

ASPECTOS COMBINATORIOS DE LAS SUBDIVISIONES
MATROIDALES

POR

EDGAR FELIPE RINCÓN

UNA TESIS

PRESENTADA AL DEPARTAMENTO

DE MATEMÁTICAS

COMO PARTE DE LOS REQUISITOS

PARA EL GRADO DE

MAGÍSTER EN MATEMÁTICAS

DIRECTOR: FEDERICO ARDILA

UNIVERSIDAD DE LOS ANDES

BOGOTÁ, COLOMBIA

JULIO, 2007

Índice general

1. Introducción	1
2. Preliminares	3
2.1. Definiciones básicas	3
2.1.1. Independencia	3
2.1.2. Bases	6
2.1.3. Rango	10
2.1.4. Circuitos	10
2.2. Menores	12
2.3. Conexidad	13
2.4. El polinomio de Tutte	15
2.4.1. Actividad sobre las bases	18
2.5. Órdenes parciales	20
2.5.1. La función de Möbius	21
3. Politopos matroidales	23
3.1. Definición	23
3.2. Dimensión	25
3.3. Caras	26
3.4. Descripción por desigualdades	28
4. Subdivisiones matroidales	31
4.1. Generalidades	31
4.2. Separaciones por hiperplanos	34
4.3. Una subdivisión de $U_{m,mk}$	36
5. Funciones bien comportadas bajo subdivisiones	38
5.1. Definición y ejemplos	39
5.2. Una definición equivalente	40
5.3. Funciones características	45
5.4. Rango	47
5.5. Actividad sobre las bases	48
6. Algunas aplicaciones de la lógica	55
6.1. Notación	55
6.2. Representabilidad de matroides	56

6.3. Sistemas de polinomios	59
Bibliografía	61

Capítulo 1

Introducción

A lo largo de las distintas áreas de la matemática existen muchas nociones de independencia: independencia lineal entre elementos de un espacio vectorial, independencia afín entre puntos de una geometría, independencia algebraica en una extensión de campos, independencia entre las aristas de un grafo, etc. Sin embargo las propiedades combinatorias de cada una de estas nociones son muy similares, lo que permite enmarcarlas dentro de un mismo contexto como es el de las matroides.

Las matroides fueron definidas por Whitney en 1935, y desde entonces han probado ser un objeto fundamental en la combinatoria. Su definición es lo suficientemente general para permitir una gran cantidad de aplicaciones, y también lo suficientemente específica para dar lugar a una teoría bastante poderosa. Recientemente ha venido tomando bastante importancia el estudio de los politopos asociados a las matroides, y las subdivisiones matroidales de éstos.

Este trabajo tiene varios objetivos. En primer lugar pretende exponer de manera clara y concisa los preliminares combinatorios necesarios para el estudio básico de los politopos matroidales, y presentar las propiedades geométricas básicas de éstos. También busca estudiar las subdivisiones de estos politopos, tanto de forma geométrica como de forma algebraica. Gran parte del trabajo se dedica a estudiar las funciones bien comportadas bajo subdivisiones desde un marco general y unificado, y a presentar nuevos avances desarrollados en este tema. Al final se expone una aplicación de la lógica a la representabilidad de matroides y a la solubilidad de sistemas de polinomios con coeficientes enteros.

El trabajo está organizado de la siguiente manera. En el capítulo 2 se presentan todos los preliminares combinatorios necesarios para el resto del documento. Allí se definen las matroides y se estudian con cierta profundidad, probando los teoremas básicos sobre éstas. Al final del capítulo se revisa rápidamente la teoría de ordenes parciales y se

estudian sus funciones de Möbius.

El tercer capítulo se centra en el estudio de los politopos matroidales y sus propiedades básicas. Se describen de manera combinatoria sus vértices y aristas, su dimensión y las desigualdades que los definen.

En el cuarto capítulo se estudian las subdivisiones de los politopos matroidales desde un punto de vista geométrico. Se investigan con cierto detalle las subdivisiones que son obtenidas al cortar con un hiperplano y también los hiperplanos que las generan. Además se presenta un ejemplo de una subdivisión que no es generada mediante cortes con hiperplanos, y se generaliza a una familia de subdivisiones de matroides uniformes.

El capítulo 5 presenta un estudio de las funciones bien comportadas bajo subdivisiones. Debido a que estas funciones han venido apareciendo en distintas áreas y bajo distintos contextos se les trata de manera general, y se da una equivalencia entre dos definiciones que han surgido en diferentes partes de la literatura. También se presenta una amplia familia de funciones que es bien comportada bajo subdivisiones y permite gran cantidad de especializaciones. De esta forma se prueba que dos funciones sorprendentemente finas son bien comportadas bajo subdivisiones, como lo son el rango de cada subconjunto y la actividad sobre cada base de una matroide.

En el último capítulo se muestra una aplicación de la lógica a la representabilidad de matroides y la solubilidad de sistemas de polinomios con coeficientes enteros, probando de manera interesante algunos hechos algebraicos.

Los resultados que se exponen en los capítulos 4 y 5 son parte del trabajo conjunto con Alex Fink bajo la dirección de Federico Ardila, como parte de la “SFSU-Colombia Combinatorics Initiative”.

Capítulo 2

Preliminares

En este capítulo se expondrán de manera autocontenida los conceptos combinatorios necesarios para el resto del trabajo. La gran mayoría del capítulo está dedicado a desarrollar la teoría básica de matroides, mientras que al final se hablará un poco de órdenes parciales. Si se quiere profundizar en estos temas se pueden consultar las excelentes referencias [8] y [12].

En la primera sección daremos las definiciones básicas, algunos ejemplos y también varios resultados fundamentales sobre matroides. En la segunda sección definiremos rápidamente los menores de una matroide. La tercera parte presenta los resultados básicos sobre conexidad en matroides. En la cuarta parte estudiaremos los invariantes de Tutte-Grothendieck, sobre todo el polinomio de Tutte. Finalmente en la última sección daremos las definiciones básicas en la teoría de órdenes parciales y entenderemos un poco las funciones de Möbius.

2.1. Definiciones básicas

Para simplificar la notación, a través de todo el documento denotaremos por $[n]$ al conjunto de enteros positivos $\{1, 2, \dots, n\}$. También escribiremos $A \cup b$ y $A \setminus b$ en vez de $A \cup \{b\}$ y $A \setminus \{b\}$ respectivamente, cuando no se presente confusión.

2.1.1. Independencia

Definición 2.1.1. Una *matroide* M es una pareja (E, \mathcal{I}) , donde E es un conjunto finito e \mathcal{I} es una familia de subconjuntos de E que satisface:

$$(I1) \quad \emptyset \in \mathcal{I}.$$

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

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

En este caso diremos que M es una matroide sobre el conjunto E , al que llamaremos su *conjunto base*. A los elementos de \mathcal{I} los llamaremos subconjuntos *independientes* de M y a los demás subconjuntos de E los llamaremos *dependientes*. A la colección \mathcal{I} también la denotaremos $\mathcal{I}(M)$ para evitar confusiones cuando trabajemos con distintas matroides.

El nombre “matroide” fue inspirado por la siguiente familia de ejemplos, con la que se observa que en su definición realmente se está capturando una noción de independencia.

Ejemplo 2.1.2. Sea F un campo, y sea A una matriz de $m \times n$ con entradas en F y columnas c_1, c_2, \dots, c_n . Tomemos $E = [n]$, y definamos \mathcal{I} como la familia de subconjuntos $\{i_1, i_2, \dots, i_k\}$ de E tal que las columnas $c_{i_1}, c_{i_2}, \dots, c_{i_k}$ son linealmente independientes (en el espacio vectorial F^m sobre el campo F). Entonces $M(A) = (E, \mathcal{I})$ es una matroide.

Claramente \mathcal{I} satisface los axiomas (I1) e (I2). Para probar (I3), supongamos que $I, J \in \mathcal{I}$ y $|I| < |J|$. Llamemos $V_I = \text{gen}\{c_i : i \in I\}$ y $V_J = \text{gen}\{c_j : j \in J\}$. Entonces como

$$\dim(V_I) = |I| < |J| = \dim(V_J)$$

tenemos que $V_I \not\subseteq V_J$, por lo que debe existir $j \in J \setminus I$ tal que $I \cup j \in \mathcal{I}$.

Otra gran familia de ejemplos proviene de la teoría de grafos.

Definición 2.1.3. Un *grafo* G es una pareja (V, E) , donde V es un conjunto (finito) cuyos elementos llamaremos *vértices* y E es un multiconjunto de parejas no ordenadas de vértices (posiblemente iguales). A los elementos de E los llamaremos *aristas*. Se acostumbra representar gráficamente al grafo G , dibujando un punto en el plano por cada vértice y una línea entre dos puntos por cada arista entre sus correspondientes vértices.

En la Figura 2.1 se muestra una representación gráfica del grafo G con vértices v_1, v_2, v_3, v_4 y aristas $e_1 = \{v_1, v_1\}, e_2 = \{v_1, v_2\}, e_3 = \{v_2, v_3\}, e_4 = \{v_2, v_3\}, e_5 = \{v_3, v_1\}$.

Un *ciclo* es un conjunto de aristas $\{e_1, e_2, \dots, e_k\}$ tal que $e_1 = \{v_1, v_2\}, e_2 = \{v_2, v_3\}, \dots, e_{k-1} = \{v_{k-1}, v_k\}, e_k = \{v_k, v_1\}$, para algunos vértices v_1, v_2, \dots, v_n . En el grafo de la Figura 2.1, algunos ciclos son $\{e_2, e_4, e_5\}, \{e_3, e_4\}$ y $\{e_1\}$.

Un *camino* entre dos vértices v, u de G es una sucesión de vértices $v = v_0, v_1, \dots, v_k = u$ tal que para todo $i \in [k]$ se tiene que $\{v_{i-1}, v_i\}$ es una arista. La relación definida por $v \sim u$ si existe un camino entre v y u es claramente una relación de equivalencia, sus

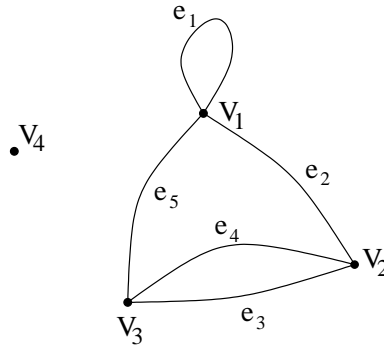


Figura 2.1: Representación gráfica de un grafo

clases de equivalencia se denominan las *componentes conexas* de G . Si G tiene una sola componente conexa, diremos que G es un grafo *conexo*. Las componentes conexas del grafo de la Figura 2.1 son $\{v_1, v_2, v_3\}$ y $\{v_4\}$.

Ejemplo 2.1.4. Sea $G = (V, E)$ un grafo, y tomemos \mathcal{I} como la familia de subconjuntos de E que no contienen ningún ciclo. Entonces $M(G) = (E, \mathcal{I})$ es una matroide.

De nuevo es claro que \mathcal{I} satisface (I1) e (I2). Ahora, es fácil probar por inducción que si $I \in \mathcal{I}$ entonces el grafo $G_I = (V, I)$ tiene $|V| - |I|$ componentes conexas. Luego si $I, J \in \mathcal{I}$ y $|I| < |J|$ entonces el grafo G_I tiene más componentes conexas que el grafo G_J , por lo que debe existir una arista $j \in J$ cuyos vértices estén en componentes distintas de G_I (y por lo tanto $j \notin I$). Esta arista cumple entonces que $I \cup j \in \mathcal{I}$, probando así (I3).

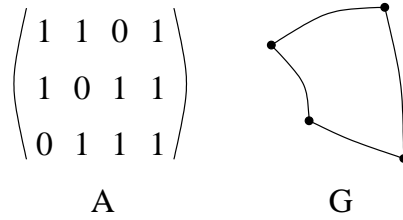
El siguiente ejemplo nos será muy útil en lo que viene.

Ejemplo 2.1.5. Sean $m \leq n$ enteros no negativos. Si tomamos $E = [n]$ e \mathcal{I} como la familia de subconjuntos de E que tienen a lo más m elementos entonces claramente $U_{m,n} = (E, \mathcal{I})$ es una matroide, a la que denominaremos la *matroide uniforme* $U_{m,n}$.

Ahora estableceremos el concepto de isomorfismo entre matroides.

Definición 2.1.6. Diremos que dos matroides $M = (E, \mathcal{I})$ y $M' = (E', \mathcal{I}')$ son *isomorfas*, denotado por $M \cong M'$, si existe una biyección $f : E \rightarrow E'$ tal que para todo $A \subseteq E$ se tiene que $A \in \mathcal{I}$ si y sólo si $f(A) \in \mathcal{I}'$, es decir, f preserva conjuntos independientes. A la función f la llamaremos un *isomorfismo* entre M y M' .

Nótese que toda matroide de n elementos es isomorfa a una sobre el conjunto $[n]$. Por lo tanto, de ahora en adelante escribiremos indistintamente E o $[n]$ para el conjunto base de las matroides que consideremos.

Figura 2.2: Matriz A y grafo G

Ejemplo 2.1.7. Es fácil ver que si A y G son la matriz y el grafo de la Figura 2.2, entonces las matroides $M(A)$, $M(G)$ y $U_{3,4}$ son todas isomorfas.

2.1.2. Bases

Definición 2.1.8. Una *base* de una matroide M es un conjunto independiente maximal respecto a la inclusión. A la colección de todas las bases de M la denotaremos por $\mathcal{B}(M)$, o simplemente \mathcal{B} cuando no se presente confusión.

Obsérvese que la colección \mathcal{B} determina la matroide M , ya que los conjuntos independientes son aquellos subconjuntos de E que están contenidos en alguna base.

Ejemplo 2.1.9. Es claro que las bases de la matroide uniforme $U_{m,n}$ son los subconjuntos de $[n]$ de tamaño m . Si A es una matriz entonces las bases de $M(A)$ corresponden a los subconjuntos linealmente independientes maximales de columnas de A , es decir, a los subconjuntos de columnas que formen una base para la imagen de A . También es fácil ver que si G es un grafo conexo entonces una base de $M(G)$ es un *árbol generador*, es decir, un conjunto de aristas sin ciclos que conecta todos los vértices.

El siguiente es un hecho familiar en el contexto de álgebra lineal y es válido más generalmente en el contexto de matroides.

Proposición 2.1.10. *Todas las bases de una matroide tienen el mismo tamaño.*

Demostración. Supongamos por contradicción que existen dos bases A y B con $|A| < |B|$. Entonces por el axioma (I3) tenemos que existe un elemento $b \in B \setminus A$ tal que $A \cup b \in \mathcal{I}$, lo que contradice la maximalidad de A . \square

Vale la pena anotar que la anterior proposición implica que si un conjunto independiente I tiene el tamaño de una base (y por lo tanto de todas), entonces I debe ser una base también.

Nos será bastante útil la siguiente caracterización de las colecciones que son el conjunto de bases de alguna matroide.

Teorema 2.1.11. *Una colección \mathcal{B} de subconjuntos de E es el conjunto de bases de una matroide sobre E si y sólo si \mathcal{B} satisface:*

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

(B2) (Propiedad de intercambio) Si $A, B \in \mathcal{B}$ y $a \in A \setminus B$, entonces existe $b \in B \setminus A$ tal que $(A \setminus a) \cup b \in \mathcal{B}$.

Demostración. Para ver que estas condiciones son necesarias, supongamos que M es una matroide sobre E con $\mathcal{B}(M) = \mathcal{B}$. Ya que $\emptyset \in \mathcal{I}(M)$ entonces $\mathcal{I}(M) \neq \emptyset$, por lo que tenemos (B1). Para probar (B2), supongamos que A y B son dos bases de M y sea $a \in A \setminus B$. Entonces el conjunto $A \setminus a$ es un conjunto independiente de tamaño $|A| - 1 = |B| - 1 < |B|$, por lo que por (I3) debe existir $b \in B \setminus (A \setminus a)$ tal que $A \setminus a \cup b \in \mathcal{I}(M)$. Como $a \notin B$ entonces $B \setminus (A \setminus a) = B \setminus A$, luego $b \in B \setminus A$. Finalmente, como $|A \setminus a \cup b| = |A|$ entonces $A \setminus a \cup b$ debe ser una base como queríamos.

Probemos ahora que las condiciones son suficientes. Supongamos que \mathcal{B} es una familia de subconjuntos de E que satisface (B1) y (B2). Haremos la prueba en dos pasos:

1. *Todos los elementos de \mathcal{B} tienen el mismo tamaño.*

Supongamos por contradicción que existen dos elementos $A, B \in \mathcal{B}$ tal que $|A| > |B|$, y tomémoslos de tal forma que $|A \setminus B|$ sea mínimo entre todas estas parejas. Sea $a \in A \setminus B$. Por (B2) sabemos que existe $b \in B \setminus A$ tal que $C = A \setminus a \cup b \in \mathcal{B}$. Entonces $|C| = |A| > |B|$ y además

$$\begin{aligned} |C \setminus B| &= |(A \setminus a \cup b) \setminus B| \\ &= |(A \setminus a) \setminus B| \\ &= |(A \setminus B) \setminus a| \\ &= |A \setminus B| - 1, \end{aligned}$$

lo que contradice la escogencia de A y B .

2. *Sea \mathcal{I} la colección de subconjuntos de E que son subconjuntos de algún elemento de \mathcal{B} . Entonces (E, \mathcal{I}) es una matroide.*

Claramente \mathcal{I} satisface (I1) e (I2). Para probar (I3), supongamos que $I, J \in \mathcal{I}$ y $|I| < |J|$. Por definición sabemos que existen $A, B \in \mathcal{B}$ tal que $I \subseteq A$ y $J \subseteq B$, y tomémoslos de tal forma que $|(A \setminus I) \setminus B|$ sea mínimo.

Si $|(A \setminus I) \setminus B| > 0$, entonces existe $a \in (A \setminus I) \setminus B \subseteq A \setminus B$. Aplicando (B2)

tenemos que existe $b \in B \setminus A$ tal que $C = A \setminus a \cup b \in \mathcal{B}$. Pero entonces $I \subseteq C$ y

$$\begin{aligned} |(C \setminus I) \setminus B| &= |((A \setminus a \cup b) \setminus I) \setminus B| \\ &= |((A \setminus a) \setminus I) \setminus B| \\ &= |((A \setminus I) \setminus B) \setminus a| \\ &= |(A \setminus I) \setminus B| - 1, \end{aligned}$$

lo que contradice la escogencia de A y B .

Por lo tanto se debe tener que $A \setminus I \subseteq B$. Además, como $|A| = |B|$ entonces $|A \setminus I| = |A| - |I| > |B| - |J| = |B \setminus J|$ y luego $A \setminus I \not\subseteq B \setminus J$, por lo que existe $j \in (A \setminus I) \cap J$. Luego $I \cup j \subseteq A$ y entonces $I \cup j \in \mathcal{I}$, lo que prueba (I3).

Finalmente, es claro de la definición y el paso 1 que \mathcal{B} es el conjunto de bases de (E, \mathcal{I}) , con lo que termina la prueba. \square

La anterior caracterización nos ayudará en el siguiente ejemplo.

Ejemplo 2.1.12. Sea n un entero positivo, y sean $1 \leq c_1 < c_2 < \dots < c_k \leq n$ enteros. Llamemos $\mathcal{B}_{c_1, c_2, \dots, c_k}$ a la colección de conjuntos de la forma $\{a_1 < a_2 < \dots < a_k\}$ tal que $a_i \leq c_i$. Entonces $\mathcal{B}_{c_1, c_2, \dots, c_k}$ es la colección de bases de una matroide B_{c_1, c_2, \dots, c_k} , a la que llamaremos *matroide de Schubert*. En diversas partes de la literatura estas matroides reciben también otros nombres como “shifted matroids”, PI-matroides, matroides generalizadas de Catalán o matroides de libertad.

