemáticas.

Establecemos la siguiente notación. Sean P un conjunto, $A \subseteq P$ y $x \in P$. Denotaremos al conjunto potencia de P con $\mathcal{P}(P)$, y en lo sucesivo, cuando no exista riesgo de confusión, escribiremos las operaciones con un conjunto unitario prescindiendo de las llaves. Por ejemplo, con $A \setminus x$ denotaremos al conjunto $A \setminus \{x\}$, y $A \cup \{x\}$ lo escribiremos como $A \cup x$.

1.1. Conceptos básicos

1.1.1. Conjuntos independientes

El concepto de matroide abstrae la noción de independencia que surge en diversas áreas de las matemáticas, tales como la independencia lineal de álgebra lineal o la independencia en teoría de gráficas. Una de las principales cualidades de la teoría de matroides es que podemos dar diferentes definiciones equivalentes del concepto de matroide. La definición que emplearemos más a menudo será la Definición 1.1.

Definición 1.1 ([14, Definición 2.1])**.** Un *matroide* $\mathcal{M}$ es un par ordenado $(E, \mathcal{I})$, donde E es un conjunto finito e $\mathcal{I}$ es una familia de subconjuntos de E que satisface las siguientes tres condiciones:

(I1) $\mathcal{I} \neq \emptyset$.

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

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

En este caso decimos que E es el *conjunto subyacente* de $\mathcal{M}$ y que $\mathcal{M}$ es un matroide *sobre* E. A los elementos de $\mathcal{I}$ los llamamos *conjuntos independientes* de $\mathcal{M}$ y a los subconjuntos de E que no pertenecen a $\mathcal{I}$ los llamamos *conjuntos dependientes*. Nos referimos a los elementos de E como *puntos* del matroide.

En lo sucesivo, en cualquiera de las definiciones alternativas que presentemos, asumiremos que los conceptos que permanecen sin cambios reciben el mismo nombre, tales como matroide *sobre* un conjunto E y *conjunto subyacente* de un matroide.

Existe una definición muy similar a la Definición 1.1, que parece decir esencialmente lo mismo, pero que en la práctica simplifica los cálculos. Esta definición proviene del siguiente teorema.

Teorema 1.2 ([14, Proposición 2.3]). *Sean E un conjunto finito e $\mathcal{I}$ una familia de subconjuntos de E. El par $\mathcal{M} = (E, \mathcal{I})$ es un matroide si y sólo si satisface las siguientes tres condiciones:*

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

1.1.2. Bases

Una manera eficiente de conocer los conjuntos independientes de un matroide es listando los conjuntos independientes maximales, ya que por (I2) todos sus subconjuntos son independientes y dado que estamos trabajando con conjuntos finitos, todo conjunto independiente está contenido en un conjunto independiente maximal. De ahí la importancia de definir el siguiente concepto.

Definición 1.3 ([14, Definición 2.4]). Sea $\mathcal{M} = (E, \mathcal{I})$ un matroide. Un subconjunto $B \subseteq E$ es una *base* del matroide $\mathcal{M}$ si B es un conjunto independiente maximal. Denotaremos a la familia de bases de $\mathcal{M}$ por $\mathcal{B}$.

En el Teorema 1.4 resumimos algunas de las propiedades que cumple la familia de bases de un matroide y explicamos cómo podemos construir un matroide a partir de una familia de conjuntos que cumple con las características para ser una familia de bases.

Teorema 1.4 ([14, Ejercicio 2.14], [10, Lema 2.1, Teoremas 2.2-2.5]). *La familia de bases $\mathcal{B}$ de un matroide $\mathcal{M}$ verifica las siguientes propiedades:*

(B1) $\mathcal{B} \neq \emptyset$.

(B2) *Si* $B_1, B_2 \in \mathcal{B}$ *y* $B_1 \subseteq B_2$, *entonces* $B_1 = B_2$.

(B2)* *Si* $B_1, B_2 \in \mathcal{B}$, *entonces* $|B_1| = |B_2|$.

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

Ahora, sean E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E que satisface las propiedades de alguno de los siguientes incisos:

i. *(B1), (B2) y (B3); o*

ii. *(B1), (B2*) y (B3).*

Si definimos el conjunto

$$\mathcal{I} = \{I \subseteq E \mid \exists B \in \mathcal{B} : I \subseteq B\},$$

entonces $\mathcal{M} = (E, \mathcal{I})$ es un matroide que tiene a $\mathcal{B}$ como su colección de bases.

El Teorema 1.4 justifica el establecimiento de la siguiente definición alternativa de matroide.

Definición 1.5 (Por bases). Un *matroide* $\mathcal{M}$ 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 propiedades (B1), (B2) y (B3). Los elementos de $\mathcal{B}$ se llaman *bases* de $\mathcal{M}$.

1.1.3. Circuitos

A continuación introducimos un nuevo término que, en cierto sentido, es el concepto dual de base. Nos referimos a aquellos conjuntos que son dependientes minimales.

Definición 1.6 ([14, Definición 2.9]). Sea $\mathcal{M} = (E, \mathcal{I})$ 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. Denotamos con $\mathcal{C}$ el conjunto de circuitos de $\mathcal{M}$. En símbolos:

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

Es importante enfatizar que, a diferencia de las bases, los circuitos de un matroide pueden tener diferente cardinalidad entre ellos. Además, si $\mathcal{M} = (E, \mathcal{I})$ es un matroide en el cual $\mathcal{I} = \mathcal{P}(E)$, entonces $\mathcal{C} = \emptyset$, a diferencia de su familia de bases $\mathcal{B}$, que siempre contiene al menos un elemento.

Teorema 1.7 ([10, Teoremas 2.6, 2.7]). *La colección de circuitos $\mathcal{C}$ de un matroide $\mathcal{M}$ verifica las siguientes propiedades:*

(C1) $\emptyset \notin \mathcal{C}$.

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

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

Ahora, sean E un conjunto y $\mathcal{C}$ una familia de subconjuntos de E que satisface (C1), (C2) y (C3). Si definimos

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

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

El Teorema 1.7 nos permite establecer otra definición de matroide.

Definición 1.8 (Por circuitos). Un *matroide* $\mathcal{M}$ 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 condiciones (C1), (C2) y (C3). Los elementos de $\mathcal{C}$ se llaman *circuitos* de $\mathcal{M}$.

La condición (C3) señala que si tenemos dos circuitos distintos y un elemento en su intersección, siempre podemos hallar un circuito contenido en la unión de los primeros dos circuitos quitándole el elemento en común. El Teorema 1.9 nos aporta un resultado más potente que denotaremos por (C3*).

Teorema 1.9 ([28, Teorema 1.9.2]). *Sea $\mathcal{M}$ un matroide con familia de circuitos $\mathcal{C}$.*

(C3) Si C_1 y C_2 son dos circuitos de $\mathcal{M}$ distintos y $x \in C_1 \cap C_2$, entonces para todo $y \in (C_1 \setminus C_2) \cup (C_2 \setminus C_1)$ existe un circuito C_y tal que $y \in C_y \subseteq (C_1 \cup C_2) \setminus x$.*

Demostración.

Supongamos que (C3*) no se verifica. Sean C_1 y C_2 dos circuitos distintos, $x \in C_1 \cap C_2$ y $y \in (C_1 \setminus C_2) \cup (C_2 \setminus C_1)$ tal que ningún circuito C satisface que $y \in C \subseteq (C_1 \cup C_2) \setminus x$, y tal que $|C_1 \cup C_2|$ es minimal. Supongamos que $y \in C_1 \setminus C_2$ (el caso en el que $y \in C_2 \setminus C_1$

se desarrolla de manera análoga). Por (C3) existe un circuito $C_3 \subseteq (C_1 \cup C_2) \setminus x$, pero por hipótesis $y \notin C_3$. Si $C_3 \cap (C_2 \setminus C_1) = \emptyset$, entonces $C_3 \subseteq C_1 \setminus x \subsetneq C_1$, lo cual no puede ocurrir ya que C_1 es un conjunto dependiente minimal, así que $C_3 \cap (C_2 \setminus C_1) \neq \emptyset$ y podemos elegir $z \in C_3 \cap (C_2 \setminus C_1)$, en particular $z \in C_2 \cap C_3$. Además, $x \in C_2 \setminus C_3$, por lo que C_2 y C_3 son circuitos distintos, y como $C_3 \subseteq C_1 \cup C_2$ y $C_2 \subseteq C_1 \cup C_2$, tenemos que $C_2 \cup C_3 \subseteq C_1 \cup C_2$, y dado que $y \in C_1 \cup C_2$ pero $y \notin C_2 \cup C_3$, entonces $C_2 \cup C_3 \subsetneq C_1 \cup C_2$. Por la minimalidad de $|C_1 \cup C_2|$ existe un circuito C_4 tal que $x \in C_4 \subseteq (C_2 \cup C_3) \setminus z$. Ahora consideremos los circuitos C_1 y C_4; $x \in C_1 \cap C_4$, $y \notin C_2 \cup C_3$, luego, $y \notin C_4$, así que $y \in C_1 \setminus C_4$, de donde $C_1 \neq C_4$. Además, dado que $z \in C_3$ y $z \notin C_1 \cup C_4$, tenemos que

$$C_1 \cup C_4 \subsetneq C_1 \cup (C_2 \cup C_3) = (C_1 \cup C_2) \cup C_3 \subseteq (C_1 \cup C_2) \cup (C_1 \cup C_2) = C_1 \cup C_2$$

entonces $C_1 \cup C_4 \subsetneq C_1 \cup C_2$. Empleando nuevamente la minimalidad de $|C_1 \cup C_2|$, existe $C_5 \in \mathcal{C}$ tal que $y \in C_5 \subseteq (C_1 \cup C_4) \setminus x$, y como $C_1 \cup C_4 \subsetneq C_1 \cup C_2$, C_5 es un circuito de $\mathcal{M}$ tal que $y \in C_5 \subseteq (C_1 \cup C_2) \setminus x$, pero esto contradice lo supuesto. Entonces la conclusión del teorema debe ser verdadera. □

Sea $\mathcal{M}$ un matroide sobre un conjunto E y sean x, y y z tres puntos distintos de E. Supongamos que existe un circuito que contiene a x y a y, y uno que contiene a y y a z. Demostraremos que existe un circuito que contiene a los elementos x y z. Primero vamos a definir la restricción de un matroide. Posteriormente, dado que realizaremos la prueba por inducción, vamos a probar el caso base, para lo cual necesitamos conocer todos los matroides que pueden construirse con 3 elementos.

Consideremos un matroide $\mathcal{M} = (E, \mathcal{I})$ y T un subconjunto de E. Estamos interesados en lo que sucede cuando restringimos el estudio de $\mathcal{M}$ a T, es decir, a los conjuntos independientes de $\mathcal{M}$ que además son subconjuntos de T. Para ello definimos la familia $\mathcal{I}(\mathcal{M}|_T) = \{I \subseteq T : I \in \mathcal{I}\}$. Podemos verificar fácilmente que el par $(T, \mathcal{I}(\mathcal{M}|_T))$ es un matroide, lo llamamos la *restricción* de $\mathcal{M}$ a T, y lo denotamos por $\mathcal{M}|_T$.

Las propiedades que se enuncian en el siguiente teorema son consecuencia inmediata de la definición de restricción de un matroide.

Teorema 1.10 ([21]). *Sean $\mathcal{M} = (E, \mathcal{I})$ un matroide y $T \subseteq E$. En el matroide $\mathcal{M}|_T$ se verifican las siguientes propiedades:*

I. X es un conjunto dependiente en $\mathcal{M}|_T$ si y sólo si $X \subseteq T$ y X es dependiente en $\mathcal{M}$.

II. Los circuitos de $\mathcal{M}|_T$ son los circuitos de $\mathcal{M}$ que están contenidos en T.

Ahora, sea $E = \{x, y, z\}$. Podemos verificar que las siguientes familias de subconjuntos de E son las únicas que satisfacen las propiedades (I1), (I2) e (I3). Escribimos también sus

respectivas familias de circuitos:

$$\mathcal{I}_1 = \{\emptyset\}, \mathcal{C}_1 = \{\{x\},\{y\},\{z\}\}$$
$$\mathcal{I}_2 = \{\emptyset,\{x\}\}, \mathcal{C}_2 = \{\{y\},\{z\}\}$$
$$\mathcal{I}_3 = \{\emptyset,\{y\}\}, \mathcal{C}_3 = \{\{x\},\{z\}\}$$
$$\mathcal{I}_4 = \{\emptyset,\{z\}\}, \mathcal{C}_4 = \{\{x\},\{y\}\}$$
$$\mathcal{I}_5 = \{\emptyset,\{x\},\{y\}\}, \mathcal{C}_5 = \{\{z\},\{x,y\}\}$$
$$\mathcal{I}_6 = \{\emptyset,\{x\},\{z\}\}, \mathcal{C}_6 = \{\{y\},\{x,z\}\}$$
$$\mathcal{I}_7 = \{\emptyset,\{y\},\{z\}\}, \mathcal{C}_7 = \{\{x\},\{y,z\}\}$$
$$\mathcal{I}_8 = \{\emptyset,\{x\},\{y\},\{x,y\}\}, \mathcal{C}_8 = \{\{z\}\}$$
$$\mathcal{I}_9 = \{\emptyset,\{x\},\{z\},\{x,z\}\}, \mathcal{C}_9 = \{\{y\}\}$$
$$\mathcal{I}_{10} = \{\emptyset,\{y\},\{z\},\{y,z\}\}, \mathcal{C}_{10} = \{\{x\}\}$$
$$\mathcal{I}_{11} = \{\emptyset,\{x\},\{y\},\{z\}\}, \mathcal{C}_{11} = \{\{x,y\},\{x,z\},\{y,z\}\}$$
$$\mathcal{I}_{12} = \{\emptyset,\{x\},\{y\},\{z\},\{x,y\},\{x,z\}\}, \mathcal{C}_{12} = \{\{y,z\}\}$$
$$\mathcal{I}_{13} = \{\emptyset,\{x\},\{y\},\{z\},\{x,y\},\{y,z\}\}, \mathcal{C}_{13} = \{\{x,z\}\}$$
$$\mathcal{I}_{14} = \{\emptyset,\{x\},\{y\},\{z\},\{x,z\},\{y,z\}\}, \mathcal{C}_{14} = \{\{x,y\}\}$$
$$\mathcal{I}_{15} = \{\emptyset,\{x\},\{y\},\{z\},\{x,y\},\{x,z\},\{y,z\}\}, \mathcal{C}_{15} = \{\{x,y,z\}\}$$
$$\mathcal{I}_{16} = \{\emptyset,\{x\},\{y\},\{z\},\{x,y\},\{x,z\},\{y,z\},\{x,y,z\}\}, \mathcal{C}_{16} = \emptyset \tag{1.1}$$

Entonces existen 16 matroides sobre el conjunto E de cardinalidad 3. Así que, si $\mathcal{M} = (E,\mathcal{C})$ es un matroide tal que existe un circuito $C_{x,y}$ que contiene a $\{x,y\}$ y existe un circuito $C_{y,z}$ que contiene a $\{y,z\}$, entonces necesariamente $\mathcal{C} = \mathcal{C}_{11}$ o $\mathcal{C} = \mathcal{C}_{15}$, y en ambos casos existe un circuito $C_{x,z}$ tal que $\{x,z\} \subseteq C_{x,z}$.

Teorema 1.11 ([28, Teorema 5.1.2]). *Sea $\mathcal{M} = (E,\mathcal{I})$ un matroide y sean $x, y, z \in E$ distintos. Si existe un circuito $C_{x,y}$ tal que $x, y \in C_{x,y}$, y un circuito $C_{y,z}$ tal que $y, z \in C_{y,z}$, entonces existe un circuito $C_{x,z}$ que verifica que $x, z \in C_{x,z}$.*

Demostración.

Realizaremos esta demostración por inducción sobre $|E|$, con $|E| \geq 3$. Si $|E| = 3$, entonces por lo mostrado anteriormente la conclusión del teorema se verifica. Supongamos que existe $n \in \mathbb{N}$, $n \geq 3$ tal que el resultado se verifica para todos los matroides sobre conjuntos de cardinalidad mayor o igual a 3 y menor o igual a n. Sea $\mathcal{M} = (E,\mathcal{I})$ un matroide tal que $|E| = n+1$, y sean x, y y z puntos distintos de E. Supongamos que existen dos circuitos $C_{x,y}$ y $C_{y,z}$ tales que $x, y \in C_{x,y}$ y $y, z \in C_{y,z}$. Si $C_{x,y} = C_{y,z}$, entonces tomando $C_{x,z} = C_{x,y}$ se

verifica la conclusión del teorema. Supongamos ahora que $C_{x,y} \neq C_{y,z}$ y que $E \neq C_{x,y} \cup C_{y,z}$. Sea $u \in E \setminus (C_{x,y} \cup C_{y,z})$ y sea $T = E \setminus u$. T es un subconjunto de E de cardinalidad n que contiene a los conjuntos $\{x, y, z\}$, $C_{x,y}$ y $C_{y,z}$. Por hipótesis de inducción existe un circuito $C_{x,z}$ de $\mathcal{M}|_T$ tal que $x, z \in C_{x,z}$, más aún, $C_{x,z}$ es un circuito de $\mathcal{M}$ y verifica la conclusión del teorema. Ahora supongamos que $E = C_{x,y} \cup C_{y,z}$. Si $x \in C_{y,z}$, entonces basta tomar $C_{x,z} = C_{y,z}$, mientras que si $z \in C_{x,y}$, conviene establecer $C_{x,z} = C_{x,y}$. Supongamos que $x \in C_{x,y} \setminus C_{y,z}$ y $z \in C_{y,z} \setminus C_{x,y}$. Como $C_{x,y} \neq C_{y,z}$, por el Teorema 1.9, existen dos circuitos C_x y C_z tales que

$$\begin{aligned} x \in C_x \subseteq (C_{x,y} \cup C_{y,z}) \setminus y \\ z \in C_z \subseteq (C_{x,y} \cup C_{y,z}) \setminus y \end{aligned} \tag{1.2}$$

Si $C_x \cap (C_{y,z} \setminus C_{x,y}) = \emptyset$, entonces $C_x \subseteq C_{x,y} \setminus y$, de donde $C_x \subsetneq C_{x,y}$, lo cual no puede ocurrir ya que por ser $C_{x,y}$ un circuito, todos sus subconjuntos propios son independientes, entonces $C_x \cap (C_{y,z} \setminus C_{x,y}) \neq \emptyset$. Supongamos que $C_{x,y} \setminus C_{y,z} \nsubseteq C_x$, entonces $C_x \cup C_{y,z} \subsetneq C_{x,y} \cup C_{y,z} = E$, por lo que $|C_x \cup C_{y,z}| < |C_{x,y} \cup C_{y,z}| = |E|$. Tenemos que $x \in C_x$, $z \in C_{y,z}$ y $C_x \cap C_{y,z} \neq \emptyset$, así que existe $u \in E$ tal que $x, u \in C_x$ y $u, z \in C_{y,z}$, con $|C_x \cup C_{y,z}| < |E|$. Por hipótesis de inducción, existe un circuito C de $\mathcal{M}|_{C_x \cup C_{y,z}}$ al que pertenecen x y z, en particular C es un circuito de $\mathcal{M}$ que cumple con la conclusión del teorema. Si suponemos que $C_{y,z} \setminus C_{x,y} \nsubseteq C_z$, empleando un razonamiento análogo al anterior también obtenemos que existe un circuito C de $\mathcal{M}$ al que pertenecen x y z. Ahora supongamos que $C_{x,y} \setminus C_{y,z} \subseteq C_x$ y $C_{y,z} \setminus C_{x,y} \subseteq C_z$. Por (1.2), $C_x \cup C_z \subseteq (C_{x,y} \cup C_{y,z}) \setminus y = E \setminus y$. Puesto que $C_x \cap (C_{y,z} \setminus C_{x,y}) \neq \emptyset$, y $C_{y,z} \setminus C_{x,y} \subseteq C_z$, entonces $C_x \cap C_z \neq \emptyset$, así que existe $v \in E \setminus y$ tal que $x, v \in C_x$ y $v, z \in C_z$, luego, por la hipótesis de inducción existe un circuito C de $\mathcal{M}|_{E \setminus y}$ tal que $x, z \in C$, más aún C es un circuito de $\mathcal{M}$ que verifica la conclusión del teorema. Por lo tanto, el resultado es válido para cualquier matroide de cardinalidad $n \geq 3$. □

En el desarrollo de este texto, frecuentemente necesitaremos la propiedad de que dados dos puntos cualesquiera de un matroide podemos encontrar un circuito al que pertenecen ambos puntos. De la lista en (1.1), vemos que esto no siempre es así. Por ejemplo, el matroide con familia de conjuntos independientes $\mathcal{I}_1$ no contiene circuitos de cardinalidad mayor o igual a 2. En cambio, el matroide correspondiente a la familia $\mathcal{I}_{11}$ y el correspondiente a $\mathcal{I}_{15}$ sí tienen esta propiedad. Este tipo de matroides se definen a continuación.

Definición 1.12 ([14, Definición 3.42])**.** Sea $\mathcal{M}$ un matroide. Si dados dos puntos distintos de $\mathcal{M}$ existe un circuito que los contiene, diremos que $\mathcal{M}$ es *conexo*.

1.1.4. Rango

Definición 1.13 ([14, Definición 2.12]). Sean $\mathcal{M} = (E, \mathcal{I})$ un matroide y $A \subseteq E$. El *rango* de A es la mayor de las cardinalidades de los conjuntos independientes que están contenidos en A y se denota por $\text{rank}(A)$, es decir,

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

El valor $\text{rank}(E)$ se llama el *rango del matroide* $\mathcal{M}$ y se denota por $\text{rank}(\mathcal{M})$.

Nos referimos a la *función rango* de un matroide a la inducida por el propio concepto, es decir, a la función de valor entero no negativo definida de la siguiente forma:

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

Teorema 1.14 ([10, Teoremas 2.8-2.12]). *Sea $\mathcal{M} = (E, \mathcal{I})$ un matroide. La función rango* rank *de $\mathcal{M}$ satisface las siguientes propiedades para cualesquiera $A, B \subseteq E$:*

(r1) $0 \leq \text{rank}(A) \leq |A|$.

(r1)* $\text{rank}(\emptyset) = 0$.

(r2) Si $A \subseteq B$, entonces $\text{rank}(A) \leq \text{rank}(B)$.

(r2) Para todo $x \in E$ se tiene que* $\text{rank}(A) \leq \text{rank}(A \cup x) \leq \text{rank}(A) + 1$.

(r3) $\text{rank}(A \cup B) + \text{rank}(A \cap B) \leq \text{rank}(A) + \text{rank}(B)$.

(r3) Para cualesquiera $x, y \in E \setminus A$, si* $\text{rank}(A \cup x) = \text{rank}(A) = \text{rank}(A \cup y)$, *entonces* $\text{rank}(A \cup \{x, y\}) = \text{rank}(A)$.

Ahora, sean E un conjunto finito y rank *una función de valor entero con dominio $\mathcal{P}(E)$ que satisface las propiedades de alguno de los siguientes incisos:*

i. (r1), (r2) y (r3); o

ii. (r1), (r2*) y (r3*).*

Definamos la familia

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

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

Gracias al Teorema 1.14, podemos establecer una definición más del concepto de matroide.

Definición 1.15 (Por función rango)**.** Un *matroide* $\mathcal{M}$ es un par ordenado (E, rank) donde E es un conjunto finito y rank es una función de valor entero con dominio $\mathcal{P}(E)$ que cumple las propiedades (r1), (r2) y (r3). La función rank se conoce como la *función rango* de $\mathcal{M}$.

A continuación mostramos dos ejemplos muy sencillos de matroides, pero confiamos que ayuden a tener una mejor comprensión de los conceptos que se han abordado hasta el momento.

Ejemplo 1.16. Este es uno de los ejemplos que motivaron la definición de matroide. Sean V un espacio vectorial sobre un campo $\mathbb{F}$ y E un subconjunto finito de V. Definimos $\mathcal{I}$ como la colección de subconjuntos de E que son linealmente independientes sobre $\mathbb{F}$. El par $\mathcal{M} = (E, \mathcal{I})$ es un matroide y lo llamamos *matroide vector*. Una base de $\mathcal{M}$ es un conjunto de vectores de E linealmente independiente maximal, es decir, una base para el generado de E. Si el generado de E es igual al espacio vectorial V, entonces una base para $\mathcal{M}$ es una base para V. Los circuitos de $\mathcal{M}$ son conjuntos de vectores linealmente dependientes, cuyos subconjuntos propios son todos linealmente independientes. El rango de un conjunto $A \subseteq E$ es el mayor número de vectores linealmente independientes que pertenecen a A.

Ejemplo 1.17. Sean n y k enteros no negativos tales que $k \leq n$. Sea E un conjunto de cardinalidad n. Tomemos $\mathcal{I}$ como la familia de todos los subconjuntos de E que tienen cardinalidad menor o igual a k. $\mathcal{M} = (E, \mathcal{I})$ es un matroide y lo llamamos el *matroide uniforme de rango k sobre un conjunto de n elementos* y lo denotamos por $U_{k,n}$. En este caso, la familia de bases $\mathcal{B}$ es la colección de todos los subconjuntos de E de cardinalidad k, y la familia de circuitos $\mathcal{C}$ es la colección de subconjuntos de E de cardinalidad $k+1$. Sea $A \subseteq E$: si $|A| \leq k$, entonces $A \in \mathcal{I}$, por lo que $\text{rank}(A) = |A|$; si $|A| > k$, entonces A contiene a un subconjunto de cardinalidad k, por lo que $\text{rank}(A) = k$. En resumen, $\text{rank}(A) = \text{mín}\{k, |A|\}$.

Para finalizar este apartado presentamos un par de resultados sencillos pero muy útiles. El resultado que se presenta a continuación lo emplearemos con frecuencia a lo largo del texto, ya que nos da una caracterización de los circuitos de un matroide a partir de una propiedad de su función rango.

Teorema 1.18 ([21, Proposición 1.3.5(iii)])**.** *Sea $\mathcal{M} = (E, \mathcal{C})$ un matroide. $X \subseteq E$ es un circuito de $\mathcal{M}$ si y sólo si $X \neq \emptyset$ y para todo $x \in X$, $\text{rank}(X \setminus x) = |X| - 1 = \text{rank}(X)$.*

Demostración.

Si X es un circuito de $\mathcal{M}$, entonces $X \neq \emptyset$ y todos sus subconjuntos propios son conjuntos independientes, en particular para todo $x \in X$, $X \setminus x \in \mathcal{I}$, por lo que $\text{rank}(X \setminus x) = |X \setminus x| = |X| - 1$. Además, $\text{rank}(X) = |X| - 1$, ya que los subconjuntos independientes de X de mayor

cardinalidad son justamente los conjuntos de la forma $X \setminus x$, con $x \in X$. Por lo tanto, $\text{rank}(X \setminus x) = |X| - 1 = \text{rank}(X)$. Ahora, sea $X \subseteq E$ no vacío tal que para todo $x \in X$, $\text{rank}(X \setminus x) = |X| - 1 = \text{rank}(X)$, entonces el conjunto X es dependiente, pues su rango no coincide con su cardinalidad, mientras que para todo $x \in X$ el conjunto $X \setminus x$ es independiente, de aquí que todos los subconjuntos propios de X son independientes, por lo tanto, X es un circuito de $\mathcal{M}$. □

El siguiente teorema afirma que si el rango de un conjunto B cambia cuando le agregamos el elemento x y A es un subconjunto de B, entonces el rango de A también cambia cuando le agregamos el elemento x.

Teorema 1.19 ([14, Ejercicio 24(a)]). *Sea $\mathcal{M}$ un matroide sobre E y sean $A, B \subseteq E$ y $x \in E$ tales que $A \subseteq B$ y $\text{rank}(B \cup x) = \text{rank}(B) + 1$. Entonces $\text{rank}(A \cup x) = \text{rank}(A) + 1$.*

Demostración.

Dado que $\text{rank}(B \cup x) = \text{rank}(B) + 1$ sabemos que $x \notin B$ y por consiguiente, $x \notin A$. Como $(A \cup x) \cup B = B \cup x$ y $(A \cup x) \cap B = A$, por la propiedad (r3) tenemos que $\text{rank}(B \cup x) + \text{rank}(A) \leq \text{rank}(A \cup x) + \text{rank}(B)$, y puesto que $\text{rank}(B \cup x) = \text{rank}(B) + 1$, obtenemos que $\text{rank}(B) + 1 + \text{rank}(A) \leq \text{rank}(A \cup x) + \text{rank}(B)$, de donde $\text{rank}(A \cup x) \geq \text{rank}(A) + 1$, y por (r2*) sabemos que $\text{rank}(A \cup x) \leq \text{rank}(A) + 1$, por lo tanto, $\text{rank}(A \cup x) = \text{rank}(A) + 1$. □

1.2. Isomorfismos de matroides

Cuando estudiamos funciones entre dos matroides, cobran especial importancia aquellas que preservan la independencia de los subconjuntos. Por ello establecemos la siguiente definición.

Definición 1.20 ([21]). Sean $\mathcal{M}_1 = (E_1, \mathcal{I}_1)$ y $\mathcal{M}_2 = (E_2, \mathcal{I}_2)$ matroides. Una función $\phi : E_1 \to E_2$ es un *isomorfismo de matroides* si es una función biyectiva y si para todo $X \subseteq E_1$, el conjunto $\phi(X)$ es independiente en $\mathcal{M}_2$ si y sólo si X es independiente en $\mathcal{M}_1$. Si existe un isomorfismo de matroides entre $\mathcal{M}_1$ y $\mathcal{M}_2$, decimos que $\mathcal{M}_1$ y $\mathcal{M}_2$ son *isomorfos* y lo denotamos por $\mathcal{M}_1 \cong \mathcal{M}_2$.

Un resultado muy conocido en teoría de matroides que nos permite establecer una conexión con muchas otras áreas es que a partir de una matriz con entradas en un campo podemos construir un matroide. La manera en la que esto se logra se especifica en el siguiente teorema. Con $[n]$ denotaremos al conjunto de los naturales menores o iguales a n, es decir, $[n] = \{1, 2, \ldots, n\}$.

Teorema 1.21 ([10, Teorema 2.13]). *Sea G una matriz de tamaño $k \times n$ sobre un campo $\mathbb{F}$, cuyas columnas están etiquetadas por los elementos del conjunto $E_G = [n]$ (en orden ascendente), y sea $\mathcal{I}_G$ la familia de subconjuntos I de E_G para los cuales el multiconjunto 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.*

Definición 1.22 ([21]). El matroide que se obtiene como en el Teorema 1.21 a partir de una matriz G se denota por $\mathcal{M}[G]$ y se llama el *matroide vector* de G.

A continuación mostramos un ejemplo de construcción de un matroide vector a partir de una matriz, analizando la dependencia lineal entre sus vectores columna; mencionamos la lista de sus bases y circuitos, y especificamos su rango.

Ejemplo 1.23 ([21, Ejemplo 1.1.2]). Definimos la matriz G de la siguiente forma:

$$G = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

sobre el campo de los números reales. Si tomamos E_G e $\mathcal{I}_G$ como en el Teorema 1.21, 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 $\mathcal{M}[G]$ es $\mathcal{B} = \{\{1,2\}, \{1,5\}, \{2,4\}, \{2,5\}, \{4,5\}\}$; la familia de conjuntos dependientes de este matroide es $\{\{3\}, \{1,3\}, \{1,4\}, \{2,3\}, \{3,4\}, \{3,5\}\} \cup \{X \subseteq E : |X| \geq 3\}$ y su familia de circuitos es $\{\{3\}, \{1,4\}, \{1,2,5\}, \{2,4,5\}\}$. Notemos que $\mathcal{M}[G]$ es un matroide de rango 2.

Más adelante se apreciará la importancia de aquellos matroides que pueden verse como el matroide vector de una matriz con entradas en un campo mediante un isomorfismo. Este es el tipo de matroide que definimos a continuación.

Definición 1.24 ([21]). Sea $\mathcal{M}$ un matroide. Decimos que $\mathcal{M}$ es *representable sobre el campo* $\mathbb{F}$ si existe una matriz G con entradas en $\mathbb{F}$ tal que $\mathcal{M}$ es isomorfo al matroide $\mathcal{M}[G]$. G se llama *representación* para $\mathcal{M}$ sobre $\mathbb{F}$ o $\mathbb{F}-$*representación* para $\mathcal{M}$. Un matroide es *representable* si tiene una representación sobre algún campo.

Claramente un matroide vector es un matroide representable. Por esta razón, un matroide vector también recibe el nombre de *matroide representable*.

1.3. Representación geométrica de un matroide

Definición 1.25 ([21]). Sea $\mathcal{M}$ un matroide sobre un conjunto E. Si $e \in E$ es tal que el conjunto unitario $\{e\}$ es un circuito de $\mathcal{M}$, decimos que e es un *bucle* de $\mathcal{M}$. Si f y g son elementos de E tales que $\{f, g\}$ es un circuito, decimos que f y g son *paralelos* en $\mathcal{M}$. Una *clase paralela* de $\mathcal{M}$ es un subconjunto maximal X de E tal que cualesquiera dos elementos distintos de X son paralelos y ningún elemento de X es un bucle. Una clase paralela es *trivial* si contiene un único elemento. Si $\mathcal{M}$ no tiene bucles y no contiene clases paralelas no triviales se llama *matroide simple*.

En muchas ocasiones es útil representar un matroide mediante un diagrama, como en el siguiente ejemplo.

Ejemplo 1.26 ([21, Ejemplo 1.5.4]). Consideremos el matroide vector $\mathcal{M}[G]$ de rango 2 del Ejemplo 1.23. El diagrama de la Figura 1.1 representa al matroide $\mathcal{M}[G]$ si consideramos que la nube indicada con el número 3 corresponde al bucle 3, que los puntos 1 y 4 corresponden al circuito $\{1, 4\}$ y que los circuitos $\{1, 2, 5\}$ y $\{2, 4, 5\}$ se representan con una recta con 3 puntos.

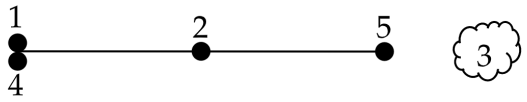


Figura 1.1: Diagrama del matroide $M[G]$ del Ejemplo 1.23.

De manera general, podemos representar cualquier matroide $\mathcal{M}$ de rango menor o igual a 4 mediante un diagrama de puntos, líneas y planos, cumpliendo con las siguientes reglas:

- El diagrama se elabora en $\mathbb{R}^{\text{rank}(\mathcal{M})-1}$, es decir, si $\mathcal{M}$ es de rango 4 el diagrama se elabora en el espacio; si es de rango 3, en el plano; si es de rango 2, en una recta.
- Las líneas y los planos pueden ser curvos.
- Toda línea contiene al menos dos puntos.
- Representamos un bucle con una figura cerrada como en la Figura 1.1, donde el bucle 3 se representó con una nube. Un conjunto unitario independiente se representa por un punto.
- Si $\text{rank}(\mathcal{M}) \geq 2$, los elementos paralelos de $\mathcal{M}$ se representan con dos puntos que se colocan en la misma posición o con un punto que tiene dos etiquetas distintas. Más

aún, si X es una clase paralela de $\mathcal{M}$, representamos a X con un único punto que tiene como etiquetas a todos los elementos de X. Un conjunto independiente de cardinalidad 2 se representa con dos puntos en distinta posición que pueden estar o no unidos por una recta.

- Si $\text{rank}(\mathcal{M}) \geq 3$, un circuito de cardinalidad 3 se representa mediante tres puntos en una misma línea. Un conjunto independiente de cardinalidad 3 se representa con tres puntos que no pertenecen a una misma línea.
- Si $\text{rank}(\mathcal{M}) = 4$, los circuitos de cardinalidad 4 se representan con 4 puntos coplanares.

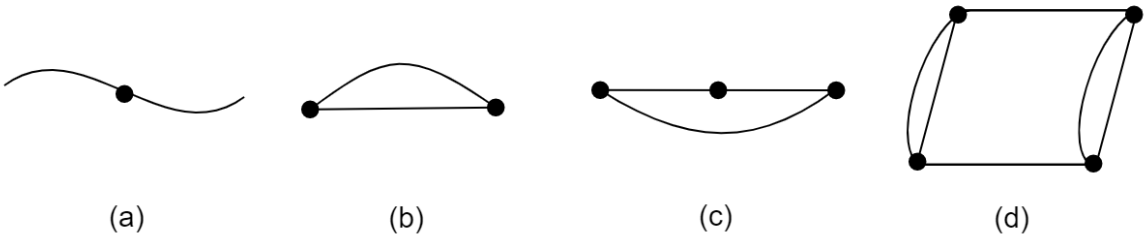


Figura 1.2: Elementos no permitidos en la representación geométrica de un matroide.

- En general, el diagrama debe ser lo más simple posible. No es útil dibujar una línea que pase por un único punto, o dos líneas o planos que pasen por los mismos puntos. En la Figura 1.2 se muestran elementos de diagramas de matroides que pueden presentarse de manera más simple. Por ejemplo, en la Figura 1.2(c) no tiene sentido dibujar la línea que une dos de los tres puntos, es suficiente dibujar los tres puntos separados y la línea a la que pertenecen los 3 puntos. Una forma simplificada de estos elementos se muestra en la Figura 1.3.

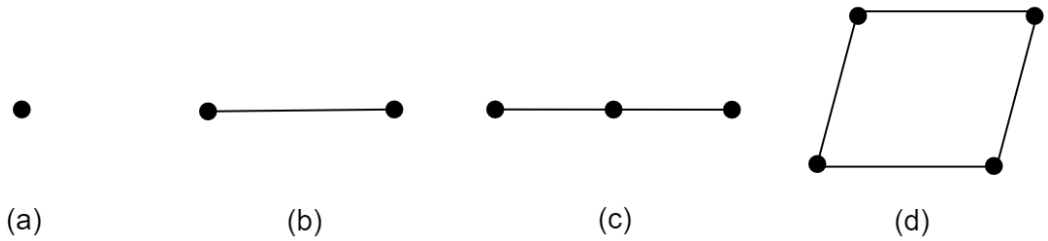


Figura 1.3: Simplificación de los diagramas de la Figura 1.2.

A veces para simplificar el diagrama ciertas líneas y planos se mencionan en lugar de dibujarse, y otras veces ciertas líneas con menos de tres puntos se dibujan para tener una visualización más clara del diagrama.

Al diagrama que se construye a partir de un matroide siguiendo las reglas anteriores lo llamamos la *representación geométrica* del matroide $\mathcal{M}$. Esta representación es de gran utilidad ya que nos permite estudiar el matroide $\mathcal{M}$ de una manera más simple. De hecho, muchos matroides se dan a conocer por su representación geométrica. En sentido estricto deberíamos llamarla *una* representación geométrica porque podemos tener diferentes representaciones geométricas para un matroide, pero por simplicidad nos referiremos a ella como si fuera única.

Hemos visto que para todo matroide de rango a lo más 4 podemos construir su representación geométrica. Ahora nos preguntamos si cualquier diagrama de puntos, líneas y planos es la representación geométrica de un matroide. Podemos reducir este análisis a los matroides simples, pues ahora ya sabemos cómo representar bucles y clases paralelas. En el siguiente teorema, establecemos condiciones necesarias y suficientes para asegurar que un diagrama de puntos y líneas en el plano representa un matroide.

Teorema 1.27 ([21]). *Un diagrama con un número finito de puntos y líneas (posiblemente curvas) en el plano es la representación geométrica de un matroide simple de rango menor o igual a 3 si y sólo si verifica las siguientes condiciones:*

I. *No existen conjuntos de puntos en la misma posición.*

II. *Toda línea contiene al menos dos puntos.*

III. *Todo par de líneas distintas se intersectan en a lo más un punto.*

Demostración.

