Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

PESOS DE HAMMING GENERALIZADOS Y NÚMEROS DE BETTI

Autor: Gonzalo Rodríguez Pajares
Tutor: Umberto Martínez Peñas
Año: 2022/2023

Abstract

Generalized Hamming weights of a code C are a set of parameters that generalize its minimum distance. One may also define generalized weights for any matroid M. If M is the matroid associated to a parity check matrix of the code, both definitions coincide. The set of independent sets of a matroid is a simplicial complex, Δ. The aim of this project is, using [JV13] as main reference, to show the relation between the $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of the simplicial complex Δ and the generalized weights of a matroid M. Such Betti numbers can be computed with the graded minimal resolution of the Stanley-Reisner ring associated to Δ.

Resumen

Los pesos de Hamming generalizados de un código C son un conjunto de parámetros del código, que generalizan su distancia mínima. Dada una matroide M, podemos definir también sus pesos generalizados. En caso de que M sea la matroide asociada a una matriz de control H del código C, los pesos de la matroide coinciden con los pesos de Hamming del código. El objetivo de este trabajo es, siguiendo [JV13], demostrar la relación que existe entre los pesos generalizados de una matroide M, y los números de Betti $\mathbb{N}$-graduados del anillo de Stanley-Reisner asociado al complejo simplicial Δ de conjuntos independientes de M. Dichos números de Betti pueden calcularse a través de la resolución graduada minimal del anillo de Stanley-Reisner del complejo.

Índice general

Introducción

El presente trabajo tiene como objetivo estudiar la relación entre los pesos de Hamming generalizados de un código C y los números de Betti $\mathbb{N}$-graduados del anillo de Stanley-Reisner de la matroide M asociada a una matriz de control de C. Este resultado, que ofrece una bonita conexión entre el álgebra combinatoria y la teoría de códigos, fue probado en el año 2013 por Trygve Johnsen y Thomas Verdure (ver [JV13]). Desarrollaremos en esta memoria el marco teórico necesario para llegar a los resultados fundamentales de dicho artículo, recogidos en los teoremas 4.4 y 4.7, y daremos algunos ejemplos de cálculo para códigos concretos.

Este trabajo guarda estrecha relación con la asignatura de *Códigos Correctores*, impartida en el cuarto curso del grado. También son de capital importancia las asignaturas de la rama de álgebra impartidas a lo largo del grado, con especial mención a *Álgebra Lineal I*, *Estructuras algebraicas*, *Ecuaciones Algebraicas* y *Álgebra Conmutativa*. Debido a los contenidos de homología simplicial, la memoria está también relacionada con la asignatura de *Topología Algebraica*.

Los códigos C que vamos a tratar son todos lineales, esto es, son subespacios vectoriales de $\mathbb{F}_q^n$. Para estos códigos se puede definir una métrica, conocida como métrica de Hamming, con la que puede medirse la capacidad correctora del código. Los parámetros fundamentales de un código son $[n, k, d_1, \ldots, d_k]$. El primero de ellos, n, es la longitud de los elementos de C. El segundo, k, es la dimensión de C como $\mathbb{F}_q$-espacio vectorial. El vector $(d_1, \ldots, d_k)$ se conoce como jerarquía de pesos del código. Si denotamos por D_h el conjunto de subespacios vectoriales de C de dimensión h, se define d_h como

$$d_h = \min\{|\chi(\mathrm{D})| : \mathrm{D} \in \mathrm{D}_h\}.$$

Uno de los principales objetivos de la teoría de códigos es, por una parte, el cálculo (eficiente) de los pesos de Hamming generalizados, y por otra, maximizar la distancia mínima d_1 de un código, ya que de ella depende la

capacidad de corrección de errores del código. Los resultados de este trabajo ofrecen un algoritmo de cálculo para los pesos de Hamming, y por tanto para la distancia mínima de C.