Probaremos que la colección $\mathcal{B}_{c_1, c_2, \dots, c_k}$ cumple los axiomas (B1) y (B2). Claramente $\mathcal{B}_{c_1, c_2, \dots, c_k}$ cumple (B1), ya que $\{c_1 < c_2 < \dots < c_k\} \in \mathcal{B}_{c_1, c_2, \dots, c_k}$. Para ver que $\mathcal{B}_{c_1, c_2, \dots, c_k}$ cumple (B2), tomemos dos conjuntos distintos $A = \{a_1 < a_2 < \dots < a_k\}$ y $B = \{b_1 < b_2 < \dots < b_k\}$ en $\mathcal{B}_{c_1, c_2, \dots, c_k}$, y supongamos que $a_j \in A \setminus B$. Llamemos m al menor entero tal que $b_m \in B \setminus A$. Sea l el entero tal que $a_{l-1} < b_m < a_l$ (con la convención que $a_0 = 0$ y $a_{k+1} = n + 1$). Nótese que por la definición de m tenemos que para todo $r < m$ existe un elemento a_{i_r} tal que $b_r = a_{i_r}$. En particular, esto implica que $m \leq l$.

Mostraremos que $A \setminus a_j \cup b_m \in \mathcal{B}_{c_1, c_2, \dots, c_k}$, por lo que $\mathcal{B}_{c_1, c_2, \dots, c_k}$ cumple (B2). Para esto consideremos los siguientes casos:

- Si $l < j$ entonces

$$A \setminus a_j \cup b_m = \{a_1 < a_2 < \dots < a_{l-1} < b_m < a_l < \dots < a_{j-1} < a_{j+1} < \dots < a_k\}.$$

Nótese que $b_m \leq b_l \leq c_l$ y además para todo $l \leq s \leq j - 1$ se tiene que $a_s \leq c_s < c_{s+1}$, por lo que $A \setminus a_j \cup b_m \in \mathcal{B}_{c_1, c_2, \dots, c_k}$.

- Si $l = j$ entonces

$$A \setminus a_j \cup b_m = \{a_1 < a_2 < \cdots < a_{l-1} < b_m < a_{l+1} < \cdots < a_k\},$$

de donde es claro que $A \setminus a_j \cup b_m \in \mathcal{B}_{c_1, c_2, \dots, c_k}$ ya que $b_m \leq b_l \leq c_l$.

- Si $l = j + 1$ entonces

$$A \setminus a_j \cup b_m = \{a_1 < a_2 < \cdots < a_{l-2} < b_m < a_l < \cdots < a_k\}.$$

Como ningún $b_r = a_{i_r}$ es igual a $a_j = a_{l-1}$ entonces $m \leq l - 1$, por lo que $b_m \leq b_{l-1} \leq c_{l-1}$ y luego $A \setminus a_j \cup b_m \in \mathcal{B}_{c_1, c_2, \dots, c_k}$.

- Si $l > j + 1$ entonces

$$A \setminus a_j \cup b_m = \{a_1 < a_2 < \cdots < a_{j-1} < a_{j+1} < \cdots < a_{l-1} < b_m < a_l < \cdots < a_k\}.$$

Tomemos s tal que $j + 1 \leq s \leq l - 1$. Sea t el menor entero tal que $a_s \leq b_t$. Como ningún $b_r = a_{i_r}$ es igual a a_j tenemos que $t \leq s - 1$, por lo que $a_s \leq b_t \leq b_{s-1} \leq c_{s-1}$. Además, al igual que en el caso anterior, se cumple que $m \leq l - 1$ y entonces $b_m \leq b_{l-1} \leq c_{l-1}$. De esta forma tenemos que $A \setminus a_j \cup b_m \in \mathcal{B}_{c_1, c_2, \dots, c_k}$.

En cualquier caso $A \setminus a_j \cup b_m \in \mathcal{B}_{c_1, c_2, \dots, c_k}$, con lo que termina la prueba.

De manera un poco sorprendente, las bases de una matroide cumplen la siguiente propiedad de intercambio simétrico.

Teorema 2.1.13. *Sea \mathcal{B} la colección de bases de una matroide. Si $A, B \in \mathcal{B}$ y $a \in A \setminus B$ entonces existe $b \in B \setminus A$ tal que $A \setminus a \cup b \in \mathcal{B}$ y también $B \setminus b \cup a \in \mathcal{B}$.*

Demostración. Supongamos por contradicción que no se cumple el resultado. Tomemos $A, B \in \mathcal{B}$ tal que $|A \setminus B| = |B \setminus A|$ sea mínimo entre todas las parejas de bases que son contraejemplo al teorema. Sea $a \in A \setminus B$ tal que para todo $b \in B \setminus A$ vale que $A \setminus a \cup b \notin \mathcal{B}$ o $B \setminus b \cup a \notin \mathcal{B}$. Aplicando la propiedad de intercambio (B2), sabemos que existe $b \in B \setminus A$ tal que $A \setminus a \cup b \in \mathcal{B}$. Aplicando de nuevo (B2) a las bases B y A con el elemento $b \in B \setminus A$ tenemos que existe $a' \in A \setminus B$ tal que $B' = B \setminus b \cup a' \in \mathcal{B}$. Nótese que $a' \neq a$ debido a la escogencia de a , luego $a \in A \setminus B'$. Además $|A \setminus B'| = |A \setminus B \setminus a'| = |A \setminus B| - 1$, por lo que por la escogencia de A y B tenemos que existe $b' \in B' \setminus A = B \setminus A \setminus b$ tal que $A \setminus a \cup b' \in \mathcal{B}$ y además $B'' = B' \setminus b' \cup a = B \setminus \{b, b'\} \cup \{a, a'\} \in \mathcal{B}$. Finalmente, aplicando (B2) a B'' y B con el elemento $a' \in B'' \setminus B$ tenemos que alguno de los conjuntos $B'' \setminus a' \cup b = B \setminus b \cup a$ y $B'' \setminus a' \cup b = B \setminus b' \cup a$ está en \mathcal{B} , lo que es una contradicción con la escogencia de a . \square

La siguiente definición nos será de utilidad más adelante.

Definición 2.1.14. Sea M una matroide sobre E . Diremos que el elemento $e \in E$ es un *coloop* si para toda base B se tiene que $e \in B$, y que es un *loop* si para toda base B ocurre que $e \notin B$.

2.1.3. Rango

La anterior noción de independencia nos permite definir una noción de rango, que generaliza la que tenemos en los distintos ejemplos. Primero necesitamos un resultado sencillo.

Proposición 2.1.15. Sea M una matroide sobre E , y sea $X \subseteq E$. Entonces todos los subconjuntos independientes de X maximales tienen el mismo tamaño. A estos subconjuntos los llamaremos bases de X .

Demostración. La prueba es básicamente la misma que para las bases de M . Supongamos por contradicción que existen $A, B \subseteq X$ independientes maximales con $|A| < |B|$. Entonces por el axioma (I3) tenemos que existe un elemento $b \in B \setminus A$ tal que $A \cup b$ es independiente (y subconjunto de X), lo que contradice la maximalidad de A . \square

Definición 2.1.16. La *función rango* de una matroide M , denotada por r_M (o simplemente r cuando no haya confusión), es la función que le asigna a cada subconjunto X de E el tamaño de cualquiera de sus bases. Al rango de E , es decir al tamaño de las bases de M , lo llamaremos también el *rango de M* y lo denotaremos por $r(M)$.

Nótese que la función rango determina completamente la matroide M , ya que los conjuntos independientes de M son precisamente aquellos subconjuntos X de E que cumplen que $r(X) = |X|$.

2.1.4. Circuitos

Muchas veces nos será útil también tratar con los conjuntos dependientes.

Definición 2.1.17. Un *circuito* de una matroide M es un conjunto dependiente minimal respecto a la inclusión. A la colección de circuitos de M la denotaremos por $\mathcal{C}(M)$, o simplemente \mathcal{C} cuando no se presente confusión.

De nuevo, la colección \mathcal{C} determina completamente la matroide M , ya que los conjuntos independientes son los subconjuntos de E que no contienen ningún circuito.

Ejemplo 2.1.18. Los circuitos en la matroide uniforme $U_{m,n}$ son los subconjuntos de $[n]$ de tamaño $m + 1$ (si $m < n$). Si G es un grafo entonces los circuitos de $M(G)$ son los ciclos que no pasan más de una vez por un mismo vértice.

En el siguiente teorema se listan las principales propiedades de los circuitos de una matroide.

Teorema 2.1.19. *Sea M una matroide. Entonces la colección $\mathcal{C} = \mathcal{C}(M)$ satisface:*

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

(C2) Si $C, D \in \mathcal{C}$ y $C \subseteq D$ entonces $C = D$.

(C3) (Propiedad de eliminación) Si $C, D \in \mathcal{C}$ con $C \neq D$ y $e \in C \cap D$ entonces existe $F \in \mathcal{C}$ tal que $F \subseteq (C \cup D) \setminus e$.

Demostración. Es claro que \mathcal{C} satisface (C1) y (C2). Para probar (C3), tomemos $C, D \in \mathcal{C}$ con $C \neq D$ y $e \in C \cap D$. Supongamos por contradicción que $(C \cup D) \setminus e$ no contiene ningún circuito, es decir, $(C \cup D) \setminus e$ es independiente. Por (C2) sabemos que existe $c \in C \setminus D$. La familia

$$\mathcal{A} = \{J \in \mathcal{I}(M) : C \setminus c \subseteq J \subseteq C \cup D\}$$

es no vacía ya que $C \setminus c \in \mathcal{A}$, luego existe un elemento $I \in \mathcal{A}$ de cardinalidad máxima. Claramente $c \notin I$ y además como D es dependiente entonces existe $d \in D \setminus I$. Como $c \in C \setminus D$ entonces $c \neq d$. Luego

$$|I| \leq |(C \cup D) \setminus \{x, y\}| = |C \cup D| - 2 < |(C \cup D) \setminus e|,$$

por lo que aplicando (I3) llegamos a una contradicción con la maximalidad de $|I|$. \square

De hecho, las anteriores condiciones son también suficientes para que una colección de subconjuntos de E sea el conjunto de circuitos de una matroide, aunque este hecho no lo necesitaremos aquí.

Proposición 2.1.20. *Sea B una base de la matroide M , y sea $e \notin B$. Entonces existe un único circuito contenido en $B \cup e$, que además contiene al elemento e . A este circuito lo llamaremos el circuito fundamental de e sobre B y lo denotaremos por $C(e, B)$.*

Demostración. Como $B \cup e$ es dependiente entonces debe contener un circuito, que debe contener a e ya que B no contiene ningún circuito. Además, si existiera otro circuito en $B \cup e$ de igual forma debería contener al elemento e , por lo que aplicando (C3) tendríamos que B contiene un circuito. \square

Una caracterización que necesitaremos de los circuitos fundamentales es la siguiente.

Proposición 2.1.21. *Sea B una base de la matroide M , y sea $a \notin B$. Entonces $b \in C(a, B)$ si y sólo si $B \setminus b \cup a$ es una base.*

Demostración. Si $b \in C(a, B)$ entonces $B \setminus b \cup a$ no contiene ningún circuito, luego es un conjunto independiente. Además $B \setminus b \cup a$ tiene el mismo tamaño de B , por lo que debe ser una base. De la misma manera, si $B \setminus b \cup a$ es una base entonces no contiene ningún circuito, por lo tanto $b \in C(a, B)$. \square

2.2. Menores

Las siguientes proposiciones nos muestran cómo obtener nuevas matroides “dentro” de otras. A las matroides que se pueden obtener de esta forma a partir de una matroide M las llamaremos *menores de M* .

Proposición 2.2.1. *Sea M una matroide sobre E , y sea $X \subseteq E$. Consideremos la colección*

$$\mathcal{I}_{E \setminus X} = \{I \subseteq E \setminus X : I \in \mathcal{I}(M)\}.$$

Entonces $(E \setminus X, \mathcal{I}_{E \setminus X})$ es una matroide, a la que llamaremos la eliminación de X de la matroide M y la denotaremos por $M \setminus X$. También la llamaremos la restricción de M al conjunto $E \setminus X$, denotada por $M|(E \setminus X)$.

Demostración. La prueba de los axiomas de independencia es directa. \square

Proposición 2.2.2. *Sea M una matroide sobre E , y $X \subseteq E$. Sea B_X una base de X . Si definimos*

$$\mathcal{I}'_{E \setminus X} = \{I \subseteq E \setminus X : I \cup B_X \in \mathcal{I}(M)\}$$

entonces $(E \setminus X, \mathcal{I}'_{E \setminus X})$ es una matroide, que además no depende de la escogencia de la base B_X de X . A esta matroide la llamaremos la contracción de X de la matroide M y la denotaremos M/X .

Demostración. Claramente $\mathcal{I}'_{E \setminus X}$ cumple (I1) e (I2). Para probar (I3) supongamos que $I, J \in \mathcal{I}'_{E \setminus X}$ y $|I| < |J|$. Entonces $I \cup B_X, J \cup B_X \in \mathcal{I}(M)$ y $|I \cup B_X| < |J \cup B_X|$ por lo que existe $j \in (J \cup B_X) \setminus (I \cup B_X) = J \setminus I$ tal que $I \cup j \cup B_X \in \mathcal{I}(M)$, es decir, $I \cup j \in \mathcal{I}'_{E \setminus X}$ como queríamos.

Para ver que esta matroide no depende de la escogencia de B_X , tomemos $Y \subseteq E \setminus X$. Nótese que B_Y es una base de Y en M/X si y sólo si $B_Y \cup B_X$ es una base de $Y \cup X$ en M , por lo que $r_{M/X}(Y) = r_M(Y \cup X) - r_M(X)$, que no depende de la escogencia de B_X . \square

En el caso en que tratemos con conjuntos de un sólo elemento, escribiremos $M \setminus e$, $M|e$ y M/e en vez de $M \setminus \{e\}$, $M|\{e\}$ y $M/\{e\}$ respectivamente.

Resumiremos para mayor claridad la relación entre el rango de M y el de la eliminación, restricción y contracción de algún subconjunto.

Proposición 2.2.3. *Sea M una matroide sobre E , y sea $X \subseteq E$. Entonces para todo $Y \subseteq E \setminus X$*

$$r_{M \setminus X}(Y) = r_{M|(E \setminus X)}(Y) = r_M(Y),$$

y también

$$r_{M/X}(Y) = r_M(Y \cup X) - r_M(X).$$

2.3. Conexidad

Desarrollaremos en esta sección una noción de conexidad para matroides, que generaliza el concepto de 2-conexidad en grafos. Para esto necesitamos probar primero una propiedad de eliminación fuerte para los circuitos de una matroide.

Proposición 2.3.1. *Sea \mathcal{C} la colección de circuitos de una matroide. Si $C, D \in \mathcal{C}$, $e \in C \cap D$ y $f \in C \setminus D$; entonces existe $F \in \mathcal{C}$ tal que $f \in F \subseteq (C \cup D) \setminus e$.*

Demostración. Supongamos por contradicción que esto no se cumple. Tomemos $C, D \in \mathcal{C}$ para los que falla la proposición, tal que $|C \cup D|$ sea mínimo (entre todas las parejas de contraejemplos). Tomemos $e \in C \cap D$ y $f \in C \setminus D$ tal que no existe $F \in \mathcal{C}$ con $f \in F \subseteq (C \cup D) \setminus e$. Aplicando el axioma de eliminación (C3), sabemos que existe $C' \in \mathcal{C}$ tal que $C' \subseteq (C \cup D) \setminus e$. Como $C' \not\subseteq C$ (ya que son circuitos distintos) entonces existe $g \in C' \setminus C$. Además por hipótesis $f \notin C'$, por lo que $C' \cup D \subseteq (C \cup D) \setminus f$ y entonces $|C' \cup D| < |C \cup D|$. Luego C' y D sí satisfacen la proposición, así que como $g \in D \cap C'$ y $e \in D \setminus C'$ entonces existe $D' \in \mathcal{C}$ tal que $e \in D' \subseteq (D \cup C') \setminus g$. De nuevo tenemos que C y D' cumplen la propiedad de eliminación fuerte, ya que $C \cup D' \subseteq (C \cup D) \setminus g$. Como $e \in C \cap D'$ y $f \in C \setminus D'$ entonces existe $F \in \mathcal{C}$ tal que $f \in F \subseteq (C \cup D') \setminus e \subseteq (C \cup D) \setminus e$, lo que es una contradicción. \square

Definición 2.3.2. Sea M una matroide con conjunto base E . Llamaremos $\gamma = \gamma_M$ a la relación binaria sobre E definida por

$$a \gamma b \iff a = b \text{ o existe un circuito de } M \text{ que contiene tanto a } a \text{ como a } b.$$

Teorema 2.3.3. *Sea M una matroide sobre E . Entonces γ es una relación de equivalencia en E .*

Demostración. Claramente γ es reflexiva y simétrica. Para ver que γ es transitiva, tomemos $e, f, g \in E$ distintos tal que $e \gamma f$ y $f \gamma g$. Existen entonces circuitos C_1 y

C_2 tal que $e \in C_1$, $g \in C_2$ y $C_1 \cap C_2 \neq \emptyset$, y escojámoslos de tal forma que $|C_1 \cup C_2|$ sea mínimo entre todas las parejas que cumplen dichas condiciones. Supongamos por contradicción que no existe un circuito que contenga tanto a e como a g , en particular $C_1 \neq C_2$. Tomemos $h \in C_1 \cap C_2$. Por la Proposición 2.3.1 existe un circuito C_3 tal que $e \in C_3 \subseteq (C_1 \cup C_2) \setminus h$. Por hipótesis, $g \notin C_3$. Como $C_3 \not\subseteq C_1$ entonces existe $i \in (C_2 \setminus C_1) \cap C_3$. Aplicando nuevamente la Proposición 2.3.1 a C_2 y C_3 tenemos que existe un circuito C_4 tal que $g \in C_4 \subseteq (C_2 \cup C_3) \setminus i$. Como $C_4 \not\subseteq C_2$ entonces $C_4 \cap (C_3 \setminus C_2) \neq \emptyset$, y por lo tanto $C_4 \cap C_1 \neq \emptyset$. Además $C_1 \cup C_4 \subseteq (C_1 \cup C_2) \setminus i$, por lo que $|C_1 \cup C_4| < |C_1 \cup C_2|$. Pero entonces la existencia de los circuitos C_1 y C_4 contradice la escogencia de C_1 y C_2 , con lo que termina la prueba. \square

Definición 2.3.4. Sea M una matroide con conjunto base E . A las clases de equivalencia de γ las llamaremos *componentes conexas de M* . Si M tiene sólo una componente conexa diremos que M es una *matroide conexa*.

Existen otras maneras equivalentes de definir la relación γ , como veremos a continuación.

Definición 2.3.5. Sea M una matroide sobre E . Si existen $A, B \in \mathcal{B}(M)$, $a \in A \setminus B$ y $b \in B \setminus A$ tal que $A = B \setminus b \cup a$; entonces diremos que (a, b) es un *cambio elemental en M entre las bases A y B* .

Proposición 2.3.6. Sea M una matroide sobre E , y $a, b \in E$. Entonces $a \gamma b$ si y sólo si (a, b) es un cambio elemental (o $a = b$).

Demostración. Si $a \gamma b$ y $a \neq b$, tomemos un circuito C que contenga tanto a a como a b . El conjunto $C \setminus a$ es independiente, por lo que existe una base B que lo contiene. El circuito fundamental $C(a, B)$ es entonces C , por lo que por la Proposición 2.1.21 tenemos que (a, b) es un cambio elemental.

Supongamos ahora que (a, b) es un cambio elemental entre las bases A y B . Por la Proposición 2.1.21 tenemos que $b \in C(a, B)$, luego $a \gamma b$. \square

La razón por la que estamos interesados en la conexidad de una matroide es por su relación con las sumas directas.

Definición 2.3.7. Sean M_1, M_2, \dots, M_k matroides. Llamemos E_i al conjunto base de M_i y $\mathcal{B}_i = \mathcal{B}(M_i)$. Supongamos que los conjuntos E_i son disyuntos dos a dos. Es fácil ver que el conjunto

$$\mathcal{B} = \{B_1 \cup B_2 \cup \dots \cup B_k : B_i \in \mathcal{B}_i\}$$

es la colección de bases de una matroide M sobre $E_1 \cup E_2 \cup \dots \cup E_k$. En este caso diremos que M es la *suma directa de las matroides M_1, M_2, \dots, M_k* y lo denotaremos por $M = M_1 \oplus M_2 \oplus \dots \oplus M_k$.

