Capítulo 7

Matroides

El objetivo de este capítulo es dar una breve introducción a qué una matroide, así como mostrar varios resultados interesantes sobre esta estructura y útiles para lo que resta de esta tesis ¹.

Un poco de independencia lineal

Sea V un espacio vectorial finito y sea \mathcal{F} una colección de subconjuntos de V con la propiedad que si A pertenece a \mathcal{F} es porque A es linealmente independiente. Cualquier persona que ha tomado un curso en álgebra lineal puede ver que se cumplen las siguientes tres cosas:

- 1. El conjunto vacío (\emptyset) pertenece a \mathcal{F} .
- 2. Si X pertenece a \mathcal{F} y Y es un subconjunto de X, entonces Y pertenece a \mathcal{F} .
- 3. Si X y Y pertenecen a \mathcal{F} y la cardinalidad de X es uno más la cardinalidad de Y, entonces existe un elemento v en $X \setminus Y$ tal que $Y \cup \{v\}$ pertenece a \mathcal{F} .

A partir de esto definimos una matroide de la siguiente forma:

 $^{^1{\}rm La}$ gran mayoría de los resultados presentados en este capítulo fueron sacados de Welsh (2010), otros resultados fueron sacados de Cook y cols. (s.f.), Lawler (2015) y Papadimitriou y Steiglitz (2016)

Definición 7.1. Una matroide $M=(S,\mathcal{F})$ es un conjunto S de cardinalidad finita y una colección \mathcal{F} de subconjuntos de S (llamada **conjuntos independientes**) que cumplen los puntos 1, 2 y 3 mencionados arriba. Todo subconjunto de S que no pertenece a \mathcal{F} es llamado **conjunto dependendiente**.

Un primer resultado es el teorema del aumento, en términos simples es una forma de generalizar el punto 3 para conjuntos independientes que difieren en tamaño más de una unidad.

Teorema 7.2. Teorema del aumento

Sea $M = (S, \mathcal{F})$ una matroide y sean X, Y en \mathcal{F} con la propiedad que la cardinalidad de Y es estrictamente mayor a la cardinalidad de X. Entonces, existe Z subconjunto de $Y \setminus X$ de tal forma que la cardinalidad de $X \cup Z$ es igual a la cardinalidad de Y y donde además $X \cup Z$ es independiente.

Demostración. Sea Z subconjunto de $Y \setminus X$ tal que $X \cup Z$ es independiente y tal que Z es máximo 2 .

Supongamos que la cardinalidad $X \cup Z$ es menor a la cardinalidad de Y, entonces existe y_0 subconjunto de Y tal que la cardinalidad de y_0 es uno más la cardinalidad de $X \cup Z$, entonces por la propiedad 3 de las matroides existe y en $y_o \setminus (Y \setminus X)$ con la propiedad de que $X \cup Z \cup \{y\}$ es independiente. Esto contradice la elección de Z porque se pedía que esta sea máxima, por lo tanto, la cardinalidad de $X \cup Z$ es igual a la cardinalidad de Y y el teorema se cumple.

A continuación, aprovecharemos la similitud que existe entre el álgebra lineal y la teoría de matroides para mostrar algunas definiciones y resultados interesantes.

7.1. Bases

Las bases son una de las propiedades más importantes del álgebra lineal, aprovechando la intersección que existe entre independencia e independencia lineal decimos que para una matroide una base es:

² en este contexto máximo se refiere a que Z es el conjunto en S de máxima cardinalidad que cumple lo que se pide, en lo que sigue de la tesis se utiliza esta definición de máximo.

7.1. BASES 49

Definición 7.3. Sea $M = (S, \mathcal{F})$ una matroide, decimos que B es una base si:

- 1. B es independiente.
- 2. B es máximo, es decir, no existe ningún elemento v en $S \setminus B$ tal que $B \cup \{v\}$ sea independiente.

Al conjunto de todas las bases en M se le denota como $\mathcal{B}(M)$.

Es claro que esta definición es equivalente para espacios vectoriales a la de una base. El primer resultado que veremos es que todas las bases son del mismo tamaño, esto sale directo del teorema 7.2.

Corolario 7.4. Sea $M = (S, \mathcal{F})$ una matroide, entonces todas las bases en M tienen la misma cardinalidad.

Demostración. Sean B_1 y B_2 dos bases en M y supongamos que la cardinalidad de B_1 es estrictamente menos a la cardinalidad de B_2 , entonces por el teorema 7.2 existe Z subconjunto de $B_2 \setminus B_1$ con la propiedad que $B_1 \cup Z$ es independiente, lo cual contradice la definición de qué es una base. Por lo tanto, la cardinalidad de B_1 es igual a la cardinalidad de B_2 y podemos concluir que todas las bases tienen el mismo número de elementos.

Una propiedad interesante de las bases es que es posible definir a una matroide de una forma alternativa haciendo uso de ellas, esto se muestra en el siguiente teorema.

Teorema 7.5. Axiomatización por bases

Sea S un conjunto finito, decimos que \mathcal{B} es el conjunto de bases de una matroide si y solo si para cualquier par de conjuntos B_1 y B_2 en \mathcal{B} se cumple que para toda x en $B_1 \setminus B_2$ existe una y con la propiedad que $(B_1 \cup \{y\}) \setminus \{x\}$ pertenece a \mathcal{B} .

Demostración. Sea $M = (S, \mathcal{F})$ una matroide, como el conjunto vacío es independiente es claro que $\mathcal{B}(M)$ es diferente del vacío (existe por lo menos un elemento que es base en M). Al mismo tiempo, si tomamos 2 bases B_1, B_2 en B(M) y consideramos una x arbitraria en $B_1 \setminus B_2$ entonces por el teorema 7.2 existe y en $B_2 \setminus (B_1 \setminus \{x\})$ de tal forma que la cardinalidad de $(B_1 \cup \{y\}) \setminus \{x\}$ es igual a la cardinalidad de B_2 y donde

 $(B_1 \cup \{y\}) \setminus \{x\}$ es independiente. Además, por el corolario 7.4 podemos concluir que $(B_1 \cup \{y\}) \setminus \{x\}$ es base.