Supongamos que un diagrama con un número finito de puntos y líneas en el plano es la representación geométrica de un matroide simple, entonces claramente se verifican las condiciones I y II. Supongamos que existe un par de líneas distintas l_1 y l_2 que se intersectan en dos puntos distintos, digamos a y b. Como l_1 y l_2 son líneas distintas, entonces existen dos puntos distintos entre sí c y d tales que c incide con l_1, d incide con l_2, y $c, d \notin \{a, b\}$, como en la Figura 1.4. Entonces los conjuntos $\{a, b\}$ y $\{b, c, d\}$ son independientes. Luego, por

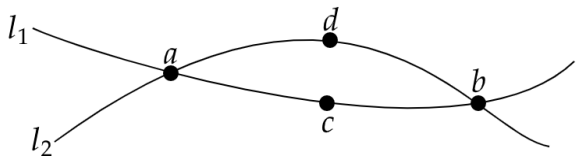


Figura 1.4: Dos líneas distintas con dos puntos de intersección.

la propiedad (I3) existe $x \in \{b, c, d\} \setminus \{a, b\} = \{c, d\}$ tal que $\{a, b\} \cup x$ es independiente,

pero $\{a, b, c\}$ y $\{a, b, d\}$ son conjuntos de puntos colineales, entonces ambos son circuitos, lo cual contradice (I3). Por lo tanto, III se verifica. Ahora, supongamos que tenemos un diagrama con un número finito de puntos y líneas en el plano que verifica las propiedades I, II y III. Denotemos el conjunto de puntos con E. Sea $\mathcal{I}$ la familia formada por los subconjuntos de E de cardinalidad menor o igual a 2 y los conjuntos de tres puntos de E que no pertenecen a una misma línea. Veamos que el par $\mathcal{M} = (E, \mathcal{I})$ es un matroide empleando el Teorema 1.2. Por construcción, la propiedad (J1) se verifica. Sean $I \in \mathcal{I}$ y $J \subsetneq I$. Dado que $|I| \leq 3$, tenemos que $|J| \leq 2$, por lo que $J \in \mathcal{I}$, así que se cumple (J2). Ahora, sean $I, J \in \mathcal{I}$ tales que $|I| = |J| + 1$. Si $|J| \leq 1$ y x es cualquier elemento de $I \setminus J$, entonces $|J \cup x| \leq 2$, por lo que $J \cup x \in \mathcal{I}$. Supongamos que existen dos conjuntos $J = \{a, b\}$ e $I = \{c, d, e\}$ tales que ningún $x \in I \setminus J$ satisface que $J \cup x \in \mathcal{I}$, entonces para todo $x \in I \setminus J$ los puntos a, b y x pertenecen a una misma línea. Sean l_1 la línea incidente con a, b y c; l_2 la línea que pasa por a, b y d; l_3 la línea que contiene a a, b y e. Por III las líneas l_1, l_2 y l_3 no pueden ser distintas entre sí, ya que se intersectan en los puntos a y b, luego, l_1, l_2 y l_3 son iguales, de donde los puntos c, d y e pertenecen a una misma línea, lo cual contradice que $I \in \mathcal{I}$. Así que, para todo par de conjuntos $I, J \in \mathcal{I}$ tales que $|J| = 2$ y $|I| = 3$ existe $x \in I \setminus J$ tal que $J \cup x \in \mathcal{I}$, y por lo tanto, (J3) se verifica. Concluimos que $\mathcal{M} = (E, \mathcal{I})$ es un matroide de rango menor o igual a 3, y dado que no tiene bucles ni clases paralelas, $\mathcal{M}$ es simple. □

En la demostración del Teorema 1.27 vimos cómo construir la familia de conjuntos independientes $\mathcal{I}$ de un matroide simple $\mathcal{M}$ a partir de su representación geométrica en el plano. Las modificaciones que debemos considerar para la representación geométrica de un matroide no-simple son las siguientes:

I. Todo elemento en una nube (o alguna figura cerrada) representa un bucle.

II. Dos puntos colocados en la misma posición representan dos puntos paralelos.

III. Los conjuntos que contengan un bucle o un par de puntos paralelos son dependientes.

El siguiente teorema presenta condiciones necesarias y suficientes para que un diagrama con puntos, líneas y planos en el espacio sea la representación geométrica de un matroide simple.

Teorema 1.28 ([19, p. 18],[21]). *Un diagrama con un número finito de puntos, líneas y planos en el espacio es la representación geométrica de un matroide simple de rango menor o igual a 4 si y sólo si se verifican las siguientes condiciones:*

I. *No existen conjuntos de puntos en la misma posición.*

II. *Toda línea contiene al menos dos puntos.*

III. *Todo plano contiene al menos tres puntos que no pertenecen a la misma línea.*

IV. *Si existen dos planos distintos que se intersectan en más de dos puntos, se intersectan en una línea.*

V. *Si dos líneas distintas se intersectan lo hacen en a lo más un punto y pertenecen a un mismo plano.*

VI. *Si una recta no pertenece a un plano, la recta intersecta a dicho plano en a lo más un punto.*

A partir de un diagrama de puntos, líneas y planos en el espacio que verifica las hipótesis del Teorema 1.28 podemos determinar los conjuntos independientes del matroide simple correspondiente considerando los conjuntos independientes dados por la demostración del Teorema 1.27 agregando que un conjunto de 4 puntos es independiente si y sólo si los 4 puntos no pertenecen a un mismo plano. Para un matroide no-simple seguimos las mismas indicaciones adicionales que se establecieron para una representación geométrica en el plano. En el Ejemplo 1.29 seguimos estas reglas para conocer los conjuntos dependientes e independientes de un matroide a partir de su representación geométrica en el espacio.

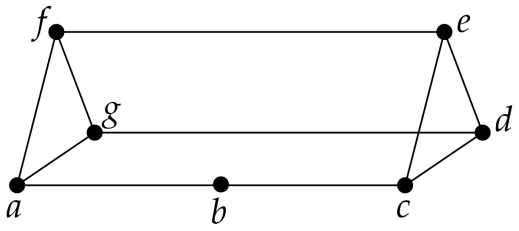


Figura 1.5: Representación geométrica de un matroide de rango 4.

Ejemplo 1.29 ([14, Ejemplo 1.11])**.** Consideremos el diagrama de puntos, líneas y planos de la Figura 1.5. Podemos comprobar sin dificultad que este diagrama verifica las hipótesis del Teorema 1.28, por lo tanto, la Figura 1.5 es la representación geométrica de un matroide simple $\mathcal{M}$ sobre el conjunto $E = \{a, b, c, d, e, f, g\}$ en el cual todos los conjuntos de cardinalidad menor o igual a 3 son independientes excepto $\{a, b, c\}$ y los conjuntos dependientes de cardinalidad 4 son $\{a, b, c, d\}$, $\{a, b, c, e\}$, $\{a, b, c, f\}$, $\{a, b, c, g\}$, $\{a, b, d, g\}$, $\{a, b, e, f\}$, $\{a, c, d, g\}$, $\{a, c, e, f\}$, $\{b, c, d, g\}$, $\{b, c, e, f\}$, $\{d, e, f, g\}$, y de estos conjuntos dependientes, aquellos que no contengan al circuito $\{a, b, c\}$ son, además, circuitos.

Es importante señalar que aunque la representación geométrica de un matroide muestra algunos circuitos, estos no necesariamente son los únicos circuitos del matroide. Pueden existir circuitos de mayor cardinalidad que no se aprecian en la representación, como es el caso del matroide de Vamos, que se estudiará en la Sección 1.4.2. El rango de este matroide es 4, por lo que su representación geométrica requiere de tres dimensiones y en ella se aprecian los circuitos de cardinalidad 4, pero no son los únicos: en (1.4) se presenta una lista completa de sus circuitos de cardinalidad 5.

Los Teoremas 1.27 y 1.28 son herramientas muy útiles para construir matroides empleando únicamente puntos, líneas y planos; además, nos permiten decidir si una figura de este tipo representa a un matroide sin tener que verificar algún conjunto de propiedades dado en la Sección 1.1. Particularmente en la Sección 1.4 se podrá apreciar el valor de estos resultados.

1.4. Algunos matroides importantes

1.4.1. Matroide de Fano

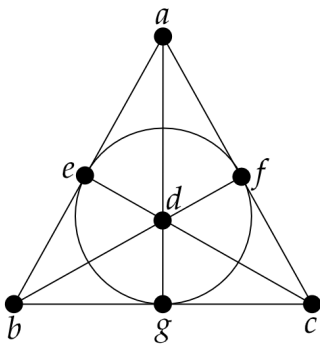


Figura 1.6: Matroide de Fano F_7.

El diagrama de la figura 1.6 verifica las condiciones del Teorema 1.27, así que es la representación geométrica de un matroide simple sobre el conjunto $E = \{a, b, c, d, e, f, g\}$. A este matroide lo llamamos el *matroide* o *plano de Fano* y lo denotamos por F_7. Los conjuntos independientes de F_7 son todos los conjuntos de cardinalidad menor o igual a 3 a excepción de los conjuntos de 3 puntos colineales de la Figura 1.6, es decir, los 7 conjuntos $\{a, b, e\}$, $\{a, c, f\}$, $\{a, d, g\}$, $\{b, c, g\}$, $\{b, d, f\}$, $\{c, d, e\}$ y $\{e, f, g\}$. Los circuitos de F_7 son los conjuntos dependientes de cardinalidad tres junto con los conjuntos $\{a, b, c, d\}$, $\{a, b, f, g\}$, $\{a, c, e, g\}$, $\{a, d, e, f\}$, $\{b, c, e, f\}$, $\{b, d, e, g\}$, $\{c, d, f, g\}$. Todos los subconjuntos de E de cardinalidad mayor o igual a 4 son dependientes. Notemos que F_7 es conexo. La representación geométrica del matroide de Fano consta de líneas rectas a excepción de

la línea que une los puntos e, f y g. Nos preguntamos si existe otra representación de F_7 en la cual todas las líneas sean rectas. En la representación geométrica de F_7 de la Figura 1.6 toda línea que une dos de sus puntos contiene un tercer punto y esta propiedad debe conservarse en cualquier otra representación. Sin embargo, se demuestra que si tenemos un conjunto E de $n > 2$ puntos en el plano tales que toda línea recta que une dos puntos de E contiene otro punto de E, entonces todos los puntos de E son colineales ([14], p. 37). Así que la manera en la que evitamos que todos los puntos pertenezcan a una misma recta es dibujando una de las líneas del diagrama de manera curva.

La siguiente proposición nos habla acerca de la representabilidad del matroide de Fano.

Proposición 1.30 ([14, Proposición 6.16]). *El plano de Fano F_7 es representable sobre un campo $\mathbb{F}$ si y sólo si la característica de $\mathbb{F}$ es 2.*

1.4.2. Matroide de Vamos

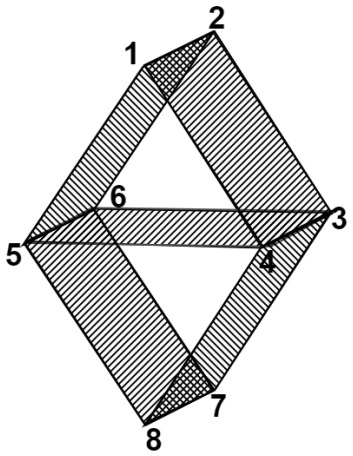


Figura 1.7: Matroide de Vamos $\mathcal{V}$.

Consideremos el diagrama de la Figura 1.7, donde las regiones sombreadas representan planos (aunque visualmente así lo parezca, los puntos 1, 2, 7 y 8 no son coplanares). Por el Teorema 1.28, existe un matroide sobre el conjunto $E = [8]$ cuya familia de bases $\mathcal{B}$ está formada por todos los subconjuntos de E de cardinalidad 4, excepto los siguientes 5 conjuntos:

$$\{1,2,3,4\}, \{1,2,5,6\}, \{3,4,5,6\}, \{3,4,7,8\}, \{5,6,7,8\}. \tag{1.3}$$

Denotamos por $\mathcal{V}$ al matroide $(E, \mathcal{B})$ y lo llamamos *matroide de Vamos*. Fue nombrado en honor al matemático húngaro Peter Vámos quien lo presentó en el artículo no publicado [27] como el primer ejemplo de un matroide de rango 4 sobre un conjunto de 8 elementos que

no es representable sobre ningún campo. Frecuentemente la representación geométrica del matroide de Vamos se da mediante un cubo con una cara transversal y por esta razón también se le conoce como el *cubo de Vamos*.

Los circuitos de $\mathcal{V}$ son los 5 conjuntos de (1.3) junto con los siguientes conjuntos de cardinalidad 5:

$$\begin{array}{l}\{1,2,3,5,7\},\{1,2,3,5,8\},\{1,2,3,6,7\},\{1,2,3,6,8\},\{1,2,3,7,8\},\{1,2,4,5,7\},\\ \{1,2,4,5,8\},\{1,2,4,6,7\},\{1,2,4,6,8\},\{1,2,4,7,8\},\{1,2,5,7,8\},\{1,2,6,7,8\},\\ \{1,3,4,5,7\},\{1,3,4,5,8\},\{1,3,4,6,7\},\{1,3,4,6,8\},\{1,3,5,6,7\},\{1,3,5,6,8\},\\ \{1,3,5,7,8\},\{1,3,6,7,8\},\{1,4,5,6,7\},\{1,4,5,6,8\},\{1,4,5,7,8\},\{1,4,6,7,8\},\\ \{2,3,4,5,7\},\{2,3,4,5,8\},\{2,3,4,6,7\},\{2,3,4,6,8\},\{2,3,5,6,7\},\{2,3,5,6,8\},\\ \{2,3,5,7,8\},\{2,3,6,7,8\},\{2,4,5,6,7\},\{2,4,5,6,8\},\{2,4,5,7,8\},\{2,4,6,7,8\}.\end{array} \tag{1.4}$$

$\mathcal{V}$ es un matroide conexo. Se demuestra que todos los matroides que tienen menos de ocho elementos son representables [21, Proposición 6.4.10]. Por lo tanto, el matroide de Vamos es uno de los matroides conocidos más pequeños que no son representables sobre ningún campo.

1.4.3. Matroides de Pappus

Si x y y son dos puntos distintos del plano, denotamos con $\overline{xy}$ a la recta que determinan los puntos x y y. Sea $\{a,b,c,d,e,f\}$ un conjunto de puntos distintos en el plano, tales que a,b,c son incidentes en la recta $\overline{ab}$, y d,e,f son incidentes en la recta $\overline{de}$, donde $\overline{ab}$ y $\overline{de}$ son rectas distintas. Sea g el punto de intersección de las rectas $\overline{ae}$ y $\overline{bd}$, h el punto de intersección de $\overline{af}$ y $\overline{cd}$, e i el punto de intersección de $\overline{bf}$ y $\overline{ce}$. El Teorema de Pappus establece que los puntos g, h, e i son colineales, como puede apreciarse en la Figura 1.8, y fue establecido por Pappus de Alejandría (290-350 d. C.). Por el Teorema 1.27 podemos afirmar que la Figura 1.8 es la representación geométrica de un matroide simple $\mathcal{M}_1$ de rango 3 con conjunto subyacente $E=\{a,b,c,d,e,f,g,h,i\}$ y circuitos de cardinalidad 3 los conjuntos de tres puntos colineales. A $\mathcal{M}_1$ lo llamamos el *matroide de Pappus*.

Ahora consideremos un diagrama con conjunto de puntos E y con las mismas rectas que en la Figura 1.8, excepto la recta que une a los puntos g, h e i, como el de la Figura 1.9. Por el Teorema 1.27, dicho diagrama es la representación geométrica de un matroide que denotamos por $\mathcal{M}_2$ y lo llamamos *matroide de non-Pappus*.

El Teorema de Pappus muestra que el matroide $\mathcal{M}_1$ es $\mathbb{R}$-representable [15], y el matroide $\mathcal{M}_2$ no lo es. De hecho, $\mathcal{M}_2$ no es representable sobre ningún campo.

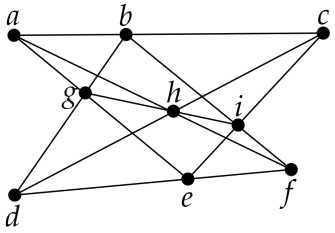


Figura 1.8: Matroide de Pappus.

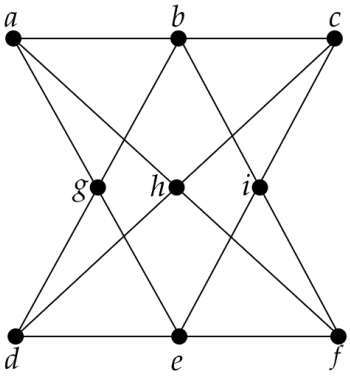


Figura 1.9: Matroide de non-Pappus.

Teorema 1.31 ([14, Teorema 6.21]). *El matroide de non-Pappus no es representable sobre ningún campo.*

Finalizamos esta sección con el planteamiento de un teorema cuya importancia se verá más adelante. Este teorema establece que si $\mathcal{M}$ es un matroide conexo y e es cualquier punto de $\mathcal{M}$, entonces para conocer los circuitos de $\mathcal{M}$ es suficiente listar a aquellos circuitos que contienen a e, ya que con ciertas operaciones conjuntistas entre estos circuitos generaremos a los circuitos restantes.

Teorema 1.32 ([28, Teorema 5.4.1]). *Sean $\mathcal{M} = (E, \mathcal{C})$ un matroide conexo y $e \in E$. Denotemos con $\mathcal{C}_e$ a la familia de circuitos de $\mathcal{M}$ que contienen al punto e. Para $C_1, C_2 \in \mathcal{C}_e$ definimos*

$$\begin{aligned} J_e(C_1, C_2) &= \bigcap \{C \in \mathcal{C}_e : C \subseteq C_1 \cup C_2\}; \\ D_e(C_1, C_2) &= (C_1 \cup C_2) \setminus J_e(C_1, C_2). \end{aligned} \tag{1.5}$$

Entonces todos los circuitos de $\mathcal{M}$ que no contienen al punto e son los conjuntos minimales de la forma $D_e(C_1, C_2)$, con $C_1, C_2 \in \mathcal{C}_e$, $C_1 \neq C_2$.

Ejemplo 1.33. Sea $\mathcal{M}$ el matroide del Ejemplo 1.29, el cual podemos verificar fácilmente que

es conexo. Definimos:

$$C_1 = \{a, b, e, f\},\ C_2 = \{a, c, e, f\},\ C_3 = \{b, c, e, f\},\ C_4 = \{d, e, f, g\}$$
$$C_5 = \{a, b, d, g\},\ C_6 = \{a, c, d, g\},\ C_7 = \{b, c, d, g\},\ C_8 = \{a, b, c\}$$

Entonces $\mathcal{C}_e = \{C_1, C_2, C_3, C_4\}$. Tenemos lo siguiente:

$$J_e(C_1, C_2) = \bigcap\{C \in \mathcal{C}_e : C \subseteq \{a, b, c, e, f\}\} = \bigcap\{C_1, C_2, C_3\} = \{e, f\};$$
$$D_e(C_1, C_2) = \{a, b, c, e, f\} \setminus \{e, f\} = \{a, b, c\} = C_8.$$
$$J_e(C_1, C_4) = \bigcap\{C \in \mathcal{C}_e : C \subseteq \{a, b, d, e, f, g\}\} = \bigcap\{C_1, C_4\} = \{e, f\};$$
$$D_e(C_1, C_4) = \{a, b, d, e, f, g\} \setminus \{e, f\} = \{a, b, d, g\} = C_5.$$
$$J_e(C_2, C_4) = \bigcap\{C \in \mathcal{C}_e : C \subseteq \{a, c, d, e, f, g\}\} = \bigcap\{C_2, C_4\} = \{e, f\};$$
$$D_e(C_2, C_4) = \{a, c, d, e, f, g\} \setminus \{e, f\} = \{a, c, d, g\} = C_6.$$
$$J_e(C_3, C_4) = \bigcap\{C \in \mathcal{C}_e : C \subseteq \{b, c, d, e, f, g\}\} = \bigcap\{C_3, C_4\} = \{e, f\};$$
$$D_e(C_3, C_4) = \{b, c, d, e, f, g\} \setminus \{e, f\} = \{b, c, d, g\} = C_7.$$

Hemos verificado que, en efecto, a partir de operaciones conjuntistas entre los circuitos de $\mathcal{M}$ que contienen a e podemos obtener los circuitos que no contienen al punto e. Omitimos algunos cálculos que repetían alguno de los resultados ya obtenidos. Por ejemplo, $D_e(C_1, C_3) = C_8$. De lo anterior podemos concluir que no existe una única manera de construir a los circuitos que no contienen al punto e.

Ejemplo 1.34. Consideremos el matroide de Fano F_7. Definimos:

$$C_1 = \{a, b, e\},\ C_2 = \{a, c, f\},\ C_3 = \{a, d, g\},\ C_4 = \{a, b, c, d\},\ C_5 = \{a, b, f, g\}$$
$$C_6 = \{a, c, e, g\},\ C_7 = \{a, d, e, f\},\ C_8 = \{c, d, e\},\ C_9 = \{b, d, f\},\ C_{10} = \{e, f, g\}$$
$$C_{11} = \{b, c, g\},\ C_{12} = \{b, c, e, f\},\ C_{13} = \{b, d, e, g\},\ C_{14} = \{c, d, f, g\}$$

A continuación enlistamos los conjuntos que podemos formar mediante (1.5) con los elementos de la familia $\mathcal{C}_a = \{C_i : i \in [7]\}$. Omitimos aquellos cálculos que generan algún elemento que ya se había obtenido a partir de otros conjuntos.

$$J_a(C_1, C_2) = \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a, b, c, e, f\}\} = \bigcap\{\{a, b, e\}, \{a, c, f\}\} = \{a\};$$
$$D_a(C_1, C_2) = \{a, b, c, e, f\} \setminus \{a\} = \{b, c, e, f\} = C_{12}$$
$$J_a(C_1, C_3) = \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a, b, d, e, g\}\} = \bigcap\{\{a, b, e\}, \{a, d, g\}\} = \{a\};$$
$$D_a(C_1, C_3) = \{a, b, d, e, g\} \setminus \{a\} = \{b, d, e, g\} = C_{13}$$
$$J_a(C_1, C_4) = \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a, b, c, d, e\}\} = \bigcap\{\{a, b, e\}, \{a, b, c, d\}\} = \{a, b\};$$
$$D_a(C_1, C_4) = \{a, b, c, d, e\} \setminus \{a, b\} = \{c, d, e\} = C_8$$

$$
\begin{aligned}
J_a(C_1, C_5) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,e,f,g\}\} = \bigcap\{\{a,b,e\},\{a,b,f,g\}\} \\
&= \{a,b\}; \\
D_a(C_1, C_5) &= \{a,b,e,f,g\} \setminus \{a,b\} = \{e,f,g\} = C_{10} \\
J_a(C_1, C_6) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,c,e,g\}\} = \bigcap\{\{a,b,e\},\{a,c,e,g\}\} \\
&= \{a,e\}; \\
D_a(C_1, C_6) &= \{a,b,c,e,g\} \setminus \{a,e\} = \{b,c,g\} = C_{11} \\
J_a(C_1, C_7) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,d,e,f\} = \bigcap\{\{a,b,e\},\{a,d,e,f\}\} \\
&= \{a,e\}; \\
D_a(C_1, C_7) &= \{a,b,d,e,f\} \setminus \{a,e\} = \{b,d,f\} = C_9 \\
J_a(C_2, C_3) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,c,d,f,g\}\} = \bigcap\{\{a,c,f\},\{a,d,g\}\} \\
&= \{a\}; \\
D_a(C_2, C_3) &= \{a,c,d,f,g\} \setminus \{a\} = \{c,d,f,g\} = C_{14} \\
J_a(C_4, C_5) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,c,d,f,g\}\} \\
&= \bigcap\{\{a,c,f\},\{a,d,g\},\{a,b,c,d\},\{a,b,f,g\}\} = \{a\}; \\
D_a(C_4, C_5) &= \{a,b,c,d,f,g\} \setminus \{a\} = \{b,c,d,f,g\} \\
J_a(C_4, C_6) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,c,d,e,g\}\} \\
&= \bigcap\{\{a,b,e\},\{a,d,g\},\{a,b,c,d\},\{a,c,e,g\}\} = \{a\}; \\
D_a(C_4, C_6) &= \{a,b,c,d,e,g\} \setminus \{a\} = \{b,c,d,e,g\} \\
J_a(C_4, C_7) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,c,d,e,f\}\} \\
&= \bigcap\{\{a,b,e\},\{a,c,f\},\{a,b,c,d\},\{a,d,e,f\}\} = \{a\}; \\
D_a(C_4, C_7) &= \{a,b,c,d,e,f\} \setminus \{a\} = \{b,c,d,e,f\} \\
J_a(C_5, C_6) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,c,e,f,g\}\} \\
&= \bigcap\{\{a,b,e\},\{a,c,f\},\{a,b,f,g\},\{a,c,e,g\}\} = \{a\}; \\
D_a(C_5, C_6) &= \{a,b,c,e,f,g\} \setminus \{a\} = \{b,c,e,f,g\} \\
J_a(C_5, C_7) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,b,d,e,f,g\}\} \\
&= \bigcap\{\{a,b,e\},\{a,d,g\},\{a,b,f,g\},\{a,d,e,f\}\} = \{a\}; \\
D_a(C_5, C_7) &= \{a,b,d,e,f,g\} \setminus \{a\} = \{b,d,e,f,g\} \\
J_a(C_6, C_7) &= \bigcap\{C \in \mathcal{C}_a : C \subseteq \{a,c,d,e,f,g\}\}
\end{aligned}
$$

$$= \bigcap \{\{a, c, f\}, \{a, d, g\}, \{a, c, e, g\}, \{a, d, e, f\}\} = \{a\};$$
$$D_a(C_6, C_7) = \{a, c, d, e, f, g\} \setminus \{a\} = \{c, d, e, f, g\}$$

Como podemos apreciar, hemos obtenido todos los circuitos que no contienen al punto a partiendo de los circuitos de $\mathcal{C}_a$, pero también hemos obtenido conjuntos adicionales, todos ellos de cardinalidad 5, que no son minimales, pues contienen un circuito de cardinalidad 3, así que no los tomamos en cuenta, ya que el Teorema 1.32 nos dice que sólo debemos considerar los conjuntos minimales de la forma $D_a(C, C')$, con $C, C' \in \mathcal{C}_a$, $C \neq C'$.

1.5. Matroides de caminos reticulares

La teoría de matroides fue creada en la década de los treinta del siglo XX, pero el interés en ella aumentó de forma significativa en 1965 cuando Edmonds y Fulkerson [12] probaron un importante teorema que relaciona la teoría de transversales con la teoría de matroides [28]. Específicamente demostraron que la familia de transversales parciales de una familia finita de conjuntos es la familia de conjuntos independientes de un matroide. Un matroide creado de esta forma se llama *matroide transversal*.

Los matroides de caminos reticulares fueron introducidos por Bonin, de Mier y Noy en [6], como un tipo de matroides transversales. En esta sección revisamos los conceptos y resultados que involucran esta clase de matroides y que nos serán útiles en el Capítulo 4. El contenido expuesto está basado principalmente en [5] y [6]. Recomendamos al lector consultar estas fuentes para un estudio más profundo de los matroides de caminos reticulares.

1.5.1. Matroides transversales

Definición 1.35 ([6])**.** Sean E un conjunto finito y $\mathcal{A} = \{A_i \subseteq E : i \in [m]\}$ un multiconjunto de subconjuntos de E. Una *transversal* de $\mathcal{A}$ es un subconjunto $\{x_1, \ldots, x_m\} \subseteq E$ tal que para todo $i \in [m]$, $x_i \in A_i$ y todos los elementos de este subconjunto son distintos. Decimos que $X \subseteq E$ es una *transversal parcial* de $\mathcal{A}$ si X es una transversal de $\{A_i : i \in K\}$, con $K \subseteq [m]$.

En otras palabras, un subconjunto $X \subseteq E$ es una transversal de $\mathcal{A}$ si tiene cardinalidad m y cada uno de sus elementos es un representante de exactamente uno de los conjuntos de $\mathcal{A}$, es decir, lo que necesitamos para formar una transversal de $\mathcal{A}$ es un conjunto $X \subseteq E$ tal que podemos establecer una función biyectiva entre X y $\mathcal{A}$. Una transversal de $\mathcal{A}$ también

recibe el nombre de *sistema de distintos representantes* para $\mathcal{A}$. Notemos que la Definición 1.35 no pide que los conjuntos de la familia $\mathcal{A}$ sean disjuntos entre sí, entonces pueden existir elementos que pertenecen a más de un conjunto de $\mathcal{A}$.

Ejemplo 1.36. Sea $E = [6]$, y sean $A_1 = \{1,3,4,6\}$, $A_2 = \{1,2,3,6\}$, $A_3 = \{4,5,6\}$, $\mathcal{A} = \{A_1, A_2, A_3\}$. El conjunto $\{1,2,4\}$ es una transversal de $\mathcal{A}$, ya que $1 \in A_1$, $2 \in A_2$ y $4 \in A_3$. Notemos que, aunque $1 \in A_1 \cap A_2$, al momento de formar la transversal asignamos al elemento 1 un único conjunto para representar. El conjunto $\{3,4\}$ no es una transversal de $\mathcal{A}$, pues su cardinalidad es menor que 3, pero sí es una transversal parcial de $\mathcal{A}$, ya que $3 \in A_1$ y $4 \in A_3$.

Podríamos pensar que cualquier familia de subconjuntos de un conjunto tiene una transversal, pero esto no es así, como podemos ver en el siguiente ejemplo.

Ejemplo 1.37. Sea $E = \{1,2\}$. Definimos los conjuntos $A_1 = \{1\}$, $A_2 = \{2\}$ y $A_3 = \{1,2\}$ y sea $\mathcal{A} = \{A_1, A_2, A_3\}$. Rápidamente podemos verificar que ningún subconjunto de E puede ser una transversal de $\mathcal{A}$, pues el único representante de A_1 es 1, el único representante de A_2 es 2 y necesitaríamos de un elemento adicional que represente a A_3. Sin embargo, no podemos elegir un representante de A_3 distinto del representante de A_1 y del representante de A_2, por lo que no podemos completar una transversal de $\mathcal{A}$.

Un problema fundamental en la teoría de transversales fue encontrar condiciones para que una familia de conjuntos tenga una transversal. Este problema fue resuelto por Philip Hall en 1935. En lo sucesivo frecuentemente denotaremos a la familia $\mathcal{A} = \{A_i \subseteq E : i \in [m]\}$ como $\mathcal{A} = (A_1, \ldots, A_m)$ o $\mathcal{A} = (A_i : i \in [m])$, como se aprecia en el enunciado del siguiente teorema.

Teorema 1.38 ([28, Teorema 7.1.1])**.** *La familia finita de subconjuntos* $(A_i : i \in [m])$ *tiene una transversal si y sólo si para todo* $K \subseteq [m]$,

$$\left|\bigcup(A_k : k \in K)\right| \geq |K|.$$

La familia del Ejemplo 1.37 no cumple con la condición necesaria del Teorema 1.38, pues $\left|\bigcup(A_k : k \in [3])\right| = |\{1,2\}| = 2 < 3 = |[3]|$. Por lo tanto, no podemos encontrar una transversal de la familia $\mathcal{A}$, como ya habíamos concluido anteriormente. Sin embargo, sí podemos encontrar transversales parciales de esta familia.

Otra forma de ver transversales parciales es mediante emparejamientos en una gráfica bipartita. Para ello asociaremos una gráfica bipartita a cada familia de conjuntos de la manera descrita en [21], la cual explicamos a continuación. Si $\mathcal{A}$ es una familia $(A_1, \ldots, A_m)$

de subconjuntos de un conjunto E, entonces la *gráfica bipartita* $\Delta[\mathcal{A}]$ *asociada con* $\mathcal{A}$ tiene conjunto de vértices $E \cup [m]$ y su conjunto de aristas es $\{\{u, j\} : u \in E, j \in [m] \text{ y } u \in A_j\}$, es decir, una arista en $\Delta[\mathcal{A}]$ está formada por un punto de E y uno de los subíndices de los conjuntos a los cuales pertenece dicho punto. Un *emparejamiento* en una gráfica G es un conjunto de aristas en la gráfica tal que ningún par de aristas tiene un punto final en común. Si $X \subseteq E$ es una transversal parcial de $\mathcal{A}$, entonces existe $K \subseteq [m]$ tal que $X = \{x_k : k \in K\}$, donde para cada $k \in K$, $x_k \in A_k$, y todos los elementos de X son distintos. Entonces existe un conjunto de aristas de la gráfica bipartita asociada $\Delta[\mathcal{A}]$ que tienen un punto final en X y que forman un emparejamiento en $\Delta[\mathcal{A}]$, pues cada punto de X tiene asociado uno y sólo un conjunto de la familia $\mathcal{A}$, y además, no existen dos elementos de X que representen simultáneamente al mismo conjunto. Ahora, si un conjunto de aristas de la gráfica bipartita asociada $\Delta[\mathcal{A}]$ que tienen un punto final en X forman un emparejamiento en $\Delta[\mathcal{A}]$, entonces existe una función biyectiva entre los puntos de X y una subfamilia de $\mathcal{A}$. Con esto hemos demostrado que un subconjunto X de E es una transversal parcial de $\mathcal{A}$ si y sólo si existe un emparejamiento en $\Delta[\mathcal{A}]$ donde cada arista tiene un punto final en X.

Ejemplo 1.39. Sean $E = \{v_i : i \in [10]\}$, $A_1 = \{v_1, v_3, v_{10}\}$, $A_2 = \{v_2, v_5\}$, $A_3 = \{v_1, v_3, v_7\}$, $A_4 = \{v_4, v_6, v_9\}$, $A_5 = \{v_1, v_7, v_8\}$, $A_6 = \{v_2, v_9, v_{10}\}$. Para la familia $\mathcal{A} = \{A_i : i \in [6]\}$ su gráfica bipartita asociada $\Delta[\mathcal{A}]$ es la que se muestra en la Figura 1.10. Los conjuntos $\{\{v_1, 1\}, \{v_3, 3\}, \{v_5, 2\}, \{v_6, 4\}, \{v_8, 5\}, \{v_{10}, 6\}\}$ y $\{\{v_2, 2\}, \{v_4, 4\}, \{v_9, 6\}\}$ son ejemplos de emparejamientos de $\Delta[\mathcal{A}]$.

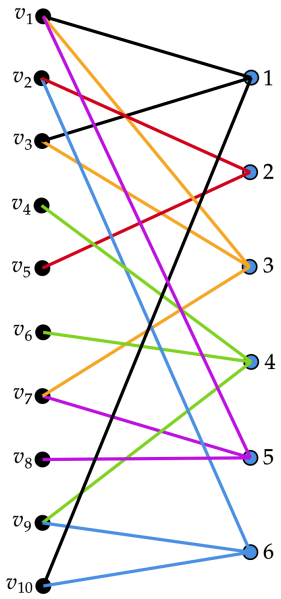


Figura 1.10: Gráfica bipartita $\Delta[\mathcal{A}]$.

A continuación presentamos uno de los teoremas más importantes de este capítulo. Como ya lo mencionamos anteriormente, la familia de transversales parciales de un multiconjunto de subconjuntos de un conjunto E es la familia de conjuntos independientes de un matroide sobre E. Para su demostración requerimos de dos resultados conocidos en teoría de gráficas, los cuales se enuncian a continuación.

Lema 1.40 ([21, Ejercicio]). *Sea G una gráfica. Si todo vértice de G tiene grado a lo más 2, entonces G es una unión disjunta de caminos simples y ciclos.*

Lema 1.41 ([11, Proposición 1.6.1]). *Una gráfica es bipartita si y sólo si no contiene ciclos impares.*

Recordemos que una *componente conexa* de una gráfica G es una subgráfica inducida de G en la que cualesquiera dos vértices están conectados mediante un camino.

Teorema 1.42 ([28, Teorema 7.3.1]). *Sean E un conjunto finito y $\mathcal{A} = (A_1, \ldots, A_m)$ una familia de subconjuntos de E. Sea $\mathcal{I}$ la familia de transversales parciales de $\mathcal{A}$. Entonces $\mathcal{I}$ es la familia de conjuntos independientes de un matroide $\mathcal{M}$ sobre E.*

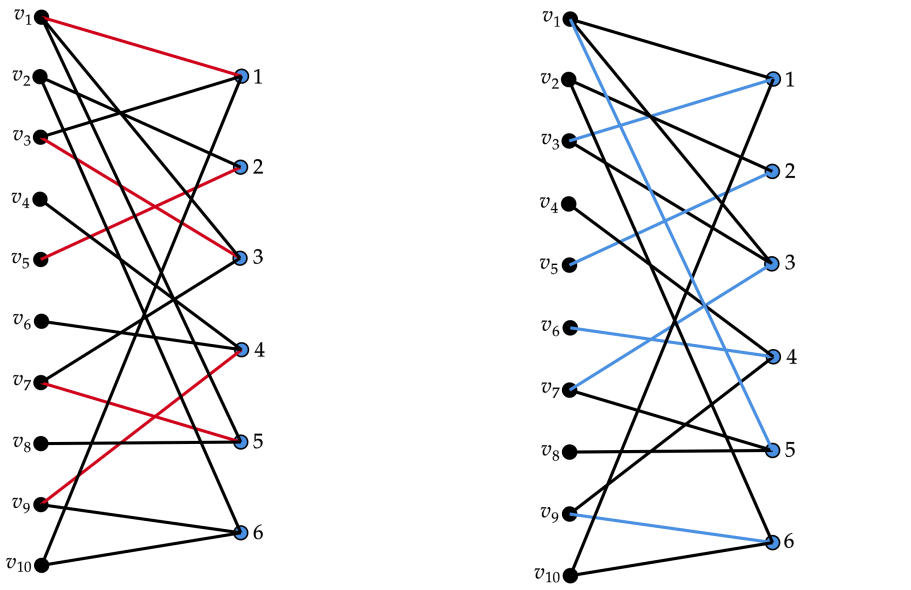
Demostración.

Sea $\mathcal{I}$ la familia de transversales parciales de $\mathcal{A}$. Tenemos que:

(I1) El conjunto vacío $\emptyset$ es una transversal de la subfamilia vacía de $\mathcal{A}$, así que $\emptyset \in \mathcal{I}$, y por lo tanto, $\mathcal{I} \neq \emptyset$.

(I2) Sean $I \in \mathcal{I}$ y $J \subseteq I$, entonces I es una transversal parcial de $\mathcal{A}$, es decir, existe $K \subseteq [m]$ tal que I es una transversal de $\{A_i : i \in K\}$, luego, I es de la forma $I = \{x_i : i \in K\}$. Como $J \subseteq I$, entonces existe $K' \subseteq K$ tal que $J = \{x_i : i \in K'\}$, de aquí que J es una transversal de la familia de conjuntos $\{A_j : j \in K'\}$, y por lo tanto, es una transversal parcial de $\mathcal{A}$, luego $J \in \mathcal{I}$.

(I3) Ilustraremos el desarrollo de la prueba de este inciso tomando como ejemplo el conjunto E y la familia $\mathcal{A}$ de subconjuntos de E, definidos en el Ejemplo 1.39. Sean $I, J \in \mathcal{I}$ tales que $|J| < |I|$, entonces I y J son transversales parciales de $\mathcal{A}$, es decir, existen subconjuntos $K_1, K_2 \subseteq [m]$ tales que $|K_1| < |K_2|$, J es una transversal de $\{A_j : j \in K_1\}$ e I es una transversal de $\{A_j : j \in K_2\}$. Por ejemplo, si establecemos $J = \{v_1, v_3, v_5, v_7, v_9\}$ entonces J puede considerarse como transversal de varias subfamilias de $\mathcal{A}$, pero en este caso consideraremos a J como una transversal de $\{A_j : j \in [5]\}$ ya que $v_1 \in A_1$, $v_5 \in A_2$, $v_3 \in A_3$, $v_9 \in A_4$ y $v_7 \in A_5$, así que



(a) Emparejamiento U en la gráfica G. (b) Emparejamiento W en la gráfica G.