Proposición 2.3.8. *Sea M una matroide sobre E , y sea $A \subseteq E$. Entonces $M = (M|A) \oplus (M|(E \setminus A))$ si y sólo si A es unión de componentes conexas de M .*

Demostración. Es fácil ver que si $M = (M|A) \oplus (M|(E \setminus A))$ entonces todo cambio elemental en M se da entre dos elementos de A o entre dos elementos de $E \setminus A$, por lo que A es unión de componentes conexas de M .

Supongamos ahora que A es unión de componentes conexas de M . Tomemos B_1 base de $M|A$ y B_2 base de $M|(E \setminus A)$. Mostraremos que $B_1 \cup B_2$ es base de M . Sabemos que existen dos bases B'_1, B'_2 de M tal que $B'_1 \cap A = B_1$ y $B'_2 \cap (E \setminus A) = B_2$, y tomémoslas de tal forma que $k = |B'_1 \setminus B'_2| = |B'_2 \setminus B'_1|$ sea mínimo. Supongamos que $k \neq 0$, es decir, que existe $b_1 \in B'_1 \setminus B'_2$. Aplicando el Teorema 2.1.13 tenemos entonces que existe $b_2 \in B'_2 \setminus B'_1$ tal que $B''_1 = B'_1 \setminus b_1 \cup b_2$ y $B''_2 = B'_2 \setminus b_2 \cup b_1$ son bases de M . Como b y b' están en la misma componente conexa de M entonces ambos están en A o ambos están en $E \setminus A$, así que sin pérdida de generalidad supongamos que están en A . Las bases B'_1 y B''_2 cumplen entonces que $B'_1 \cap A = B_1$ y $B''_2 \cap (E \setminus A) = B_2$, pero además $|B'_1 \setminus B''_2| = |B'_1 \setminus B'_2| - 1$, lo que contradice la escogencia de B'_1 y B'_2 . Hemos mostrado entonces que $k = 0$, y por lo tanto $B'_1 = B'_2 = B_1 \cup B_2$ es una base de M .

Ahora tomemos una base B de M . Mostraremos que B es unión de una base de $M|A$ con una base de $M|(E \setminus A)$. Como $I_1 = B \cap A$ es independiente en $M|A$ entonces está contenido en una base B_1 de $M|A$. De la misma forma $I_2 = B \cap (E \setminus A)$ está contenido en una base B_2 de $M|(E \setminus A)$. Por lo que mostramos antes, $B' = B_1 \cup B_2$ es una base de M , que además contiene a B . Por lo tanto $B = B' = B_1 \cup B_2$ como queríamos. \square

Corolario 2.3.9. *Sea M una matroide con componentes conexas C_1, C_2, \dots, C_k . Entonces*

$$M = M|C_1 \oplus M|C_2 \oplus \dots \oplus M|C_k$$

es la descomposición más fina posible de la matroide M como una suma directa.

Demostración. Nótese que si $M = N_1 \oplus N_2$ entonces las componentes conexas de M son las componentes conexas de N_1 junto con las de N_2 . Por lo tanto en vista de la Proposición 2.3.8 se tiene el resultado. \square

2.4. El polinomio de Tutte

Tal vez la mejor manera de presentar el polinomio de Tutte es a través de la siguiente familia de invariantes.

Definición 2.4.1. Un *invariante de Tutte-Grothendieck* es una función $f : \text{Matroides} \rightarrow R$, donde R es un anillo conmutativo con identidad, con las siguientes propiedades:

1. Si $M \cong N$ entonces $f(M) = f(N)$.
2. Si $e \in M$ no es un coloop ni un loop, entonces $f(M) = f(M \setminus e) + f(M/e)$.
3. Si $e \in M$ es un coloop o un loop, entonces $f(M) = f(M|e)f(M \setminus e)$.

Nótese que el valor de un invariante f de Tutte-Grothendieck queda entonces determinado por su valor en las dos matroides M_{coloop} y M_{loop} que constan de sólo un coloop y de sólo un loop respectivamente, ya que aplicando las propiedades 2 y 3 podemos hallar recursivamente el valor de $f(M)$ para cualquier matroide M sólo en términos de $f(M_{\text{coloop}})$ y $f(M_{\text{loop}})$.

Ejemplo 2.4.2. No es difícil ver que las siguientes funciones son invariantes de Tutte-Grothendieck:

- $b(M)$ = número de bases de M .
- $i(M)$ = número de conjuntos independientes de M .
- $s(M)$ = número de conjuntos generadores de M (es decir, subconjuntos de E que contienen alguna base de M).
- $e(M) = 2^{\text{número de elementos de } M}$.

Definición 2.4.3. Sea M una matroide sobre el conjunto E . El *polinomio de Tutte* de la matroide M es el polinomio en $\mathbb{Z}[x, y]$ definido por

$$T(M; x, y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)} (y-1)^{|A|-r(A)}.$$

El siguiente teorema muestra la gran importancia del polinomio de Tutte.

Teorema 2.4.4. *El polinomio de Tutte es un invariante de Tutte-Grothendieck. Además, se cumple que $T(M_{\text{coloop}}; x, y) = x$ y $T(M_{\text{loop}}; x, y) = y$.*

Demostración. Es rutinario comprobar que $T(M_{\text{coloop}}; x, y) = x$ y $T(M_{\text{loop}}; x, y) = y$. Además es claro que el polinomio de Tutte cumple la propiedad 1 de la Definición 2.4.1. Para comprobar la propiedad 2, supongamos que $e \in M$ no es un loop ni un coloop. Entonces

$$\begin{aligned} T(M \setminus e; x, y) &= \sum_{A \subseteq E \setminus e} (x-1)^{r_{M \setminus e}(E \setminus e) - r_{M \setminus e}(A)} (y-1)^{|A| - r_{M \setminus e}(A)} \\ &= \sum_{e \notin A \subseteq E} (x-1)^{r_M(E \setminus e) - r_M(A)} (y-1)^{|A| - r_M(A)} \\ &= \sum_{e \notin A \subseteq E} (x-1)^{r_M(E) - r_M(A)} (y-1)^{|A| - r_M(A)} \end{aligned}$$

y también

$$\begin{aligned}
T(M/e; x, y) &= \sum_{A \subseteq E \setminus e} (x-1)^{r_{M/e}(E \setminus e) - r_{M/e}(A)} (y-1)^{|A| - r_{M/e}(A)} \\
&= \sum_{A \subseteq E \setminus e} (x-1)^{r_M(E) - r(e) - r_M(A \cup e) + r(e)} (y-1)^{|A| - r_M(A \cup e) + r(e)} \\
&= \sum_{e \notin A \subseteq E} (x-1)^{r_M(E) - r_M(A \cup e)} (y-1)^{|A| + 1 - r_M(A \cup e)} \\
&= \sum_{e \in A' \subseteq E} (x-1)^{r_M(E) - r_M(A')} (y-1)^{|A'| - r_M(A')},
\end{aligned}$$

por lo que $T(M; x, y) = T(M \setminus e; x, y) + T(M/e; x, y)$. De la misma manera, si $e \in M$ es un coloop entonces

$$\begin{aligned}
T(M; x, y) &= \sum_{A \subseteq E} (x-1)^{r_M(E) - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&= \sum_{e \notin A \subseteq E} (x-1)^{r_M(E) - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&\quad + \sum_{e \in A \subseteq E} (x-1)^{r_M(E) - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&= \sum_{e \notin A \subseteq E} (x-1)^{r_M(E \setminus e) + 1 - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&\quad + \sum_{e \in A \subseteq E} (x-1)^{r_M(E \setminus e) + 1 - r_M(A \setminus e) - 1} (y-1)^{|A \setminus e| + 1 - r_M(A \setminus e) - 1} \\
&= (x-1) \sum_{e \notin A \subseteq E} (x-1)^{r_M(E \setminus e) - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&\quad + \sum_{e \in A \subseteq E} (x-1)^{r_M(E \setminus e) - r_M(A \setminus e)} (y-1)^{|A \setminus e| - r_M(A \setminus e)} \\
&= (x-1) \sum_{e \notin A \subseteq E} (x-1)^{r_M(E \setminus e) - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&\quad + \sum_{e \notin A' \subseteq E} (x-1)^{r_M(E \setminus e) - r_M(A')} (y-1)^{|A'| - r_M(A')} \\
&= x \sum_{e \notin A \subseteq E} (x-1)^{r_M(E \setminus e) - r_M(A)} (y-1)^{|A| - r_M(A)} \\
&= x \sum_{e \notin A \subseteq E} (x-1)^{r_{M \setminus e}(E \setminus e) - r_{M \setminus e}(A)} (y-1)^{|A| - r_{M \setminus e}(A)} \\
&= x T(M \setminus e; x, y) \\
&= T(M_{\text{coloop}}; x, y) T(M \setminus e; x, y).
\end{aligned}$$

En el caso en que e sea un loop, un argumento similar muestra que $T(M; x, y) = T(M_{\text{loop}}; x, y) T(M \setminus e; x, y)$, con lo que termina la prueba. \square

El siguiente corolario describe al polinomio de Tutte como el invariante de Tutte-Grothendieck universal.

Corolario 2.4.5. *Sea R es un anillo conmutativo con identidad, y sean $c, l \in R$. Entonces existe un único invariante f de Tutte-Grothendieck tal que $f(M_{\text{coloop}}) = c$ y $f(M_{\text{loop}}) = l$. Además este invariante es una evaluación del polinomio de Tutte, a saber, $f(M) = T(M; c, l)$.*

Demostración. Por el Teorema 2.4.4, la evaluación $T(M; c, l)$ del polinomio de Tutte es un invariante f de Tutte-Grothendieck que cumple que $f(M_{\text{coloop}}) = c$ y $f(M_{\text{loop}}) = l$. Además es el único de éstos, ya que los invariantes de Tutte-Grothendieck están determinados por su valor en M_{coloop} y M_{loop} . \square

Ejemplo 2.4.6. Continuando con el Ejemplo 2.4.2, en vista del Corolario 2.4.5 tenemos que:

- $b(M) =$ número de bases de $M = T(M; 1, 1)$.
- $i(M) =$ número de conjuntos independientes de $M = T(M; 2, 1)$.
- $s(M) =$ número de conjuntos generadores de $M = T(M; 1, 2)$.
- $e(M) = 2^{\text{número de elementos de } M} = T(M; 2, 2)$.

2.4.1. Actividad sobre las bases

La definición que tenemos del polinomio de Tutte no nos permite conocer fácilmente el coeficiente de cada uno de sus monomios. Para lograr esto necesitaremos la siguiente definición.

Definición 2.4.7. Sea M una matroide sobre $[n]$ y B una base de M . Diremos que el elemento $i \in [n] \setminus B$ es *externamente activo sobre B* si $i < j$ para todo $j \in B$ tal que $B \setminus j \cup i$ es una base de M . Análogamente diremos que $i \in B$ es *internamente activo sobre B* si $i < j$ para todo $j \in [n] \setminus B$ tal que $B \setminus i \cup j$ es una base de M . Al conjunto de los elementos externamente activos sobre B lo denotaremos por $E(B) = E_M(B)$, y al de internamente activos sobre B por $I(B) = I_M(B)$. También escribiremos $e(B) = e_M(B) = |E_M(B)|$ e $i(B) = i_M(B) = |I_M(B)|$.

Teorema 2.4.8. *Si M es una matroide sobre $[n]$ entonces*

$$T(M; x, y) = \sum_{B \in \mathcal{B}(M)} x^{i(B)} y^{e(B)}. \quad (2.1)$$

Demostración. Llamemos $T'(M; x, y)$ al polinomio de la derecha en la ecuación (2.1). Es fácil ver que $T'(M_{\text{coloop}}; x, y) = x$ y que $T'(M_{\text{loop}}; x, y) = y$. Probaremos entonces que T' satisface la misma recursión que el polinomio de Tutte, de donde se sigue el teorema.

Tomemos una matroide M sobre $[n]$. Supongamos que n no es un coloop ni un loop, y tomemos una base B de M . Si B contiene a n entonces tomando una base A que no contenga a n y aplicando (B2) tenemos que existe $i < n$ tal que $B \setminus n \cup i$ es una base. De la misma forma, si B no contiene a n entonces tomando una base A que contenga a n y aplicando el Teorema 2.1.13 llegamos a que existe $i < n$ tal que $B \setminus i \cup n$ es una base. Luego n no es externamente activo ni internamente activo sobre ninguna base. Ahora, si B no contiene a n entonces es fácil ver que $E_{M \setminus n}(B) = E_M(B)$ e $I_{M \setminus n}(B) = I_M(B)$. De la misma forma, si B contiene a n entonces $E_{M/n}(B \setminus n) = E_M(B)$ e $I_{M/n}(B \setminus n) = I_M(B)$. Luego

$$\begin{aligned} T'(M; x, y) &= \sum_{B \in \mathcal{B}(M)} x^{i_M(B)} y^{e_M(B)} \\ &= \sum_{n \notin B \in \mathcal{B}(M)} x^{i_M(B)} y^{e_M(B)} + \sum_{n \in B \in \mathcal{B}(M)} x^{i_M(B)} y^{e_M(B)} \\ &= \sum_{B \in \mathcal{B}(M \setminus n)} x^{i_{M \setminus n}(B)} y^{e_{M \setminus n}(B)} + \sum_{B \in \mathcal{B}(M/n)} x^{i_{M/n}(B)} y^{e_{M/n}(B)} \\ &= T'(M \setminus n; x, y) + T'(M/n; x, y). \end{aligned}$$

Si n es un coloop en M , es decir, si n está en todas las bases, directamente de la definición se tiene que n es internamente activo sobre todas las bases y no es externamente activo en ninguna. Además para toda base B se tiene que $E_{M \setminus n}(B \setminus n) = E_M(B)$ e $I_{M \setminus n}(B \setminus n) = I_M(B) \setminus n$, por lo que

$$\begin{aligned} T'(M; x, y) &= \sum_{B \in \mathcal{B}(M)} x^{i_M(B)} y^{e_M(B)} \\ &= \sum_{B \in \mathcal{B}(M \setminus n)} x^{i_{M \setminus n}(B)+1} y^{e_{M \setminus n}(B)} \\ &= x \cdot \sum_{B \in \mathcal{B}(M \setminus n)} x^{i_{M \setminus n}(B)} y^{e_{M \setminus n}(B)} \\ &= x \cdot T'(M \setminus n, x, y). \end{aligned}$$

De manera completamente análoga se puede ver que si n es un loop en M entonces $T'(M; x, y) = y \cdot T'(M \setminus n; x, y)$. \square

Nótese que el anterior teorema es equivalente a que el coeficiente de $x^i y^e$ en el polinomio de Tutte de una matroide M es igual al número de bases de M con i elementos internamente activos y e elementos externamente activos.

Como corolarios inmediatos tenemos los siguientes.

Corolario 2.4.9. *Todos los coeficientes del polinomio de Tutte de una matroide son no negativos.*

Corolario 2.4.10. *Si M es una matroide sobre $[n]$ entonces la suma*

$$\sum_{B \in \mathcal{B}(M)} x^{i(B)} y^{e(B)}$$

es invariante bajo isomorfismo.

Este último resultado es algo sorprendente, ya que un reordenamiento de los elementos de una matroide M puede cambiar drásticamente la actividad sobre cada base.

2.5. Órdenes parciales

Definición 2.5.1. Un *conjunto parcialmente ordenado* u *orden parcial* es un conjunto P junto con una relación binaria \leq que satisface las siguientes tres propiedades:

1. (Reflexividad) Para todo $x \in P$, se tiene que $x \leq x$.
2. (Antisimetría) Para todo $x, y \in P$, si $x \leq y$ y $y \leq x$ entonces $x = y$.
3. (Transitividad) Para todo $x, y, z \in P$, si $x \leq y$ y $y \leq z$ entonces $x \leq z$.

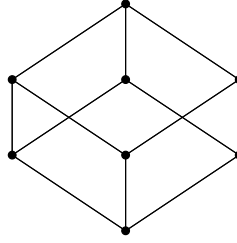
Usaremos las abreviaciones comunes, por ejemplo $x < y$ cuando $x \leq y$ y $x \neq y$, o $y \geq x$ cuando $x \leq y$. Si $x \leq y$ en P entonces el *intervalo (cerrado) $[x, y]$ de P* se define como

$$[x, y] = \{z \in P \mid x \leq z \leq y\}.$$

Un elemento $x \in P$ es un elemento *minimal* (resp. *maximal*) de P si no existe $y \in P$ tal que $y < x$ (resp. $y > x$). Diremos también que $x \in P$ es *mínimo* (resp. *máximo*) si para todo $y \in P$ se cumple que $x \leq y$ (resp. $x \geq y$).

Si x y y son elementos de un orden parcial P , diremos que y *cubre a x* , y lo denotaremos $x \triangleleft y$, si $x < y$ y no existe $z \in P$ tal que $x < z < y$. El *diagrama (de Hasse)* de un orden parcial finito P se obtiene dibujando los elementos de P como puntos, con x mas abajo que y si $x < y$, y dibujando una arista entre x y y si $x \triangleleft y$. En la Figura 2.3 se muestra el diagrama del orden parcial \mathcal{B}_3 que consta de los subconjuntos de $[3]$ ordenados por inclusión.

Una *cadena de longitud k* en un orden parcial P es un conjunto $x_0 < x_1 < \cdots < x_k$ de elementos de P . Diremos que el orden parcial P es *graduado de rango m* si toda cadena maximal en P tiene longitud m .

Figura 2.3: Diagrama del orden parcial \mathcal{B}_3

Si el intervalo $[x, y]$ del orden parcial P es un orden parcial graduado de rango k , diremos que la *longitud del intervalo* $[x, y]$, denotada por $l(x, y)$, es igual a k .

2.5.1. La función de Möbius

Un orden parcial P es *localmente finito* si todo intervalo $[x, y]$ de P es finito. Denotaremos por $\text{Int}(P)$ al conjunto de todos los intervalos (cerrados) de P . Simplificando la notación, para cualquier función $f : \text{Int}(P) \rightarrow \mathbb{Z}$ escribiremos $f(x, y)$ en vez de $f([x, y])$.

Definición 2.5.2. Sea P un orden parcial localmente finito. La función $\mu = \mu_P : \text{Int}(P) \rightarrow \mathbb{Z}$, llamada la *función de Möbius de P* , se define recursivamente de la siguiente manera:

$$\begin{aligned} \mu(x, x) &= 1, \text{ para todo } x \in P \\ \mu(x, y) &= - \sum_{x < z < y} \mu(x, z), \text{ para todo } x < y \text{ en } P. \end{aligned}$$

Nótese que esta última condición es equivalente a

$$\sum_{x \leq z \leq y} \mu(x, z) = 0, \text{ para todo } x < y \text{ en } P.$$

Desarrollaremos un poco la teoría de álgebras de incidencia para una mejor comprensión de esta función.