Por lo tanto para cualquier par de conjuntos B_1 y B_2 en $\mathcal{B}(M)$ se cumple que para toda x en $B_1 \setminus B_2$ existe una y con la propiedad que $(B_1 \cup \{y\}) \setminus \{x\}$ pertenece a $\mathcal{B}(M)$.

Ahora por el otro lado, supongamos que existe \mathcal{B} una familia de subconjuntos de S con la propiedad que para cualquier par de conjuntos B_1 y B_2 en \mathcal{B} se cumple que para toda x en $B_1 \setminus B_2$ existe una y con la propiedad que $(B_1 \cup \{y\}) \setminus \{x\}$ pertenece a \mathcal{B} . Decimos que un conjunto es independiente si es un subconjunto de cualquier elemento en \mathcal{B} .

Claramente, el conjunto vacío es independiente y además se cumple que si X es independiente y Y es un subconjunto de X entonces Y también es independiente. Por lo tanto, las propiedades 1 y 2 de la definición de matroides se cumplen.

Ahora, sean X y Y dos subconjuntos independientes de S en donde la cardinalidad de X es igual a k y la cardinalidad de Y es igual a k + 1. Como X es independiente entonces existe B_1 en \mathcal{B} de tal forma que X es un subconjunto de B_1 y de forma análoga como Y es independiente entonces existe B_2 en \mathcal{B} de tal forma que Y es un subconjunto de B_2 .

Para facilitar la notación sean

$$X = \{x_1, x_2, \dots, x_k\}$$

$$Y = \{y_1, y_2, \dots, y_{k+1}\}$$

$$B_1 = \{x_1, x_2, \dots, x_k, b_1, \dots, b_q\}$$

$$B_2 = \{y_1, y_2, \dots, y_{k+1}, c_1, \dots, c_{q-1}\}.$$

Sea $W = B_1 \setminus \{b_1\}$, entonces existe z en B_2 tal que $W \cup \{z\}$ está en \mathcal{B} . Si z está en Y entonces $X \cup \{z\}$ es independiente y se cumple la propiedad 3. Si z no es un elemento de Y, sea $W_1 = (W \cup \{z\}) \setminus \{b_2\}$. De nuevo, existe z_1 en B_2 tal que $W_1 \cup \{z_1\}$ está en \mathcal{B} . Si z_1 está en Y entonces $X \cup \{z_1\}$ es independiente y se cumple la propiedad 3.

Si z_1 no es un elemento de Y entonces se repite el mismo procedimiento para $b_3, b_4, \ldots b_q$, como la cardinalidad de $\{b1, b2, \ldots, b_q\}$ es mayor a la cardinalidad de $\{c1, c2, \ldots, c_{q-1}\}$ eventualmente existe z_j en Y, lo que implica que $X \cup \{z_j\}$ es independiente y se cumple la propiedad 3 y por lo tanto \mathcal{B} es el conjunto de bases de una matroide y el teorema se cumple.

51

7.2. Función rango

El rango de un conjunto es una propiedad clave del álgebra lineal, aprovechando la intersección que existe entre independencia e independencia lineal decimos que para una matroide la función rango queda definida como:

Definición 7.6. Sea $M=(S,\mathcal{F})$ una matroide, la **función rango** ρ se define como una función que va del conjunto potencia de S a los enteros no negativos, de tal forma que si A es un subconjunto arbitrario de S entonces $\rho(A)$ es igual a la cardinalidad del subconjunto independiente más grande de A.

Es claro que esta definición es equivalente para espacios vectoriales a la del rango de un conjunto de vectores. Algunas propiedades de la función rango que salen casi directo de la definición son:

Corolario 7.7. Sea $M = (S, \mathcal{F})$ una matroide y ρ su función rango entonces el rango del conjunto vacío es igual a cero.

Demostración. Como el conjunto vacío es el único subconjunto de sí mismo, como este es independiente y no contiene ningún elemento, entonces $\rho(\emptyset) = 0$.

Corolario 7.8. Sea $M = (S, \mathcal{F})$ una matroide, ρ su función rango y A, B dos subconjuntos de S tales que A es un subconjunto de B entonces $\rho(B) \ge \rho(A)$.

Demostración. Como todos los subconjuntos de A son subconjuntos de B no puede existir un subconjunto de A independiente que se más grande que todos los subconjuntos independientes de B. Por lo tanto $\rho(B) \geq \rho(A)$. \square

Corolario 7.9. Sea $M = (S, \mathcal{F})$ una matroide y ρ su función rango, entonces para todo subconjunto A de S se cumple que $\rho(A)$ es no negativo y que $\rho(A)$ es menor o igual a la cardinalidad de A.

Demostración. Sea A un subconjunto de S arbitrario. Como la cardinalidad de un conjunto es siempre no negativa eso implica que $\rho(A)$ es siempre no negativa. El subconjunto de A de mayor cardinalidad es el mismo por lo tanto $\rho(A)$ es menor o igual a la cardinalidad de A

Corolario 7.10. Sea $M = (S, \mathcal{F})$ una matroide y ρ su función rango, entonces para todo subconjunto X de S y para todo elemento y de S se cumple que

$$\rho(X) \le \rho(X \cup \{y\}) \le \rho(X) + 1.$$

Demostración. La desigualdad sale directo de que para todo conjunto X se cumple que el agregar un elemento y a este puede incrementar la cardinalidad de su subconjunto independiente más grande en máximo una unidad.

Corolario 7.11. Sea $M=(S,\mathcal{F})$ una matroide y ρ su función rango, supongamos que para X subconjunto de S y para x,y elementos de S se cumple que

$$\rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\})$$

entonces

$$\rho(X) = \rho(X \cup \{x\} \cup \{y\}).$$

Demostración. Supongamos que para X subconjunto de S y para x,y elementos de S se cumple que

$$\rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\}).$$

Sea $A = X \cup \{x\} \cup \{y\}$, es claro por el corolario 7.9 que $\rho(A) \ge \rho(X)$. Supongamos que $\rho(A) > \rho(X)$, sea Y un subconjunto independiente de X máximo. Como $\rho(A) > \rho(X)$ eso implica que $Y \cup \{x\}$ es independiente o que $Y \cup \{y\}$ es independiente, ambas afirmaciones son falsas porque claramente contradicen que $\rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\})$. Por lo tanto, $\rho(A) = \rho(X)$ y el corolario se cumple.