Figura 1.11: Emparejamientos en la gráfica G.

en este caso $K_1 = [5]$. Por otro lado, si $I = \{v_1, v_3, v_5, v_6, v_7, v_9\}$ entonces I es una transversal de $\{A_j : j \in [6]\}$ ya que $v_3 \in A_1$, $v_5 \in A_2$, $v_7 \in A_3$, $v_6 \in A_4$, $v_1 \in A_5$ y $v_9 \in A_6$, por lo que $K_2 = [6]$. Denotemos con G a la gráfica $\Delta[\mathcal{A}]$. En G existen dos emparejamientos U y W que aparean J con K_1 e I con K_2, respectivamente. En el ejemplo, $U = \{\{v_1, 1\}, \{v_5, 2\}, \{v_3, 3\}, \{v_9, 4\}, \{v_7, 5\}\}$ se muestra en la Figura 1.11a, mientras que $W = \{\{v_3, 1\}, \{v_5, 2\}, \{v_7, 3\}, \{v_6, 4\}, \{v_1, 5\}, \{v_9, 6\}\}$ se presenta en la Figura 1.11b.

Sea H la subgráfica de G inducida por las aristas del conjunto $(U \setminus W) \cup (W \setminus U)$. Notemos que $U \setminus W$ y $W \setminus U$ no comparten aristas, pero sí pueden compartir vértices. Tenemos que $|U| = |K_1|$, $|W| = |K_2|$ y $|K_1| < |K_2|$, y como $|U \setminus W| + |U \cap W| = |U| = |K_1| < |K_2| = |W| = |W \setminus U| + |U \cap W|$, entonces $|U \setminus W| < |W \setminus U|$. Coloreemos las aristas del conjunto $U \setminus W$ de color rojo, las aristas del conjunto $W \setminus U$ de color azul y las aristas de $U \cap W$ de color verde, así que hay más aristas azules que rojas. En nuestro ejemplo, $U \setminus W = \{\{v_1, 1\}, \{v_3, 3\}, \{v_9, 4\}, \{v_7, 5\}\}$, $W \setminus U = \{\{v_3, 1\}, \{v_7, 3\}, \{v_6, 4\}, \{v_1, 5\}, \{v_9, 6\}\}$ y $U \cap W = \{\{v_5, 2\}\}$, los cuales se muestran en la Figura 1.12.

Como U y W son emparejamientos, entonces cada uno de los vértices de cada una de las subgráficas inducidas $G[U]$ y $G[W]$ tiene grado 1, y lo mismo ocurre en las subgráficas inducidas $G[U \setminus W]$ y $G[W \setminus U]$, de manera que los vértices de H tienen

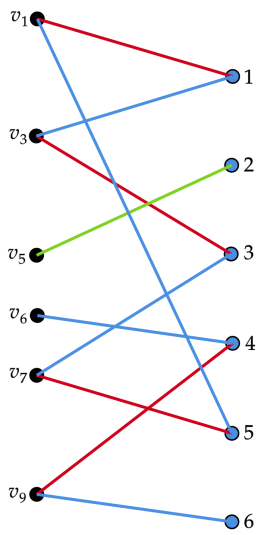


Figura 1.12: Conjuntos de aristas $U \setminus W$, $W \setminus U$ y $U \cap W$ de la gráfica G.

grado 1 o 2, dependiendo de si pertenecen únicamente a uno de los conjuntos $U \setminus W$ o $W \setminus U$ o a ambos. Por el Lema 1.40, toda componente conexa de H es un camino simple o un ciclo, y como H es bipartito, por el Lema 1.41 todo ciclo de H es par. En la Figura 1.13 se muestran las dos componentes conexas de la gráfica H, las cuales son un ciclo par de longitud 6 y un camino simple de longitud 3.

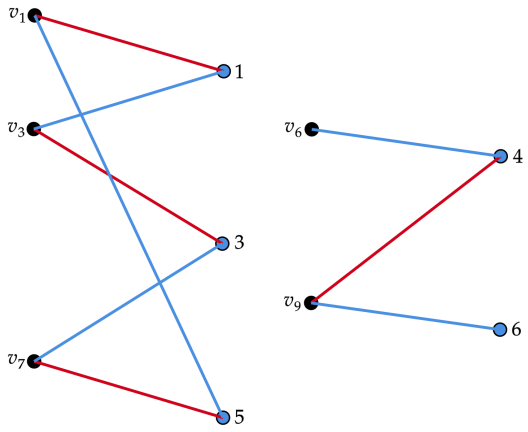


Figura 1.13: Componentes conexas de la gráfica H.

En cada ciclo y en cada camino par de H, cada arista roja va seguida por una arista azul y viceversa, pues si existiera un par de aristas consecutivas del mismo color, entonces estas aristas se intersectarían en un punto, lo cual contradice que formen parte de un emparejamiento, así que cada ciclo y cada camino par tiene el mismo número de

aristas rojas que azules. Recordemos que existen más aristas azules que rojas, y esto sólo puede ocurrir si existe al menos un camino simple impar P en H, cuyas primera y última arista sean azules, y como P tiene un número impar de aristas, entonces tiene un número par de vértices, digamos $u_1, \ldots, u_{2k}$, donde si $u_1 \in E$, entonces $u_{2k} \in [m]$, y si $u_1 \in [m]$, entonces $u_{2k} \in E$. Supongamos que $u_1 \in E$, como es el caso del camino simple P de la Figura 1.14. El caso en el que $u_1 \in [m]$ es análogo. Como la primera

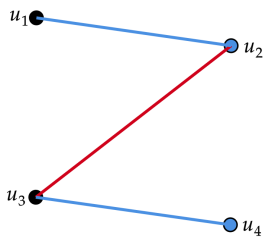


Figura 1.14: Camino simple en H.

arista de P es azul, entonces u_1 incide con una arista azul, es decir, u_1 es uno de los vértices del emparejamiento W, entonces u_1 es uno de los representantes en I. Además, como u_1 es el primer vértice del camino, sólo forma parte de una arista, que es de color azul, por lo que no puede formar parte de una arista roja, es decir, u_1 no es uno de los elementos de J, en conclusión, $u_1 \in I \setminus J$. Como $u_1 \in E$ y H es una gráfica bipartita entonces $\{u_2, u_4, \ldots, u_{2k}\} \subseteq [m]$ y dado que los vértices $\{u_3, u_5, \ldots, u_{2k-1}\}$ forman parte de una arista azul y una arista roja, entonces cada uno de estos vértices pertenece a la interseccción $J \cap I$. Ahora intercambiemos de color únicamente las aristas de P, las aristas de $G \setminus P$ permanecen del mismo color que al comienzo, como en la Figura 1.15. En el camino simple P el número de aristas azules era uno más que el número de aristas rojas, así que en el camino P recoloreado el número de aristas rojas es uno más que el número de aristas azules, más aún, en toda la gráfica recoloreada G', hay una arista roja más que en la gráfica original G. De hecho, todo vértice en $J \cup u_1$ es el extremo de un arista roja o verde. Más aún, este conjunto de aristas rojas y verdes forman un emparejamiento. Por lo tanto, $J \cup u_1$ es una transversal parcial de $\mathcal{A}$.

Por lo tanto, $\mathcal{I}$ es la familia de conjuntos independientes de un matroide $\mathcal{M}$ sobre E. □

Definición 1.43 ([5]). El matroide $\mathcal{M}$ construido como en el Teorema 1.42 se llama *matroide transversal* y a $\mathcal{A} = (A_1, \ldots, A_m)$ le llamamos una *presentación* de $\mathcal{M}$. La *función de*

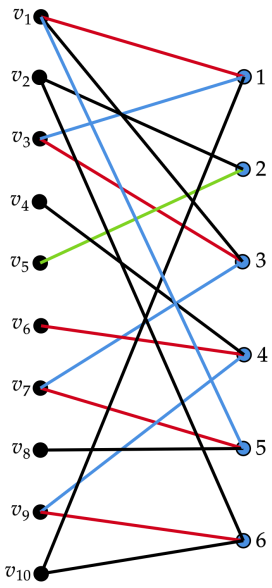


Figura 1.15: Gráfica recoloreada G'.

incidencia de $\mathcal{A}$ está dada por:

$$\begin{aligned} \eta : \mathcal{P}(E) &\to \mathcal{P}([m]) \\ X &\mapsto \{i : X \cap A_i \neq \emptyset\}. \end{aligned}$$

1.5.2. Matroides de caminos reticulares

Los matroides de caminos reticulares fueron introducidos por Bonin, de Mier y Noy en [6]. Son un tipo de matroides transversales para los cuales tenemos resultados muy específicos, entre ellos, condiciones necesarias y suficientes para determinar sus bases y sus circuitos. Durante este apartado estudiaremos las nociones básicas y propiedades acerca de los matroides de caminos reticulares. Uno de los resultados principales que presentaremos es una refutación a un corolario presentado en [5], el cual fue empleado en uno de los principales resultados de [20].

Denotaremos con $\mathbb{Z}^{\geq}$ al conjunto de enteros no negativos.

Definición 1.44 ([20]). Un *camino reticular Norte-Este de longitud n* es una sucesión de puntos $v_0, v_1, \ldots, v_n \in (\mathbb{Z}^{\geq})^2$ tales que cada diferencia consecutiva $v_i - v_{i-1}$ pertenece al conjunto $\{(0,1),(1,0)\}$. Llamamos a $(0,1)$ *paso al norte* y lo denotamos por N; a $(1,0)$ lo llamamos *paso al este* y lo denotamos por E. A los puntos v_0 y v_n los llamamos *punto inicial* y *punto final* del camino reticular, respectivamente.

Todos los caminos reticulares que se mencionan en este trabajo son caminos reticulares

Norte-Este cuyo punto inicial es el punto $(0,0)$. Si el punto final de un camino reticular S es el punto (m,r), decimos que S es un camino *hacia* (m,r). Aunque no lo mencionemos de manera explícita, supondremos que (m,r) es el punto final de los caminos reticulares que se aborden.

De manera geométrica representaremos a $(\mathbb{Z}^{\geq})^2$ como una retícula y a sus elementos los identificaremos con los puntos de intersección que se forman en la retícula. Mostraremos un camino reticular hacia un punto (m,r) como una trayectoria que comienza en el punto $(0,0)$, recorre únicamente los puntos de la sucesión que constituyen el camino reticular y finaliza en el punto (m,r). Como herramienta auxiliar escribiremos el número correspondiente a cada uno de los pasos que conforman dicho camino.

Una forma compacta de describir un camino reticular es mediante una lista ordenada de los pasos al norte y los pasos al este que involucra dicho camino, así que representaremos los caminos reticulares como palabras sobre el alfabeto $\{E,N\}$, tal como muestra el siguiente ejemplo.

Ejemplo 1.45. Consideremos el camino reticular S_1 hacia el punto $(6,5)$ definido como la siguiente sucesión de puntos: $(0,0)$, $(1,0)$, $(1,1)$, $(2,1)$, $(3,1)$, $(3,2)$, $(3,3)$, $(4,3)$, $(4,4)$, $(5,4)$, $(6,4)$, $(6,5)$. Como podemos apreciar, no es práctico dar la lista de los elementos de la sucesión de puntos. El camino S_1 puede describirse de forma abreviada como $S_1 = ENE^2N^2ENE^2N$ y lo representamos gráficamente de color lila en la Figura 1.16. También en la Figura 1.16 están representados los caminos reticulares $S_2 = N^2E^2N^2E^3NE$, $S_3 = E^6N^5$ y $S_4 = N^5E^6$ en colores verde, negro y azul, respectivamente.

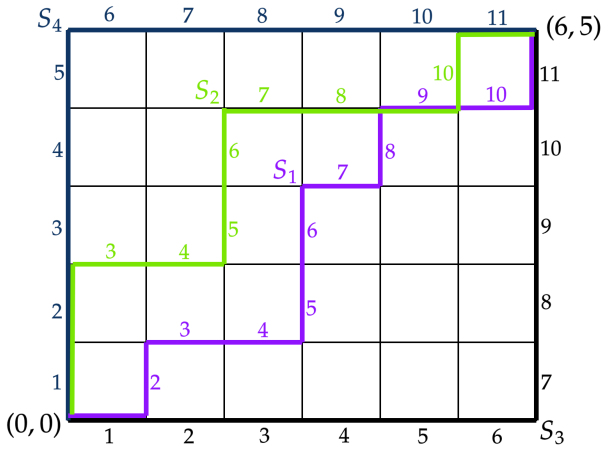


Figura 1.16: Caminos reticulares hacia $(6,5)$.

Sea (m,r) un punto en $(\mathbb{Z}^{\geq})^2$ y sean W y Q dos caminos reticulares hacia (m,r) de tal forma que W nunca esté sobre Q. Denotamos con $\mathcal{P}(W,Q)$ al conjunto de todos los caminos

reticulares hacia (m, r) que no están sobre Q ni debajo de W. A los caminos W y Q los llamamos *camino límite inferior* y *camino límite superior* de $\mathcal{P}(W, Q)$, respectivamente. En lo sucesivo supondremos que W y Q son dos caminos reticulares hacia el punto (m, r) con las características mencionadas en este párrafo.

Para todo $i \in [r]$ definimos el conjunto

$N_i = \{j \in [m+r] : \text{el paso } j \text{ es el } i\text{—ésimo paso al norte de un camino reticular en } \mathcal{P}(W, Q)\}$.

Para aclarar la definición de los conjuntos N_i veamos el siguiente ejemplo.

Ejemplo 1.46. Consideremos los caminos reticulares $Q = N^2E^3$ y $W = E^3N^2$ hacia $(3, 2)$ mostrados en la Figura 1.17.

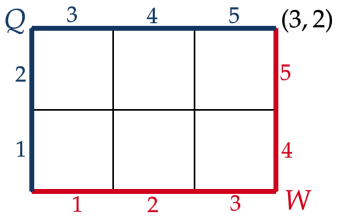


Figura 1.17: Caminos reticulares hacia $(3, 2)$.

Podemos verificar que $\mathcal{P}(W, Q) = \{E^2NEN, E^2N^2E, E^3N^2, EN^2E^2, ENE^2N, ENENE, N^2E^3, NENE^2, NE^2NE, NE^3N\}$.

Por definición, $N_1 = \{j \in [5] : \text{el paso } j \text{ es el primer paso al norte de un camino reticular en } \mathcal{P}(W, Q)\}$. Para el camino reticular E^2NEN primero damos dos pasos al este y el primer paso al norte se da en el tercer paso, así que $3 \in N_1$; en el camino reticular NE^2NE damos el primer paso al norte en el primer paso, luego $1 \in N_1$; para el camino reticular E^3N^2 primero damos 3 pasos al este y en el cuarto paso damos el primer paso al norte, de manera que $4 \in N_1$; en el camino reticular EN^2E^2 comenzamos con un paso al este y continuamos con un paso al norte, por lo que $2 \in N_1$. Analizando de esta manera cada uno de los caminos reticulares restantes de $\mathcal{P}(W, Q)$ vemos que que $N_1 = \{1, 2, 3, 4\}$.

Ahora, por definición, $N_2 = \{j \in [5] : \text{el paso } j \text{ es el segundo paso al norte de un camino reticular en } \mathcal{P}(W, Q)\}$. Notemos que en el camino reticular E^2NEN comenzamos con dos pasos al este, continuamos con el primer paso al norte seguido por un paso al este, y finalmente en el quinto paso damos el segundo paso al norte, entonces $5 \in N_2$; en el camino reticular E^2N^2E los primeros dos pasos son pasos al este y el tercer y cuarto pasos son pasos al norte, por lo que el segundo paso al norte lo damos en el cuarto paso y $4 \in N_2$; para el camino reticular EN^2E^2 el primer paso corresponde a un paso al este y el segundo y tercer pasos son pasos al norte, entonces $3 \in N_2$; en el camino reticular N^2E^3 los primeros

dos pasos son pasos al norte, así que $2 \in N_2$. Continuando con este análisis con los caminos reticulares restantes de $\mathcal{P}(W, Q)$ vemos que $N_2 = \{2, 3, 4, 5\}$.

Introducimos la siguiente notación: si i y j son enteros tales que $i < j$, entonces con $[i, j]$ denotamos al conjunto $\{i, i+1, \ldots, j\}$ y nos referimos a él como el *intervalo de enteros con extremo inferior* i y *extremo superior* j.

Notemos que $N_1, \ldots, N_r$ es una sucesión de intervalos contenidos en $[m + r]$, y que la sucesión de extremos inferiores así como la sucesión de extremos superiores son sucesiones estrictamente crecientes. También observemos que una manera más sencilla de definir el intervalo N_i es como el intervalo $[q_i, w_i]$, donde q_i es dónde ocurre el i-ésimo paso al norte de Q y w_i es dónde ocurre el i-ésimo paso al norte de W.

Para cada punto (m, r) y para cada par de caminos reticulares límite W y Q tenemos una familia de conjuntos $(N_1, \ldots, N_r)$ y para formar un matroide transversal únicamente necesitamos una familia de subconjuntos de un conjunto dado. Entonces tiene sentido presentar la siguiente definición.

Definición 1.47 ([20])**.** Al matroide transversal con conjunto subyacente $[m + r]$ que tiene a $(N_1, \ldots, N_r)$ como su presentación lo denotamos por $\mathcal{M}[W, Q]$, a $(N_1, \ldots, N_r)$ la llamamos *presentación estándar* de $\mathcal{M}[W, Q]$ y al par (W, Q) lo llamamos la *presentación de caminos reticulares* de $\mathcal{M}[W, Q]$.

Decimos que un matroide $\mathcal{M}$ es *de caminos reticulares* si existen dos caminos reticulares W y Q hacia el punto (m, r) tales que $\mathcal{M}$ es isomorfo a $\mathcal{M}[W, Q]$. Si fijamos $W = E^m N^r$, entonces el matroide de caminos reticulares se llama *matroide anidado*.

Ejemplo 1.48. En la figura 1.18 mostramos la presentación de caminos reticulares del matroide $\mathcal{M}[W, Q]$, donde $Q = N^2E^2N^2E^4$ y $W = E^3NE^2N^2ENN$, cuya presentación estándar es $([1, 4], [2, 7], [5, 8], [6, 10])$.

Un conjunto independiente en un matroide de caminos reticulares $\mathcal{M}[W, Q]$ con presentación estándar $(N_1, \ldots, N_r)$ es una transversal parcial de $(N_1, \ldots, N_r)$, y una base de $\mathcal{M}[W, Q]$ es una transversal de $(N_1, \ldots, N_r)$, es decir, un sistema de distintos representantes de $(N_1, \ldots, N_r)$.

A cualquier subconjunto X de $[m + r]$ le podemos asociar un camino reticular en $(\mathbb{Z}^{\geq})^2$, tal como se establece en la siguiente definición.

Definición 1.49 ([6, Definición 3.2])**.** Sea X un subconjunto del conjunto subyacente $[m + r]$ del matroide de caminos reticulares $\mathcal{M}[W, Q]$. El *camino reticular asociado a* X, denotado

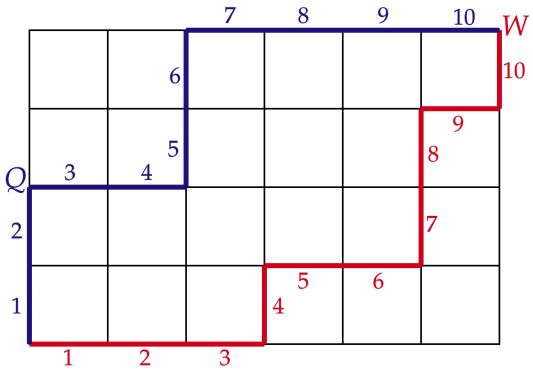


Figura 1.18: Presentación de caminos reticulares de un matroide.

por $\mathcal{P}(X)$, es la palabra $s_1 s_2 \dots s_{m+r}$ sobre el alfabeto $\{E, N\}$, donde

$$s_i = \begin{cases} N, & \text{si } i \in X; \\ E, & \text{en otro caso.} \end{cases}$$

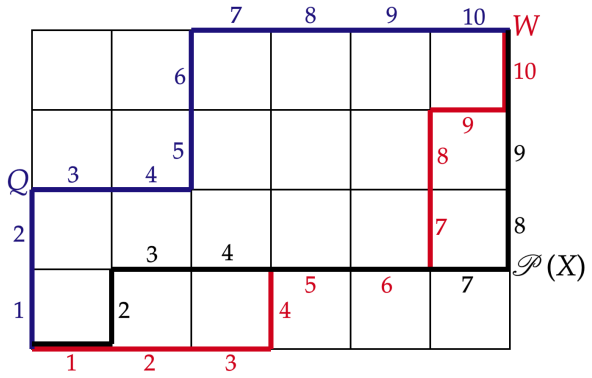
Es decir, para formar el camino reticular $\mathcal{P}(X)$ escribimos de forma concatenada los números del 1 a $m+r$ y reemplazamos cada uno de los números por N o por E, dependiendo de si dicho número pertenece o no a X.

Ejemplo 1.50. Sean $(m, r) = (6, 4)$, $W = E^3NE^2N^2EN$ y $Q = N^2E^2N^2E^4$. Definimos los conjuntos $X = \{2, 8, 9, 10\}$, $Y = \{3, 5, 6, 8\}$ y $Z = [6]$. Por definición, el camino reticular asociado a X es $\mathcal{P}(X) = ENE^5N^3$ (Figura 1.19a), el camino reticular asociado a Y es $\mathcal{P}(Y) = E^2NEN^2ENE^2$ (Figura 1.19b) y el camino reticular asociado a Z es $\mathcal{P}(Z) = N^6E^4$ (Figura 1.19c).

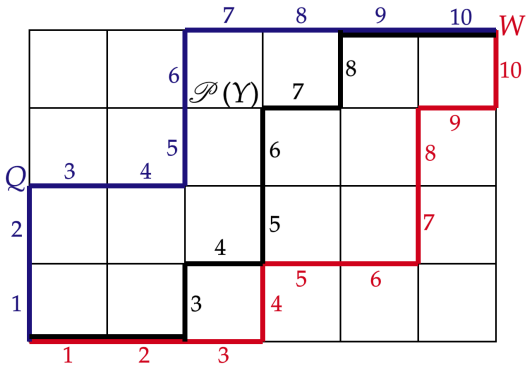
En el Ejemplo 1.50 vemos que el camino reticular asociado a un conjunto X puede estar o no dentro de la región delimitada por los caminos reticulares límite W y Q, es más, puede que el camino $\mathcal{P}(X)$ incluso tenga punto final distinto a (m, r). Sólo los subconjuntos X de cardinalidad r generan caminos reticulares que terminan en (m, r), ya que tendrán r pasos al norte y los restantes m pasos corresponderán a pasos al este.

El siguiente teorema presenta una condición necesaria y suficiente para identificar una base de un matroide de caminos reticulares $\mathcal{M}$ de manera geométrica: un subconjunto X de cardinalidad r es una base de $\mathcal{M}$ si y sólo si al trazar su camino reticular asociado $\mathcal{P}(X)$, éste queda entre W y Q.

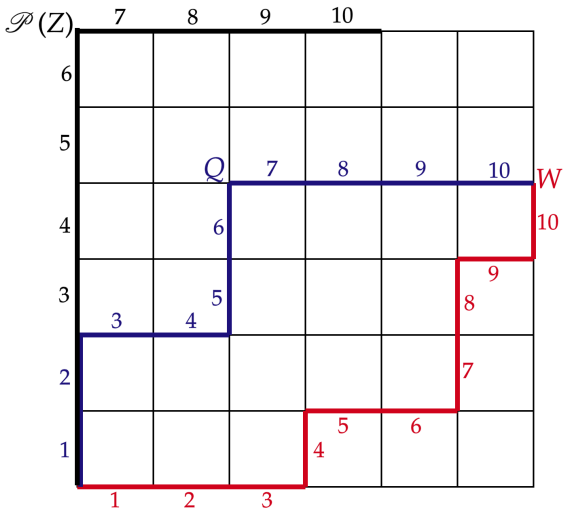
Teorema 1.51 ([6, Teorema 3.3]). *Sea $\mathcal{M}[W, Q]$ un matroide de caminos reticulares. Un subconjunto B de $[m+r]$ tal que $|B| = r$ es una base de $\mathcal{M}[W, Q]$ si y sólo si el camino reticular*



(a) Camino reticular $\mathcal{P}(X)$.



(b) Camino reticular $\mathcal{P}(Y)$.



(c) Camino reticular $\mathcal{P}(Z)$.

Figura 1.19: Caminos reticulares asociados a distintos conjuntos.

asociado $\mathcal{P}(B)$ pertenece a la región delimitada por W y Q, es decir, nunca está por encima de Q y nunca está por debajo de W.

Demostración.

Sea $B = \{b_1, \ldots, b_r\}$, con $b_1 < \cdots < b_r$. Supongamos que B es una base de $\mathcal{M}[W, Q]$, es decir, que B es una transversal de $(N_1, \ldots, N_r)$. Queremos demostrar que el camino reticular asociado $\mathcal{P}(B)$ pertenece a la región delimitada por W y Q. Por definición, el camino reticular asociado $\mathcal{P}(B)$ es aquél en el cual para todo $i \in [r]$, el paso b_i es un paso al norte y para todo $x \in [m + r] \setminus B$, el paso x es un paso al este. Para que $\mathcal{P}(B)$ sea un camino reticular entre W y Q debe ocurrir que cada uno de sus pasos al norte es un elemento de N_i, es decir, que para todo $i \in [r]$, $b_i \in N_i$, o equivalentemente, que para todo $i \in [r]$, $q_i \leq b_i \leq w_i$. Supongamos que existe $i \in [r]$ tal que $b_i < q_i$, y que para todo $j < i$ se cumple que $b_j \in N_j$,

así que i es el primer subíndice para el cual $b_i \notin N_i$. Para cualesquiera $s, t \in [r]$ tales que $s < t$ tenemos que $q_s < q_t$, entonces para todo $j > i$ se verifica que $b_i < q_i < q_j$, luego $b_i \notin N_j$, pero como B es una transversal de $(N_1, \ldots, N_r)$, existe $j_0 < i$ tal que $b_i \in N_{j_0}$, pero como $j_0 < i$ e i es el primer subíndice para el cual $b_i \notin N_i$, sabemos que $b_{j_0} \in N_{j_0}$, y dado que B es una base de $\mathcal{M}[W, Q]$, no podemos tener dos representantes del mismo conjunto N_{j_0}, así que esto no puede ocurrir. Si ahora suponemos que existe $i \in [r]$ tal que $b_i > w_i$, siguiendo un razonamiento similar al anterior obtendríamos que existe $j > i$ tal que N_j tiene dos representantes en B, lo cual tampoco puede ocurrir. Por lo tanto, para todo $i \in [r]$, $q_i \leq b_i \leq w_i$, es decir, $b_i \in N_i$, de donde $\mathcal{P}(X) \in \mathcal{P}(W, Q)$. Ahora supongamos que el camino reticular asociado $\mathcal{P}(B)$ pertenece a la región delimitada por W y Q. Los elementos de B son precisamente los pasos al norte del camino reticular $\mathcal{P}(B)$, entonces para cada $i \in [r]$ tenemos que $q_i \leq b_i \leq w_i$, es decir, $b_i \in N_i$, así que B es una transversal de $(N_1, \ldots, N_r)$, luego B es una base de $\mathcal{M}[W, Q]$. □

En el siguiente ejemplo veremos que los matroides de caminos reticulares no son tan extraños como pudieran parecernos, pues un ejemplo de ellos es un matroide que ya conocemos.

Ejemplo 1.52 ([6])**.** Consideremos los caminos reticulares $W = E^m N^r$ y $Q = N^r E^m$, como los caminos límite de la Figura 1.17. En este caso tenemos que $N_1 = [1, m+1]$, $N_2 = [2, m+2]$, $\ldots$, $N_r = [r, m+r]$. Notemos que en este ejemplo todos los conjuntos N_i son de la forma $[i, m+i]$ y tienen cardinalidad $m+1$. Como en este caso todos los caminos reticulares pertenecen a la región delimitada por W y Q, entonces por el Teorema 1.51 todos los subconjuntos de $[m+r]$ de cardinalidad r son bases de $\mathcal{M}[W, Q]$, así que el matroide $\mathcal{M}[W, Q]$ tiene $\binom{m+r}{r}$ bases. Con esto hemos demostrado que el matroide uniforme $U_{r,m+r}$ es un matroide de caminos reticulares.

Por lo tanto, los matroides de caminos reticulares incluyen a los matroides uniformes.

Ejemplo 1.53. Consideremos el matroide de caminos reticulares $\mathcal{M}[W, Q]$, donde W y Q son los caminos reticulares límite definidos en el Ejemplo 1.50, $(m, r) = (6, 4)$ y sea $Y = \{3, 5, 6, 8\}$. El conjunto Y tiene cardinalidad 4 que es igual a r y de la Figura 1.19b vemos que el camino reticular asociado $\mathcal{P}(Y)$ pertenece a la región delimitada por W y Q, entonces por el Teorema 1.51 sabemos que el conjunto Y es una base de $\mathcal{M}[W, Q]$. Otras bases de este matroide son $\{2, 4, 6, 7\}$, $\{1, 2, 5, 6\}$ y $\{4, 7, 8, 10\}$, como podemos apreciar en la Figura 1.20.

El siguiente es un resultado extraído del enunciado del Teorema 1.51 y de su demostración, pero dada su importancia lo enunciamos en el siguiente corolario.

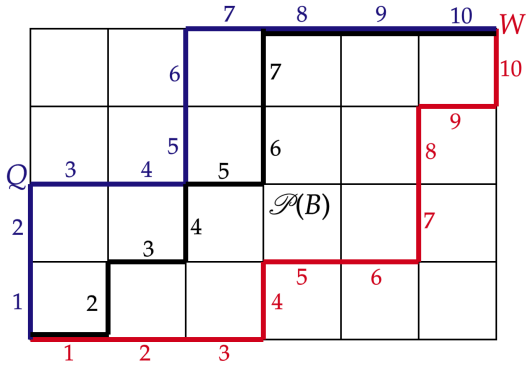


Figura 1.20: Caminos reticulares asociados a bases.

Corolario 1.54 ([5, Lema 2.3]). *Supongamos que* $\{b_1, b_2, \ldots, b_r\}$ *es una base de un matroide de caminos reticulares* $\mathcal{M}[W, Q]$*, con* $b_1 < b_2 < \cdots < b_r$*. Entonces para todo* $i \in [r]$*,* $b_i \in N_i$*.*

Por el Corolario 1.54 si un conjunto B de r elementos ordenados de menor a mayor es una base, entonces este mismo orden debe respetarse para los conjuntos que están representando; así, el primer elemento de B debe representar al primer conjunto N_1, el segundo elemento de B debe ser representante del segundo conjunto N_2, etcétera. El siguiente corolario presenta un resultado más general pues afirma que para aquellos conjuntos independientes cuya cardinalidad coincide con la cardinalidad de su incidencia una conclusión análoga a la del Corolario 1.54 se verifica.

Corolario 1.55 ([5, Corolario 2.4]). *Sea* $\mathcal{M}[W, Q]$ *un matroide de caminos reticulares y sea* I *un conjunto independiente de* $\mathcal{M}[W, Q]$ *con* $|I| = k = |\eta(I)|$*. Sea* $I = \{a_1, \ldots, a_k\}$*, con* $a_1 < \cdots < a_k$*, y sea* $\eta(I) = \{i_1, \ldots, i_k\}$*, con* $i_1 < \cdots < i_k$*. Entonces para todo* $j \in [k]$*,* $a_j \in N_{i_j}$*.*

Demostración.

Tomando B una base cualquiera de $\mathcal{M}[W, Q]$ y empleando de manera repetida la propiedad (I3) podemos extender I a una base B' de $\mathcal{M}[W, Q]$, digamos

$$B' = \{b_1, b_2, \ldots, b_{m_1}, \mathbf{b_{m_1+1}}, b_{m_1+2}, \ldots, b_{m_1+m_2}, \mathbf{b_{m_1+m_2+1}}, \ldots, b_{m_1+\cdots+m_k}, \mathbf{b_{m_1+\cdots+m_k+1}}, b_{m_1+\cdots+m_k+2}, \ldots, b_r\},$$

donde los elementos de B' están escritos de menor a mayor y para todo $j \in [k]$, $b_{(\sum_{t=1}^{j} m_t)+1} = a_j$. El conjunto B' tiene cardinalidad r porque es una base. Los elementos b_s que escribimos adicionales a los elementos $b_{(\sum_{t=1}^{j} m_t)+1} = a_j$ indican que al extender I a la base B' puede ser necesario agregar elementos menores o mayores a los que ya teníamos en I, o incluso elementos intermedios entre ellos. Como B' es base, por el Corolario 1.54 tenemos que para

todo $s \in [r]$, $b_s \in N_s$, así que en particular para todo $j \in [k]$,

$$a_j = b_{(\sum_{t=1}^{j} m_t)+1} \in N_{(\sum_{t=1}^{j} m_t)+1} \tag{1.6}$$

de aquí que $\{m_1 + 1, m_1 + m_2 + 1, \ldots, m_1 + \cdots + m_k + 1\} \subseteq \eta(I)$, y puesto que $|\{m_1 + 1, m_1 + m_2 + 1, \ldots, m_1 + \cdots + m_k + 1\}| = k = |\eta(I)|$, tenemos que $\eta(I) = \{m_1 + 1, m_1 + m_2 + 1, \ldots, m_1 + \cdots + m_k + 1\}$, y dado que los elementos de $\eta(I)$ y los elementos de $\{m_1 + 1, m_1 + m_2 + 1, \ldots, m_1 + \cdots + m_k + 1\}$ están escritos de menor a mayor, concluimos que $(\sum_{t=1}^{j} m_t) + 1 = i_j$, y por (1.6), $a_j \in N_{i_j}$. □

El siguiente lema nos permite conocer la cardinalidad de la incidencia de un circuito de un matroide transversal a partir de su rango.

Lema 1.56 ([5, Lema 3.8]). *Sea η la función de incidencia de una presentación de un matroide transversal $\mathcal{M}$. Si C es un circuito de rango k de $\mathcal{M}$, entonces $|\eta(C)| = k$, y para todo $x \in C$, $|\eta(C \setminus x)| = k$.*

A continuación mostramos un criterio que permite determinar si un conjunto es o no un circuito de un matroide de caminos reticulares, y también constituye una serie de pasos para construir circuitos en dicho matroide.

Teorema 1.57 ([5, Teorema 3.9]). *Sea $\mathcal{M}[W, Q]$ un matroide de caminos reticulares sobre el conjunto $[m + r]$ con presentación estándar $(N_1, \ldots, N_r)$. Sea $C = \{c_0, c_1, \ldots, c_k\} \subseteq [m + r]$, con $c_0 < c_1 < \cdots < c_k$, y sea $\eta(C) = \{i_1, \ldots, i_s\}$, con $i_1 < \cdots < i_s$. Entonces C es un circuito de $\mathcal{M}[W, Q]$ si y sólo si*

(I) $s = k$,

(II) $c_0 \in N_{i_1}$,

(III) $c_k \in N_{i_k} = N_{i_s}$, *y*

(IV) para todo $0 < j < k$, $c_j \in N_{i_j} \cap N_{i_{j+1}}$.

Además, si C es un circuito, entonces para todo $1 \leq h < k$, $i_{h+1} = i_h + 1$.

Demostración.

Supongamos que C es un circuito. Por el Teorema 1.18, tenemos que $\text{rank}(C) = |C| - 1 = k$, luego, por el Lema 1.56, $s = |\eta(C)| = k$, así que $s = k$, con lo cual tenemos que se verifica la condición (I). Además, como C es un circuito y $c_0 \in C$, entonces $C \setminus c_0$ es un conjunto independiente y por el Lema 1.56 tenemos que $|\eta(C \setminus c_0)| = k = |\eta(C)|$, y dado que $\eta(C \setminus c_0) \subseteq \eta(C)$, concluimos que $\eta(C \setminus c_0) = \eta(C) = \{i_1, \ldots, i_s\}$. Por el Corolario 1.55, tenemos

que para todo $j \in [k]$, $c_j \in N_{i_j}$, en particular hemos obtenido que $c_k \in N_{i_k} = N_{i_s}$, es decir, que (III) se verifica. Puesto que $c_k \in C$, entonces $C \setminus c_k$ también es un conjunto independiente y empleando un argumento similar al anterior obtenemos que $\eta(C \setminus c_k) = \eta(C) = \{i_1, \ldots, i_s\}$. El Corolario 1.55 nos permite afirmar que para todo $j \in [0, k-1]$, $c_j \in N_{i_{j+1}}$, en particular, $c_0 \in N_{i_1}$, de manera que (II) se verifica. También hemos obtenido que para todo $j \in [k-1]$, $c_j \in N_{i_j} \cap N_{i_{j+1}}$, por lo cual (IV) es cierta. Hemos demostrado que se verifican (I)-(IV). Ahora supongamos que existen $i_j \in \eta(C)$ y $h \in [r] \setminus \eta(C)$ tales que $i_j < h < i_{j+1}$. Por (IV) sabemos que $c_j \in N_{i_j} \cap N_{i_{j+1}}$. Recordemos que la sucesión $(q_1, \ldots, q_r)$ de extremos inferiores de los intervalos N_i es una sucesión estritamente creciente, y lo mismo ocurre para la sucesión $(w_1, \ldots, w_r)$ de extremos superiores de los intervalos N_i. Así, como $h < i_{j+1}$, tenemos que $q_h < q_{i_{j+1}}$ y como $i_j < h$, entonces $w_{i_j} < w_h$. Ahora, dado que $c_j \in N_{i_j}$, se verifica que $c_j \leq w_{i_j}$, y dado que $c_j \in N_{i_{j+1}}$, se verifica que $q_{i_{j+1}} \leq c_j$. Por consiguiente tenemos la siguiente cadena de desigualdades:

$$q_h < q_{i_{j+1}} \leq c_j \leq w_{i_j} < w_h,$$

de donde $q_h < c_j < w_h$, así que $c_j \in N_h$, por lo que $h \in \eta(C)$, lo cual contradice la elección de h. Por lo tanto, para todo $h \in [k-1]$, $i_{h+1} = i_h + 1$.

Ahora supongamos que C es un subconjunto de $[m+r]$ que verifica (I)-(IV). Como el conjunto C tiene un elemento más que el conjunto $\eta(C)$, entonces C es un conjunto dependiente. Por las condiciones (III) y (IV) tenemos que $c_1 \in N_{i_1}$, $c_2 \in N_{i_2}$, $\ldots$, $c_{k-1} \in N_{i_{k-1}}$ y $c_k \in_{N_{i_k}}$, es decir, el conjunto $C \setminus c_0$ es una transversal de $(N_{i_1}, \ldots, N_{i_k})$, así que $C \setminus c_0$ es un conjunto independiente de $\mathcal{M}[W, Q]$. De forma análoga, por (II) y (IV) tenemos que $c_0 \in N_{i_1}$, $c_1 \in N_{i_2}$, $\ldots$, $c_{k-2} \in N_{i_{k-1}}$ y $c_{k-1} \in N_{i_k}$, así que $C \setminus c_k$ es una transversal de $(N_{i_1}, \ldots, N_{i_k})$, luego $C \setminus c_k$ es un conjunto independiente de $\mathcal{M}[W, Q]$. Sea $i \in [1, k-1]$. Por (II), (III) y (IV) sabemos que $c_0 \in N_{i_1}$, $c_1 \in N_{i_2}$, $\ldots$, $c_{i-1} \in N_i$, $c_{i+1} \in N_{i+1}$, $c_{i+2} \in N_{i+2}$, $\ldots$, $c_k \in N_{i_k}$, por lo que $C \setminus c_i$ es una transversal de $(N_{i_1}, \ldots, N_{i_k})$, y por lo tanto, es un conjunto independiente de $\mathcal{M}[W, Q]$. Así, para todo $i \in [0, k]$, $C \setminus c_i$ es un conjunto independiente, por lo cual todos los subconjuntos propios de C son independientes. En conclusión, C es un conjunto dependiente cuyos subconjuntos propios son todos independientes, es decir, C es un circuito. □

En el siguiente ejemplo comprobaremos la utilidad del Teorema 1.57 para identificar circuitos en un matroide.

