BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS

LICENCIATURA EN MATEMÁTICAS

MATROIDES Y CÓDIGOS: LA IDENTIDAD DE MACWILLIAMS

TESIS QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN MATEMÁTICAS

PRESENTA:

MIREYA DÍAZ LÓPEZ

DIRECTORES DE TESIS:

DR. CARLOS ALBERTO LÓPEZ ANDRADE

DR. CARLOS GUILLÉN GALVÁN

PUEBLA, PUE. MARZO 2021

II

Dedicado a mi hermosa familia: Eloy,
Elisa, Karla, Daniela y Armando.
Los amo

Agradecimientos

Le doy infinitas gracias a Dios por darme vida y salud, y por permitirme llegar a este punto de mi vida y compartir este logro con mi familia. Gracias por todas las bendiciones que me ha dado a lo largo de mi vida.

Para mis papás, María Elisa López Soriano y Eloy Díaz Ramos, no creo tener las palabras adecuadas para expresarles mi agradecimiento por todo lo que han hecho por mí durante toda mi vida, pero en ausencia de tales palabras, sólo me queda decirles gracias. En primer lugar, gracias por darme la vida. Aunque a veces todo me parece difícil trato de disfrutar la vida y realmente amo vivir. Gracias por darme una bonita familia, un hogar y una buena educación. Gracias por apoyarme en todos mis proyectos desde que era una niña. Gracias por pensar que puedo lograr todo lo que me proponga aunque yo misma no lo crea así. Gracias por trabajar sin cansancio para que a mis hermanas y a mí no nos faltara nada. Gracias por la comprensión en todos esos días en los que no pude ayudarlos o acompañarlos por las tareas que tenía pendientes. Gracias por estar siempre al pendiente de mí.

A mis hermanas, Karla Beatriz y Daniela les agradezco por soportarme durante tantos años. Yo sé lo difícil que es lidiar conmigo en muchas ocasiones, en especial cuando estoy estresada. A pesar de ello, nunca me dejaron sola. Muchas veces los chistes o anécdotas que contábamos me servían para sentirme mejor y poder continuar. Gracias por estar presentes en los mejores y peores momentos de mi vida. Me da gusto recordar todas las cosas que hemos vivido juntas e imaginar las que nos faltan por vivir. Como una vez lo dije, porque tengo dos hermanas sé que siempre tendré dos grandes amigas y doy infinitas gracias por eso.

A mi esposo, Armando Ortega Xique. Eres mi amor de estudiante, mi gran amor. Gracias por llegar a mi vida y quedarte en ella, por estar conmigo en todas mis facetas. Gracias por nunca dejar de echarme porras y acompañarme en mis días buenos y malos, por esperarme a la salida, incluso durante horas, por todas las cosas que vivimos juntos dentro de la universidad: las risas, los paseos, los desayunos y comidas juntos y por los detalles que me ayudaban a soportar los malos días. Gracias por escucharme con mucha paciencia cada vez que quería contarte algo y por aconsejarme. Además de mucho amor, siento una enorme admiración por ti. Eres mi mejor ejemplo de científico. Ojalá algún día yo tenga la mitad del amor que tú tienes por tu carrera. Eres mi biólogo favorito. Estoy feliz de que seamos una gran pareja y de poder compartir tantas cosas contigo.

A mis papás, a mis hermanas y a mi esposo quiero darles las gracias por siempre haber creído en

mí, por sus palabras de aliento, por su apoyo todas las ocasiones en las que sentí que no podía concluir mi licenciatura, por sus abrazos tan reconfortantes, por secar tantas lágrimas mías y en general por ser mis mejores amigos. Gracias también por su paciencia infinita al cuidarme en mis operaciones y cada vez que me enfermé. Es algo que tengo muy presente y no sé cómo se los pagaré. Una de las cosas que más anhelo en la vida es que ustedes se sientan tan orgullosos de mí como yo me siento de cada uno de ustedes y que se sientan tan felices de tenerme en su vida así como yo me siento por tenerlos conmigo. Los amo con todo mi corazón.

Agradezco al Dr. Carlos Alberto López Andrade por aceptarme como su tesista, por aceptar que trabajáramos juntos en varios proyectos a lo largo de mi carrera, por todos los aprendizajes que adquirí en los diversos cursos que me impartió, por todas las asesorías y por inculcarme el gusto por el área de álgebra, la cual espero seguir trabajando en un futuro.

Gracias a todos mis amigos con los cuales compartí muchas horas en clases, en la biblioteca y en las palapas. Gracias por haber estado conmigo en el día más importante para mí. Espero que nuestra amistad dure muchos años más. Los quiero mucho a todos. Toño: fuiste mi amigo durante prácticamente toda la licenciatura. Compartimos muchas clases y anécdotas, y nos apoyamos mutuamente académica y personalmente. Te agradezco que me hayas abierto tu corazón en tantas ocasiones, por tenerme tanta confianza y haberme escuchado en tantas ocasiones. Are: agradezco mucho haberte conocido, aunque me hubiera gustado haberlo hecho antes. Ambas teníamos sentimientos y pensamientos muy parecidos respecto a la carrera y el apoyo que nos dimos fue de gran ayuda para poder concluirla. Me gusta mucho contar con una persona como tú. Angel: gracias por todas las pláticas que tuvimos y por ser tan ocurrente, optimista y creyente. América: gracias por ser tan optimista. Una plática contigo es suficiente para pensar de manera positiva y sonreír. A Wendy, Eduardo Iván y Baruch les agradezco su amistad y los buenos momentos que pasamos juntos.

Agradezco a mi codirector de tesis, el Dr. Carlos Guillén Galván por la inmensa ayuda que nos brindó en especial en los primeros semestres de la carrera y por asesorarme en algunos temas de mi tesis.

Agradezco a mis sinodales, Dr. Agustín Contreras Carreto y Dr. Henry Chimal Dzul por el tiempo dedicado a la revisión de mi tesis.

Índice general

Introducción

La teoría de matroides es una rama de las matemáticas de reciente creación. Surgió en la primera mitad del siglo XX. Ha tenido un enorme crecimiento y actualmente es una de las líneas de investigación en matemáticas de mayor importancia y con mayor productividad. Esto se debe en gran parte a que conjunta áreas como álgebra lineal y abstracta, teoría de grafos, combinatoria y geometría finita. Una de las principales cualidades de la teoría de matroides es que existe una amplia variedad de definiciones equivalentes del concepto de matroide, lo cual permite abordar una gran cantidad de problemas con diferentes enfoques (cf. [1]). Como parte de este trabajo se presentan algunas de esas definiciones y se establecen las equivalencias entre ellas.

Una de las herramientas más importantes para determinar la distribución de pesos de un código es la Identidad de MacWilliams que relaciona el enumerador de pesos de un código lineal con el enumerador de pesos de su código dual. Para demostrar la Identidad de MacWilliams pueden seguirse varios caminos. En esta tesis seguiremos dos de ellos: el camino tradicional, con teoría puramente algebraica, empleando específicamente conceptos de Caracteres y Álgebra de Grupo (cf. [6]), y otro empleando Teoría de Matroides (cf. [2]). Se presentan ambas pruebas con la intención de mostrar la gran ventaja que representa emplear resultados de matroides, en particular en la demostración de tal resultado, ya que tomando este camino se obtiene una prueba elegante.

El texto está organizado de la siguiente manera: en el capítulo 1 se presentan las definiciones y teoremas básicos de la teoría de códigos lineales. En el capítulo 2 se introduce una definición de matroide que surge en el campo del álgebra lineal; posteriormente se mencionan algunas maneras alternativas de definir dicho concepto y se establecen las equivalencias entre las definiciones. Al finalizar el capítulo se asocia un matroide a un código lineal y se define el concepto de matroide dual (cf. [1], [4]). El capítulo 3 comienza con la definición de enumerador de pesos de un código y el enunciado de la Identidad de MacWilliams. Posteriormente se definen dos nuevos enumeradores de pesos, el generalizado y el extendido, y se establecen las relaciones entre ellos (cf. [2]). En el capítulo 4 se presenta la definición de Polinomio de Tutte para un matroide y se establece la conexión entre el Polinomio de Tutte del matroide asociado a un código y el enumerador de pesos extendido del código, así como entre los Polinomios de Tutte de un matroide y su dual (cf. [2]). Con estas relaciones se demuestra la Identidad de MacWilliams. Para finalizar, en el capítulo 5 se presenta la demostración clásica de dicha identidad (cf. [6]).

Capítulo 1

Códigos lineales

En este capítulo se introducen algunos conceptos y resultados fundamentales de la teoría de códigos, particularmente de los códigos lineales. Las afirmaciones se presentan sin demostración ya que son resultados bastante conocidos y pueden consultarse en [6].

A lo largo de este texto $[n]$ denotará el conjunto de números naturales menores o iguales a n, es decir, $\{1, 2, \ldots, n\}$.

Definición 1.1. Un *alfabeto* es un conjunto Q con q símbolos. Q^n denota el conjunto de las n-tuplas $x = (x_1, x_2, \ldots, x_n)$ tales que para todo $i \in [n]$, $x_i \in Q$.

Definición 1.2. Un subconjunto no vacío C de Q^n se llama *código de longitud n sobre Q* y sus elementos se llaman *palabras-código*.

Definición 1.3. Sean $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in Q^n$. La *distancia de Hamming* $\mathrm{d}(x, y)$ entre x y y es el número de coordenadas en las cuales x y y difieren, es decir,

$$\mathrm{d}(x, y) = |\{i \in [n] \colon x_i \neq y_i\}|.$$

Teorema 1.1. *Sean $x, y, z \in Q^n$. La distancia de Hamming satisface las siguientes propiedades:*

(1) $\mathrm{d}(x, y) \geq 0$.

(2) $\mathrm{d}(x, y) = 0$ *si y sólo si* $x = y$.

(3) $\mathrm{d}(x, y) = \mathrm{d}(y, x)$.

(4) $\mathrm{d}(x, z) \leq \mathrm{d}(x, y) + \mathrm{d}(y, z)$.

Esto es, la distancia de Hamming en efecto define una métrica en Q^n.

Definición 1.4. Sea C un código de longitud n. La *distancia mínima (de Hamming)* de C, denotada con d o $d(C)$, se define de la siguiente forma: si C tiene un único elemento, $d = n + 1$, y si C tiene

más de una palabra-código entonces

$$d = \min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

En este trabajo se presentan resultados en los cuales se eligen como alfabetos a los campos finitos, q denotará la potencia de algún número primo y $\mathbb{F}_q$ denotará el campo finito con q elementos. Los campos finitos son de interés especial ya que $\mathbb{F}_q^n$ es un espacio vectorial y uno de los objetos de estudio de este trabajo son aquellos códigos que además de ser subconjuntos son subespacios vectoriales de $\mathbb{F}_q^n$. En lo sucesivo cualquier matriz que se mencione se tomará con entradas en $\mathbb{F}_q$ y la dimensión de los subespacios vectoriales que se consideren será sobre el campo $\mathbb{F}_q$, a menos que se indique lo contrario.

Definición 1.5. Un *código lineal* C es un subespacio vectorial de $\mathbb{F}_q^n$. La *dimensión* de C es su dimensión como espacio vectorial sobre $\mathbb{F}_q$. Si C es de longitud n y dimensión k, entonces se dice que C es un $[n, k]$—código. Si la distancia mínima del código es d, $[n, k, d]$ son los *parámetros* del código C.

Uno de los conceptos más importantes en el presente trabajo es el de peso de una palabra-código, que se define a continuación. Más adelante se extiende esta definición a la de peso de un código, ya que la mayoría de los resultados destacados involucra este concepto en lugar del peso de cada una de las palabras-código.

Definición 1.6. Sea $c \in \mathbb{F}_q^n$. El *soporte* de c es el conjunto

$$supp(c) = \{i \in [n] \mid c_i \neq 0\}.$$

La cardinalidad del soporte de c se llama el *peso* de c y se denota por $wt(c)$.

Así, el peso de una palabra-código indica el número de sus componentes que son distintas de cero.

Definición 1.7. Sea C un código. El *peso mínimo* de C se define como $wt_{\min}(C) = n + 1$ si C sólo contiene a la palabra 0, y como

$$wt_{\min}(C) = \min\{wt(c) \mid c \in C,\ c \neq 0\}$$

si contiene una palabra código distinta de 0.

Teorema 1.2. *La distancia mínima de un código lineal C es igual a su peso mínimo.*

Sea C un $[n, k]$—código. Como C es en particular un $\mathbb{F}_q$-espacio vectorial de dimensión k, C posee una base de k vectores. Dicha base genera a C, esto es, toda palabra código puede expresarse como combinación lineal de los elementos de la base. Entonces C es igual al espacio fila de una matriz cuyas filas son los elementos de dicha base. Así que tiene sentido dar la siguiente definición.

Definición 1.8. Sea C un $[n, k]$-código. Una matriz G de tamaño $k \times n$ cuyas filas son elementos de alguna base para C se llama *matriz generadora* para C.

Observación 1.1. Un $[n, k]$-código C puede tener más de una matriz generadora (si $k > 1$, basta con permutar las filas de una matriz generadora para obtener matrices generadoras distintas), pero todas las matrices generadoras de C son de rango k.

Otra forma de describir un subespacio vectorial es mediante el espacio solución de un conjunto de ecuaciones lineales homogéneas, o equivalentemente, mediante el espacio nulo de una matriz, concepto que se retoma en la siguiente definición.

Definición 1.9. Sea M una matriz de tamaño $m \times n$. El conjunto de todos los vectores $c \in \mathbb{F}_q^n$ tales que $Mc^T = 0$ se llama el *espacio nulo* de M y se denota mediante $nul(M)$.

El espacio nulo de una matriz es un subespacio de $\mathbb{F}_q^n$. La dimensión del espacio nulo de una matriz M se llama *nulidad* de M y se denota por $nulidad(M)$.

Definición 1.10. El *rango* de una matriz M es la dimensión de sus espacios renglón o columna y se denota por $rango(M)$.

El Teorema del rango afirma que si M es una matriz de tamaño $m \times n$, entonces $rango(M) + nulidad(M) = n$.

Definición 1.11. Una matriz de tamaño $(n - k) \times n$ de rango $n - k$ se llama *matriz de verificación de paridad* del $[n, k]$-código C si C es el espacio nulo de dicha matriz.

Sea H una matriz de tamaño $m \times n$ y sea C el espacio nulo de H. Las m ecuaciones lineales homogéneas correspondientes se llaman *ecuaciones de verificación de paridad*, o simplemente *verificadoras de paridad*. Puede ocurrir que H tenga rango m, es decir, que todas sus filas sean linealmente independientes, en tal caso la dimensión k de C, es decir, $nulidad(H)$, sería igual a $n - m$, por el Teorema del rango. Pero también puede darse el caso en el que H tenga filas linealmente dependientes, y por tanto, rango menor a m. En este caso k tendría un valor mayor que $n - m$. Se concluye que la dimensión k de C es al menos $n - m$. Si existen filas dependientes en la matriz H, entonces se puede crear otra matriz H' a partir de H, suprimiendo filas inferiores que sean múltiplos de alguna fila superior, de tal manera que H' sea una matriz de tamaño $(n - k) \times n$ de rango $n - k$ y con el mismo espacio nulo que H. Lo anterior justifica que siempre es posible encontrar una matriz de verificación de paridad de un código lineal.

Teorema 1.3. *Sea C un $[n, k]$-código. Sea I_k la matriz identidad de tamaño $k \times k$. Sea P una matriz de tamaño $k \times (n - k)$. Entonces, $(I_k|P)$ es una matriz generadora de C si y sólo si $(-P^T|I_{n-k})$ es una matriz de verificación de paridad de C.*

El Teorema 1.3 permite hallar una matriz de verificación de paridad de un código lineal dada su matriz generadora y viceversa.

La siguiente definición establece el concepto de producto interno en $\mathbb{F}_q^n$, el cual es necesario para definir un tipo de código que se empleará frecuentemente más adelante: el código dual.

Definición 1.12. Sean $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. El *producto interno* de x y y, se denota y se define como:

$$\langle x, y \rangle = x_1 y_1 + x_2 y_2 \cdots + x_n y_n.$$

Si $\langle x, y \rangle = 0$ se dice que x y y son *ortogonales*.

Definición 1.13. Sea C un código. Definimos su *código dual* u *ortogonal* como

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \forall c \in C : \langle c, x \rangle = 0\}.$$

El código dual de un código lineal C es el conjunto de vectores en $\mathbb{F}_q^n$ que son ortogonales a cada una de las palabras-código de C. Si C es lineal, $C^{\perp}$ también lo es. Lo anterior queda establecido en el siguiente teorema.

Teorema 1.4. *Sea C un $[n, k]$-código con matriz generadora G. Entonces $C^{\perp}$ es un $[n, n-k]$-código con matriz de verificación de paridad G.*

El Teorema 1.4 también establece una relación entre las matrices correspondientes a los códigos: la matriz generadora de un código es la matriz de verificación de paridad de su código dual.

Teorema 1.5. *Sea C un $[n, k]$-código. Tenemos que $(C^{\perp})^{\perp} = C$.*

Corolario 1.1. *Sea C un código lineal. Entonces*

(1) G es una matriz generadora de C si y sólo G es una matriz de verificación de paridad de $C^{\perp}$.

(2) H es una matriz de verificación de paridad de C si y sólo si H es una matriz generadora de $C^{\perp}$.

Para finalizar este capítulo se presenta un resultado que da una interpretación de la distancia mínima de un código en términos de la dependencia lineal de las columnas de una matriz de verificación de paridad de dicho código. Este resultado se empleará más adelante.

Teorema 1.6. *Sea C un código lineal y H una matriz de verificación de paridad de C. Entonces la distancia mínima d de C es el número mínimo de columnas linealmente dependientes de H.*

Capítulo 2

Matroides

La teoría de matroides surgió en los años 30's del siglo XX. Hassler Whitney desarrolló una noción de independencia y rango en el contexto de la teoría de grafos y observó similitudes con los conceptos de independencia lineal y dimensión de álgebra lineal. Después de identificar las propiedades de independencia abstracta, Whitney introdujo el concepto de matroide en 1935 en [8] y se inspiró en la palabra matriz para crearlo. Otros matemáticos contemporáneos de Whitney también contribuyeron al nacimiento de la teoría de matroides. En 1937, B. L. van der Waerden, en la segunda edición de *Moderne Algebra*, estableció tres propiedades fundamentales que son comunes a la dependencia algebraica y lineal, descubriendo con ello el concepto de matroide de manera independiente a Whitney.

En este capítulo se estudiarán los conceptos fundamentales de la teoría de matroides, se establecerán las equivalencias entre algunas de las definiciones de matroide y se presentará el matroide asociado a un código que será clave para presentar el teorema central del presente trabajo: la Identidad de MacWilliams. Para el desarrollo de este capítulo se tomaron [1] y [4] como principales referencias.

2.1. Definiciones equivalentes de matroide

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

En esta sección se enunciarán algunas de las principales y más útiles definiciones de matroide. Se tomará como primera definición aquella que abstrae las propiedades que satisface un conjunto de vectores linealmente independiente. Esta definición, por tanto, proviene del álgebra lineal. Posteriormente, se definirán nuevos conceptos y se demostrarán algunas de las propiedades que dichos conceptos satisfacen. A continuación se destacarán aquellas propiedades que serán suficientes para dar una definición alternativa del concepto de matroide y se probará la equivalencia de las definiciones. El desarrollo de esta teoría estará acompañada de algunos ejemplos y observaciones.

2.1.1. Definición por conjuntos independientes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Teorema 2.1. *Sean E un conjunto finito e $\mathcal{I}$ una familia de subconjuntos de E. Entonces $\mathcal{I}$ es la familia de conjuntos independientes de un matroide si y sólo si 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* $|J| = |I| + 1$, *entonces existe un elemento* $x \in J \setminus I$ *que cumple que* $I \cup \{x\} \in \mathcal{I}$.

Demostración.

Sea $M = (E, \mathcal{I})$ un matroide. Veamos que $\mathcal{I}$ verifica las propiedades (J1) y (J3). Dado que $\mathcal{I}$ satisface la condición (I1), $\mathcal{I} \neq \emptyset$. Así, existe un conjunto independiente, al que llamamos X. Como también se cumple (I2) y tenemos que $\emptyset \subseteq X$, concluimos que $\emptyset \in \mathcal{I}$, es decir, se satisface (J1). La condición (J3) es un caso particular de (I3) y por lo tanto, se verifica.

Para la suficiencia supongamos que E es un conjunto finito y que $\mathcal{I}$ es una familia de subconjuntos de E que satisface las propiedades (J1), (J2) y (J3). Veamos que $M = (E, \mathcal{I})$ es un matroide. Por (J1), $\emptyset \in \mathcal{I}$, entonces se verifica (I1). Ahora, sean $I, J \in \mathcal{I}$ con $|I| < |J|$. Como I y J son conjuntos finitos, entonces existe $I_1 \subseteq J$ tal que $|I_1| = |I| + 1$. Por (J2), $I_1 \in \mathcal{I}$, luego por (J3) existe $x \in I_1 \setminus I$ tal que $I \cup \{x\} \in \mathcal{I}$. Más aún, $x \in J \setminus I$. Por lo tanto, M es un matroide. □

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

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

Ejemplo 2.1. Sean V un espacio vectorial sobre un campo $\mathbb{F}$ y E un subconjunto finito de V. Defínase $\mathcal{I}$ como la colección de subconjuntos de E que son linealmente independientes sobre $\mathbb{F}$. Como $\emptyset$ es un conjunto linealmente independiente entonces $\emptyset \in \mathcal{I}$. Además, $\mathcal{I}$ satisface las propiedades a) y b) mencionadas anteriormente. Por lo tanto, $M = (E, \mathcal{I})$ es un matroide y se llama *matroide vector* o

matroide representable y se dice que M es *representable sobre* $\mathbb{F}$. Este es uno de los ejemplos que motivaron la definición de matroide.

Ejemplo 2.2. Sean n y k enteros no negativos tales que $k \leq n$. Sea E un conjunto de cardinalidad n. Tómese $\mathcal{I}$ como la familia de todos los subconjuntos de E que tienen una cardinalidad menor o igual a k. Como $\emptyset \subseteq E$ y $|\emptyset| = 0 \leq k$, entonces $\emptyset \in \mathcal{I}$. Ahora, supóngase que $I \in \mathcal{I}$ y $J \subseteq I$. Entonces $|I| \leq k$, $|J| \leq |I|$, y por tanto $|J| \leq k$, de donde $J \in \mathcal{I}$. Finalmente, sean $I, J \in \mathcal{I}$ tales que $|I| < |J|$. Como $|I| < |J|$, entonces existe un elemento $x \in J \setminus I$ y se tiene que $|I \cup \{x\}| \leq |J|$. Dado que $J \in \mathcal{I}$, verifica que $|J| \leq k$ y por ello $|I \cup \{x\}| \leq |J| \leq k$. Por consiguiente $I \cup \{x\} \in \mathcal{I}$. Así que M es un matroide. M se llama el *matroide uniforme* de rango k sobre un conjunto de n elementos y se denota por $U_{k,n}$. El matroide $U_{n,n}$ se llama *matroide libre*. Nótese que en el matroide libre todos los subconjuntos de E son independientes, es decir, $\mathcal{I} = \mathcal{P}(E)$.