Sea K un campo. Si P es un orden parcial localmente finito, llamaremos $\mathcal{J}(P) = \mathcal{J}(P, K)$ al espacio vectorial de todas las funciones $f : \text{Int}(P) \rightarrow K$. De nuevo para simplificar la notación, si $f \in \mathcal{J}(P)$ escribiremos $f(x, y)$ en vez de $f([x, y])$. Podemos considerar de manera natural a la función $\mu = \mu_P$ como un elemento de $\mathcal{J}(P)$. Ahora, para $f, g \in \mathcal{J}(P)$ definamos el producto (o convolución) $fg \in \mathcal{J}(P)$ de la siguiente manera:

$$fg(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y).$$

Es fácil ver que este producto hace de $\mathcal{J}(P)$ un álgebra asociativa, con identidad multiplicativa $\delta \in \mathcal{J}(P)$ (llamada la *función δ de Kronecker*) definida por

$$\delta(x, y) = \begin{cases} 1, & \text{si } x = y \\ 0, & \text{si } x < y. \end{cases}$$

Proposición 2.5.3. *Sea $f \in \mathcal{J}(P)$. Entonces las siguientes condiciones son equivalentes:*

- (a) *f tiene inverso por la derecha.*
- (b) *f tiene inverso por la izquierda.*
- (c) *f es invertible (es decir, f tiene un inverso por ambos lados).*
- (d) *$f(x, x) \neq 0$ para todo $x \in P$.*

Demostración. Supongamos que f tiene inverso por la derecha, es decir, existe $g \in \mathcal{J}(P)$ tal que $fg = \delta$ en $\mathcal{J}(P)$. Esto es equivalente a

$$f(x, x)g(x, x) = 1, \text{ para todo } x \in P,$$

y

$$g(x, y) = -f(x, x)^{-1} \sum_{x < z \leq y} f(x, z)g(z, y), \text{ para todo } x < y \text{ en } P.$$

Luego f tiene inverso por la derecha si y solo si $f(x, x) \neq 0$ para todo $x \in P$. De la misma forma podemos ver que f tiene inverso por la izquierda si y solo si $f(x, x) \neq 0$ para todo $x \in P$, y por lo tanto, si y solo si f tiene inverso por la derecha. Pero si f tiene inverso por la izquierda y por la derecha entonces estos deben ser iguales, por lo que f es invertible. \square

La *función zeta* $\zeta \in \mathcal{J}(P)$ se define como $\zeta(x, y) = 1$ para todo $x \leq y$ en P . Nótese que la definición de la función μ (Definición 2.5.2) expresa simplemente la relación $\mu\zeta = \delta$ en $\mathcal{J}(P)$. Por la proposición anterior, esto implica que ζ es invertible y que $\zeta^{-1} = \mu$. En particular, $\zeta\mu = \delta$ y por lo tanto

$$\sum_{x \leq z \leq y} \mu(z, y) = 0, \text{ para todo } x < y \text{ en } P.$$

Luego una definición equivalente de la función de Möbius es:

$$\begin{aligned} \mu(x, x) &= 1, \text{ para todo } x \in P \\ \mu(x, y) &= - \sum_{x < z \leq y} \mu(z, y), \text{ para todo } x < y \text{ en } P. \end{aligned}$$

Capítulo 3

Politopos matroidales

El propósito de este capítulo es desarrollar los resultados básicos sobre los politopos matroidales y brindar al lector cierta familiaridad con ellos. Aunque daremos las definiciones principales (más que todo para fijar la notación), se asumirá que el lector tiene conocimiento de los resultados básicos sobre politopos convexos. Una excelente introducción al tema se puede encontrar en [15].

En la primera sección del capítulo daremos la definición de politopo matroidal y también algunos ejemplos. En la segunda parte investigaremos la dimensión de estos politopos. En la tercera parte estudiaremos mejor las caras de los politopos matroidales, en particular sus vértices y aristas. Demostraremos el importante teorema de Gelfand, Goresky, MacPherson y Serganova que caracteriza dichos politopos en términos de sus aristas. Finalmente, en la última parte encontraremos una descripción de los politopos matroidales en términos de desigualdades.

3.1. Definición

Definición 3.1.1. Sea M una matroide sobre $[n]$. Si $A \subseteq [n]$ entonces al punto en \mathbb{R}^n

$$v_A = \sum_{i \in A} e_i$$

lo llamaremos el *vector característico de A* , donde e_i es el i -ésimo vector en la base canónica de \mathbb{R}^n . El *politopo asociado a la matroide M* está definido por

$$\Gamma(M) = \text{conv} \{v_B : B \in \mathcal{B}(M)\},$$

donde

$$\text{conv} \{v_1, v_2, \dots, v_k\} = \left\{ \sum_{i=1}^k \lambda_i v_i : \lambda_i \geq 0 \text{ para todo } i, \text{ y } \sum_{i=1}^k \lambda_i = 1 \right\},$$

o equivalentemente, $\text{conv}\{v_1, v_2, \dots, v_k\}$ es el mínimo conjunto convexo que contiene a los puntos v_1, v_2, \dots, v_k . A $\Gamma(M)$ también lo llamaremos el *politopo de M* , y diremos que es un *politopo matroidal*.

Para matroides con conjunto base E distinto de $[n]$, su politopo asociado se define de igual forma después de una identificación entre E y $[n]$. Aunque dos identificaciones distintas no dan lugar a politopos idénticos, sí resultan ser politopos isométricos.

Ejemplo 3.1.2. Tomemos $M = U_{1,3}$. El conjunto de bases de M es $\{\{1\}, \{2\}, \{3\}\}$, por lo que $\Gamma(M) = \text{conv}\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. En la Figura 3.1 se muestra el politopo $\Gamma(M)$.

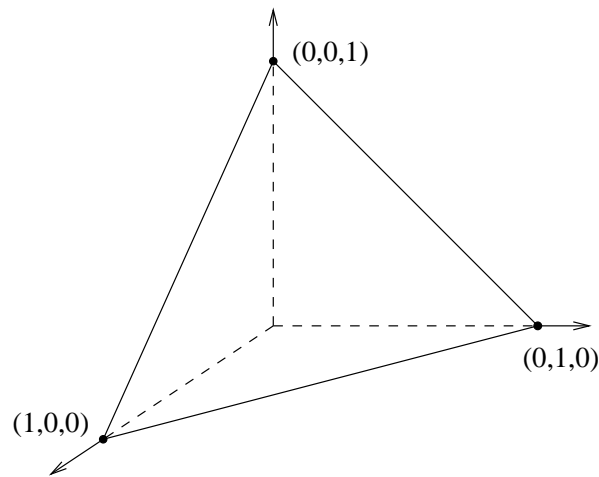


Figura 3.1: Politopo de la matroide $U_{1,3}$

Un ejemplo que nos será mucho más útil es el siguiente.

Ejemplo 3.1.3. Sea $M = U_{2,4}$. Para simplificar la notación, escribiremos vectores característicos sin paréntesis ni comas. Entonces

$$\Gamma(M) = \text{conv}\{1100, 1010, 1001, 0110, 0101, 0011\}.$$

Aunque este politopo vive en \mathbb{R}^4 , en realidad está contenido dentro del subespacio afín 3-dimensional dado por $x_1 + x_2 + x_3 + x_4 = 2$. En la Figura 3.2 se muestra este subespacio y adentro el octaedro $\Gamma(M)$.

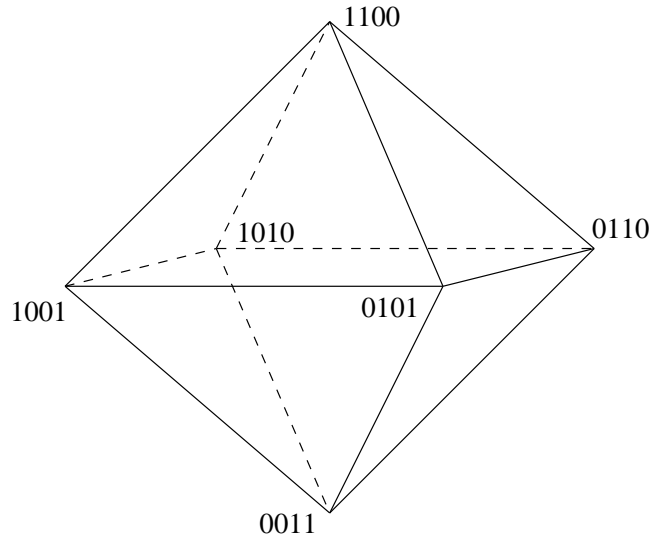


Figura 3.2: $\Gamma(U_{2,4})$ en el subespacio afín $x_1 + x_2 + x_3 + x_4 = 2$ de \mathbb{R}^4

3.2. Dimensión

Definición 3.2.1. Sea P un polítopo con vértices v_1, v_2, \dots, v_k . Denotaremos

$$\text{af}(P) = \left\{ \sum_{i=1}^k \lambda_i v_i : \sum_{i=1}^k \lambda_i = 1 \right\},$$

y lo llamaremos el *espacio ambiente de P* . Es fácil ver que $\text{af}(P)$ es el mínimo subespacio afín que contiene a P . La *dimensión de P* , denotada por $\dim(P)$, es la dimensión del subespacio afín $\text{af}(P)$.

Ejemplo 3.2.2. Continuando con los ejemplos del final de la sección anterior, el espacio $\text{af}(\Gamma(U_{1,3}))$ es el plano definido por $x_1 + x_2 + x_3 = 1$, por lo que $\dim(\Gamma(U_{1,3}))$ es 2. De la misma forma, $\Gamma(U_{2,4})$ es un polítopo 3-dimensional ya que $\text{af}(\Gamma(U_{2,4}))$ es el subespacio afín definido por $x_1 + x_2 + x_3 + x_4 = 2$.

Estamos interesados en determinar la dimensión del polítopo de una matroide M de una manera sencilla a partir de M . Para esto calcularemos primero el espacio ambiente de estos polítopos.

La siguiente definición nos permitirá simplificar la notación en el resto del trabajo.

Definición 3.2.3. Si $A \subseteq [n]$ y s es un entero no negativo, denotaremos por $H_{A,s}$ al hiperplano definido por $\sum_{i \in A} x_i = s$, y por $H_{A,s}^+$ y $H_{A,s}^-$ a los semiespacios cerrados definidos por $\sum_{i \in A} x_i \geq s$ y $\sum_{i \in A} x_i \leq s$ respectivamente.

Lema 3.2.4. Sea M una matroide conexa sobre $[n]$. Entonces $\text{af}(\Gamma(M)) = H_{[n],r(M)}$.

Demostración. Como todos los vértices de $\Gamma(M)$ están en $H_{[n],r(M)}$ entonces $\Gamma(M) \subseteq H_{[n],r(M)}$. En particular, tenemos que $\dim(\Gamma(M)) \leq n - 1$. Tomemos ahora $i, j \in [n]$. Como M es conexa sabemos que (i, j) es un cambio elemental en M , digamos entre las bases B_1 y B_2 . Ya que $\Gamma(M)$ contiene a los puntos v_{B_1} y v_{B_2} entonces $\text{af}(\Gamma(M))$ contiene la recta determinada por ellos, que tiene vector director $v_{B_1} - v_{B_2} = e_i - e_j$. Como esto pasa para toda pareja (i, j) entonces $\text{af}(\Gamma(M))$ contiene una traslación del subespacio

$$\text{gen} \{e_i - e_j : i, j \in [n]\},$$

que tiene dimensión $n - 1$. Luego $\dim(\Gamma(M)) = n - 1$, por lo que se da la igualdad entre $\text{af}(\Gamma(M))$ y $H_{[n],r(M)}$. \square

Teorema 3.2.5. *Sea M una matroide sobre $[n]$. Supongamos que M tiene componentes conexas C_1, C_2, \dots, C_m . Entonces*

$$\text{af}(\Gamma(M)) = \bigcap_{i=1}^m H_{C_i, r_M(C_i)}. \quad (3.1)$$

Demostración. Nótese que si N_1 y N_2 son matroides con conjuntos base disjuntos entonces $\Gamma(N_1 \oplus N_2) = \Gamma(N_1) \times \Gamma(N_2)$. Luego

$$\begin{aligned} \text{af}(\Gamma(M)) &= \text{af}(\Gamma(M|C_1 \oplus M|C_2 \oplus \dots \oplus M|C_m)) \\ &= \text{af}(\Gamma(M|C_1) \times \Gamma(M|C_2) \times \dots \times \Gamma(M|C_m)) \\ &= \text{af}(\Gamma(M|C_1)) \times \text{af}(\Gamma(M|C_2)) \times \dots \times \text{af}(\Gamma(M|C_m)), \end{aligned}$$

por lo que por el Lema 3.2.4 tenemos el resultado buscado. \square

Corolario 3.2.6. *Sea M una matroide sobre E con m componentes conexas. Entonces $\dim(\Gamma(M)) = |E| - m$.*

Demostración. Por el Teorema 3.2.5 sabemos que $\text{af}(\Gamma(M)) = \bigcap_{i=1}^m H_{C_i, r_M(C_i)}$, donde C_1, C_2, \dots, C_m son las componentes conexas de M . Como esta es una intersección de m hiperplanos independientes (sus vectores normales son independientes), entonces $\dim(\Gamma(M)) = |E| - m$. \square

3.3. Caras

Definición 3.3.1. Sea P un politopo. Un *hiperplano de soporte para P* es un hiperplano H que intersecta a P , tal que P está contenido en alguno de los dos semiespacios cerrados que determina H . Diremos que F es una *cara de P* si F es la intersección de P con algún hiperplano de soporte. Por convención, también permitiremos que P sea una cara de P .

A las caras de dimensión 0 las llamaremos *vértices* y a las de dimensión 1 *aristas*. A las caras propias de P maximales respecto a la inclusión las llamaremos simplemente *caras maximales*.

Determinar los vértices del politopo de una matroide es bastante sencillo.

Proposición 3.3.2. *Sea M una matroide. Entonces el conjunto de vértices del politopo $\Gamma = \Gamma(M)$ es $V(M) = \{v_B : B \in \mathcal{B}(M)\}$.*

Demostración. De la definición es fácil ver que los vértices de Γ son de la forma v_B con $B \in \mathcal{B}(M)$. Para ver que todos los puntos de esta forma efectivamente son vértices de Γ , nótese que si $B \in \mathcal{B}(M)$ entonces el hiperplano $H = H_{B,r(M)}$ es un hiperplano de soporte para Γ . Además, como v_B es el único punto de $V(M)$ en H , entonces la cara $\Gamma \cap H$ de Γ es el punto v_B . \square

Las aristas del politopo de una matroide M también se pueden determinar de manera sencilla a partir de M . De hecho, el siguiente teorema [5] caracteriza los politopos matroidales en términos de sus aristas.

Teorema 3.3.3. *Sea \mathcal{B} una colección no vacía de subconjuntos de $[n]$. Consideremos el politopo $P_{\mathcal{B}} = \text{conv}\{v_B : B \in \mathcal{B}\}$. Entonces \mathcal{B} es la colección de bases de una matroide sobre $[n]$ si y sólo si todas las aristas de $P_{\mathcal{B}}$ son de la forma $e_i - e_j$ con $i, j \in [n]$.*

Demostración. Supongamos primero que \mathcal{B} es la colección de bases de una matroide M sobre $[n]$. Tomemos una arista l de $P_{\mathcal{B}} = \Gamma(M)$ con vértices v_A y v_B , determinada por un hiperplano de soporte H . Como A y B son distintos y del mismo tamaño, entonces existe $a \in A \setminus B$. Aplicando el Teorema 2.1.13, sabemos que existe $b \in B \setminus A$ tal que $A' = A \setminus a \cup b$ y $B' = B \setminus b \cup a$ son bases de M . Como $v_{A'} = v_A - (e_a - e_b)$ y $v_{B'} = v_B + (e_a - e_b)$ entonces $v_{A'}$ y $v_{B'}$ están ambos sobre H , ya que si no, estarían a distintos lados de H contradiciendo que H es un hiperplano de soporte. Pero como H sólo contiene a los vértices v_A y v_B , tenemos entonces que $A' = B$ y $B' = A$, por lo que la arista l es de la forma buscada.

Para la otra implicación, asumamos que todas las aristas de $P_{\mathcal{B}}$ son de la forma $e_i - e_j$. Probaremos que \mathcal{B} cumple la propiedad de intercambio (B2) del Teorema 2.1.11. Supongamos que $A, B \in \mathcal{B}$ y $a \in A \setminus B$. Sabemos que todo el politopo $P_{\mathcal{B}}$, en particular el punto v_B , está dentro del cono con vértice en v_A generado por las aristas adyacentes a v_A . Luego, si las aristas adyacentes a v_A son $e_{b_i} - e_{a_i}$ con $i \in [m]$, tenemos que

$$v_B = v_A + \sum_{i=1}^m \lambda_i (e_{b_i} - e_{a_i}),$$

donde los λ_i son todos positivos. Entonces

$$v = v_B - v_A = \sum_{i=1}^m \lambda_i (e_{b_i} - e_{a_i}).$$

Nótese que los elementos b_i no están en A mientras que los a_i sí, por lo que en esta suma no se cancelan términos. Como $a \in A \setminus B$ entonces la a -ésima coordenada de v es -1 . Luego, existe $j \in [m]$ tal que $\lambda_j \neq 0$ y $a_j = a$. Pero entonces la b_j -ésima coordenada de v es positiva y por lo tanto igual a 1, lo que quiere decir que $b_j \in B \setminus A$. Finalmente, como el punto $w = v_A + (e_{b_j} - e_a)$ es un vértice de $P_{\mathcal{B}}$ entonces el conjunto $A \setminus a \cup b_j$ está en \mathcal{B} , que era lo que buscábamos. \square

La anterior caracterización tiene como consecuencia inmediata un interesante resultado.

Corolario 3.3.4. *Toda cara de un politopo matroidal es también un politopo matroidal.*

Demostración. Sea M una matroide. Si F es una cara de $\Gamma(M)$ entonces las aristas de F son las aristas de $\Gamma(M)$ que están contenidas en F , por lo que tienen la forma $e_i - e_j$. Luego por el Teorema 3.3.3, F es un politopo matroidal. \square

3.4. Descripción por desigualdades

En esta sección daremos una descripción de los politopos matroidales usando únicamente desigualdades. De paso entenderemos los hiperplanos que intersectan “bien” al politopo de una matroide, resultado que usaremos después.

Lema 3.4.1. *Si M y N son matroides sobre $[n]$ tal que $\mathcal{B}(N) \subseteq \mathcal{B}(M)$ entonces toda componente conexa de N está contenida en una componente conexa de M .*

Demostración. Si $i, j \in [n]$ están en la misma componente conexa de N entonces (i, j) es un cambio elemental en N , luego (i, j) es también un cambio elemental en M y por lo tanto están en la misma componente conexa de M . \square

Teorema 3.4.2. *Sea M una matroide sobre $[n]$, y sea H un hiperplano que intersecta a $\Gamma = \Gamma(M)$ en el politopo de una matroide N , de dimensión $\dim(\Gamma) - 1$. Entonces existe un hiperplano de la forma $H_{A,s}$, donde A es un subconjunto de alguna componente conexa de M y s es un entero no negativo, tal que $H \cap \Gamma = H_{A,s} \cap \Gamma$.*

Demostración. Debido a la dimensión de $\Gamma(N)$ sabemos que N tiene una componente conexa más que M . Por el Lema 3.4.1 sabemos entonces que las componentes conexas

de N son exactamente las mismas que las de M , excepto por una componente C de M que se parte en dos componentes C_1 y C_2 de N .

Supongamos ahora que H está dado por la ecuación $\sum_{i \in [n]} a_i x_i = s$. Primero, nótese que si $j, k \in [n]$ están en la misma componente conexa de N entonces $a_j = a_k$, ya que existen dos bases en N asociadas al cambio elemental (j, k) . Además si C' es una componente conexa de M distinta de C (y por lo tanto también componente conexa de N) entonces Γ está dentro del subespacio $\sum_{i \in C'} x_i = r_M(C')$, por lo que podemos modificar la ecuación de H sin cambiar su intersección con Γ , y llegar a una en la que si $i \notin C$ entonces $a_i = 0$. Es decir, podemos suponer que H está dado por una ecuación de la forma $\sum_{i \in C_1} a x_i + \sum_{j \in C_2} b x_j = s$. Usando ahora que $\sum_{i \in C} x_i = r_M(C)$ se cumple para todos los puntos de Γ , podemos lograr que $b = 0$. Finalmente, después de multiplicar por un escalar, podemos lograr que H sea de la forma $H_{C_1, s}$, con s un entero no negativo (ya que $s = r_N(C_1)$). \square

El anterior teorema nos permite probar de una manera sencilla la siguiente descripción de los politopos matroidales en términos de desigualdades.