Ejemplo 1.58. Consideremos el matroide de caminos reticulares $\mathcal{M}[W, Q]$ definido en el Ejemplo 1.48, donde $N_1 = [1, 4]$, $N_2 = [2, 7]$, $N_3 = [5, 8]$ y $N_4 = [6, 10]$ y cuya presentación de caminos reticulares se muestra en la Figura 1.18. Sea $C_1 = \{1, 2, 5, 8, 10\}$. Tenemos que $\eta(C_1) = [4]$, así que C_1 tiene un elemento más que su incidencia; $1 \in N_1$, $2 \in N_1 \cap N_2$,

$5 \in N_2 \cap N_3$, $8 \in N_3 \cap N_4$ y $10 \in N_4$. Por el Teorema 1.57 sabemos que C_1 es un circuito de $\mathcal{M}[W, Q]$. Sea $C_2 = \{5, 6, 8, 9\}$. Tenemos que $\eta(C_2) = \{2, 3, 4\}$, así que $|C_2| = |\eta(C_2)| + 1$; $5 \in N_2$, $6 \in N_2 \cap N_3$, $8 \in N_3 \cap N_4$ y $9 \in N_4$, luego, por el Teorema 1.57 concluimos que C_2 es un circuito de $\mathcal{M}[W, Q]$. Si tomamos $X = \{1, 8, 9\}$, entonces $\eta(X) = \{1, 3, 4\}$, por lo que $|X| = |\eta(X)|$, así que no se verifica la propiedad (I), y por lo tanto, X no es un circuito de $\mathcal{M}[W, Q]$.

A continuación definimos un concepto que nos permite describir de manera alternativa un camino reticular.

Definición 1.59 ([5])**.** Sea S un camino reticular. Decimos que S tiene una *esquina* NE en h si el paso h de S es un paso al norte y el paso $h + 1$ es un paso al este. Si el paso h de S es un paso al este y el paso $h + 1$ es un paso al norte decimos que S tiene una *esquina* EN en h.

Ejemplo 1.60. Consideremos la presentación de caminos reticulares de la Figura 1.18. En este caso Q tiene sus esquinas NE en 2 y 6, y su única esquina EN en 4. Por su parte W tiene sus esquinas NE en 4 y 8 y sus esquinas EN en 3, 6 y 9.

Sean π_1 y π_2 dos particiones de un conjunto P. Decimos que π_1 es *más fina* que π_2 (y que π_2 es *más gruesa* que π_1) si π_1 puede obtenerse de π_2 dividiendo algunas de sus partes en piezas más pequeñas. El *ínfimo* de dos particiones, denotado por $\pi_1 \wedge \pi_2$, es la partición más gruesa que es más fina que ambas particiones.

Sea $\mathcal{M}[W, Q]$ un matroide de caminos reticulares. Supongamos que las esquinas EN de Q ocurren en los pasos $i_1, \ldots, i_h$, con $i_1 < \cdots < i_h$, y que las esquinas NE de W ocurren en $j_1, \ldots, j_k$, con $j_1 < \cdots < j_k$. Con el conjunto de esquinas EN de Q podemos formar una partición del conjunto $[m + r]$ con $h + 1$ partes, a saber,

$$\pi_1 = \{[1, i_1], [i_1 + 1, i_2], \ldots, [i_h + 1, m + r]\}.$$

Por otro lado, con el conjunto de esquinas NE de W obtenemos otra partición del conjunto $[m + r]$ con $k + 1$ partes, concretamente,

$$\pi_2 = \{[1, j_1], [j_1 + 1, j_2], \ldots, [j_k + 1, m + r]\}.$$

Llamamos a la partición $\pi_1 \wedge \pi_2$ la *partición ordenada natural* de $[m + r]$ en $\mathcal{M}$. La parte que contiene a 1 se llama la *cabeza* de la partición y la parte que contiene a $m + r$ se llama la *cola* de la partición.

1.5.3. Un corolario de Bonin y de Mier que no se verifica

En [5] se enuncia el siguiente resultado:

> **Corolario (3.13 en [5]).** Sea $C = \{c_0, c_1, \ldots, c_k\}$ un circuito de $\mathcal{M}[W, Q]$ tal que $c_0 < c_1 < \cdots < c_k$. Si $x \in [m+r] \setminus C$ y existe un subconjunto $Z \subseteq C$ tal que $Z \cup x$ es un circuito de $\mathcal{M}[W, Q]$, entonces Z es un segmento inicial $\{c_0, c_1, \ldots, c_i\}$ o un segmento final $\{c_j, c_{j+1}, \ldots, c_k\}$ de C.

Bonin y de Mier afirman en [5] que este resultado puede demostrarse a partir del Lema 1.56 y del siguiente corolario del Teorema 1.57:

> **Corolario A.** Sea $C = \{c_0, c_1, \ldots, c_k\}$ un circuito de $\mathcal{M}[W, Q]$ tal que $c_0 < c_1 < \cdots < c_k$. Si X un subconjunto propio de C que no es segmento inicial ni segmento final de C entonces $|\eta(X)| > |X|$.

Nosotros afirmamos que ambos corolarios son falsos y a continuación presentamos dos matroides de caminos reticulares en los cuales no se verifican ambos resultados.

Contraejemplo 1. Sean $W = E^{10}N^5$ y $Q = NE^2NE^2NE^2NE^2NE^2$. La presentación del matroide anidado $\mathcal{M}[W, Q]$ se muestra en la Figura 1.21, y su presentación estándar es $(N_1, N_2, N_3, N_4, N_5)$, donde $N_1 = [1, 11]$, $N_2 = [4, 12]$, $N_3 = [7, 13]$, $N_4 = [10, 14]$ y $N_5 = [13, 15]$. Sea $C = \{10, 11, 12, 13, 14, 15\}$. Tenemos que $\eta(C) = [5]$, así que C tiene un elemento más que su incidencia; además, $10 \in N_1$, $11 \in N_1 \cap N_2$, $12 \in N_2 \cap N_3$, $13 \in N_3 \cap N_4$, $14 \in N_4 \cap N_5$ y $15 \in N_5$. Por el Teorema 1.57 sabemos que C es un circuito de $\mathcal{M}[W, Q]$. El conjunto $Z = \{10, 12, 13, 14, 15\} \subsetneq C$ no es segmento inicial ni segmento final de C. Tenemos que $\eta(Z) = [5]$, así que $|Z| = 5 = |\eta(Z)|$, por lo que el Corolario A no se verifica. Sea $X = Z \cup \{1\} = \{1, 10, 12, 13, 14, 15\}$. Notemos que $1 \in [15] \setminus C$, $|X| = 6$, $\eta(X) = [5]$, $1 \in N_1$, $10 \in N_1 \cap N_2$, $12 \in N_2 \cap N_3$, $13 \in N_3 \cap N_4$, $14 \in N_4 \cap N_5$, $15 \in N_5$. Por el Teorema 1.57 sabemos que $X = Z \cup x$ es un circuito. En conclusión, Z es un subconjunto propio de C tal que $Z \cup \{1\}$ es un circuito, con $1 \in [15] \setminus C$, y sin embargo, Z no es un segmento inicial ni un segmento final de C. Por lo tanto, no se verifica la conclusión del Corolario 3.13.

Contraejemplo 2. Sean $Q = NENE^3NE^2NE^2$ y $W = E^4NE^2NE^2N^2$. En la Figura 1.22 mostramos la presentación del matroide $\mathcal{M}[W, Q]$. En este caso tenemos que $N_1 = [1, 5]$, $N_2 = [3, 8]$, $N_3 = [7, 11]$, $N_4 = [10, 12]$. Sea $C = \{1, 4, 7, 9\}$. Tenemos que $\eta(C) = \{1, 2, 3\}$, por lo que $|C| = |\eta(C)| + 1$; $1 \in N_1$, $4 \in N_1 \cap N_2$, $7 \in N_2 \cap N_3$ y $9 \in N_3$. Por el Teorema 1.57, C es un circuito. Sea $Z = \{1, 7, 9\} \subsetneq C$. Z no es un segmento inicial ni un segmento

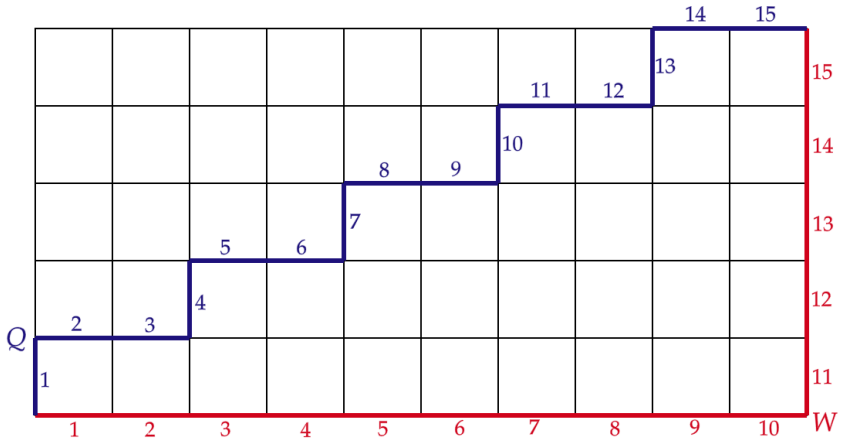


Figura 1.21: Presentación de un matroide de caminos reticulares que no verifica el Corolario 3.13.

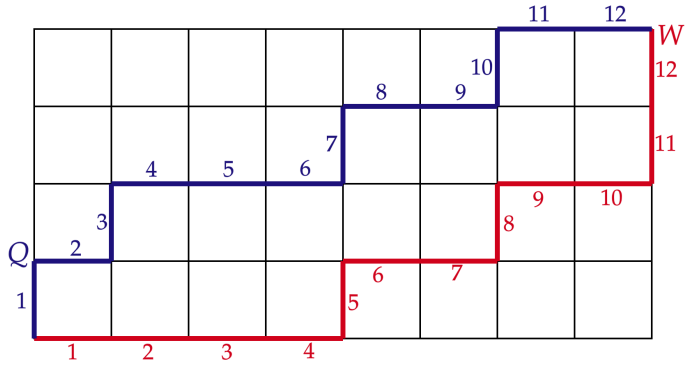


Figura 1.22: Presentación de un matroide de caminos reticulares que no verifica el Corolario 3.13.

final de C. Dado que $|\eta(Z)| = |\{1,2,3\}| = 3 = |Z|$, el Corolario A no se verifica. Ahora, si $X = Z \cup \{3\} = \{1,3,7,9\}$ entonces $|X| = 4 = |\{1,2,3\}| + 1 = |\eta(X)| + 1$, $1 \in N_1$, $3 \in N_1 \cap N_2$, $7 \in N_2 \cap N_3$ y $9 \in N_3$. Por el Teorema 1.57, el conjunto $X = Z \cup \{3\}$ es un circuito de $\mathcal{M}[W, Q]$, pero Z no es un segmento inicial ni un segmento final de C, por lo cual el Corolario 3.13 es falso.

Capítulo 2

Esquemas de compartición de secretos y matroides

2.1. Introducción

Para introducir el tema de esquemas de compartición de secretos exponemos un ejemplo típico que se presenta en [25]. Supongamos que un banco tiene una bóveda que necesita ser abierta cada día. El banco cuenta con tres empleados, pero no confía a ninguno de ellos la combinación que da acceso a la bóveda. Buscamos un método para repartir información de la combinación de manera que sólo si se reúnen al menos dos empleados del banco y juntan su información pueden conocer la combinación de acceso, pero si sólo un empleado intenta abrir la bóveda, no lo consiga.

De manera general, consideremos una entidad p_0, que puede ser una organización, una empresa, un grupo o una sola persona, que tiene un *secreto* k, y un grupo P ajeno a la entidad. Esta entidad quiere otorgar información parcial del secreto a cada elemento de P de manera que únicamente ciertos subconjuntos de P puedan conocer el secreto k. Los distintos métodos que podemos emplear para resolver este problema son los *esquemas de compartición de secretos*. Para adentrarnos en este tema, damos la siguiente definición.

Definición 2.1 ([2])**.** Sean P un conjunto finito y $\Gamma \subseteq \mathcal{P}(P)$. Γ es una familia *monótona creciente* si para todo $A \in \Gamma$ y para todo $B \in \mathcal{P}(P)$ tal que $A \subseteq B$, se tiene que $B \in \Gamma$, es decir, si Γ es una familia cerrada bajo superconjuntos. Una *estructura de acceso* sobre P es una familia monótona creciente no vacía Γ de subconjuntos de P. A los elementos de Γ los llamamos *conjuntos autorizados* y a los elementos de $\mathcal{P}(P) \setminus \Gamma$ los llamamos *conjuntos no autorizados*.

Sea Γ una estructura de acceso. Dado que Γ es una familia monótona creciente, una manera efectiva de proporcionar a todos sus elementos, es mediante la familia de conjuntos autorizados minimales, la cual denotamos por Γ_0 y a sus elementos se les llama *bases* de Γ. En este texto no emplearemos la palabra base para no causar confusión con el concepto de base de un matroide.

Ejemplo 2.2. Sean $P = \{a, b, c, d, e, f\}$ y $\Gamma = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, a\}, \{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{a, b, f\}, \{a, c, d\}, \{a, c, f\}, \{a, d, e\}, \{a, d, f\}, \{a, e, f\}, \{b, c, d\}, \{b, c, e\}, \{b, c, f\}, \{b, d, e\}, \{b, e, f\}, \{c, d, e\}, \{c, d, f\}, \{c, e, f\}, \{d, e, f\}, \{a, b, c, d\}, \{a, b, c, e\}, \{a, b, c, f\}, \{a, b, d, e\}, \{a, b, d, f\}, \{a, b, e, f\}, \{a, c, d, e\}, \{a, c, d, f\}, \{a, c, e, f\}, \{a, d, e, f\}, \{b, c, d, e\}, \{b, c, d, f\}, \{b, c, e, f\}, \{b, d, e, f\}, \{c, d, e, f\}, \{a, b, c, d, e\}, \{a, b, c, d, f\}, \{a, b, c, e, f\}, \{a, b, d, e, f\}, \{a, c, d, e, f\}, \{b, c, d, e, f\}, \{a, b, c, d, e, f\}\}$. Como podemos ver, en este caso resulta muy tedioso proporcionar la lista completa de los conjuntos autorizados de Γ. Podemos verificar que la familia de conjuntos autorizados minimales de Γ es $\Gamma_0 = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, a\}\}$, la cual es una manera más práctica de describir a la familia Γ.

En la siguiente definición veremos que siempre es posible construir una estructura de acceso a partir de una familia de conjuntos arbitraria no vacía.

Definición 2.3 ([9])**.** Sea P un conjunto y $\mathcal{A}$ una familia de subconjuntos de P no vacía. Definimos y denotamos la *cerradura* de $\mathcal{A}$ como

$$\mathrm{cl}(\mathcal{A}) = \{A \subseteq P \mid \exists B \in \mathcal{A} : B \subseteq A\}.$$

Sea $A \in \mathrm{cl}(\mathcal{A})$ y $C \subseteq P$ tal que $A \subseteq C$. Como $A \in \mathrm{cl}(\mathcal{A})$, entonces existe $B \in \mathcal{A}$ tal que $B \subseteq A \subseteq C$, es decir, $B \subseteq C$, de donde $C \in \mathrm{cl}(\mathcal{A})$, así que $\mathrm{cl}(\mathcal{A})$ es una familia monótona creciente no vacía de subconjuntos, por consiguiente $\mathrm{cl}(\mathcal{A})$ es la estructura de acceso más pequeña que contiene a $\mathcal{A}$.

Ejemplo 2.4. Sea $\mathcal{A} = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}\}$. Por el Ejemplo 2.2 sabemos que $\mathrm{cl}(\mathcal{A}) = \Gamma$.

Sean p_0 una entidad, P un conjunto finito tal que $p_0 \notin P$ y $\Gamma \subseteq \mathcal{P}(P)$ una estructura de acceso. Un *esquema de compartición de secretos con estructura de acceso* Γ es un método que p_0 puede usar para repartir información del secreto k en privado a cada elemento de P de manera que un subconjunto de P puede conocer el secreto si y sólo si el subconjunto pertenece a Γ. A p_0 lo llamamos el *distribuidor* y los elementos del conjunto P son los *participantes*. El *fragmento* de un participante es la información que recibió por parte del

distribuidor. Nos referimos a Γ como la *estructura de acceso* del esquema de compartición de secretos.

Los esquemas de compartición de secretos se emplean normalmente cuando hay falta de confianza en una sola persona o cuando la responsabilidad de una sola persona debe delegarse a un grupo durante la ausencia de dicha persona [13]. La compartición de secretos también puede verse como una posesión colectiva de un secreto por un conjunto de personas que tienen fragmentos de él [13].

Decimos que el esquema de compartición de secretos es *perfecto* respecto a Γ si se verifican las siguientes condiciones [9]:

(P1) Si los participantes de un subconjunto autorizado A reúnen sus fragmentos, entonces los participantes de A pueden determinar el valor de k.

(P2) Si los participantes de un subconjunto no autorizado A reúnen sus fragmentos, entonces ellos no pueden obtener ninguna información sobre el valor de k, incluso con un número infinito de recursos computacionales.

Un esquema de compartición de secretos es *ideal* si es perfecto y, además, el conjunto de fragmentos coincide con el conjunto de secretos.

Brickell y Davenport [8] presentan una casi-caracterización de esquemas de compartición de secretos ideales mediante matroides representables conexos. La información expuesta en este capítulo se basa principalmente en [8] y en [2].

Como primer paso daremos definiciones más precisas, matemáticamente hablando, de los conceptos que ya introdujimos al inicio de este apartado.

2.2. Esquemas de compartición de secretos

Definición 2.5. Sean $P = \{p_1, \ldots, p_n\}$ un conjunto de participantes y $p_0 \notin P$ un participante especial al que llamaremos *distribuidor*. Sean $\mathcal{K}$ un conjunto de secretos y $\mathcal{S}$ un conjunto de fragmentos que el distribuidor p_0 puede repartir a cada uno de los participantes del conjunto P. Un *esquema de distribución con conjunto de secretos $\mathcal{K}$ y conjunto de fragmentos $\mathcal{S}$* es una matriz M con las siguientes características:

i. tiene $n + 1$ columnas que se identifican con los $n + 1$ elementos de $\{p_0, p_1, \ldots, p_n\}$ (en el mismo orden);

ii. las entradas de la columna p_0 pertenecen a $\mathcal{K}$ y las entradas de las columnas correspondientes a los elementos de P se toman de $\mathcal{S}$;

III. no existen filas repetidas y cada elemento de $\mathcal{K}$ aparece al menos una vez en la columna p_0;

IV. para cada $k \in \mathcal{K}$ existe una distribución de probabilidad Π_k sobre las filas en las que aparece k en la columna correspondiente a p_0.

Denotaremos el conjunto de vectores fila de M con $\mathcal{F}$. Nos referiremos a la primera columna como la *columna del distribuidor*. Aunque no se mencione explícitamente, de ahora en adelante entenderemos que $p_0 \notin P$ denota al distribuidor.

Sea M un esquema de distribución. Denotamos con $M(r, p)$ a la entrada de la fila r y la columna p de la matriz M. Definimos

$$s(p) = \{M(r, p) : r \in \mathcal{F}\},$$

es decir, $s(p)$ es el conjunto de entradas de la columna p y $s(p_0) = \mathcal{K}$. Si r es una fila tal que $M(r, p_0) = k_0$ decimos que r *corresponde al valor secreto* k_0. Sea $A \subseteq P \cup p_0$. Escribimos $M(r, A)$ para referirnos a la fila r de M restringida a las columnas indexadas por A y lo llamamos el *vector de fragmentos para* A *correspondiente a la fila* r o simplemente *vector de fragmentos para* A si no es necesario indicar la fila de la que se obtuvo.

El inciso IV de la Definición 2.5 permite que exista cualquier distribución de probabilidad entre las filas que corresponden al mismo valor secreto. Sin embargo, nosotros trabajaremos sólo con esquemas en los cuales para cada $k \in \mathcal{K}$, Π_k es la distribución uniforme. Cuando el distribuidor quiere repartir un secreto $\alpha \in s(p_0)$, elige una fila r de la matriz correspondiente al valor secreto α usando la distribución uniforme sobre todas las filas correspondientes al mismo valor secreto α, y otorgando a cada $p \in P$ la entrada $M(r, p)$ como fragmento. La matriz M es de conocimiento público, pero la elección de r del distribuidor es privada.

Consideremos un conjunto de participantes $A \subseteq P$. Cada participante $a \in A$ recibió del distribuidor un fragmento, que denotaremos por α_a. Si los participantes de A reúnen su información, ellos sabrán que el distribuidor eligió una fila r en la que, para cada $a \in A$, $M(r, a) = \alpha_a$. Sin embargo, un esquema de distribución aún no nos permite garantizar que en efecto los conjuntos seleccionados pueden conocer el secreto y que los conjuntos restantes no tienen acceso a él. Para ello necesitamos pedirle algunas condiciones más.

Definición 2.6. Sean P un conjunto de participantes, $p_0 \notin P$ el distribuidor, Γ una estructura de acceso sobre P y M un esquema de distribución con conjunto de secretos $\mathcal{K}$ y conjunto de fragmentos $\mathcal{S}$. Decimos que M es un *esquema de compartición de secretos débilmente perfecto que materializa la estructura de acceso* Γ si se verifican las siguientes dos condiciones:

I. *Regularidad*. Si $A \in \Gamma$ se cumple que:

$$\forall r, r' \in \mathcal{F} : M(r, A) = M(r', A) \Rightarrow M(r, p_0) = M(r', p_0). \tag{2.1}$$

II. *Privacidad débil*. Para todo $B \notin \Gamma$ se verifica lo siguiente:

$$\forall r \in \mathcal{F}\ \forall \alpha \in \mathcal{K}\ \exists r' \in \mathcal{F} : M(r', B) = M(r, B)\ \wedge\ M(r', p_0) = \alpha. \tag{2.2}$$

Si M es un esquema de compartición de secretos que materializa la estructura de acceso Γ sobre P, en ocasiones simplemente diremos que M es un esquema con estructura de acceso Γ y conjunto de participantes P. Un participante que no pertenece a ningún elemento de Γ_0 lo llamamos *innecesario* o *redundante*. Decimos que un esquema de compartición de secretos es *conexo* y que su estructura de acceso es *conexa* si ningún participante $p \in P$ es innecesario, es decir, si todo participante $p \in P$ pertenece a algún elemento de Γ_0.

La condición de regularidad de la Definición 2.6 es la formalización de la propiedad (P1) que mencionamos en el apartado 2.1: si los elementos de un conjunto autorizado A reúnen sus fragmentos, puede que encuentren varias filas que generan los mismos vectores de fragmentos para A, pero todas ellas corresponden al mismo valor secreto, así que existe certidumbre de cuál es el valor del secreto que tiene el distribuidor.

El requisito de privacidad débil de la Definición 2.6 corresponde a la propiedad (P2) e indica que si los miembros de un conjunto no autorizado B reúnen sus fragmentos, entonces para toda fila r y para cada posible valor del secreto α existirá al menos una fila r' que genere el mismo vector de fragmentos para B que la fila r y tal que la fila r' corresponda al valor secreto α, lo cual implica que un conjunto no autorizado no conoce el valor secreto y tampoco puede descartar ningún valor de $\mathcal{K}$ como el valor que repartió p_0.

Existe otra propiedad que exige más que la condición de privacidad débil. Diremos que M es un esquema de compartición de secretos que verifica la condición de *privacidad fuerte* o que es *fuertemente perfecto* si verifica (P1) y la siguiente propiedad:

(P2**) Si $B \notin \Gamma$ y $f\colon B \to \mathcal{S}$ es cualquier función, entonces existe un entero no negativo $\lambda(f, B)$ tal que

$$\lambda(f, B) = |\{r \in \mathcal{F}\colon \{(b, M(r, b))\colon b \in B\} = \{(b, f(b)) : b \in B\} \text{ y } M(r, p_0) = k\}|$$

independiente del valor de k.

Consideremos un conjunto no autorizado B, f una función que asigna a cada miembro de B un fragmento de $\mathcal{S}$ y $k \in \mathcal{K}$. Si el esquema de compartición de secretos es fuertemente perfecto, para la función f el número de filas que asignan a los elementos de B los mismos valores que f y que al participante especial p_0 le asignan el valor k, es el mismo para todos

los elementos de $\mathcal{K}$, a diferencia del caso de los esquemas débilmente perfectos, en los cuales sabemos que todos los elementos de $\mathcal{K}$ son posibles, pero el número de filas que coinciden en $A \cup p_0$ no necesariamente es el mismo para cada cada valor posible de k.

Observemos que la clase de los esquemas débilmente perfectos contiene a la clase de los esquemas fuertemente perfectos. Así que los resultados que se establecen para esquemas débilmente perfectos también son válidos para esquemas fuertemente perfectos. En el Ejemplo 2.7 probaremos que la condición de débilmente perfecto no implica la de fuertemente perfecto.

Ejemplo 2.7 ([9, Ejemplo 1.1]). Sea $P = \{a, b\}$. La matriz M es un esquema de compartición de secretos con estructura de acceso $\Gamma = \{\{a, b\}\}$, conjunto de secretos $\mathcal{K} = \{0, 1\}$ y conjunto de fragmentos $\mathcal{S} = \{0, 1, 2\}$:

$$M = \begin{array}{c} \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_7 \\ r_8 \end{array} \begin{array}{c} \begin{array}{ccc} p_0 & a & b \end{array} \\ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 2 \\ 1 & 2 & 1 \end{bmatrix} \end{array}$$

El conjunto $\{a\}$ no es autorizado. Supongamos que el fragmento que recibió a por parte de p_0 es 0. Las filas que corresponden a este fragmento son r_1, r_2, r_5; en las primeras dos el valor del secreto es 0 y en r_5 es 1, así que a no puede determinar cuál es el valor secreto que repartió p_0. Sin embargo, cuando b comparte su fragmento es posible conocer el secreto; si b recibió como fragmento 1 o 2, entonces el valor secreto es 0 y si b tiene como fragmento a 0, entonces el valor secreto es 1. Podemos continuar este análisis y concluir que M es débilmente perfecto. Además, tenemos que

$$|\{r \in \mathcal{F} : (a, M(r, a)) = (a, 0) \text{ y } M(r, p_0) = 0\}| = |\{r_1, r_2\}| = 2,$$
$$|\{r \in \mathcal{F} : (a, M(r, a)) = (a, 0) \text{ y } M(r, p_0) = 1\}| = |\{r_5\}| = 1.$$

Como los valores anteriores no coinciden entonces M no es un esquema fuertemente perfecto.

Ejemplo 2.8 ([9, Ejemplo 3.1]). Sean $P = \{a, b, c, d, e, f\}, \Gamma_0 = \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, a\}\}$, $\Gamma = \text{cl}(\Gamma_0)$, $\mathcal{K} = \{0, 1\}$ y $\mathcal{S} = \{0, 1, 2\}$. La siguiente matriz M es un esquema

de compartición de secretos con estructura de acceso Γ.

$$M = \begin{array}{c} \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_7 \\ r_8 \\ r_9 \\ r_{10} \\ r_{11} \\ r_{12} \end{array} \begin{array}{c} \begin{array}{ccccccc} p_0 & a & b & c & d & e & f \end{array} \\ \left[\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 2 & 2 \\ 0 & 2 & 2 & 0 & 0 & 1 & 1 \\ 0 & 2 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 & 2 & 0 \\ 1 & 0 & 2 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 2 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 2 & 2 & 1 \\ 1 & 2 & 0 & 0 & 1 & 1 & 2 \\ 1 & 2 & 1 & 1 & 0 & 0 & 2 \end{array}\right] \end{array}$$

Hemos indicado que $\{a, b\}$ es un conjunto autorizado. Observamos que las parejas de filas $\{r_1, r_2\}$, $\{r_3, r_4\}$ y $\{r_5, r_6\}$ otorgan los mismos fragmentos a a y a b y, en efecto, cada una de dichas parejas coinciden en el valor de p_0. Por otro lado, el conjunto $\{a, c\}$ es un conjunto no autorizado. Si denotamos con s_a y s_c los fragmentos correspondientes a a y a c, respectivamente, entonces para cada vector de fragmentos (s_a, s_c) existe exactamente una fila r tal que $M(r, \{a, c\}) = (s_a, s_c)$ y $M(r, p_0) = 0$ y exactamente una fila t donde $M(t, \{a, c\}) = (s_a, s_c)$ y $M(t, p_0) = 1$. Así que, empleando la notación de la propiedad (P2**), tenemos que

$$\lambda(f, \{a, c\}) = |\{r \in \mathcal{F} \colon \{(a, M(r, a)), (c, M(r, c))\} = \{(a, f(a)), (c, f(c))\} \text{ y } M(r, p_0) = k\}|,$$

y $\lambda(f, \{a, c\}) = 1$, independientemente del valor de k, si existe un vector de fragmentos (s_a, s_c) en M tal que $(f(a), f(c)) = (s_a, s_c)$ (como es el caso de la función $f(a) = 0$, $f(c) = 1$), y $\lambda(f, \{a, c\}) = 0$ en caso contrario (como ocurre para la función $f(a) = 0$, $f(c) = 0$), y puede comprobarse que lo mismo ocurre para todos los conjuntos no autorizados. Concluimos que M es un esquema de compartición de secretos fuertemente perfecto.

En lo sucesivo cuando hagamos referencia a un esquema perfecto estaremos hablando de un esquema débilmente perfecto.

Las primeras construcciones de esquemas perfectos fueron dadas por Blakley [4] y Shamir [23]. En el siguiente ejemplo comentaremos brevemente el esquema de Shamir.

Ejemplo 2.9 ([2, Ejemplo 2.4]). Sean $P = \{p_1, \ldots, p_n\}$ y t y n dos números naturales tales

que $t \leq n$. Definimos la estructura de acceso

$$\Gamma_{t,n} = \{A \subseteq P : |A| \geq t\}.$$

Elegimos un número primo $q > n$ y definimos un esquema de compartición de secretos con conjunto de secretos $\mathbb{F}_q$ como sigue. Para repartir un secreto $k \in \mathbb{F}_q$, el distribuidor elige de manera aleatoria, empleando la distribución uniforme, un polinomio Q de grado menor o igual a $t-1$ sobre $\mathbb{F}_q$ tal que $Q(0) = k$. El distribuidor otorga a cada participante $p_i \in P$ el fragmento $Q(i)$. Si los elementos de un conjunto autorizado A reúnen sus fragmentos, entonces tendrán un número mayor o igual a t puntos distintos del polinomio Q de grado $t-1$, y por el Teorema de Interpolación de Lagrange para campos finitos los elementos de A pueden determinar Q y calcular $k = Q(0)$. Si B es un conjunto no autorizado, entonces los elementos de B tendrían un número de fragmentos menor a t, así que para todo $k \in \mathbb{F}_q$ existe el mismo número de polinomios que pasan por los fragmentos de los participantes de B y el punto $(0, k)$. Por lo tanto, B no tiene información sobre el secreto. Dado que para cada $k \in \mathbb{F}_q$ existen q^{t-1} polinomios de grado a lo más $t-1$ sobre $\mathbb{F}_q$ con término independiente $k = Q(0)$, entonces en este esquema, para cada $k \in \mathbb{F}_q$ existen q^{t-1} filas correspondientes al valor secreto k. Por lo tanto, la matriz M tiene q^t filas, y cada una de estas filas es de la forma

$$(k, Q(1), Q(2), \ldots, Q(n)).$$

La estructura de acceso $\Gamma_{t,n}$ del Ejemplo 2.9 se llama (t, n)-*estructura de acceso umbral* o *estructura de acceso umbral* t de n.

Ito, Saito y Nishizeki [16] fueron los primeros en trabajar con esquemas de compartición de secretos con estructuras de acceso más generales, no solamente las umbrales. Demostraron que para toda familia monótona creciente Γ existe un esquema de compartición de secretos perfecto con estructura de acceso Γ. Esta prueba es, además, constructiva. Benaloh y Leichter [3] describieron una manera más eficiente de materializar estructuras de acceso. El problema con estas dos construcciones es que la mayoría de los esquemas generados requieren fragmentos de tamaño exponencial y, como veremos más adelante, queremos obtener esquemas para los cuales los fragmentos tengan el menor tamaño posible. Por ello estamos interesados en la construcción de esquemas mediante otros métodos de manera que se optimice el tamaño de los fragmentos.

Para finalizar este apartado, introducimos algunos términos más, y principalmente establecemos el significado de diversos símbolos que nos facilitarán expresar ciertos conceptos en las secciones posteriores.

Consideremos un esquema de compartición de secretos M con estructura de acceso Γ y

conjunto de participantes P. La Definición 2.10 es muy similar a la condición de privacidad débil, pero nótese que para esta definición el conjunto A puede o no ser autorizado y el punto b, que en la condición de privacidad débil únicamente podía ser igual a p_0, en la Definición 2.10 puede ser cualquier participante que no pertenece a A.

Definición 2.10 ([8]). Sea $A \subseteq P \cup p_0$ y $b \in (P \setminus A) \cup p_0$. Decimos que A *no tiene información sobre* b, lo cual denotamos por $A \not\to b$, si

$$\forall r \in \mathcal{F}\ \forall \alpha \in \mathcal{S}\ \exists r' \in \mathcal{F} : M(r', A) = M(r, A)\ \wedge\ M(r', b) = \alpha. \tag{2.3}$$

En otro caso decimos que A *tiene alguna información sobre* b, y lo denotamos por $A \to b$. Entonces $A \to b$ si

$$\exists r \in \mathcal{F}\ \exists \alpha \in \mathcal{S}\ \forall t \in \mathcal{F} : M(r, A) = M(t, A) \Rightarrow M(t, b) \neq \alpha.$$

En (2.3), si $b = p_0$ el conjunto de fragmentos $\mathcal{S}$ lo interpretamos como el conjunto de secretos $\mathcal{K}$.

Definición 2.11 ([8]). Sea $A \subseteq P \cup p_0$ y $b \in P \cup p_0$. Decimos que A *conoce* a b, lo cual denotamos por $A \Longrightarrow b$, si

$$\forall r, r' \in \mathcal{F} : M(r, A) = M(r', A) \Rightarrow M(r, b) = M(r', b),$$

es decir, si a todas las filas que generan el mismo vector de fragmentos para A les corresponde el mismo valor para b. Si A no conoce a b escribimos $A \not\Longrightarrow b$.

Por la Definición 2.11, podemos describir la estructura de acceso de M como

$$\Gamma = \{A \subseteq P : A \Longrightarrow p_0\},$$

y por la Definición 2.10 podemos interpretar un esquema perfecto como aquél en el que para todo $A \subseteq P$, $A \to p_0$ implica que $A \Longrightarrow p_0$, es decir, si un conjunto sabe algo acerca del secreto k entonces sabe el valor de k.

Generalizamos la noción de conocer a un participante a la de conocer a un conjunto de participantes como explicamos a continuación.

Definición 2.12. Sean $A, B \subseteq P \cup p_0$. Decimos que A *conoce* a B si y sólo si

$$\forall r, r' \in \mathcal{F} : M(r, A) = M(r', A) \Rightarrow M(r, B) = M(r', B),$$

lo cual denotamos por $A \Longrightarrow B$.

El Lema 2.13 es un resultado inmediato de la Definición 2.12. Nos dice que la propiedad de conocer a un conjunto es transitiva.

Lema 2.13. *Sean $A, B, C \subseteq P \cup p_0$. Si $A \Longrightarrow B$ y $B \Longrightarrow C$, entonces $A \Longrightarrow C$.*

Demostración.

Sean $r, r' \in \mathcal{F}$ tales que $M(r, A) = M(r', A)$. Como $A \Longrightarrow B$, entonces $M(r, B) = M(r', B)$ y dado que $B \Longrightarrow C$ tenemos que $M(r, C) = M(r', C)$. Concluimos que $A \Longrightarrow C$. □

2.3. Esquemas de compartición de secretos ideales

Karnin, Greene y Hellman [17] demostraron que en un esquema de compartición de secretos M la cardinalidad del conjunto de fragmentos es mayor o igual que la cardinalidad del conjunto de secretos. En la práctica, la situación "ideal" se presenta cuando el tamaño de los fragmentos es el más pequeño posible, ya que eso significa que el distribuidor no ha tenido que repartir una gran cantidad de información a los participantes. El primero en introducir el concepto de estructura de acceso ideal fue Brickell en [7]. Nosotros presentamos a continuación una definición alternativa.

Definición 2.14 ([2])**.** Sea M un esquema de compartición de secretos perfecto con conjunto de participantes P, conjunto de secretos $\mathcal{K}$ y conjunto de fragmentos $\mathcal{S}$. Decimos que M es *ideal* si para todo $p \in P$, $s(p) = \mathcal{S} = \mathcal{K}$. Una estructura de acceso Γ es *k-ideal* si existe un esquema de compartición de secretos ideal que materializa dicha estructura con conjunto de secretos $\mathcal{K}$ de cardinalidad k. Una estructura de acceso es *ideal* si es k-ideal para algún $k \geq 2$.

Sea M un esquema de compartición de secretos ideal con conjunto de secretos y fragmentos $\mathcal{K}$. Con frecuencia diremos simplemente que M es un esquema ideal. Dado que M es en particular un esquema de distribución ya sabíamos que cada elemento de $\mathcal{K}$ aparece al menos una vez en la columna correspondiente al distribuidor p_0, y por la condición de ideal ahora sabemos también que cada elemento de $\mathcal{K}$ aparece al menos una vez en cada columna de la matriz M.

Definición 2.15. Sea M un esquema de compartición de secretos ideal con conjunto de participantes P y $A \subseteq P$. Decimos que A es un conjunto *redundante* si existe $y \in A$ tal que $A \setminus y \Longrightarrow y$. Denotaremos a la familia de conjuntos redundantes respecto a M por $\mathcal{R}(M)$.

La palabra redundante fue elegida *ad hoc*, ya que podemos decir que en un conjunto redundante existen participantes superfluos, pues los elementos restantes pueden conocer el fragmento que el distribuidor p_0 les había repartido a cada uno de ellos. En este punto empezamos a notar cierta relación de dependencia en los conjuntos, lo cual es crucial para establecer la conexión con matroides.

2.4. Esquemas de compartición de secretos ideales conexos

Consideremos un esquema de compartición de secretos conexo ideal M con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$. Sean $q = |\mathcal{S}|$ y $A \subseteq P \cup p_0$. Sea $\sim_A$ la relación definida en $\mathcal{F}$ por

$$r \sim_A r' \Leftrightarrow M(r, A) = M(r', A).$$

Claramente $\sim_A$ es una relación de equivalencia, y por lo tanto, induce una partición sobre $\mathcal{F}$. Sea $\mathcal{A}$ un conjunto completo de representantes respecto de $\sim_A$. Definimos el conjunto

$$s(A) = \{M(r, A) : r \in \mathcal{A}\},$$

es decir, $s(A)$ es el conjunto de vectores de fragmentos para A. Definimos

$$\#A = |s(A)|.$$

$\#A$ es el número de clases de equivalencia en $\mathcal{F}/\sim_A$ y el número de vectores de fragmentos distintos para A. Notemos que para todo $A \subseteq P \cup p_0$ siempre se verifica que

$$\#A \leq q^{|A|}. \tag{2.4}$$

Además, si $A \subseteq B$, entonces $\#A \leq \#B$, ya que pueden existir filas que sean iguales al restringirlas a los participantes de A, pero que sean distintas en alguna de las columnas correspondientes a los participantes de $B \setminus A$. Es importante tener presentes estas observaciones ya que las emplearemos frecuentemente en las demostraciones de los resultados del presente capítulo.

El siguiente lema nos dice que si un conjunto A conoce a un participante p, entonces el número de vectores de fragmentos para $A \cup p$ no cambia respecto al número de vectores de fragmentos para A, y que, más aún, el recíproco también se verifica: si el número de vectores de fragmentos para un conjunto $A \cup p$ es igual que el número de vectores de fragmentos para A, entonces el conjunto A conoce a p.

Lema 2.16 ([8, Lema 1]). *Sea M un esquema de compartición de secretos ideal conexo M con conjunto de participantes P. Sea $A \subseteq P \cup p_0$ y $p \in P \cup p_0$. Si $A \Longrightarrow p$, entonces $\#(A \cup p) = \#A$, y recíprocamente, si $\#(A \cup p) = \#A$, entonces $A \Longrightarrow p$.*

Demostración.