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

Ejemplo 2.3. Sean $E = \{a, b, c, d\}$, $\mathcal{I} = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{c, d\}\}$. Se puede ver claramente que $\mathcal{I}$ satisface las propiedades (I1) e (I2), sin embargo, no cumple con (I3). Para comprobar esto, tómese los conjuntos $\{a\}$ y $\{c, d\}$ de la familia $\mathcal{I}$. Puede verse que no existe elemento x en $\{c, d\} \setminus \{a\}$ tal que $\{a\} \cup \{x\} \in \mathcal{I}$, ya que ni $\{a, c\}$ ni $\{a, d\}$ son elementos de $\mathcal{I}$. Por lo tanto, $\mathcal{I}$ no es una familia de conjuntos independientes.

2.1.2. Definición por bases

Sea $M = (E, \mathcal{I})$ un matroide. Para conocer por completo a M es necesario poder identificar todos sus conjuntos independientes. Si M posee una gran cantidad de conjuntos independientes dar una lista exhaustiva de todos ellos podría resultar una tarea complicada. Sin embargo, existe una manera de facilitar este trabajo. Sea I un conjunto independiente de M. Si no existe un conjunto independiente que contenga propiamente a I entonces I es un conjunto independiente maximal. En otro caso, supóngase que $I_1 \in \mathcal{I}$ es tal que $I \subsetneq I_1$. Si no existe un conjunto independiente que contenga propiamente a I_1 entonces I_1 es independiente maximal. De lo contrario existe un conjunto independiente I_2 diferente a I_1 que lo contiene. Podemos continuar este proceso, pero no de manera indefinida, pues como E es finito también lo es su conjunto potencia. Así que después de un número finito de pasos hallaremos un conjunto independiente que contiene a I y que no está contenido propiamente en otro conjunto independiente, es decir, independiente maximal. De aquí concluimos que todo conjunto independiente está contenido en un conjunto independiente maximal. Además, todo subconjunto de un conjunto independiente es independiente por (I2). Así que una manera efectiva de enlistar todos los conjuntos independientes es proporcionar una lista de los conjuntos independientes maximales. De aquí la importancia de definir el siguiente concepto.

Definición 2.3. Sea $M = (E, \mathcal{I})$ un matroide. B es una *base* del matroide M si B es un conjunto independiente maximal. Se denotará el conjunto de las bases de M por $\mathcal{B}$.

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

Lema 2.1. *Sea M un matroide. Si $B_1, B_2 \in \mathcal{B}$, entonces $|B_1| = |B_2|$.*

Demostración.

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

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

Teorema 2.2. *El conjunto de bases $\mathcal{B}$ de un matroide M verifica las siguientes propiedades:*

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

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

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

Demostración.

Sabemos que $\emptyset$ es un conjunto independiente. Entonces existe un conjunto independiente maximal B que lo contiene. Por la definición de $\mathcal{B}$, $B \in \mathcal{B}$ y por lo tanto (B1) se cumple. Tomemos $B_1, B_2 \in \mathcal{B}$ tales que $B_1 \subseteq B_2$. Si suponemos que $B_1 \subsetneq B_2$ entonces $|B_1| < |B_2|$, lo cual no puede ocurrir por el Lema 2.1. Entonces $B_1 = B_2$. Para probar que se cumple (B3), sean $B_1, B_2 \in \mathcal{B}$ y $x \in B_1 \setminus B_2$. Como $B_1 \setminus \{x\} \subseteq B_1$ y $B_1 \in \mathcal{I}$, por (I2) tenemos que $B_1 \setminus \{x\} \in \mathcal{I}$. Por el Lema 2.1, $|B_1| = |B_2|$, luego $|B_1 \setminus \{x\}| < |B_2|$. Por (I3) existe un elemento $y \in B_2 \setminus (B_1 \setminus \{x\})$ tal que $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{I}$. Queremos probar que $(B_1 \setminus \{x\}) \cup \{y\}$ es una base, así que sólo falta probar que es conjunto independiente maximal. Tenemos que $|(B_1 \setminus \{x\}) \cup \{y\}| = |B_1|$. Si suponemos que $(B_1 \setminus \{x\}) \cup \{y\} \notin \mathcal{B}$, debe existir $B_3 \in \mathcal{B}$ tal que $(B_1 \setminus \{x\}) \cup \{y\} \subsetneq B_3$ y por tanto $|B_1| = |(B_1 \setminus \{x\}) \cup \{y\}| < |B_3|$, lo cual contradice el Lema 2.1. Concluimos que $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$, por lo que (B3) se verifica. □

La propiedad (B2) manifiesta que $\mathcal{B}$ es una familia Sperner o clutter, es decir, que los conjuntos de dicha familia no se contienen entre sí. La propiedad (B3) expresa que dadas dos bases B_1 y B_2, para un elemento $x \in B_1 \setminus B_2$ existe un elemento en la otra diferencia de conjuntos $y \in B_2 \setminus B_1$ tal que x puede "intercambiarse" por y para obtener nuevamente una base, es decir, $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ (de ahí el nombre de propiedad de intercambio débil en bases). Aplicando la propiedad (B3) al elemento y

se tiene que existe $z \in B_1 \setminus B_2$ tal que $(B_2 \setminus \{y\}) \cup \{z\} \in \mathcal{B}$. Sin embargo, dicha propiedad no afirma algo acerca del conjunto $(B_2 \setminus \{y\}) \cup \{x\}$. El Teorema 2.3 es una versión más fuerte de la propiedad de intercambio débil en bases, pues asegura que siempre es posible que se dé un intercambio doble, es decir, que para cada elemento de $B_1 \setminus B_2$ es posible encontrar un elemento en $B_2 \setminus B_1$ de tal forma que pueden intercambiarse (el primero por el segundo y el segundo por el primero) para obtener dos bases. En muchas ocasiones bastará con tener la primera versión de esta propiedad, pero se menciona a continuación ya que será de utilidad más adelante.

Teorema 2.3. *([1]) Sea M un matroide. $\mathcal{B}$ satisface la siguiente propiedad:*

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

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

Como pudo apreciarse, el Lema 2.1 fue crucial en la demostración del Teorema 2.2. En el Teorema 2.4 se verá que dicho lema puede emplearse para formular una nueva caracterización de matroide. Para ello identificaremos a la propiedad enunciada en el Lema 2.1 como (B2*).

Teorema 2.4. *Sean E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E. La familia $\mathcal{B}$ satisface (B1), (B2) y (B3) si y sólo si satisface (B1), (B2*) y (B3).*

Demostración.

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

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

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

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

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

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

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

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

Hasta este momento se ha abordado la manera mediante la cual pueden conocerse las bases de un matroide considerando sus conjuntos independientes, y las propiedades que dichas bases cumplen. Es de interés saber si puede construirse un matroide a partir de una familia $\mathcal{B}$ que cumple (B1), (B2) y (B3). La respuesta es sí. Esto se logra formando a partir de $\mathcal{B}$ una familia $\mathcal{I}$ de lo que serán los conjuntos independientes y demostrando que dicha familia satisface las propiedades (I1), (I2) e (I3). El punto clave de esta construcción es saber cómo definir la familia $\mathcal{I}$. Las bases se definieron como los conjuntos independientes maximales, luego todo conjunto independiente está contenido en una base y cualquier subconjunto de una base es un conjunto independiente, así que de manera natural $\mathcal{I}$ se toma como el conjunto de todos los subconjuntos de los elementos de $\mathcal{B}$. Esto se aborda en el Teorema 2.5.

Teorema 2.5. *Sean E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E que satisface (B1), (B2) y (B3). Se define el conjunto $\mathcal{I} = \{I \subseteq E \mid \exists B \in \mathcal{B} : I \subseteq B\}$. Entonces $M = (E, \mathcal{I})$ es un matroide que tiene a $\mathcal{B}$ como su colección de bases.*

Demostración.

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

Sean $I_1, I_2 \in \mathcal{I}$ tales que $|I_1| < |I_2|$ y supongamos que (I3) no se cumple, es decir, que para todo $x \in I_2 \setminus I_1$, $I_1 \cup \{x\} \notin \mathcal{I}$. Como $I_1, I_2 \in \mathcal{I}$, existen $B_1, B_2 \in \mathcal{B}$ tales que $I_1 \subseteq B_1$ e $I_2 \subseteq B_2$. Queremos analizar el conjunto coloreado de negro de la Figura 2.1, es decir, el conjunto $(I_2 \cap B_1) \setminus I_1$. Si $(I_2 \cap B_1) \setminus I_1 \neq \emptyset$, entonces existe $x \in (I_2 \cap B_1) \setminus I_1$, esto es, $x \in I_2 \setminus I_1$ y $x \in B_1$, por lo que $I_1 \cup \{x\} \subseteq B_1$, de donde $I_1 \cup \{x\} \in \mathcal{I}$, lo cual contradice nuestra suposición. Por lo tanto, $(I_2 \cap B_1) \setminus I_1 = \emptyset$, o expresado de otra forma, $I_2 \cap (B_1 \setminus I_1) = \emptyset$, y como $B_1 \cap I_2 = (I_2 \cap I_1) \cup (I_2 \cap (B_1 \setminus I_1))$ concluimos que $B_1 \cap I_2 = I_1 \cap I_2$. Por otro lado, puede existir más de un elemento en $\mathcal{B}$ que contenga a I_2. Tomaremos

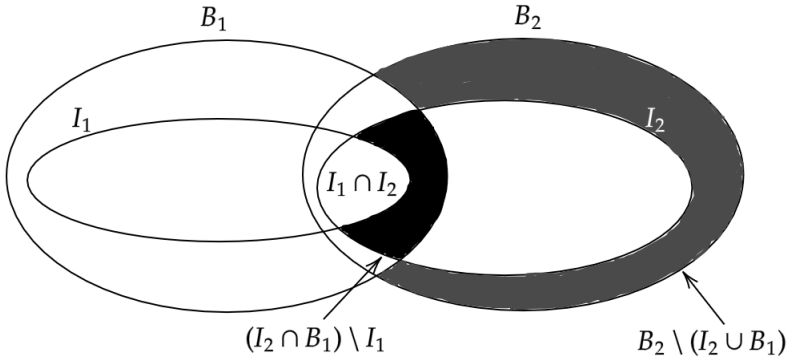

Figura 2.1: Diagrama de Venn de las relaciones entre B_1, B_2, I_1 e I_2.

a B_2 de tal forma que $|B_2 \setminus (I_2 \cup B_1)|$ sea minimal (ver en la Figura 2.1 región coloreada de gris). Afirmamos que $B_2 \setminus (I_2 \cup B_1) = \emptyset$. Si existe $x \in B_2 \setminus (I_2 \cup B_1)$, en particular $x \in B_2 \setminus B_1$, luego aplicando la propiedad (B3) a B_2 y a B_1 (en ese orden), existe $y \in B_1 \setminus B_2$ tal que $B_3 = (B_2 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$. Veamos que $B_3 \setminus (I_2 \cup B_1) \subsetneq B_2 \setminus (I_2 \cup B_1)$.

$$
\begin{aligned}
B_3 \setminus (I_2 \cup B_1) &= [(B_2 \setminus \{x\}) \cup \{y\}] \setminus (I_2 \cup B_1) = [(B_2 \cap \{x\}^C) \cup \{y\}] \setminus (I_2 \cup B_1) \\
&= [(B_2 \cup \{y\}) \cap (\{x\}^C \cup \{y\})] \setminus (I_2 \cup B_1) = [(B_2 \cup \{y\}) \cap \{x\}^C] \setminus (I_2 \cup B_1) \\
&= [(B_2 \cup \{y\}) \cap \{x\}^C] \cap (I_2 \cup B_1)^C = [(B_2 \cup \{y\}) \cap (I_2 \cup B_1)^C] \cap \{x\}^C \\
&= [(B_2 \cap (I_2 \cup B_1)^C) \cup (\{y\} \cap (I_2 \cup B_1)^C)] \cap \{x\}^C \\
&= [(B_2 \setminus (I_2 \cup B_1)) \cup (\{y\} \cap (I_2 \cup B_1)^C)] \cap \{x\}^C \\
&= [B_2 \setminus (I_2 \cup B_1)] \setminus \{x\} \subsetneq [B_2 \setminus (I_2 \cup B_1)]
\end{aligned} \tag{2.1}
$$

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

$$
B_2 \setminus B_1 = I_2 \setminus B_1 = I_2 \setminus I_1. \tag{2.2}
$$

Puede demostrarse también que $B_1 \setminus B_2 = I_1 \setminus B_2$. Además, como $I_2 \subseteq B_2$, entonces $I_1 \setminus B_2 \subseteq I_1 \setminus I_2$.

Por tanto, tenemos las siguientes contenciones de conjuntos:

$$B_1 \setminus B_2 = I_1 \setminus B_2 \subseteq I_1 \setminus I_2 \tag{2.3}$$

Como $\mathcal{B}$ cumple (B1), (B2) y (B3), por el Teorema 2.4 también satisface (B2*), así, $|B_1| = |B_2|$, y como $B_1 = (B_1 \cap B_2) \cup (B_1 \setminus B_2)$, $B_2 = (B_1 \cap B_2) \cup (B_2 \setminus B_1)$, y dichas uniones son disjuntas, entonces $|B_1 \setminus B_2| = |B_2 \setminus B_1|$. Por las relaciones establecidas en (2.2) y (2.3), resulta que

$$|I_2 \setminus I_1| \leq |I_1 \setminus I_2|. \tag{2.4}$$

Pero I_1 e I_2 son tales que $|I_1| < |I_2|$, y pueden escribirse como las uniones disjuntas $I_1 = (I_1 \cap I_2) \cup (I_1 \setminus I_2)$, $I_2 = (I_1 \cap I_2) \cup (I_2 \setminus I_1)$, entonces $|I_1 \setminus I_2| < |I_2 \setminus I_1|$, lo cual contradice (2.4). Por lo tanto, (I3) es verdadera. Así que en efecto $M = (E, \mathcal{I})$ es un matroide.

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

Los Teoremas 2.2 y 2.5 justifican la equivalencia entre la definición de matroide por conjuntos independientes (Definición 2.2) y la que se da a continuación.

Definición 2.4 (Por bases)**.** Un *matroide* M es un par ordenado $(E, \mathcal{B})$ donde E es un conjunto finito y $\mathcal{B}$ es una familia de subconjuntos de E que satisface las siguientes tres condiciones:

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

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

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

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

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

linealmente dependiente, de manera que existen escalares $\alpha_1, \alpha_2, \ldots, \alpha_n$ no todos iguales a cero tales que:

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

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

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

Esto es, para todo $i \in [n]$, $w_i \in gen(\{v_2, \ldots, v_n\})$, por lo que $gen(\{w_1, w_2, \ldots, w_n\}) \subseteq gen(\{v_2, \ldots, v_n\})$ y como $gen(\{w_1, w_2, \ldots, w_n\}) = V$, luego $V = gen(\{v_2, \ldots, v_n\})$, pero esto contradice que la dimensión de V sea n. Entonces se cumple (B3).

Sin embargo, ésta no es la única manera de definir un matroide a partir de sus bases. El Teorema 2.4 presenta propiedades equivalentes que pueden emplearse para tal fin además de (B1), (B2) y (B3). El siguiente corolario expone una equivalencia más que es consecuencia inmediata de resultados anteriores, pero se enuncia ya que se empleará posteriormente.

Corolario 2.1. *Sea E un conjunto finito y $\mathcal{B}$ una familia de subconjuntos de E que satisface las propiedades (B1), (B2*) y (B3*). Sea $\mathcal{I}$ la familia de subconjuntos de E que están contenidos en algún elemento de $\mathcal{B}$. Entonces $M = (E, \mathcal{I})$ es un matroide y $\mathcal{B}$ es su conjunto de bases. De manera inversa, si M es un matroide, entonces su familia de bases $\mathcal{B}$ satisface las propiedades (B1), (B2*) y (B3*).*

Demostración.

Para la necesidad supongamos que $\mathcal{B}$ satisface las propiedades (B1), (B2*) y (B3*). Por ser un caso particular de (B3*), $\mathcal{B}$ cumple (B3). Por el Teorema 2.4, $\mathcal{B}$ satisface (B1), (B2) y (B3). La conclusión del corolario es inmediata por el Teorema 2.5.

Para la suficiencia, sea M un matroide. Por el Lema 2.1 y por los Teoremas 2.2 y 2.3, la familia de bases $\mathcal{B}$ satisface las propiedades (B1), (B2*) y (B3*). □

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

Ejemplo 2.4. Sea $M = (E, \mathcal{I})$ un matroide representable. Una base de M es un conjunto de vectores de E linealmente independiente maximal, es decir, es una base para el generado de E en el sentido usual de álgebra lineal. En caso de que el generado de E sea igual al espacio vectorial V, entonces una base para M es una base para V.

Ejemplo 2.5. Sea $M = (E, \mathcal{I})$ el matroide uniforme de rango k sobre un conjunto de n elementos definido en el Ejemplo 2.2. Veamos que $\mathcal{B}$ es la familia de todos los subconjuntos de E de cardinalidad k. Sea $B \subseteq E$ de cardinalidad k. Claramente $B \in \mathcal{I}$. Ahora, supongamos que B' es un conjunto independiente tal que $B \subseteq B'$, entonces $k = |B| \leq |B'|$. Como $B' \in \mathcal{I}$, entonces $|B'| \leq k$. Concluimos pues que $|B'| = k$ y por tanto $B = B'$, con lo cual queda probado que B es una base. A la inversa,

supongamos que B es una base de M y supongamos que $|B| \neq k$. Como B es un conjunto independiente ocurre que $|B| \leq k$, luego $|B| < k$. Como $B \subseteq E$ y $k \leq n = |E|$ entonces existe un subconjunto B_1 de E que contiene propiamente a B y cuya cardinalidad es igual k. Por sus características B_1 es elemento de $\mathcal{I}$, pero esto contradice que B sea un conjunto independiente maximal. Así, $|B| = k$.

2.1.3. Definición por circuitos

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

Definición 2.5. Sea $M = (E, \mathcal{I})$ un matroide. Un subconjunto C de E se llama *circuito* si es un conjunto dependiente minimal, es decir, si es dependiente pero todos sus subconjuntos propios son independientes. Se denota con $\mathcal{C}$ el conjunto de circuitos de M. En símbolos:

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

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

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

Teorema 2.6. *Sea M un matroide. Su colección de circuitos $\mathcal{C}$ tiene las siguientes propiedades:*

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

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

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

Demostración.

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

Probemos ahora que (C3) es cierta. Tomemos dos circuitos diferentes C_1 y C_2, y un elemento $e \in C_1 \cap C_2$. Supongamos que ningún subconjunto de $(C_1 \cup C_2) \setminus \{e\}$ es circuito, en particular tenemos que $(C_1 \cup C_2) \setminus \{e\}$ no es un circuito. Entonces $(C_1 \cup C_2) \setminus \{e\}$ no es un conjunto dependiente o es un conjunto dependiente pero no minimal. Lo segundo no puede ocurrir, pues en caso de que sí,

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

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

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

Existen dos tipos de conjuntos dependientes en un matroide: los minimales, que son los circuitos, y los que no son minimales, y por lo tanto, contienen un circuito. Entonces los conjuntos independientes son todos aquellos que no pertenecen a ninguna de esas dos clases de conjuntos, es decir, conjuntos que no son un circuito y que no contienen un circuito, en resumen, conjuntos que no contienen un circuito. Esta idea se emplea en el siguiente teorema que establece cómo puede construirse un matroide a partir de una familia de conjuntos que verifica las tres propiedades dadas en el Teorema 2.6.

Teorema 2.7. *Sean E un conjunto y $\mathcal{C}$ una familia de subconjuntos de E que satisface (C1), (C2) y (C3). Sea $\mathcal{I}$ la familia de subconjuntos de E tales que ninguno de sus subconjuntos es elemento de $\mathcal{C}$, es decir,*

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

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

Demostración.

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

Veamos por último que (I3) es verdadera. Sean $I_1, I_2 \in \mathcal{I}$ tales que $|I_1| < |I_2|$. Supongamos que para toda $x \in I_2 \setminus I_1$, $I_1 \cup \{x\} \notin \mathcal{I}$. Elijamos un elemento I_3 de $\mathcal{I}$ que esté contenido en $I_1 \cup I_2$, cuya cardinalidad sea mayor que la de I_1 (I_2 satisface tales condiciones) y tal que $|I_1 \setminus I_3|$ sea mínima. Si suponemos que $I_1 \setminus I_3 = \emptyset$, entonces $I_1 \subseteq I_3$ y como $|I_1| < |I_3|$, entonces existe $x \in I_3 \setminus I_1$, y dado

que $I_3 \subseteq I_1 \cup I_2$, entonces $x \in I_2 \setminus I_1$ y como $I_1 \cup \{x\} \subseteq I_3$, por (I2) $I_1 \cup \{x\} \in \mathcal{I}$, lo cual contradice lo supuesto. Así pues, $I_1 \setminus I_3 \neq \emptyset$; elegimos un elemento e de $I_1 \setminus I_3$. Si suponemos que $I_3 \setminus I_1 = \emptyset$, entonces $I_3 \subseteq I_1$, lo cual no ocurre porque la cardinalidad de I_1 es menor que la cardinalidad de I_3. Por tanto, $I_3 \setminus I_1 \neq \emptyset$. Para cada elemento f de $I_3 \setminus I_1$, sea $T_f = (I_3 \cup \{e\}) \setminus \{f\}$. Por su definición, $T_f \subseteq I_1 \cup I_2$. Además, tomando en cuenta que $e \in I_1 \cap I_3^C$ y $f \notin I_1$ se cumple lo siguiente:

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

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

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

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

Ahora veamos que $\mathcal{C}$ es el conjunto de circuitos de M. Sea C un circuito de M, veamos que $C \in \mathcal{C}$. Como C es circuito, no es un conjunto independiente, así que por la definición de $\mathcal{I}$, C debe tener un subconjunto C' que es elemento de $\mathcal{C}$. Como C es circuito, todo subconjunto propio de C es independiente. Sea I un subconjunto propio de C. Para todo $C \in \mathcal{C}$ se cumple que $C \nsubseteq I$ y como $I \subseteq I$ entonces $I \notin \mathcal{C}$ y por lo tanto todo subconjunto propio de C no es elemento de $\mathcal{C}$, por consiguiente $C' = C$, es decir, $C \in \mathcal{C}$. Ahora, si $C \in \mathcal{C}$, como $C \subseteq C$, entonces $C \notin \mathcal{I}$, luego C es dependiente. Si suponemos que un subconjunto C' de C también es dependiente, entonces $C' \notin \mathcal{I}$, de donde existe $C'' \in \mathcal{C}$ tal que $C'' \subseteq C'$. En particular tenemos que $C'' \subseteq C$. Para C y C'' se cumple (C2) y por tanto concluimos que $C = C''$, más aún, $C' = C$ lo cual verifica que C es conjunto dependiente minimal, y por tanto C es circuito de M. □

Los Teoremas 2.6 y 2.7 justifican la siguiente definición.