El trabajo se divide en 4 capítulos. En el **primer capítulo**, definiremos el concepto de código lineal y estudiaremos sus parámetros fundamentales. Daremos la definición de los pesos de Hamming generalizados para un código y exploraremos algunas de sus propiedades. En el Teorema 1,18 damos una expresión alternativa para el cálculo de los pesos generalizados, que coincidirá con la expresión que usaremos para definir los pesos de una matroide M. Las principales referencias para este capítulo son [PWBJ17] y [Wei91].

El **segundo capítulo** está dedicado a la teoría básica de las matroides. En él, estudiaremos los conjuntos independientes, circuitos, bases y función de rango y nulidad de una matroide M y daremos definiciones equivalentes utilizando cada uno de estos conceptos. En la Sección 2.4 damos algunos ejemplos fundamentales de matroides. La Sección 2.6 explora resultados que luego nos serán tremendamente útiles a la hora de probar los dos teoremas fundamentales de la memoria. Finalmente, en la Sección 2.7 explicamos cómo asociar una matroide a un código. La principal referencia para este capítulo es [Oxl06].

En el **tercer capítulo**, definiremos los conceptos de anillo y módulo graduados. Definiremos para dichos objetos las resoluciones libres y estudiaremos la minimalidad de dichas resoluciones. Daremos la definición de los números de Betti globales, graduados y multigraduados. En la Sección 3.4 definimos los complejos simpliciales y el anillo de Stanley-Reisner asociado a un complejo. Finalizamos el capítulo dando una expresión para los números de Betti multigraduados. Las principales referencias para este capítulo son [MS05] y [Pee10].

En el **cuarto capítulo** estudiamos de qué manera los números de Betti (globales, graduados y multigraduados) de la resolución del anillo de Stanley-Reisner permiten determinar los pesos generalizados de una matroide. El resultado prinicipal es el Teorema 4.7, que afirma que los números de Betti graduados determinan la jerarquía de pesos. En la Sección 4.1, damos algún ejemplo de cálculo y varios ejemplos que permiten ver que el Teorema 4.7 no se cumple para los números de Betti globales. Finalizamos el capítulo dando una caracterización de los códigos MDS. Los resultados fundamentales de este capítulo son el contenido de [JV13], referencia principal que sirve de motivación para la realización del presente trabajo.

Capítulo 1

Códigos lineales

Comenzamos este capítulo introduciendo el concepto de código lineal y estudiando sus parámetros fundamentales. Damos también dos representaciones diferentes para los códigos lineales: en función de una matriz generatriz y en función de una matriz de control. Posteriormente, definiremos los pesos de Hamming generalizados para un código lineal y exploraremos algunas de sus propiedades. En la última sección trataremos brevemente la noción de dualidad de un código.

1.1. Parámetros de un código

Definición 1.1 (Código lineal)**.** Un **código lineal** sobre un cuerpo $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$ para algún $n \geq 1$. Los elementos del códigos se llaman **palabras**. Denotaremos a los códigos lineales con la letra C.

Los parámetros fundamentales que vamos a estudiar para un código lineal son su longitud, su dimensión y su distancia mínima.

La **longitud** de $\mathrm{C} \subset \mathbb{F}_q^n$ se define como n, y se dice que las palabras de C tienen tamaño n. La **dimensión** k de un código C es la dimensión como $\mathbb{F}_q$ espacio vectorial.

Vamos a dar una noción de distancia entre las palabras de un código de la manera siguiente:

Definición 1.2 (Distancia de Hamming)**.** Sean $x = (x_1, ..., x_n)$ e $y = (y_1, ..., y_n)$ elementos de $\mathbb{F}_q^n$. La **distancia de Hamming** entre x e y es

$$d(x, y) = |\{j,\, 1 \leq j \leq n \,|\, x_j - y_j \neq 0\}|.$$

Es decir, es el número de coordenadas distintas entre x e y. La **distancia mínima** de un código es $d = d(\mathrm{C}) = \min\{d(x,y) : x, y \in \mathrm{C}\,,\ x \neq y\}$

Si un código lineal C tiene como parámetros fundamentales n, k y d diremos que es un código lineal de tipo $[n, k, d]$.