Corolario 7.12. designaldad submodular

Sea $M=(S,\mathcal{F})$ una matroide y ρ su función rango, supongamos que A,B son dos subconjuntos arbitrarios de S entonces

$$\rho(A \cup B) + \rho(A \cap B) \le \rho(A) + \rho(B).$$

Demostración. Para facilitar la notación sea $\rho(A \cup B) = p$ y sea $\rho(A \cap B) = q$. Sea X un subconjunto independiente de $A \cap B$ de cardinalidad q entonces existe un conjunto Y con las siguientes propiedades:

- 1. Y es independiente.
- 2. X es un subconjunto de Y.
- 3. Y es un subconjunto de $A \cup B$.
- 4. La cardinalidad de Y es p.

A Y lo podemos escribir como $Y = X \cup V \cup W$, donde V es un subconjunto independiente de $A \setminus B$. Además se cumple que $X \cup V$ es un subconjunto independiente de B y $X \cup W$ es un subconjunto independiente de A. Vale la pena mencionar que X, V, W son tres conjuntos ajenos y por lo tanto la cardinalidad de $X \cup V$ más la cardinalidad de $X \cup W$ es igual a dos veces la cardinalidad de X más la cardinalidad de X y por construcción esto es igual a $\rho(A \cup B) + \rho(A \cap B)$.

Como $\rho(B)$ es mayor igual que la cardinalidad de $X \cup V$ y $\rho(A)$ es mayor igual que la cardinalidad de $X \cup W$ esto implica que

$$\rho(A \cup B) + \rho(A \cap B) \le \rho(A) + \rho(B).$$

De igual forma que con las bases existe una forma de definir las matroides a través de su función rango, en particular si una función cumple 7.7, 7.10 y 7.11 entonces es una función rango. El resultado se ve formalmente en el siguiente teorema:

Teorema 7.13. Axiomas de rango 1

Una función ρ que va del conjunto potencia de S a los enteros no negativos es la función rango de una matroide en S si y solo si para todo X subconjunto de S y para todos x, y elementos de S se cumple que:

- 1. $\rho(\emptyset) = 0$.
- 2. $\rho(X) \le \rho(X \cup \{y\}) \le \rho(X) + 1$.
- 3. $Si \ \rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\}) \ entonces \ \rho(X) = \rho(X \cup \{x\} \cup \{y\}).$

Demostración. Si ρ es la función rango de M por los corolarios 7.7, 7.10 y 7.11, claramente se cumplen los puntos 1,2 y 3 del teorema.

Supongamos que tenemos una función ρ que va del conjunto potencia de S a los enteros no negativos y que además para ρ se cumplen los puntos 1,2 y 3 del teorema.

Decimos que X es un subconjunto independiente de S si y solo si $\rho(X)$ es igual a la cardinalidad de X. Es claro a partir de esta definición que el conjunto vacío es independiente.

Supongamos que A subconjunto de S es independiente y sea B un subconjunto arbitrario de A, supongamos también que B no es independiente. Como B no es independiente eso implica que $\rho(B)$ es estrictamente menor a la cardinalidad de B, sea

$$A \setminus B = \{c_1, c_2, \dots c_k\},\$$

por el punto 2 del teorema tenemos que $\rho(B) \leq \rho(B \cup \{c_1\}) \leq \rho(B) + 1$, si aplicamos esta propiedad k veces obtenemos que $\rho(B) \leq \rho(B \cup \{c_1, c_2, \ldots c_k\}) = \rho(A) \leq \rho(B) + k$. Por el otro lado, la cardinalidad de A es igual a la cardinalidad de B más k y como $\rho(B)$ es estrictamente menor a la cardinalidad de B, entonces $\rho(A)$ es estrictamente menor que su cardinalidad lo cual claramente es una contradicción porque A es independente y por lo tanto B es independente.

Ahora, sean X,Y dos conjuntos independientes con la propiedad de que la cardinalidad de Y es mayor a la cardinalidad de X por una unidad, para facilitar la notación sean

$$X = \{x_1, x_2, \dots, x_q, y_{q+1}, \dots y_k\}$$

$$Y = \{x_1, x_2, \dots, x_q, z_{q+1}, \dots z_{k+1}\}$$

donde y_i es distinto a z_j para toda i y para toda j.

Supongamos que para toda j se tiene que $X \cup \{z_j\}$ no es independente, esto implica que $\rho(X) = \rho(X \cup \{z_j\})$ para toda j. Si aplicamos la propiedad $3 \ k+1-q$ veces obtenemos que $\rho(X \cup \{z_{q+1}, \ldots z_{k+1}\}) = \rho(X)$. Además sabemos que $X \cup \{z_{q+1}, \ldots z_{k+1}\} = X \cup Y$, lo cual implicaría que $\rho(Y) = \rho(X)$, esto es claramente una contradicción porque esto implicaría que $\rho(X)$ no es independiente por lo tanto existe $\rho(X)$ tal que $\rho(X)$ es independiente y podemos concluir que el teorema se cumple.

Además de esta forma de definir a las matroides usando la función rango existe otra, en particular si una función cumple 7.9, 7.8 y 7.12 entonces es una función rango para alguna matroide. El siguiente teorema muestra formalmente como sucede esto:

Teorema 7.14. Axiomas de rango 2

Una función ρ que va del conjunto potencia de S a los enteros no negativos es la función rango de una matroide en S si y solo si para todo par X,Y de subconjuntos de S se cumple que:

- ρ(X) toma un valor que se encuentra entre cero y la cardinalidad de X.
- 2. Si X es un subconjunto de Y esto implica que $\rho(X) \leq \rho(Y)$.

3.
$$\rho(A \cup B) + \rho(A \cap B) \le \rho(A) + \rho(B)$$
.

Demostración. Si ρ es la función rango de M por los corolarios 7.9, 7.8 y 7.12, claramente se cumplen los puntos 1,2 y 3 del teorema.