Definición 2.6 (Por circuitos)**.** Un *matroide* M es un par ordenado $(E, \mathcal{C})$, donde E es un conjunto finito y $\mathcal{C}$ es un subconjunto de $\mathcal{P}(E)$ que verifica las siguientes tres propiedades:

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

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

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

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

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

Ejemplo 2.6. Sea M un matroide representable. Los circuitos de M son conjuntos de vectores linealmente dependientes, cuyos subconjuntos propios son todos linealmente independientes.

Ejemplo 2.7. Sea M el matroide uniforme de rango k sobre el conjunto E de n elementos. Claramente $\mathcal{C}$ es la familia de subconjuntos de E de cardinalidad $k+1$. En este ejemplo, todos los circuitos del matroide tienen la misma cardinalidad. Sin embargo, no siempre es así.

2.1.4. Definición por función rango

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

Definición 2.7. Sean $M = (E, \mathcal{I})$ un matroide y $A \subseteq E$. El *rango* o la *dimensión* de A es la mayor de las cardinalidades de los conjuntos independientes que están contenidos en A y se denota por $r(A)$, es decir:

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

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

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

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

Puede darse una definición de matroide en términos de la función rango. La manera de hacerlo se presenta en los teoremas siguientes. Para probarlos se necesita una generalización de la propiedad (I3) que se enuncia y se demuestra a continuación.

Lema 2.2. *Sea $M = (E, \mathcal{I})$ un matroide, y sean I y J dos conjuntos independientes tales que $|I| < |J|$, $n = |J| - |I|$. Entonces existen $x_1, x_2, \ldots, x_n \in J \setminus I$ tales que $I \cup \{x_1, x_2, \ldots, x_n\} \in \mathcal{I}$.*

Demostración.

Sean $I, J \in \mathcal{I}$ tales que $|J|-|I| = n$, $n \geq 1$. Si $n = 1$, la proposición es cierta ya que es justamente (I3). Supongamos que el resultado es válido para cualquier pareja de conjuntos independientes tales que la diferencia de sus cardinalidades es igual a n. Si $|J| - |I| = n + 1$, elijamos $x \in J$. Por (I2), $J \setminus \{x\} \in \mathcal{I}$, además $|J \setminus \{x\}| - |I| = n$. Por la hipótesis de inducción existen $x_1, x_2, \ldots, x_n \in (J \setminus \{x\}) \setminus I$ tales que $I \cup \{x_1, x_2, \ldots, x_n\} \in \mathcal{I}$. Ahora, $I \cup \{x_1, x_2, \ldots, x_n\}$ y J son dos conjuntos independientes tales que $|J| = |I \cup \{x_1, x_2, \ldots, x_n\}| + 1$. Por (I3) tenemos que existe $x_{n+1} \in J \setminus (I \cup \{x_1, x_2, \ldots, x_n\})$ tal que $I \cup \{x_1, x_2, \ldots, x_n, x_{n+1}\} \in \mathcal{I}$, es decir, $x_1, x_2, \ldots, x_n, x_{n+1} \in J \setminus I$ son tales que $I \cup \{x_1, x_2, \ldots, x_n, x_{n+1}\} \in \mathcal{I}$, con lo cual el lema queda establecido. □

Teorema 2.8. *Sea $M = (E, \mathcal{I})$ un matroide. La función rango r de M satisface las siguientes propiedades para cualesquiera $A, B \subseteq E$:*

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

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

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

Demostración.

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

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

Esto prueba que (r2) se satisface. Sea I_1 un conjunto independiente contenido en $A \cap B$ tal que $r(A \cap B) = |I_1|$. Queremos encontrar un subconjunto I de $A \cup B$ que sea independiente, que satisfaga que $r(A \cup B) = |I|$ y que contenga a I_1. Lo haremos de la siguiente forma: como $A \cap B \subseteq A \cup B$, por (r2) ocurre que $r(A \cap B) = r(A \cup B)$ o $r(A \cap B) < r(A \cup B)$. Si ocurre lo primero, entonces I_1 es un subconjunto de $A \cup B$ que es independiente y que satisface que $r(A \cup B) = |I_1|$, así que elegimos $I = I_1$. Si ocurre lo segundo, sea I_2 un conjunto independiente contenido en $A \cup B$ tal que $r(A \cup B) = |I_2|$. Tenemos que $|I_1| < |I_2|$, sea $n = |I_2| - |I_1|$. Por el Lema 2.2, existen $x_1, x_2, \ldots, x_n \in I_2 \setminus I_1$ tales que $I_1 \cup \{x_1, x_2, \ldots, x_n\} \in \mathcal{I}$. En particular, $x_1, x_2, \ldots, x_n \in A \cup B$, por lo tanto, $I_1 \cup \{x_1, x_2, \ldots, x_n\}$ es un subconjunto independiente de $A \cup B$ de la misma cardinalidad que I_2, entonces $r(A \cup B) = |I_1 \cup \{x_1, x_2, \ldots, x_n\}|$, así que elegimos

$I = I_1 \cup \{x_1, x_2, \ldots, x_n\}$. Podemos descomponer a I como la siguiente unión disjunta:

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

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

$$r(A \cup B) = |I| = |I_1| + |I_A| + |I_B|. \tag{2.5}$$

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

$$|I_1| + |I_A| + |I_B| + r(A \cap B) \leq r(A) + r(B). \tag{2.6}$$

De (2.5) y (2.6) obtenemos la desigualdad esperada. Así que la función rango r de M satisface (r1), (r2) y (r3). □

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

Teorema 2.9. *Sea r una función de valor entero con dominio el conjunto potencia de un conjunto finito E que satisface las propiedades (r1), (r2) y (r3). También r satisface lo siguiente:*

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

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

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

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

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

Demostración.

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

cualquier subconjunto de E es mayor o igual que 0, así que $r(A) - r(A \cap \{x\}) \leq r(A) < r(A) + 1$. Si $r(\{x\}) = 1$, entonces $r(A \cup \{x\}) \leq r(A) + 1 - r(A \cap \{x\}) \leq r(A) + 1$. Podemos concluir entonces que (r2*) se satisface.

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

$$r\big((A \cup \{x\}) \cup (A \cup \{y\})\big) + r\big((A \cup \{x\}) \cap (A \cup \{y\})\big) \leq r(A \cup \{x\}) + r(A \cup \{y\}) = r(A) + r(A).$$

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

A continuación se demostrará el recíproco del Teorema 2.9, es decir, que una función de valor entero r que satisface las propiedades (r1*), (r2*) y (r3*) también verifica (r1), (r2) y (r3). Primero se probará que se cumplen (r1) y (r2).

Teorema 2.10. *Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Entonces r satisface las propiedades (r1) y (r2).*

Demostración.

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

$$0 \leq r(A') \leq |A'|. \tag{2.7}$$

Por (r2*) obtenemos la siguiente desigualdad:

$$r(A') \leq r(A' \cup \{x\}) \leq r(A') + 1. \tag{2.8}$$

Así que por (2.7) y por (2.8) obtenemos que

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

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

Sean $A, B \subseteq E$ tales que $A \subseteq B$. Demostraremos que se cumple (r2) por inducción sobre $|B \setminus A|$. Si $|B \setminus A| = 0$, entonces $A = B$ y (r2) se satisface. Supongamos ahora que la afirmación se cumple para todas las parejas de conjuntos tales que uno es subconjunto del otro y tales que la cardinalidad

de la diferencia del más grande con el más pequeño igual a n. Supongamos que $|B \setminus A| = n + 1$. Podemos elegir $x \in B \setminus A$ tal que $|B \setminus (A \cup \{x\})| = n$. Como $A \cup \{x\} \subseteq B$, podemos aplicar la hipótesis de inducción y obtenemos que $r(A \cup \{x\}) \leq r(B)$. Por (r2*), $r(A) \leq r(A \cup \{x\})$, así que $r(A) \leq r(B)$. Por lo tanto, (r2) se cumple. □

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

Lema 2.3. *Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Si $A \subseteq E$, y $x_1, x_2, \ldots, x_n \in E \setminus A$ son tales que $r(A) = r(A \cup \{x_1\}) = r(A \cup \{x_2\}) = \cdots = r(A \cup \{x_n\})$, entonces*

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

Demostración.

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

$$r(A) = r(A \cup \{x_1, x_2, \ldots, x_{n-1}, x_n\}) = r(A \cup \{x_1, x_2, \ldots, x_{n-1}, x_{n+1}\}). \tag{2.9}$$

Por el Teorema 2.10 (r2) se cumple, así que las siguientes desigualdades son ciertas:

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

por lo cual $r(A \cup \{x_1, x_2, \ldots, x_{n-1}\}) = r(A)$. Por (2.9) se tiene que:

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

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

La propiedad mencionada en el Lema 2.3 se identificará con (r3**).

Lema 2.4. *([1] Lema 2.47, pág. 69) Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Sean $A, B \subseteq E$ tales que $A \subseteq B$, y sea $x \in E$. Se cumple que*

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

Teorema 2.11. *Sean E un conjunto finito y r una función de valor entero con dominio $\mathcal{P}(E)$ que satisface (r1*), (r2*) y (r3*). Entonces r satisface la propiedad (r3).*

Demostración.

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

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

Como $A \setminus \{x\} \subseteq (A \setminus \{x\}) \cup B$, por el Lema 2.4 se verifica que

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

de donde

$$r(A) - r(A \setminus \{x\}) \geq r(A \cup B) - r((A \setminus x) \cup B). \tag{2.10}$$

De (2.10) y de la hipótesis de inducción obtenemos las siguientes desigualdades:

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

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

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

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

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

Teorema 2.12. *Sea E un conjunto finito con una función de valor entero r con dominio $\mathcal{P}(E)$ tal que*

satisface las propiedades (r1), (r2) y (r3). Definimos la familia

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

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

Demostración.

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

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

$$|I| \leq r(I \setminus J) + r(J). \tag{2.11}$$

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

$$r(I \setminus J) + r(J) \leq |I \setminus J| + |J| = |I|. \tag{2.12}$$

De (2.11) y de (2.12) tenemos que $|I| \leq r(I \setminus J) + r(J) \leq |I|$, así que $r(I \setminus J) + r(J) = |I| = |I \setminus J| + |J|$, de donde $|I \setminus J| - r(I \setminus J) = r(J) - |J|$. Como $r(I \setminus J) \leq |I \setminus J|$ y $r(J) \leq |J|$, entonces $0 \leq |I \setminus J| - r(I \setminus J)$ y $r(J) - |J| \leq 0$, por lo que $0 \leq |I \setminus J| - r(I \setminus J) = r(J) - |J| \leq 0$, luego $0 = |I \setminus J| - r(I \setminus J) = r(J) - |J|$, por consiguiente, $r(I \setminus J) = |I \setminus J|$ y $r(J) = |J|$. Así queda demostrado que $J \in \mathcal{I}$, es decir, (I2) se satisface. Para probar (I3), sean $I, J \in \mathcal{I}$ tales que $|I| < |J|$. Como $I, J \in \mathcal{I}$, entonces $r(I) = |I|$ y $r(J) = |J|$. Sea $J \setminus I = \{x_1, x_2, \ldots, x_k\}$, para alguna $k \geq 1$. Supongamos que (I3) no se cumple, es decir, que para todo $i \in [k]$, $I \cup \{x_i\} \notin \mathcal{I}$, entonces $r(I \cup \{x_i\}) \neq |I \cup \{x_i\}| = |I| + 1$. Por (r1), $r(I \cup \{x_i\}) \leq |I \cup \{x_i\}| = |I| + 1$, entonces $r(I \cup \{x_i\}) < |I| + 1$. Por (r2), $r(I) \leq r(I \cup \{x_i\})$, así que $|I| \leq r(I \cup \{x_i\}) < |I| + 1$. Por lo tanto, para todo $i \in [k]$, $r(I \cup \{x_i\}) = |I|$. Si $|J \setminus I| = 1$, entonces $I \cup \{x_1\} = J$ y por lo anterior tenemos que $r(J) = r(I \cup \{x_1\}) = r(I) = |I| < |J| = r(J)$, lo cual es una contradicción. Entonces $|J \setminus I| > 1$, es decir, existe $k > 1$ tal que $J \setminus I = \{x_1, x_2, \ldots, x_k\}$. Como r verifica (r1), (r2) y (r3), por el Teorema 2.9 r cumple con (r1*), (r2*) y (r3*), luego por el Lema 2.3 se cumple (r3**), así que $r(I \cup \{x_1, x_2, \ldots, x_k\}) = |I|$, pero $I \cup \{x_1, x_2, \ldots, x_k\} = J$, entonces $|J| = r(J) = |I| < |J|$, lo cual es una contradiccón. Por lo tanto, (I3) se satisface y en efecto $M = (E, \mathcal{I})$ es un matroide.

Por último, vamos a demostrar que en efecto r es la función rango de M. Sea s la función rango de M, es decir, la función que a cada subconjunto de E le asigna la mayor de las cardinalidades de los conjuntos independientes contenidos en él. Nuestro objetivo es comprobar que $r = s$. El dominio de ambas funciones es $\mathcal{P}(E)$, así que sólo falta verificar que su regla de correspondencia es la misma. Sean $A \subseteq E$ e $I \subseteq A$ un conjunto independiente tal que $s(A) = |I|$. Como $I \in \mathcal{I}$, cumple que $r(I) = |I|$, de manera que $s(A) = |I| = r(I)$. Además, por (r2) tenemos que $r(I) \leq r(A)$. Por lo tanto, para todo $A \in \mathcal{P}(E)$, $s(A) \leq r(A)$. Supongamos que la otra desigualdad no se cumple, es decir, que existe

$A \in \mathcal{P}(E)$ tal que $s(A) < r(A)$. Sea $I \in \mathcal{I}$ subconjunto de A tal que $s(A) = |I|$, entonces $|I| < r(A)$ y para todo $x \in A \setminus I$, $I \cup \{x\} \notin \mathcal{I}$. Por (r2*), $|I| = r(I) \leq r(I \cup \{x\}) \leq r(I) + 1 = |I| + 1$, pero por la manera en la que se tomó I no puede ocurrir que $r(I \cup \{x\}) = |I| + 1$, por lo que $r(I \cup \{x\}) = r(I)$. Como r verifica (r3**), obtenemos que $r(A) = r(I) = |I|$, lo cual contradice que $|I| < r(A)$. Concluimos entonces que para todo $A \in \mathcal{P}(E)$, $r(A) \leq s(A)$. Así que en efecto, r es la función rango de M. □

Los Teoremas 2.8 y 2.12 permiten establecer una cuarta definición de matroide.

Definición 2.8 (Por función rango)**.** Un *matroide* M es un par ordenado (E, r) donde E es un conjunto finito y r es una función de valor entero con dominio $\mathcal{P}(E)$ que cumple las siguientes propiedades para cualesquiera $A, B \subseteq E$:

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

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

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

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

2.2. Representación gráfica de un matroide

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

Ejemplo 2.8. Las reglas para elaborar la representación gráfica de un matroide de rango 3 son las siguientes:

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

- Cualquier conjunto de 4 o más puntos representa a un conjunto dependiente.

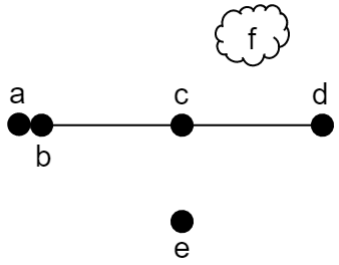

Figura 2.2: Representación de un matroide.

Sea M el matroide representado en la Figura 2.2. M tiene como conjunto subyacente a $E = \{a, b, c, d, e, f\}$. M tiene 20 conjuntos independientes y son los siguientes:

- Cardinalidad 0: $\emptyset$.
- Cardinalidad 1: $\{a\}, \{b\}, \{c\}, \{d\}, \{e\}$.
- Cardinalidad 2: $\{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{b, d\}, \{b, e\}, \{c, d\}, \{c, e\}, \{d, e\}$.
- Cardinalidad 3: $\{a, c, e\}, \{a, d, e\}, \{b, c, e\}, \{b, d, e\}, \{c, d, e\}$.

Las bases de M, son justamente todos los conjuntos independientes de cardinalidad 3.
Los conjuntos dependientes de M son los siguientes 44 conjuntos:

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

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

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

- Rango 0: $\emptyset$, $\{f\}$.
- Rango 1: $\{a, b\}$, $\{a, f\}$, $\{b, f\}$, $\{c, f\}$, $\{d, f\}$, $\{e, f\}$ y todos los conjuntos independientes de cardinalidad 1.
- Rango 2: $\{a, b, c\}$, $\{a, b, d\}$, $\{a, b, e\}$, $\{a, c, d\}$, $\{a, c, f\}$, $\{a, d, f\}$, $\{a, e, f\}$, $\{b, c, d\}$, $\{b, c, f\}$, $\{b, d, f\}$, $\{b, e, f\}$, $\{c, d, f\}$, $\{c, e, f\}$, $\{d, e, f\}$, $\{a, b, c, d\}$, $\{a, b, c, f\}$, $\{a, b, d, f\}$, $\{a, b, e, f\}$, $\{a, c, d, f\}$, $\{b, c, d, f\}$, $\{a, b, c, d, f\}$ y los conjuntos independientes de cardinalidad 2.
- Rango 3: los conjuntos independientes de cardinalidad 3 y los conjuntos restantes.

2.3. Matroide asociado a un código lineal

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

Definición 2.9. Sean $M_1 = (E_1, \mathcal{I}_1)$ y $M_2 = (E_2, \mathcal{I}_2)$ matroides. Una función $\varphi\colon E_1 \to E_2$ es un *morfismo de matroides* si para cada $I \in \mathcal{I}_1$, $\varphi(I) \in \mathcal{I}_2$. La función φ se llama *isomorfismo de matroides* si φ es morfismo de matroides, φ es biyectiva y φ^{-1} es también un morfismo de matroides. Si existe un isomorfismo de matroides entre M_1 y M_2, decimos que M_1 y M_2 son *isomorfos*.

Recuérdese que uno de los objetivos principales de este trabajo es asociar un matroide a un código lineal. Se ha visto que ciertos resultados de la teoría de códigos pueden demostrarse con menos dificultad empleando resultados de la teoría de matroides. A un código lineal ya se le ha asignado su matriz generadora. Lo que se hará a continuación es relacionar una matriz con un matroide, con lo cual se cumplirá dicho objetivo.

Teorema 2.13. *Sea $E_G = [n]$ el conjunto de etiquetas de las columnas de una matriz G de tamaño $k \times n$ sobre un campo $\mathbb{F}$ y sea $\mathcal{I}_G$ la familia de subconjuntos I de E_G para los cuales el conjunto de columnas con etiquetas en I es linealmente independiente en el espacio vectorial $\mathbb{F}^k$. Entonces $(E_G, \mathcal{I}_G)$ es un matroide.*

Demostración.

Demostraremos que $(E_G, \mathcal{I}_G)$ es un matroide mediante la caracterización de conjuntos independientes. La condición (I1) se satisface ya que el conjunto de columnas etiquetadas por $\emptyset$ es el conjunto $\emptyset$, que es linealmente independiente en $\mathbb{F}^k$. Sea $I \in \mathcal{I}_G$, entonces el conjunto de columnas etiquetadas por I es linealmente independiente en $\mathbb{F}^k$, así que si $J \subseteq I$, el conjunto de columnas etiquetadas por J está contenido en el conjunto de columnas etiquetadas por I, y por ello también es linealmente independiente en $\mathbb{F}^k$. Por lo tanto, se cumple (I2). Para probar (I3), tomemos $I, J \in \mathcal{I}$, tales que $|I| < |J|$. Sea W el subespacio de $\mathbb{F}^k$ generado por los vectores columna etiquetados por $I \cup J$. Tenemos que $\dim W \geq |J|$. Supongamos que para todo elemento e de $J \setminus I$, el conjunto de vectores columna etiquetados por $I \cup \{e\}$ es linealmente dependiente. Sea $\{v_1, v_2, \ldots, v_k\}$ el conjunto de vectores etiquetados por I y $\{u_1, u_2, \ldots, u_l\}$ el conjunto de vectores correspondiente al conjunto $J \setminus I$. Entonces para cada $i \in \{1, 2, \ldots, l\}$ existen escalares $\lambda_1^{(i)}, \lambda_2^{(i)}, \ldots, \lambda_k^{(i)}, \lambda_{k+1}^{(i)}$ no todos iguales a 0, tales que

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

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

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

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

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

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

Definición 2.10. El matroide que se obtiene como en el Teorema 2.13 a partir de una matriz G se denota por $M[G]$ y se llama el *matroide vector* de G.

Nótese que el Teorema 2.13 es más general, ya que no se limita a matrices con entradas en un campo finito, sino que abarca incluso campos infinitos como es el caso del siguiente ejemplo.

Ejemplo 2.9. Sea G la matriz

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

sobre el campo de los números reales. Sean E_G e $\mathcal{I}_G$ como en el Teorema 2.13. Entonces $E_G = \{1, 2, 3, 4, 5\}$ e $\mathcal{I}_G = \{\emptyset, \{1\}, \{2\}, \{4\}, \{5\}, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}$. La familia de bases de $M[G]$ es $\mathcal{B} = \{\{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}$; la familia de conjuntos dependientes de este

matroide es $\{\{3\},\{1,3\},\{1,4\},\{2,3\},\{3,4\},\{3,5\}\} \cup \{X \subseteq E : |X| \geq 3\}$ y su familia de circuitos es $\{\{3\},\{1,4\},\{1,2,5\},\{2,4,5\}\}$. Note que $M[G]$ es un matroide de rango 2.

Definición 2.11. Un matroide M se llama *representable* sobre el campo $\mathbb{F}$ si existe una matriz G con entradas en $\mathbb{F}$ tal que M es isomorfo al matroide $M[G]$. G se llama *representación* para M sobre $\mathbb{F}$ o $\mathbb{F}-$*representación* para M. Un matroide es *representable* si tiene una representación sobre algún campo.

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

Teorema 2.14. *Sea G una matriz de tamaño $k \times n$ con entradas en un campo $\mathbb{F}$. Sea G' una matriz que se obtiene realizando algunas de las operaciones elementales con los renglones de G (es decir, intercambio de renglones, multiplicación de un renglón por una constante diferente de cero o sumar un múltiplo de un renglón a otro renglón). Entonces $M[G] = M[G']$.*

Demostración.