Teorema 3.4.3. *Sea M una matroide sobre $[n]$. Entonces*

$$\Gamma(M) = \left\{ x \in [0, 1]^n : \sum_{i \in [n]} x_i = r(M), \text{ y para todo } A \subseteq [n] \sum_{i \in A} x_i \leq r(A) \right\}. \quad (3.2)$$

Demostración. Llamemos P al politopo de la derecha en la ecuación (3.2). Es fácil ver que $\Gamma(M) \subseteq P$, ya que todos los vértices de $\Gamma(M)$ están en P . Para probar la otra inclusión, supongamos que F_1, F_2, \dots, F_m son las caras maximales (propias) de $\Gamma(M)$. Por el Teorema 3.4.2 sabemos que para todo $i \in [m]$ existen $A_i \subseteq [n]$ y s_i tal que $H_{A_i, s_i} \cap \Gamma(M) = F_i$. Podemos suponer que $\Gamma(M)$ se encuentra dentro de H_{A_i, s_i}^- para todo i , si no basta considerar $H_{[n] \setminus A_i, r(M) - r(A_i)}$. Nótese que $s_i = r(A_i)$ para todo $i \in [m]$, ya que H_{A_i, s_i} es un hiperplano de soporte para $\Gamma(M)$. Ahora, como todo politopo es la intersección de su espacio ambiente con algunos semiespacios cerrados que determinen todas sus caras maximales, entonces

$$\Gamma(M) = \text{af}(\Gamma(M)) \cap \bigcap_{i \in [m]} H_{A_i, r(A_i)}^-.$$

Denotemos por C_1, C_2, \dots, C_k a las componentes conexas de M . Como $r(C_1) + r(C_2) +$

$\cdots + r(C_k) = r(M)$, en vista del Teorema 3.2.5 tenemos que

$$\begin{aligned}
 \Gamma(M) &= \bigcap_{j \in [k]} H_{C_j, r(C_j)} \cap \bigcap_{i \in [m]} H_{A_i, r(A_i)}^- \\
 &= H_{[n], r(M)} \cap \bigcap_{j \in [k]} H_{C_j, r(C_j)} \cap \bigcap_{i \in [m]} H_{A_i, r(A_i)}^- \\
 &= H_{[n], r(M)} \cap \bigcap_{j \in [k]} H_{C_j, r(C_j)}^- \cap \bigcap_{i \in [m]} H_{A_i, r(A_i)}^-,
 \end{aligned}$$

de donde es claro que $\Gamma(M) \supseteq P$. □

Capítulo 4

Subdivisiones matroidales

En este capítulo estudiaremos las subdivisiones matroidales desde un punto de vista geométrico. En la primera sección daremos su definición y algunas propiedades básicas que necesitaremos en lo que sigue.

En la segunda parte del capítulo, nos concentraremos en las subdivisiones que se obtienen al cortar con un hiperplano. Investigaremos con cierta profundidad su geometría, y la estructura de los hiperplanos que las generan. También daremos una caracterización combinatoria de estas subdivisiones. Al final presentaremos un ejemplo de una subdivisión que no es obtenida mediante una sucesión de cortes con hiperplanos.

Para terminar, en la tercera sección mostraremos una subdivisión del politopo de la matroide $U_{m,km}$ con matroides de Schubert, que generaliza las subdivisiones de los distintos ejemplos que damos.

Los resultados de este capítulo fueron obtenidos en trabajo conjunto con Alex Fink.

4.1. Generalidades

Definición 4.1.1. Sea M una matroide. Una *subdivisión* del politopo matroidal $\Gamma = \Gamma(M)$ es una colección $S = \{\Gamma_1, \Gamma_2, \dots, \Gamma_k\}$ de politopos de la misma dimensión que Γ (a los que llamaremos las *partes* de la subdivisión) cuya unión es Γ , tal que para cualesquiera $i, j \in [k]$ distintos se tiene que la intersección $\Gamma_i \cap \Gamma_j$ es vacía o es una cara propia tanto de Γ_i como de Γ_j . En el caso en el que todos los politopos en S sean politopos matroidales, diremos que la subdivisión es *matroidal*. Denotaremos por M_i a la matroide tal que $\Gamma_i = \Gamma(M_i)$. Algunas veces abusaremos del lenguaje y diremos que $\{M_1, M_2, \dots, M_k\}$ es una subdivisión de la matroide M . En este trabajo consideraremos únicamente subdivisiones matroidales, por lo que hablaremos simplemente de subdivisiones para referirnos a éstas.

Ejemplo 4.1.2. Tomemos $M = U_{2,4}$. Sean $M_1 = M(G_1)$ y $M_2 = M(G_2)$ las matroides dadas por los grafos de la Figura 4.1. Los politopos $\Gamma_1 = \Gamma(M_1)$ y $\Gamma_2 = \Gamma(M_2)$ forman una subdivisión (matroidal) de $\Gamma = \Gamma(M)$, ya que su unión es todo Γ y su intersección es el politopo $\Gamma_{1,2}$ de la matroide $M_{1,2} = M(G_3)$ (ver Figura 4.1), que es una cara de ambos. En la Figura 4.2 se muestra esta subdivisión. La pirámide superior es Γ_1 y la inferior es Γ_2 , que se intersectan en el cuadrado de la mitad $\Gamma_{1,2}$.

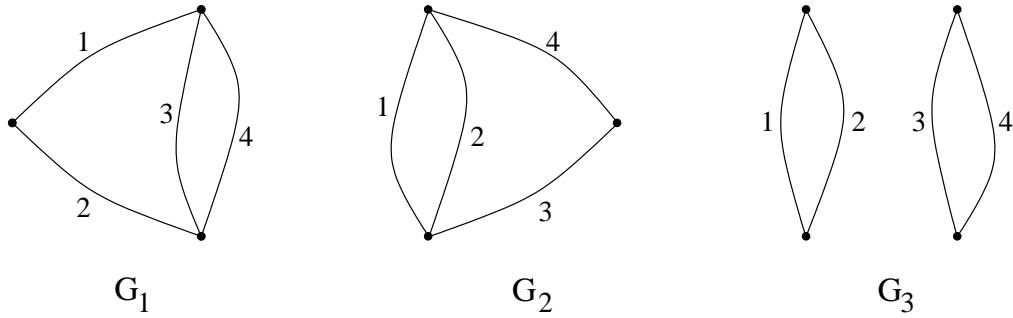


Figura 4.1: Grafos G_1 , G_2 y G_3

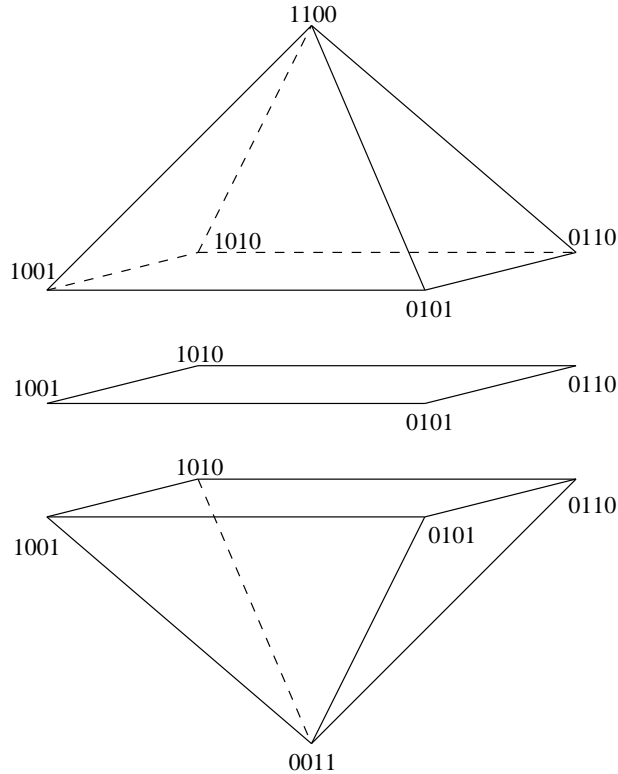


Figura 4.2: Subdivisión de $U_{2,4}$

Desafortunadamente, el anterior ejemplo es el único caso de una subdivisión no trivial

en dimensión menor o igual que tres.

Definición 4.1.3. Sea $S = \{\Gamma_1, \Gamma_2, \dots, \Gamma_k\}$ una subdivisión de Γ , y sea $A \subseteq [k]$. Denotaremos por $\Gamma_{A,S} = \bigcap_{i \in A} \Gamma_i$, tomando por convención que $\Gamma_{\emptyset, S} = \Gamma$. Cuando no haya confusión escribiremos simplemente Γ_A en vez de $\Gamma_{A,S}$. Si $A = \{a_1, a_2, \dots, a_m\}$, a veces escribiremos $\Gamma_{a_1, a_2, \dots, a_m}$ en vez de Γ_A .

Las distintas partes de una subdivisión se intersectan de buena manera, como lo muestra la siguiente proposición.

Proposición 4.1.4. *Sea S una subdivisión de Γ con k partes, y sean $A, B \subseteq [k]$ no vacíos tal que $A \subseteq B$ y $\Gamma_B \neq \emptyset$. Entonces Γ_B es una cara de Γ_A .*

Demostración. Tomemos $a \in A$. Por definición $\Gamma_A \subseteq \Gamma_a$, por lo que

$$\begin{aligned} \Gamma_A &= \Gamma_a \cap \Gamma_A \\ &= \Gamma_a \cap \bigcap_{i \in A} \Gamma_i \\ &= \bigcap_{i \in A} (\Gamma_a \cap \Gamma_i), \end{aligned}$$

que es una intersección de caras de Γ_a y por lo tanto una cara de Γ_a . De la misma forma

$$\Gamma_B = \bigcap_{i \in B} (\Gamma_a \cap \Gamma_i),$$

por lo que Γ_B también es una cara de Γ_a . Finalmente, como $\Gamma_B \subseteq \Gamma_A$ entonces se tiene el resultado buscado. \square

Corolario 4.1.5. *Sea S una subdivisión de Γ con k partes, y sea $A \subseteq [k]$ tal que $\Gamma_A \neq \emptyset$. Entonces Γ_A es el politopo de una matroide, a la que denotaremos M_A .*

Demostración. Esto es claro si $A = \emptyset$. Si por el contrario existe $a \in A$ entonces Γ_A es una cara de $\Gamma_a = \Gamma(M_a)$, y por lo tanto Γ_A es un politopo matroidal. \square

Una de las razones para el gran interés en las subdivisiones matroidales se presenta a continuación.

Definición 4.1.6. Diremos que el politopo Γ es *indescomponible* si no admite ninguna subdivisión no trivial, es decir, una subdivisión con por lo menos dos partes.

Ejemplo 4.1.7. Los politopos asociados a las matroides uniformes $U_{0,n}$ y $U_{n,n}$ son un punto, por lo que son indescomponibles. Los politopos de las matroides $U_{1,n}$ y $U_{n-1,n}$ son símlices, luego cualquier subconjunto propio de sus vértices genera un politopo de menor dimensión y por lo tanto también son politopos indescomponibles.

El siguiente resultado (Lafforgue [6, 7]) es bastante sorprendente. No presentaremos su prueba, ya que usa métodos más avanzados que los aquí expuestos.

Teorema 4.1.8. *Sea m es un entero positivo, \mathbb{F} un campo y M una matroide tal que su politopo $\Gamma(M)$ es indescomponible. Entonces existen finitas matrices A (posiblemente 0) con m filas y entradas en \mathbb{F} (módulo la multiplicación de sus columnas por un escalar o la acción de una matriz en $GL(m, \mathbb{F})$) tal que $M \cong M(A)$.*

4.2. Separaciones por hiperplanos

Así como en el Ejemplo 4.1.2, una gran cantidad de subdivisiones se obtienen al cortar con un hiperplano en dos partes un politopo matroidal. Formalizaremos esto en la siguiente definición.

Definición 4.2.1. Una subdivisión $S = \{\Gamma_1, \Gamma_2\}$ de Γ es una *separación por hiperplano* si existe un hiperplano H (en el espacio $V = \text{af}(\Gamma)$) tal que $\Gamma_1 = \Gamma \cap H^+$ y $\Gamma_2 = \Gamma \cap H^-$, donde H^+ y H^- son los dos semiespacios cerrados en los que H divide a V . En este caso diremos que H induce la subdivisión S .

Proposición 4.2.2. *Sea S una subdivisión de Γ con 2 partes. Entonces S es una separación por hiperplano.*

Demostración. Sea $H = \text{af}(\Gamma_{1,2})$. Como $\Gamma_{1,2}$ es una cara de Γ_1 y de Γ_2 , entonces $H \cap \Gamma_1 = H \cap \Gamma_2 = \Gamma_{1,2}$. Además, como todo segmento entre un punto de Γ_1 y un punto de Γ_2 debe intersectar a $\Gamma_{1,2}$ (si no, no estaría completamente contenido en Γ) entonces H es un hiperplano de $V = \text{af}(\Gamma)$. Finalmente, es fácil ver que Γ_1 y Γ_2 están en distintos lados de H , por lo que S es una separación por hiperplano. \square

El siguiente teorema nos permite caracterizar las separaciones por hiperplanos de una manera más simple.

Teorema 4.2.3. *Sea Γ un politopo matroidal, y sea H un hiperplano que separa a Γ en dos politopos (de la misma dimensión que Γ) P_1 y P_2 . Entonces las siguientes son equivalentes:*

- a) H induce una separación por hiperplano en Γ .
- b) Ambos politopos P_1 y P_2 son politopos matroidales.
- c) Alguno de los politopos P_1 o P_2 es un politopo matroidal.
- d) $\Gamma \cap H$ es un politopo matroidal.

Demostración. Claramente $a) \Rightarrow b) \Rightarrow c)$. Nótese que $\Gamma \cap H$ es cara de P_1 y de P_2 , por lo que $c) \Rightarrow d)$. Además, para probar que $d) \Rightarrow a)$ basta con mostrar que P_1 y P_2 son politopos matroidales.

Supongamos por contradicción que alguno de los dos politopos, digamos P_1 , no es un politopo matroidal. Sea v un vértice de P_1 . Si v está en H entonces v es vértice de $\Gamma \cap H$ (porque $\Gamma \cap H$ es una cara de P_1), y si v no está en H entonces v es un vértice de Γ . En ambos casos v es vértice de un politopo matroidal, por lo que $v \in \{0, 1\}^n$.

Luego debe existir una arista a de P_1 que no es de la forma $e_i - e_j$ (sin embargo, sus dos extremos están en $\{0, 1\}^n$). Esta arista no puede estar contenida completamente en H , porque si no sería una arista del politopo $\Gamma \cap H$. Por lo tanto, si J es un hiperplano de soporte en P_1 que determina la arista a , J es también un hiperplano de soporte en Γ . Como a no es una arista de Γ entonces $J \cap \Gamma$ es una arista de Γ que contiene propiamente a a , pero esto contradice que los extremos de a estén en $\{0, 1\}^n$. \square

Las separaciones por hiperplanos son inducidas por hiperplanos “sencillos”, como lo muestra la siguiente proposición.

Proposición 4.2.4. *Sea M una matroide sobre $[n]$. Entonces toda separación por hiperplano de $\Gamma(M)$ es inducida por un hiperplano de la forma $H_{A,s}$, donde A es un subconjunto de alguna componente conexa de M y s es un entero no negativo.*

Demostración. Supongamos que S es una separación por hiperplano de $\Gamma = \Gamma(M)$ inducida por el hiperplano H . Como $\Gamma_{1,2}$ es la intersección de un hiperplano (que no es hiperplano de soporte) con Γ entonces $\dim(\Gamma_{1,2}) = \dim(\Gamma) - 1$, por lo que por el Teorema 3.4.2 se tiene lo buscado. \square

Como consecuencia de los resultados anteriores tenemos la siguiente caracterización.

Proposición 4.2.5. *Sea M una matroide con conjunto base E . Entonces $\Gamma = \Gamma(M)$ admite una separación por hiperplano si y sólo si existen $A \subseteq [n]$ y s entero no negativo, tal que $r(M) - r(E \setminus A) < s < r(A)$ y el conjunto*

$$\mathcal{B}_{A,s} = \{B \in \mathcal{B}(M) : |B \cap A| = s\}$$

es la colección de bases de una matroide sobre E .

Demostración. En vista del Teorema 4.2.3 y la Proposición 4.2.4, el politopo Γ admite una separación por hiperplano si y sólo si existe un hiperplano (que no es de soporte) de la forma $H_{A,s}$ tal que $\Gamma \cap H_{A,s}$ es un politopo matroidal. Como ninguna arista de Γ cruza el hiperplano $H_{A,s}$, esto es equivalente a que $\mathcal{B}_{A,s}$ es la colección de bases de una matroide sobre E , y que además existen bases B_1 y B_2 de M tal que $|B_1 \cap A| > s$ y

$|B_2 \cap A| < s$. Esto último se traduce en que existen bases B_1 y B_2 tal que $|B_1 \cap A| > s$ y $|B_2 \cap (E \setminus A)| > r(M) - s$, es decir, $r(M) - r(E \setminus A) < s < r(A)$. \square

Nótese que en particular, la proposición anterior implica que si una matroide M sobre E admite una separación por hiperplano entonces existe $A \subseteq E$ tal que $r(A) + r(E \setminus A) \geq r(M) + 2$.

Aunque una subdivisión tenga más de dos partes, es posible que se pueda obtener mediante una sucesión de separaciones por hiperplano. Daremos un nombre a estas subdivisiones.

Definición 4.2.6. Diremos que una subdivisión S de Γ es *generada por separaciones por hiperplanos* si se puede obtener mediante una sucesión de separaciones por hiperplanos, es decir, si el conjunto S se puede obtener comenzando con el conjunto $\{\Gamma\}$ y cambiando varias veces un elemento Γ' del conjunto por las dos partes obtenidas al efectuar una separación por hiperplano en Γ' .

Una gran cantidad de subdivisiones son generadas por separaciones por hiperplanos. De hecho, Lafforgue ha mostrado [7] que toda subdivisión del politopo de una matroide de rango 2 es generada por separaciones por hiperplanos.

El ejemplo más pequeño de una subdivisión que no es generada por separaciones por hiperplanos es el siguiente ([4], Ejemplo 7.13).

Ejemplo 4.2.7. Tomemos $M = U_{3,6}$, y consideremos la matroide de Schubert sobre seis elementos $M_1 = B_{2,4,6}$. Nótese que la permutación $\sigma = \begin{pmatrix} 123456 \\ 345612 \end{pmatrix}$ actúa naturalmente sobre las matroides con conjunto base $[6]$, así que llamemos $M_2 = \sigma M_1$ y $M_3 = \sigma^2 M_1$. En la Sección 4.3 veremos que $\{M_1, M_2, M_3\}$ es una subdivisión de M . Esta subdivisión no es generada por separaciones por hiperplanos, ya que la unión de cualesquiera dos de estas matroide (de sus bases) no es una matroide. Por ejemplo, la colección de bases en $M_1 \cup M_2$ son todos los subconjuntos de $[6]$ con tres elementos excepto $\{1, 5, 6\}$ y $\{2, 5, 6\}$, que no cumple el axioma de intercambio (tomando $A = \{4, 5, 6\}$, $B = \{1, 2, 6\}$ y el elemento $4 \in A \setminus B$).

4.3. Una subdivisión de $U_{m,mk}$

En esta sección estudiaremos una subdivisión de $U_{m,mk}$ con m partes, cada una isomorfa a una matroide de Schubert. Esta subdivisión generaliza las de los ejemplos 4.1.2 y 4.2.7.

Sean m y k enteros positivos, con $k \geq 2$. Llamemos $M = U_{m,mk}$ y $M_1 = B_{k,2k,\dots,mk}$ (con conjunto base $[mk]$). Consideremos la permutación σ de $[mk]$ definida por $\sigma(i) =$

$i + k \pmod{mk}$, y las matroides $M_j = \sigma^{j-1}M_1$ para $j \in [m]$. Llamemos $\Gamma = \Gamma(M)$ y $\Gamma_j = \Gamma(M_j)$. Probaremos que $\{\Gamma_1, \Gamma_2, \dots, \Gamma_m\}$ es una subdivisión de Γ .

Es fácil ver que, como $k \geq 2$, las matroides M_j son conexas y por lo tanto los politopos Γ_j tienen la misma dimensión que Γ .

Para simplificar la notación, si $x \in \mathbb{R}^{mk}$ y $j \in [m]$ llamaremos

$$x^j = \sum_{i=(j-1)k+1}^{jk} x_i,$$

es decir, x^j es la suma de las coordenadas de x en el j -ésimo bloque de k entradas. Por el Teorema 3.4.3 sabemos que el politopo de la matroide $U_{m,mk}$ es simplemente la intersección del hipercubo $[0, 1]^{mk}$ con el hiperplano $H_{[mk],m}$. De la misma forma se puede ver que

$$\Gamma_1 = \left\{ x \in [0, 1]^{mk} : x \in H_{[mk],m}, \text{ y para todo } j \in [m] \sum_{i=j}^m x^i \leq m - j + 1 \right\}.$$

En general, por la construcción de las matroides M_j , tenemos que los politopos Γ_j son el mismo politopo que Γ_1 pero rotando las coordenadas mediante σ^j .