Sea $\phi : s(A) \to s(A \cup p)$ definida por $\phi(M(r, A)) = M(r, A \cup p)$. La función ϕ está bien definida ya que, aunque pueden existir varias filas que restringidas a los elementos de A sean iguales, al considerarlas como elementos de $s(A)$ estamos fijando un representante de cada clase de equivalencia. Sean $r, t \in \mathcal{A}$ tales que $\phi(M(r, A)) = \phi(M(t, A))$, entonces

$M(r, A \cup p) = M(t, A \cup p)$, en particular $M(r, A) = M(t, A)$. Por lo tanto, ϕ es una función inyectiva. Ahora, sea $M(t, A \cup p) \in s(A \cup p)$. Puede que $t \notin \mathcal{A}$, pero existe $r \in \mathcal{A}$ tal que $[t]_{\sim_A} = [r]_{\sim_A}$, o equivalentemente, $M(t, A) = M(r, A)$. Como $A \Longrightarrow p$, entonces $M(t, p) = M(r, p)$, en resumen, $M(t, A \cup p) = M(r, A \cup p) = \phi(M(r, A))$, y por lo tanto, ϕ es sobreyectiva. Concluimos que ϕ es una biyección y por lo tanto, $|s(A)| = |s(A \cup p)|$, es decir, $\#A = \#(A \cup p)$.

Ahora supongamos que $A \not\Longrightarrow p$, entonces existen dos filas r, t tales que $[r]_{\sim_A} = [t]_{\sim_A}$ y que $M(r, p) \neq M(t, p)$, entonces $\#(A \cup p) > \#A$. Por lo tanto, si $\#(A \cup p) = \#A$, entonces $A \Longrightarrow p$. □

El Lema 2.17 asegura que si A no es un conjunto autorizado pero $A \cup p$ sí lo es, entonces el conjunto $A \cup p_0$ conoce al participante p.

Lema 2.17 ([8, Lema 2]). *Sea M un esquema de compartición de secretos ideal conexo M con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$. Sea $A \subseteq P$ y $p \in P$. Si $A \not\Longrightarrow p_0$ y $A \cup p \Longrightarrow p_0$, entonces $A \cup p_0 \Longrightarrow p$.*

Demostración.

M es un esquema de compartición de secretos ideal, en particular, M es perfecto, así que, si $A \not\Longrightarrow p_0$, entonces $A \not\to p_0$, es decir, que

$$\forall r \in \mathcal{F}\ \forall \alpha \in \mathcal{S}\ \exists t \in \mathcal{F} : M(r, A) = M(t, A)\ \wedge\ M(t, p_0) = \alpha. \tag{2.5}$$

Dado que $A \cup p \Longrightarrow p_0$, entonces

$$\forall r, t \in \mathcal{F} : M(r, A \cup p) = M(t, A \cup p) \Rightarrow M(r, p_0) = M(t, p_0). \tag{2.6}$$

Para demostrar que $A \cup p_0 \Longrightarrow p$ es necesario verificar que

$$\forall r, t \in \mathcal{F} : M(r, A \cup p_0) = M(t, A \cup p_0) \Rightarrow M(r, p) = M(t, p).$$

Así pues, sean $t_1, t_2 \in \mathcal{F}$ tales que $M(t_1, A \cup p_0) = M(t_2, A \cup p_0)$. Definimos

$$\mathcal{S}^* = \{\alpha \in \mathcal{S} \mid \exists r \in \mathcal{F} : [r]_{\sim_A} = [t_1]_{\sim_A}\ \wedge\ M(r, p) = \alpha\}. \tag{2.7}$$

Si definimos $\alpha_0 = M(t_1, p)$, entonces claramente $\alpha_0 \in \mathcal{S}^*$, por lo que $\mathcal{S}^* \neq \emptyset$. Sea $\phi : \mathcal{S}^* \to \mathcal{S}$ definida por $\phi(\alpha) = M(r, p_0)$, donde r es una de las filas que existen por (2.7). Veamos que ϕ está bien definida. Sea $\alpha \in \mathcal{S}^*$. Por (2.7) existe al menos una fila r tal que $M(r, A) = M(t_1, A)$ y $M(r, p) = \alpha$. Supongamos que existe otra fila t tal que $M(t, A) = M(t_1, A)$ y $M(t, p) = \alpha$, entonces $M(r, A \cup p) = M(t, A \cup p)$, luego, por (2.6), $M(t, p_0) = M(r, p_0)$. Así que la imagen de α bajo ϕ está bien definida. Sea $\gamma \in \mathcal{S}$. Por (2.5) existe una fila r tal que $M(r, A) = M(t_1, A)$ y $M(r, p_0) = \gamma$. Sea $\alpha = M(r, p)$. Claramente $\gamma = \phi(\alpha)$. Concluimos que ϕ es sobreyectiva, de donde $|\mathcal{S}| \leq |\mathcal{S}^*|$, y dado que por definición $\mathcal{S}^* \subseteq \mathcal{S}$, concluimos que $\mathcal{S}^* = \mathcal{S}$. Como

ϕ es una función sobreyectiva de un conjunto finito en él mismo, sabemos que ϕ también es inyectiva. Ahora, como t_1 y t_2 son tales que $M(t_1, A \cup p_0) = M(t_2, A \cup p_0)$ entonces $M(t_1, A) = M(t_2, A)$ y $M(t_1, p_0) = M(t_2, p_0)$. Notemos que $M(t_1, p), M(t_2, p) \in \mathcal{S}^*$, y dado que ϕ es inyectiva tenemos que $M(t_1, p) = M(t_2, p)$, ya que estas últimas son las preimágenes bajo ϕ de $M(t_1, p_0)$ y $M(t_2, p_0)$, respectivamente. De aquí que $A \cup p_0 \Longrightarrow p$. □

Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$, y sean $q = |\mathcal{S}|$, $A \subseteq P \cup p_0$. Hasta el momento no hemos establecido algún resultado que nos permita hallar el número $\#A$, pero nos ocuparemos de ello a continuación: veremos que $\#A$ siempre es una potencia de q. La demostración de este resultado es extensa, así que la realizaremos por casos dependiendo de la naturaleza del conjunto. Durante esta sección también se hará más evidente la importancia y utilidad que tiene la condición de ideal de nuestro esquema de compartición de secretos M.

Lema 2.18 ([8, Lema 3]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Sea $A \subseteq P$ y $p \in P$. Si $A \not\Longrightarrow p_0$ y $A \cup p \Longrightarrow p_0$, entonces $\#(A \cup p) = q(\#A)$.*

Demostración.

Sea r una fila de M. Como $A \not\Longrightarrow p_0$ y M es perfecto, entonces $A \not\to p_0$, de manera que para dicha fila r y para todo $\alpha \in \mathcal{S}$, existe una fila r_α tal que $M(r_\alpha, A) = M(r, A)$ y $M(r_\alpha, p_0) = \alpha$. Para $\beta \in \mathcal{S}$ existe una fila r_β tal que $M(r_\beta, A) = M(r, A)$ y $M(r_\beta, p_0) = \beta$. Si $M(r_\alpha, p) = M(r_\beta, p)$, entonces $M(r_\alpha, A \cup p) = M(r_\beta, A \cup p)$, y dado que $A \cup p \Longrightarrow p_0$ esto implica que $M(r_\alpha, p_0) = M(r_\beta, p_0)$, es decir, $\alpha = \beta$. Tenemos, pues, que siempre que tomamos valores distintos para $\alpha, \beta \in \mathcal{S}$, obtenemos distintos fragmentos para el participante p en las filas r_α y r_β. Concluimos que para toda fila r y para todo $\alpha \in \mathcal{S}$ existe una fila r_α tal que $M(r_\alpha, A) = M(r, A)$ y $M(r_\alpha, p) = \alpha$, y dado que $|\mathcal{S}| = q$, entonces $\#(A \cup p) = q(\#A)$. □

Anteriormente mencionamos que para cualquier conjunto A se verifica la desigualdad $\#A \leq q^{|A|}$. El siguiente lema afirma que si A es un conjunto autorizado minimal, entonces la igualdad se verifica.

Lema 2.19 ([8, Lema 4]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Si $A \in \Gamma_0$, entonces $\#A = q^{|A|}$.*

Demostración.

Sea $A = \{x_1 \ldots, x_k\} \in \Gamma_0$. Supongamos que existe un multiconjunto $\Delta = \{\alpha_1, \ldots, \alpha_k\} \subseteq \mathcal{S}$ tal que ninguna fila r verifica que $M(r, x_i) = \alpha_i$, para cada $i \in [k]$. Sea $j \in [k - 1]$

el mayor entero tal que existe un subconjunto $\{x^{(1)}, \ldots, x^{(j)}\} \subseteq A$, existe un multiconjunto $\{\alpha^{(1)}, \ldots, \alpha^{(j)}\} \subseteq \Delta$ y existe una fila r tal que $M(r, \{x^{(1)}, \ldots, x^{(j)}\}) = (\alpha^{(1)}, \ldots, \alpha^{(j)})$. Como M es ideal, todos los elementos de $\mathcal{S}$ aparecen en la columna de $x^{(1)}$, por lo que, en efecto, $j \geq 1$. Sean $x \in A \setminus \{x^{(1)}, \ldots x^{(j)}\}$ y $\alpha \in \Delta \setminus \{\alpha^{(1)}, \ldots, \alpha^{(j)}\}$. Sea $t \in \mathcal{F}$ tal que $M(t, \{x^{(1)}, \ldots, x^{(j)}\}) = M(r, \{x^{(1)}, \ldots, x^{(j)}\})$. Si $M(t, x) = \alpha$, t sería una fila que restringida al conjunto $\{x^{(1)}, \ldots, x^{(j)}, x\}$ de $j+1$ elementos es igual a una $(j+1)$-ada de elementos de Δ, pero j es el mayor entero que verifica esto. Así que $M(t, x) \neq \alpha$, de aquí que $\{x^{(1)}, \ldots, x^{(j)}\} \to x$. Por lo tanto, $A \setminus x \to p_0$, y como M es perfecto, tenemos que $A \setminus x \Longrightarrow p_0$, lo cual contradice que $A \in \Gamma_0$. Entonces para cualquier arreglo $(\alpha_1, \ldots, \alpha_k) \in \mathcal{S}^k$ que consideremos podemos encontrar una fila r de M tal que $M(r, A) = (\alpha_1, \ldots, \alpha_k)$, de donde obtenemos que $\#A = q^k = q^{|A|}$. □

En el siguiente resultado veremos que si un conjunto A no es autorizado, entonces no se verificará la igualdad de la conclusión del Lema 2.19, sin embargo, sí se verifica que $\#A$ es una potencia de q.

Lema 2.20 ([8, Lema 5]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Si A es un subconjunto de P no vacío tal que $A \not\Longrightarrow p_0$, entonces $\#A = q^n$, para algún $n \in \mathbb{N}$.*

Demostración.

Supongamos que existe algún conjunto no autorizado no vacío que no satisface la conclusión del lema, entonces podemos elegir un conjunto A tal que $A \not\Longrightarrow p_0$ y $\#A$ no es una potencia de q y que es minimal en este sentido. Sea $k = |A|$ y sea $a \in A$. Como M es conexo, existe $C_a \in \Gamma_0$ tal que $a \in C_a$, y dado que $C_a = (C_a \cap A) \cup (C_a \setminus A) \subseteq A \cup (C_a \setminus A)$, entonces $A \cup (C_a \setminus A)$ contiene un conjunto autorizado, luego $A \cup (C_a \setminus A) \Longrightarrow p_0$. Además, puesto que $a \in C_a \cap A$, tenemos que $C_a \setminus A \subsetneq C_a$ y como C_a es un conjunto autorizado minimal entonces $C_a \setminus A \not\Longrightarrow p_0$. Sea $B \subseteq C_a \setminus A \subseteq P \setminus A$ minimal tal que $A \cup B \Longrightarrow p_0$ y para todo $b \in B$, $(A \cup B) \setminus b \not\Longrightarrow p_0$. Como $B \subseteq C_a \setminus A$ y $C_a \setminus A \not\Longrightarrow p_0$, entonces $B \not\Longrightarrow p_0$. Si $\#(A \cup B) = q^{|A \cup B|}$, dado que A y B son disjuntos, esto obliga a que $\#A = q^{|A|}$, lo cual contradice lo supuesto, y como sabemos que $\#(A \cup B) \leq q^{|A \cup B|}$, entonces debe ocurrir que $\#(A \cup B) < q^{|A \cup B|}$.

Demostraremos a continuación que, para todo $a \in A$, $\#(A \setminus a) = q^{|A|-1}$. Sea $n \in \mathbb{N}$ tal que

$$q^n < \#A < q^{n+1}. \tag{2.8}$$

Sea $a \in A$. Como A es un conjunto no autorizado tal que $\#A$ no es una potencia de q y es minimal con esta propiedad, entonces si B es un subconjunto propio de A, $\#B$ es una potencia de q. En particular, para todo $a \in A$, $\#(A \setminus a)$ es una potencia de q. Si

$\#(A \setminus a) < q^n$ entonces $\#(A \setminus a) \leq q^{n-1}$, de donde $\#A \leq q^n$, lo cual no ocurre, entonces $\#(A \setminus a) \geq q^n$, y como $q^n \leq \#(A \setminus a) \leq \#A < q^{n+1}$, concluimos que $\#(A \setminus a) = q^n$. Sabemos que $q^n = \#(A \setminus a) \leq q^{|A \setminus a|} = q^{k-1}$, entonces $n \leq k-1$. Dado que para todo subconjunto propio B de A, $\#B$ es una potencia de q, si suponemos que $n < k-1$, entonces existe $j \in [k-2]$, y existen $a_1, \ldots, a_j, a_{j+1} \in A$ tales que $\#(\{a_1, \ldots, a_j\}) = \#(\{a_1, \ldots, a_j, a_{j+1}\})$, así que $\#(A \setminus a_{j+1}) = \#A$, pero eso contradice la minimalidad de A. Así que, $n = k-1$, es decir, para cada $a \in A$,

$$\#(A \setminus a) = q^{k-1} = q^{|A|-1}. \tag{2.9}$$

Veamos que para todo $a \in A$, $\#(A \cup B \setminus a) = q^{|A \cup B|-1}$. Sea $B = \{b_1, \ldots, b_l\}$. Por el Lema 2.18, para todo $i \in [l]$, $\#(A \cup B) = q(\#(A \cup B \setminus b_i))$, así que, para cada $j \in [l]$, $\#((A \setminus a) \cup \{b_1, \ldots, b_j\}) = q(\#((A \setminus a) \cup \{b_1, \ldots, b_{j-1}\}))$. Esto muestra que, para todo $a \in A$, $A \cup B \setminus a \to a$ (dado que $\#(A \cup B) < q^{|A \cup B|}$), por lo que $A \cup B \setminus a \to p_0$ y, en consecuencia,

$$A \cup B \setminus a \Longrightarrow p_0, \tag{2.10}$$

de aquí que

$$A \cup B \notin \Gamma_0. \tag{2.11}$$

Ahora veamos que $\#(A \cup B) = q^{|A \cup B|-1}$. Sea $C \in \Gamma_0$ tal que $B \subseteq C \subseteq A \cup B$ (este conjunto C existe ya que $A \cup B \Longrightarrow p_0$ y $B \subseteq A \cup B$). Si $A \cap C = \emptyset$, entonces $C = B$, lo cual contradice que $B \not\Longrightarrow p_0$, entonces $A \cap C \neq \emptyset$ y podemos elegir $a \in A \cap C$. Como $C \in \Gamma_0$, ocurre que $C \setminus a \not\Longrightarrow p_0$, y por (2.10), $A \cup B \setminus a \Longrightarrow p_0$. Si $A \subseteq C$, entonces $A \cup B \subseteq C$, y por la elección de C tenemos que $A \cup B = C$, pero esto no puede ocurrir ya que por (2.11), $A \cup B \notin \Gamma_0$ y $C \in \Gamma_0$. Así que $A \nsubseteq C$ y por lo tanto, $A \setminus C \neq \emptyset$, digamos $A \setminus C = \{a^{(1)}, \ldots, a^{(m)}\}$. Como $C \subsetneq A \cup C$, entonces $A \cup C \in \Gamma \setminus \Gamma_0$, de manera que existe $j \in \{0, 1, \ldots, m-1\}$ tal que $C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}\} \not\Longrightarrow p_0$ y $C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}, a^{(j+1)}\} \Longrightarrow p_0$. Por el Lema 2.17,

$$C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}, p_0\} \Longrightarrow a^{(j+1)}. \tag{2.12}$$

Sean r y t dos filas de M tales que $M(r, A \cup B \setminus a^{(j+1)}) = M(t, A \cup B \setminus a^{(j+1)})$, entonces en particular, $M(r, C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}\}) = M(t, C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}\})$ y además, por (2.10) $A \cup B \setminus a^{(j+1)} \Longrightarrow p_0$, luego tenemos que $M(r, p_0) = M(t, p_0)$, en resumen, $M(r, C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}, p_0\}) = M(t, C \setminus a \cup \{a^{(1)}, \ldots, a^{(j)}, p_0\})$, y por (2.12), $M(r, a^{(j+1)}) = M(t, a^{(j+1)})$. Con esto hemos verificado que $(A \cup B) \setminus a^{(j+1)} \Longrightarrow a^{(j+1)}$, así que empleando el Lema 2.16 y la igualdad $\#(A \cup B \setminus a^{(j+1)}) = q^{|A \cup B|-1}$ recién probada, tenemos que

$$\#(A \cup B) = \#(A \cup B \setminus a^{(j+1)}) = q^{|A \cup B|-1}. \tag{2.13}$$

Por (2.9) tenemos que, para todo $a \in A$, $q^{|A|-1} = \#(A \setminus a) < \#A$ y por (2.13) se verifica

que $\#(A \cup B) = q^{|A \cup B|-1}$, así que existe $j \in [l-1]$, tal que $\#(A \cup \{b_1, \ldots, b_j, b_{j+1}\}) < q(\#(A \cup \{b_1, \ldots, b_j\}))$. Así que $A \cup \{b_1, \ldots, b_j\} \to b_{j+1}$, y, por lo tanto, $A \cup B \setminus b_{j+1} \to p_0$, de donde $A \cup B \setminus b_{j+1} \Longrightarrow p_0$, pero esto contradice la minimalidad de B. Concluimos que si $A \notin \Gamma$, entonces existe $n \in \mathbb{N}$ tal que $\#A = q^n$. □

Hasta ahora hemos probado que si A es un conjunto autorizado minimal o si A es un conjunto no autorizado, entonces en efecto $\#A$ es una potencia de q. Para incluir a todos los conjuntos en un resultado general resta probar esta afirmación para los conjuntos autorizados que no son minimales. De esto nos ocupamos en el siguiente lema.

Lema 2.21 ([8, Lema 6]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Si $A \subseteq P \cup p_0$ es tal que $A \Longrightarrow p_0$, entonces existe $n \in \mathbb{N}$ tal que $\#A = q^n$.*

Demostración.

Supongamos que existe algún subconjunto de $P \cup p_0$ que no satisface la conclusión del lema. Sea A un conjunto autorizado con la propiedad de que $\#A$ no es una potencia de q y A es minimal con esta propiedad. Sea $B \subseteq A$ tal que $B \in \Gamma_0$ y sea $b \in B$. Si $A \setminus b \Longrightarrow p_0$, entonces existe $C \subseteq A \setminus b$ tal que $C \in \Gamma_0$. Dado que $B \setminus b \not\Longrightarrow p_0$ y $B = (B \setminus b) \cup b \Longrightarrow p_0$, por el Lema 2.17 sabemos que $(B \setminus b) \cup p_0 \Longrightarrow b$. Sean r y t dos filas de M tales que $M(r, C \cup (B \setminus b)) = M(t, C \cup (B \setminus b))$, en particular, $M(r, C) = M(t, C)$ y como $C \Longrightarrow p_0$, ocurre que $M(r, p_0) = M(t, p_0)$, de aquí que $M(r, (B \setminus b) \cup p_0) = M(t, (B \setminus b) \cup p_0)$ y ya que $(B \setminus b) \cup p_0 \Longrightarrow b$, tenemos que $M(r, b) = M(t, b)$, así que $C \cup (B \setminus b) \Longrightarrow b$ y dado que $C \cup (B \setminus b) \subseteq A \setminus b$, entonces $A \setminus b \Longrightarrow b$, por lo que $\#A = \#(A \setminus b)$, lo cual contradice la minimalidad de A. Entonces $A \setminus b \not\Longrightarrow p_0$ y por el Lema 2.20 $\#(A \setminus b)$ es una potencia de q, además, dado que $A \Longrightarrow p_0$, por el Lema 2.18 tenemos que $\#A = q\#(A \setminus b)$, de modo que $\#A$ es una potencia de q, lo cual es una contradicción. Entonces si A es un conjunto autorizado, $\#A$ es una potencia de q. □

Podemos resumir las conclusiones obtenidas en los Lemas 2.19, 2.20 y 2.21 en el siguiente teorema.

Teorema 2.22 ([8, Proposición 1]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Para todo $A \subseteq P \cup p_0$, $\#A$ es una potencia de q.*

Por definición, en un esquema perfecto si un conjunto A tiene alguna información acerca del distribuidor p_0 entonces conoce a p_0. El siguiente teorema afirma que lo mismo ocurre si

p_0 es reemplazado por cualquier participante b y su demostración se basa fuertemente en el Teorema 2.22.

Teorema 2.23 ([8, Teorema 3]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Si $A \subseteq P \cup p_0$ y $b \in P \cup p_0$ son tales que $A \to b$, entonces $A \Longrightarrow b$.*

Demostración.

Sea $\mathcal{A}$ un conjunto completo de representantes respecto de la relación $\sim_A$ y $p \in P \cup p_0$. Tenemos que $\#(A \cup p) = q(\#A)$ si y sólo si para cada $r \in \mathcal{A}$ y para cada $\alpha \in \mathcal{S}$, existe una fila t tal que $[t]_{\sim_A} = [r]_{\sim_A}$ y $M(t, p) = \alpha$. Como en este caso $A \to b$, entonces existe una fila r y existe $\beta \in \mathcal{S}$ tal que para toda fila t, si $M(r, A) = M(t, A)$, entonces $M(t, b) \neq \beta$, así que en este caso $\#(A \cup b) < q(\#A)$. Por el Teorema 2.22, existen $n, m \in \mathbb{N}$ tales que $\#A = q^n$ y $\#(A \cup b) = q^m$, y dado que $A \subseteq A \cup b$ tenemos que $n \leq m$. Por lo anterior, $q^m = \#(A \cup b) < q(\#A) = q \cdot q^n = q^{n+1}$, de donde $m < n+1$, en resumen, $n \leq m < n+1$, de donde $m = n$, y por lo tanto, $\#(A \cup b) = \#A$, y por el Lema 2.16 concluimos que $A \Longrightarrow b$. □

Para finalizar esta serie de resultados de conteo que nos permiten conocer el número $\#A$ para un conjunto A, hallaremos este número para un conjunto que no contiene conjuntos redundantes.

Lema 2.24. *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$ y sea $q = |\mathcal{S}|$. Si $A \subseteq P \cup p_0$ es tal que para todo $B \subseteq A$ y para todo $a \in B$, $(B \setminus a) \not\Longrightarrow a$, entonces $\#A = q^{|A|}$.*

Demostración.

Sea $A = \{a_1, \ldots, a_k\}$. Como M es ideal tenemos que $s(a_1) = \mathcal{S}$, entonces $\#\{a_1\} = q$. Dado que $\{a_1, a_2\} \setminus a_2 \not\Longrightarrow a_2$, entonces por el Teorema 2.23 tenemos que $\{a_1, a_2\} \setminus a_2 \not\to a_2$, lo cual implica que para toda fila r y para todo $\alpha \in \mathcal{S}$ existe una fila t tal que $M(r, a_1) = M(t, a_1)$ y $M(t, a_2) = \alpha$, de aquí que $\#\{a_1, a_2\} = q^2$. Se verifica que $\{a_1, a_2, a_3\} \setminus a_3 \not\Longrightarrow a_3$, entonces por el Teorema 2.23 y siguiendo un razonamiento similar al anterior obtenemos que $\#\{a_1, a_2, a_3\} = q^3$. Continuando de esta forma obtenemos que $\#A = \#\{a_1, \ldots, a_k\} = q^k = q^{|A|}$. □

2.5. Una casi-caracterización de esquemas ideales conexos mediante matroides

Con los resultados establecidos en las secciones anteriores estamos listos para construir un matroide a partir de un esquema de compartición de secretos ideal conexo.

Teorema 2.25 ([8, Teorema 1]). *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$. Entonces la familia de conjuntos redundantes respecto a M, $\mathcal{R}(M)$, es la familia de conjuntos dependientes de un matroide $\mathcal{M}$ sobre $P \cup p_0$.*

Demostración.

Sea $q = |\mathcal{S}|$ y sea $\rho : \mathcal{P}(P \cup p_0) \to \mathbb{N} \cup \{0\}$ una función definida de la siguiente forma: $\rho(\emptyset) = 0$ y para todo $A \subseteq P \cup p_0$ no vacío, $\rho(A) = \log_q(\#A)$. Por el Teorema 2.22, ρ es una función de valor entero no negativa que satisface la propiedad (r1*). Probaremos a continuación que ρ satisface las propiedades (r2*) y (r3*). Para $A \subseteq P \cup p_0$ y $p \in P \cup p_0$ se verifica que $\#A \leq \#(A \cup p) \leq q(\#A)$, de donde, $\log_q(\#A) \leq \log_q(\#(A \cup p)) \leq \log_q(q(\#A)) = \log_q(\#A) + 1$, así que, $\rho(A) \leq \rho(A \cup p) \leq \rho(A) + 1$, entonces se cumple (r2*). Ahora, sean $x, y \in (P \cup p_0) \setminus A$ tales que $\rho(A) = \rho(A \cup x) = \rho(A \cup y)$, es decir, $\log_q(\#A) = \log_q(\#(A \cup x)) = \log_q(\#(A \cup y))$, o, equivalentemente, $\#A = \#(A \cup x) = \#(A \cup y)$. Por el Lema 2.16, $A \Longrightarrow x$ y $A \Longrightarrow y$, de aquí que $A \cup x \Longrightarrow y$ y nuevamente por el Lema 2.16 tenemos que $\#(A \cup \{x, y\}) = \#(A \cup x) = \#A$ en resumen, $\#(A \cup \{x, y\}) = \#A$, y, por lo tanto, $\rho(A \cup \{x, y\}) = \rho(A)$, con lo cual demostramos que se verifica (r3*). Entonces por el Teorema 1.14 existe un matroide $\mathcal{M}$ sobre $P \cup p_0$ que tiene a ρ como su función rango, es decir, rank $= \rho$, y cuyos conjuntos independientes son los conjuntos $A \subseteq P \cup p_0$ tales que $\text{rank}(A) = |A|$. Por la propiedad (r1) sabemos que para todo $A \subseteq P \cup p_0$, $0 \leq \text{rank}(A) \leq |A|$, entonces $A \subseteq P \cup p_0$ es dependiente en $\mathcal{M}$ si y sólo si $\text{rank}(A) < |A|$, es decir, si y sólo si $\log_q(\#A) < |A|$, o equivalentemente, $\#A < q^{|A|}$. Por el Lema 2.24, si $\#A < q^{|A|}$ entonces A contiene algún conjunto redundante, digamos B. Así que existe $a \in B$ tal que $B \setminus a \Longrightarrow a$, más aún, $A \setminus a \Longrightarrow a$, de donde $A \in \mathcal{R}(M)$. Ahora, si $A \in \mathcal{R}(M)$, entonces existe $a \in A$ tal que $A \setminus a \Longrightarrow a$, por el Lema 2.16 se cumple que $\#A = \#(A \setminus a)$, y como $\#(A \setminus a) \leq q^{|A \setminus a|}$, obtenemos que $\#A < q^{|A|}$. Así que un conjunto A es dependiente si y sólo si A es un conjunto redundante. Hemos verificado que $\mathcal{R}(M)$ es la familia de conjuntos dependientes del matroide $\mathcal{M}$. □

Al matroide $\mathcal{M} = (P \cup p_0, \text{rank})$ que obtenemos por el Teorema 2.25 a partir del esquema de compartición de secretos ideal conexo M lo llamamos el *matroide apropiado* para el

esquema M, y decimos que el esquema M es *inducido* por el matroide $\mathcal{M}$, y si Γ es la estructura de acceso del esquema M, también decimos que Γ es *inducida* por el matroide $\mathcal{M}$.

El siguiente resultado plantea la manera en la cual podemos conocer el número de vectores de fragmentos para un conjunto $A \subseteq P \cup p_0$ dado su valor bajo la función rango del matroide apropiado $\mathcal{M}$. Su demostración es inmediata a partir de la definición de la función rango de $\mathcal{M}$, pero lo enunciamos como corolario ya que lo mencionaremos a menudo a lo largo del texto.

Corolario 2.26 ([2, Lema 2.17])**.** *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$, con $q = |\mathcal{S}|$. Sea $\mathcal{M} = (P \cup p_0, \text{rank})$ su matroide apropiado conexo. Entonces para todo $A \subseteq P \cup p_0$,*

$$\#A = q^{\text{rank}(A)}.$$

Por el Teorema 2.25 sabemos que los conjuntos dependientes del matroide apropiado $\mathcal{M}$ son los conjuntos redundantes del esquema M, así que todo conjunto dependiente tiene un elemento superfluo, aunque no necesariamente sabemos cuál elemento es. Para el caso de los circuitos esta propiedad es más fuerte. El Corolario 2.27 establece que ningún elemento de un circuito es imprescindible, en el sentido de que podemos eliminar cualquier elemento del circuito y los elementos restantes pueden conocer el fragmento otorgado al participante eliminado.

Corolario 2.27. *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P, conjunto de secretos y fragmentos $\mathcal{S}$, con $q = |\mathcal{S}|$, y sea $\mathcal{M} = (P \cup p_0, \mathcal{C})$ su matroide apropiado. Si $C \in \mathcal{C}$, entonces para todo $x \in C$ se verifica que $C \setminus x \Longrightarrow x$.*

Demostración.

Como C es un circuito, por el Teorema 1.18 se cumple que $\text{rank}(C) = |C| - 1$ y para cada $x \in C$ tenemos que $\text{rank}(C \setminus x) = |C| - 1$. Por el Corolario 2.26 se verifica que $\#C = q^{\text{rank}(C)} = q^{|C|-1}$ y $\#(C \setminus x) = q^{\text{rank}(C \setminus x)} = q^{|C|-1}$, por lo que $\#C = \#(C \setminus x)$, y por el Lema 2.16 concluimos que $C \setminus x \Longrightarrow x$. □

Gracias al Corolario 2.27 podemos dar una versión más completa del Teorema 2.25: resulta que el matroide apropiado del Teorema 2.25 tiene, además, la propiedad de ser conexo.

Teorema 2.28 ([8, Teorema 1])**.** *Sea M un esquema de compartición de secretos ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}$. Entonces la familia de conjuntos redundantes respecto a M, $\mathcal{R}(M)$, es la familia de conjuntos dependientes de un matroide conexo $\mathcal{M}$ sobre $P \cup p_0$.*

Demostración.

Sólo falta demostrar que $\mathcal{M}$ es conexo. Como M es conexo, para cada $p \in P$ existe un conjunto $A_p \in \Gamma_0$ tal que $p \in A_p$, así que $A_p \Longrightarrow p_0$, de modo que $A_p \cup p_0$ es un conjunto dependiente y por lo tanto contiene a un circuito, digamos B_p. Si $p_0 \notin B_p$, entonces $B_p \subseteq A_p$ y por ser B_p un conjunto dependiente, es decir, un conjunto redundante, existe $a \in B_p \subseteq A_p$ tal que $B_p \setminus a \Longrightarrow a$, más aún, $A_p \setminus a \Longrightarrow a$, entonces $A_p \setminus a \Longrightarrow p_0$, lo cual contradice que $A_p \in \Gamma_0$. Entonces $p_0 \in B_p$, y por el Corolario 2.27 sabemos que $B_p \setminus p_0 \Longrightarrow p_0$, de donde $B_p \setminus p_0 \in \Gamma$. Claramente $B_p \setminus p_0 \subseteq A_p$ y si suponemos que $B_p \setminus p_0 \subsetneq A_p$ entonces A_p tendría como subconjunto propio al conjunto autorizado $B_p \setminus p_0$, lo cual contradice que A_p es un conjunto autorizado minimal, entonces ocurre que $B_p \setminus p_0 = A_p$, o equivalentemente $B_p = A_p \cup p_0$, y como $p \in A_p$, concluimos que B_p es un circuito al que pertenecen p y p_0. Por lo tanto, para todo $p \in P$ existe un circuito de $\mathcal{M}$ que contiene a p y p_0. Sean x y y dos puntos distintos de $P \cup p_0$: si x o y son iguales a p_0, por lo anterior, existe un circuito al que pertenecen x y y; si x y y son elementos de P, entonces existen dos circuitos C_{x,p_0} y C_{y,p_0} tales que $x, p_0 \in C_{x,p_0}$ y $y, p_0 \in C_{y,p_0}$, luego, por el Teorema 1.11 existe un circuito $C_{x,y}$ tal que $x, y \in C_{x,y}$, de donde $\mathcal{M}$ es un matroide conexo, con lo cual queda demostrado el teorema. □

En este momento nos preguntamos si podemos formular el recíproco del Teorema 2.28, es decir, si podemos afirmar que a partir de un matroide conexo podemos construir un esquema de compartición de secretos ideal conexo. La respuesta es que sí, parcialmente. Necesitamos agregar la condición de que el matroide sea representable sobre un campo finito para garantizar el resultado anhelado. Además, haremos uso del siguiente resultado de álgebra lineal.

Teorema 2.29 ([8]). *Sean V un espacio vectorial, $A \subseteq V$ y $v \in V$. El vector v es una combinación lineal de los vectores en A si y sólo si todo vector $u \in V$ que satisface que para todo $a \in A$, $u \cdot a = 0$ también satisface que $u \cdot v = 0$, donde $\cdot$ representa el producto escalar en V.*

Teorema 2.30 ([8, Teorema 2]). *Sea $\mathcal{M} = (E, \mathcal{I})$ un matroide conexo representable sobre un campo finito $\mathbb{F}$, y sea $v_0 \in E$. Entonces existe un esquema de compartición de secretos ideal conexo M tal que $\mathcal{S} = \mathbb{F}$, $p_0 = v_0$, $P = E \setminus v_0$ y $\mathcal{R}(M)$ es la familia de conjuntos dependientes de $\mathcal{M}$.*

Demostración.

Sean $n = |E|$ y $k = \text{rank}(\mathcal{M})$. Como $\mathcal{M}$ es representable sobre el campo finito $\mathbb{F}$, entonces existe una matriz G con entradas en $\mathbb{F}$ tal que $\mathcal{M} \cong \mathcal{M}[G]$, donde G es una matriz

con columnas etiquetadas por los elementos de $[n]$ y de rango k. Sin pérdida de generalidad supongamos que G tiene k filas y sea $\phi : E \to [n]$ el isomorfismo entre $\mathcal{M}$ y $\mathcal{M}[G]$. Por ejemplo, por [14, Ejemplo 1.10] sabemos que una $\mathbb{F}_2$-representación para el matroide de Fano F_7 que tiene rango 3 es la siguiente matriz:

$$G_{F_7} = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \left[\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right] \end{array}$$

y en este caso el isomorfismo ϕ está dado por $\phi(a) = 1$, $\phi(b) = 2$, ..., $\phi(g) = 7$. Definimos un esquema de compartición de secretos M en el que $P = E \setminus v_0$, $p_0 = v_0$, $\mathcal{S} = \mathbb{F}$, y el conjunto de etiquetas de las filas de M es $\mathbb{F}^k$. Para cada fila etiquetada con $z \in \mathbb{F}^k$ y para cada $p \in P \cup p_0$, definimos

$$M(z, p) = z \cdot [\phi(p)]^t \tag{2.14}$$

donde $[\phi(p)]^t$ es el vector columna con etiqueta $\phi(p)$ traspuesto y $\cdot$ indica el producto punto. Para el matroide de Fano fijemos $p_0 = a$, en este caso tomaremos $\mathcal{S} = \mathbb{F}_2$, el conjunto de las etiquetas del esquema M_{F_7} es $\mathbb{F}_2^3$ y siguiendo la definición de las entradas de la matriz M_{F_7} dada por (2.14), tenemos que

$$M_{F_7} = \begin{array}{c} \begin{matrix} \quad p_0{=}a & \quad b & c & d & e & f & g \end{matrix} \\ \begin{array}{c} (0,0,0) \\ (0,0,1) \\ (0,1,0) \\ (0,1,1) \\ (1,0,0) \\ (1,0,1) \\ (1,1,0) \\ (1,1,1) \end{array} \left[\begin{array}{ccccccc} (0,0,0)\cdot(1,0,0) & (0,0,0)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (0,0,0)\cdot(0,1,1) \\ (0,0,1)\cdot(1,0,0) & (0,0,1)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (0,0,1)\cdot(0,1,1) \\ (0,1,0)\cdot(1,0,0) & (0,1,0)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (0,1,0)\cdot(0,1,1) \\ (0,1,1)\cdot(1,0,0) & (0,1,1)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (0,1,1)\cdot(0,1,1) \\ (1,0,0)\cdot(1,0,0) & (1,0,0)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (1,0,0)\cdot(0,1,1) \\ (1,0,1)\cdot(1,0,0) & (1,0,1)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (1,0,1)\cdot(0,1,1) \\ (1,1,0)\cdot(1,0,0) & (1,1,0)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (1,1,0)\cdot(0,1,1) \\ (1,1,1)\cdot(1,0,0) & (1,1,1)\cdot(0,1,0) & \dots & \dots & \dots & \dots & (1,1,1)\cdot(0,1,1) \end{array}\right] \end{array}$$

$$= \begin{array}{c} \\ (0,0,0) \\ (0,0,1) \\ (0,1,0) \\ (0,1,1) \\ (1,0,0) \\ (1,0,1) \\ (1,1,0) \\ (1,1,1) \end{array} \begin{array}{c} \begin{array}{ccccccc} p_0{=}a & b & c & d & e & f & g \end{array} \\ \left[\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{array}\right] \end{array}$$

Veamos que M es perfecto. Si $A \subseteq P = E \setminus v_0$ es tal que $A \not\Longrightarrow p_0$, entonces existen dos filas con etiquetas $z_1, z_2 \in \mathbb{F}^k$ tales que $M(z_1, A) = M(z_2, A)$ y $M(z_1, p_0) \neq M(z_2, p_0)$, entonces por (2.14) esto es equivalente a

$$z_1 \cdot [\phi(p_0)]^t \neq z_2 \cdot [\phi(p_0)]^t \text{ y } \forall a \in A : z_1 \cdot [\phi(a)]^t = z_2 \cdot [\phi(a)]^t. \tag{2.15}$$

Sea $z \in \mathbb{F}^k$. Por (2.15), para todo $a \in A$ y para todo $\alpha \in \mathbb{F}$ tenemos que

$$\begin{aligned} (z + \alpha z_1 - \alpha z_2) \cdot [\phi(a)]^t &= z \cdot [\phi(a)]^t + \alpha z_1 \cdot [\phi(a)]^t - \alpha z_2 \cdot [\phi(a)]^t \\ &= z \cdot [\phi(a)]^t + \alpha[z_1 \cdot [\phi(a)]^t - z_2 \cdot [\phi(a)]^t] = z \cdot [\phi(a)]^t \end{aligned} \tag{2.16}$$

Sea $\beta \in \mathbb{F}$. Por (2.15), $z_1 \cdot [\phi(p_0)]^t - z_2 \cdot [\phi(p_0)]^t \neq 0$, así que podemos definir $\alpha = \dfrac{\beta - z \cdot [\phi(p_0)]^t}{z_1 \cdot [\phi(p_0)]^t - z_2 \cdot [\phi(p_0)]^t} \in \mathbb{F}$, por lo que

$$\alpha z_1 \cdot [\phi(p_0)]^t - \alpha z_2 \cdot [\phi(p_0)]^t = \beta - z \cdot [\phi(p_0)]^t,$$

o equivalentemente

$$\beta = (z + \alpha z_1 - \alpha z_2) \cdot [\phi(p_0)]^t. \tag{2.17}$$

Sea $z' = z + \alpha z_1 - \alpha z_2$. La igualdad (2.16) la podemos reescribir como que para todo $a \in A$, $z' \cdot [\phi(a)]^t = z \cdot [\phi(a)]^t$, es decir, que para todo $a \in A$, $M(z', a) = M(z, a)$, entonces $M(z', A) = M(z, A)$ y por (2.17), $M(z', p_0) = z' \cdot [\phi(p_0)]^t = \beta$, así que, por definición, $A \not\to p_0$. Por lo tanto, M es perfecto.