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

$$\begin{aligned} \alpha_1 g_{1l_1} + \alpha_2 g_{1l_2} + \cdots + \alpha_r g_{1l_r} &= 0 \\ \alpha_1 g_{2l_1} + \alpha_2 g_{2l_2} + \cdots + \alpha_r g_{2l_r} &= 0 \\ &\vdots \\ \alpha_1 g_{kl_1} + \alpha_2 g_{kl_2} + \cdots + \alpha_r g_{kl_r} &= 0 \end{aligned} \tag{2.13}$$

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

$$\begin{aligned} \beta_1 g'_{1l_1} + \beta_2 g'_{1l_2} + \cdots + \beta_r g'_{1l_r} &= 0 \\ \beta_1 g'_{2l_1} + \beta_2 g'_{2l_2} + \cdots + \beta_r g'_{2l_r} &= 0 \\ &\vdots \\ \beta_1 g'_{kl_1} + \beta_2 g'_{kl_2} + \cdots + \beta_r g'_{kl_r} &= 0 \end{aligned} \tag{2.14}$$

La matriz de coeficientes asociada al sistema lineal homogéneo 2.14 es (g'_{ml_n}) de tamaño $k \times r$. Como G' se obtiene mediante operaciones elementales con los renglones de G, entonces existe una serie de operaciones elementales que al aplicarlas a la matriz G' se obtiene la matriz G, así que si aplican dichas operaciones a la matriz (g'_{ml_n}) se obtiene la matriz (g_{ml_n}) que es la matriz asociada al sistema

2.13. Por lo tanto, la única solución al sistema 2.14 es el vector $[\beta_1, \beta_2, \ldots, \beta_r] = [0, 0, \ldots, 0]$, entonces los vectores columna de G' etiquetados por J en efecto son linealmente independientes, por lo que $J \in \mathcal{I}_{G'}$. Análogamente se prueba que si $J \in \mathcal{I}_{G'}$ también $J \in \mathcal{I}_G$. En conclusión, $\mathcal{I}_G = \mathcal{I}_{G'}$ y con ello queda probado que $M[G] = M[G']$. □

De álgebra lineal se sabe que dos matrices son equivalentes por renglones si y sólo si tienen el mismo espacio renglón. Si G_1 y G_2 son matrices generadoras del código C, el espacio renglón de G_1 es igual al espacio renglón de G_2, por lo que G_1 y G_2 son matrices equivalentes por renglones, es decir, es posible obtener G_2 a partir de G_1 mediante una secuencia de operaciones elementales con renglones. Así, por el Teorema 2.14, $M[G_1] = M[G_2]$. Este resultado permite denotar con $M_C = (E_C, \mathcal{I}_C)$ al matroide vector de cualquier matriz generadora de C.

Definición 2.12. Sea $M = (E, \mathcal{I})$ un matroide y $\mathcal{B}$ su familia de bases. Para cada $B \in \mathcal{B}$ se establece la notación $B^\perp = E \setminus B$. Definimos la familia $\mathcal{B}^\perp = \{B^\perp \mid B \in \mathcal{B}\}$. Sea $\mathcal{I}^\perp = \{I \subseteq E \mid \exists B \in \mathcal{B} : I \subseteq B^\perp\}$. $M^\perp = (E, \mathcal{I}^\perp)$ se llama *matroide dual* de M.

Teorema 2.15. *Sea M un matroide. Entonces $M^\perp$ es, en efecto, un matroide.*

Demostración.

En esta prueba haremos uso del Corolario 2.1: usaremos el hecho de que M es matroide y por ello la familia $\mathcal{B}$ satisface (B1), (B2*) y (B3*), y por otro lado probaremos que la familia $\mathcal{B}^\perp$ satisface las propiedades (B1), (B2*) y (B3*) para demostrar que $M^\perp$ es un matroide.

La familia $\mathcal{B}$ satisface la propiedad (B1), así que existe $B \in \mathcal{B}$, de donde $B^\perp \in \mathcal{B}^\perp$, es decir, $\mathcal{B}^\perp \neq \emptyset$ y por tanto, $\mathcal{B}^\perp$ satisface la propiedad (B1). Ahora, sean ${B_1}^\perp, {B_2}^\perp \in \mathcal{B}^\perp$, donde $B_1, B_2 \in \mathcal{B}$. Por (B2*), $|B_1| = |B_2|$, de aquí obtenemos inmediatamente que $|E \setminus B_1| = |E \setminus B_2|$, es decir, $|{B_1}^\perp| = |{B_2}^\perp|$, así que $\mathcal{B}^\perp$ también satisface (B2*). Dado que $B_1^\perp \setminus B_2^\perp = (E \setminus B_1) \setminus (E \setminus B_2) = B_2 \setminus B_1$, si $x \in B_1^\perp \setminus B_2^\perp$, entonces $x \in B_2 \setminus B_1$. $\mathcal{B}$ verifica la propiedad (B3*), es decir, la propiedad de intercambio fuerte en bases, por lo que existe $y \in B_1 \setminus B_2 = B_2^\perp \setminus B_1^\perp$ tal que $(B_1 \setminus \{y\}) \cup \{x\}$ y $(B_2 \setminus \{x\}) \cup \{y\}$ son bases del matroide M, entonces $E \setminus [(B_1 \setminus \{y\}) \cup \{x\}]$ y $E \setminus [(B_2 \setminus \{x\}) \cup \{y\}]$ son elementos de $B^\perp$. Se tiene que $E \setminus [(B_1 \setminus \{y\}) \cup \{x\}] = [E \setminus (B_1 \setminus \{y\})] \cap (E \setminus \{x\}) = [(E \setminus B_1) \cup \{y\}] \cap (E \setminus \{x\}) = [E \setminus (B_1 \cup \{x\})] \cup \{y\} = [(E \setminus B_1) \setminus \{x\}] \cup \{y\} = (B_1^\perp \setminus \{x\}) \cup \{y\}$, y de manera análoga puede mostrarse que $E \setminus [(B_2 \setminus \{x\}) \cup \{y\}] = (B_2^\perp \setminus \{y\}) \cup \{x\}$, por lo cual concluimos que $(B_1^\perp \setminus \{x\}) \cup \{y\}$ y $(B_2^\perp \setminus \{y\} \cup \{x\} \in \mathcal{B}^\perp$. Entonces $\mathcal{B}^\perp$ verifica (B3*). Por lo tanto, $M^\perp$ es un matroide. □

Teorema 2.16. *([2]) Sea C un $[n, k]$-código. Los matroides $(M_C)^\perp$ y $M_{C^\perp}$ son isomorfos.*

El siguiente teorema muestra una forma sencilla de calcular en el matroide dual el rango de un subconjunto a partir de la función rango del matroide original. Será de gran utilidad en el Capítulo 4. Se denotará la función rango del matroide dual como $r^\perp$.

Teorema 2.17. *Sea $M = (E, \mathcal{I})$ un matroide y r su función rango. Para $A \subseteq E$ se cumple lo siguiente:*

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

Demostración.

Veamos que $r^{\perp}(A) = \text{máx}\{|A \cap B^{\perp}| \colon B^{\perp} \in \mathcal{B}^{\perp}\}$. Por definición $r^{\perp}(A)$ es la cardinalidad del conjunto independiente más grande de $M^{\perp}$ que está contenido en A. Sea $I_A \subseteq A$ conjunto independiente tal que $r^{\perp}(A) = |I_A|$ y $B_1^{\perp}$ una base de $M^{\perp}$ tal que $I_A \subseteq B_1^{\perp}$, por lo tanto $I_A \subseteq A \cap B_1^{\perp}$. Además, existe una base B_1 del matroide M tal que $B_1^{\perp} = E \setminus B_1$. Si suponemos que $I_A \subsetneq A \cap B_1^{\perp}$, entonces existe $x \in A \cap B_1^{\perp}$ tal que $x \notin I_A$ y se cumple que $I_A \subsetneq I_A \cup \{x\} \subseteq A \cap B_1^{\perp}$. Como $I_A \cup \{x\} \subseteq B_1^{\perp}$ e $I_A \cup \{x\} \subseteq A$, $I_A \cup \{x\}$ es un conjunto independiente de $M^{\perp}$ que es subconjunto de A y cuya cardinalidad es mayor que I_A, lo cual es una contradicción. Por lo tanto, $I_A = A \cap B_1^{\perp}$. Finalmente, como todos los conjuntos de la forma $A \cap B^{\perp}$ son conjuntos independientes de $M^{\perp}$ que están contenidos en A e I_A es uno de tales conjuntos pero de cardinalidad máxima, entonces concluimos que $r^{\perp}(A) = |I_A| = \text{máx}\{|A \cap B^{\perp}| \colon B^{\perp} \in \mathcal{B}^{\perp}\}$. Entonces $B_1^{\perp}$ es un elemento de $\mathcal{B}^{\perp}$ cuya intersección con A es máxima, o equivalentemente, $B_1^{\perp}$ es un elemento de $\mathcal{B}^{\perp}$ cuya intersección con $E \setminus A$ es mínima, entonces la intersección de $B_1 = E \setminus B_1^{\perp}$ y $E \setminus A$ es máxima entre todos los complementos de las bases de $\mathcal{B}^{\perp}$ (que son las bases de M), así que por definición de rango del matroide M, $r(E \setminus A) = |(E \setminus A) \cap B_1|$. E se divide en los siguientes cuatro conjuntos ajenos entre sí: $A \setminus B_1^{\perp}$, $A \cap B_1^{\perp}$, $B_1^{\perp} \setminus A$ y $E \setminus (A \cup B_1^{\perp}) = (E \setminus A) \cap (E \setminus B_1^{\perp}) = (E \setminus A) \cap B_1$. Sean x_1, x_2, x_3 y x_4 las cardinalidades de dichos conjuntos, respectivamente. Tenemos que $x_2 = |A \cap B_1^{\perp}| = r^{\perp}(A)$ y $x_4 = |E \setminus (A \cup B_1^{\perp})| = |(E \setminus A) \cap B_1| = r(E \setminus A)$. Además, $x_3 + x_4 = |B_1^{\perp} \setminus A| + |E \setminus (A \cup B^{\perp})| = |E| - |A|$ y $x_2 + x_3 = |A \cap B_1^{\perp}| + |B_1^{\perp} \setminus A| = |B_1^{\perp}| = |E| - |B_1| = |E| - r(M)$, así que por el valor de x_3 en ambas igualdades tenemos que $|E| - |A| - x_4 = |E| - r(M) - x_2$, por lo que $x_2 = |A| + x_4 - r(M)$, y sustituyendo los valores ya conocidos de x_2 y x_4 concluimos finalmente que $r^{\perp}(A) = r(E \setminus A) + |A| - r(M)$. $\square$

Capítulo 3

Enumeradores de pesos

Uno de los conceptos más importantes en la teoría de códigos es el de peso de una palabra-código que se definió en el Capítulo 1 y es la base de este apartado. El resultado más importante que se presentará en este trabajo es la Identidad de MacWilliams la cual aborda una manera de conocer el peso de las palabras-código de un código dual. Dicha identidad se menciona en este capítulo pero se demuestra hasta los Capítulos 4 y 5.

La mayor parte del contenido de este capítulo se tomó del libro electrónico [2]. Algunas de las pruebas se presentan sin modificaciones, otras se completaron o se realizaron ya que no estaban incluidas originalmente en dicho libro. Los códigos que se mencionan en este capítulo son subconjuntos de $\mathbb{F}_q^n$. Cuando se presente algún resultado en el que se mencione a q recuérdese que q es el número de elementos del campo finito.

3.1. Distribución de pesos

Definición 3.1. Sea C un código de longitud n. La *distribución* o *espectro de pesos* de C es el conjunto de parejas ordenadas

$$\{(w, A_w) \mid w \in [n]\},$$

donde A_w es el número de palabras-código en C de peso w.

La distribución de pesos es un importante tema de investigación en teoría de códigos ya que contiene información crucial para estimar la capacidad de corregir errores y la probabilidad de detección y correción de errores con respecto a algunos algoritmos.

A continuación se definen dos polinomios que son representaciones útiles de la distribución de pesos y se emplean con bastante frecuencia, como se verá más adelante.

Definición 3.2. Sea C un código de longitud n. Se define el *enumerador de pesos* de C como el

polinomio

$$W_C(Z) = \sum_{w=0}^{n} A_w Z^w.$$

El polinomio *enumerador de pesos homogéneo* de C se define como

$$W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

Se puede conocer el enumerador de pesos a partir del enumerador de pesos homogéneo y viceversa. Basta con usar las siguientes relaciones:

$$W_C(Z) = W_C(1, Z),$$

$$W_C(X, Y) = X^n W_C(X^{-1} Y).$$

La distribución de pesos puede conocerse a partir de los enumeradores de pesos mediante los coeficientes de los polinomios.

El enumerador de pesos de un código lineal y su dual están relacionados mediante la Identidad de MacWilliams. Esta identidad señala cómo puede hallarse el enumerador de pesos homogéneo de un código dual dado el enumerador de pesos homogéneo del código original y se enuncia a continuación.

Teorema 3.1 (**MacWilliams**). *Sea C un $[n, k]$-código. Entonces*

$$W_{C^\perp}(X, Y) = q^{-k} W_C(X + (q-1)Y, X - Y).$$

3.2. El enumerador de pesos generalizado

Definición 3.3. Sean C un código lineal y J un subconjunto de $[n]$. Se define el siguiente conjunto:

$$C(J) = \{c \in C \mid \forall j \in J : c_j = 0\}.$$

Está claro que $C(J)$ es un subespacio vectorial de C y por ello puede darse la siguiente definición.

Definición 3.4. Sean C un código lineal, J un subconjunto de $[n]$ y $t \in \{0, 1, \ldots, n\}$. Se establecen las siguientes notaciones:

$$l(J) = \dim C(J),$$

$$B_J = q^{l(J)} - 1,$$

$$B_t = \sum_{|J|=t} B_J.$$

Observación 3.1. Nótese que B_J es el número de elementos de $C(J)$ distintos del vector cero, es decir, B_J es el número de palabras-código de C distintas de 0, tales que para todo $j \in J$ su j-ésima coordenada es igual a 0.

Teorema 3.2. *Sea C un código lineal. Es válida la siguiente relación entre los números B_t y la distribución de pesos de un código:*

$$B_t = \sum_{w=0}^{n} \binom{n-w}{t} A_w.$$

No se presenta la demostración del Teorema 3.2 porque más adelante se generaliza este teorema y su prueba sigue la misma idea.

En esta sección se trabajará con códigos que son subconjuntos de un código fijo. Por ello se da la siguiente definición.

Definición 3.5. Sea C un código de longitud n. Se dice que D es *subcódigo* de C si es un subconjunto no vacío de C.

En el Capítulo 1 se definió el peso de una sola palabra-código así como el peso mínimo de un código. A continuación se asigna un peso a cada subcódigo de un código dado C para establecer el peso mínimo por cada dimensión posible de subcódigos lineales de C.

Definición 3.6. Sean C un $[n,k]$-código y D un subcódigo de C r-dimensional. El *soporte* del subcódigo D es el conjunto

$$supp(D) = \{i \in [n] \mid \exists c \in D : c_i \neq 0\}.$$

Al número de elementos del soporte de D se le llama *peso* o *longitud efectiva del subcódigo D* y se denota por $wt(D)$.

Observación 3.2. Sea D un subcódigo r-dimensional de un $[n,k]$-código C. $supp(D)^C = \{i \in [n] \mid \forall c \in D : c_i = 0\}$. Esto es, el soporte de D es n menos el número de coordenadas que son cero para cada palabra en el subcódigo.

Definición 3.7. Sea C un $[n,k]$-código y $r \in \{0,1,\ldots,k\}$. El *r-ésimo peso de Hamming generalizado de C* es

$$d_r = \text{mín}\{wt(D) \mid D \text{ es subcódigo de } C \text{ de dimensión } r\}.$$

Observación 3.3. Sea C un $[n,k]$-código. Como C sólo tiene un subcódigo de dimensión 0 y su peso es igual a 0, entonces $d_0 = 0$. Por otro lado, $d_1 = \text{mín}\{wt(D) \mid D \text{ es subcódigo de } C \text{ de dimensión } 1\}$, es decir, d_1 es el mínimo de los pesos de los subcódigos de C generados por una sola palabra-código diferente del vector nulo. Pero el soporte de cada uno de estos códigos coincide con el soporte de su palabra-código generadora. Así que al comparar el peso de todos los subcódigos de C de dimensión 1 también se compara el peso de todas las palabras-código de C, por lo cual se concluye que $d_1 = d$.

Los números A_w se definieron para indicar el número de palabras-código de peso w que posee un código. Ahora que se ha definido el peso de un subcódigo lineal también se necesita una expresión que indique el número de subcódigos que comparten el mismo peso. Más adelante será importante además del peso la dimensión del subcódigo, por ello se establece la siguiente definición.

Definición 3.8. Sea C un $[n, k]$-código y $r \in \{0, 1, \ldots, k\}$. Con $A_w^{(r)}$ se denota el número de subcódigos de C de peso w y dimensión r, es decir, $A_w^{(r)} = |\{D \subseteq C \mid \dim D = r, wt(D) = w\}|$. Al conjunto de los números $A_w^{(r)}$ se le llama *r-ésima distribución de pesos generalizada* de C.

De manera análoga a como se definió el enumerador de pesos homogéneo de un código mediante un polinomio en dos variables cuyos coeficientes eran los números A_w, en la siguiente definición se construye un polinomio empleando la r-ésima distribución de pesos generalizada de un código.

Definición 3.9. Para un $[n, k]$-código lineal C y $r \in \{0, 1, \ldots, k\}$ se define el *r-ésimo enumerador de pesos generalizado* de C como

$$W_C^{(r)}(X, Y) = \sum_{w=0}^{n} A_w^{(r)} X^{n-w} Y^w.$$

Observación 3.4. Tenemos que $A_0^{(0)} = 1$, y para toda $0 < r \leq k$, $A_0^{(r)} = 0$, pues no existe algún código de dimensión mayor o igual a 1 y de peso 0. Además, todo subespacio de C de dimensión 1 contiene $q-1$ palabras-código diferentes de cero, así que para $0 < w \leq n$, $(q-1)A_w^{(1)} = A_w$. Entonces podemos hallar el enumerador de pesos homogéneo a partir del generalizado mediante la siguiente identidad:

$$W_C(X, Y) = W_C^{(0)}(X, Y) + (q-1)W_C^{(1)}(X, Y).$$

En los siguientes dos lemas se proporcionan fórmulas que permiten conocer el valor de $l(J)$.

Lema 3.1. *Sea C un $[n, k]$-código lineal con matriz generadora G. Sea $J \subseteq [n]$ y $|J| = t$. Sea G_J la submatriz de G de tamaño $k \times t$ formada por las columnas de G indexadas por J, y sea $r(J)$ el rango de G_J. Entonces $l(J) = k - r(J)$.*

Demostración.

Sea C_J el código generado por la submatriz G_J, y sean $g_1, g_2, \ldots, g_k$ y $g'_1, g'_2, \ldots, g'_k$ los vectores fila de G y G_J, respectivamente. Considérese la proyección

$$\pi : C \to \mathbb{F}_q^t$$

tal que de cada palabra-código se preservan en un vector solamente las componentes indexadas por J. Está claro que π es una transformación lineal y para todo $i \in [k]$, $\pi(g_i) = g'_i$. Por lo anterior puede verse que la imagen de C bajo π es un subconjunto de C_J. Por otro lado, considérese un elemento $\hat{c}$ de C_J. Éste debe ser una combinación lineal de las filas de la matriz G_J, es decir, existen escalares

$\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_q$ tales que $\hat{c} = \alpha_1 g'_1 + \alpha_2 g'_2 + \cdots + \alpha_k g'_k$. Ahora, sea $c = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_k g_k \in C$. Como π es lineal se tiene que $\pi(c) = \pi(\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_k g_k) = \alpha_1 \pi(g_1) + \alpha_2 \pi(g_2) + \cdots + \alpha_k \pi(g_k) = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_k g_k = \hat{c}$. Así que C_J es la imagen de C bajo π. Por otro lado, $C(J)$ es el conjunto de las palabras-código que tienen 0 en todas las coordenadas etiquetadas por J, entonces el kernel de π es justamente $C(J)$. Por el teorema del rango se tiene que $\dim C(J) + \dim C_J = \dim C$, es decir, $l(J) + r(J) = k$, de donde se obtiene el resultado esperado. □

Lema 3.2. *Sean d y $d^\perp$ la distancia mínima de C y $C^\perp$, respectivamente. Sean $J \subseteq [n]$ y $|J| = t$. Entonces*

$$l(J) = \begin{cases} k - t & si\ t < d^\perp \\ 0 & si\ t > n - d. \end{cases}$$

Demostración.

Supongamos que $t < d^\perp$. Sea G una matriz generadora de C. Por el Teorema 1.4, G es una matriz de verificación de paridad de $C^\perp$. Por el Lema 3.1, $l(J) = k - r(J)$, donde $r(J)$ es el rango de la submatriz G_J definida en el mismo lema. Como $t < d^\perp$, por el Teorema 1.6 cualquier conjunto de t columnas de G es linealmente independiente. Como G es de tamaño $k \times t$, G tiene rango t, así que $l(J) = k - t$, como se afirmó.

Ahora, supongamos que $t > n - d$. Sea $c \in C(J)$. Los elementos de $C(J)$ tienen la j-ésima componente igual a 0, para todo $j \in J$. Entonces $J \subseteq supp(c)^C$, de manera que $|J| \leq |supp(c)^C|$, es decir, $t \leq n - wt(c)$, de donde $wt(c) \leq n - t < d$ (pues $t > n - d$), así que $wt(c) < d$, esto es, el peso de c es menor que el peso mínimo del código C, así que c debe ser la palabra-código cero. Pero c es una palabra arbitraria de $C(J)$, entonces $C(J)$ debe ser el espacio nulo y por lo tanto $l(J) = 0$. □

Los siguientes números serán de gran utilidad más adelante en el establecimiento y demostración de algunos teoremas. Como se verá en el Teorema 3.3 estos números son una herramienta combinatoria de gran importancia en el álgebra lineal, pues permiten presentar información acerca de subespacios vectoriales sobre un campo finito.

$$\langle r \rangle_q = \prod_{i=0}^{r-1} (q^r - q^i) = (q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})$$

$$[m, r]_q = \prod_{i=0}^{r-1} (q^m - q^i) = (q^m - 1)(q^m - q) \cdots (q^m - q^{r-1})$$

$$\begin{bmatrix} k \\ r \end{bmatrix}_q = \frac{[k, r]_q}{\langle r \rangle_q} = \frac{(q^k - 1)(q^k - q) \cdots (q^k - q^{r-1})}{(q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})}$$

Teorema 3.3. *$\langle r \rangle_q$ es el número de bases de $\mathbb{F}_q^r$; $[m, r]_q$ es igual al número de matrices de tamaño $m \times r$ de rango r sobre $\mathbb{F}_q$; $\left[\begin{smallmatrix} k \\ r \end{smallmatrix} \right]_q$ representa el número de subespacios de $\mathbb{F}_q^k$ de dimensión r.*

Demostración.

Veamos el número de opciones que tenemos para construir una base $B = \{v_1, v_2, \ldots, v_r\}$ para $\mathbb{F}_q^r$: $\mathbb{F}_q^r$ tiene q^r elementos. v_1 puede ser cualquier elemento de $\mathbb{F}_q^r$ a excepción del vector cero, entonces podemos elegir v_1 de $q^r - 1$ formas. v_2 debe ser un vector que junto con v_1 forme un conjunto linealmente independiente, así que v_2 puede ser igual a cualquier elemento de $\mathbb{F}_q^r$ eliminando los elementos del conjunto $gen\{v_1\}$, cuya cardinalidad es igual a q, por ello existen $q^r - q$ posibilidades de elegir v_2. El vector v_3 puede ser cualquier elemento de $\mathbb{F}_q^r$ a excepción de los elementos del conjunto $gen\{v_1, v_2\}$, que tiene q^2 elementos, así que el número de opciones para elegir v_3 es $q^r - q^2$. Siguiendo el mismo razonamiento, el vector i-ésimo de B puede elegirse sin considerar los elementos de $gen\{v_1, v_2, \ldots, v_{i-1}\}$, el cual tiene q^{i-1} elementos, de manera que v_i puede tomar $q^r - q^{i-1}$ valores. Por consiguiente el número total de bases para $\mathbb{F}_q^r$ es igual a $\langle r \rangle_q = (q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})$.