Lema 1.3. *La distancia de Hamming definida previamente es una distancia.*

Demostración. Es inmediato ver que $d(x,y) \geq 0$ para todos $x, y \in \mathrm{C}$. Es también claro que $d(x,y) = 0 \iff x = y$ y que $d(x,y) = d(y,x)$. Probemos la desigualdad triangular. Supongamos que $x, y, z \in \mathrm{C}$, si $x_i \neq z_i$ entonces $x_i \neq y_i$ o $y_i \neq z_i$, luego $d(x,z) \leq d(x,y) + d(y,z)$. □

Definición 1.4 (Peso de Hamming)**.** Sea C un código lineal de tipo $[n, k, d]$, el **peso de Hamming** de una palabra $c = (c_1, ..., c_n) \in \mathrm{C}$ es el número de coordenadas no nulas de c, esto es:

$$w(c) = |\{i,\ 1 \leq i \leq n : c_i \neq 0\}|.$$

La distancia mínima de un código está relacionada con los pesos de Hamming de sus palabras en el sentido de la siguiente proposición.

Proposición 1.5. *La distancia mínima d de un código lineal* C *de tipo $[n, k, d]$ es el mínimo peso de Hamming de las palabras del código, es decir,*

$$d = \min\{w(c) : c \in \mathrm{C},\ c \neq 0\}.$$

Demostración. Sean $x, y \in \mathrm{C}$ tales que $x \neq y$, se tiene que $d(x,y) = w(x-y)$. Como C es lineal, $x - y \in \mathrm{C}$. Notemos además que como $x \neq y$, entonces $x - y \neq 0$. Esto prueba que $d \geq \min\{w(c) : c \in \mathrm{C},\ c \neq 0\}$. Recíprocamente, sea $c \in \mathrm{C} \setminus \{0\}$ una palabra de peso mínimo. Se tiene que $w(c) = d(c, 0)$ y por lo tanto, $d \leq w(c)$. □

Definición 1.6. Una aplicación $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ es una **isometría** si deja invariante la métrica de Hamming, es decir,

$$d(\varphi(x), \varphi(y)) = d(x,y) \ \text{ para cada } \ x, y \in \mathbb{F}_q^n.$$

1.2. Matriz generatriz y de control

Puesto que un código lineal es un subespacio vectorial, podemos representar sus elementos por medio de ecuaciones paramétricas (en función de los

elementos de una base) o por medio de ecuaciones implícitas. El papel en los códigos de las ecuaciones paramétricas lo desempeña la llamada matriz generatriz, mientras que el de las ecuaciones implícitas lo desempeña la matriz de control. Vamos a definir ambas y a dar algunas propiedades sobre ellas.

Sea C un código lineal de tipo $[n, k, d]$. Puesto que C es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k, tiene una base formada por k elementos linealmente independientes, $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$. Supongamos que $\mathbf{g}_i = (g_{i1}, \ldots, g_{in})$ para $i = 1, \ldots, k$.

Si introducimos por filas los vectores de dicha base de C en una matriz obtenemos:

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}$$

Esta matriz, cuyas filas son los elementos de una base de C recibe el nombre de **matriz generatriz** del código. Cualquier palabra del código se obtiene como combinación lineal de los elementos de la base: si $c \in$ C, entonces es de la forma $\mathbf{c} = m_1 g_1 + \cdots + m_k g_k$ con $m_i \in \mathbb{F}_q$ para cada $i = 1, \ldots, k$. Si denotamos por $\mathbf{m} = (m_1, \ldots, m_k)$, se tiene que $\mathbf{c} = \mathbf{m}G$.

Como mencionamos anteriormente, otra manera de describir un subespacio vectorial (en nuestro caso un código lineal) es mediante ecuaciones implícitas y es aquí donde entra en juego la llamada matriz de control.

Definición 1.7 (Matriz de control)**.** Sea C un código lineal de tipo $[n, k, d]$. Una **matriz de control** H del código es una matriz de rango máximo que cumple que

$$x \in \text{C} \iff H \cdot x^T = \mathbf{0}$$

para cada $x \in \mathbb{F}_q^n$.