Para demostrar que M es ideal, sea $v \in E$ y sea $[\phi(v)]^t = (v_1, \ldots, v_k)$. Como $\mathcal{M}$ es conexo, dados cualesquiera dos puntos del matroide x y y, existe un circuito $C_{x,y}$ tal que $x, y \in C_{x,y}$. Por ser un conjunto dependiente, todos los subconjuntos propios de $C_{x,y}$ son independientes, en particular, todos los subconjuntos singulares de $C_{x,y}$ son independientes. Entonces $\{v\}$ es un conjunto independiente, por lo que $[\phi(v)]^t \neq (0, \ldots, 0)$, así que existe $i \in [k]$ tal que

$v_i \neq 0$. Para cada $\alpha \in \mathbb{F}$ definimos

$$z_\alpha = (\rho_1, \ldots, \rho_k),$$

donde $\rho_j = 0$ si $j \in [k] \setminus i$ y $\rho_i = \alpha v_i^{-1}$, entonces $\alpha = z_\alpha \cdot [\phi(v)]^t = M(z_\alpha, v)$. Así que, para cada participante $v \in E$ y para cada $\alpha \in \mathbb{F}$ existe una fila z_α de M tal que $M(z_\alpha, v) = \alpha$, así que $\mathbb{F} \subseteq s(v)$, y como la otra desigualdad siempre se cumple concluimos que $s(v) = \mathbb{F}$. Por consiguiente, M es ideal.

A continuación probaremos que $\mathcal{R}(M)$ es la familia de conjuntos dependientes de $\mathcal{M}$. Sea $A \subseteq P$.

$A \in \mathcal{R}(M) \Leftrightarrow A$ es un conjunto redundante de M

$\Leftrightarrow \exists b \in A : A \setminus b \Longrightarrow b$

$\Leftrightarrow \forall z_1, z_2 \in \mathbb{F}^k : M(z_1, A \setminus b) = M(z_2, A \setminus b) \Longrightarrow M(z_1, b) = M(z_2, b)$

$\Leftrightarrow \forall z_1, z_2 \in \mathbb{F}^k :$ si $\forall a \in A \setminus b, M(z_1, a) = M(z_2, a),$ entonces $M(z_1, b) = M(z_2, b)$

$\Leftrightarrow \forall z_1, z_2 \in \mathbb{F}^k :$ si $\forall a \in A \setminus b, z_1 \cdot [\phi(a)]^t = z_2 \cdot [\phi(a)]^t,$ entonces $z_1 \cdot [\phi(b)]^t = z_2 \cdot [\phi(b)]^t$

$\Leftrightarrow \forall z_1, z_2 \in \mathbb{F}^k :$ si $\forall a \in A \setminus b, (z_1 - z_2) \cdot [\phi(a)]^t = 0,$ entonces $(z_1 - z_2) \cdot [\phi(b)]^t = 0$

$\Leftrightarrow \forall u \in \mathbb{F}^k :$ si $\forall a \in A \setminus b, u \cdot [\phi(a)]^t = 0,$ entonces $u \cdot [\phi(b)]^t = 0$

$\Leftrightarrow [\phi(b)]^t$ es una combinación lineal de los vectores en $\{[\phi(a)]^t : a \in A \setminus b\}$ (Teorema 2.29)

$\Leftrightarrow$ El conjunto $\{[\phi(a)]^t : a \in A \setminus b\} \cup \{[\phi(b)]^t\}$ es linealmente dependiente

$\Leftrightarrow$ El conjunto $\{[\phi(a)]^t : a \in A\}$ es linealmente dependiente

$\Leftrightarrow$ El conjunto A es dependiente en $\mathcal{M}$ (la función ϕ preserva la independencia)

En resumen A es un conjunto redundante en M si y sólo si A es un conjunto dependiente en $\mathcal{M}$, es decir, la familia $\mathcal{R}(M)$ es la familia de conjuntos dependientes de $\mathcal{M}$.

Para probar que M es conexo sea $p \in P$. Como $\mathcal{M}$ es un matroide conexo entonces para los puntos $p, p_0 \in V$ existe un circuito C_{p,p_0} de $\mathcal{M}$ tal que $p, p_0 \in C_{p,p_0}$. Por el Corolario 2.27 tenemos que $C_{p,p_0} \setminus p_0 \Longrightarrow p_0$, de donde $C_{p,p_0} \setminus p_0$ es un conjunto autorizado al que pertenece p y si suponemos que $C_{p,p_0} \setminus p_0$ no es minimal, entonces existe un conjunto autorizado minimal A tal que $A \subseteq C_{p,p_0} \setminus p_0$, así que $A \Longrightarrow p_0$, de donde $A \cup p_0 \subseteq C_{p,p_0}$ es un conjunto redundante de M, o equivalentemente, $A \cup p_0$ es un conjunto dependiente contenido en C_{p,p_0}, y dado que C_{p,p_0} es un circuito, debe ocurrir que $A \cup p_0 = C_{p,p_0}$, de donde $C_{p,p_0} \setminus p_0 = A$ es un conjunto autorizado minimal al que pertenece p. Concluimos que M es un esquema de compartición de secretos conexo. □

De la demostración de conexidad en los Teoremas 2.28 y 2.30 concluimos que si construimos un matroide conexo $\mathcal{M}$ a partir de un esquema de compartición de secretos ideal

conexo M, o si construimos un esquema de compartición de secretos ideal conexo M a partir de un matroide conexo representable sobre un campo finito, $\mathcal{M}$, en ambos casos la relación entre los conjuntos autorizados minimales de la estructura de acceso Γ de M y los circuitos del matroide $\mathcal{M}$ es la siguiente:

$$A \in \Gamma_0 \text{ si y sólo si } A \cup p_0 \in \mathcal{C}, \tag{2.18}$$

es decir, A es un conjunto autorizado minimal si y sólo si $A \cup p_0$ es un circuito de $\mathcal{M}$. Las estructuras de acceso que se definen de esta forma se estudian con un poco más de detalle en el Capítulo 3.

En este punto queremos comentar que Brickell y Davenport establecieron el Teorema 2.30 para un matroide $\mathcal{M}$ representable sobre un campo cercano derecho R (*right nearfield*), el cual es una estructura algebraica que satisface todos los axiomas de campo excepto, posiblemente, la ley distributiva por la izquierda (cf. [24]). Sin embargo, Simonis y Ashikhmin [24] demostraron que la prueba dada por Brickell y Davenport es errónea ya que en un punto de su prueba emplearon una propiedad que no necesariamente se verifica si en la estructura algebraica no se cumple la propiedad distributiva por la izquierda. Por esta razón nosotros enunciamos este teorema considerando matroides representables sobre campos finitos, en los cuales sí se verifica el resultado.

A la conjunción de los Teoremas 2.28 y 2.30 es a lo que nos referimos con una casi-caracterización de esquemas de compartición de secretos ideales mediante matroides conexos. El Teorema 2.28 afirma que una condición necesaria para que un esquema conexo sea ideal es que sea inducido por un matroide conexo, mientras que el Teorema 2.30 nos dice que una condición suficiente para que un esquema conexo sea ideal es que sea inducido por un matroide conexo representable sobre un campo finito. Es natural que en este momento surja la pregunta de si la casi-caracterización puede ser una caracterización, es decir, si la condición necesaria es suficiente o si la condición suficiente es necesaria. En el Capítulo 3 nos ocuparemos principalmente de dar respuesta a cada una de estas cuestiones.

Capítulo 3

Estructuras de acceso y matroides

En el Capítulo 2 abordamos el tema de estructuras de acceso teniendo como referencia a los esquemas de compartición de secretos. Sin embargo, el estudio de algunas estructuras de acceso puede realizarse de manera independiente, como lo haremos en la Sección 3.1 con las estructuras de acceso definidas como en (2.18), lo cual nos permite conocer mejor sus propiedades.

Brickell y Davenport [8] demostraron que si una estructura de acceso es ideal entonces es inducida por un matroide (Teorema 2.28). Así que una condición necesaria para que una estructura de acceso sea ideal es que sea inducida por un matroide. Sin embargo, esta condición no es suficiente, pues existen estructuras de acceso no ideales inducidas por matroides. El primero en dar un ejemplo de esta situación fue Seymour [22]: demostró que ninguna de las estructuras de acceso inducidas por el matroide de Vamos es ideal. También vimos en el Capítulo 2 que una condición suficiente para que una estructura de acceso sea ideal es que sea inducida por un matroide representable sobre un campo finito (Teorema 2.30), y nos preguntamos si esta condición es necesaria, es decir, que si un estructura de acceso es ideal entonces su matroide apropiado es representable sobre algún campo finito. La respuesta es no. Como veremos más adelante, una estructura de acceso inducida por el matroide de non-Pappus es ideal y sin embargo, por el Teorema 1.31, el matroide de Pappus no es representable sobre ningún campo. En este capítulo estudiaremos estas afirmaciones.

3.1. Estructuras de acceso inducidas por matroides

Definición 3.1 ([18]). Sean $\mathcal{M} = (E, \mathcal{C})$ un matroide y $p_0 \in E$. El *puerto del matroide* $\mathcal{M}$ *en el punto* p_0 es la familia de subconjuntos de $P = E \setminus p_0$ denotada y definida por

$$\mathcal{M}_{p_0} = \{A \subseteq P : A \cup p_0 \in \mathcal{C}\}.$$

Entonces los elementos del puerto del matroide $\mathcal{M}_{p_0}$ son los conjuntos independientes de $\mathcal{M}$ que no contienen a p_0, pero que al agregarles p_0 se convierten en circuitos de $\mathcal{M}$.

Sea $\mathcal{M} = (E, \text{rank})$ un matroide y $p_0 \in E$. Definimos sobre el conjunto $P = E \setminus p_0$ la siguiente familia:

$$\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : \text{rank}(A \cup p_0) = \text{rank}(A)\}. \tag{3.1}$$

Veamos que $\Gamma_{p_0}(\mathcal{M})$ es una familia monótona creciente. Basta probar que si $A \in \Gamma_{p_0}(\mathcal{M})$, entonces todo $B \subseteq P$ tal que $A \subseteq B$ y $|B| = |A| + 1$ verifica que $B \in \Gamma_{p_0}(\mathcal{M})$. Sea $A \in \Gamma_{p_0}(\mathcal{M})$, entonces $\text{rank}(A \cup p_0) = \text{rank}(A)$. Consideremos $B \subseteq P$ tal que $A \subseteq B$ y sea $x \in P$ tal que $B = A \cup x$. Por (r2*) tenemos que $\text{rank}(B) = \text{rank}(A)$ o $\text{rank}(B) = \text{rank}(A) + 1$. Si $\text{rank}(B) = \text{rank}(A)$, entonces $\text{rank}(A \cup x) = \text{rank}(B) = \text{rank}(A) = \text{rank}(A \cup p_0)$, y por (r3*) tenemos que $\text{rank}(A \cup \{x, p_0\}) = \text{rank}(A)$, es decir, $\text{rank}(B \cup \{p_0\}) = \text{rank}(A) = \text{rank}(B)$. Si $\text{rank}(B) = \text{rank}(A) + 1$, por (r2*) tenemos que $\text{rank}(B \cup p_0) = \text{rank}(A \cup x \cup p_0) = \text{rank}((A \cup p_0) \cup x) \leq \text{rank}(A \cup p_0) + 1 = \text{rank}(A) + 1 = \text{rank}(B)$, es decir, $\text{rank}(B \cup p_0) \leq \text{rank}(B)$, y por (r2*) ocurre que $\text{rank}(B) \leq \text{rank}(B \cup p_0)$, por lo cual $\text{rank}(B \cup p_0) = \text{rank}(B)$. Como en cualquier caso obtenemos que $\text{rank}(B \cup p_0) = \text{rank}(B)$, concluimos que $B \in \Gamma_{p_0}(\mathcal{M})$, entonces $\Gamma_{p_0}(\mathcal{M})$ es una familia monótona creciente y, por lo tanto, es una estructura de acceso. Ahora tiene sentido presentar la siguiente definición.

Definición 3.2 ([2, 18]). Sea $\mathcal{M} = (E, \text{rank})$ un matroide y $p_0 \in E$. La *estructura de acceso inducida por* $\mathcal{M}$ *con respecto a* p_0 es la estructura de acceso sobre $P = E \setminus p_0$ denotada y definida por

$$\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : \text{rank}(A \cup p_0) = \text{rank}(A)\}.$$

A p_0 lo pensamos como el distribuidor de un esquema que tiene a $\Gamma_{p_0}(\mathcal{M})$ como su estructura de acceso. Decimos que una estructura de acceso Γ es *inducida* por $\mathcal{M}$ si se obtiene fijando algún elemento de $\mathcal{M}$ como el distribuidor, y en este caso decimos que $\mathcal{M}$ es un *matroide apropiado* para Γ.

Aunque pareciera que los conceptos que acabamos de definir son muy ajenos a los que trabajamos en los capítulos anteriores, esto no es así. El siguiente ejemplo nos muestra que una estructura de acceso umbral puede construirse a partir de un matroide uniforme.

Ejemplo 3.3 ([2, Ejemplo 2.20]). Sea $\mathcal{M}$ el matroide uniforme $U_{k,n+1}$ sobre el conjunto E, $p_0 \in E$ y $P = E \setminus p_0$. Por el Ejemplo 1.17 sabemos que para todo $A \subseteq P$, $\text{rank}(A) = \text{mín}\{k, |A|\}$ y $\text{rank}(A \cup p_0) = \text{mín}\{k, |A \cup p_0|\} = \text{mín}\{k, |A| + 1\}$, así que,

$$\begin{aligned}\Gamma_{p_0}(\mathcal{M}) &= \{A \subseteq P : \text{rank}(A \cup p_0) = \text{rank}(A)\} \\ &= \{A \subseteq P : \text{mín}\{k, |A| + 1\} = \text{mín}\{k, |A|\}\}.\end{aligned}$$

Sea $A \subseteq P$ tal que $\text{mín}\{k, |A| + 1\} = \text{mín}\{k, |A|\}$. No puede ocurrir que $\text{mín}\{k, |A| + 1\} = |A| + 1$, pues como $\text{mín}\{k, |A| + 1\} = \text{mín}\{k, |A|\}$, tendríamos que $\text{mín}\{k, |A|\} = |A| + 1$, lo cual es falso. Si suponemos que $\text{mín}\{k, |A|\} = |A|$, dado que $\text{mín}\{k, |A| + 1\} = \text{mín}\{k, |A|\}$ tenemos que $\text{mín}\{k, |A| + 1\} = |A|$, por lo que debe ocurrir que $k = |A|$. Finalmente, si $\text{mín}\{k, |A| + 1\} = k = \text{mín}\{k, |A|\}$ obtenemos que $|A| \geq k$. Concluimos que $|A| \geq k$. Ahora, si $A \subseteq P$ es tal que $|A| \geq k$, entonces $\text{mín}\{k, |A| + 1\} = k = \text{mín}\{k, |A|\}$, por lo que $A \in \Gamma_{p_0}(\mathcal{M})$. En resumen, hemos demostrado que $\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P : |A| \geq k\}$, o equivalentemente, $\Gamma_{p_0}(\mathcal{M})$ es la estructura de acceso umbral $\Gamma_{k,n}$. Por lo tanto, el matroide uniforme $U_{k,n+1}$ es el matroide apropiado para la estructura de acceso umbral $\Gamma_{k,n}$ y $\Gamma_{k,n}$ es inducida por el matroide uniforme $U_{k,n+1}$.

El siguiente teorema muestra una importante relación entre las familias de conjuntos que acabamos de definir: la familia de conjuntos autorizados minimales de la estructura de acceso $\Gamma_{p_0}(\mathcal{M})$ es el puerto del matroide $\mathcal{M}$ en el punto p_0.

Teorema 3.4 ([18]). *Sean $\mathcal{M} = (E, \text{rank})$ un matroide, $p_0 \in E$ y $P = E \setminus p_0$. Se cumple que*

$$\text{mín}\,\Gamma_{p_0}(\mathcal{M}) = \mathcal{M}_{p_0},$$

donde $\text{mín}\,\Gamma_{p_0}(\mathcal{M})$ denota la familia de conjuntos autorizados minimales de $\Gamma_{p_0}(\mathcal{M})$.

Demostración.

Sea $A \subseteq P$ tal que $A \cup p_0 \in \mathcal{C}$. Por el Teorema 1.18 tenemos que $\text{rank}(A \cup p_0) = \text{rank}(A)$, de aquí que $A \in \Gamma_{p_0}(\mathcal{M})$. Sea $B \subsetneq A$, entonces $B \cup p_0 \subsetneq A \cup p_0$, y dado que $A \cup p_0$ es un circuito, entonces B y $B \cup p_0$ son conjuntos independientes, por lo que $\text{rank}(B \cup p_0) = |B \cup p_0| = |B| + 1 = \text{rank}(B) + 1$, así que $B \notin \Gamma_{p_0}(\mathcal{M})$. Por lo tanto, $A \in \text{mín}\,\Gamma_{p_0}(\mathcal{M})$. Ahora, sea $A \subseteq P$ un conjunto autorizado minimal de $\Gamma_{p_0}(\mathcal{M})$. Dado que $A \in \Gamma_{p_0}(\mathcal{M})$, entonces $\text{rank}(A \cup p_0) = \text{rank}(A) \leq |A| < |A \cup p_0|$, de aquí que $A \cup p_0$ es un conjunto dependiente. Si A es dependiente, entonces existe un subconjunto propio independiente $B \subsetneq A$ tal que $\text{rank}(A) = \text{rank}(B) = |B|$, por lo que $\text{rank}(B \cup p_0) \leq \text{rank}(A \cup p_0) = \text{rank}(A) = \text{rank}(B)$, y dado que por (r2*), $\text{rank}(B) \leq \text{rank}(B \cup p_0)$, concluimos que $\text{rank}(B \cup p_0) = \text{rank}(B)$, por lo tanto, $B \in \Gamma_{p_0}(\mathcal{M})$, lo cual contradice que A es un conjunto autorizado minimal. Entonces A es un conjunto independiente, y como $A \cup p_0$ es dependiente entonces contiene un circuito

C. Si $p_0 \notin C$, entonces $C \subseteq A$, lo cual es falso ya que A es independiente, así que $p_0 \in C$, entonces existe un subconjunto $B \subseteq A$ tal que $C = B \cup p_0$ y por el Teorema 1.18, tenemos que $\text{rank}(B \cup p_0) = \text{rank}(B)$, por lo que $B \in \Gamma_{p_0}(\mathcal{M})$, y como A es un conjunto autorizado minimal de $\Gamma_{p_0}(\mathcal{M})$, concluimos que $A = B$, y por lo tanto, $A \cup p_0$ es un circuito de $\mathcal{M}$. Así que $\min \Gamma_{p_0}(\mathcal{M}) = \mathcal{M}_{p_0}$. □

Por (2.18) sabemos que las estructuras de acceso de los esquemas de compartición de secretos de los Teoremas 2.28 y 2.30 son estructuras de acceso inducidas por un matroide respecto a un participante especial p_0.

Por el Teorema 3.4, la estructura de acceso $\Gamma_{p_0}(\mathcal{M})$ puede ser descrita de manera alternativa a (3.1) de la siguiente forma:

$$\Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P \mid \exists C \in \mathcal{C} : p_0 \in C \wedge C \setminus p_0 \subseteq A\}.$$

Por un abuso de lenguaje a las estructuras de acceso de la forma $\Gamma_{p_0}(\mathcal{M})$ se les llama también *puertos de matroide*. En este texto no las llamaremos de esta forma ya que consideramos que puede causar confusión: el puerto del matroide $\mathcal{M}_{p_0}$ sólo es la familia de conjuntos autorizados minimales de la estructura de acceso $\Gamma_{p_0}(\mathcal{M})$, por lo que los conjuntos $\mathcal{M}_{p_0}$ y $\Gamma_{p_0}(\mathcal{M})$ no necesariamente son iguales.

Ahora nos cuestionamos si existen ejemplos de estructuras de acceso diferentes que se obtienen a partir del mismo matroide pero fijando un punto distinto. El siguiente ejemplo nos dice que justamente este es el caso para el matroide de Vamos.

Ejemplo 3.5 ([2, Definición 4.2])**.** Existen dos estructuras de acceso no isomorfas inducidas por el matroide de Vamos $\mathcal{V}$; una de ellas se obtiene al establecer 1, 2, 7 u 8 como el distribuidor, y la otra se obtiene al elegir a 3, 4, 5 o 6 como el distribuidor. Estudiemos la estructura $\mathcal{V}_8 = \Gamma_8(\mathcal{V})$, que se obtiene fijando a 8 como el distribuidor. En esta estructura de acceso un conjunto de participantes es un conjunto autorizado minimal si este conjunto junto con 8 es un circuito en $\mathcal{V}$. A continuación mencionamos algunos ejemplos de conjuntos autorizados y de conjuntos no autorizados en V_8.

1. Los conjuntos $\{3,4,7\}$, $\{5,6,7\}$, $\{1,2,4,5\}$, $\{1,4,5,6\}$ y $\{2,4,6,7\}$ son conjuntos autorizados minimales, ya que al agregarles el elemento 8 obtenemos los circuitos $\{3,4,7,8\}$, $\{5,6,7,8\}$, $\{1,2,4,5,8\}$, $\{1,4,5,6,8\}$ y $\{2,4,6,7,8\}$, respectivamente. El conjunto $\{1,3,4,6,7\}$ es autorizado, ya que contiene al conjunto $\{1,3,4,6\}$ que al agregarle el elemento 8 se convierte en un circuito, pero no es minimal ya que dicha contención es propia.

II. Los circuitos en el matroide de Vamos $\mathcal{V}$ tienen cardinalidad mayor o igual a 4, así que los conjuntos autorizados en $\mathcal{V}_8$ tienen cardinalidad mayor o igual a 3, de manera que los conjuntos de cardinalidad 1 o 2 no son autorizados. Los conjuntos $\{1,2,3\}$, $\{4,5,6\}$ y $\{1,2,5\}$, no son autorizados, pues al agregar el elemento 8 a cada uno de estos conjuntos obtenemos los conjuntos $\{1,2,3,8\}$, $\{4,5,6,8\}$ y $\{1,2,5,8\}$, los cuales no contienen ningún circuito. El conjunto $\{1,2,3,4\}$ no es autorizado ya que el único circuito que contiene el conjunto $\{1,2,3,4,8\}$ es $\{1,2,3,4\}$, pero este circuito no contiene a 8. Algo similar ocurre para los conjuntos $\{1,2,5,6\}$ y $\{3,4,5,6\}$.

En la Definición 3.2 hablamos de un matroide apropiado para una estructura de acceso, en caso de existir, pero hasta el momento no podemos garantizar que este matroide sea único. Veremos a continuación que esto es así cuando la estructura de acceso es conexa. Para probar este resultado emplearemos el siguiente lema, que nos dice que hablar de estructuras de acceso conexas es equivalente a hablar de matroides apropiados conexos, en caso de que estos existan.

Lema 3.6 ([2]). *Sea P un conjunto finito y sea Γ una estructura de acceso sobre P que tiene un matroide apropiado $\mathcal{M}$. Γ es una estructura de acceso conexa si y sólo si $\mathcal{M}$ es un matroide conexo.*

Demostración.

Sea $\mathcal{M} = (E, \mathcal{C})$ un matroide apropiado para Γ y $p_0 \in E$ tal que $E = P \cup p_0$ y $\Gamma = \Gamma_{p_0}(\mathcal{M})$. Supongamos que Γ es conexa, entonces para todo $p \in P$ existe $A_p \in \min \Gamma_{p_0}(\mathcal{M}) = \mathcal{M}_{p_0}$ tal que $p \in A_p$. Entonces para todo $p \in P$ existe un circuito que lo contiene, a saber, $A_p \cup p_0 \in \mathcal{C}$. Sea $C_{p,p_0} = A_p \cup p_0$, entonces $p, p_0 \in C_{p,p_0}$. Sean x y y dos puntos distintos de E. Si $x = p_0$, entonces $x, y \in C_{y,p_0}$ y si $y = p_0$, entonces $x, y \in C_{x,p_0}$. Supongamos que $x \neq p_0 \neq y$. Entonces $x, p_0 \in C_{x,p_0}$ y $y, p_0 \in C_{y,p_0}$, luego, por el Teorema 1.11 existe un circuito $C_{x,y}$ tal que $x, y \in C_{x,y}$, de donde concluimos que $\mathcal{M}$ es un matroide conexo. Supongamos ahora que $\mathcal{M}$ es conexo, entonces para todo $x \in P$ existe un circuito C_{x,p_0} tal que $x, p_0 \in C_{x,p_0}$, entonces $C_{x,p_0} \setminus p_0 \in \mathcal{M}_{p_0} = \min \Gamma_{p_0}(\mathcal{M})$, por lo que Γ es conexa. □

Teorema 3.7 ([2]). *Sea P un conjunto finito y sea Γ una estructura de acceso sobre P, conexa. Si existe un matroide apropiado para Γ, éste es único.*

Demostración.

Sea $\mathcal{M} = (E, \mathcal{C})$ un matroide apropiado para Γ, entonces existe $p_0 \in E$ tal que $E = P \cup p_0$ y $\Gamma = \Gamma_{p_0}(\mathcal{M})$. Sea $\mathcal{C}_{p_0}$ la familia de circuitos de $\mathcal{C}$ que contiene a p_0. Los elementos de $\mathcal{C}_{p_0}$ son los elementos del puerto de matroide $\mathcal{M}_{p_0}$ agregándoles el elemento p_0, así que

por el Teorema 3.4, los elementos de $\mathcal{C}_{p_0}$ están determinados por los conjuntos autorizados minimales de Γ. Dado que Γ es conexa, por el Lema 3.6 el matroide $\mathcal{M}$ es conexo, así que por el Teorema 1.32, los circuitos de $\mathcal{M}$ que no contienen a p_0, es decir, los elementos de $\mathcal{C} \setminus \mathcal{C}_{p_0}$, son construidos por aquellos que sí lo contienen, en otras palabras, están determinados por el puerto de matroide $\mathcal{M}_{p_0}$, luego, por el Teorema 3.4, los elementos de $\mathcal{C} \setminus \mathcal{C}_{p_0}$ se obtienen a partir de los conjuntos autorizados minimales de Γ. En resumen, todos los circuitos de $\mathcal{M}$ están determinados de manera única por los conjuntos autorizados minimales de Γ. Por lo tanto, $\mathcal{M}$ es único. □

Así que las nociones de estructura de acceso inducida por un matroide y matroide apropiado para una estructura de acceso definidos en esta sección y las definidas en el Capítulo 2 son las mismas ya que el matroide a partir del cual se definen es único, sólo que en esta sección hemos abordado una manera diferente de definir la estructura de acceso.

3.2. Estructura de acceso no ideal inducida por un matroide

El objetivo de esta sección es mostrar que la condición necesaria dada por Brickell y Davenport (Teorema 2.28) no es suficiente, es decir, que existe una estructura de acceso conexa que tiene un matroide apropiado, pero que no es ideal. Presentaremos una estructura con estas características que fue dada por Seymour [22]. Para comenzar, enlistamos en la Definición 3.8 los conceptos de teoría de gráficas que requerimos para desarrollar dicha prueba.

Definición 3.8 ([22])**.** Sea G una gráfica y $X \subseteq V(G)$.

- Decimos que X es un conjunto *estable* si ningún par de elementos de X está conectado por una arista.
- Un *triángulo* de G es un ciclo de longitud 3.
- Sean $k \geq 1$ y V_1, V_2, V_3 tres conjuntos de vértices, cada uno de cardinalidad k y disjuntos dos a dos. Denotamos con $K_{k,k,k}$ a la gráfica con conjunto de vértices $V_1 \cup V_2 \cup V_3$ donde todo vértice de V_i es adyacente a todo vértice de V_j, para $i, j \in [3]$, $i \neq j$. Llamamos a $K_{k,k,k}$ *gráfica completa tripartita*.
- Un *camino simple inducido* es una sucesión de vértices distintos de G tal que cada par de vértices consecutivos en la sucesión están conectados por una arista en G y cada par de vértices no consecutivos no están conectados por ninguna arista en G.

A los conjuntos estables de G también se les llama *independientes*, pero no emplearemos esta denominación para evitar confusiones con el concepto de conjunto independiente proveniente de la teoría de matroides.

Lema 3.9 ([22, Lema 2.1]). *Sean G una gráfica y $\{V_1, V_2, V_3\}$ una partición de $V(G)$, donde cada V_i es estable y de cardinalidad k^2, con $k \in \mathbb{N}$. Supongamos que para $i, j \in [3]$, $i \neq j$, todo vértice en V_i tiene a lo más k vecinos en V_j. Supongamos también que G tiene un número mayor o igual a k^4 triángulos. Entonces cada componente conexa de G es isomorfa a $K_{k,k,k}$.*

Demostración.

Para comprender mejor la prueba, explicaremos algunos puntos empleando la gráfica G_0 de la Figura 3.1, la cual cumple con las hipótesis del lema para $k = 2$. En G_0, cada vértice en V_i tiene exactamente dos vecinos en V_j, con $i, j \in [3]$, $i \neq j$, y G tiene exactamente k^4 triángulos, que son los siguientes:

$$(a, e, i, a),\ (a, e, k, a),\ (a, i, h, a),\ (a, k, h, a),\ (b, f, j, b),\ (b, f, l, b),\ (b, j, g, b),\ (b, g, l, b),$$
$$(c, e, i, c),\ (c, e, k, c),\ (c, i, h, c),\ (c, k, h, c),\ (d, f, j, d),\ (d, f, l, d),\ (d, g, j, d),\ (d, g, l, d).$$

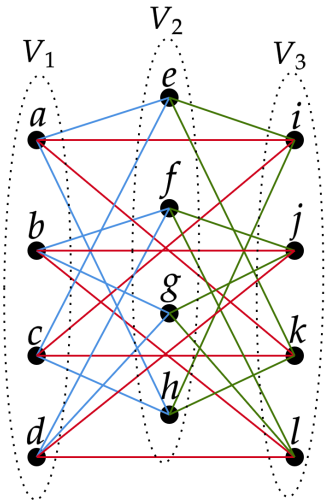


Figura 3.1: Gráfica G_0, con $k = 2$.

Para cada $v \in V(G)$ y para cada $i \in [3]$ definimos

$$d_i(v) = |N(v) \cap V_i|,$$

donde $N(v)$ denota el conjunto de vértices adyacentes a v. Queremos hallar una cota superior para el número de triángulos que tiene G. Dado que $\{V_1, V_2, V_3\}$ es una partición de $V(G)$

y que cada uno de estos conjuntos es estable, si T es un triángulo, tenemos que, para todo $i \in [3]$, $|T \cap V_i| = 1$, es decir, T tiene un vértice en cada uno de los conjuntos V_i. El número máximo de triángulos en G ocurre cuando cada vecino en V_2 de un elemento $v^{(1)} \in V_1$ también es vecino de cada vecino de $v^{(1)}$ en V_3. Por ejemplo, en G_0 los vértices $e \in V_2$ e $i \in V_3$ son vecinos de a y, dado que e es vecino de i, entonces (a, e, i, a) es un triángulo. Si denotamos con Δ al número de triángulos de G, hemos obtenido entonces que

$$\Delta \leq \sum_{v \in V_1} d_2(v) d_3(v).$$

Sea $v \in V_1$. Por hipótesis, v tiene a lo más k vecinos en V_i, $(i = 2, 3)$, entonces $d_2(v)d_3(v) \leq k^2$, además, $|V_1| = k^2$ y como G tiene un número mayor o igual a k^4 triángulos, tenemos lo siguiente:

$$k^4 \leq \Delta \leq \sum_{v \in V_1} d_2(v) d_3(v) \leq \sum_{v \in V_1} k^2 = k^2 |V_1| = k^4,$$

de donde $\sum_{v \in V_1} d_2(v)d_3(v) = \sum_{v \in V_1} k^2$, y como para todo $v \in V_1$, $d_2(v) \leq k$ y $d_3(v) \leq k$, ocurre que $d_2(v) = d_3(v) = k$. Tomando ahora $v \in V_2$ podemos probar de manera análoga que $d_1(v) = d_3(v) = k$ y si $v \in V_3$, entonces $d_1(v) = d_2(v) = k$. En resumen, si $i \in [3]$ y $v \in V(G) \setminus V_i$, entonces

$$d_i(v) = k. \tag{3.2}$$

Además, hemos obtenido que $\sum_{v \in V_1} d_2(v)d_3(v)$ no sólo es una cota superior para el número de triángulos en G, sino que, de hecho, $\Delta = \sum_{v \in V_1} d_2(v)d_3(v)$, y anteriormente habíamos analizado lo que debe suceder para obtener el número máximo de triángulos en G, así que cada vecino en V_2 de un elemento $v^{(1)} \in V_1$ también es vecino de cada vecino de $v^{(1)}$ en V_3. La elección de V_1 fue indistinta, así que la misma conclusión obtenemos para los elementos de V_2 y V_3, lo cual podemos resumir de la siguiente manera: si tenemos tres vértices $v^{(1)}, v^{(2)}, v^{(3)}$ tales que $v^{(i)} \in V_i$ y tales que algún $v^{(i)}$ es adyacente a los otros dos vértices, entonces los tres vértices forman un triángulo. Dicho de otra manera, en G la relación de "ser vecino de" es transitiva.

Ahora, supongamos que existe P un camino simple inducido de G que intersecta a los tres conjuntos V_1, V_2 y V_3. Entonces podemos encontrar un vértice $v^{(j)} \in V(P) \cap V_j$ que es adyacente a un vértice $v^{(i)} \in V(P) \cap V_i$ y a un vértice $v^{(k)} \in V(P) \cap V_k$, donde los conjuntos V_i, V_j y V_k son distintos dos a dos, de manera que $(v^{(i)}, v^{(j)}, v^{(k)})$ es un camino simple inducido. Por la conclusión del párrafo anterior tenemos que $v^{(i)}$ y $v^{(k)}$ son adyacentes, lo cual contradice que $(v^{(i)}, v^{(j)}, v^{(k)})$ es un camino simple inducido. Así que todo camino simple inducido de G no vacío intersecta exactamente a dos conjuntos V_i.

Supongamos que existe P un camino simple inducido con 3 o más aristas y sean v_1, v_2, v_3

y v_4 los primeros cuatro vértices de P. Sabemos que P intersecta exactamente a dos de los conjuntos V_i. Sin pérdida de generalidad supongamos que $v_1, v_3 \in V_1$ y $v_2, v_4 \in V_2$. Por (3.2) tenemos que $d_3(v_2) = k \geq 1$, entonces podemos elegir un vecino de v_2 en V_3, digamos u. Como v_1 y v_3 son vecinos de v_2 y v_2 es vecino de u, entonces por la transitividad de esta relación, tenemos que u es vecino de v_1 y v_3. Como v_4 es adyacente a v_3 y v_3 es adyacente a u, nuevamente por la transitividad de esta relación tenemos que u es adyacente a v_4, así que $u \in V_3$ es adyacente a $v_1 \in V_1$ y a $v_4 \in V_2$, luego, por transitividad tenemos que v_1 es vecino de v_4, lo cual contradice que P es un camino simple inducido. Por lo tanto, todo camino simple inducido de G tiene a lo más dos aristas.

Sean $u \in V_i$ y $v \in V_j$ dos elementos de la misma componente conexa de G, entonces existe un camino que los conecta. Sea $P(u, v)$ el camino más corto en G entre u y v, entonces $P(u, v)$ es un camino simple inducido. Como $P(u, v)$ intersecta a dos conjuntos de la partición, estos conjuntos deben ser V_i y V_j, así que $V(P(u, v)) \subseteq V_i \cup V_j$ y por la conclusión del párrafo anterior, $|E(P(u, v))| \leq 2$. Si $|E(P(u, v))| = 2$, entonces existe un vértice $w \in V_i \cup V_j$ tal que $P(u, v) = (u, w, v)$. Si $w \in V_i$, entonces existe una arista entre los vértices $u, w \in V_i$, lo cual contradice que V_i es estable; si $w \in V_j$, existe una arista entre los vértices $w, v \in V_j$, lo cual contradice que V_j es estable. Por consiguiente, $|E(P(u, v))| = 1$, de donde u y v son adyacentes. Luego, si C es una componente conexa de G, entonces para todo $i, j \in [3]$, $i \neq j$, todo vértice de $V(C) \cap V_i$ es adyacente a todo vértice de $V(C) \cap V_j$. Por lo anterior, si $v \in V(C) \cap V_i$, todo vértice de $V(C) \cap V_j$, $i \neq j$, es adyacente a v, de manera que $V(C) \cap V_j \subseteq N(v) \cap V_j$. Por definición de componente conexa, todos los vecinos de v pertenecen a la misma componente conexa C, de manera que $N(v) \cap V_j \subseteq V(C) \cap V_j$, entonces $N(v) \cap V_j = V(C) \cap V_j$, de donde $|V(C) \cap V_j| = |N(v) \cap V_j| = d_j(v) = k$. Así, para todo $j \in [3]$, $|V(C) \cap V_j| = k$. En resumen, la componente conexa C es tal que $V(C) = (V(C) \cap V_1) \cup (V(C) \cap V_2) \cup (V(C) \cap V_3)$, estos conjuntos son de cardinalidad k, disjuntos dos a dos y cada vértice de $V(C) \cap V_i$ es adyacente a cada vértice de $V(C) \cap V_j$, con $i \neq j$. Concluimos que C es isomorfa a $K_{k,k,k}$. Podemos verificar que en G_0 la conclusión del teorema es válida, como debía ocurrir: la gráfica G_0 es la unión de las componentes conexas C_1 y C_2, que son isomorfas a $K_{2,2,2}$, como puede apreciarse en la Figura 3.2. □

El Lema 3.9 es crucial para la demostración de la afirmación de Seymour [22], la cual enunciamos y probamos a continuación.

Teorema 3.10 ([22, Teorema 2.2]). *Si Γ es una estructura de acceso inducida por el matroide de Vamos $\mathcal{V}$ entonces Γ no es ideal.*

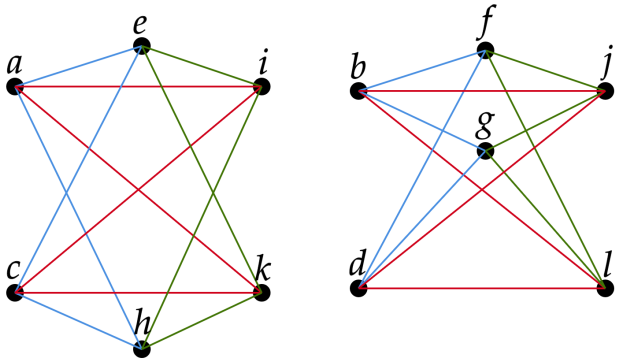


Figura 3.2: Componentes conexas de la gráfica G_0.

Demostración.