Sea A una matriz de tamaño $m \times r$ sobre $\mathbb{F}_q$. Para que $A = \begin{bmatrix} v_1 & v_2 & \cdots & v_r \end{bmatrix}$ tenga rango r es necesario y suficiente que $\{v_1, v_2, \ldots, v_r\}$ sea un conjunto linealmente independiente. El proceso de selección de dichos vectores es análogo al proceso anterior de creación de una base para $\mathbb{F}_q^r$ con la diferencia de que en este caso $v_1, v_2, \ldots, v_n \in \mathbb{F}_q^m$.

Por último, $(q^k - 1)(q^k - q) \cdots (q^k - q^{r-1})$ es el número de bases de todos los subespacios de $\mathbb{F}_q^k$ de dimensión r. Así que para hallar el número de dichos subespacios basta dividir el número total de bases entre el número de bases de un subespacio de dimensión r, que es igual a $(q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})$, con lo cual queda demostrado el teorema. □

Es importante notar que el Teorema 3.3 considera el número de bases ordenadas de $\mathbb{F}_q^r$, tal como se ve en la prueba de dicho teorema. Sin embargo, es posible obtener el número de bases no ordenadas simplemente diviendo $\langle r \rangle_q$ entre $n!$.

Sean C un $[n, k]$-código lineal, $J \subseteq [n]$, $r \in \{0, 1, \ldots, k\}$ y $t \in \{0, 1, \ldots, n\}$. Establecemos las siguientes notaciones:

$$B_J^{(r)} = |\{D \subseteq C(J) : D \text{ es subespacio de dimensión } r\}|,$$

$$B_t^{(r)} = \sum_{|J|=t} B_J^{(r)}.$$

Observación 3.5. Sean $J \subseteq [n]$ y $r \in \{0, 1, \ldots, k\}$. El código $C(J)$ por ser de dimensión $l(J)$ es isomorfo a $\mathbb{F}_q^{l(J)}$. Entonces contar el número de subcódigos de $C(J)$ de dimensión r es equivalente a contar el número de subespacios vectoriales de $\mathbb{F}_q^{l(J)}$ de dimensión r, es decir, $B_J^{(r)} = \begin{bmatrix} l(J) \\ r \end{bmatrix}_q$.

Teorema 3.4. *Sean C un $[n, k]$-código, $r \in \{0, 1, \ldots, k\}$ y $t \in \{0, 1, \ldots, n\}$. Se cumple lo siguiente:*

$$B_t^{(r)} = \begin{cases} \binom{n}{t} \begin{bmatrix} k-t \\ r \end{bmatrix}_q & si\ t < d^\perp \\ 0 & si\ t > n - d_r. \end{cases}$$

Demostración.

Supongamos que $t < d^{\perp}$. Sea $J \subseteq [n]$ tal que $|J| = t$. Por el Lema 3.2 tenemos que $l(J) = k - t$ y por la Observación 3.5, $B_J^{(r)} = \begin{bmatrix} l(J) \\ r \end{bmatrix}_q$, entonces

$$B_t^{(r)} = \sum_{|J|=t} B_J^{(r)} = \sum_{|J|=t} \begin{bmatrix} l(J) \\ r \end{bmatrix}_q = \sum_{|J|=t} \begin{bmatrix} k-t \\ r \end{bmatrix}_q = \begin{bmatrix} k-t \\ r \end{bmatrix}_q \sum_{|J|=t} 1 = \begin{bmatrix} k-t \\ r \end{bmatrix}_q \binom{n}{t}.$$

Ahora, supongamos que $t > n - d_r$. Si $B_t^{(r)} \neq 0$, existe $J \subseteq [n]$ tal que $|J| = t$ y $B_J^{(r)} \neq 0$, es decir, $\{D \subseteq C(J) \mid D \text{ es subespacio de dimensión } r\} \neq \emptyset$. Entonces existe un subespacio $D \subseteq C(J)$ de dimensión r. Se cumple que $J \subseteq supp(D)^C$, lo cual implica que $|J| \leq |supp(D)^C|$, por lo tanto, $t \leq n - wt(D)$. Por lo anterior y por la hipótesis tenemos que $wt(D) \leq n - t \leq d_r$, de donde concluimos que $wt(D) < d_r$, pero d_r es el mínimo de los pesos de los subcódigos de C de dimensión r, por lo que $wt(D) < d_r$ no puede ocurrir. Por consiguiente, $B_t^{(r)} = 0$. □

El siguiente teorema es una generalización del Teorema 3.2: hace explícita la relación entre los números $B_t^{(r)}$ asociados a un código y su r-ésima distribución de pesos generalizada.

Teorema 3.5. *Sean C un $[n, k]$-código, $r \in \{0, 1, \ldots, k\}$ y $t \in \{0, 1, \ldots, n\}$. La siguiente identidad es válida:*

$$B_t^{(r)} = \sum_{w=0}^{n} \binom{n-w}{t} A_w^{(r)}.$$

Demostración.

$B_t^{(r)}$ es el número de subespacios de $C(J)$ de dimensión r, donde J puede ser cualquier subconjunto de $[n]$ de cardinalidad t. Lo que haremos a continuación será contar el número de tales subespacios por sus respectivos pesos. Existen $A_w^{(r)}$ subcódigos de C de dimensión r y de peso w. Sea D uno de tales subcódigos. D puede ser subespacio de $C(J)$ para varios conjuntos J tales que $|J| = t$. $supp(D)^C$ es el conjunto de coordenadas que son iguales a 0 para toda palabra-código de D, entonces para que D sea subcódigo de $C(J)$ basta con que el conjunto J sea un subconjunto de $supp(D)^C$, y el número de formas en las que podemos elegir tal conjunto es $\binom{|supp(D)^C|}{t}$, es decir, $\binom{n-w}{t}$. Así que el número de subespacios de $C(J)$ de dimensión r y de peso w es $\binom{n-w}{t}$, y por lo tanto $B_t^{(r)} = \sum_{w=0}^{n} \binom{n-w}{t} A_w^{(r)}$. □

Observación 3.6. Por definición, para todo $w < d_r$, $A_w^{(r)} = 0$. Además, si $w > n - t$, tenemos que $\binom{n-w}{t} = 0$. Entonces podemos escribir la igualdad del Teorema 3.5 como

$$B_t^{(r)} = \sum_{w=d_r}^{n-t} \binom{n-w}{t} A_w^{(r)}.$$

Teorema 3.6. *Sean C un $[n, k]$-código, $t \in \{0, 1, \ldots, n\}$ y $r \in \{0, 1, \ldots, k\}$. La relación entre el enumerador de pesos generalizado de C y los números $B_t^{(r)}$ asociados a C queda establecida por la*

siguiente igualdad:

$$W_C^{(r)}(X,Y) = \sum_{t=0}^{n} B_t^{(r)}(X-Y)^t Y^{n-t}.$$

Demostración.

Por el Teorema 3.5, $B_t^{(r)} = \sum_{w=0}^{n} \binom{n-w}{t} A_w^{(r)}$. Así que, aplicando el teorema del binomio a la expresión $[(X-Y)+Y]^{n-w}$ y teniendo en cuenta que para $t > n-w$, $\binom{n-w}{t} = 0$, se tiene lo siguiente:

$$\begin{aligned}
W_C^{(r)}(X,Y) &= \sum_{w=0}^{n} A_w^{(r)} X^{n-w} Y^w = \sum_{w=0}^{n} A_w^{(r)} [(X-Y)+Y]^{n-w} Y^w \\
&= \sum_{w=0}^{n} A_w^{(r)} \left(\sum_{t=0}^{n-w} \binom{n-w}{t} (X-Y)^t Y^{n-w-t} \right) Y^w = \sum_{w=0}^{n} A_w^{(r)} \sum_{t=0}^{n-w} \binom{n-w}{t} (X-Y)^t Y^{n-t} \\
&= \sum_{w=0}^{n} \sum_{t=0}^{n} A_w^{(r)} \binom{n-w}{t} (X-Y)^t Y^{n-t} = \sum_{t=0}^{n} \sum_{w=0}^{n} A_w^{(r)} \binom{n-w}{t} (X-Y)^t Y^{n-t} \\
&= \sum_{t=0}^{n} (X-Y)^t Y^{n-t} \left(\sum_{w=0}^{n} \binom{n-w}{t} A_w^{(r)} \right) = \sum_{t=0}^{n-w} B_t^{(r)} (X-Y)^t Y^{n-t}.
\end{aligned}$$

□

3.3. El enumerador de pesos extendido

Definición 3.10. Sea C un $[n,k]$-código con matriz generadora G. Denotamos con $C \otimes \mathbb{F}_{q^m}$ al conjunto de todas las $\mathbb{F}_{q^m}$-combinaciones lineales de las palabras-código de C. A $C \otimes \mathbb{F}_{q^m}$ lo llamamos el *código de extensión de C sobre $\mathbb{F}_{q^m}$*. Empleamos $A_{C\otimes\mathbb{F}_{q^m},w}$ para referirnos al número de palabras-código en $C \otimes \mathbb{F}_{q^m}$ de peso w .

Sea C un $[n,k]$—código y G una matriz generadora de C. Como las entradas de la matriz G pueden verse como elementos de $\mathbb{F}_{q^m}$, entonces G también es matriz generadora para el código de extensión $C \otimes \mathbb{F}_{q^m}$. Más aún, como $C \otimes \mathbb{F}_{q^m}$ es generado por un conjunto de vectores, entonces $C \otimes \mathbb{F}_{q^m}$ es un subespacio vectorial de $\mathbb{F}_{q^m}^n$.

Sea $J \subseteq [n]$. Por el Lema 3.1, sabemos que $l(J) = k - r(J)$, y dado que $r(J)$ es independiente de la extensión de campo $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$, tenemos que $\dim_{\mathbb{F}_q} C(J) = \dim_{\mathbb{F}_{q^m}} C \otimes \mathbb{F}_{q^m}(J)$.

Definición 3.11. Sean C un código lineal, $J \subseteq [n]$ y $t \in \{0,1,\ldots,n\}$. Definimos

$$B_J(T) = T^{l(J)} - 1$$

$$B_t(T) = \sum_{|J|=t} B_J(T).$$

Observación 3.7. $B_J(q^m)$ es el número de palabras-código distintas de cero en el código $C \otimes \mathbb{F}_{q^m}(J)$.

Nótese que a diferencia de apartados anteriores, en la Definición 3.11 no se establece notación para números sino para polinomios en la variable T. A continuación se presenta una forma alternativa de expresar dichos polinomios.

Teorema 3.7. *Sean C un código lineal, $t \in \{0, 1, \ldots, n\}$, d y $d^\perp$ la distancia mínima de C y $C^\perp$, respectivamente. Tenemos que*

$$B_t(T) = \begin{cases} \binom{n}{t}(T^{k-t} - 1) & si\ t < d^\perp \\ 0 & si\ t > n - d. \end{cases}$$

Demostración.

Por el Lema 3.2 tenemos lo siguiente: si $t < d^\perp$, entonces $l(J) = k - t$, luego $B_J(T) = T^{l(J)} - 1 = T^{k-t} - 1$ y por lo tanto, $B_t(T) = \sum_{|J|=t} B_J(T) = \sum_{|J|=t} T^{k-t} - 1 = \binom{n}{t}(T^{k-t} - 1)$. Ahora, para $t > n - d$, $l(J) = 0$, entonces $B_J(T) = T^{l(J)} - 1 = T^0 - 1 = 1 - 1 = 0$, y así, $B_t(T) = \sum_{|J|=t} B_J(T) = \sum_{|J|=t} 0 = 0$. □

A continuación se define un nuevo polinomio enumerador de pesos.

Definición 3.12. Sea C un código lineal. El *enumerador de pesos extendido* de C es:

$$W_C(X, Y, T) = X^n + \sum_{t=0}^{n} B_t(T)(X - Y)^t Y^{n-t}.$$

Definición 3.13. Definimos $A_w(T) \in \mathbb{Z}[T]$ como

$$A_w(T) = \begin{cases} 1 & \text{si } w = 0 \\ \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) & \text{si } 0 < w \leq n. \end{cases}$$

Observación 3.8. Nótese que la definición de $A_0(T)$ no es un caso particular de la forma general dada para todos los enteros mayores que 0 y menores o iguales que n, ya que para $w = 0$ tenemos que $\sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) = (-1)^{2n} \binom{n}{n} B_n(T) = B_n(T) = \sum_{|J|=n} B_J(T) = B_{[n]}(T) = T^{l[n]-1} = T^0 - 1 = 1 - 1 = 0$, ya que $l([n]) = \dim\{c \in C \mid \forall j \in [n] : c_j = 0\} = \dim\{0\} = 0$. Entonces $\sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) \neq A_0(T)$.

Observación 3.9. Si $0 < w < d$ y $t \geq n - w$ entonces $t > n - d$ y por el Teorema 3.7 tenemos $B_t(T) = 0$. Entonces $A_w(T) = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} 0 = 0$. Esto es, $A_w(T) =$ para $0 < w < d$.

Observación 3.10. Por el Teorema 3.7, para todo $t > n - d$, $B_t(T) = 0$, entonces si $0 < w \leq n$, podemos definir $A_w(T)$ como $A_w(T) = \sum_{t=n-w}^{\mathbf{n-d}} (-1)^{n+w+t} \binom{t}{n-w} B_t(T)$.

La Definición 3.13 se estableció con la finalidad de escribir el enumerador de pesos extendido de un código de manera semejante al enumerador de pesos homogéneo y al r-ésimo enumerador de pesos generalizado de un código. Esto se establece en el siguiente teorema.

Teorema 3.8. *Una forma equivalente de escribir el enumerador de pesos extendido de un código lineal C es:*

$$W_C(X, Y, T) = \sum_{w=0}^{n} A_w(T) X^{n-w} Y^w.$$

Demostración.

Por el Teorema del Binomio, tomando $w = n - t + j$ y teniendo en cuenta que si $j > i$, $\binom{i}{j} = 0$ se verifican las siguientes igualdades:

$$\begin{aligned}
W_C(X, Y, T) &= X^n + \sum_{t=0}^{n} B_t(T)(X - Y)^t Y^{n-t} = X^n + \sum_{t=0}^{n} B_t(T) \left[\sum_{j=0}^{t} (-1)^j \binom{t}{j} X^{t-j} Y^j \right] Y^{n-t} \\
&= X^n + \sum_{t=0}^{n} \sum_{j=0}^{t} (-1)^j \binom{t}{j} B_t(T) X^{t-j} Y^{n-t+j} \\
&= X^n + \sum_{t=0}^{n} \sum_{w=n-t}^{n} (-1)^{t-n+w} \binom{t}{t-n+w} B_t(T) X^{n-w} Y^w \\
&= X^n + \sum_{t=0}^{n} \sum_{w=n-t}^{n} (-1)^{n+w+t} \binom{t}{t-(n-w)} B_t(T) X^{n-w} Y^w \\
&= X^n + \sum_{t=0}^{n} \sum_{w=n-t}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) X^{n-w} Y^w \\
&= X^n + \sum_{t=0}^{n} \sum_{w=0}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) X^{n-w} Y^w \\
&= X^n + \sum_{w=0}^{n} \sum_{t=0}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) X^{n-w} Y^w \\
&= X^n + \sum_{w=0}^{n} \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) X^{n-w} Y^w
\end{aligned} \tag{3.1}$$

Por otro lado, tenemos que

$$\begin{aligned}
\sum_{w=0}^{n} A_w(T) X^{n-w} Y^w &= A_0(T) X^n + \sum_{w=1}^{n} A_w(T) X^{n-w} Y^w \\
&= X^n + \sum_{w=1}^{n} \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) X^{n-w} Y^w \\
&= X^n + \sum_{w=0}^{n} \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) X^{n-w} Y^w
\end{aligned} \tag{3.2}$$

La última igualdad es válida por la Observación 3.8. De (3.1) y (3.2) obtenemos la igualdad buscada.

□

Los polinomios $A_w(T)$ se definieron a partir de los polinomios $B_t(T)$. Ahora se desea establecer la relación inversa, es decir, la manera en la que pueden hallarse los polinomios $B_t(T)$ a partir de los polinomios $A_w(T)$. Para ello se empleará el siguiente lema.

Lema 3.3. *Sea V un espacio vectorial de dimensión $n+1$ y sean $a = (a_0, a_1, \ldots, a_n)$ y $b = (b_0, b_1, \ldots, b_n)$ vectores en V. Las siguientes afirmaciones son equivalentes:*

(1) Para cada $j \in [n]$, $a_j = \sum_{i=0}^{n} \binom{i}{j} b_i$.

(2) Para cada $j \in [n]$, $b_j = \sum_{i=j}^{n} (-1)^{i+j} \binom{i}{j} a_i$.

Demostración.

Consideremos las matrices

$$A = \left[(-1)^{i+j}\binom{i}{j}\right]_{i,j=0,1,\ldots,n} = \begin{bmatrix} (-1)^{0+0}\binom{0}{0} & (-1)^{0+1}\binom{0}{1} & \cdots & (-1)^{0+n}\binom{0}{n} \\ (-1)^{1+0}\binom{1}{0} & (-1)^{1+1}\binom{1}{1} & \cdots & (-1)^{1+n}\binom{1}{n} \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^{n+0}\binom{n}{0} & (-1)^{n+1}\binom{n}{1} & \cdots & (-1)^{n+n}\binom{n}{n} \end{bmatrix}$$

y

$$B = \left[\binom{i}{j}\right]_{i,j=0,1,\ldots,n} = \begin{bmatrix} \binom{0}{0} & \binom{0}{1} & \cdots & \binom{0}{n} \\ \binom{1}{0} & \binom{1}{1} & \cdots & \binom{1}{n} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{n}{0} & \binom{n}{1} & \cdots & \binom{n}{n} \end{bmatrix}.$$

Notamos que (1) es equivalente a decir que $a = bB$, mientras que (2) es decir que $b = aA$. De esta forma, podemos ver las relaciones entre a y b como transformaciones lineales. Entonces si suponemos (1) y demostramos que la inversa de la matriz de la transformación B es la matriz A, como consecuencia inmediata tenemos (2), y viceversa. Así, pues, veamos que $BA = I_{(n+1)\times(n+1)}$.

Sea $C = BA$. Emplearemos los siguientes resultados en el desarrollo de (3.3): para $l > i$, $\binom{i}{l} = 0$; si $l < j$, $\binom{l}{j} = 0$; $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$.

$$\begin{aligned} c_{ij} &= \sum_{l=0}^{n} \binom{i}{l}(-1)^{l+j}\binom{l}{j} = \sum_{l=j}^{i}(-1)^{j+l-2j}\binom{i}{l}\binom{l}{j} = \sum_{l=j}^{i}(-1)^{l-j}\binom{i}{j}\binom{i-j}{l-j} \\ &= \sum_{k=0}^{i-j}(-1)^{k}\binom{i}{j}\binom{i-j}{k} = \binom{i}{j}\sum_{k=0}^{i-j}\binom{i-j}{k}(-1)^{k} \end{aligned} \tag{3.3}$$

Aquí tenemos dos casos: si $i = j$, entonces por (3.3), tenemos que $c_{ij} = 1$, mientras que si $i \neq j$, por (3.3) y por el Teorema del Binomio, $c_{ij} = \binom{i}{j}(1-1)^{i-j} = 0$. En resumen, $c_i j = \delta_{ij}$, donde δ_{ij} es la delta de Kronecker. Entonces las entradas de la matriz BA son las mismas de la matriz $I_{(n+1)\times(n+1)}$. De aquí tenemos que A y B son matrices inversas una de la otra. □

Teorema 3.9. *La siguiente igualdad es válida:*

$$B_t(T) = \sum_{w=d}^{n-t} \binom{n-w}{t} A_w(T).$$

Demostración.

Para poder aplicar el Lema 3.3 en esta ocasión tomamos A_w como en la Definición 3.13 para $0 < w \leq n$, que por la Observación 3.8 es igual a 0. Entonces, para para $w \in \{0, 1 \ldots, n\}$ tenemos que $A_w(T) = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T) = \sum_{t=n-w}^{n} (-1)^{t+(n-w)} \binom{t}{n-w} B_t(T)$. Renombramos a $A_w(T)$ como C_{n-w}, y hacemos el cambio de variable $r = n - w$. Entonces, para cada entero r tal que $0 \leq r \leq n$ tenemos que

$$C_r = \sum_{t=r}^{n} (-1)^{t+r} \binom{t}{r} B_t(T).$$

Así que aplicando directamente el Lema 3.3 tenemos lo siguiente:

$$B_t(T) = \sum_{i=0}^{n} \binom{i}{t} C_i = \sum_{w=0}^{n} \binom{n-w}{t} C_{n-w} = \sum_{w=0}^{n} \binom{n-w}{t} A_w(T) = \sum_{w=d}^{n-t} \binom{n-w}{t} A_w(T) \tag{3.4}$$

La última igualdad es cierta por las Observaciones 3.8 y 3.9 y dado que si $w > n - t$, entonces $\binom{n-w}{t} = 0$. De (3.4) tenemos el resultado. □

Al inicio de este apartado se definió el código de extensión de un código lineal. Es natural preguntarse si existe alguna relación entre los enumeradores de pesos de ambos códigos. La respuesta es que sí. Resulta que el enumerador de pesos homogéneo del código de extensión es igual al enumerador de pesos extendido del código original tomando $T = q^m$. Este resultado es de gran importancia pues afirma que la distribución de pesos del código de extensión puede conocerse simplemente con información del código original.

Teorema 3.10. *Sea C un $[n, k]$-código lineal. Entonces:*

$$W_{C \otimes \mathbb{F}_{q^m}}(X, Y) = W_C(X, Y, q^m).$$

Demostración.