Supongamos que tenemos una función ρ que va del conjunto potencia de S a los enteros no negativos y que además para ρ se cumplen los puntos 1,2 y 3 del teorema.

Al igual que en la última demostración, decimos que X es un subconjunto independiente de S si y solo si $\rho(X)$ es igual a la cardinalidad de X. Es claro a partir de esta definición que el conjunto vacío es independiente.

Claramente, por el punto 1 se cumple que $\rho(\emptyset) = 0$.

Sea X un subconjunto arbitrario de S y y un elemento arbitrario de S, como la cardinalidad de $\{y\}$ es igual a uno es claro por el punto 1 que $\rho(\{y\}) \leq 1$. Además, sabemos que

$$\rho(X \cup \{y\}) \le \rho(X \cup \{y\}) + \rho(X \cap \{y\}) \le \rho(X) + \rho(\{y\}) \le \rho(X) + 1.$$

Si le agregamos la propiedad 2 del teorema obtenemos que $\rho(X) \leq \rho(X \cup \{y\}) \leq \rho(X) + 1$.

Sea A un subconjunto de S y sean x, y dos elementos de S tales que $\rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\})$. Por el punto 3 del teorema tenemos que

$$\rho(A \cup \{x\} \cup \{y\}) + \rho(A) \le \rho(X \cup \{x\} + \rho(X \cup \{y\})) = 2\rho(A),$$

por lo tanto $\rho(A \cup \{x\} \cup \{y\}) = \rho(A)$.

Como ρ cumple que

- 1. $\rho(\emptyset) = 0$.
- 2. $\rho(X) \le \rho(X \cup \{y\}) \le \rho(X) + 1$.
- 3. Si $\rho(X) = \rho(X \cup \{x\}) = \rho(X \cup \{y\})$ entonces $\rho(X) = \rho(X \cup \{x\} \cup \{y\})$.

Por el teorema 7.13 podemos concluir que ρ es la función rango de una matroide en S y por lo tanto se cumple el teorema.

Las matroides además de tener análogos con el álgebra lineal también tienen análogos con la teoría de gráficas, la siguiente sección muestra como es qué esto sucede.

7.3. Circuitos

En teoría de gráficas los circuitos son de vital importancia, en particular sería imposible definir que es un árbol sin el concepto de circuito. La siguiente definición viene de la intersección que existe entre la teoría de gráficas y las matroides ³, decimos que para una matroide los circuitos quedan definidos como:

Definición 7.15. Sea $M=(S,\mathcal{F})$ una matroide, decimos que C es un circuito si

- C es un conjunto dependiente.
- C es mínimo, es decir, no existe ningún subconjunto D de C tal que D es dependiente.

Al conjunto de todos los circuitos en M se le denota como C(M).

Algunas propiedades de los circuitos que salen casi directo de la definición son:

Corolario 7.16. 7.3 Sea $M = (S, \mathcal{F})$ una matroide, C un circuito en M y ρ su función rango entonces, $\rho(C)$ es igual a su cardinalidad menos uno.

³Si el lector no tiene familiaridad con la existencia de esta intersección, al finalizar esta sección tendrá claro cuál es la naturaleza de esta.

7.3. CIRCUITOS 57

Demostración. Por definición la cardinalidad del subconjunto independiente más grande de C es igual a la cardinalidad de C menos 1, por lo tanto $\rho(C)$ es igual a su cardinalidad menos uno.

Corolario 7.17. Sea $M = (S, \mathcal{F})$ una matroide y C un circuito en M. Entonces la cardinalidad de C es menor iqual que $\rho(S) + 1$.

Demostración. Si $\rho(S) = k$ esto implica que el subconjunto independiente de S más grande es de cardinalidad k si a este conjunto le agregamos un elemento obtenemos un circuito de cardinalidad k+1, es claro que este circuito es el de mayor cardinalidad de todos los elementos de $\mathcal{C}(M)$ y por lo tanto la cardinalidad de C es menor igual que $\rho(S)+1$ para todo circuito C.

Corolario 7.18. Sea $M = (S, \mathcal{F})$ una matroide, si $\mathcal{C}(M) = \emptyset$ entonces $\mathcal{B}(M) = \{S\}$.

Demostración. Supongamos que $C(M) = \emptyset$, esto implicaría que no existe ningún subconjunto dependiente de S y por lo tanto S es un subconjunto independiente de S máximo. Por lo tanto, $\mathcal{B}(M) = \{S\}$.

Corolario 7.19. Sea $M = (S, \mathcal{F})$ una matroide, C un circuito en M y A un subconjunto propio de C. Entonces A es un subconjunto independiente de S.

Demostración. Si A fuera dependiente esto implicaría que C no es mínimo como se pide en la definición, por lo tanto A es un subconjunto independiente de S.

Corolario 7.20. Sea $M = (S, \mathcal{F})$ una matroide y sean C_1, C_2 dos circuitos distintos en M. Entonces, C_1 no es un subconjunto de C_2 .

Demostración. Supongamos que C_1 es un subconjunto de C_2 , entonces $C_2 = C_1 \cup (C_2 \setminus C_1)$. Como $(C_2 \setminus C_1)$ no es vacío entonces C_1 es un subconjunto propio de C_2 lo que implica que C_1 es un subconjunto independiente en S. Esto es claramente una contradicción porque C_1 es un circuito, por lo tanto C_1 no es un subconjunto de C_2 .

Corolario 7.21. Sea $M = (S, \mathcal{F})$ una matroide, sean C_1, C_2 dos circuitos distintos en M y sea z un elemento en $C_1 \cap C_2$. Entonces, existe un circuito C_3 subconjunto de $(C_1 \cup C_2) \setminus \{z\}$.