Para ver que $\bigcup_{j \in [m]} \Gamma_j = \Gamma$, tomemos $x \in \Gamma$. Si $l \in [m]$ definamos

$$a_l = \left(\sum_{i=1}^l x^i \right) - l,$$

y tomemos p tal que a_p sea mínimo. Esto quiere decir que

$$\sum_{i=j}^m x^{\sigma^p(i)} \leq m - j + 1$$

para todo $j \in [m]$ y por lo tanto $x \in \Gamma_p$, mostrando que los politopos Γ_j cubren a Γ .

Finalmente, tomemos $i, j \in [m]$ con $i < j$. Sea H el hiperplano definido por

$$\sum_{s=i+1}^j x^s = j - i.$$

Es fácil ver que H es un hiperplano de soporte para Γ_i y para Γ_j , y además $\Gamma_i \cap \Gamma_j = \Gamma_i \cap H = \Gamma_j \cap H$, por lo que $\Gamma_i \cap \Gamma_j$ es una cara tanto de Γ_i como de Γ_j .

Capítulo 5

Funciones bien comportadas bajo subdivisiones

En este capítulo estudiaremos una clase de funciones a las que llamaremos “funciones bien comportadas bajo subdivisiones”. Estas funciones han venido apareciendo en variados contextos como lo son los espacios tropicales lineales y las funciones cuasisimétricas, por lo que trataremos de darles un estudio general y unificado. Su definición precisa y algunos ejemplos se presentan en la primera parte.

En la segunda sección del capítulo estableceremos la equivalencia entre dos nociones de “buen comportamiento”, que aparecen en distintos trabajos como [4] y [11]. Para esto usaremos la maquinaria de la topología algebraica y su relación con la combinatoria.

También utilizaremos esta maquinaria en la sección tres, donde mostraremos el buen comportamiento de una amplia familia de funciones. Esta familia admite una gran cantidad de especializaciones, permitiendo así reunir bajo un mismo marco a la mayoría de las funciones bien comportadas que se han estudiado hasta el momento en la literatura.

En las últimas dos partes del capítulo presentaremos dos funciones bastante finas que se comportan bien bajo subdivisiones. Estas funciones son inyectivas y de mucho contenido combinatorio, por lo que posiblemente serán de gran utilidad en el futuro.

Los resultados de este capítulo se obtuvieron en trabajo conjunto con Alex Fink, bajo la dirección de Federico Ardila. Para una exposición más concreta puede consultarse [1].

Para no repetir en cada resultado, a lo largo de este capítulo fijaremos el entero positivo n .

5.1. Definición y ejemplos

Definición 5.1.1. Sea f una función del conjunto de matroides con conjunto base $[n]$, que denotaremos por $\mathcal{M} = \mathcal{M}_n$, en un grupo abeliano G . Diremos que f se *comporta bien bajo subdivisiones* si para toda matroide $M \in \mathcal{M}$ y toda subdivisión S de $\Gamma = \Gamma(M)$ se tiene que

$$\sum_{\substack{A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|} f(M_A) = 0, \quad (5.1)$$

donde k es el número de partes de la subdivisión S y M_A es como definimos en el Corolario 4.1.5. Nótese que esta última ecuación se puede reescribir como

$$f(M) = \sum_{\substack{\emptyset \neq A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|-1} f(M_A). \quad (5.2)$$

Aunque esta definición parezca un poco extraña, veremos que una gran cantidad de funciones se comporta bien bajo subdivisiones. Intuitivamente, estamos llamando bien comportadas a las funciones que satisfacen cierto principio de inclusión-exclusión en los politopos matroidales.

Ejemplo 5.1.2. La función vol , que le asigna a cada matroide $M \in \mathcal{M}$ el volumen $n-1$ dimensional de su politopo asociado, se comporta bien bajo subdivisiones. De hecho, como $\text{vol}(N)$ es cero si el politopo de N tiene dimensión menor a $n-1$ entonces la ecuación (5.2) se convierte en

$$\text{vol}(M) = \sum_{i \in [k]} \text{vol}(M_i),$$

que claramente es cierta debido a la aditividad del volumen.

Una ejemplo más elaborado es el siguiente.

Proposición 5.1.3. Sea P un punto en \mathbb{R}^n . Llamemos $i_P : \mathcal{M} \rightarrow \mathbb{Z}$ a la función definida por

$$i_P(M) = \begin{cases} 1 & \text{si } P \in \Gamma(M) \\ 0 & \text{si no.} \end{cases}$$

Entonces i_P se comporta bien bajo subdivisiones.

Demostración. Sea S una subdivisión del politopo $\Gamma(M)$ con k partes. Si $P \notin \Gamma(M)$ claramente se cumple la ecuación (5.1), por lo que podemos asumir que $P \in \Gamma(M)$. Definamos

$$B = \{i \in [k] : P \in \Gamma_i\},$$

que es no vacío. Nótese que $P \in \Gamma_B$, por lo que $\Gamma_B \neq \emptyset$. Además $P \in \Gamma_A$ si y sólo si $A \subseteq B$, luego

$$\sum_{\substack{A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|} i_P(M_A) = \sum_{A \subseteq B} (-1)^{|A|} = 0,$$

mostrando el buen comportamiento de i_P . \square

Un corolario interesante es el siguiente.

Corolario 5.1.4. *La función $b : \mathcal{M} \rightarrow \mathbb{Z}$ que le asigna a cada matroide su número de bases se comporta bien bajo subdivisiones.*

Demostración. El número de bases de una matroide M es

$$b(M) = \sum_{P \in \{0,1\}^n} i_P(M),$$

que es una suma de funciones bien comportadas bajo subdivisiones. \square

Más adelante veremos que de hecho todo invariante de Tutte-Grothendieck se comporta bien bajo subdivisiones.

5.2. Una definición equivalente

El propósito de esta sección es desarrollar una formulación equivalente del buen comportamiento bajo subdivisiones de una función. Para esto necesitamos primero algunas definiciones y resultados.

Definición 5.2.1. Sea P un politopo. Llamaremos *frontera de P* a la unión de las caras propias de P , y la denotaremos por ∂P . No es difícil ver que ∂P es también la frontera topológica de P en el espacio $\text{af}(P)$. Al conjunto $\text{int}(P) = P \setminus \partial P$ lo llamaremos el *interior de P* .

Definición 5.2.2. Sea S una subdivisión de Γ con k partes. A las caras de los politopos Γ_i ($i \in [k]$) las llamaremos *caras de la subdivisión S* . Diremos que una cara F de S es una *cara interna de S* si F no está contenida en $\partial \Gamma$. Al conjunto de cara internas de S lo denotaremos por $\text{int}(S)$.

Lema 5.2.3. *Sea S una subdivisión de Γ con k partes, y sea F una cara interna de S . Entonces existe $A \subseteq [k]$ tal que $F = \Gamma_A$.*

Demostración. Probaremos que $F = \Gamma_A$, donde

$$A = \{i \in [k] : F \subseteq \Gamma_i\}.$$

Claramente $F \subseteq \Gamma_A$, así que supongamos por contradicción que $\Gamma_A \supsetneq F$. Sea $a \in A$ tal que F es cara de Γ_a . Nótese que F es una cara de Γ_A , ya que Γ_A es cara de Γ_a . Además, si $i \notin A$ entonces $F \cap \Gamma_i$ es una cara propia de F o es vacío (por ambos ser cara de Γ_a).

Trabajaremos ahora en el espacio $\text{af}(\Gamma)$. La Figura 5.1 ayudará a seguir la demostración. Como F es una cara interna de S sabemos que F contiene un punto x

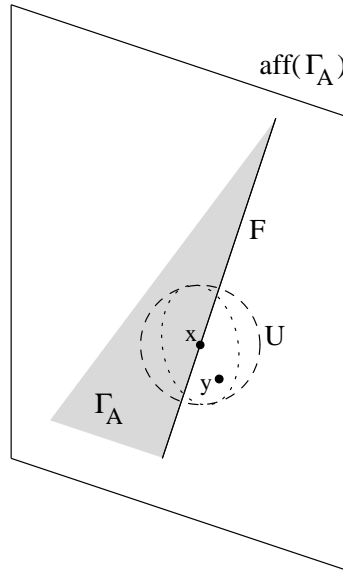


Figura 5.1: Prueba del Lema 5.2.3

interior de Γ , y podemos escogerlo de tal manera que no esté contenido en ninguna cara propia de F . Tomemos U una vecindad de x contenida en Γ que separe a x de los polítopos Γ_i con $i \notin A$, es decir, tal que si $\Gamma_i \cap U \neq \emptyset$ entonces $i \in A$. Tomemos un punto $y \in (\text{af}(\Gamma_A) \cap U) \setminus \Gamma_A$. Como $y \in \Gamma$ entonces debe existir un $l \in [k]$ tal que $y \in \Gamma_l$. Pero entonces $l \in A$ y por lo tanto Γ_A es una cara de Γ_l , lo que es una contradicción debido a que $y \in \text{af}(\Gamma_A) \setminus \Gamma_l$. □

Ahora usaremos la poderosa maquinaria de la topología algebraica. Necesitaremos las siguientes definiciones.

Definición 5.2.4. Un *complejo de celdas regular* es un conjunto (finito) $C = \{\sigma_1, \sigma_2, \dots, \sigma_s\}$ de *celdas* no vacías $\sigma_i \subseteq \mathbb{R}^m$ (para algún entero no negativo m) y disyuntas dos a dos, tal que para todo $i \in [s]$ se cumple lo siguiente:

1. Existe un entero no negativo m_i tal que $\overline{\sigma_i} \approx \mathbb{B}^{m_i}$ y $\overline{\sigma_i} \setminus \sigma_i \approx \mathbb{S}^{m_i-1}$. A m_i lo llamaremos la *dimensión de σ_i* , denotada por $\dim(\sigma_i)$.

2. $\overline{\sigma_i} \setminus \sigma_i$ es unión de algunos σ_j .

Aquí usamos $\overline{\sigma_i}$ para denotar la clausura topológica de σ_i y \approx para homeomorfismo. \mathbb{B}^l y \mathbb{S}^l son la bola cerrada y la esfera unitarias de dimensión l , respectivamente. Llamaremos *espacio subyacente de C* al espacio topológico $\bigcup_{i \in [s]} \sigma_i$, y lo denotaremos por $|C|$.

Definición 5.2.5. Sea C un complejo de celdas regular. Denotemos por c_i al número de celdas de C de dimensión i . La *característica de Euler* de C se define como

$$\chi(C) = \sum_{\sigma \in C} (-1)^{\dim(\sigma)} = \sum_{i \in \mathbb{N}} (-1)^i c_i = c_0 - c_1 + c_2 - c_3 \cdots$$

La característica de Euler *reducida* de C se define como $\tilde{\chi}(C) = \chi(C) - 1$. Un hecho fundamental de la topología algebraica es que la característica de Euler de C depende sólo del tipo de homotopía de $|C|$, y por lo tanto si C' es otro complejo de celdas regular tal que $|C'| \approx |C|$ entonces $\tilde{\chi}(C') = \tilde{\chi}(C)$.

El siguiente ejemplo nos será muy útil después.

Ejemplo 5.2.6. Sea M una matroide, y S una subdivisión de $\Gamma = \Gamma(M)$ con k partes. El conjunto

$$C(S) = \{\text{int}(F) : F \text{ es una cara de } S\}$$

es un complejo de celdas regular, ya que todo politopo P es homeomorfo a $\mathbb{B}^{\dim(P)}$ y su frontera a $\mathbb{S}^{\dim(P)-1}$. El espacio $|C(S)|$ es el politopo Γ .

Definición 5.2.7. Sea C un complejo de celdas regular. Llamaremos $P(C)$ al orden parcial de las celdas de C , con el orden definido por $\sigma_i \leq \sigma_j$ si $\overline{\sigma_i} \subseteq \overline{\sigma_j}$. También denotaremos por $\hat{P}(C)$ al orden parcial $P(C)$ adjuntándole un elemento mínimo $\hat{0}$ y un elemento máximo $\hat{1}$.

Ejemplo 5.2.8. El diagrama de la Figura 5.2 representa un complejo de celdas regular C (las regiones sombreadas representan celdas de dimensión dos), y a la derecha su correspondiente orden parcial $\hat{P}(C)$. El espacio subyacente $|C|$ es claramente homeomorfo a \mathbb{B}^2 . La característica de Euler reducida de C es $\tilde{\chi}(C) = (2 - 3 + 2) - 1 = 0$.

El siguiente es un poderoso teorema ([12], Proposición 3.8.9) que relaciona la topología y la combinatoria de un complejo de celdas regular. No daremos aquí su prueba.

Teorema 5.2.9. *Sea C un complejo de celdas regular. Supongamos que $|C|$ es una variedad, con o sin frontera. Llamemos $P = \hat{P}(C)$. Entonces*

$$\mu_P(x, y) = \begin{cases} \tilde{\chi}(|C|) & \text{si } x = \hat{0} \text{ y } y = \hat{1} \\ 0 & \text{si } x \neq \hat{0}, y = \hat{1} \text{ y la celda } x \text{ está en la frontera de } |C| \\ (-1)^{l(x,y)} & \text{en otro caso.} \end{cases}$$

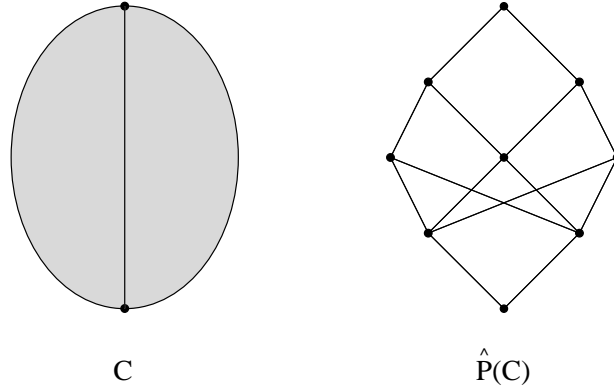


Figura 5.2: Complejo de celdas C y su orden parcial $\hat{P}(C)$

Ahora sí probaremos el teorema principal.

Teorema 5.2.10. *Sea $f : \mathcal{M} \rightarrow G$, donde G es un grupo abeliano. Sea S una subdivisión de $\Gamma = \Gamma(M)$ con k partes. Entonces*

$$\sum_{\substack{\emptyset \neq A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|-1} f(M_A) = \sum_{F \in \text{int}(S)} (-1)^{\dim(\Gamma) - \dim(F)} f(M(F)), \quad (5.3)$$

donde $M(F)$ es la matroide tal que $F = \Gamma(M(F))$.

Demostración. Llamemos

$$H = \{\Gamma_A : \emptyset \neq A \subseteq [k] \text{ y } \Gamma_A \neq \emptyset\},$$

y $P = \hat{P}(C(S))$. En la sumatoria de la izquierda en la ecuación (5.3) estamos sumando $f(M(F))$ sobre todos los elementos $F \in H$, con algunas repeticiones y signos apropiados. Probaremos primero que si $F \in H$ entonces el número de veces que sumamos $f(M(F))$ en esta suma es exactamente $-\mu_P(\text{int}(F), \hat{1})$, es decir,

$$\sum_{\substack{\emptyset \neq A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|-1} f(M_A) = \sum_{F \in H} -\mu_P(\text{int}(F), \hat{1}) f(M(F)).$$

Claramente el número de veces que sumamos $f(M(F))$ en la sumatoria es

$$g(F) = \sum_{\substack{A \subseteq [k] \\ \Gamma_A = F}} (-1)^{|A|-1} = - \sum_{\substack{A \subseteq [k] \\ \Gamma_A = F}} (-1)^{|A|},$$

así que probaremos por inducción en $\dim(\Gamma) - \dim(F)$ que $g(F) = -\mu_P(\text{int}(F), \hat{1})$. Si $\dim(F) = \dim(\Gamma)$ entonces $F = \Gamma_i$ para algún $i \in [k]$, por lo que $g(F) = -(-1)^{|\{i\}|} = 1$. Además, como el intervalo $[\text{int}(\Gamma_i), \hat{1}]$ de P consta de sólo dos elementos entonces

$\mu_P(\text{int}(\Gamma_i), \hat{1}) = -1$ como queríamos. Supongamos ahora que el resultado es cierto para toda $F \in H$ tal que $\dim(F) > m$, y tomemos $G \in H$ tal que $\dim(G) = m$. Para todo $F \in H$ definamos

$$A(F) = \{i \in [k] : F \subseteq \Gamma_i\}.$$

Nótese que $\Gamma_{A(F)} = F$ y además $\Gamma_A \supseteq F$ si y sólo si $A \subseteq A(F)$. Luego

$$\begin{aligned} g(G) &= - \sum_{\substack{A \subseteq [k] \\ \Gamma_A = G}} (-1)^{|A|} \\ &= - \sum_{\substack{A \subseteq A(G) \\ \Gamma_A = G}} (-1)^{|A|} \\ &= - \left(\sum_{A \subseteq A(G)} (-1)^{|A|} - \sum_{\substack{A \subseteq A(G) \\ \Gamma_A \not\supseteq G}} (-1)^{|A|} \right) \\ &= \sum_{\substack{A \subseteq A(G) \\ \Gamma_A \not\supseteq G}} (-1)^{|A|} \\ &= (-1)^{|\emptyset|} + \sum_{\substack{F \in H \\ F \not\supseteq G}} \left(\sum_{\substack{A \subseteq [k] \\ \Gamma_A = F}} (-1)^{|A|} \right) \\ &= \mu_P(\hat{1}, \hat{1}) + \sum_{\substack{F \in H \\ F \not\supseteq G}} \mu_P(\text{int}(F), \hat{1}) \\ &= \sum_{\substack{p \in P \\ p > \text{int}(G)}} \mu_P(p, \hat{1}) \\ &= -\mu_P(\text{int}(G), \hat{1}). \end{aligned}$$

Ahora, en vista del Teorema 5.2.9, tenemos que si $F \in H$ es una cara de S contenida en $\partial\Gamma$ entonces $\mu_P(\text{int}(F), \hat{1}) = 0$, y si F es una cara interna de S entonces $\mu_P(\text{int}(F), \hat{1}) = (-1)^{l(\text{int}(F), \hat{1})} = (-1)^{\dim(\Gamma) - \dim(F) + 1}$. Además por el Lema 5.2.3 sabemos que todas las caras internas de S están en H , por lo que

$$\sum_{F \in H} -\mu_P(\text{int}(F), \hat{1}) f(M(F)) = \sum_{F \in \text{int}(S)} (-1)^{\dim(\Gamma) - \dim(F)} f(M(F)),$$

con lo que termina la prueba. \square

Corolario 5.2.11. *Sea $f : \mathcal{M} \rightarrow G$, donde G es un grupo abeliano. Entonces f se comporta bien bajo subdivisiones si y sólo si para toda matroide $M \in \mathcal{M}$ y toda subdivisión S de $\Gamma = \Gamma(M)$ se tiene que*

$$f(M) = \sum_{F \in \text{int}(S)} (-1)^{\dim(\Gamma) - \dim(F)} f(M(F)). \quad (5.4)$$

5.3. Funciones características

Definición 5.3.1. Sea $X \subseteq \mathbb{R}^n$. Denotaremos por $i_X : \mathcal{M} \rightarrow \mathbb{Z}$ a la función definida por

$$i_X(M) = \begin{cases} 1 & \text{si } \Gamma(M) \cap X \neq \emptyset \\ 0 & \text{si no,} \end{cases}$$

y la llamaremos la *función característica de X* .

Nuestro interés en las funciones características se debe a su buen comportamiento bajo subdivisiones cuando X satisface ciertas condiciones.

Teorema 5.3.2. *Si $X \subseteq \mathbb{R}^n$ es convexo y abierto (en \mathbb{R}^n) entonces i_X se comporta bien bajo subdivisiones.*

Demostración. Sea $M \in \mathcal{M}$ una matroide y S una subdivisión de $\Gamma = \Gamma(M)$. Podemos suponer que $\Gamma \cap X \neq \emptyset$, ya que si no i_X se comporta bien bajo esta subdivisión. También podemos asumir que X es acotado, ya que todos los politopos matroidales se encuentran dentro del cubo $[0, 1]^n$.