Por definición $W_{C \otimes \mathbb{F}_{q^m}}(X, Y) = \sum_{w=0}^{n} A_{C \otimes \mathbb{F}_{q^m}, w} X^{n-w} Y^w$, y por el Teorema 3.8, tenemos que $W_C(X, Y, q^m) = \sum_{w=0}^{n} A_w(q^m) X^{n-w} Y^w$. Entonces es suficiente que comprobemos que para cada $w \in \{0, 1, \ldots, n\}$, $A_{C \otimes \mathbb{F}_{q^m}, w} = A_w(q^m)$. Si $w = 0$, entonces $A_{C \otimes \mathbb{F}_{q^m}, w} = 1$. Además, por definición $A_w(q^m) = 1$. En este caso tenemos la igualdad esperada. Por otro lado, si $w \neq 0$, por la Observación 3.4, $A_{C \otimes \mathbb{F}_{q^m}, w} = (q^m - 1) A^1_{C \otimes \mathbb{F}_{q^m}, w}$. Queremos probar entonces que $A_w(q^m) = (q^m - 1) A^1_{C \otimes \mathbb{F}_{q^m}, w}$. Tomando en cuenta que el número de palabras-código que son distintas de 0 en un subcódigo de

dimensión 1 es igual a $q^m - 1$ y por las Observaciones 3.6 y 3.7, tenemos lo siguiente:

$$\begin{aligned} B_t(q^m) &= \sum_{|J|=t} B_J(q^m) = \sum_{|J|=t} |\{c \in (C \otimes \mathbb{F}_{q^m})(J) : c \neq 0\}| \\ &= (q^m - 1) \sum_{|J|=t} |\{D \subseteq (C \otimes F_{q^m})(J) : \dim D = 1\}| \\ &= (q^m - 1) \sum_{|J|=t} B_J^1 = (q^m - 1) B_t^1 = (q^m - 1) \sum_{w=0}^{n-t} \binom{n-w}{t} A^1_{C \otimes \mathbb{F}_{q^m}, w} \end{aligned} \tag{3.5}$$

Entonces, por (3.5) y por el Teorema 3.9, tenemos que $\sum_{w=0}^{n-t} \binom{n-w}{t} A_w(q^m) = \sum_{w=0}^{n-t} \binom{n-w}{t} (q^m - 1) A^1_{C \otimes \mathbb{F}_{q^m}, w}$. De aquí que $A_w(q^m) = (q^m - 1) A^1_{C \otimes \mathbb{F}_{q^m}, w}$. □

Observación 3.11. Por los Teoremas 3.8 y 3.10, $A_w(q^m)$ es el número de palabras-código de peso w en el código de extensión $C \otimes \mathbb{F}_{q^m}$.

Para finalizar este apartado se proporciona una equivalencia más al enumerador de pesos extendido de un código que se empleará un poco más adelante.

Teorema 3.11. *El enumerador de pesos extendido de un código lineal C puede escribirse como*

$$W_C(X, Y, T) = \sum_{t=0}^{n} \sum_{|J|=t} T^{l(J)} (X - Y)^t Y^{n-t}.$$

Demostración.

$$\begin{aligned} W_C(X, Y, T) &= \sum_{t=0}^{n} B_t(T)(X - Y)^t Y^{n-t} + X^n = \sum_{t=0}^{n} B_t(T)(X - Y)^t Y^{n-t} + [(X - Y) + Y]^n \\ &= \sum_{t=0}^{n} B_t(T)(X - Y)^t Y^{n-t} + \sum_{t=0}^{n} \binom{n}{t} (X - Y)^t Y^{n-t} \\ &= \sum_{t=0}^{n} [(X - Y)^t Y^{n-t}] \left(B_t(T) + \binom{n}{t} \right) = \sum_{t=0}^{n} [(X - Y)^t Y^{n-t}] \left(\sum_{|J|=t} B_J(T) + \binom{n}{t} \right) \\ &= \sum_{t=0}^{n} [(X - Y)^t Y^{n-t}] \left(\sum_{|J|=t} (T^{l(J)} - 1) + \binom{n}{t} \right) \\ &= \sum_{t=0}^{n} [(X - Y)^t Y^{n-t}] \left(\sum_{|J|=t} [(T^{l(J)} - 1) + 1] \right) = \sum_{t=0}^{n} [(X - Y)^t Y^{n-t}] \sum_{|J|=t} T^{l(J)} \\ &= \sum_{t=0}^{n} \sum_{|J|=t} T^{l(J)} (X - Y)^t Y^{n-t} \end{aligned} \tag{3.6}$$

De (3.6) tenemos la igualdad esperada. □

3.4. Relación entre los enumeradores de pesos

En las secciones anteriores se definieron los enumeradores de pesos homogéneo, extendido y generalizado. Se establecieron y demostraron algunas identidades que relacionaban a cada uno de ellos con otros polinomios. En esta sección se establece la conexión entre ellos.

La primera relación que se muestra es entre la distribución de pesos de un código de extensión y las distribuciones de pesos generalizadas del código. Afirma que el número de palabras-código de peso w en el código de extensión puede conocerse a partir de los subcódigos de peso w. Para establecer esta relación se requieren algunos lemas que se mencionan a continuación.

Lema 3.4. *([2]) Sea C un $[n, k]$-código lineal, y sea C^m el subespacio lineal de todas las matrices de tamaño $m \times n$ sobre $\mathbb{F}_q$ cuyas filas son palabras-código de C. Entonces existe un isomorfismo de $\mathbb{F}_q$-espacios vectoriales entre $C \otimes \mathbb{F}_{q^m}$ y C^m.*

Lema 3.5. *Sea c un elemento del código de extensión $C \otimes \mathbb{F}_{q^m}$ y M la matriz de C^m correspondiente bajo el isomorfismo dado en el Lema 3.4. Sea $D \subseteq C$ el código generado por las filas de M. Entonces $wt(c) = wt(D)$.*

Demostración.

Veamos que $\{j \in [n] \mid c_j = 0\} = \{j \in [n] \mid \forall x \in D : x_j = 0\}$, es decir, que $supp(c)^C = supp(D)^C$.

Supongamos que $i \in \{j \in [n] \mid c_j = 0\}$, es decir, que $c_i = 0$. Entonces la j-ésima columna de la matriz M consta sólo de ceros, ya que tal columna es la representación en la base $(1, \alpha, \alpha^2, \ldots, \alpha^{m-1})$ del elemento c_i y dicha representación es única. Entonces todas las filas de M, que son palabras-código de C, tienen i-ésima cooordenada igual a 0, de manera que cualquier palabra-código que sea $\mathbb{F}_q$-combinación lineal de dichas palabras-código tendrá también i-ésima componente igual a 0, esto es, todo elemento x de D satisface que $x_i = 0$. Por lo tanto, $i \in \{j \in [n] \mid \forall x \in D : x_j = 0\}$. Ahora tomemos $i \in \{j \in [n] \mid \forall x \in D : x_j = 0\}$. Entonces toda palabra-código en D tiene i-ésima coordenada igual a 0. Supongamos que existe una fila de M tal que su i-ésima componente es distinta de 0, digamos $(c_{k1}, c_{k2}, \ldots, c_{kn})$, con $c_{ki} \neq 0$. Sea $\lambda \in \mathbb{F}_q \setminus \{0\}$. Como D es el subespacio generado por las filas de M, $\lambda(c_{k1}, c_{k2}, \ldots, c_{kn})$ es una palabra-código de D, con i-ésima coordenada distinta de 0, lo cual es una contradicción. Por lo tanto todas las filas de M tienen i-ésima componente igual a 0 y por consiguiente $c_i = 0$.

Concluimos pues que $\{j \in [n] \mid c_j \neq 0\} = \{j \in [n] \mid \exists x \in D : x_j \neq 0\}$, de donde $wt(c) = wt(D)$. □

Teorema 3.12. *Sea C un código lineal. Se cumple que:*

$$A_w(q^m) = \sum_{r=0}^{m} [m, r]_q A_w^{(r)}.$$

Demostración.

Fijemos un peso w y una dimensión r. En la Observación 3.11 notamos que $A_w(q^m)$ es igual al número de palabras-código de peso w en $C \otimes \mathbb{F}_{q^m}$. Ahora, por el Lema 3.5 cada matriz $M \in C^m$ genera un subcódigo de C con el mismo peso que su palabra-código de $C \otimes \mathbb{F}_{q^m}$ correspondiente bajo el isomorfismo del Lema 3.4. $A_w^{(r)}$ denota el número de subcódigos de C de dimensión r y de peso w. Sea D uno de tales subcódigos. Por ser de dimensión r, D es generado por una matriz B de tamaño $r \times n$ cuyas filas son palabras de C. Si multiplicamos B a la izquierda por una matriz A de tamaño $m \times r$ y de rango r obtenemos una matriz AB de C^m que genera el mismo subcódigo que B y todos los elementos de C^m se obtienen de esta forma. El número de matrices de tamaño $m \times r$ y de rango r es $[m, r]_q$, entonces considerando todas las dimensiones de subcódigos tenemos que

$$A_w(q^m) = \sum_{r=0}^{k} [m, r]_q A_w^{(r)}.$$

La igualdad enunciada se consigue notando que para $r > k$, $A_w^{(r)} = 0$. □

Para continuar con las equivalencias se hará uso del siguiente resultado.

Teorema 3.13 (Interpolación de Lagrange)**.** *Sean $x_1, x_2, \ldots, x_{k+1}$ números distintos y sea $f(x)$ una función definida en un dominio al cual pertenecen tales números. Entonces el polinomio*

$$L(x) = \sum_{j=1}^{k+1} f(x_j) L_j(x)$$

es el único polinomio de grado a lo más k que satisface que para cada $j \in \{1, 2, \ldots, k+1\}$, $L(x_j) = f(x_j)$, donde los polinomios $\{L_j\}$, $j \in \{1, 2, \ldots, k+1\}$ se llaman Polinomios de Lagrange para los puntos de interpolación $x_1, x_2, \ldots, x_{k+1}$ y se definen como

$$L_j(x) = \prod_{\substack{i=1 \\ i \neq j}}^{k+1} \frac{x - x_i}{x_j - x_i}.$$

Una demostración del Teorema 3.13 para el campo $\mathbb{Z}_p$ puede consultarse en [5].

A continuación se menciona otra relación que es incluso más explícita a la dada en el Teorema 3.12, pues no sólo enlaza las distribuciones de pesos, sino que proporciona una manera de encontrar el enumerador de pesos extendido de un código conociendo los enumeradores de pesos generalizados de dicho código.

Teorema 3.14. *Sea C un código lineal. Es cierto que:*

$$W_C(X, Y, T) = \sum_{r=0}^{k} \left(\prod_{j=0}^{r-1} (T - q^j) \right) W_C^{(r)}(X, Y).$$

Demostración.

Supongamos que tenemos $k+1$ valores de m para los cuales conocemos su correspondiente valor de $A_w(q^m)$. Si $0 < w \leq n$, $A_w(T)$ por definición es igual a $\sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T)$, es decir, $A_w(T)$ es una suma de los polinomios $B_t(T)$, los cuales son a su vez sumas de polinomios en los cuales tenemos exponentes que son dimensiones de algunos subcódigos de C y por ende no pueden exceder a k. Entonces siempre tenemos que $A_w(T)$ es un polinomio de grado a lo más k. Se cumplen las hipótesis del Teorema de Lagrange, con $f(T) = A_w(T)$. Dicho teorema afirma que existe un único polinomio de grado a lo más k que satisface que el valor del polinomio en cada uno de los $k+1$ puntos conocidos es igual al valor de la función original en dicho punto. Pero justamente el polinomio $A_w(T)$ tiene esas características. Entonces $A_w(T)$ es el Polinomio de Lagrange.

Por otro lado, por el Teorema 3.12 tenemos que

$$A_w(q^m) = \sum_{r=0}^{m} \left[\prod_{i=0}^{r-1} (q^m - q^i) \right] A_w^{(r)} \tag{3.7}$$

entonces el polinomio de grado k

$$\sum_{r=0}^{m} \left[\prod_{i=0}^{r-1} (T - q^i) \right] A_w^{(r)} = \sum_{r=0}^{k} \left[\prod_{i=0}^{r-1} (T - q^i) \right] A_w^{(r)}$$

también satisface que al evaluarlos en cada uno los $k+1$ valores de q^m obtenemos la igualdad dada en (3.7). Entonces por la unicidad que se afirma en el Teorema de Interpolación de Lagrange tenemos que

$$A_w(T) = \sum_{r=0}^{k} \left[\prod_{i=0}^{r-1} (T - q^i) \right] A_w^{(r)}.$$

Finalmente por el Teorema 3.8 tenemos lo siguiente:

$$\begin{aligned} W_C(X, Y, T) &= \sum_{w=0}^{n} A_w(T) X^{n-w} Y^w = \sum_{w=0}^{n} \left(\sum_{r=0}^{k} \left[\prod_{i=0}^{r-1} (T - q^i) \right] A_w^{(r)} \right) X^{n-w} Y^w \\ &= \sum_{r=0}^{k} \left[\prod_{i=0}^{r-1} (T - q^i) \right] \sum_{w=0}^{n} A_w^{(r)} X^{n-w} Y^w = \sum_{r=0}^{k} \left[\prod_{i=0}^{r-1} (T - q^i) \right] W_C^{(r)}(X, Y) \end{aligned} \tag{3.8}$$

En la ecuación (3.8) se establece la igualdad mencionada en el teorema. □

Recíprocamente, puede conocerse cada uno de los enumeradores de pesos generalizados si se conoce el enumerador de pesos extendido de un código. Primero se menciona una igualdad que será útil en la demostración de tal resultado.

Lema 3.6. *([3])*

$$\prod_{i=0}^{j-1}(x-q^i)=\sum_{i=0}^{j}\begin{bmatrix} j \\ i \end{bmatrix}_q (-1)^{j-i}q^{\binom{j-i}{2}}x^i.$$

Teorema 3.15. *Sea C un código lineal. La siguiente igualdad es válida:*

$$W_C^{(r)}(X,Y)=\frac{1}{\langle r\rangle_q}\sum_{j=0}^{r}\begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j}q^{\binom{r-j}{2}}W_C(X,Y,q^j).$$

Demostración.

Por el Lema 3.6, los Teoremas 3.6 y 3.11 y la Observación 3.5 se verifican las siguientes igualdades:

$$\begin{aligned}
W_C^{(r)}(X,Y)&=\sum_{t=0}^{n}B_t^{(r)}(X-Y)^tY^{n-t}=\sum_{t=0}^{n}\left(\sum_{|J|=t}B_J^{(r)}\right)(X-Y)^tY^{n-t}\\
&=\sum_{t=0}^{n}\sum_{|J|=t}\begin{bmatrix} l(J) \\ r \end{bmatrix}_q(X-Y)^tY^{n-t}=\sum_{t=0}^{n}\sum_{|J|=t}\left(\frac{\prod_{j=0}^{r-1}(q^{l(J)}-q^j)}{\prod_{j=0}^{r-1}(q^r-q^j)}\right)(X-Y)^tY^{n-t}\\
&=\frac{1}{\prod_{j=0}^{r-1}(q^r-q^j)}\sum_{t=0}^{n}\sum_{|J|=t}\left(\prod_{j=0}^{r-1}(q^{l(J)}-q^j)\right)(X-Y)^tY^{n-t}\\
&=\frac{1}{\langle r\rangle_q}\sum_{t=0}^{n}\sum_{|J|=t}\left(\sum_{j=0}^{r}\begin{bmatrix} r \\ j \end{bmatrix}_q(-1)^{r-j}q^{\binom{r-j}{2}}q^{l(J)\cdot j}\right)(X-Y)^tY^{n-t}\\
&=\frac{1}{\langle r\rangle_q}\sum_{j=0}^{r}\begin{bmatrix} r \\ j \end{bmatrix}_q(-1)^{r-j}q^{\binom{r-j}{2}}\sum_{t=0}^{n}\sum_{|J|=t}(q^j)^{l(J)}(X-Y)^tY^{n-t}\\
&=\frac{1}{\langle r\rangle_q}\sum_{j=0}^{r}\begin{bmatrix} r \\ j \end{bmatrix}_q(-1)^{r-j}q^{\binom{r-j}{2}}W_C(X,Y,q^j)
\end{aligned}$$

□

Capítulo 4

El enumerador de pesos y el polinomio de Tutte

Como se ha mencionado anteriormente, la Identidad de MacWilliams es un importante resultado en teoría de códigos lineales. Si se conoce el enumerador de pesos de un código, esta identidad permite conocer el enumerador de pesos de su código dual de manera sencilla. Este resultado es de gran ayuda, pues no es fácil hallar el enumerador de pesos de algunos códigos.

El objetivo de este capítulo es emplear los conceptos y algunos resultados del Capítulo 2 de matroides y la teoría acerca de los polinomios enumeradores de pesos estudiada en el Capítulo 3 para proporcionar la demostración de la Identidad de MacWilliams para los enumeradores de pesos extendido de un código y su dual. El contenido se basa principalmente en [2].

Definición 4.1. Sea $M = (E, \mathcal{I})$ un matroide. La *función generadora de rango de Whitney* para M se define como

$$R_M(X, Y) = \sum_{J \subseteq E} X^{r(E)-r(J)} Y^{|J|-r(J)}.$$

El *Polinomio de Tutte*, también llamado *Polinomio de Tutte-Whitney*, para M es

$$t_M(X, Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)} (Y-1)^{|J|-r(J)}.$$

Observación 4.1. Nótese que la función generadora de rango de Whitney y el Polinomio de Tutte se encuentran ligados mediante la siguiente relación:

$$t_M(X, Y) = R_M(X-1, Y-1).$$

Como se vio en el Capítulo 2 a partir de alguna matriz generadora de un $[n, k]$-código lineal C sobre $\mathbb{F}_q$ se obtiene un matroide vector denotado por M_C. Por ello tiene sentido enunciar el siguiente teorema.

Teorema 4.1. *Sea C un $[n, k]$-código lineal. El Polinomio de Tutte asociado con el matroide M_C del código C es*

$$t_{M_C}(X, Y) = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)}.$$

Demostración.

Por definición, $r(E)$ es la cardinalidad de un subconjunto independiente maximal de E, siendo E el conjunto $[n]$; $\mathcal{I}$ es la familia de subconjuntos I de $[n]$ tales que las columnas etiquetadas por I de una matriz generadora G del código lineal C son linealmente independientes. Como C es de dimensión k, entonces G tiene rango k, esto es, el número máximo de columnas linealmente independientes de G es k. Por lo tanto, $r(E) = k$. Además por el Lema 3.1 tenemos que $l(J) = k - r(J)$, y por tanto:

$$\begin{aligned} t_{M_C}(X, Y) &= \sum_{J \subseteq E} (X-1)^{r(E)-r(J)} (Y-1)^{|J|-r(J)} = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{k-r(J)} (Y-1)^{t-r(J)} \\ &= \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{t-k+l(J)} = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)} \end{aligned}$$

□

Al observar los polinomios definidos para un código en el Capítulo 3 y el Polinomio de Tutte del matroide asociado a un código que se estableció en el Teorema 4.1 surge la duda de si estos polinomios están relacionados de alguna forma pues parecieran tener algunas similitudes. El siguiente teorema da la respuesta.

Teorema 4.2. *Sea C un $[n, k]$-código lineal. Existe la siguiente relación entre el enumerador de pesos extendido del código C y el Polinomio de Tutte del matroide asociado a C:*

$$W_C(X, Y, T) = (X-Y)^k Y^{n-k} t_{M_C}\left(\frac{X + (T-1)Y}{X-Y}, \frac{X}{Y}\right).$$

Demostración.

Por el Teorema 4.1 tenemos lo siguiente:

$$\begin{aligned} &(X-Y)^k Y^{n-k} t_{M_C}\left(\frac{X + (T-1)Y}{X-Y}, \frac{X}{Y}\right) \\ &= (X-Y)^k Y^{n-k} \sum_{t=0}^{n} \sum_{|J|=t} \left(\frac{X + (T-1)Y}{X-Y} - 1\right)^{l(J)} \left(\frac{X}{Y} - 1\right)^{l(J)-(k-t)} \\ &= (X-Y)^k Y^{n-k} \sum_{t=0}^{n} \sum_{|J|=t} \left(\frac{TY}{X-Y}\right)^{l(J)} \left(\frac{X-Y}{Y}\right)^{l(J)-(k-t)} \\ &= (X-Y)^k Y^{n-k} \sum_{t=0}^{n} \sum_{|J|=t} T^{l(J)} Y^{k-t} (X-Y)^{-(k-t)} \end{aligned}$$

$$= \sum_{t=0}^{n} \sum_{|J|=t} T^{l(J)}(X-Y)^t Y^{n-t} = W_C(X, Y, T)$$

La última igualdad es cierta por el Teorema 3.11. □

El Teorema 4.2 enuncia la manera en la cual puede expresarse el enumerador de pesos extendido de un código C en términos del Polinomio de Tutte del matroide M_C. En el siguiente teorema se encuentra la relación inversa, es decir, cómo puede hallarse el Polinomio de Tutte del matroide asociado a un código cuando se conoce el enumerador de pesos extendido de dicho código.

Teorema 4.3. *Sea C un $[n, k]$-código. El Polinomio de Tutte de M_C y el enumerador de pesos extendido de C satisfacen la siguiente relación:*

$$t_{M_C}(X, Y) = Y^n(Y-1)^{-k} W_C(1, Y^{-1}, (X-1)(Y-1)).$$

Demostración.

Por el Teorema 3.11 se cumple que:

$$\begin{aligned}
&Y^n(Y-1)^{-k} W_C(1, Y^{-1}, (X-1)(Y-1)) \\
&= Y^n(Y-1)^{-k} \sum_{t=0}^{n} \sum_{|J|=t} ((X-1)(Y-1))^{l(J)} (1-Y^{-1})^t Y^{-(n-t)} \\
&= Y^n(Y-1)^{-k} \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)} \left(\frac{Y-1}{Y}\right)^t Y^{-(n-t)} \\
&= \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)} (Y-1)^t Y^{-t} Y^{-(n-t)} Y^n (Y-1)^{-k} \\
&= \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)} = t_{M_C}(X, Y)
\end{aligned}$$

La última igualdad se verifica por el Teorema 4.1. □

A continuación se establecen las relaciones existentes entre los enumeradores de pesos generalizados del código y el polinomio de Tutte del matroide asociado al código.

Teorema 4.4.

$$W_C^{(r)}(X, Y) = \frac{1}{\langle r \rangle_q} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} (X-Y)^k Y^{n-k} t_{M_C}\left(\frac{X + (q^j-1)Y}{X-Y}, \frac{X}{Y}\right).$$

Demostración.

Por el Teorema 3.15, tenemos que

$$W_C^{(r)}(X,Y) = \frac{1}{\langle r \rangle_q} \sum_{j=0}^{r} \begin{bmatrix} r \\ j \end{bmatrix}_q (-1)^{r-j} q^{\binom{r-j}{2}} W_C(X,Y,q^j)$$

y por el Teorema 4.2, $W_C(X,Y,q^j) = (X-Y)^k Y^{n-k} t_{M_C}\left(\frac{X+(q^j-1)Y}{X-Y}, \frac{X}{Y}\right)$. Combinando estos resultados se obtiene la igualdad deseada. □

Teorema 4.5.

$$t_{M_C}(X,Y) = Y^n (Y-1)^{-k} \sum_{r=0}^{k} \left(\prod_{j=0}^{r-1} \left((X-1)(Y-1) - q^j \right) \right) W_C^{(r)}(1, Y^{-1}).$$

Demostración.

Por el Teorema 4.3, tenemos que

$$t_{M_C}(X,Y) = Y^n (Y-1)^{-k} W_C\left(1, Y^{-1}, (X-1)(Y-1)\right)$$

y por el Teorema 3.14,

$$W_C\left(1, Y^{-1}, (X-1)(Y-1)\right) = \sum_{r=0}^{k} \left(\prod_{j=0}^{r-1} \left((X-1)(Y-1) - q^j \right) \right) W_C^{r}(1, Y^{-1}).$$

Con estos resultados queda probado el teorema. □

El siguiente teorema enuncia la relación existente entre el polinomio de Tutte de un matroide y el polinomio de Tutte de su matroide dual, específicamente, que dado el polinomio del matroide dual, para hallar el polinomio del matroide basta con intercambiar las variables en la evaluación de dicho polinomio.