Notemos que si $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ y si $h = (h_1, \ldots, h_n)$ es una fila de H, se cumple que $h \cdot x^T = 0$, es decir, $h_1 x_1 + \cdots + h_n x_n = 0$, lo que nos da una ecuación implícita sobre C. Cada una de las distintas filas de H nos van a dar una ecuación implícita del código. Como C es un subespacio vectorial de dimensión k en $\mathbb{F}_q^n$, vamos a necesitar $n - k$ ecuaciones implícitas para describir C. Como hemos dicho que cada fila de H nos va a dar una ecuación implícita, la matriz de control es de la forma $(n - k) \times n$. Obviamente se pueden añadir ecuaciones implícitas redundantes pero esto carece de interés.

El mínimo necesario serán $(n-k)$ ecuaciones y la matriz de control tendrá rango $n-k$.

Observación. Es importante destacar que ni la matriz generatriz G, ni la matriz de control H de un código lineal C de tipo $[n,k]$ son únicas.

Puesto que las filas de una matriz generatriz son los elementos de una base de C, se tiene que $H \cdot G^T = 0$ (o también $G \cdot H^T = 0$). Esta propiedad es inmediata de la definición de matriz de control y, de hecho, caracteriza a ésta junto con la condición de tener rango máximo.

Esta caracterización la resumimos en la siguiente proposición. La demostración se puede encontrar en [PWBJ17, Prop. 1.3.6].

Proposición 1.8. *Sea* C *un código lineal de tipo* $[n,k,d]$*. Sea* G *una matriz generatriz* $k \times n$ *y sea* H *una matriz* $(n-k) \times n$ *de rango* $n-k$*.* H *es una matriz de control de* C *si y solo si* $G \cdot H^T = 0$ *donde* 0 *es la matriz nula de tamaño* $k \times (n-k)$*.*

1.3. Pesos de Hamming generalizados

Antes de comenzar la exposición sobre los pesos de Hamming generalizados, vamos a dar una cota muy importante sobre la distancia mínima de un código: la cota de Singleton. Una vez hayamos definido los pesos generalizados podremos probar una versión un poco más general.

Teorema 1.9 (Cota de Singleton)**.** *Sea* C *un código lineal de tipo* $[n,k,d]$ *sobre* $\mathbb{F}_q^n$*. Entonces*

$$d \leq n - k + 1.$$

Demostración. Puesto que la dimensión de C es k, el número total de palabras del código es q^k. En cada una de las palabras del códigos vamos a quitar $d-1$ dígitos, los mismos en todas las palabras. Se puede suponer sin pérdida de generalidad que quitamos los $d-1$ últimos dígitos de cada palabra de manera que conseguimos q^k palabras de longitud $n-(d-1)$. Estas palabras resultantes son todas distintas. En efecto, si hubiera dos que son iguales, al considerar de nuevo los $d-1$ dígitos que habíamos retirado obtendríamos dos palabras de C que están a distancia menor o igual que $d-1 < d$, lo cual es absurdo. En consecuencia, tenemos q^k elementos distintos de $\mathbb{F}_q^{n-(d-1)}$. Esto implica que

$$k \leq n - (d-1),$$

o equivalentemente,

$$d \leq n - k + 1.$$

□

Definición 1.10. Los códigos para los cuales la cota de Singleton se alcanza reciben el nombre de **códigos MDS**.

Las siguientes definiciones son necesarias para poder presentar los pesos de Hamming generalizados.

Definición 1.11 (Subcódigo lineal)**.** Sea C un código lineal de tipo $[n, k, d]$ sobre $\mathbb{F}_q^n$. Se dice que $\mathrm{D} \subset \mathrm{C}$ es un **subcódigo** de C si D es un subespacio vectorial de C.