Primero reduciremos la prueba al caso en que X es el interior de un politopo (de dimensión n , ya que X es abierto). Por el teorema de separación de Hahn-Banach ([10], Teorema 3.4), para cada cara F de S tal que $F \cap X = \emptyset$ existe un semiespacio abierto A_F que contiene a X y es disyunto de F . Sea

$$X' = \bigcap_{F \cap X = \emptyset} A_F$$

la intersección de estos semiespacios. Entonces $X' \supseteq X$ y además $X' \cap F = \emptyset$ para cada cara F que no intersecciona a X , por lo que $i_{X'}$ e i_X son iguales en todas las matroides de esta subdivisión. Si definimos X'' como la intersección de X' con algún cubo abierto que contenga a Γ , tenemos que X'' es el interior de un politopo y además $i_{X''}$ e i_X son iguales para esta subdivisión.

Podemos entonces asumir que X es el interior de un politopo de dimensión n . Nótese que $X \cap \text{int}(\Gamma)$ es el interior $\text{int}(R)$ de un politopo $R \subseteq \Gamma$. Como X es abierto entonces R y Γ tienen la misma dimensión, luego $R \approx \mathbb{B}^{\dim(\Gamma)}$ y $\partial R \approx \mathbb{S}^{\dim(\Gamma)-1}$. Si F es una cara de la subdivisión S y σ es una cara del politopo R , llamemos $c_{F,\sigma} = \text{int}(F) \cap \text{int}(\sigma)$. Como $c_{F,\sigma}$ es el interior de un politopo entonces su clausura es homeomorfa a una bola cerrada y su frontera es homeomorfa a la esfera de dimensión correspondiente (cuando $c_{F,\sigma}$ es no vacío). Definamos

$$C = \{c_{F,\sigma} : c_{F,\sigma} \neq \emptyset\}$$

$$\partial C = \{c_{F,\sigma} : c_{F,\sigma} \neq \emptyset \text{ y } \sigma \neq R\}.$$

Los elementos de C forman una partición de R , por lo que C es un complejo de celdas regular con espacio subyacente R . Similarmente ∂C es un complejo de celdas regular con espacio subyacente ∂R . Nótese que si F es una cara interna de S , $c_{F,R} = \text{int}(F) \cap \text{int}(R) \neq \emptyset$ si y sólo si $F \cap X \neq \emptyset$, y en este caso $\dim(c_{F,R}) = \dim(F)$.

Tenemos entonces que

$$\begin{aligned}
\sum_{F \in \text{int}(S)} (-1)^{\dim(F)} i_X(M(F)) &= \sum_{\substack{F \in \text{int}(S) \\ F \cap X \neq \emptyset}} (-1)^{\dim(F)} \\
&= \sum_{\substack{F \in \text{int}(S) \\ c_{F,R} \neq \emptyset}} (-1)^{\dim(c_{F,R})} \\
&= \sum_{c_{F,R} \neq \emptyset} (-1)^{\dim(c_{F,R})} \\
&= \sum_{c \in C} (-1)^{\dim(c)} - \sum_{c \in \partial C} (-1)^{\dim(c)} \\
&= \chi(R) - \chi(\partial R) \\
&= 1 - \left(1 + (-1)^{\dim(\Gamma)-1}\right) \\
&= (-1)^{\dim(\Gamma)} \\
&= (-1)^{\dim(\Gamma)} i_X(M),
\end{aligned}$$

así que en vista del Corolario 5.2.11 se tiene lo buscado. \square

Corolario 5.3.3. *Si $X \subseteq \mathbb{R}^n$ es convexo y cerrado (en \mathbb{R}^n) entonces i_X se comporta bien bajo subdivisiones.*

Demostración. Podemos suponer que X es acotado, ya que si C es el hipercubo $[0,1]^n$ entonces $i_X = i_{X \cap C}$ (porque los politopos matroidales están siempre contenidos en C). Ahora, sea S una subdivisión de $\Gamma = \Gamma(M)$ con k partes. Para todo $A \subseteq [k]$ tal que $X \cap \Gamma_A = \emptyset$ se tiene que la distancia $d(X, \Gamma_A)$ es positiva, ya que X es compacto y Γ_A es cerrado. Tomemos un número real positivo ϵ menor que todas estas distancias. Si definimos el conjunto convexo y abierto

$$U = \{x \in \mathbb{R}^n : d(x, X) < \epsilon\},$$

tenemos entonces que para todo $A \subseteq [k]$ se cumple que $X \cap \Gamma_A \neq \emptyset$ si y sólo si $U \cap \Gamma_A \neq \emptyset$. Luego por el Teorema 5.3.2,

$$\sum_{\substack{A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|} i_X(M_A) = \sum_{\substack{A \subseteq [k] \\ \Gamma_A \neq \emptyset}} (-1)^{|A|} i_U(M_A) = 0$$

como se buscaba. \square

Nótese que en particular si $P \subseteq \mathbb{R}^n$ es un politopo entonces i_P se comporta bien bajo subdivisiones.

Las funciones características nos permiten establecer el buen comportamiento de muchas otras funciones, como veremos a continuación.

Proposición 5.3.4. *Si G es un grupo abeliano y $c : \mathcal{M} \rightarrow G$ es una función constante entonces c se comporta bien bajo subdivisiones.*

Demostración. Claramente sólo necesitamos ver que la función constante $\mathbf{1} : \mathcal{M} \rightarrow \mathbb{Z}$ (que asigna 1 a toda matroide) se comporta bien bajo subdivisiones. Para esto, basta notar que si C es el hipercubo $[0, 1]^n$ entonces $\mathbf{1} = i_C$. \square

Proposición 5.3.5. *Si $X \subseteq \mathbb{R}^n$ es convexo, y es abierto o cerrado (en \mathbb{R}^n); entonces la función $\overline{i_X} : \mathcal{M} \rightarrow \mathbb{Z}$ definida por*

$$\overline{i_X}(M) = \begin{cases} 0 & \text{si } \Gamma(M) \cap X \neq \emptyset \\ 1 & \text{si no,} \end{cases}$$

se comporta bien bajo subdivisiones.

Demostración. Nótese que $\overline{i_X} = \mathbf{1} - i_X$, que es una suma de funciones bien comportadas bajo subdivisiones. \square

5.4. Rango

En esta sección probaremos que el rango de cualquier subconjunto A de $[n]$ se comporta bien bajo subdivisiones. La mejor forma de expresar ésto es la siguiente.

Definición 5.4.1. Sea \mathcal{H} el grupo abeliano libre generado por la parejas (A, s) , donde $A \subseteq [n]$ y $s \in \mathbb{N}$. Denotaremos por $R : \mathcal{M} \rightarrow \mathcal{H}$ a la función definida por

$$R(M) = \sum_{A \subseteq [n]} (A, r_M(A)). \quad (5.5)$$

Nótese que la función R está codificando el rango de todos los subconjuntos de $[n]$ y por lo tanto es inyectiva.

Teorema 5.4.2. *La función R se comporta bien bajo subdivisiones.*

Demostración. Debido a la definición de \mathcal{H} , probar el buen comportamiento de R es equivalente a probar que para todo $A \subseteq [n]$ y $s \in \mathbb{N}$, la función $f_{A,s} : \mathcal{M} \rightarrow \mathbb{Z}$ definida

por

$$f_{A,s}(M) = \begin{cases} 1 & \text{si } r_M(A) = s \\ 0 & \text{si no} \end{cases}$$

se comporta bien bajo subdivisiones. Definamos el politopo

$$P_{A,s} = \left\{ x \in [0, 1]^n : \sum_{i \in A} x_i \geq s \right\}.$$

Nótese que una matroide M cumple que $r_M(A) = s$ si y sólo si existe una base B de M tal que $|A \cap B| \geq s$ y no existe ninguna base B tal que $|A \cap B| \geq s + 1$. Esto es equivalente a que $\Gamma(M) \cap P_{A,s} \neq \emptyset$ y además $\Gamma(M) \cap P_{A,s+1} = \emptyset$. Por lo tanto $f_{A,s} = i_{P_{A,s}} - i_{P_{A,s+1}}$, que es suma de funciones bien comportadas. \square

Como corolario, podemos establecer el buen comportamiento de uno de los invariantes más importantes de una matroide.

Corolario 5.4.3. *El polinomio de Tutte, y por lo tanto todo invariante de Tutte-Grothendieck, se comporta bien bajo subdivisiones.*

Demostración. Sea S una subdivisión de $\Gamma = \Gamma(M)$ con k partes. Nótese que todas las matroides M_A , con $A \subseteq [k]$ y $\Gamma_A \neq \emptyset$, tienen el mismo rango $r = r(M)$. El polinomio de Tutte de estas matroides está dado por

$$T(M_A; x, y) = \sum_{B \subseteq [n]} (x-1)^{r-r_{M_A}(B)} (y-1)^{|B|-r_{M_A}(B)},$$

que es la composición del homomorfismo $h_r : \mathcal{H} \rightarrow \mathbb{Z}[x, y]$ dado por

$$h_r(B, s) = (x-1)^{r-s} (y-1)^{|B|-s}$$

con la función R (bien comportada bajo subdivisiones). \square

5.5. Actividad sobre las bases

Veremos que no sólo el polinomio de Tutte se comporta bien bajo subdivisiones, sino también la actividad externa e interna sobre cada base de una matroide.

Definición 5.5.1. Sea \mathcal{G} el grupo abeliano libre generado por la triplas (B, E, I) , donde $B \subseteq [n]$, $E \subseteq [n] \setminus B$ e $I \subseteq B$. Llamaremos $F : \mathcal{M} \rightarrow \mathcal{G}$ a la función definida por

$$F(M) = \sum_{B \in \mathcal{B}(M)} (B, E(B), I(B)), \quad (5.6)$$

donde $E(B)$ y $I(B)$ son los elementos externamente e internamente activos sobre B , respectivamente.

La función F codifica la actividad externa e interna sobre cada una de las bases de la matroide M . En particular, nótese que F es inyectiva.

Mostraremos que la función F se comporta bien bajo subdivisiones. Antes de dar la prueba daremos un ejemplo que ilustrará el poder de este resultado.

Ejemplo 5.5.2. La Tabla 5.1 muestra la actividad externa e interna sobre cada una de las bases de las matroides involucradas en la subdivisión de $U_{3,6}$ descrita en el Ejemplo 4.2.7. Esta información fue calculada usando un programa diseñado por el autor. Para simplificar la notación, no se usan corchetes ni comas en la escritura de los conjuntos. En la tabla se observa el buen comportamiento de la función F : en cada fila, cualquier escogencia de (E, I) aparece el mismo número de veces bajo las columnas de M_{A_S} con $|A|$ par que bajo las columnas de M_{A_S} con $|A|$ impar.

B	M		M_1		M_2		M_3		$M_{1,2}$		$M_{1,3}$		$M_{2,3}$		$M_{1,2,3}$	
	$E(B)$	$I(B)$	$E(B)$	$I(B)$	$E(B)$	$I(B)$	$E(B)$	$I(B)$	$E(B)$	$I(B)$	$E(B)$	$I(B)$	$E(B)$	$I(B)$	$E(B)$	$I(B)$
123	\emptyset	123	\emptyset	123												
124	\emptyset	12	\emptyset	12												
125	\emptyset	12	\emptyset	12			\emptyset	125			\emptyset	125				
126	\emptyset	12	5	12			\emptyset	12			5	12				
134	\emptyset	1	\emptyset	1	\emptyset	134			\emptyset	134						
135	\emptyset	1	\emptyset	1	\emptyset	13	\emptyset	15	\emptyset	13	\emptyset	15	\emptyset	135	\emptyset	135
136	\emptyset	1	5	1	\emptyset	13	\emptyset	1	5	13	5	1	\emptyset	13	5	13
145	\emptyset	1	3	1	\emptyset	1	3	15	3	1	3	15	3	15	3	15
146	\emptyset	1	35	1	\emptyset	1	3	1	35	1	35	1	3	1	35	1
156	\emptyset	1					\emptyset	1								
234	1	\emptyset	1	\emptyset	1	34			1	34						
235	1	\emptyset	1	\emptyset	1	3	1	5	1	3	1	5	1	35	1	35
236	1	\emptyset	15	\emptyset	1	3	1	\emptyset	15	3	15	\emptyset	1	3	15	3
245	1	\emptyset	13	\emptyset	1	\emptyset	13	5	13	\emptyset	13	5	13	5	13	5
246	1	\emptyset	135	\emptyset	1	\emptyset	13	\emptyset	135	\emptyset	135	\emptyset	13	\emptyset	135	\emptyset
256	1	\emptyset					1	\emptyset								
345	12	\emptyset			12	\emptyset										
346	12	\emptyset			12	\emptyset										
356	12	\emptyset			12	3	12	\emptyset					12	3		
456	123	\emptyset			123	\emptyset	123	\emptyset					123	\emptyset		

Tabla 5.1: Actividad externa e interna en la subdivisión de $U_{3,6}$

Ahora sí probaremos el buen comportamiento de la función F . Para mayor claridad separaremos la prueba en varios lemas.

Lema 5.5.3. Sean $B \subseteq [n]$, $E \subseteq [n] \setminus B$ e $I \subseteq B$. Sean

$$S(B, E, I) = \{A \subseteq [n] : v_A - v_B = e_a - e_b \text{ con } a \in E \text{ y } a > b, \text{ o con } b \in I \text{ y } a < b\}$$

y

$$P(B, E, I) = \text{conv} \left\{ \frac{v_A + v_B}{2} : A \in S(B, E, I) \right\}.$$

Entonces para toda matroide $M \in \mathcal{M}$, $\Gamma(M) \cap P(B, E, I) = \emptyset$ si y sólo si B no es una base de M , o B es una base de M con $E \subseteq E(B)$ e $I \subseteq I(B)$.

Para ilustrar un poco, consideremos el caso $n = 4$, $B = \{1, 3\}$, $E = \{2\}$ e $I = \{3\}$. Entonces $S(B, E, I) = \{\{1, 2\}, \{2, 3\}\}$. En la Figura 5.3 se muestra el politopo $P = P(B, E, I)$ dentro del politopo cuyos vértices son los vectores característicos de los subconjuntos de $[4]$ con dos elementos. El politopo de la matroide M_1 con bases $\mathcal{B}_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$ no intersecta a P , debido a que B no es base de M_1 . El politopo de la matroide M_2 con bases $\mathcal{B}_2 = \{\{1, 3\}, \{1, 4\}, \{3, 4\}\}$ tampoco intersecta a P , ya que B es una base de M_2 pero 2 es externamente activo sobre B y 3 es internamente activo sobre B . Por último, el politopo de la matroide M_3 con bases $\mathcal{B}_3 = \{\{1, 3\}, \{2, 3\}, \{3, 4\}\}$ sí intersecta a P , gracias a que B es una base de M_3 y 2 no es externamente activo sobre B .

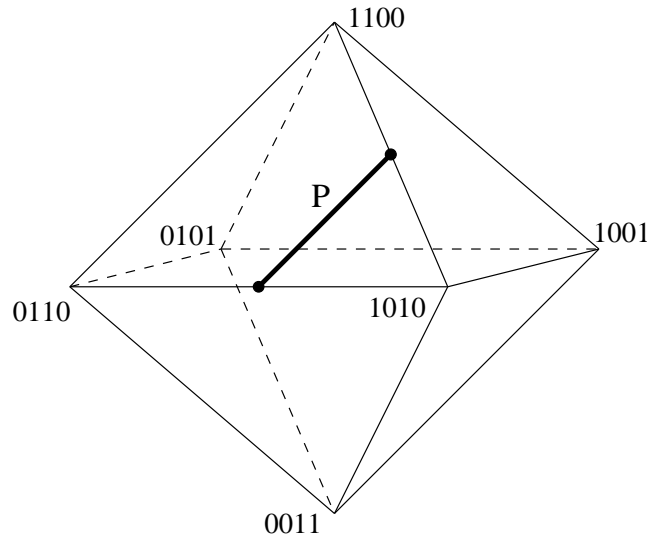


Figura 5.3: Politopo $P = P(B, E, I)$ dentro de $\Gamma(U_{2,4})$

Demostración. Nótese que si B es una base de M y $a \notin B$ entonces

$$\{b \in B : B \setminus b \cup a \in \mathcal{B}(M)\} = \{b \in B : e_a - e_b \text{ es una arista de } \Gamma(M) \text{ adyacente a } v_B\}.$$

Por lo tanto a es externamente activo sobre B si y sólo si no existen aristas en $\Gamma(M)$ adyacentes a v_B de la forma $e_a - e_b$ con $a > b$. De la misma forma, b es internamente activo sobre B si y sólo si no existen aristas en $\Gamma(M)$ adyacentes a v_B de la forma $e_a - e_b$ con $a < b$. Luego, como los vértices de $P(B, E, I)$ son puntos medios de estas aristas, si $\Gamma(M) \cap P(B, E, I) = \emptyset$ y B es una base M entonces $E \subseteq E(B)$ e $I \subseteq I(B)$.

Para la otra implicación supongamos que $\Gamma(M) \cap P(B, E, I) \neq \emptyset$. Nótese primero que como $P(B, E, I)$ está en el hiperplano $x_1 + x_2 + \cdots + x_n = |B|$ y $\Gamma(M)$ está en el hiperplano $x_1 + x_2 + \cdots + x_n = r(M)$ entonces $|B| = r(M)$. Además B debe ser una base de M , ya que si no los vértices v de $P(B, E, I)$ cumplirían que $v_B \cdot v = r(M) - 1/2$, mientras que los vértices w de $\Gamma(M)$ cumplirían $v_B \cdot w \leq r(M) - 1$.

Ahora, sea $q \in \Gamma(M) \cap P(B, E, I)$. Como $q \in \Gamma(M)$ tenemos que q está en el cono con vértice en v_B generado por las aristas de $\Gamma(M)$ adyacentes a v_B . Es decir, si llamamos A_1, A_2, \dots, A_m a las bases adyacentes a B ,

$$q = v_B + \sum_{i=1}^m \lambda_i (v_{A_i} - v_B),$$

donde los λ_i son todos positivos. Si denotamos $e_{c_i} - e_{d_i} = v_{A_i} - v_B$ entonces

$$q = v_B + \sum_{i=1}^m \lambda_i (e_{c_i} - e_{d_i}).$$

Por otro lado, como $q \in P(B, E, I)$ entonces

$$q = \sum_{A \in \mathcal{B}(B, E, I)} \gamma_A \frac{v_A + v_B}{2},$$

donde los γ_A son positivos y suman 1. Igualando estas expresiones tenemos que

$$q = v_B + \sum_{i=1}^m \lambda_i (e_{c_i} - e_{d_i}) = \sum_{A \in \mathcal{B}(B, E, I)} \gamma_A \frac{v_A + v_B}{2}$$

y por lo tanto

$$r = q - v_B = \sum_{i=1}^m \lambda_i (e_{c_i} - e_{d_i}) = \sum_{A \in \mathcal{B}(B, E, I)} \gamma_A \frac{v_A - v_B}{2}.$$

Si $A \in \mathcal{S}(B, E, I)$ llamemos $e_{a_A} - e_{b_A} = v_A - v_B$. Reescribiendo,

$$r = \sum_{i=1}^m \lambda_i (e_{c_i} - e_{d_i}) = \sum_{A \in \mathcal{B}(B, E, I)} \gamma_A \frac{e_{a_A} - e_{b_A}}{2}. \quad (5.7)$$

Nótese que en la ecuación (5.7) los d_i y los b_A son elementos de B mientras que los c_i y los a_A no, por lo que en las sumatorias no se cancelan términos. Digamos que $r = (r_1, r_2, \dots, r_n)$, y sea k el mayor entero tal que r_k es diferente de cero.