Demostraci'on. Supongamos que no existe un circuito C_3 subconjunto de $(C_1 \cup C_2) \setminus \{z\}$. Esto implica directamente que $(C_1 \cup C_2) \setminus \{z\}$ es un subconjunto independiente de S, lo cual implica que $\rho((C_1 \cup C_2) \setminus \{z\}) = \rho((C_1 \setminus \{z\}) + (C_2 \setminus \{z\}))$ es igual a la cardinalidad de $C_1 \cap C_2$ menos uno. Además, por el corolario tenemos que $\rho(C_1)$ es igual a la cardinalidad de C_1 menos uno y que $\rho(C_2)$ es igual a la cardinalidad de C_2 menos uno. Si aplicamos la desigualdad de submodularidad obtenemos que $\rho(C_1 \cup C_2) + \rho(C_1 \cap C_2)$ es menor o igual que la cardinalidad de C_1 más la cardinalidad de C_2 menos dos lo cual es igual a la cardinalidad de $C_1 \cup C_2$ más la cardinalidad de $C_1 \cap C_2$ menos dos.

Ahora, sabemos que $C_1 \cap C_2$ es un subconjunto independiente de S y por lo tanto $\rho(C_1 \cap C_2)$ es igual a la cardinalidad de $C_1 \cap C_2$. Por lo tanto, $\rho(C_1 \cup C_2)$ es menor o igual que la cardinalidad de $C_1 \cup C_2$ menos dos. Además, $\rho(C_1 \cup C_2) \geq \rho((C_1 \cup C_2) \setminus \{z\})$, donde $\rho((C_1 \cup C_2) \setminus \{z\})$ es igual a la cardinalidad de $C_1 \cup C_2$ menos uno.

Por lo tanto, la cardinalidad de $C_1 \cup C_2$ menos uno es menor o igual a la cardinalidad de $C_1 \cup C_2$ menos dos, esto implicaría que 1 > 2, lo cual claramente es una contradicción y podemos concluir que existe un circuito C_3 subconjunto de $(C_1 \cup C_2) \setminus \{z\}$.

De igual forma que con las bases y con la función rango existe una forma de definir las matroides a través de sus circuitos, en particular si una familia $\mathcal C$ de subconjuntos de S cumple 7.20 y 7.21 entonces son los circuitos de una matroide. Antes de enunciar y demostrar esto se requiere de un lema y dos teoremas.

Lema 7.22. Sea $M = (S, \mathcal{F})$ una matroide, A un subconjunto independiente de S y x un elemento de x. Entonces $A \cup \{x\}$ contiene a lo más un circuito.

Demostración. Supongamos que existen dos circuitos C_1, C_2 subconjuntos de $A \cup \{x\}$. Como A es un subconjunto independiente de S, tenemos que x está contenida en $C_1 \cap C_2$. Por 7.21 existe un circuito C_3 subconjunto de $(C_1 \cup C_2) \setminus \{x\}$, lo que directamente implica que C_3 está contenido en

7.3. CIRCUITOS 59

A, lo cual es claramente una contradicción porque A es un subconjunto independiente de S. Por lo tanto $A \cup \{x\}$ contiene a lo más un circuito. \square

Un corolario directo de este resultado que vale la pena mencionar el siguiente:

Corolario 7.23. Sean $M = (S, \mathcal{F})$ una matroide, B una base en M y x un elemento en $S \setminus B$. Entonces, existe un único circuito C tal que C es un subconjunto de $B \cup \{x\}$.

Demostración. La demostración es directa del lema 7.22, del hecho de que todas las bases en M son subconjuntos independientes de S y que estas son subconjuntos independientes máximos (si les unes un elemento se vuelven dependientes).

A este circuito C = C(x, B) se le llama el **circuito fundamental** de x en la base B. Un resultado importante de esta definición es el siguiente:

Teorema 7.24. Sean $M = (S, \mathcal{F})$ una matroide y B una base en M, entonces para toda x en $S \setminus B$ $(B \setminus \{y\}) \cup \{x\}$ es una base en M si y solo si y pertenece a C(x, B) o si y = x.

Demostración. Si y = x el resultado es directo porque por hipótesis $B = (B \setminus \{x\}) \cup \{x\}$ es una base.

Supongamos que $(B \setminus \{y\}) \cup \{x\}$ es una base en M, supongamos además que y no pertenece a C(x,B). Como y no pertenece a C(x,B), tenemos que C(x,B) es un subconjunto de la base $(B \setminus \{y\}) \cup \{x\}$ y por lo tanto que C(x,B) es un subconjunto independiente de S, lo cual es claramente una contradicción porque C(x,B) es un subconjunto dependiente de S y podemos entonces concluir que y pertenece a C(x,B).

Por el otro lado, supongamos que y pertenece a C(x,B) y además supongamos que $(B \setminus \{y\}) \cup \{x\}$ no es una base. Como $(B \setminus \{y\}) \cup \{x\}$ tiene la misma cardinalidad que B y no es base, como todas las bases tienen el mismo tamaño podemos ver que $(B \setminus \{y\}) \cup \{x\}$ es un subconjunto dependiente de S. Ahora, $\text{como}(B \setminus \{y\}) \cup \{x\}$ es dependiente entonces existe un circuito C' (distinto de C(x,B) subconjunto de $(B \setminus \{y\}) \cup \{x\}$, lo que implica que $B \cup \{x\}$ contiene dos circuitos distintos, lo cual es una contradicción al lema 7.22 y por lo tanto $(B \setminus \{y\}) \cup \{x\}$ es una base y el teorema es cierto.

Antes de mostrar la equivalencia entre circuitos y matroides es necesario mostrar el siguiente resultado, este teorema puede ser interpretado como un resultado más fuerte que el corolario 7.21.

Teorema 7.25. Sean $M = (S, \mathcal{F})$ una matroide, C_1, C_2 dos circuitos en M y x un elemento en $C_1 \cap C_2$, entonces para todo elemento y en $C_1 \setminus C_2$ existe un circuito C tal que

- 1. y pertenece a C.
- 2. C es un subconjunto de $(C_1 \cup C_2) \setminus \{x\}$.

Demostración. Supongamos que existen dos circuitos C_1, C_2 , un elemento x en $C_1 \cap C_2$ y un elemento y en $C_1 \setminus C_2$ que muestran que el teorema es falso, además supongamos la cardinal de $C_1 \cup C_2$ es mínima con esta propiedad, es decir no existen otros dos circuitos con la cardinalidad de su unión menor a la de C_1 y C_2 que no cumplen esta propiedad.

Por el corolario 7.21, existe un circuito C_3 subconjunto de $(C_1 \cup C_2) \setminus \{x\}$ (no tenemos garantía alguna de que y pertenezca a C_3).