Teorema 4.6. *Sea M un matroide. Se cumple que:*

$$t_M(X,Y) = t_{M^\perp}(Y,X).$$

Demostración.

M es un matroide sobre el conjunto E. Por definición, $M^\perp$ también es un matroide sobre E. Por el Teorema 2.17, se cumple que $r^\perp(J) = |J| - r(E) + r(E \setminus J)$, en particular para el conjunto E tenemos que $r^\perp(E) = |E| - r(E) + r(E \setminus E) = |E| - r(E)$, así que $r^\perp(E) - r^\perp(J) = |E| - r(E) - \left(|J| - r(E) + r(E \setminus J)\right) =$

$|E| - |J| - r(E \setminus J) = |E \setminus J| - r(E \setminus J)$. Luego, por definición tenemos que

$$\begin{aligned} t_{M^\perp}(Y, X) &= \sum_{J \subseteq E} (Y-1)^{r^\perp(E)-r^\perp(J)}(X-1)^{|J|-r^\perp(J)} = \sum_{J \subseteq E} (Y-1)^{|E\setminus J|-r(E\setminus J)}(X-1)^{r(E)-r(E\setminus J)} \\ &= \sum_{J \subseteq E} (X-1)^{r(E)-r(E\setminus J)}(Y-1)^{|E\setminus J|-r(E\setminus J)} = \sum_{K \subseteq E} (X-1)^{r(E)-r(K)}(Y-1)^{|K|-r(K)} = t_M(X, Y). \end{aligned}$$

□

4.1. La Identidad de MacWilliams

La Identidad de MacWilliams afirma que el enumerador de pesos extendido de un código y el de su dual pueden conocerse uno a partir de otro mediante una sencilla fórmula. A continuación se presenta su demostración empleando resultados previos.

Teorema 4.7 (MacWilliams). *Sea C un código. La siguiente igualdad es válida:*

$$W_{C^\perp}(X, Y, T) = T^{-k} W_C\Big(X + (T-1)Y, X - Y, T\Big).$$

Demostración.

Empleando el resultado del Teorema 2.16 se tiene que:

$$\begin{aligned} & T^{-k} W_C\left(X + (T-1)Y, X - Y, T\right) \\ &= T^{-k}(TY)^k (X-Y)^{n-k} t_{M_C}\left(\frac{X + (T-1)Y + (T-1)(X-Y)}{TY}, \frac{X + (T-1)Y}{X-Y}\right) \\ &= Y^k (X-Y)^{n-k} t_{M_C}\left(\frac{X}{Y}, \frac{X + (T-1)Y}{X-Y}\right) = Y^k (X-Y)^{n-k} t_{M_{C^\perp}}\left(\frac{X + (T-1)Y}{X-Y}, \frac{X}{Y}\right) \\ &= (X-Y)^{n-k} Y^k t_{M_{C^\perp}}\left(\frac{X + (T-1)Y}{X-Y}, \frac{X}{Y}\right) = W_{C^\perp}(X, Y, T) \end{aligned}$$

La última igualdad es válida por el Teorema 4.2 y dado que la dimensión del código dual es $n-k$. □

Pudiera parecer en este momento que la demostración del Teorema 4.7 es bastante simple pues sólo requirió de unas pocas igualdades para establecerse. Con lo que se estudió para poder realizar la prueba en efecto lo es. Sin embargo, ésta no es la manera tradicional en la que se demuestra dicho resultado. Esto se aborda en el siguiente capítulo.

Capítulo 5

La Identidad de MacWilliams

La Identidad de MacWilliams ya se ha enunciado en los Capítulos 3 y 4, y en este último se proporcionó una prueba de dicha identidad empleando el enumerador de pesos extendido de un código y teoría de matroides. El objetivo de este capítulo es enunciar y demostrar esta identidad de la forma tradicional empleando conceptos de caracteres y álgebra de grupo, a fin de que el lector pueda comparar la teoría que está detrás de ambas demostraciones. El contenido de esta sección se extrajo de [6], por lo que el lector puede consultar dicha fuente si desea profundizar en el tema.

5.1. Caracteres

Definición 5.1. Sea $(G, +)$ un grupo y sea $\mathbb{C}_1$ el grupo multiplicativo de los números complejos con módulo igual a 1. Un homomorfismo $\chi\colon G \to \mathbb{C}_1$ se llama *caracter* de G.

El *caracter principal* de G es el caracter ϕ definido por $\phi(g) = 1$ para todo $g \in G$.

Teorema 5.1. *Sean G un grupo y χ un caracter de G. Entonces*

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \text{si } \chi \text{ es principal} \\ 0 & \text{en otro caso} \end{cases}$$

Demostración.

Si χ es el caracter principal, entonces para todo $g \in G$, $\chi(g) = 1$, luego

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} 1 = |G|.$$

Si χ no es el caracter principal, entonces existe $h \in G$ tal que $\chi(h) \neq 1$ y así $\chi(h) - 1 \neq 0$. Dado

que χ es un homomorfismo, tenemos que

$$\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(h)\chi(g)=\sum_{g\in G}\chi(h+g). \tag{5.1}$$

Como G es un grupo, $h+g\in G$. g recorre todo G, entonces $h+g$ toma como valor cada uno de los elementos de G. Así, $\sum_{g\in G}\chi(h+g)=\sum_{g\in G}\chi(g)$, y por (5.1) resulta que $\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(g)$, de donde $\chi(h)\sum_{g\in G}\chi(g)-\sum_{g\in G}\chi(g)=0$, luego $[\chi(h)-1]\sum_{g\in G}\chi(g)=0$, y como el primer factor es distinto de 0 concluimos que $\sum_{g\in G}\chi(g)=0$. □

Sean $\chi\colon \mathbb{F}_q\to\mathbb{C}_1$ un caracter no principal en $(\mathbb{F}_q,+)$, $u\in\mathbb{F}_q^n$ y C un código lineal. Se define la siguiente función en C:

$$\begin{aligned}\chi_u\colon C &\to \mathbb{C}_1\\ c &\to \chi\big(\langle c,u\rangle\big)\end{aligned}$$

En lo sucesivo $\chi\langle c,u\rangle$ denotará a $\chi\big(\langle c,u\rangle\big)$.

Teorema 5.2. *χ_u es un caracter en C.*

Demostración.

Sean $c,d\in C$. Como χ es caracter se cumple que

$$\chi_u(c+d)=\chi\langle c+d,u\rangle=\chi\big(\langle c,u\rangle+\langle d,u\rangle\big)=\chi\langle c,u\rangle\chi\langle d,u\rangle=\chi_u(c)\chi_u(d).$$

Así, χ_u es homomorfismo de grupos. □

También se cumple que $\chi_c(d)=\chi\langle d,c\rangle=\chi\langle c,d\rangle=\chi_d(c)$.

Teorema 5.3. *El caracter $\chi_u\colon C\to\mathbb{C}_1$ es principal si y sólo si $u\in C^\perp$.*

Demostración.

Para la necesidad supongamos que χ_u es principal, entonces para todo $c\in C$, $1=\chi_u(c)=\chi\langle c,u\rangle$. Supongamos que $u\notin C^\perp$. Definimos la siguiente función:

$$\begin{aligned}T\colon C &\to \mathbb{F}_q\\ c &\to \alpha=\langle c,u\rangle\end{aligned}$$

T es una transformación lineal por las propiedades del producto escalar.

Puesto que $\dim\mathbb{F}_q=1$ y que $\operatorname{Im}T$ es un subespacio vectorial de $\mathbb{F}_q$, tenemos que $\dim(\operatorname{Im}T)=0$ o $\dim(\operatorname{Im}T)=1$. Si $\dim(\operatorname{Im}T)=0$, por el teorema del rango se cumple que $\dim C=\dim\ker T$, y dado que $\ker T$ es subespacio de C tenemos que $C=\ker T$, es decir, para todo $c\in C$, $\langle c,u\rangle=0$, de donde $u\in C^\perp$, lo cual es una contradicción. Ahora, si $\dim(\operatorname{Im}T)=1$ entonces $\operatorname{Im}T=\mathbb{F}_q$. Luego T es sobreyectiva. Entonces si $\alpha\in\mathbb{F}_q$, existe $c\in C$ para el cual $\alpha=\langle c,u\rangle$, así $\chi(\alpha)=\chi\langle c,u\rangle=1$,

es decir que para todo $\alpha \in \mathbb{F}_q$, $\chi(\alpha) = 1$, luego χ es principal, lo cual es una contradicción. Por lo tanto, $u \in L^{\perp}$.

Para la suficiencia supongamos que $u \in C^{\perp}$, entonces para todo $c \in C$, $\langle c, u\rangle = 0$, de donde $\chi_u(c) = \chi\langle c, u\rangle = \chi(0) = 1$, ya que χ es un homomorfismo. Concluimos que para todo $c \in C$, $\chi_u(c) = 1$ lo cual implica que χ_u es principal. □

Corolario 5.1. *Sea C un código lineal. Entonces para $u \in \mathbb{F}_q^n$ se tiene que $\sum_{c\in C} \chi_u(c) = |C|\delta_{u\in C^{\perp}}$, donde* $\delta_{u\in C^{\perp}} = \begin{cases} 1 \text{ si } u \in C^{\perp} \\ 0 \text{ si } u \notin C^{\perp} \end{cases}$.

Demostración.

Por los Teoremas 5.1 y 5.3 tenemos que

$$\sum_{c\in L} \chi_u(c) = \begin{cases} |C| & \text{si } \chi_u \text{ es principal} \\ 0 & \text{en otro caso} \end{cases} = \begin{cases} |C| & \text{si } u \in C^{\perp} \\ 0 & \text{si } u \notin C^{\perp} \end{cases} = |C|\delta_{u\in C^{\perp}}.$$

□

5.2. El álgebra de grupo

Definición 5.2. Sea V un espacio vectorial sobre el campo $\mathbb{F}$, donde además de la operación suma de vectores existe una operación binaria

$$\cdot : V \times V \to V$$

llamada *multiplicación de vectores* que cumple las siguientes propiedades para todo $u, v, w \in V$ y para todo $\lambda \in \mathbb{F}$:

(1) $u \cdot (v \cdot w) = (u \cdot v) \cdot w$.

(2) $\exists e \in V \; \forall u \in V : e \cdot u = u = u \cdot e$.

(3) $u \cdot (v + w) = u \cdot v + u \cdot w$.

(4) $(v + w) \cdot u = v \cdot u + w \cdot u$.

(5) $u \cdot (\lambda v) = (\lambda u) \cdot v = \lambda(u \cdot v)$.

En este caso se dice que V es un *álgebra sobre el campo* $\mathbb{F}$. Dicho de otra forma, un álgebra V sobre un campo $\mathbb{F}$ es un anillo con identidad que a la vez es un espacio vectorial sobre $\mathbb{F}$ en el que cual se satisface además que:

$$\forall u, v \in V \; \forall \lambda \in \mathbb{F} : \lambda(u \cdot v) = (\lambda u) \cdot v = u \cdot (\lambda v).$$

Sea t una variable independiente y sea $\mathbb{C}\mathbb{F}_q^n$ el conjunto de todas las sumas formales

$$g = g(t) = \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x$$

donde para todo $x \in \mathbb{F}_q^n$, $\alpha_x \in \mathbb{C}$. Se define la suma entre elementos de $\mathbb{C}\mathbb{F}_q^n$, la multiplicación de elementos de $\mathbb{C}\mathbb{F}_q^n$ por escalares de $\mathbb{C}$ y la multiplicación entre elementos de $\mathbb{C}\mathbb{F}_q^n$ como:

$$\sum_{x \in \mathbb{F}_q^n} a_x t^x + \sum_{x \in \mathbb{F}_q^n} \beta_x t^x = \sum_{x \in \mathbb{F}_q^n} (a_x + \beta_x) t^x$$

$$\beta \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x = \sum_{x \in \mathbb{F}_q^n} (\beta \cdot \alpha_x) t^x$$

$$\Big(\sum_{x \in \mathbb{F}_q^n} \alpha_x t^x \Big) \Big(\sum_{y \in \mathbb{F}_q^n} \beta_y t^y \Big) = \sum_{x,y \in \mathbb{F}_q^n} (\alpha_x \beta_y) t^{x+y} = \sum_{z \in \mathbb{F}_q^n} \Big(\sum_{z=x+y} \alpha_x \beta_y \Big) t^z$$

Teorema 5.4. *$\mathbb{C}\mathbb{F}_q^n$, con las operaciones definidas, es un álgebra sobre el campo complejo $\mathbb{C}$.*

Demostración.

Sean $g_1 = \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x, g_2 = \sum_{x \in \mathbb{F}_q^n} \beta_x t^x, g_3 = \sum_{x \in \mathbb{F}_q^n} \gamma_x t^x$, $\lambda_1, \lambda_2 \in \mathbb{C}$. Las igualdades que se presentan a continuación son válidas por la definición de las operaciones en $\mathbb{C}\mathbb{F}_q^n$ y por las propiedades que satisfacen los elementos del campo complejo $\mathbb{C}$.

$$\begin{aligned} g_1 + g_2 &= \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x + \sum_{x \in \mathbb{F}_q^n} \beta_x t^x = \sum_{x \in \mathbb{F}_q^n} (\alpha_x + \beta_x) t^x = \sum_{x \in \mathbb{F}_q^n} (\beta_x + \alpha_x) t^x \\ &= \sum_{x \in \mathbb{F}_q^n} \beta_x t^x + \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x = g_2 + g_1 \end{aligned}$$

$$\begin{aligned} (g_1 + g_2) + g_3 &= \Big(\sum_{x \in \mathbb{F}_q^n} \alpha_x t^x + \sum_{x \in \mathbb{F}_q^n} \beta_x t^x \Big) + \sum_{x \in \mathbb{F}_q^n} \gamma_x t^x = \sum_{x \in \mathbb{F}_q^n} (\alpha_x + \beta_x) t^x + \sum_{x \in \mathbb{F}_q^n} \gamma_x t^x \\ &= \sum_{x \in \mathbb{F}_q^n} \big[(\alpha_x + \beta_x) + \gamma_x \big] t^x = \sum_{x \in \mathbb{F}_q^n} \big[\alpha_x + (\beta_x + \gamma_x) \big] t^x = \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x + \sum_{x \in \mathbb{F}_q^n} (\beta_x + \gamma_x) t^x \\ &= \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x + \Big(\sum_{x \in \mathbb{F}_q^n} \beta_x t^x + \sum_{x \in \mathbb{F}_q^n} \gamma_x t^x \Big) = g_1 + (g_2 + g_3) \end{aligned}$$

Sea $0 = \sum_{x \in \mathbb{F}_q^n} 0 t^x \in \mathbb{C}\mathbb{F}_q^n$. Entonces

$$g_1 + 0 = \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x + \sum_{x \in \mathbb{F}_q^n} 0 t^x = \sum_{x \in \mathbb{F}_q^n} (\alpha_x + 0) t^x = \sum_{x \in \mathbb{F}_q^n} \alpha_x t^x = g_1$$

Sea $-g_1 = \sum_{x\in\mathbb{F}_q^n}(-\alpha_x)t^x$. Entonces

$$g_1 + (-g_1) = \sum_{x\in\mathbb{F}_q^n}\alpha_x t^x + \sum_{x\in\mathbb{F}_q^n}(-\alpha_x)t^x = \sum_{x\in\mathbb{F}_q^n}\big(\alpha_x + (-\alpha_x)\big)t^x = \sum_{x\in\mathbb{F}_q^n} 0t^x = 0$$

$$\begin{aligned}\lambda_1(g_1+g_2) &= \lambda_1\Big[\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x + \sum_{x\in\mathbb{F}_q^n}\beta_x t^x\Big] = \lambda_1\sum_{x\in\mathbb{F}_q^n}(\alpha_x+\beta_x)t^x = \sum_{x\in\mathbb{F}_q^n}\big[\lambda_1(\alpha_x+\beta_x)\big]t^x\\ &= \sum_{x\in\mathbb{F}_q^n}(\lambda_1\alpha_x + \lambda_1\beta_x)t^x = \sum_{x\in\mathbb{F}_q^n}(\lambda_1\alpha_x)t^x + \sum_{x\in\mathbb{F}_q^n}(\lambda_1\beta_x)t^x\\ &= \lambda_1\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x + \lambda_1\sum_{x\in\mathbb{F}_q^n}\beta_x t^x = \lambda_1 g_1 + \lambda_1 g_2\end{aligned}$$

$$\begin{aligned}(\lambda_1+\lambda_2)g_1 &= (\lambda_1+\lambda_2)\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x = \sum_{x\in\mathbb{F}_q^n}\big[(\lambda_1+\lambda_2)\alpha_x\big]t^x = \sum_{x\in\mathbb{F}_q^n}(\lambda_1\alpha_x+\lambda_2\alpha_x)t^x\\ &= \sum_{x\in\mathbb{F}_q^n}(\lambda_1\alpha_x)t^x + \sum_{x\in\mathbb{F}_q^n}(\lambda_2\alpha_x)t^x = \lambda_1\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x + \lambda_2\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x = \lambda_1 g_1 + \lambda_2 g_1\end{aligned}$$

$$\begin{aligned}\lambda_1(\lambda_2 g_1) &= \lambda_1\Big[\lambda_2\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big] = \lambda_1\Big[\sum_{x\in\mathbb{F}_q^n}(\lambda_2\alpha_x)t^x\Big] = \sum_{x\in\mathbb{F}_q^n}\big[\lambda_1(\lambda_2\alpha_x)\big]t^x\\ &= \sum_{x\in\mathbb{F}_q^n}\big[(\lambda_1\lambda_2)\alpha_x\big]t^x = (\lambda_1\lambda_2)\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x = (\lambda_1\lambda_2)g_1\end{aligned}$$

$$1\cdot g_1 = 1\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x = \sum_{x\in\mathbb{F}_q^n}(1\cdot\alpha_x)t^x = \sum_{x\in\mathbb{F}_q^n}\alpha_x t^x = g_1$$

Hasta este punto se ha demostrado que $\mathbb{C}\mathbb{F}_q^n$ es un espacio vectorial sobre $\mathbb{C}$. La demostración de la asociatividad del producto se omite. $1 = \sum_{x\in\mathbb{F}_q^n} 1_x t^x$ es el elemento neutro con respecto a la multiplicación, donde para todo $x \in \mathbb{F}_q^n$, 1_x es la identidad en $\mathbb{C}$.

Ahora sean $g = \sum_{x\in\mathbb{F}_q^n}\alpha_x t^x$, $h = \sum_{y\in\mathbb{F}_q^n}\beta_y t^y$, $j = \sum_{y\in\mathbb{F}_q^n}\gamma_y t^y$, $\lambda \in \mathbb{C}$. Entonces

$$\begin{aligned}g(h+j) &= \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\beta_y t^y + \sum_{y\in\mathbb{F}_q^n}\gamma_y t^y\Big) = \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}(\beta_y+\gamma_y)t^y\Big)\\ &= \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\alpha_x(\beta_y+\gamma_y)\Big)t^z = \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}(\alpha_x\beta_y+\alpha_x\gamma_y)\Big)t^z\\ &= \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\alpha_x\beta_y + \sum_{z=x+y}\alpha_x\gamma_y\Big)t^z = \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\alpha_x\beta_y\Big)t^z + \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\alpha_x\gamma_y\Big)t^z\\ &= \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\beta_y t^y\Big) + \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\gamma_y t^y\Big) = gh + gj\end{aligned}$$

La demostración de que $(h+j)g = hg + jg$ es completamente análoga. Además:

$$\begin{aligned}\lambda(gh) &= \lambda\Big[\Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\beta_y t^y\Big)\Big] = \lambda\Big[\sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\alpha_x\beta_y\Big)t^z\Big] = \sum_{z\in\mathbb{F}_q^n}\Big(\lambda\sum_{z=x+y}\alpha_x\beta_y\Big)t^z \\ &= \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\lambda(\alpha_x\beta_y)\Big)t^z = \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}(\lambda\alpha_x)\beta_y\Big)t^z = \Big(\sum_{x\in\mathbb{F}_q^n}(\lambda\alpha_x)t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\beta_y t^y\Big) \\ &= \Big(\lambda\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\beta_y t^y\Big) = (\lambda g)h,\end{aligned}$$

y por otro lado tenemos que

$$\begin{aligned}\lambda(gh) &= \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\lambda(\alpha_x\beta_y)\Big)t^z = \sum_{z\in\mathbb{F}_q^n}\Big(\sum_{z=x+y}\alpha_x(\lambda\beta_y)\Big)t^z = \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\sum_{y\in\mathbb{F}_q^n}(\lambda\beta_y)t^y\Big) \\ &= \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big)\Big(\lambda\sum_{y\in\mathbb{F}_q^n}\beta_y t^y\Big) = g(\lambda h)\end{aligned}$$

Por lo tanto, $\mathbb{C}\mathbb{F}_q^n$ es un álgebra sobre $\mathbb{C}$. □

Definición 5.3. $\mathbb{C}\mathbb{F}_q^n$ se llama el *álgebra de grupo* de $\mathbb{F}_q^n$ sobre $\mathbb{C}$.

Sea χ_u como se definió previamente y $g \in \mathbb{C}\mathbb{F}_q^n$. Se define la aplicación $\widetilde{\chi}_u$ en el elemento g de la siguiente forma:

$$\widetilde{\chi}_u(g) = \widetilde{\chi}_u\Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x t^x\Big) = \sum_{x\in\mathbb{F}_q^n}\alpha_x\chi_u(x) = \sum_{x\in\mathbb{F}_q^n}\alpha_x\chi\langle x,u\rangle,$$

es decir, para cada elemento g en $\mathbb{C}\mathbb{F}_q^n$, $\widetilde{\chi}_u(g) = \sum_{x\in\mathbb{F}_q^n}\alpha_x\chi\langle x,u\rangle$.

Teorema 5.5. *Sean $g, h \in \mathbb{C}\mathbb{F}_q^n$. Entonces $\widetilde{\chi}_u(gh) = \widetilde{\chi}_u(g)\widetilde{\chi}_u(h)$.*

Demostración.