Sea Γ una estructura de acceso inducida por el matroide de Vamos $\mathcal{V}$. Por la Sección 1.4.2 sabemos que $\mathcal{V}$ es un matroide conexo, luego, por el Lema 3.6 la estructura de acceso Γ es conexa. Supongamos que Γ es ideal y sea $M = (M(r, j) : r \in \mathcal{F}, j \in [8])$ un esquema de compartición de secretos que materializa la estructura de acceso Γ, con conjunto de secretos (y fragmentos) $\mathcal{S}$ y $q = |\mathcal{S}|$. Recordemos que $\mathcal{F}$ denota el conjunto de vectores fila de M. Entonces M es un esquema de compartición de secretos ideal conexo. Para cada $i \in [4]$, definimos el siguiente conjunto:

$$V_i = \{(k_1, k_2, i) : k_1, k_2 \in \mathcal{S}\}.$$

Cada uno de los conjuntos V_i es de cardinalidad q^2. Por la definición de la tercera coordenada de los elementos de V_i, tenemos que los conjuntos V_1, V_2, V_3, V_4 son disjuntos dos a dos. Sea G la gráfica tal que $V(G) = \bigcup_{i\in[4]} V_i$, en la cual (k_1, k_2, i) es adyacente a (k_1', k_2', j) si $i \neq j$ y si existe $r \in \mathcal{F}$ tal que

$$M(r, 2i-1) = k_1,\ M(r, 2i) = k_2,\ M(r, 2j-1) = k_1',\ M(r, 2j) = k_2', \tag{3.3}$$

es decir, si existe una fila r tal que los valores k_1, k_2, k_1' y k_2' se encuentran en dicha fila en las columnas correspondientes a los participantes $2i-1$, $2i$, $2j-1$ y $2j$, respectivamente, o escrito de manera compacta, (3.3) es equivalente a lo siguiente:

$$M(r, \{2i-1, 2i, 2j-1, 2j\}) = (k_1, k_2, k_1', k_2').$$

Así, para cada $r \in \mathcal{F}$ son mutuamente adyacentes las siguientes ternas:

$$(M(r,1), M(r,2), 1),\ (M(r,3), M(r,4), 2),\ (M(r,5), M(r,6), 3),\ (M(r,7), M(r,8), 4). \tag{3.4}$$

Esto lo podemos visualizar de manera más clara en la Figura 3.3. Para simplificar la notación escribimos $M(r, j) = a_{rj}$. Una elipse representa el vértice cuyas dos primeras coordenadas

corresponden a la pareja ordenada que delimita dicha elipse, y cuya tercera coordenada es el número correspondiente al color de la elipse, el cual se indica en la parte inferior de la Figura 3.3. Las líneas que unen las elipses representan las aristas de G que unen a los vértices correspondientes. Como podemos apreciar, los vértices pertenecientes a la misma fila son adyacentes dos a dos y no existen aristas que conecten dos vértices de distinta fila.

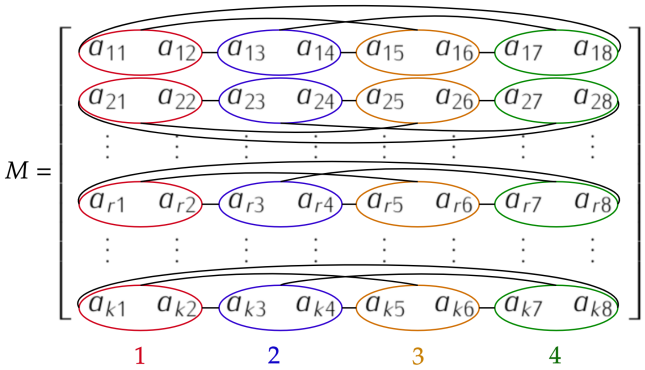


Figura 3.3: Representación de la gráfica G sobre el esquema M.

Los conjuntos de la forma $\{2i-1, 2i, 2j-1, 2j\}$, con $i, j \in [4]$ e $i \neq j$ son $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{1,2,7,8\}$, $\{5,6,7,8\}$, $\{3,4,5,6\}$ y $\{3,4,7,8\}$, de los cuales todos son circuitos de $\mathcal{V}$ a excepción del conjunto $\{1,2,7,8\}$ (ver (1.3)), que corresponde a la elección del conjunto $\{i,j\} = \{1,4\}$. Entonces, para todo $i, j \in [4]$, con $i \neq j$, $\{i,j\} \neq \{1,4\}$, el conjunto $\{2i-1, 2i, 2j-1, 2j\}$ es un circuito de $\mathcal{V}$. Sean $i, j \in [4]$, con $i \neq j$, $\{i,j\} \neq \{1,4\}$, sea (k_1, k_2, i) un vértice de V_i y sean (k_1', k_2', j) y (k_1'', k_2'', j) dos vecinos distintos de (k_1, k_2, i) en V_j. Entonces existen dos filas r y t de M tales que

$$M(r, \{2i-1, 2i, 2j-1, 2j\}) = (k_1, k_2, k_1', k_2'),$$
$$M(t, \{2i-1, 2i, 2j-1, 2j\}) = (k_1, k_2, k_1'', k_2''),$$

y si suponemos que $k_1' = k_1''$, tenemos que

$$\begin{aligned} M(r, \{2i-1, 2i, 2j-1, 2j\}) &= (k_1, k_2, k_1', k_2'), \\ M(t, \{2i-1, 2i, 2j-1, 2j\}) &= (k_1, k_2, k_1', k_2''). \end{aligned} \tag{3.5}$$

Dado que M es un esquema de compartición de secretos ideal conexo y que $\{2i-1, 2i, 2j-1, 2j\}$ es un circuito de $\mathcal{V}$, por el Corolario 2.27 cualesquiera 3 elementos de $\{2i-1, 2i, 2j-1, 2j\}$ conocen al participante restante, por lo que $\{2i-1, 2i, 2j-1\} \Longrightarrow 2j$, y por (3.5), $k_2' = k_2''$, lo cual no puede ocurrir ya que $(k_1', k_2', j) \neq (k_1'', k_2'', j)$. Entonces $k_1' \neq k_1''$, es decir, (k_1, k_2, i) puede tener a lo más un vecino en V_j cuya primera coordenada sea $k \in \mathcal{S}$, para cada $k \in \mathcal{S}$. De aquí que, para todo $i, j \in [4]$, con $i \neq j$ y $\{i,j\} \neq \{1,4\}$, cada vértice en V_i

tiene un número menor o igual que q vecinos en V_j.

Sea $X \subseteq V(G)$. Por (3.4) para cada $r \in \mathcal{F}$ los vértices

$$(M(r,1), M(r,2), 1),\ (M(r,3), M(r,4), 2) \text{ y } (M(r,5), M(r,6), 3)$$

forman un triángulo en $G \setminus V_4$. Como el conjunto $\{1,2,3,4,5,6\}$ tiene rango 4 (contiene a la base $\{1,2,3,5\}$), por el Corolario 2.26 tenemos que

$$\#\{1,2,3,4,5,6\} = q^{\text{rank}(\{1,2,3,4,5,6\})} = q^4, \tag{3.6}$$

así que existen q^4 vectores de fragmentos diferentes correspondientes a los participantes del conjunto $\{1,2,3,4,5,6\}$, por lo que $G \setminus V_4$ tiene q^4 triángulos. Siguiendo el mismo razonamiento obtenemos que $G \setminus V_1$ tiene q^4 triángulos. Las gráficas $G \setminus V_1$ y $G \setminus V_4$ satisfacen las hipótesis del Lema 3.9, así que cada componente conexa de $G \setminus V_1$ y cada componente conexa de $G \setminus V_4$ es isomorfa a $K_{q,q,q}$. Por lo tanto, existe una partición $\{X_j : j \in [q]\}$ de $V(G)$ tal que para todo $j \in [q]$, $X_j \cap (V_1 \cup V_2 \cup V_3)$ es el conjunto de vértices de una componente de $G \setminus V_4$ y $X_j \cap (V_2 \cup V_3 \cup V_4)$ es el conjunto de vértices de una componente de $G \setminus V_1$ y para todo $r \in [4]$, $|X_j \cap V_r| = q$.

Sea $r \in \mathcal{F}$ y $(M(r,1), M(r,2), 1) \in V_1$. Como $\{X_j : j \in [q]\}$ es una partición de $V(G)$, existe $j \in [q]$ tal que $(M(r,1), M(r,2), 1) \in X_j$. Como el vértice $(M(r,3), M(r,4), 2)$ es adyacente al vértice $(M(r,1), M(r,2), 1)$ en $G \setminus V_4$, entonces $(M(r,3), M(r,4), 2) \in X_j$. Asimismo, como $(M(r,7), M(r,8), 4)$ es adyacente al vértice $(M(r,3), M(r,4), 2)$ en $G \setminus V_1$, tenemos que $(M(r,7), M(r,8), 4) \in X_j$. Por lo tanto, todo vecino de $(M(r,1), M(r,2), 1)$ en el conjunto de vértices V_4 también es elemento de X_j, y dado que $|X_j \cap V_4| = q$, concluimos que $(M(r,1), M(r,2), 1)$ tiene a lo más q vecinos en V_4. Como los conjuntos V_1 y V_4 son estables, $|V_1| = q^2$ y cada elemento de V_1 tiene a lo más q vecinos en V_4, entonces el número máximo de aristas de $G \setminus (V_2 \cup V_3)$ es q^3, por lo tanto, $\#\{1,2,7,8\} \leq q^3$. Pero por el Corolario 2.26 tenemos que $\#\{1,2,7,8\} = q^{\text{rank}(\{1,2,7,8\})} = q^4$, lo cual es una contradicción. Por lo tanto, Γ no es ideal. □

Notemos que la demostración del Teorema 3.10 es una prueba general en la cual no importa respecto a qué punto del matroide de Vamos $\mathcal{V}$ construyamos la estructura de acceso, así que ninguna de las estructuras de acceso inducidas por el matroide de Vamos es ideal. Concluimos que la condición necesaria dada por Brickell y Davenport (Teorema 2.28) no es suficiente.

3.3. Estructura de acceso ideal inducida por un matroide no representable

Brickell y Davenport presentaron en [8] una condición suficiente para que una estructura de acceso sea ideal: si una estructura de acceso es creada a partir de un matroide $\mathcal{M}$ representable sobre un campo finito $\mathbb{F}$, entonces es ideal (Teorema 2.30). Sin embargo, en general no es cierto que si una estructura de acceso creada a partir de un matroide $\mathcal{M}$ es ideal, entonces $\mathcal{M}$ es representable sobre algún campo finito, lo cual fue demostrado por Simonis y Ashikhmin en [24] y el estudio de este resultado es el objetivo principal de esta sección. Como resultado adicional mostramos una interesante conexión entre códigos, matroides y esquemas de compartición de secretos. El contenido de esta sección se basa en [24] y sugerimos al lector consultar esta referencia para profundizar en este tema.

3.3.1. Códigos casi afines

Sea F un conjunto finito de cardinalidad $q \geq 2$, y sea $X \subseteq [n]$ no vacío. Denotemos con F^X al conjunto de todas las funciones con dominio X y codominio F. En muchas ocasiones será conveniente hacer la siguiente identificación: si $X \subseteq [n]$, $X = \{x_1, \ldots, x_k\}$, con $x_1 < \cdots < x_k$, y $f \in F^X$, a f lo denotamos como la k-ada $(f(x_1), \ldots, f(x_k))$.

Un *código q-ario de longitud n sobre F* es un subconjunto no vacío de $F^{[n]}$. Para $X \subseteq [n]$ no vacío, definimos la función

$$\begin{aligned} \rho_X : F^{[n]} &\to F^X \\ f &\mapsto f \circ \iota_X \end{aligned}$$

donde ι_X es la función inclusión de X en $[n]$. Si $\mathfrak{C} \subseteq F^{[n]}$ es un código q-ario de longitud n denotamos con $\mathfrak{C}_X$ al conjunto $\rho_X(\mathfrak{C})$. Notemos que $\rho_X(\mathfrak{C})$ es un conjunto de funciones de X en F, que también puede verse como un conjunto de $|X|$-adas. Al conjunto $\mathfrak{C}_X$ lo llamamos la *proyección* de $\mathfrak{C}$ en F^X.

Definición 3.11 ([24, Definición 1])**.** Un código $\mathfrak{C} \subseteq F^{[n]}$ es *casi afín* si para todo $X \subseteq [n]$ no vacío se verifica que

$$\log_q(|\mathfrak{C}_X|) \in \mathbb{N}. \tag{3.7}$$

Dicho de otra forma, un código $\mathfrak{C} \subseteq F^{[n]}$ es casi afín si para todo $X \subseteq [n]$, $|\mathfrak{C}_X|$ es una potencia de q. Aunque esta última interpretación es más fácil de comprender, adoptamos la Definición 3.11 ya que nos permitirá establecer la relación de códigos afines con matroides.

Ejemplo 3.12 ([24, Ejemplo 1]). Un *conjunto afín* $\mathfrak{C}$ es la traslación de un subespacio lineal $V \subseteq \mathbb{F}_q^n$ por un vector $x_0 \in \mathbb{F}_q^n$, es decir,

$$\mathfrak{C} = \{x_0 + v : v \in V\}.$$

Sean $F = \mathbb{F}_q$ y $\mathfrak{C}$ un conjunto afín obtenido a partir del subespacio vectorial V. Si identificamos a F^n con $F^{[n]}$, entonces podemos ver a $\mathfrak{C}$ como un código q-ario de longitud n. Claramente para todo $X \subseteq [n]$, la función ρ_X es una transformación lineal sobre V, así que $\rho_X(V)$ es un espacio vectorial sobre F, por lo que $|\mathfrak{C}_X| = |\rho_X(V)| = q^{\dim(\rho_X(V))}$. Así que se satisface la condición establecida en (3.7) y por lo tanto, $\mathfrak{C}$ es un código casi afín sobre F.

Sea F un espacio vectorial de dimensión m sobre un campo finito $\mathbb{F}_q$, entonces $|F| = q^m$, y sea $\mathfrak{C}$ un subespacio lineal del espacio vectorial de dimensión nm, F^n. Supongamos que $\mathfrak{C}$ es un código casi afín de longitud n sobre F. Como $\mathfrak{C}$ es un subespacio vectorial, entonces para todo $X \subseteq [n]$, $\mathfrak{C}_X$ es un espacio vectorial sobre $\mathbb{F}_q$ y por ser un código casi afín sobre F, donde $|F| = q^m$, existe $k \in \mathbb{N} \cup \{0\}$ tal que $|\mathfrak{C}_X| = (q^m)^k$, de donde concluimos que $\mathfrak{C}_X$ es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión mk. Ahora, si suponemos que para todo $X \subseteq [n]$, la dimensión del espacio vectorial $\mathfrak{C}_X$ sobre $\mathbb{F}_q$ es un múltiplo de m, entonces dado $X \subseteq [n]$ existe $k \in \mathbb{N} \cup \{0\}$ tal que $|\mathfrak{C}_X| = q^{km} = (q^m)^k$, y, por lo tanto, $\mathfrak{C}$ es un código casi afín. En conclusión, $\mathfrak{C}$ es un código casi afín de longitud n sobre F si y sólo si para todo $X \subseteq [n]$, la dimensión del espacio vectorial $\mathfrak{C}_X$ es un múltiplo de m. A los códigos sobre F construidos de esta forma los llamamos *multilineales*.

Ejemplo 3.13 ([24, Ejemplo 2]). Sea $F = (\mathbb{F}_3)^2$ y sea $E = \{v_i : i \in [6]\}$, donde v_i es uno de los vectores fila de la matriz A definida a continuación:

$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} (1,0) & (1,0) & (0,0) & (1,0) & (0,0) & (1,0) & (1,0) & (1,0) & (0,0) \\ (0,1) & (0,1) & (0,0) & (0,1) & (0,0) & (0,1) & (0,1) & (0,1) & (0,0) \\ (0,0) & (0,0) & (0,0) & (1,0) & (1,0) & (2,1) & (0,1) & (1,0) & (1,0) \\ (0,0) & (0,0) & (0,0) & (0,2) & (0,1) & (2,0) & (1,2) & (0,2) & (0,1) \\ (0,0) & (1,0) & (1,0) & (0,1) & (0,0) & (0,1) & (0,0) & (1,1) & (1,0) \\ (0,0) & (0,1) & (0,1) & (2,1) & (0,0) & (2,1) & (0,0) & (1,0) & (0,1) \end{bmatrix} \end{array}$$

Podemos verificar inmediatamente que el conjunto E es linealmente independiente. Sea $\mathfrak{C}$ el subespacio lineal de F^9, definido por

$$\mathfrak{C} = \text{gen}(E).$$

Entonces E es una base para $\mathfrak{C}$ y $\dim(\mathfrak{C}) = 6$. Sea $X \subseteq [9]$. Para encontrar el código $\mathfrak{C}_X$ tomamos cada uno de los vectores v_i, $i \in [6]$, y conservamos únicamente las coordenadas

correspondientes a las etiquetas de X: los vectores resultantes, $\rho_X(v_i)$, con $i \in [6]$, son los generadores de $\mathfrak{C}_X$. Para conocer la dimensión de $\mathfrak{C}_X$ calculamos el rango de la matriz cuyas filas son los vectores $\rho_X(v_i)$. Así verificamos que para un conjunto X de cardinalidad 1, $\dim(\mathfrak{C}_X) = 2$, y para un conjunto X de cardinalidad 2, $\dim(\mathfrak{C}_X) = 4$. Además, $\mathfrak{C}_X$ es un código de dimensión 6 para todos los conjuntos X de cardinalidad 3, a excepción de los 8 conjuntos $\{1,2,3\}$, $\{1,5,7\}$, $\{1,6,8\}$, $\{2,4,7\}$, $\{2,6,9\}$, $\{3,4,8\}$, $\{3,5,9\}$ y $\{4,5,6\}$, para los cuales se cumple que $\dim(\mathfrak{C}_X) = 4$. Finalmente, si X es tal que $|X| \geq 4$, entonces $\dim(\mathfrak{C}_X) = 6$. Por lo tanto, para todo $X \subseteq [9]$ se verifica que $\dim(\mathfrak{C}_X)$ es un múltiplo de 2 y 2 es la dimensión de F sobre $\mathbb{F}_3$. Concluimos que $\mathfrak{C}$ es un código casi afín de longitud 9 sobre F.

3.3.2. El matroide de un código casi afín

Sea $\mathfrak{C} \subseteq F^{[n]}$ un código casi afín. Definimos la función

$$r : \mathcal{P}([n]) \to \mathbb{N} \cup \{0\}$$
$$X \mapsto \begin{cases} 0, \text{ si } X = \emptyset \\ \log_q(|\mathfrak{C}_X|), \text{ si } X \neq \emptyset \end{cases}.$$

Siguiendo un razonamiento análogo al que empleamos en la primera parte de la demostración del Teorema 2.25, podemos verificar inmediatamente que r es la función rango de un matroide sobre $[n]$, al cual denotamos por $\mathcal{M}(\mathfrak{C})$ y llamamos *matroide del código casi afín* $\mathfrak{C}$. Entonces los conjuntos independientes no vacíos de $\mathcal{M}(\mathfrak{C})$ son los subconjuntos $I \subseteq [n]$ tales que $\log_q(|\mathfrak{C}_I|) = |I|$, o equivalentemente, $|\mathfrak{C}_I| = q^{|I|}$. Una base B de $\mathcal{M}(\mathfrak{C})$ es un subconjunto de $[n]$ que satisface que $r(B) = r([n])$, es decir, $|\mathfrak{C}_B| = |\mathfrak{C}|$. Un circuito C de $\mathcal{M}(\mathfrak{C})$ es un subconjunto de $[n]$ que, para todo $x \in C$, verifica que $r(C) = r(C \setminus x) = |C| - 1$, por lo que $|\mathfrak{C}_C| = |\mathfrak{C}_{C\setminus x}| = q^{|C|-1}$. Un bucle de $\mathcal{M}(\mathfrak{C})$ es un elemento $i \in [n]$ tal que $\{i\} \in \mathcal{C}$, es decir, tal que $|C_{\{i\}}| = q^0 = 1$, lo cual indica que todos los elementos de $\mathfrak{C}$ asignan el mismo valor a i.

Ejemplo 3.14. Consideremos el código casi afín $\mathfrak{C}$ del Ejemplo 3.13 y sea $q = |F| = 9$. Los subconjuntos X de $[9]$ de cardinalidad 1 verifican que $|\mathfrak{C}_X| = 3^2 = q = q^{|X|}$, mientras que los de cardinalidad 2 satisfacen que $|\mathfrak{C}_X| = 3^4 = q^2 = q^{|X|}$, así que los subconjuntos de $[9]$ de cardinalidad 1 y 2 son independientes. Sea $X \subseteq [9]$ de cardinalidad 3 tal que X no es uno de los conjuntos $\{1,2,3\}$, $\{1,5,7\}$, $\{1,6,8\}$, $\{2,4,7\}$, $\{2,6,9\}$, $\{3,4,8\}$, $\{3,5,9\}$ y $\{4,5,6\}$. Entonces $|\mathfrak{C}_X| = 3^6 = q^3 = q^{|X|}$ y por lo tanto, es independiente. Ahora, si X es uno de los anteriores 8 conjuntos, X satisface que $|\mathfrak{C}_X| = 3^4 = |F|^2 = |F|^{|X|-1}$, por lo que X es un circuito. Finalmente, si $|X| \geq 4$, entonces $|\mathfrak{C}_X| = 3^6 = |F|^3 < |F|^{|X|}$, por lo que X es

un conjunto dependiente. Concluimos que el matroide del código casi afín $\mathfrak{C}$ es el matroide de non-Pappus de la Figura 3.4.

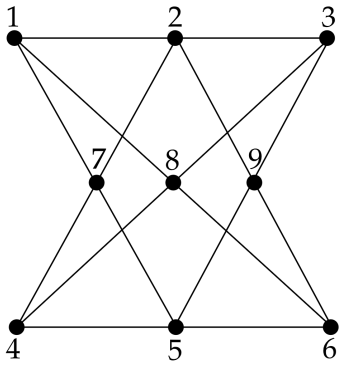


Figura 3.4: Matroide de non-Pappus correspondiente al código casi afín del Ejemplo 3.14.

Definición 3.15. Sea $\mathcal{M}$ un matroide. Decimos que $\mathcal{M}$ es *casi afinamente representable* si existe un código casi afín $\mathfrak{C}$ tal que $\mathcal{M} = \mathcal{M}(\mathfrak{C})$.

Por el Ejemplo 3.14, el matroide de non-Pappus es casi afinamente representable. Por el Teorema 1.31, el matroide de non-Pappus no es representable sobre ningún campo. Por lo tanto, la condición de representabilidad casi afín es más débil que la condición de representabilidad.

Sea $\mathfrak{C} \subseteq F^{\{0\}\cup[n]}$ un código casi afín tal que su matroide $\mathcal{M}(\mathfrak{C})$ no tiene bucles. Claramente $\mathfrak{C}$ es un esquema de compartición de secretos ideal conexo para la estructura de acceso $\Gamma_0(\mathcal{M}(\mathfrak{C}))$. Entonces si $\mathfrak{C}$ es el esquema de compartición de secretos ideal del Ejemplo 3.14, la estructura de acceso $\Gamma_0(\mathcal{M}(\mathfrak{C}))$ es ideal y es inducida por el matroide de non-Pappus que no es representable sobre ningún campo (Teorema 1.31). Esto demuestra que la condición suficiente dada por Brickell y Davenport (Teorema 2.30) no es necesaria.

Capítulo 4

Dos ejemplos de estructuras de acceso ideales

Por los Capítulos 2 y 3 tenemos una casi-caracterización de estructuras de acceso ideales conexas. Demostramos que una estructura ideal es inducida por un matroide conexo (Teorema 2.28), la cual es una condición necesaria pero no suficiente y también probamos que un matroide conexo representable sobre un campo finito induce una estructura de acceso ideal conexa (Teorema 2.30), que es una condición suficiente pero no necesaria. En este capítulo veremos un par de ejemplos en los cuales las estructuras de acceso tienen alguna propiedad muy específica. El primer ejemplo que analizaremos será el de estructuras de acceso universalmente ideales, para las cuales la casi-caracterización de hecho es una caracterización. El segundo ejemplo es sobre estructuras de acceso jerárquicas ideales. En [20] el autor presenta una caracterización de estructuras de acceso jerárquicas ideales mediante matroides de caminos reticulares. Sin embargo, no estamos seguros de que este resultado en efecto se cumpla, ya que se basa en gran medida en los resultados erróneos que presentamos en la Sección 1.5.3. Esto lo comentaremos en la Sección 4.2.

4.1. Estructuras de acceso universalmente ideales

Por definición, una estructura de acceso Γ es m-ideal si existe un esquema de compartición de secretos ideal que materializa la estructura Γ con conjunto de secretos $\mathcal{K}$ de cardinalidad m. Por ejemplo, consideremos $P = [n]$, $m = |\mathcal{K}|$ y t un entero menor o igual a n. La estructura de acceso umbral t de n es m-ideal si $m \geq n$ [1], pero si $m < n$ y $2 \leq t \leq n-1$, entonces la estructura de acceso umbral t de n no es m-ideal [17]. Esto lleva a preguntarnos si existen estructuras de acceso para las cuales podemos encontrar un esquema de compartición de

secretos ideal con conjunto de secretos de cardinalidad m, para cualquier entero positivo m, y la respuesta es afirmativa. Estas estructuras reciben el nombre de *estructuras de acceso universalmente ideales* y son cómodas para trabajar porque son eficientes sin importar el dominio de secretos [1].

Verificar que una estructura de acceso es universalmente ideal pareciera en principio una tarea imposible, o al menos complicada. Sin embargo, Beimel y Chor [1] presentaron una caracterización de este tipo de estructuras de acceso mediante matroides representables. Como veremos más adelante, una estructura de acceso conexa es universalmente ideal si y sólo si tiene un matroide apropiado que es $\mathbb{F}_2$-representable y $\mathbb{F}_3$-representable. Esta caracterización se basa en la casi-caracterización de estructuras ideales conexas a través de matroides dada por Brickell y Davenport [8], que estudiamos en el Capítulo 2 y un resultado muy interesante que afirma que un matroide es representable sobre cualquier campo si y sólo si es representable sobre $\mathbb{F}_2$ y sobre $\mathbb{F}_3$ [26].

En esta sección realizamos un estudio de algunos de los resultados presentados en [1] para facilitar la comprensión al lector que no está familiarizado en esta área.

4.1.1. Esquemas lineales

Sea M un esquema de compartición de secretos con conjunto de participantes P. Sean $A \subseteq P \cup p_0$ y $p \in P$ tales que $A \Longrightarrow p$. Por definición, si r y t son dos filas de M tales que $M(r, A) = M(t, A)$ entonces $M(r, p) = M(t, p)$, así que podemos definir la función

$$\begin{aligned} f_{A,p} : s(A) &\to s(p) \\ M(r, A) &\mapsto M(r, p). \end{aligned}$$

A esta función la llamamos *función de reconstrucción de p a partir de A*. En esta sección estamos interesados en un tipo de funciones de reconstrucción que es muy cómodo para trabajar y que definimos a continuación.

Definición 4.1 ([1, Definición 3.6])**.** Sea q la potencia de un primo y M un esquema de compartición de secretos q-ideal con conjunto de participantes P y conjunto de secretos y fragmentos $\mathbb{F}_q$. Decimos que M es *lineal* si para todo $A \subseteq P \cup p_0$ y para todo $p \in (P \cup p_0) \setminus A$ tal que $A \Longrightarrow p$ existen constantes $\{\alpha_a\}_{a \in A}$, no todas iguales a cero, y σ en $\mathbb{F}_q$ tales que para toda $r \in \mathcal{F}$,

$$M(r, p) = \sigma + \sum_{a \in A} \alpha_a M(r, a).$$

Así que en un esquema lineal todas las funciones de reconstrucción son lineales. Por el Teorema 2.30 sabemos que si una estructura de acceso conexa Γ tiene un matroide apropiado

que es representable sobre $\mathbb{F}_q$, entonces Γ es q-ideal. El esquema que se construye en la prueba de dicho teorema es un esquema q-ideal lineal [1]. En el siguiente teorema veremos que para esquemas lineales se verifica el recíproco de esta afirmación, es decir, que si Γ es la estructura de acceso conexa de un esquema de compartición de secretos ideal lineal entonces el matroide asociado a Γ es representable. Antes de probar dicho resultado establecemos la siguiente notación. Sea M un esquema de compartición de secretos con conjunto de participantes P y sea $p \in P$. Si r es una fila correspondiente al valor secreto s escribiremos $M_s(r, p)$ para denotar al fragmento de p correspondiente a la fila r donde el valor secreto correspondiente es s.

Teorema 4.2 ([1, Lema 3.7]). *Sean Γ una estructura de acceso conexa sobre el conjunto P y M un esquema de compartición de secretos q-ideal lineal que tiene a Γ como su estructura de acceso. Entonces Γ tiene un matroide apropiado que es representable sobre $\mathbb{F}_q$.*

Demostración.

Como M es un esquema q-ideal, por el Teorema 2.28 existe un matroide $\mathcal{M}$ apropiado para Γ. Empleando M construiremos un isomorfismo de matroides ϕ del conjunto de puntos del matroide en un espacio vectorial sobre $\mathbb{F}_q$. Para simplificar la notación vamos a suponer que el conjunto de participantes del esquema es $P = [n]$ y el distribuidor del esquema lo denotaremos con 0. Entonces el conjunto subyacente de $\mathcal{M}$ es $E = [0, n]$. Para cada $s \in \mathbb{F}_q$ denotemos con $r^{(s)}$ el número de filas de M correspondientes al valor secreto s. Definimos la función

$$\phi_1 : E \to \mathbb{F}_q^{r^{(0)} \times r^{(1)} \times \cdots \times r^{(q-1)}}$$

$$p \mapsto \left(M_0(1, p), \ldots, M_0(r^{(0)}, p), \ldots, M_{q-1}(1 + \sum_{i=0}^{q-2} r^{(i)}, p), \ldots, M_{q-1}(\sum_{i=0}^{q-1} r^{(i)}, p) \right),$$

es decir, el vector $\phi_1(p)$ describe de manera ordenada todos los fragmentos correspondientes al participante p en el esquema M. Sea $A = \{a_1, \ldots, a_{|A|}\} \subseteq P \cup p_0$ un conjunto dependiente de $\mathcal{M}$. Por el Teorema 2.28 esto equivale a que A es un conjunto redundante en M, y por lo tanto, existe $a \in A$ tal que $A \setminus a \implies a$. Dado que M es un esquema lineal existen constantes $\{\alpha_p\}_{p \in A \setminus a}$, no todas iguales a cero, y σ en $\mathbb{F}_q$ tal que para toda fila $r \in \mathcal{F}$ se verifica que

$$M(r, a) = -\sigma + \sum_{p \in A \setminus a} \alpha_p M(r, p),$$

así que si definimos $\alpha_a = -1$ obtenemos la igualdad

$$\sigma = \sum_{p \in A} \alpha_p M(r, p), \tag{4.1}$$

por lo que

$$
\begin{aligned}
&\sum_{p\in A}\alpha_p\phi_1(p)\\
&=\alpha_{a_1}\Big(M_0(1,a_1),\ldots,M_0(r^{(0)},a_1),\ldots,M_{q-1}(1+\sum_{i=0}^{q-2}r^{(i)},a_1),\ldots,M_{q-1}(\sum_{i=0}^{q-1}r^{(i)},a_1)\Big)\\
&+\alpha_{a_2}\Big(M_0(1,a_2),\ldots,M_0(r^{(0)},a_2),\ldots,M_{q-1}(1+\sum_{i=0}^{q-2}r^{(i)},a_2),\ldots,M_{q-1}(\sum_{i=0}^{q-1}r^{(i)},a_2)\Big)\\
&+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&+\alpha_{a_{|A|}}\Big(M_0(1,a_{|A|}),\ldots,M_0(r^{(0)},a_{|A|}),\ldots,M_{q-1}(1+\sum_{i=0}^{q-2}r^{(i)},a_{|A|}),\ldots,M_{q-1}(\sum_{i=0}^{q-1}r^{(i)},a_{|A|})\Big)\\
&=\Big(\sum_{p\in A}\alpha_aM_0(1,a),\ldots,\sum_{p\in A}\alpha_aM_0(r^{(0)},a),\ldots,\sum_{p\in A}\alpha_aM_{q-1}(1+\sum_{i=0}^{q-2}r^{(i)},a),\ldots,\\
&\qquad\sum_{p\in A}\alpha_aM_{q-1}(\sum_{i=0}^{q-1}r^{(i)},a_{|A|})\Big)\\
&=(\sigma,\ldots,\sigma,\ldots,\sigma,\ldots,\sigma)\ \ (\text{Ecuación } (4.1)),
\end{aligned}
$$

así que

$$\sum_{p\in A}\alpha_p\phi_1(p)=\bar{\sigma} \tag{4.2}$$

donde $\bar{\sigma}$ denota el vector con todas las entradas iguales a σ en $\mathbb{F}_q^{r^{(0)}\times r^{(1)}\times\cdots\times r^{(q-1)}}$. Hemos obtenido una combinación lineal de las imágenes bajo ϕ_1 de los elementos del conjunto dependiente A igualada con un múltiplo de $\bar{1}$ en $\mathbb{F}_q^{r^{(0)}\times r^{(1)}\times\cdots\times r^{(q-1)}}$.

Sea $Y=\text{gen}(\bar{1},\phi_1(0),\phi_1(1),\ldots,\phi_1(n))\leq\mathbb{F}_q^{r^{(0)}\times r^{(1)}\times\cdots\times r^{(q-1)}}$ y sea $t=\dim(Y)-1$. Sea $\phi_2: Y\longrightarrow\mathbb{F}_q^t$ una transformación lineal con $\ker(\phi_2)=\text{gen}(\bar{1})$. Si $X\subseteq Y$ el conjunto $\{\phi_2(x):x\in X\}$ es linealmente dependiente si y sólo si existen escalares $\{\alpha_x:x\in X\}$ no todos iguales a cero tales que $\sum_{x\in X}\alpha_x\phi_2(x)=0$, o equivalentemente dado que ϕ_2 es una transformación lineal, $\phi_2(\sum_{x\in X}\alpha_x x)=0$, es decir, siempre y cuando $\sum_{x\in X}\alpha_x x\in\ker(\phi_2)$, en resumen,

$$\{\phi_2(x):x\in X\}\text{ es linealmente dependiente }\Leftrightarrow\text{ existen escalares }\{\alpha_x:x\in X\}\text{ no todos iguales a cero tales que }\sum_{x\in X}\alpha_x x\in\text{gen}(\bar{1}). \tag{4.3}$$

Notemos que $\text{Im}\,\phi_1=\{\phi_1(0),\phi_1(1),\ldots,\phi_1(n)\}\subseteq Y$, por lo que la función $\phi_2\circ\phi_1:E\rightarrow\mathbb{F}_q^t$ está bien definida. Sea $A\subseteq E$. Por (4.3) tenemos que $(\phi_2\circ\phi_1)(A)$ es linealmente dependiente en $\mathbb{F}_q^t$ si y sólo si existen escalares $\{\alpha_a:a\in A\}$ no todos iguales a cero y un escalar δ en

$\mathbb{F}_q^t$ tales que $\sum_{a\in A}\alpha_a\phi_1(a)=\bar{\delta}$ y por (4.2) esto es equivalente a que A es dependiente en $\mathcal{M}$, es decir, A es dependiente en $\mathcal{M}$ si y sólo si $(\phi_2\circ\phi_1)(A)$ es linealmente dependiente en $\mathbb{F}_q^t$. Por lo tanto, $\phi=\phi_2\circ\phi_1 : E\to \mathrm{Im}(\phi_2\circ\phi_1)\leq\mathbb{F}_q^t$ es una función biyectiva entre matroides que preserva la dependencia. Así que el matroide apropiado para Γ, $\mathcal{M}$, es representable sobre $\mathbb{F}_q^t$. □

4.1.2. Una caracterización de estructuras de acceso 2-ideales y 3-ideales mediante matroides representables

Definición 4.3 ([1, Definición 3.8]). Sean $\mathcal{S}$ un conjunto, $t\in\mathbb{N}$ y $f:\mathcal{S}^t\to\mathcal{S}$ un función. Decimos que f es *sensible por componentes* si para todo $i\in[t]$ y para cualesquiera $s_1,\ldots,s_{i-1},s_i,s_i',s_{i+1},\ldots,s_t\in\mathcal{S}$ tales que $s_i'\neq s_i$ se verifica que

$$f(s_1,\ldots,s_{i-1},s_i,s_{i+1},\ldots,s_t)\neq f(s_1,\ldots,s_{i-1},s_i',s_{i+1},\ldots,s_t).$$

Por lo tanto, una función es sensible por componentes si y sólo si todo cambio en el valor de una variable en el argumento cambia el valor de f en dicho argumento.

En el siguiente lema veremos que las funciones de reconstrucción en un esquema ideal conexo son funciones sensibles por componentes, lo cual tiene sentido, pues si tenemos un vector de fragmentos para un conjunto A que conoce a un participante p y si cambiamos el fragmento de un participante de A debería cambiar también el fragmento del participante b.

Lema 4.4 ([1, Lema 3.9]). *Sea M un esquema q-ideal conexo con conjunto de participantes P y conjunto de secretos y fragmentos $\mathcal{S}=\mathbb{F}_q$, y sean $p\in P\cup p_0$ y $A\subseteq P\cup p_0$ un conjunto tal que $A\Longrightarrow p$, con $p\notin A$, y tal que A es minimal en este sentido. Si $f_{A,p}:s(A)\to s(p)$ es la función de reconstrucción del fragmento de p a partir de A entonces f es sensible por componentes.*

Demostración.

Por simplicidad y sin pérdida de generalidad supongamos que $A=[t]$. Si A es un conjunto redundante existe un elemento $a\in A$ tal que $A\setminus a\Longrightarrow a$, de aquí que $A\setminus a\Longrightarrow p$, pero esto contradice la minimalidad de A. Entonces A no es redundante, así que por el Lema 2.24 sabemos que $\#A=q^{|A|}$, o equivalentemente, $s(A)=\mathbb{F}_q^{|A|}=\mathcal{S}^{|A|}$. Supongamos que f no es sensible por componentes, entonces existen $j\in A$ y $x_1,\ldots,x_{j-1},x_j,x_j',x_{j+1},\ldots,x_t\in\mathcal{S}$, con $x_j\neq x_j'$, y $s_p\in\mathcal{S}$ tales que $(x_1,\ldots,x_{j-1},x_j,x_{j+1},\ldots,x_t)$ y $(x_1,\ldots,x_{j-1},x_j',x_{j+1},\ldots,x_t)$ son dos vectores de fragmentos para A y

$$f(x_1,\ldots,x_{j-1},x_j,x_{j+1},\ldots,x_t)=s_p=f(x_1,\ldots,x_{j-1},x_j',x_{j+1},\ldots,x_t),$$

así que existen $r, r' \in \mathcal{F}$ dos filas tales que

I. $M(r, A \setminus j) = (x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_t) = M(r', A \setminus j)$ y $M(r, j) = x_j \neq x'_j = M(r', j)$,

II. como $f_{A,p}$ es la función de reconstrucción del participante p a partir de los participantes de A, entonces la imagen bajo $f_{A,p}$ de un vector de fragmentos de A correspondiente a la fila r es el fragmento que se le otorgó a p en la fila r, así que $M(r, p) = s_p = M(r', p)$.

Tenemos que el conjunto $A \setminus j$ con el vector de fragmentos $(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_t)$ reconstruye el mismo valor del fragmento de p para dos valores diferentes del fragmento de j. De aquí tenemos que $A \setminus j \to p$, y como M es ideal, por el Teorema 2.23 concluimos que $A \setminus j \Longrightarrow p$, lo cual contradice la minimalidad de A. Por lo tanto, $f_{A,p}$ es sensible por componentes. □

Veremos a continuación que las funciones sensibles por componentes sobre $\mathbb{F}_2$ y sobre $\mathbb{F}_3$ son lineales. Recordemos que el *peso* de un vector $v \in \mathbb{F}_q^t$ es el número de entradas en v distintas de cero y la *distancia de Hamming* entre dos vectores u y v de $\mathbb{F}_q^n$ es el número de entradas en las que difieren u y v.