Como C_3 no es un subconjunto de C_1 (corolario 7.20), tenemos que $C_3 \cap (C_2 \setminus C_1)$ no es vacío. Sea z en $C_3 \cap (C_2 \setminus C_1)$ arbitraria, podemos ver que z pertenece a $C_3 \cap C_2$ y que x pertenece a $C_2 \setminus C_3$. Como y no pertenece a $C_2 \cup C_3$ podemos ver que $C_2 \cup C_3$ es un subconjunto propio de $C_1 \cup C_2$. Por la minimalidad de $C_1 \cup C_2$ existe C_4 tal que x pertenece a C_4 y C_4 es un subconjunto de $(C_2 \cup C_3) \setminus \{z\}$.

Ahora, tenemos que x pertenece a $C_1 \cap C_4$ y que y no pertenece a $C_2 \cup C_3$. Como y no pertenece a $C_2 \cup C_3$ tenemos que y pertenece a $C_1 \setminus C_4$. Además tenemos que $C_1 \cup C_4$ es un subconjunto de $C_1 \cup C_2^4$, de nuevo por la minimalidad de $C_1 \cup C_2$ tenemos que existe un circuito C_5 tal que y pertenece a C_5 y donde C_5 es un subconjunto de $(C_1 \cup C_4) \setminus \{x\}$. Como $C_1 \cup C_4$ es un subconjunto de $C_1 \cup C_2$ tenemos que C_5 es un subconjunto de $(C_1 \cup C_2) \setminus \{x\}$, lo cual claramente es una contradicción porque viola directamente la hipótesis de que para C_1, C_2, x y y el teorema es falso y por lo tanto el teorema es cierto.

Ahora sí, podemos ver la equivalencia que existen entre circuitos y matroides. Una nota importante es que en la última demostración únicamente

 $^{^4}$ es un subconjunto propio porque $C_1 \cup C_4$ no contiene a z y $C_1 \cup C_2$ si la contiene.

7.3. CIRCUITOS 61

se utilizan los corolarios 7.20 y 7.21, entonces el siguiente teorema en vez de pedir las propiedades C_1 y C_2 podría haber pedido en su lugar las propiedades 7.20 y 7.25.

Teorema 7.26. Axiomatización por circuitos

Una colección C de subconjuntos de S es el conjunto de circuitos de una matroide si y solo si se cumple que

- 1. Si dos conjuntos distintos X, Y pertenecen a C, entonces X no es un subconjunto de Y.
- 2. Si C_1, C_2 son dos subconjuntos distintos de C y z es un elemento en $C_1 \cap C_2$, entonces existe C_3 en C tal que C_3 es un subconjunto de $(C_1 \cup C_2) \setminus \{z\}$.

Demostración. Si \mathcal{C} es la colección de circuitos de una matroide sabemos por los corolarios 7.20 y 7.21 que las propiedades 1 y 2 se cumplen. Ahora, sea $\{x_1, x_2, \ldots, x_q\}$ una familia ordenada arbitraria de objetos en S y sea θ de la siguiente manera

$$\theta_i = \begin{cases} 0 & \text{si } \{x_1, x_2, \dots, x_i\} \text{ contiene a un elemento } C \text{ de } \mathcal{C} \\ & \text{tal que } x_i \text{ pertenece a } C \\ 1 & \text{en otro caso.} \end{cases}$$

Sea t una función que va de subconjuntos ordenados de S a los enteros no negativos definida como

$$t(\{x_1, x_2, \dots, x_q\}) = \sum_{i=1}^{q} \theta_i, \tag{7.1}$$

Afirmamos 5 que para toda permutación π se cumple que

$$t(\{x_1, x_2, \dots, x_q\}) = t(\{x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(q)}\}).$$
 (7.2)

A partir de esto definimos r como una función que va de los subconjuntos de S a los enteros no negativos y que sigue la regla de correspondencia

⁵La demostración de la afirmación se muestra más adelante.

 $r(A) = t(\{x_1, x_2, \dots, x_q\})$, donde $x_1, x_2, \dots, x_q\}$ es una representación ordenada de los elementos de A. Por la afirmación mencionada en la ecuación 7.2 sabemos que r está bien definida.

Ahora, es claro que $r(\emptyset) = 0$ porque la suma sobre ningún elemento siempre es cero. Además, podemos ver que para cualquier subconjunto X de S y para cualquier elemento y de S claramente se cumple que $r(X) \leq r(X \cup \{y\}) \leq r(X) + 1$ porque al agregar un elemento al conjunto la función no puede decrecer por propiedades de la suma y está a lo más puede crecer en una unidad.

Por el otro lado, sea A un subconjunto de S y sean x,y dos elementos de S y supongamos que

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

entonces por definición se cumple que existen C_1 , C_2 en \mathcal{C} tales que x pertenece a C_1 , con C_1 subconjunto de $X \cup \{x\}$ y de forma análoga y pertenece a C_2 , con C_2 subconjunto de $X \cup \{y\}$. Por lo tanto, podemos concluir que $r(A) = r(X \cup \{x\} \cup \{y\})$ y por el teorema 7.13 r es la función rango de una matroide y podemos concluir que \mathcal{C} es la familia de circuitos de esa matroide.

La demostración de arriba no está completa, hace falta la demostración de la afirmación mencionada en 7.2. Esta se muestra a continuación.