Supongamos que $k \notin B$. Por la expresión de la derecha en la ecuación (5.7), teniendo en cuenta la definición de $S(B, E, I)$ tenemos que $k \in E$, y por la expresión de la izquierda sabemos que existe un i tal que $c_i = k$. Pero entonces $e_{c_i} - e_{d_i}$ es una arista de $\Gamma(M)$ adyacente a v_B (y $d_i < c_i$ por la escogencia de k), por lo que k no es externamente activo sobre B . En el caso en que $k \in B$, de manera similar se tiene que $k \in I$ y que existe j tal que $d_j = k$. Entonces $e_{c_i} - e_{d_i}$ es una arista de $\Gamma(M)$ adyacente a v_B , por lo que k no es internamente activo sobre B . En ambos casos concluimos que $B \not\subseteq E(B)$ o $I \not\subseteq I(B)$, con lo que termina la prueba. \square

Lema 5.5.4. *Sea B un subconjunto de $[n]$, y sean $E \subseteq [n] \setminus B$ e $I \subseteq B$. La función $G_{B,E,I} : \mathcal{M} \rightarrow \mathbb{Z}$ definida por*

$$G_{B,E,I}(M) = \begin{cases} 1 & \text{si } B \text{ es una base de } M, E = E(B) \text{ e } I = I(B) \\ 0 & \text{en otro caso.} \end{cases}$$

se comporta bien bajo subdivisiones.

Demostración. Para simplificar la notación, escribiremos $\overline{i_B}$ en vez de $\overline{i_{\{v_B\}}}$. Probaremos que la función $G_{B,E,I}$ es igual a la función

$$G'_{B,E,I}(M) = (-1)^{|E|+|I|} \cdot \sum_{\substack{E \subseteq X \subseteq [n] \\ I \subseteq Y \subseteq [n]}} (-1)^{|X|+|Y|} (\overline{i_{P(B,X,Y)}}(M) - \overline{i_B}(M)), \quad (5.8)$$

que claramente es bien comportada bajo subdivisiones por ser suma de funciones bien comportadas.

Sea $M \in \mathcal{M}$. Si B no es una base de M entonces $\overline{i_B}(M) = 1$, y por el Lema 5.5.3 también $\overline{i_{P(B,X,Y)}}(M) = 1$ para todo X y Y . Entonces $G'_{B,E,I}(M) = 0 = G_{B,E,I}(M)$ como queremos. Si B es una base de M entonces $\overline{i_B}(M) = 0$, y por el Lema 5.5.3 la ecuación (5.8) se vuelve

$$\begin{aligned} G'_{B,E,I}(M) &= (-1)^{|E|+|I|} \cdot \sum_{\substack{E \subseteq X \subseteq E(B) \\ I \subseteq Y \subseteq I(B)}} (-1)^{|X|+|Y|} \\ &= (-1)^{|E|+|I|} \cdot \sum_{E \subseteq X \subseteq E(B)} (-1)^{|X|} \cdot \sum_{I \subseteq Y \subseteq I(B)} (-1)^{|Y|} \\ &= \begin{cases} 1 & \text{si } E = E(B) \text{ e } I = I(B) \\ 0 & \text{en otro caso,} \end{cases} \end{aligned}$$

como buscamos. \square

Teorema 5.5.5. *La función F se comporta bien bajo subdivisiones.*

Demostración. El coeficiente de (B, E, I) en la definición (5.6) está dado precisamente por la función $G_{B,E,I}(M)$, por lo que por el Lema 5.5.4 se tiene el resultado buscado. \square

Ahora podemos dar una prueba distinta para el buen comportamiento del polinomio de Tutte.

Corolario 5.5.6. *El polinomio de Tutte, y por lo tanto todo invariante de Tutte-Grothendieck, se comporta bien bajo subdivisiones.*

Demostración. Por el Teorema 2.4.8 sabemos que

$$T(M; x, y) = \sum_{B \in \mathcal{B}(M)} x^{i(B)} y^{e(B)},$$

que es la composición del homomorfismo $h : \mathcal{G} \rightarrow \mathbb{Z}[x, y]$ dado por $h(B, E, I) = x^{|I|} y^{|E|}$ con la función F . \square

Capítulo 6

Algunas aplicaciones de la lógica

En este capítulo daremos algunas aplicaciones de la lógica a la representabilidad de matroides y a la solubilidad de sistemas de polinomios con coeficientes enteros. Estos dos problemas están bastante relacionados, como mostró por primera vez Vámos en [13].

En la primera parte describiremos la notación y el lenguaje que usaremos a lo largo de todo el capítulo. También introduciremos algunas teorías de la lógica de primer orden con las que trabajaremos.

En la segunda sección estudiaremos la relación entre las distintas características de los campos sobre los que es representable un matroide. La implicación $iii) \Rightarrow i)$ del Teorema 6.2.5 fue probada por primera vez por Rado [9], mientras que la implicación $ii) \Rightarrow iii)$ fue probada por primera vez por Vámos [13], ambas pruebas mediante métodos algebraicos. Usando argumentos muy similares a los de este capítulo, Wagstaff probó [14] que $ii) \Rightarrow iii)$.

En la tercera parte generalizaremos de manera muy natural los resultados del segundo capítulo a la solubilidad de sistemas de polinomios con coeficientes enteros. El Teorema 6.3.1 fue probado primero por Baines y Vámos [3] mediante métodos constructivos basados en la teoría de bases de Gröbner, aunque también presentaron una prueba completamente algebraica.

6.1. Notación

Durante todo este capítulo trabajaremos con la lógica de primer orden sobre el lenguaje de campos $\mathcal{L} = \{+, \cdot, 0, 1\}$. Denotaremos por TC a la teoría consistente de todos los axiomas de campos (sentencias de primer orden), y por $TCAC$ a la teoría TC junto con

el axioma

$$\forall a_0 \dots \forall a_{n-1} \exists x \ x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

para cada entero positivo n . Claramente $TCAC$ es una teoría que axiomatiza los campos algebraicamente cerrados. Si $n \in \mathbb{N}$ llamaremos ϕ_n a la sentencia

$$\underbrace{1 + 1 + \dots + 1}_{n \text{ veces}} = 0.$$

La teoría TC_0 de los campos de característica 0 será simplemente

$$TC_0 = TC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots\}.$$

Tomaremos la teoría $TCAC_p$ de los campos algebraicamente cerrados de característica p como $TCAC_p = TCAC \cup \{\phi_p\}$, y llamaremos también $TCAC_0 = TCAC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots\}$ (la teoría de los campos algebraicamente cerrados de característica cero). Es conocido el hecho que si n es un número primo o n es 0 entonces $TCAC_n$ es una teoría completa, es decir, para cada sentencia ϕ se tiene que $TCAC_n \vdash \phi$ o $TCAC_n \vdash \neg\phi$.

6.2. Representabilidad de matroides

Definición 6.2.1. Diremos que una matroide M es *representable sobre el campo K* si existe una matriz A con entradas en K tal que $M \cong M(A)$ (véase el Ejemplo 2.1.2). En este caso diremos que A es una representación de M sobre K . Nótese que si M es una matroide con n elementos y de rango r , representable sobre K ; mediante un cambio de coordenadas podemos asumir que existe una matriz A de tamaño $r \times n$ con entradas en K tal que $M \cong M(A)$.

Ejemplo 6.2.2. En la Figura 6.1 se muestran dos esquemas que describen a las matroides F_7 y F_7^- . La matroide F_7 , también llamada matroide de Fano, es la matroide sobre $[7]$ cuyas bases son todos los subconjuntos de $[7]$ de tamaño tres tal que sus elementos no están sobre una misma línea en el dibujo de la izquierda de la Figura 6.1 (por ejemplo $\{1, 4, 7\}$ y $\{4, 5, 6\}$ no son bases de F_7). De la misma manera, la matroide F_7^- (o matroide no-Fano) es la matroide sobre $[7]$ cuyas bases son todos los subconjuntos de $[7]$ de tamaño tres tal que sus elementos no están en una misma línea en el dibujo de la derecha de la Figura 6.1.

El hecho de que F_7 y F_7^- sean matroides se sigue de que tomando

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix},$$

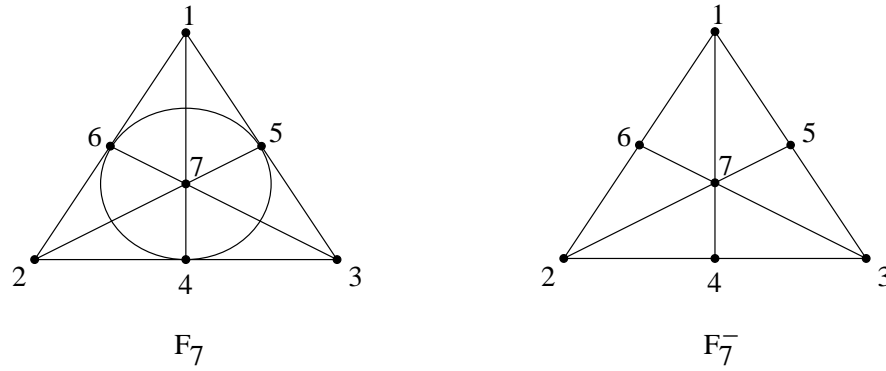


Figura 6.1: Matroides F_7 y F_7^-

si consideramos A con entradas en el campo de dos elementos \mathbb{F}_2 entonces $F_7 \cong M(A)$, y si consideramos A con entradas en el campo de tres elementos \mathbb{F}_3 entonces $F_7^- \cong M(A)$. De hecho, no es difícil ver que la matroide F_7 es representable sólo sobre los campos de característica 2, mientras que la matroide F_7^- es representable sólo sobre los campos de característica distinta de 2.

La conexión entre la lógica y la representabilidad de matroides es la siguiente. Tomemos M una matroide. Nótese que existe una sentencia de primer orden ψ_M tal que para cada campo F , $F \models \psi_M$ si y sólo si M es representable sobre F (ψ_M puede ser una lista de todas las bases y circuitos de M). Por ejemplo, para la matroide $U_{2,3}$ esta sentencia sería

$$\begin{aligned} \exists a_1, a_2, b_1, b_2, c_1, c_2 \text{ tal que } & \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \text{ y } \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \text{ son linealmente dependientes,} \\ & \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \text{ y } \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \text{ son linealmente independientes,} \\ & \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \text{ y } \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \text{ son linealmente independientes} \\ & \text{y } \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \text{ y } \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \text{ son linealmente independientes} \end{aligned}$$

(ser linealmente independientes se puede expresar fácilmente en una fórmula de primer orden).

Para algunas de las pruebas posteriores necesitaremos el siguiente lema.

Lema 6.2.3. *Sea $F \leq K$ una extensión de campos, y sea A una matriz de $m \times n$ con entradas en F (por lo tanto A también puede ser vista como una matriz con entradas en K). Entonces la matroide $M(A)$ es la misma cuando las columnas de A son vistas*

como elementos del espacio vectorial F^m sobre el campo F , que cuando son vistas como elementos del espacio vectorial K^m sobre el campo K .

Demostración. Nótese que las columnas $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ de A son linealmente independientes si y sólo si la matriz reducida por renglones equivalente a la matriz con columnas $v_{i_1}, v_{i_2}, \dots, v_{i_k}$ tiene k pivotes. Como la reducción por renglones puede ser realizada usando sólo coeficientes en F , se tiene el resultado. \square

Corolario 6.2.4. *Sea M una matroide, y sea $F \leq K$ una extensión de campos. Si M es representable sobre F entonces M es representable sobre K .*

El siguiente teorema relaciona las distintas características de los campos sobre los que es representable una matroide.

Teorema 6.2.5. *Sea M una matroide. Entonces las siguientes son equivalentes:*

- i) M es representable sobre un campo de característica p para primos p suficientemente grandes.*
- ii) M es representable sobre un campo de característica p para primos p arbitrariamente grandes.*
- iii) M es representable sobre un campo de característica cero.*

Demostración. *i) \Rightarrow ii).* Claro.

ii) \Rightarrow iii). Supongamos por contradicción que M no es representable sobre ningún campo de característica 0, es decir, $TC_0 \models \neg\psi_M$. Entonces por el teorema de completitud de Gödel tenemos que $TC_0 \vdash \neg\psi_M$. Como las deducciones son finitas, esta deducción de $\neg\psi_M$ usa únicamente finitos de los axiomas de TC_0 . Por lo tanto, existe un $N \in \mathbb{N}$ tal que $TC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots, \neg\phi_N\} \vdash \neg\psi_M$. Pero por validez entonces $TC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots, \neg\phi_N\} \models \neg\psi_M$, es decir, M no es representable sobre ningún campo de característica mayor que N .

iii) \Rightarrow i). Supongamos que M es representable sobre un campo K de característica cero. Por el Corolario 6.2.4, M es representable sobre su clausura algebraica \overline{K} , es decir, $\overline{K} \models \psi_M$. Como $\overline{K} \not\models \neg\psi_M$ entonces $TCAC_0 \not\models \neg\psi_M$, y ya que $TCAC_0$ es una teoría completa tenemos que $TCAC_0 \vdash \psi_M$. Al igual que antes, existe un $N \in \mathbb{N}$ tal que $TCAC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots, \neg\phi_N\} \vdash \psi_M$. Esto es equivalente a que $TCAC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots, \neg\phi_N\} \models \psi_M$, luego M es representable en todos los campos algebraicamente cerrados de característica mayor que N . \square

De manera similar tenemos el siguiente resultado.

Teorema 6.2.6. *Sea M una matroide representable sobre \mathbb{Q} . Entonces M es representable sobre todos los campos de característica p para p suficientemente grande.*

Demostración. Por el Corolario 6.2.3, M es representable sobre todos los campos de característica cero, es decir, $TC_0 \models \psi_M$. Tenemos entonces que $TC_0 \vdash \psi_M$, y por lo tanto existe un $N \in \mathbb{N}$ tal que $TC \cup \{\neg\phi_1, \neg\phi_2, \neg\phi_3, \dots, \neg\phi_N\} \vdash \psi_M$. Esto implica que para cualquier primo p mayor que N , la matroide M es representable sobre todos los campos de característica p . \square

Otro interesante teorema es el siguiente.

Teorema 6.2.7. *Sea M una matroide, y sea n un número primo o cero. Llamemos \mathbb{F}_n al campo primo de característica n . Entonces M es representable sobre un campo de característica n si y sólo si M es representable sobre $\mathbb{F}_n[\alpha]$ para algún α algebraico sobre \mathbb{F}_n .*

Demostración. Supongamos que M es representable sobre un campo K de característica n . De nuevo por el Corolario 6.2.4, M es representable sobre su clausura algebraica \overline{K} y por lo tanto $TCAC_n \vdash \psi_M$. Entonces $TCAC_n \models \psi_M$, es decir, M es representable sobre todos los campos algebraicamente cerrados de característica n . En particular M es representable sobre $\overline{\mathbb{F}_n}$, digamos por una matriz A . Sea F el campo obtenido a partir de \mathbb{F}_n mediante la adjunción de todas las entradas de A . Por el Lema 6.2.4, A es también una representación de M sobre F , luego M es representable sobre F . Ahora, como \mathbb{F}_n es finito o tiene característica cero (y es por lo tanto perfecto) y además F es una extensión finita (y separable) de \mathbb{F}_n , por el teorema del elemento primitivo tenemos que F es una extensión algebraica simple de \mathbb{F}_n , es decir, $F = \mathbb{F}_n[\alpha]$ para algún α algebraico sobre \mathbb{F}_n . \square

6.3. Sistemas de polinomios

Veamos cómo la representabilidad sobre un campo F de una matroide es equivalente a la solubilidad sobre F de un sistema de polinomios con coeficientes en \mathbb{Z} . Supongamos que la matroide M tiene a $[n]$ como conjunto base, y tiene rango r . Tomemos una matriz X de tamaño $r \times n$ cuyas entradas sean todas variables indeterminadas distintas. Para cada $A \subseteq [n]$ llamemos X_A a la matriz de tamaño $r \times |A|$ que tiene como columnas a las columnas de X indexadas por A . Definamos el sistema $P = P_M$ de polinomios con coeficientes enteros de la siguiente manera.

- Para cada circuito C de M y para cada submatriz cuadrada X' de X_C de tamaño $|C| \times |C|$, agreguemos el polinomio $\det(X')$ al sistema P .

- Para cada base B de M , agreguemos el polinomio $w \cdot \det(X_B) - 1$ al sistema P , donde w es una nueva indeterminada.

De esta forma, la matroide M es representable sobre F si y sólo si el sistema P_M tiene solución en F (interpretando sus coeficientes como elementos de F), ya que la primera condición asegura que columnas correspondientes a circuitos de M sean linealmente dependientes, mientras que la segunda asegura que columnas correspondientes a bases de M sean linealmente independientes.

Ahora veremos cómo generalizar los resultados de la sección anterior a la solubilidad de sistemas de polinomios con coeficientes en \mathbb{Z} . Por el teorema de la base de Hilbert, todo sistema de polinomios es equivalente a un sistema finito de polinomios. Ahora, claramente para todo sistema (finito) P de polinomios con coeficientes enteros existe una fórmula ψ_P de primer orden tal que para todo campo F , $F \models \psi_P$ si y sólo si el sistema P tiene solución en F . Esto nos permite generalizar los resultados de la sección anterior a solubilidad de sistemas de polinomios. No daremos las pruebas ya que son exactamente iguales a las de la sección anterior.

Teorema 6.3.1. *Sea P un sistema de polinomios con coeficientes en \mathbb{Z} . Entonces las siguientes son equivalentes:*

- i) P tiene solución sobre un campo de característica p para primos p suficientemente grandes.*
- ii) P tiene solución sobre un campo de característica p para primos p arbitrariamente grandes.*
- iii) P tiene solución sobre un campo de característica cero.*

Teorema 6.3.2. *Sea P un sistema de polinomios con coeficientes en \mathbb{Z} . Si P tiene solución sobre \mathbb{Q} entonces P tiene solución sobre todos los campos de característica p para p suficientemente grande.*

Teorema 6.3.3. *Sea P un sistema de polinomios con coeficientes en \mathbb{Z} , y sea n un número primo o cero. Entonces P tiene solución sobre un campo de característica n si y sólo si P tiene solución sobre $\mathbb{F}_n[\alpha]$ para algún α algebraico sobre \mathbb{F}_n .*

Estos últimos dos resultados pueden ser probados sencillamente de una manera algebraica. Sin embargo, es interesante ver cómo pueden obtenerse mediante aplicaciones bastante simples de la lógica.

Bibliografía

- [1] F. Ardila, A. Fink, F. Rincón, *Valuations for matroid polytope subdivisions*, arXiv:0710.4424, 24 Octubre, 2007.
- [2] F. Ardila, *Matroid Theory (notas de clase)*, San Francisco State University y Universidad de los Andes, 2007.
- [3] R. Baines, P. Vámos, *An Algorithm to Compute the Set of Characteristics of a System of Polynomial Equations over the Integers*, Journal of Symbolic Computation 35, 269-279, 2003.
- [4] L. Billera, N. Jia y V. Reiner, *A Quasisymmetric Function for Matroids*, arXiv:math.CO/0606646, 26 Junio, 2006.
- [5] I.M. Gelfand, R.M. Goresky, R.D. MacPherson, V.V. Serganova, *Combinatorial geometries, convex polyhedra, and Schubert cells*, Adv. Math. 63 (1987) 301-316.
- [6] L. Lafforgue, *Pavages des simplexes, schémas de graphes recollés et compactification des $\mathrm{PGL}_r^{n+1}/\mathrm{PGL}_r$* . Invent. Math. 136 (1999), no. 1, 233-271.
- [7] L. Lafforgue, *Chirurgie des grassmanniennes*. CRM Monograph Series 19, American Mathematical Society, Providence, RI, 2003.
- [8] J. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.
- [9] R. Rado, *Note on independence functions*. Proc. London Math. Soc. (3) 7, 300-320, 1957.
- [10] W. Rudin, *Functional Analysis*. McGraw-Hill, New York, 1973.
- [11] D. Speyer, *Tropical Linear Spaces*, arXiv:math.CO/0410455, 21 Octubre, 2004.
- [12] R. Stanley, *Enumerative Combinatorics*, vol. 1, Cambridge University Press, Cambridge, 1996.

- [13] P. Vámos, *A Necessary and Sufficient Condition for a Matroid to be Linear*. In: Möbius Algebras (Proc. Conf., Univ. Waterloo, Waterloo, ON, 1971), University of Waterloo, Waterloo, ON, pp. 162-169, 1971.
- [14] S. Wagstaff, Jr., *Infinite Matroids*. Trans. of the Amer. Math. Soc., vol. 175, Jan. 1973.
- [15] G. Ziegler, *Lectures on Polytopes*, Graduate Texts in Mathematics 152, Springer-Verlag, New York, 1995.