Lema 4.5 ([1, Lema 3.10]). *Sea $f : \mathbb{F}_2^t \to \mathbb{F}_2$ una función sensible por componentes. Entonces f es una función lineal con coeficientes no nulos sobre $\mathbb{F}_2$. Es decir, existe $\sigma \in \mathbb{F}_2$ tal que para todo $(x_1, \ldots, x_t) \in \mathbb{F}_2^t$,*

$$f(x_1, \ldots, x_t) = \sigma + \sum_{i=1}^{t} x_i.$$

Demostración.

Supongamos que $f(0, \ldots, 0) = 0$ y sea $(x_1, \ldots, x_t) \in \mathbb{F}_2^t$ de peso k. Podemos definir una sucesión de elementos en $\mathbb{F}_2^t$ que comience en $(0, \ldots, 0)$ y termine en $(x_1, \ldots, x_t)$, tenga longitud $k + 1$ y los elementos sucesivos tengan entre sí distancia de Hamming igual a 1. Por ejemplo, para el vector $(1_1, 1_2, \ldots, 1_k, 0_{k+1}, \ldots, 0_t)$ una sucesión de elementos en $\mathbb{F}_2^t$ que cumple con estas características es la siguiente:

$$(0, 0, \ldots, 0), (1_1, 0, \ldots, 0), (1_1, 1_2, 0, \ldots, 0), \ldots, (1_1, 1_2, \ldots, 1_k, 0_{k+1}, \ldots, 0_t).$$

Así que f es una función sensible por componentes que toma valores en $\mathbb{F}_2$ y dos elementos consecutivos de la sucesión de vectores en $\mathbb{F}_q^n$ difieren únicamente en una entrada. Como $f(0, \ldots, 0) = 0$, entonces f en el segundo elemento de la sucesión toma el valor de 1, en el tercer elemento el valor de 0, y así sucesivamente. De manera general, f en el i-ésimo elemento de la sucesión toma el valor $1 + i \pmod 2$. Como el vector $(x_1, \ldots, x_t)$ es el $(k+1)$-ésimo elemento de la sucesión, entonces

$$f(x_1, \ldots, x_t) = 1 + (k + 1) \pmod 2 = k \pmod 2 = \sum_{i=1}^{t} x_i = 0 + \sum_{i=1}^{t} x_i.$$

Si ahora suponemos que $f(0,\ldots,0) = 1$, siguiendo un razonamiento análogo al anterior tenemos que

$$f(x_1,\ldots,x_t) = (k+1) \pmod 2 = 1 + \sum_{i=1}^{t} x_i = 1 + \sum_{i=1}^{t} x_i.$$

En cualquier caso tenemos que, en efecto, f es una función lineal sobre $\mathbb{F}_2^t$. □

Diremos que una estructura de acceso es *binaria-ideal* si es 2-ideal y que es *ternaria-ideal* si es 3-ideal. El Lema 4.5 es útil para dar una caracterización exacta de las estructuras de acceso ideales-binarias conexas mediante matroides $\mathbb{F}_2$-representables.

Corolario 4.6 ([1, Corolario 3.11]). *Una estructura de acceso Γ es binaria-ideal conexa si y sólo si existe un matroide $\mathcal{M}$ representable sobre $\mathbb{F}_2$ apropiado para Γ.*

Demostración.

Supongamos que Γ es una estructura de acceso binaria-ideal conexa y sea M un esquema que materializa la estructura de acceso Γ. Por el Lema 4.4 la función de reconstrucción de un participante p a partir de un conjunto A tal que $A \Longrightarrow p$ y A es minimal en este sentido es una función $f_{A,p} : \mathbb{F}_2^{|A|} \to \mathbb{F}_2$ sensible por componentes. Por el Lema 4.5 toda función sensible por componentes sobre $\mathbb{F}_2$ es lineal. Por lo tanto, toda función de reconstrucción es lineal sobre $\mathbb{F}_2$ y por definición, M es un esquema lineal. Por el Teorema 4.2, Γ tiene un matroide apropiado representable sobre $\mathbb{F}_2$. El otro sentido está garantizado por el Teorema 2.30. □

Ahora deseamos caracterizar las estructuras de acceso ternarias-ideales conexas mediante matroides $\mathbb{F}_3$-representables, pero la demostración de este resultado no es tan inmediata como en el caso de las estructuras binarias-ideales. Necesitamos dos afirmaciones adicionales que enunciamos a continuación como lemas.

Lema 4.7 ([1]). *Si $f : \mathbb{F}_q^t \to \mathbb{F}_q$ es una función, entonces f puede expresarse como un polinomio multivariable con coeficientes en $\mathbb{F}_q$, en el cual cada monomio de f contiene variables cuyas potencias son menores o iguales a $q-1$.*

Lema 4.8 ([1]). *Los polinomios de grado 1 sobre $\mathbb{F}_3$ son las permutaciones de $\mathbb{F}_3$.*

Demostración.

En $\mathbb{F}_3$ ocurre que si $a, b \in \mathbb{F}_3$, con $a \neq 0$, entonces $ay + b = az + b$ si y sólo si $y = z$, por lo que todo polinomio $p(x) = ax + b$ sobre $\mathbb{F}_3$ es una función inyectiva de $\mathbb{F}_3$ en $\mathbb{F}_3$, de donde $p(x)$ es una función biyectiva, es decir, una permutación de $\mathbb{F}_3$. Dado que a puede tomar 2 valores y b puede tomar 3 valores, entonces existen 6 polinomios de grado 1 sobre

$\mathbb{F}_3$. Por otro lado, existen $3! = 6$ permutaciones de $\mathbb{F}_3$. Entonces los polinomios de grado 1 sobre $\mathbb{F}_3$ son las permutaciones de $\mathbb{F}_3$. □

Lema 4.9 ([1, Lema 3.12]). *Sea $f : \mathbb{F}_3^t \to \mathbb{F}_3$ una función sensible por componentes. Entonces f es una función lineal con coeficientes en $\mathbb{F}_3$ no nulos, es decir, existen $\sigma \in \mathbb{F}_3$, $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_3 \setminus \{0\}$ tales que para todo $(x_1, \ldots, x_t) \in \mathbb{F}_3^t$,*

$$f(x_1, \ldots, x_t) = \sigma + \sum_{i=1}^{t} \alpha_i x_i.$$

Demostración.

Por el Lema 4.7 la función f es un polinomio en el que cada monomio es el producto de variables con potencias menores o iguales a 2. Supongamos que existe una variable de grado 2, y sin pérdida de generalidad supongamos que dicha variable es x_1. Entonces f puede escribirse como

$$f(x_1, \ldots, x_t) = x_1^2 p_1(x_2, \ldots, x_t) + x_1 p_2(x_2, \ldots, x_t) + p_3(x_2, \ldots, x_t),$$

donde p_1, p_2 y p_3 son polinomios y p_1 no es idénticamente cero, por lo que existen valores para $x_2, \ldots, x_t$, digamos $a_2, \ldots, a_t \in \mathbb{F}_3$, tales que $p_1(a_2, \ldots, a_t) \neq 0$, así que

$$f(x_1, a_2, \ldots, a_t) = a x_1^2 + b x_1 + c,$$

donde $a = p(a_2, \ldots, a_t) \neq 0$, $b = p_2(a_2, \ldots, a_t)$ y $c = p_3(a_2, \ldots, a_t)$, así que $f(x_1, a_2, \ldots, a_t)$ es un polinomio de grado 2 en la variable x_1. Dado que f es una función sensible por componentes, si fijamos el valor de ciertas variables y mantenemos f como función de las variables restantes, entonces f es una función sensible por componentes respecto a las variables restantes. Por consiguiente, f como función de x_1 es una función sensible por componentes, lo cual es equivalente en este caso a que f como función de x_1 es una función inyectiva, y como el dominio y el codominio de dicha función es $\mathbb{F}_3$, entonces $f(x_1, a_2, \ldots, a_t)$ es una función biyectiva, o equivalentemente, una permutación. Por el Lema 4.8, $f(x_1, a_2, \ldots, a_t)$ es un polinomio de grado 1, pero ya teníamos que f es un polinomio de grado 2, así que hemos obtenido una contradicción. Por lo tanto, f no contiene ninguna variable de grado 2, así que sus monomios son multilineales.

Supongamos que f tiene un monomio con 2 o más variables. Sea $r(x_1, \ldots, x_t)$ un monomio que tiene al menos dos variables y que tiene longitud mínima. Sin pérdida de generalidad supongamos que estas variables son $x_1, x_2, \ldots, x_r$. Fijando las variables $x_3 = \cdots = x_r = 1$ y $x_{r+1} = \cdots = x_t = 0$, tenemos que

$$f(x_1, x_2, 1, \ldots, 1, 0, \ldots, 0) = a x_1 x_2 + b x_1 + c x_2 + d,$$

para algunos $a, b, c, d \in \mathbb{F}_3$, con $a \neq 0$. Si ahora fijamos $x_2 = -\frac{b}{a}$ tenemos que

$$f(x_1, -\frac{b}{a}, 1, \ldots, 1, 0, \ldots, 0) = ax_1(-\frac{b}{a}) + bx_1 + c(-\frac{b}{a}) + d = -bx_1 + bx_1 - \frac{bc}{a} + d = -\frac{bc}{a} + d,$$

que es una función constante, y por lo tanto, no es sensible respecto a la primera componente, lo cual contradice que f es sensible por componentes. Por lo tanto, f no contiene variables de grado mayor o igual a 2 ni monomios con 2 o más variables, tampoco puede ser un polinomio constante porque es sensible por componentes. Entonces f es un polinomio lineal, es decir,

$$f(x_1, \ldots, x_t) = \sigma + \sum_{i=1}^{t} \alpha_i x_i.$$

Ahora, si suponemos que existe una constante $\alpha_k = 0$, entonces estableciendo $x_i = 0$ para todo $i \in [t] \setminus \{k\}$, tenemos que

$$f(0_1, \ldots, 0_{k-1}, \beta_k, 0_{k+1}, \ldots, 0_t) = \sigma = f(0_1, \ldots, 0_{k-1}, \beta'_k, 0_{k+1}, \ldots, 0_t),$$

lo cual contradice que f es sensible respecto a la componente k-ésima. Por lo tanto, para todo $i \in [t]$, $\alpha_i \neq 0$. □

Gracias al Lema 4.9 establecemos el siguiente resultado.

Corolario 4.10 ([1, Corolario 3.13]). *Una estructura de acceso Γ es ternaria-ideal conexa si y sólo si existe un matroide apropiado para Γ representable sobre $\mathbb{F}_3$.*

Demostración.

Análoga a la demostración del Corolario 4.6. □

4.1.3. Una caracterización de estructuras de acceso universalmente ideales mediante matroides representables

En la Sección 4.1.2 establecimos que una estructura de acceso conexa es q-ideal si y sólo si existe un matroide apropiado para dicha estructura que es representable sobre $\mathbb{F}_q$, cuando q es igual a 2 o 3. Claramente una condición necesaria para que una estructura de acceso sea universalmente ideal es que sea 2-ideal y 3-ideal. En esta sección ocuparemos la caracterización dada en la Sección 4.1.2 para demostrar que esta condición necesaria también es suficiente.

Comenzamos citando un resultado muy fuerte acerca de matroides representables, el cual afirma que si deseamos establecer que un matroide es representable sobre cualquier campo basta con verificar que dicho matroide es $\mathbb{F}_2$-representable y $\mathbb{F}_3$-representable.

Proposición 4.11 ([26, Teorema 9.2.9]). *Un matroide $\mathcal{M}$ es representable sobre cualquier campo si y sólo si $\mathcal{M}$ es representable sobre $\mathbb{F}_2$ y sobre $\mathbb{F}_3$.*

Con el siguiente corolario nos acercamos a nuestro objetivo: establecemos que es suficiente saber que una estructura de acceso conexa es 2-ideal y 3-ideal para asegurar que es q-ideal, para q potencia de un primo.

Corolario 4.12 ([1, Corolario 3.15]). *Sea Γ una estructura de acceso conexa binaria-ideal y ternaria-ideal. Para cada entero q tal que q es potencia de un primo, Γ es q-ideal.*

Demostración.

Dado que Γ es binaria-ideal conexa, por el Corolario 4.6 la estructura Γ tiene un matroide apropiado $\mathcal{M}$ que es representable sobre $\mathbb{F}_2$ y como Γ es ternaria-ideal conexa, por el Corolario 4.10 la estructura Γ tiene un matroide apropiado $\mathcal{M}'$ que es representable sobre $\mathbb{F}_3$. Como Γ es conexa, por el Teorema 3.7 su matroide apropiado es único, por lo que $\mathcal{M} = \mathcal{M}'$ y por lo tanto, $\mathcal{M}$ es representable sobre $\mathbb{F}_2$ y sobre $\mathbb{F}_3$. Por la Proposición 4.11 concluimos que $\mathcal{M}$ es representable sobre cualquier campo, en particular es representable sobre cualquier campo finito. Por el Teorema 2.30 concluimos que Γ es ideal sobre cualquier campo finito, es decir, Γ es q-ideal para todo q potencia de un primo. □

Para poder establecer la conclusión del Corolario 4.12 para cualquier entero positivo m haremos uso del Teorema Chino del Residuo que recordamos a continuación.

Proposición 4.13 (Teorema Chino del Residuo). *Sean $a_i \in \mathbb{Z}$ y $n_i \in \mathbb{N}$ tales que $(n_j, n_k) = 1$, con $i, j, k \in [r]$, $j \neq k$. Entonces el sistema lineal de congruencias*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

tiene solución única módulo $N = n_1 n_2 \dots n_r$.

Corolario 4.14 ([1, Corolario 3.16]). *Si Γ es una estructura de acceso conexa binaria-ideal y ternaria-ideal, entonces para todo entero positivo m la estructura de acceso Γ es m-ideal.*

Demostración.

Sea $\mathcal{S}$ un conjunto de secretos de tamaño m, con

$$m = p_1^{i_1} p_2^{i_2} \dots p_t^{i_t},$$

donde los p_j son primos distintos. Dado un secreto $s \in \mathcal{S}$, usamos el esquema $p_j^{i_j}$-ideal para repartir

$$s \pmod{p_j^{i_j}}$$

para todo $1 \leq j \leq t$, de manera independiente. Todo conjunto $A \in \Gamma$ puede reconstruir $s \pmod{p_j^{i_j}}$, y por el Teorema Chino del Residuo, A puede reconstruir el secreto s. Dado que para todo j, $s \pmod{p_j^{i_j}}$ se comparte de manera independiente, entonces todo conjunto $A \notin \Gamma$ no obtiene información parcial del secreto. □

Empleando los Corolarios 4.6, 4.10 y 4.14 podemos caracterizar las estructuras de acceso universalmente ideales mediante matroides representables de la siguiente forma.

Teorema 4.15 ([1, Teorema 3.1]). *Sea Γ una estructura de acceso conexa. Las siguientes afirmaciones son equivalentes:*

I. Γ es universalmente ideal.

II. Γ es binaria-ideal y ternaria-ideal.

III. Γ tiene un matroide apropiado que es representable sobre $\mathbb{F}_2$ y $\mathbb{F}_3$.

Podríamos preguntarnos si estamos dando información innecesaria. Tal vez sería suficiente establecer que una estructura de acceso es 2-ideal o 3-ideal (donde la o es una disyunción exclusiva) para afirmar que dicha estructura de acceso es universalmente ideal. Como es de esperarse, esto no es así. Los siguientes ejemplos demuestran que la condición de ser una estructura de acceso conexa únicamente binaria-ideal o ternaria-ideal no basta para ser universalmente ideales. Primero presentamos una proposición acerca de la representabilidad del matroide uniforme.

Proposición 4.16 ([21, Teorema 6.5.2]). *Sea $\mathbb{F}$ un campo y $n \geq 2$. El matroide $U_{2,n}$ es $\mathbb{F}$-representable si y sólo si $|\mathbb{F}| \geq n - 1$.*

Ejemplo 4.17 ([1, Ejemplo 4.1]). Sea Γ la estructura de acceso $(2, 3)$-umbral. Por el Ejemplo 3.3 el matroide apropiado para Γ es el matroide uniforme $U_{2,4}$, el cual por la Proposición 4.16 no es representable sobre $\mathbb{F}_2$. Por el Corolario 4.6, Γ no es binaria-ideal. Sin embargo, por la Proposición 4.16 el matroide $U_{2,4}$ sí es representable sobre $\mathbb{F}_3$, así que por el Corolario 4.10 la estructura Γ sí es ternaria-ideal. De hecho, el esquema 3-ideal M es el que se muestra a continuación:

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 1 & 0 \end{bmatrix} \end{array}$$

Ejemplo 4.18 ([1, Ejemplo 4.3]). Sea $P = [6]$ y consideremos la estructura de acceso $\mathcal{A}$ sobre P definida por la familia de conjuntos autorizados minimales siguientes:

$$\mathcal{A}_0 = \{\{1,4\},\{2,5\},\{3,6\},\{1,2,6\},\{1,3,5\},\{2,3,4\},\{4,5,6\}\}.$$

Por lo visto en la Sección 1.4.1 tenemos que $\mathcal{A}_0$ es el puerto del matroide de Fano F_7 en el

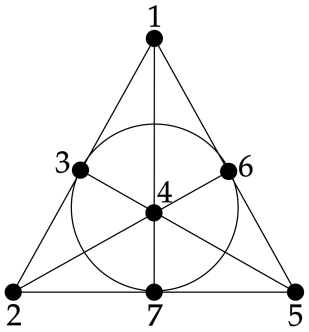


Figura 4.1: Matroide de Fano F_7.

punto 7 que se muestra en la Figura 4.1, por lo que el matroide apropiado para $\mathcal{A}$ es F_7, que por la Proposición 1.30 es representable únicamente sobre campos de característica 2. Por lo

tanto, $\mathcal{A}$ es 2-ideal pero no 3-ideal. El esquema 2-ideal M correspondiente es el siguiente:

$$M = \begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \left[\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \end{array}$$

4.2. Estructuras de acceso jerárquicas ideales

Como pudimos apreciar en el Ejemplo 2.9, en un esquema de compartición de secretos umbral todos los participantes tienen la misma importancia y desempeñan la misma función. Por ello los esquemas umbrales son adecuados para aquellos grupos en los cuales a cada participante se le asigna el mismo grado de confianza [13]. Sin embargo, la mayoría de las organizaciones tienen una estructura compleja donde la confianza asignada a un participante está directamente relacionada a su posición en la estructura. Así que ahora estamos interesados en esquemas de compartición de secretos (y sus estructuras de acceso) en los cuales la confianza no está distribuida de manera uniforme sobre el conjunto de todos los participantes.

Comenzamos con una definición que nos permite clasificar al conjunto de participantes de una estructura de acceso.

Definición 4.19 ([20, Definición 2])**.** Sea Γ una estructura de acceso sobre P y sean $p, q \in P$. Decimos que p es *jerárquicamente superior* a q, y lo denotamos por $q \preceq p$, si para todo $A \subseteq P \setminus \{p, q\}$, $A \cup p \in \Gamma$ siempre que $A \cup q \in \Gamma$. Decimos que los participantes p y q son *jerárquicamente equivalentes* si $p \preceq q$ y $q \preceq p$ y lo denotamos por $p \sim q$. Decimos que p es *jerárquicamente estrictamente superior* a q, y lo denotamos por $q \prec p$, si $q \preceq p$, pero $p \npreceq q$.

Claramente la relación $\preceq$ es reflexiva y transitiva, es decir, es un preorden sobre P, mientras que la relación $\sim$ es una relación de equivalencia. Notemos que la relación $\preceq$ puede definirse sobre cualquier estructura de acceso, sin embargo, nosotros estamos interesados en aquellas estructuras de acceso donde esta relación tiene una propiedad adicional. Recordemos que un preorden total es una relación binaria reflexiva, transitiva y total.

Definición 4.20 ([20, Definición 5])**.** Sea Γ una estructura de acceso sobre P. Si la relación $\preceq$ es un preorden total decimos que la estructura de acceso Γ es *jerárquica*.

Definición 4.21 ([20, Definición 5]). Sea Γ una estructura de acceso sobre un conjunto P. Decimos que Γ es *m-partita* si P puede dividirse en m partes de tal manera que los elementos en la misma parte son jerárquicamente equivalentes, y es *estrictamente m-partita* si los elementos de distintas partes no son jerárquicamente equivalentes.

Dado que podemos definir la relación $\sim$ sobre cualquier estructura de acceso, entonces toda estructura de acceso es m-partita. Las estructuras de acceso más interesantes son las estrictamente m-partitas, pues en ellas todos los participantes pueden clasificarse en niveles de jerarquía, como vemos a continuación.

Sea Γ una estructura de acceso jerárquica sobre un conjunto de participantes P. Como $\sim$ es una relación de equivalencia sobre P, el conjunto de participantes P puede dividirse en m diferentes clases de equivalencia $P_1, \ldots, P_m$, para algún $m \in \mathbb{N}$, de tal manera que Γ es una estructura de acceso estrictamente m-partita y

$$P = \bigcup_{i=1}^{m} P_i,$$

donde para todo $i, j \in [m]$, con $i < j$, y para cualesquiera $p \in P_i$ y $q \in P_j$ se verifica que $q \prec p$. Es decir, los participantes en el primer nivel son estrictamente superiores a los del segundo nivel; los participantes en el segundo nivel son superiores a los del tercer nivel, y así sucesivamente.

En la siguiente definición presentamos dos tipos de estructuras de acceso jerárquicas muy importantes.

Definición 4.22 ([20, Definición 6]). Sea P un conjunto de participantes con partición $(P_1, \ldots, P_m)$, y sea $k_1 < k_2 < \cdots < k_m$ una sucesión de enteros positivos. Sea $k = (k_1, k_2, \ldots, k_m)$. Definimos una *estructura de acceso jerárquica disyuntiva*, y la denotamos por $\Gamma_\exists(P, k)$, como la siguiente familia de conjuntos:

$$\Gamma_\exists(P, k) = \{X \subseteq P : \exists i \in [m] : |X \cap \bigcup_{j=1}^{i} P_j| \geq k_i\}.$$

Definimos una *estructura de acceso jerárquica conjuntiva*, y la denotamos por $\Gamma_\forall(P, k)$, como la siguiente familia de conjuntos:

$$\Gamma_\forall(P, k) = \{X \subseteq P : \forall i \in [m] : |X \cap \bigcup_{j=1}^{i} P_j| \geq k_i\}.$$

A continuación presentamos un par de ejemplos de estructuras de acceso jerárquicas disyuntivas.

Ejemplo 4.23 ([13]). Consideremos como ejemplo un banco en el cual las transacciones monetarias pueden ser autenticadas por dos vicepresidentes o por tres cajeros Seniors. En este caso existen dos niveles de jerarquía. El primer nivel consiste de los dos vicepresidentes, $\Pi_1 = \{p_1, p_2\}$. El segundo nivel está formado por los tres cajeros Seniors $\Pi_2 = \{p_3, p_4, p_5\}$. Para recuperar el secreto es necesario que los dos participantes del primer nivel o los tres participantes del segundo nivel o tres participantes de ambos niveles reúnan sus fragmentos, es decir, en este caso $k_1 = 2$ y $k_2 = 3$.

Ejemplo 4.24. Consideremos una empresa que está formada por su director general, el conjunto de 4 directores P_1, el conjunto de 6 gerentes P_2, el conjunto de 15 supervisores P_3 y el conjunto de 100 empleados P_4. Sea $k = (3, 4, 10, 80)$. Algunos conjuntos autorizados de la estructura de acceso jerárquica disyuntiva $\Gamma_\exists(P, k)$ son los formados por: 2 directores y 2 gerentes; 1 director, 2 gerentes y 7 supervisores; 9 supervisores y 71 empleados.

Las estructuras de acceso jerárquicas disyuntivas y las estructuras de acceso jerárquicas conjuntivas son ideales [7].

4.2.1. Una caracterización de estructuras de acceso jerárquicas ideales mediante matroides de caminos reticulares

Songbao Mo [20] presenta una caracterización de estructuras de acceso jerárquicas ideales mediante matroides de caminos reticulares. El resultado más importante que Songbao Mo presenta es el siguiente teorema.

Teorema 4.25 ([20, Teorema 16]). *Una estructura de acceso Γ es una estructura de acceso jerárquica ideal si y sólo si $\Gamma = \Gamma_p(\mathcal{M})$ para algún matroide de caminos reticulares $\mathcal{M}$, donde p pertenece a la cabeza o a la cola de la partición natural ordenada de $\mathcal{M}$.*

Más aún, presenta una caracterización de las estructuras de acceso jerárquicas disyuntivas y conjuntivas mediante matroides de caminos reticulares anidados.

Corolario 4.26 ([20, Corolario 19]). *Una estructura de acceso Γ es jerárquica disyuntiva si y sólo si existe un matroide anidado $\mathcal{M}$ sobre un conjunto de n elementos tales que $\Gamma = \Gamma_p(\mathcal{M})$ y p pertenece a la cabeza de la partición.*

Corolario 4.27 ([20, Corolario 20]). *Una estructura de acceso Γ es jerárquica conjuntiva si y sólo si existe un matroide $\mathcal{M}$ sobre un conjunto de n elementos tal que $\Gamma = \Gamma_p(\mathcal{M})$ y p pertenece a la cola de la partición.*

Estas caracterizaciones son muy bellas. El problema con estos resultados es que se demuestran a partir de una larga serie de proposiciones cuya demostración depende en gran medida del Corolario 3.13 de [5] que mencionamos en la Sección 1.5.3 y que demostramos que no es válido mediante contraejemplo. Entonces es necesario replantear la demostración del Teorema 4.25 y de los Corolarios 4.26 y 4.27, o bien, presentar un ejemplo de una estructura de acceso donde el resultado no sea cierto. Esto queda pendiente para un trabajo posterior.

Conclusiones

En este trabajo realizamos un estudio de la relación entre matroides y estructuras de acceso ideales conexas. Al consultar varios de los artículos que estudian esta relación nos pareció que mucha de la información existente en este sentido se encuentra muy dispersa, por lo cual quisimos reunir en un mismo documento la información que consideramos más relevante, con el objetivo de que le resulte de ayuda a quien esté interesado en adentrarse en esta línea de investigación. A lo largo de este trabajo mostramos conceptos y resultados destacados de la teoría de matroides y presentamos algunos matroides importantes, entre ellos los matroides de Fano, Vamos, Pappus y non-Pappus, así como los matroides de caminos reticulares. Presentamos un análisis detallado de la casi-caracterización de estructuras de acceso ideales conexas mediante matroides dada por Brickell y Davenport [8] y analizamos por qué de manera general esta casi-caracterización no es una caracterización completa. Estudiamos esquemas de compartición de secretos y estructuras de acceso tanto de manera conjunta como aislada y exhibimos varios ejemplos de esquemas de compartición de secretos conexos ideales y no ideales, así como varias estructuras de acceso creadas a partir de matroides. Como un caso particular de estructuras de acceso ideales estudiamos las estructuras de acceso conexas universalmente ideales, para las cuales existe una caracterización mediante matroides que son $\mathbb{F}_2$-representables y $\mathbb{F}_3$-representables.

En [20], Songbao Mo presentó una caracterización de estructuras de acceso jerárquicas ideales mediante matroides de caminos reticulares. Este resultado se basa en una serie de resultados dados por Bonin y de Mier [5]. Sin embargo, nos percatamos de que existe un error en la demostración de dos corolarios presentados en [5] a partir del cual se garantiza la veracidad de varias afirmaciones posteriores, entre ellos la caracterización de Mo. Como un trabajo a futuro nos planteamos estudiar si existe una forma alternativa de demostrar estos resultados o si, al igual que ocurrió con dichos corolarios, es posible encontrar matroides de caminos reticulares donde tales afirmaciones sean falsas. También queda pendiente el estudio de otras familias de estructuras de acceso conexas ideales en las cuales se puedan obtener resultados más específicos empleando el resultado de Brickell y Davenport.

Referencias Bibliográficas

[1] Beimel, A. y Chor, B. "Universally ideal secret-sharing schemes". En: *IEEE Transactions on Information Theory* 40(3) (1994), págs. 786-794. DOI: 10.1109/18.335890.

[2] Beimel, A. y Livne, N. "On Matroids and Nonideal Secret Sharing". En: *IEEE Transactions on Information Theory* 54(6) (2008), págs. 2626-2643. DOI: 10.1109/TIT.2008.921708.

[3] Benaloh, J. y Leichter, J. "Generalized secret sharing and monotone functions". En: *Advances in Cryptology — CRYPTO' 88*. Ed. por Goldwasser, S. Vol. 403. Lecture Notes in Computer Science. New York: Springer-Verlag, 1990, págs. 27-35. DOI: 10.1007/0-387-34799-2_3.

[4] Blakley, G. R. "Safeguarding cryptographic keys". En: *AFIPS Conf. Proc.* 48 (1979), págs. 313-317. DOI: 10.1109/MARK.1979.8817296.

[5] Bonin, J. E. y de Mier, A. "Lattice path matroids: Structural properties". En: *European Journal of Combinatorics* 27(5) (2006), págs. 701-738. DOI: 10.1016/j.ejc.2005.01.008.

[6] Bonin, J. E., de Mier, A. y Noy, M. "Lattice path matroids: enumerative aspects and Tutte polynomials". En: *Journal of Combinatorial Theory, Series A* 104(1) (2003), págs. 63-94. DOI: 10.1016/S0097-3165(03)00122-5.

[7] Brickell, E. F. "Some ideal secret sharing schemes". En: *Workshop on the Theory and Application of Cryptographic Techniques*. Springer. 1989, págs. 468-475.

[8] Brickell, E. F. y Davenport, D. M. "On the classification of ideal secret sharing schemes". En: *Journal of Cryptology* 4 (1991), págs. 123-134. DOI: 10.1007/BF00196772.

[9] Brickell, E. F. y Stinson, D. R. "Some improved bounds on the information rate of perfect secret sharing schemes". En: *Journal of Cryptology* 5 (1992), págs. 153-166. DOI: 10.1007/BF02451112.

[10] Díaz-López, M. "Matroides y códigos: la identidad de MacWilliams". Tesis de licenciatura. Benemérita Universidad Autónoma de Puebla, 2021.

[11] Diestel, R. *Graph Theory*. 5.ª ed. Graduate Texts in Mathematics. Springer Berlin, Heidelberg, 2017. DOI: https://doi.org/10.1007/978-3-662-53622-3.

[12] Edmonds, J. y Fulkerson, D. R. "Transversals and matroid partition". En: *Journal of Research of the National Bureau of Standards Sect. B* 69(3) (1965), págs. 147-153.

[13] Ghodosi, H., Pieprzyk, J. y Safavi-Naini, R. "Secret sharing in multilevel and compartmented groups". En: *Information Security and Privacy*. Ed. por Boyd, C. y Dawson, E. Vol. 1438. ACISP 1998. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer-Verlag, 1998, págs. 367-378. DOI: 10.1007/BFb0053748.

[14] Gordon, G. y McNulty, J. *Matroids: A Geometric Introduction*. Cambridge University Press, 2012.

[15] Hoersch, F. "Extending Pappus' Theorem". Tesis de maestría. University of Waterloo, 2017.

[16] Ito, M., Saito, A. y Nishizeki, T. "Secret sharing schemes realizing general access structure". En: *Proc. IEEE Global Telecommunication Conf., Globecom 87* (1987), págs. 99-102.

[17] Karnin, E., Greene, J. y Hellman, M. "On secret sharing systems". En: *IEEE Transactions on Information Theory* 29(1) (1983), págs. 35-41. DOI: 10.1109/TIT.1983.1056621.

[18] Martí-Farré, J. y Padró, C. "Ideal secret sharing schemes whose minimal qualified subsets have at most three participants". En: *Designs, Codes and Cryptography* 52 (2009), págs. 1-14. DOI: 10.1007/s10623-008-9264-9.

[19] Mason, J. H. "Geometrical realization of combinatorial geometries". En: *Proceedings of the American Mathematical Society* 30(1) (1971), págs. 15-21. DOI: 10.2307/2038210.

[20] Mo, S. "Ideal hierarchical secret sharing and lattice path matroids". En: *Designs, Codes and Cryptography* 91 (2023), págs. 1335-1349. DOI: 10.1007/s10623-022-01154-9.

[21] Oxley, J. *Matroid Theory*. 2.ª ed. Oxford University Press, 2011. DOI: 10.1093/acprof:oso/9780198566946.001.0001.

[22] Seymour, P. D. "On secret-sharing matroids". En: *Journal of Combinatorial Theory, Series B* 56 (1992), págs. 69-73. DOI: 10.1016/0095-8956(92)90007-K.

[23] Shamir, A. "How to Share a Secret". En: *Commun. ACM* 22(11) (1979), págs. 612-613. DOI: 10.1145/359168.359176.

[24] Simonis, J. y Ashikhmin, A. "Almost affine codes". En: *Designs, Codes and Cryptography* 14 (1998), págs. 179-197. DOI: 10.1023/A:1008244215660.

[25] Stinson, D. R. *Cryptography: theory and practice*. Chapman y Hall/CRC, 2005.

[26] Truemper, K. *Matroid decomposition*. Vol. 6. Boston: Academic Press, 1992.

[27] Vamos, P. "On the representation of independence structures". En: *Unpublished manuscript* 120 (1968).

[28] Welsh, D. J. A. *Matroid Theory*. Academic Press Inc., 1976.

Notación

$\mathcal{P}(P)$	conjunto potencia del conjunto P	1
$\mathcal{M}$	matroide	1
E	conjunto subyacente de un matroide	1
$\mathcal{I}$	familia de conjuntos independientes de un matroide	1
B	base de un matroide	2
$\mathcal{B}$	familia de bases de un matroide	2
C	circuito de un matroide	3
$\mathcal{C}$	familia de circuitos de un matroide	3
$\mathcal{M}\|_T$	restricción del matroide $\mathcal{M}$ al subconjunto T	5
rank(A)	rango del conjunto A	8
$U_{k,n}$	matroide uniforme de rango k sobre un conjunto de n elementos	9
$\mathcal{M}_1 \cong \mathcal{M}_2$	los matroides $\mathcal{M}_1$ y $\mathcal{M}_2$ son isomorfos	10
$[n]$	conjunto de enteros positivos menores o iguales a n	10
$\mathcal{M}[G]$	matroide vector de una matriz G	11
F_7	matroide de Fano	17
$\mathcal{V}$	matroide de Vamos	18
$\Delta[\mathcal{A}]$	gráfica bipartita asociada con la familia $\mathcal{A}$	25
$\mathcal{A} = (A_1, \ldots, A_m)$	presentación de un matroide transversal	29
η	función de incidencia de una familia de conjuntos $\mathcal{A}$	30
N	paso al norte	30
E	paso al este	30
$\mathcal{P}(W, Q)$	conjunto de caminos reticulares en la región delimitada por W y Q	31
N_i	conjunto de i-ésimos pasos al norte	32
$[i, j]$	conjunto de enteros mayores o iguales a i y menores o iguales a j	33
q_i	paso donde ocurre el i-ésimo paso al norte de Q	33
w_i	paso donde ocurre el i-ésimo paso al norte de W	33
$\mathcal{M}[W, Q]$	matroide de caminos reticulares	33

$\mathcal{P}(X)$	camino reticular asociado a un conjunto X	34
Γ	estructura de acceso/familia de conjuntos autorizados	43
Γ_0	familia de conjuntos autorizados minimales	44
$\mathrm{cl}(\mathcal{A})$	cerradura de una familia de conjuntos $\mathcal{A}$	44
p_0	distribuidor en un esquema de compartición de secretos	44
P	conjunto de participantes en un esquema de compartición de secretos	44
$\mathcal{K}$	conjunto de secretos de un esquema de compartición de secretos	45
$\mathcal{S}$	conjunto de fragmentos de un esquema de compartición de secretos	45
$\mathcal{F}$	conjunto de vectores fila de una matriz	46
$M(r,p)$	entrada de la fila r y la columna p de la matriz M	46
$s(p)$	conjunto de entradas de la columna p	46
$M(r,A)$	fila r de la matriz M restringida a las columnas indexadas por A	46
M	esquema de compartición de secretos	46
$\Gamma_{t,n}$	estructura de acceso umbral t de n	50
$A \not\to b$	el conjunto A no tiene información sobre el participante b	51
$A \to b$	el conjunto A tiene alguna información sobre el participante b	51
$A \Longrightarrow b$	el conjunto A conoce el fragmento otorgado al participante b	51
$A \not\Longrightarrow b$	el conjunto A no conoce el fragmento otorgado al participante b	51
$A \Longrightarrow B$	el conjunto A conoce los fragmentos otorgados a los participantes del conjunto B	51
$\mathcal{R}(M)$	familia de conjuntos redundantes de un esquema de compatición de secretos	52
$s(A)$	conjunto de vectores de fragmentos para el conjunto A	53
$\#A$	número de vectores de fragmentos para el conjunto A	53
$\mathcal{M}_{p_0}$	puerto del matroide $\mathcal{M}$ en el punto p_0	68
$\Gamma_{p_0}(\mathcal{M})$	estructura de acceso inducida por el matroide $\mathcal{M}$ con respecto al punto p_0	68
$K_{k,k,k}$	gráfica completa tripartita	72
F^X	conjunto de funciones con dominio X y codominio F	79
$\mathfrak{C}$	código q-ario de longitud n	79
$\mathfrak{C}_X$	proyección del código $\mathfrak{C}$ en F^X	79
$\mathcal{M}(\mathfrak{C})$	matroide del código casi afín $\mathfrak{C}$	81
$M_s(r,p)$	fragmento otorgado a p en la fila r correspondiente al valor secreto s	85

$q \preceq p$	p es jerárquicamente superior a q	95
$p \sim q$	p es jerárquicamente equivalente a q	95
$q \prec p$	p es jerárquicamente estrictamente superior a q	95

Índice alfabético

base, 2, 3
bucle, 12

camino límite inferior, 31
camino reticular, 30
    asociado, 34
    punto final de, 30
    punto inicial de, 30
cerradura
    de una familia, 44
circuito, 3, 4
clase paralela, 12
    trivial, 12
conjunto
    afín, 79
    autorizado, 43
    dependiente, 2
    independiente, 2
    no autorizado, 43
    redundante, 52
conocer un participante, 51
cubo de Vamos, 19
código, 79
    casi afín, 79
    multineal, 80
    proyección, 79

distribuidor, 44, 45

elementos paralelos, 12
emparejamiento, 24
esquema de compartición de secretos, 44, 47
    conexo, 47
    fuertemente perfecto, 47
    ideal, 45, 52
    inducido por un matroide, 61
    lineal, 84
    perfecto, 45
esquema de distribución, 45
esquina NE, 40
esquina NE, 40
estructura de acceso, 43
    m-partita, 96
    base de, 44
    binaria-ideal, 89
    conexa, 47
    ideal, 52
    inducida por un matroide, 61, 68
    jerárquica, 96
      conjuntiva, 96
      disyuntiva, 96
    ternaria-ideal, 89
    umbral, 50
    universalmente ideal, 84

familia monótona creciente, 43
fragmento, 44
función
    de incidencia, 30
    de reconstrucción, 84
    rango, 8

sensible por componentes, 87

gráfica bipartita asociada con una familia de conjuntos, 24

matroide
de un código casi afín, 81
apropiado, 60, 68
casi afinamente representable, 81
conexo, 7
conjunto subyacente de, 2
de caminos reticulares, 33
presentación estándar de, 33
anidado, 33
presentación de, 33
de Fano, 17
de non-Pappus, 20
de Pappus, 19
de Vamos, 18
definición
por bases, 3
por circuitos, 4
por conjuntos independientes, 1
por función rango, 9
isomorfismo de, 10
puerto de, 67
punto de, 2
representable, 11
representación geométrica de, 14
restricción, 5
simple, 12
transversal, 30
presentación de, 30
uniforme, 9
vector, 9, 11

partición
cabeza de, 40
cola, 40
natural ordenada, 40
participante, 44
innecesario, 47
jeráquicamente equivalente, 95
jerárquicamente superior, 95
redundante, 47
paso al este, 30
paso al norte, 30
plano
de Fano, 17
privacidad
débil, 47
fuerte, 47

rango, 8, 9

secreto, 43
sistema de distintos representantes, 23

tener información sobre un participante, 51
transversal, 23
parcial, 23

vector de fragmentos, 46