Sean $g = \sum_{x\in\mathbb{F}_q^n}\alpha_x t^x, h = \sum_{y\in\mathbb{F}_q^n}\beta_y t^y \in \mathbb{C}\mathbb{F}_q^n$, entonces

$$\begin{aligned}\widetilde{\chi}_u(gh) &= \chi_u\Big(\sum_{x,y\in\mathbb{F}_q^n}(\alpha_x\beta_y)t^{x+y}\Big) = \sum_{x,y\in\mathbb{F}_q^n}(\alpha_x\beta_y)\chi\langle x+y,u\rangle = \sum_{x\in\mathbb{F}_q^n}\sum_{y\in\mathbb{F}_q^n}(\alpha_x\beta_y)\chi\big(\langle x,u\rangle+\langle y,u\rangle\big) \\ &= \sum_{x\in\mathbb{F}_q^n}\sum_{y\in\mathbb{F}_q^n}(\alpha_x\beta_y)\chi\langle x,u\rangle\chi\langle y,u\rangle = \Big(\sum_{x\in\mathbb{F}_q^n}\alpha_x\chi\langle x,u\rangle\Big)\Big(\sum_{y\in\mathbb{F}_q^n}\beta_y\chi\langle y,u\rangle\Big) = \widetilde{\chi}_u(g)\widetilde{\chi}_u(h)\end{aligned}$$

□

5.3. La transformada de un elemento del álgebra de grupo

Definición 5.4. Sea $g(t) = \sum_{x\in\mathbb{F}_q^n} \alpha_x t^x \in \mathbb{C}\mathbb{F}_q^n$. A la suma

$$\hat{g}(t) = \sum_{x\in\mathbb{F}_q^n} \widetilde{\chi}_x(g)t^x$$

se le denomina la *transformada* de g.

Teorema 5.6. *Si* $g(t) = \sum_{x\in\mathbb{F}_q^n} \alpha_x t^x$ *entonces*

(1) $\alpha_x = q^{-n}\widetilde{\chi}_{-x}(\hat{g})$

(2) $\hat{\hat{g}}(t) = q^n g(t^{-1})$

Demostración.

$$\begin{aligned}\widetilde{\chi}_x(\hat{g}) &= \widetilde{\chi}_x\Big(\sum_{y\in\mathbb{F}_q^n}\widetilde{\chi}_y(g)t^y\Big) = \sum_{y\in\mathbb{F}_q^n}\widetilde{\chi}_y(g)\chi_x(y) = \sum_{y\in\mathbb{F}_q^n}\widetilde{\chi}_y\Big(\sum_{z\in\mathbb{F}_q^n}\alpha_z t^z\Big)\chi_x(y)\\ &= \sum_{y\in\mathbb{F}_q^n}\sum_{z\in\mathbb{F}_q^n}\alpha_z\chi_y(z)\chi_x(y) = \sum_{z\in\mathbb{F}_q^n}\sum_{y\in\mathbb{F}_q^n}\alpha_z\chi_y(z)\chi_y(x)\\ &= \sum_{z\in\mathbb{F}_q^n}\alpha_z\sum_{y\in\mathbb{F}_q^n}\chi_y(z)\chi_y(x) = \sum_{z\in\mathbb{F}_q^n}\alpha_z\sum_{y\in\mathbb{F}_q^n}\chi_y(z+x) = \sum_{z\in\mathbb{F}_q^n}\alpha_z\sum_{y\in\mathbb{F}_q^n}\chi_{z+x}(y)\end{aligned} \tag{5.2}$$

En la segunda sumatoria de la última igualdad de (5.2) puede considerarse $z+x$ como un elemento fijo. Por el Corolario 5.1 aplicado a $\mathbb{F}_q^n$, tenemos que $\sum_{y\in\mathbb{F}_q^n}\chi_{z+x}(y) = |\mathbb{F}_q^n|\delta_{z+x\in(\mathbb{F}_q^n)^\perp}$, pero $(\mathbb{F}_q^n)^\perp = \{0\}$, así que

$$\sum_{z\in\mathbb{F}_q^n}\alpha_z\sum_{y\in\mathbb{F}_q^n}\chi_{z+x}(y) = \sum_{z\in\mathbb{F}_q^n}\alpha_z|\mathbb{F}_q^n|\delta_{x+z=0} = \sum_{z\in\mathbb{F}_q^n}\alpha_z q^n\delta_{x+z=0} = q^n\sum_{z\in\mathbb{F}_q^n}\alpha_z\delta_{z=-x} = q^n\alpha_{-x} \tag{5.3}$$

De (5.2) y (5.3) concluimos que $\widetilde{\chi}_{-x}(\hat{g}) = q^n\alpha_x$, luego $\alpha_x = \widetilde{\chi}_{-x}(\hat{g})q^{-n}$, con lo cual queda demostrado el inciso (1) del teorema.

Por (1) se cumple que

$$\hat{\hat{g}}(t) = \sum_{x\in\mathbb{F}_q^n}\widetilde{\chi}_x(\hat{g})t^x = \sum_{x\in\mathbb{F}_q^n} q^n\alpha_{-x}t^x = q^n\sum_{x\in\mathbb{F}_q^n}\alpha_x t^{-x} = q^n g(t^{-1})$$

Por lo tanto, el inciso (2) del teorema también es válido. □

5.4. Enumerador de peso en el álgebra de grupo

Definición 5.5. Sea $g(t) = \sum_{x\in\mathbb{F}_q^n} \alpha_x t^x$. Se define el *enumerador de peso* de g como la suma

$$W_g(s) = \sum_{x\in\mathbb{F}_q^n} \alpha_x s^{wt(x)} = \sum_{k=0}^{n}\Big[\sum_{k=wt(x)} \alpha_x\Big]s^k = \sum_{k=0}^{n} A_k s^k.$$

Se dice que los coeficientes $A_k = \sum_{k=wt(x)} \alpha_x$ forman la *distribución de peso* de g.

De la Definición 5.5 se tiene que el enumerador de peso de la transformada $\hat{g}$ de g es $W_{\hat{g}}(s) = \sum_{x\in\mathbb{F}_q^n} \widetilde{\chi}_x(g)s^{wt(x)} = \sum_{k=0}^{n}\Big[\sum_{k=wt(x)} \widetilde{\chi}_x(g)\Big]s^k = \sum_{k=0}^{n} \hat{A}_k s^k$, donde los coeficientes $\hat{A}_k = \sum_{k=wt(x)} \widetilde{\chi}_x(g)$ forman la distribución de peso de $\hat{g}$.

5.5. La Identidad de MacWilliams

La Identidad de MacWilliams describe la relación entre el enumerador de peso de g y el enumerador de peso de $\hat{g}$.

Teorema 5.7 (La Identidad de MacWilliams)**.** *Sea $g \in \mathbb{C}\mathbb{F}_q^n$. Entonces*

$$W_{\hat{g}}(s) = [1 + (q-1)s]^n W_g\Big(\frac{1-s}{1+(q-1)s}\Big)$$

Demostración.

Se cumple que

$$\begin{aligned} W_{\hat{g}}(s) &= \sum_{x\in\mathbb{F}_q^n} \widetilde{\chi}_x(g)s^{wt(x)} = \sum_{x\in\mathbb{F}_q^n}\sum_{y\in\mathbb{F}_q^n} \alpha_y \chi\langle y,x\rangle s^{wt(x)} = \sum_{y\in\mathbb{F}_q^n}\sum_{x\in\mathbb{F}_q^n} \alpha_y \chi\langle x,y\rangle s^{wt(x)} \\ &= \sum_{y\in\mathbb{F}_q^n} \alpha_y \sum_{x\in\mathbb{F}_q^n} \chi\langle x,y\rangle s^{wt(x)} \end{aligned} \tag{5.4}$$

Sean $x = (x_1, x_2, \ldots, x_n)$ y $y = (y_1, y_2, \ldots, y_n)$. Escribimos $wt(x_i) = 0$ si $x_i = 0$ y $wt(x_i) = 1$ si $x_i \neq 0$, entonces

$$\begin{aligned} \sum_{x\in\mathbb{F}_q^n} \chi\langle x,y\rangle s^{wt(x)} &= \sum_{x\in\mathbb{F}_q^n} \chi(x_1y_1 + x_2y_2 + \cdots + x_ny_n)s^{wt(x_1)+wt(x_2)+\cdots+wt(x_n)} \\ &= \sum_{x\in\mathbb{F}_q^n} \chi(x_1y_1)\chi(x_2y_2)\cdots\chi(x_ny_n)s^{wt(x_1)}s^{wt(x_2)}\cdots s^{wt(x_n)} \\ &= \sum_{x_1,x_2\ldots,x_n\in\mathbb{F}_q} \big(\chi(x_1y_1)s^{wt(x_1)}\big)\big(\chi(x_2y_2)s^{wt(x_2)}\big)\cdots\big(\chi(x_ny_n)s^{wt(x_n)}\big) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{x_1\in\mathbb{F}_q}\sum_{x_2\in\mathbb{F}_q}\cdots\sum_{x_n\in\mathbb{F}_q}\big(\chi(x_1y_1)s^{wt(x_1)}\big)\big(\chi(x_2y_2)s^{wt(x_2)}\big)\cdots\big(\chi(x_ny_n)s^{wt(x_n)}\big)\\
&= \sum_{x_1\in\mathbb{F}_q}\chi(x_1y_1)s^{wt(x_1)}\sum_{x_2\in\mathbb{F}_q}\chi(x_2y_2)s^{wt(x_1)}\cdots\sum_{x_n\in\mathbb{F}_q}\chi(x_ny_n)s^{wt(x_n)}\\
&= \sum_{x\in\mathbb{F}_q}\chi(xy_1)s^{wt(x)}\sum_{x\in\mathbb{F}_q}\chi(xy_2)s^{wt(x)}\cdots\sum_{x\in\mathbb{F}_q}\chi(xy_n)s^{wt(x)}\\
&= \prod_{i=1}^{n}\sum_{x\in\mathbb{F}_q}\chi(xy_i)s^{wt(x)}
\end{aligned}
$$

Si $y_i = 0$ entonces

$$
\begin{aligned}
\sum_{x\in\mathbb{F}_q}\chi(xy_i)s^{wt(x)} &= \sum_{x\in\mathbb{F}_q}\chi(0)s^{wt(x)} = \sum_{x\in\mathbb{F}_q}1\cdot s^{wt(x)} = \sum_{x\in\mathbb{F}_q}s^{wt(x)} = \sum_{x\in\mathbb{F}_q\setminus\{0\}}s^{wt(x)} + s^{wt(0)}\\
&= \sum_{x\in\mathbb{F}_q\setminus\{0\}}s + 1 = s\Big(\sum_{x\in\mathbb{F}_q\setminus\{0\}}1\Big) + 1 = 1 + (q-1)s
\end{aligned}
$$

Dado que χ es un caracter no principal en $\mathbb{F}$, por el Teorema 5.1 tenemos que $\sum_{z\in\mathbb{F}_q}\chi(z) = 0$, de manera que si $y_i \neq 0$

$$
\begin{aligned}
\sum_{x\in\mathbb{F}_q}\chi(xy_i)s^{wt(x)} &= \sum_{x\in\mathbb{F}_q\setminus\{0\}}\chi(xy_i)s^{wt(x)} + \chi(0)s^{wt(0)} = \sum_{x\in\mathbb{F}_q\setminus\{0\}}\chi(xy_i)s + 1 = s\Big(\sum_{x\in\mathbb{F}_q\setminus\{0\}}\chi(xy_i)\Big) + 1\\
&= s\Big(\sum_{x\in\mathbb{F}_q}\chi(xy_i) - \chi(0)\Big) + 1 = s\Big(\sum_{z\in\mathbb{F}_q}\chi(z) - 1\Big) + 1 = s(0-1) + 1 = 1 - s
\end{aligned}
$$

Por lo tanto, $\sum_{x\in\mathbb{F}_q^n}\chi\langle x,y\rangle s^{wt(x)} = (1-s)^{wt(y)}\big[1+(q-1)s\big]^{n-wt(y)}$. Luego, por (5.4) se cumple que

$$
\begin{aligned}
W_{\hat{g}}(s) &= \sum_{y\in\mathbb{F}_q^n}\alpha_y(1-s)^{wt(y)}\big[1+(q-1)s\big]^{n-wt(y)}\\
&= \sum_{y\in\mathbb{F}_q^n}\alpha_y(1-s)^{wt(y)}\big[1+(q-1)s\big]^{n}\big[1+(q-1)s\big]^{-wt(y)}\\
&= \big[1+(q-1)s\big]^{n}\sum_{y\in\mathbb{F}_q^n}\alpha_y(1-s)^{wt(y)}\big[1+(q-1)s\big]^{-wt(y)}\\
&= \big[1+(q-1)s\big]^{n}\sum_{y\in\mathbb{F}_q^n}\alpha_y\Big(\frac{1-s}{1+(q-1)s)}\Big)^{wt(y)}
\end{aligned}
\tag{5.5}
$$

Por la Definición 5.5 tenemos que $\sum_{y\in\mathbb{F}_q^n}\alpha_y\Big(\frac{1-s}{1+(q-1)s}\Big)^{w(y)} = W_g\Big(\frac{1-s}{1+(q-1)s}\Big)$. Por lo tanto

$W_{\hat{g}}(s) = \big[1 + (q-1)s\big]^n W_g\Big(\frac{1-s}{1+(q-1)s}\Big)$. □

Definición 5.6. Sea C un código. A la suma $g_C = g_C(t) = \sum_{c\in C} t^c \in \mathbb{C}\mathbb{F}_q^n$ se le llama la *función generadora* de C.

Puesto que

$$W_{g_C}(s) = \sum_{k=0}^{n}\Big[\sum_{k=wt(c)} 1\Big]s^k = \sum_{k=0}^{n} A_k s^k = W_C(s), \tag{5.6}$$

el enumerador de peso de la función generadora g_C es igual al enumerador de peso del código C.

Teorema 5.8. *Sea C un código lineal. Entonces $\widetilde{\chi}_u(g_C) = |C|\delta_{u\in C^\perp}$.*

Demostración.

Por el Corolario 5.1 se cumple que $\widetilde{\chi}_u(g_C) = \widetilde{\chi}_u\Big(\sum_{c\in C} t^c\Big) = \sum_{c\in C}\chi_u(c) = |C|\delta_{u\in C^\perp}$. □

Teorema 5.9. *Sea C un código lineal. Entonces $\hat{g}_C = |C| g_{C^\perp}$.*

Demostración.

Por el Teorema 5.8, $\hat{g_C} = \sum_{x\in\mathbb{F}_q^n}\chi_x(g_C)t^x = \sum_{x\in\mathbb{F}_q^n}|C|(\delta_{x\in C^\perp})t^x = |C|\sum_{x\in C^\perp} t^x = |C| g_{C^\perp}$. □

Ejemplo 5.1. Consideremos el código lineal binario $L = \{000, 111\}$ que tiene como función generadora a $g_C(t) = \sum_{c\in C} t^c = t^{000} + t^{111}$.

Definimos el caracter χ como $\chi(\alpha) = (-1)^\alpha$, para $\alpha \in \mathbb{F}_2$. Para ver que χ no es principal tomemos $\alpha = 1$, entonces $\chi(\alpha) = \chi(1) = (-1)^1 = -1 \neq 1$.

Dado que para cualesquiera $x, y \in \mathbb{F}_2^3$, $\langle x, y\rangle \in \mathbb{F}_2$, tenemos que $\chi_u(x) = \chi\langle x, u\rangle = (-1)^{\langle x,u\rangle}$, luego $\widetilde{\chi}_x(g_C) = \sum_{c\in C}\chi_x(c) = \chi_x(000) + \chi_x(111) = (-1)^{\langle 000,x\rangle} + (-1)^{\langle 111,x\rangle}$. Dado que x varía en $\mathbb{F}_2^3$ y $|\,\mathbb{F}_2^3\,| = 8$, se tiene lo siguiente:

$$\begin{aligned}
\widetilde{\chi}_{111}(g_C) &= (-1)^{\langle 000,111\rangle} + (-1)^{\langle 111,111\rangle} = (-1)^0 + (-1)^3 = 1 - 1 = 0\\
\widetilde{\chi}_{110}(g_C) &= (-1)^{\langle 000,110\rangle} + (-1)^{\langle 111,110\rangle} = (-1)^0 + (-1)^2 = 1 + 1 = 2\\
\widetilde{\chi}_{101}(g_C) &= (-1)^{\langle 000,101\rangle} + (-1)^{\langle 111,101\rangle} = (-1)^0 + (-1)^2 = 1 + 1 = 2\\
\widetilde{\chi}_{100}(g_C) &= (-1)^{\langle 000,100\rangle} + (-1)^{\langle 111,100\rangle} = (-1)^0 + (-1)^1 = 1 - 1 = 0\\
\widetilde{\chi}_{010}(g_C) &= (-1)^{\langle 000,010\rangle} + (-1)^{\langle 111,010\rangle} = (-1)^0 + (-1)^1 = 1 - 1 = 0\\
\widetilde{\chi}_{011}(g_C) &= (-1)^{\langle 000,011\rangle} + (-1)^{\langle 111,011\rangle} = (-1)^0 + (-1)^2 = 1 + 1 = 2\\
\widetilde{\chi}_{001}(g_C) &= (-1)^{\langle 000,001\rangle} + (-1)^{\langle 111,001\rangle} = (-1)^0 + (-1)^1 = 1 - 1 = 0\\
\widetilde{\chi}_{000}(g_C) &= (-1)^{\langle 000,000\rangle} + (-1)^{\langle 111,000\rangle} = (-1)^0 + (-1)^0 = 1 + 1 = 2
\end{aligned}$$

Por lo tanto, $\hat{g}_C = \sum_{x\in\mathbb{F}_2^3}\widetilde{\chi}_x(g_C)t^x = \widetilde{\chi}_{111}(g_C)t^{111} + \widetilde{\chi}_{110}(g_C)t^{110} + \widetilde{\chi}_{101}(g_C)t^{101} + \widetilde{\chi}_{100}(g_C)t^{100} + \widetilde{\chi}_{010}(g_C)t^{010} + \widetilde{\chi}_{011}(g_C)t^{011} + \widetilde{\chi}_{001}(g_C)t^{001} + \widetilde{\chi}_{000}(g_C)t^{000} = 2t^{110} + 2t^{101} + 2t^{011} + 2t^{000}$. Por el Teorema

5.9 se cumple que $\hat{g}_{C} = |C| g_{C^{\perp}}$, de donde $2(t^{110} + t^{101} + t^{011} + t^{000}) = 2g_{C^{\perp}}$, por tanto $g_{C^{\perp}} = t^{110} + t^{101} + t^{011} + t^{000}$ y como $g_{C^{\perp}} = \sum_{x \in C^{\perp}} t^{x}$, tenemos que $C^{\perp} = \{110, 101, 011, 000\}$.

Por el Teorema 5.8 se tiene que

$$\begin{aligned} W_{\hat{g}_{C}}(s) &= \sum_{x \in \mathbb{F}_q^n} \widetilde{\chi}_x(g_C) s^{wt(x)} = \sum_{x \in \mathbb{F}_q^n} |C| \delta_{x \in C^{\perp}} s^{wt(x)} = |C| \sum_{x \in \mathbb{F}_q^n} \delta_{x \in C^{\perp}} s^{wt(x)} \\ &= |C| \sum_{x \in C^{\perp}} s^{wt(x)} = |C| W_{g_{C^{\perp}}}(s) = |C| W_{C^{\perp}}(s) \end{aligned} \tag{5.7}$$

esto último por (5.6).

Así, se obtiene una versión de la Identidad de MacWilliams para códigos lineales.

Corolario 5.2 (La Identidad de MacWilliams para códigos lineales)**.** *Sean C un código lineal, $C^{\perp}$ su código dual y $W_C(s) = \sum_{k=0}^{n} A_k s^k$ y $W_{C^{\perp}} = \sum_{k=0}^{n} {A_k}^{\perp} s^k$ los enumeradores de peso de C y $C^{\perp}$, respectivamente. Entonces*

$$W_{C^{\perp}}(s) = \frac{1}{|C|}\big[1 + (q-1)s\big]^n W_C\Big(\frac{1-s}{1+(q-1)s}\Big).$$

Demostración.

Por (5.7) tenemos que $|C| W_{C^{\perp}}(s) = W_{\hat{g}_{C}}$. Entonces, por la Identidad de MacWilliams (Teorema 5.7) por (5.6) se cumple que:

$$|C| W_{C^{\perp}}(s) = \big[1 + (q-1)s\big]^n W_{g_C}\Big(\frac{1-s}{1+(q-1)s}\Big) = \big[1 + (q-1)s\big]^n W_C\Big(\frac{1-s}{1+(q-1)s}\Big)$$

de donde se obtiene el resultado. □

Ejemplo 5.2. Consideremos nuevamente el código lineal binario $C = \{000, 111\}$ del Ejemplo 5.1. Dado que C tiene una palabra de peso 0, 0 palabras de peso 1, 0 palabras de peso 2 y una palabra de peso 3, el enumerador de pesos de C es $\sum_{k=0}^{n} A_k s^k = \sum_{k=0}^{3} A_k s^k = A_0 s^0 + A_1 s^1 + A_2 s^2 + A_3 s^3 = 1 + s^3$. Puesto que $|C| = 2$ por la Identidad de MacWilliams para códigos lineales (Corolario 5.2) tenemos que

$$\begin{aligned} W_{C^{\perp}}(s) &= \frac{1}{2}(1+s)^3\left[1 + \left(\frac{1-s}{1+s}\right)^3\right] = \frac{1}{2}\left[(1+s)^3 + (1+s)^3\frac{(1-s)^3}{(1+s)^3}\right] \\ &= \frac{1}{2}\big[(1+s)^3 + (1-s)^3\big] = 1 + 3s^2 \end{aligned}$$

Esto indica que $C^{\perp}$ tiene una palabra de peso 0 y 3 palabras de peso 2. Así, $C^{\perp} = \{000, 110, 101, 011\}$, que es congruente con el resultado obtenido en el Ejemplo 5.1.

Conclusiones

En este trabajo se estudiaron los conceptos básicos de la teoría de matroides. Se puso atención especial al establecimiento de las equivalencias entre algunas de las definiciones del concepto de matroide y se presentaron algunos ejemplos. También se abordaron conceptos y resultados de la teoría de códigos y se proporcionaron dos demostraciones distintas de la Identidad de MacWilliams, que es un resultado de mucha importancia dentro de esta área. Una de tales demostraciones se realizó empleando matroides y una de las ventajas de hacerlo por esta vía es que la demostración es más corta y elegante. Lo que tuvo que pagarse a cambio fue la extensión de la teoría acerca del polinomio enumerador de pesos de un código, pero vale la pena pues en la actualidad existen varias publicaciones en las que se establecen conexiones entre matroides y teoría de códigos, así como con otras áreas de la matemática, y este representaría un primer acercamiento.

Referencias

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

[2] R. Jurrius and R. Pellikaan. *Algebraic Geometry Modeling in Information Theory*, volume 8 of *Series on Coding Theory and Cryptology*, chapter Codes, Arrangements and Matroids, pages 219–325. World Scientific, 02 2013.

[3] T. Kløve. The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$. *Discrete Mathematics*, 23:159–168, 1978.

[4] J. Oxley. *Matroid Theory*. Oxford University Press, 1992.

[5] A. Rendón-Espinosa. Compartición de secretos: una aplicación a imágenes. Tesis de licenciatura, Benemérita Universidad Autónoma de Puebla, 2018.

[6] S. Roman. *Coding and Information Theory*. Springer-Verlag, 1992.

[7] D. J. A. Welsh. *Matroid Theory*. Academic Press Inc., 1976.

[8] H. Whitney. On the abstract properties of linear dependence. *American Journal of Mathematics*, 57:63–87, 1935.

Índice alfabético