Lema 7.27. Para la función t definida 7.1 se cumple que para cualquier familia ordenada $\{x_1, x_2, \ldots, x_q\}$ de objetos de S y para cualquier permutación π que

$$t(\{x_1, x_2, \dots, x_q\}) = t(\{x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(q)}\}).$$

Demostración. Para demostrar el lema solo es necesario mostrar que

$$t({x_1, x_2, \dots x_{q-1}, x_q}) = t({x_1, x_2, \dots, x_q, x_{q-1}}),$$

esto es porque toda permutación puede ser representada como un producto de ciclos de orden dos (ver Fraleigh (1976)). Para facilitar la notación sean

$$Y = t(\{x_1, x_2, \dots x_{q-1}, x_{q-2}\}),$$

7.3. CIRCUITOS 63

$$t(Y) = a,$$

$$t(Y, x_{q-1}) = a_1,$$

$$t(Y, x_q) = a_2,$$

$$t(Y, x_{q-1}) = a_1,$$

$$t(Y, x_{q-1}, x_q) = a_{1,2},$$

$$t(Y, x_q, x_{q-1}) = a_{2,1}.$$

Para demostrar lo deseado es necesario suponer cuatro casos distintos:

- 1. Supongamos que no existe C en C subconjunto de $Y \cup x_{q-1}$ tal que x_{q-1} es un elemento de C y supongamos que no existe C en C subconjunto de $Y \cup x_q$ tal que x_q es un elemento de C. Entonces podemos ver que $a_1 = a_2 = a$, entonces existen dos escenarios posibles:
 - a) Existe C en C subconjunto de $Y \cup \{x_{q-1}\} \cup \{x_q\}$ tal que contiene a x_{q-1} y a x_q lo que implicaría que

$$a_{1,2} = a_1 = a_2 = a_{2,1}$$
.

b) No existe C en C subconjunto de $Y \cup \{x_{q-1}\} \cup \{x_q\}$ tal que contiene a x_{q-1} y a x_q lo que implicaría que

$$a_{1,2} = a_1 + 1 = a_2 + 1 = a_{2,1}.$$

En los dos escenarios se cumple que $a_{1,2} = a_{2,1}$ como deseamos.

2. Supongamos que existe C_2 en \mathcal{C} contenido en $Y \cup \{x_{q-1}\}$ tal que contiene a x_{q-1} y además supongamos que existe C_1 en \mathcal{C} contenido en $Y \cup \{x_{q-1}\} \cup \{x_q\}$ tal que contiene a x_{q-1} y a x_q . Entonces por hipótesis sabemos que existe C_3 en \mathcal{C} subconjunto de $Y \cup \{x_q\}$ tal que contiene a x_q y podemos concluir que

$$a_{1,2} = a_1 = a = a_2 = a_{2,1}.$$

3. Supongamos que existe C_2 en \mathcal{C} contenido en $Y \cup \{x_{q-1}\}$ tal que contiene a x_{q-1} y además supongamos que no existe C_1 en \mathcal{C} contenido en $Y \cup \{x_{q-1}\} \cup \{x_q\}$ tal que contiene a x_{q-1} y a x_q . A partir de esto podemos ver que existen dos escenarios posibles:

a) Existe C_3 en $\mathcal C$ subconjunto de $Y \cup \{x_q\}$ tal que contiene a x_q y podemos concluir que

$$a_{1,2} = a_1 = a = a_2 = a_{2,1}.$$

b) No existe C_3 en \mathcal{C} subconjunto de $Y \cup \{x_q\}$ tal que contiene a x_q y podemos concluir que

$$a_{1,2} = a_1 + 1 = a + 1 = a_2 = a_{2,1}.$$

En los dos escenarios se cumple que $a_{1,2} = a_{2,1}$ como deseamos.

4. Existe C en C subconjunto de $Y \cup \{x_q\}$ tal que contiene a x_q . Este caso es análogo a los casos 2 y 3, podemos concluir que $a_{1,2} = a_{2,1}$.

Después de plantear todos los casos podemos concluir que

$$t(\{x_1, x_2, \dots x_{q-1}, x_q\}) = t(\{x_1, x_2, \dots, x_q, x_{q-1}\})$$

y que por lo tanto el lema es cierto.

El siguiente resultado muestra de donde viene la conexión entre las matroides y las gráficas, además muestra de donde viene la definición de circuitos.

Teorema 7.28. Sea G = (V.E) una gráfica entonces los ciclos en G forman los circuitos de una matroide.

Demostración. Claramente ningún ciclo contiene a otro ciclo porque se pide minimalidad en la definición de estos. Sean C_1 y C_2 dos ciclos en G y sea e una arista en $C_1 \cap C_2$ ⁶. Para facilitar la notación sean

$$C_1 = \{e, a_1, \dots, a_p\}$$

$$C_2 = \{e, b_1, \dots, b_q\},\$$

Es claro que el conjunto $(C_1 \cup C_2) \setminus \{e\} = \{a_1, \dots, a_p, b_1, \dots, b_q\}$ contiene un ciclo porque a_1 y b_q inciden en el mismo vértice.

Por lo tanto, por el teorema 7.26, los ciclos en G forman los circuitos de una matroide. $\hfill\Box$

La siguiente sección muestra cómo toda esta teoría se aplica en particular a los problemas de optimización y mostraremos un algoritmo basado en esta teoría muy usado en la investigación de operaciones.

⁶En este caso representamos a un ciclo por el conjunto de aristas que lo forman

7.4. El algoritmo glotón

Esta sección muestra el resultado más importante sobre matroides para este trabajo y ejemplifica porque estas son muy importantes en la investigación de operaciones. Para definir el algoritmo glotón es necesario antes definir qué es una matroide con pesos y cuál es el problema de optimización asociada a este.

Definición 7.29. Decimos que (M, ω) es una **matroide con pesos** si $M = (S, \mathcal{F})$ es una matroide y ω es una función que va del conjunto potencia de S a los reales positivos, con la propiedad de que si $A = \{e_1, e_2, \ldots_e p\}$ es un subconjunto de S entonces se cumple que

$$\omega(A) = \sum_{k=0}^{p} \omega(e_k).$$

De forma casi directa se define el algoritmo de optimización de la siguiente manera:

Definición 7.30. Sea (M, ω) una matroide, si $M = (S, \mathcal{F})$ definimos el problema de optimización (\mathcal{F}, ω) como encontrar el conjunto A en \mathcal{F} con la propiedad de que $\omega(A)$ sea máximo, es decir no existe B en \mathcal{F} tal que $\omega(B) > \omega(A)$.

Ahora sí ya encaminados podemos definir el algoritmo glotón, más adelante veremos que este además de ser sencillo y fácil de entender, converge para el problema (\mathcal{F}, ω) . El seudocódigo del algoritmo es el siguiente:

Algoritmo 8: Glotón

```
input: Una matroide con pesos (M, \omega).
output: Un conjunto A en \mathcal{F}.
```

- 1 Sea $J = \emptyset$;
- 2 repeat
- 3 Escogemos e^* en S tal que $\omega(J \cup \{e^*\}) \ge \omega(J \cup \{e\})$ para toda e tal que $J \cup \{e\}$ pertenece a \mathcal{F} (con $J \cup \{e^*\}$ también en \mathcal{F}) y con $\omega(J \cup \{e^*\}) > \omega(J)$;
- 4 Actualizamos $J = J \cup \{e^*\};$
- **5 until** hasta que no existe e no en J con la propiedad de que $J \cup \{e\}$ pertenece a \mathcal{F} ;

El siguiente resultado muestra que el algoritmo converge a pesar de ser relativamente sencillo.

Teorema 7.31. Sean $M=(S,\mathcal{F})$ y ω una función de pesos para M, entonces el algoritmo glotón converge para el problema de optimización (\mathcal{F},ω) .

Demostración. Sea B la base en M elegida por el algoritmo glotón 7 , supongamos que existe otra base T tal que $\omega(T) > \omega(B)$ y con la propiedad de que la cardinalidad de $T \cap B$ es máxima en el sentido de que no existe T' tal que $\omega(T') > \omega(B)$ y la cardinalidad de $T' \cap B$ es estrictamente mayor a la cardinalidad de $T \cap B$.

Sea x_k el primer elemento que el glotón escogió en $B \setminus T$, por el corolario 7.23 existe un circuito $C(x_k, T)$ tal que x_k pertenece a $C(x_k, T)$ y que $C(x_k, T)$ es un subconjunto de $T \cup \{x_k\}$.

Sea y en $C(x_k, T) \setminus B$ de tal forma que $(T \cup \{x_k\}) \setminus \{y\}$ es una base (teorema 7.5).

Ahora, sabemos que $\omega(y) \leq \omega(x_k)$ (porque el glotón lo escogió), como T tiene peso máximo eso implica que $\omega(y) = \omega(x_k)$ lo que también implica que $\omega(T) = \omega((T \cup \{x_k\}) \setminus \{y\})$, lo cual es claramente una contradicción porque la cardinalidad de $T \cap B$ es máxima. Por lo tanto, el algoritmo glotón converge para el problema de optimización (\mathcal{F}, ω) .

Algo muy interesante sobre el algoritmo es que al igual que en las secciones anteriores es posible definir a las matroides por medio del algoritmo glotón.

Teorema 7.32. Sea S un conjunto finito y sea \mathcal{F} una familia de subconjuntos (no vacía) de S con las siguientes propiedades:

- 1. Si A pertenece a \mathcal{F} y B es un subconjunto de A, entonces B pertenece a \mathcal{F} .
- 2. El algoritmo glotón converge para el problema de optimización (\mathcal{F}, ω) para toda función que va del conjunto potencia de S a los reales positivos.

 $^{^7}$ el algoritmo glotón siempre converge a una base porque frena cuando encuentra un subconjunto independiente de S máximo.

Entonces, \mathcal{F} es la familia de conjuntos independientes de una matroide.

Demostración. Para demostrar que \mathcal{F} es la familia de conjuntos independientes de una matroide solo es necesario ver que si X y Y pertenecen a \mathcal{F} y la cardinalidad de X es uno más la cardinalidad de Y, entonces existe un elemento v en $X \setminus Y$ tal que $Y \cup \{v\}$ pertenece a \mathcal{F} 3. Para facilitar la notación sean

$$X = \{x_1, x_2, \dots, x_n\}$$
$$Y = \{y_1, y_2, \dots, y_{n+1}\}.$$

Definimos ω una función que va del conjunto potencia de S a los reales positivos según la siguiente regla:

$$\omega(x_i) = u$$
 para toda i entre 0 y n , $\omega(y_j) = v$ para toda y_j en $X \setminus Y$, $\omega(e) = 0$ para toda e en $S \setminus (X \cup Y)$.

Supongamos que u > v y que queremos resolver el problema de optimización (\mathcal{F}, ω) , por hipótesis sabemos que el algoritmo glotón converge para este problema. El algoritmo en sus primeras n iteraciones escoge a $J = x_1, x_2, \ldots, x_n = X$ (sabemos esto porque X está en \mathcal{F} y porque todo subconjunto de X está en \mathcal{F}). Ahora tenemos dos escenarios posibles, el algoritmo ya convergió después de n pasos o todavía no converge y realiza por lo menos otra iteración. Supongamos que el algoritmo convergió. Sea t igual a la cardinalidad de $X \cap Y$, notamos que se cumple lo siguiente:

$$\omega(X) = n \cdot u$$

$$\omega(Y) = t \cdot u + (n+1-t)v.$$

Si u es igual a $\left(1+\frac{1}{2(n-t)}\right)v^8$, tenemos que $\omega(Y)>\omega(X)$. Por lo tanto, podemos concluir que el algoritmo no convergió porque claramente no encontró al óptimo. Como el algoritmo no convergió, este realiza por lo menos un paso más en el que selecciona y_j en $X\setminus Y$ de tal forma que $X\cup y_j$ pertenece a \mathcal{F} . Concluimos que se cumple 3 y por lo tanto \mathcal{F} es la familia de conjuntos independientes de una matroide.

 $^{^{8}}$ con este supuesto se sigue cumpliendo que u > v

Este teorema se puede rescribir de la siguiente forma para encontrar una forma de definir las matroides:

Corolario 7.33. Axiomatización por algoritmo glotón.

Una colección \mathcal{F} no vacía de subconjuntos de S es la familia de conjuntos independientes de S si y solo si

- 1. Si A pertenece a \mathcal{F} y B es un subconjunto de A, entonces B pertenece a \mathcal{F} .
- 2. Para toda función ω que va de S a los reales el algoritmo glotón escoge al conjunto A en $\mathcal F$ que maximiza la función

$$f(A) = \sum_{k=1}^{n} \omega(a_k) \ con \ A = \{a_1, \dots, a_n\}$$

es decir, no existe B en $\mathcal{F}talquef(B) > f(A)$.

Demostración. El corolario es un caso particular del teorema 7.32.