Definición 1.12 (Soporte de un código)**.** Sea C un código lineal de tipo $[n, k, d]$ y sea D un subcódigo de C. El **soporte** de D, denotado por $\chi(\mathrm{D})$, es el conjunto de posiciones no nulas para algún elemento de D, es decir,

$$\chi(\mathrm{D}) = \{i : \exists\, (x_1, \ldots, x_n) \in \mathrm{D}\,,\, x_i \neq 0\}$$

Ejemplo 1.13. Consideremos el código lineal siguiente sobre $\mathbb{F}_2$:

$$\mathrm{C} = \{(0,0,0,0), (0,0,0,1), (1,1,1,0), (1,1,1,1)\}.$$

Tomemos $\mathrm{D}_1 = \{(0,0,0,0), (0,0,0,1)\}$ y $\mathrm{D}_2 = \{(0,0,0,0), (1,1,1,0)\}$. Es sencillo comprobar que son subcódigos de C. Se tiene que $\chi(\mathrm{D}_1) = \{4\}$ y $\chi(\mathrm{D}_2) = \{1,2,3\}$. ◇

Definición 1.14 (Código degenerado)**.** Un código C de tipo $[n, k]$ es **degenerado** si $\chi(\mathrm{C}) < n$, es decir, existe un $i \in \{1, \ldots, n\}$ tal que todas las palabras de C son nulas en la coordenada i.

Para finalizar la sección, vamos a dar la definición de los pesos generalizados y a demostrar algunos teoremas interesantes sobre ellos. Estos teoremas, junto con algunas propiedades interesantes a mayores, así como ejemplos de familias de códigos concretas, pueden encontrarse en [Wei91].

Definición 1.15 (Pesos de Hamming generalizados)**.** Sea C un código lineal de tipo $[n, k]$. El **r-ésimo peso de Hamming generalizado** de C, que denotamos por $d_r(\mathrm{C})$, es el menor tamaño del soporte de un subcódigo de dimensión r, es decir,

$$d_r(\mathrm{C}) = \text{mín}\{|\chi(\mathrm{D})| : \mathrm{D} \text{ es un subcódigo de C con } \dim(\mathrm{D}) = r\}.$$

Como el código C tiene dimensión k, tiene sentido definir $d_r(\mathrm{C})$ hasta el valor $r = k$. Además, como la longitud es n, se tendrá que $d_i(\mathrm{C}) \leq n$ para cada $i = 1, \ldots, k$.

Observación. Notemos que $d_1(\mathrm{C})$ es la distancia mínima del código C. En efecto, $d_1(\mathrm{C})$ es el menor soporte de un subcódigo de dimensión 1 de C, pero estos subcódigos son los generados por las propias palabras de C y el soporte es el número de coordenadas no nulas del generador, es decir, su peso de Hamming. Como la distancia mínima d es el mínimo de los pesos de Hamming de las palabras del código, se tiene que $d = d_1(\mathrm{C})$.

Vamos a llamar **jerarquía de pesos** al vector formado por los pesos de Hamming generalizados $(d_1(\mathrm{C}), \ldots, d_k(\mathrm{C}))$.

Probaremos ahora dos teoremas importantes acerca de estos pesos, el primero aborda la monotonía (de éste podremos conseguir una generalización de la cota de Singleton); el segundo da una forma de calcular los pesos generalizados. Este segundo teorema es muy importante porque cuando hablemos de pesos generalizados asociados a matroides, daremos una definición muy parecida a la expresión del teorema.

Teorema 1.16. *Sea* C *un código lineal de longitud* n *y dimensión* k*. Se cumple que*

$$1 \leq d_1(\mathrm{C}) < d_2(\mathrm{C}) < \cdots < d_k(\mathrm{C}) \leq n.$$

Demostración. De la definición es claro que $d_{r-1}(\mathrm{C}) \leq d_r(\mathrm{C})$. Tenemos que probar ahora que la desigualdad es estricta. Sea D un subcódigo de C tal que $|\chi(\mathrm{D})| = d_r(\mathrm{C})$ con $\dim(\mathrm{D}) = r$. Vamos a construir un código de dimensión $r-1$ cuyo soporte sea estrictamente menor que el de D. Sea $i \in \chi(\mathrm{D})$ y sea $D_i = \{c \in D : c_i = 0\}$. Nótese que $\mathrm{D}_i = \mathrm{D} \cap V_i$ donde $V_i = \{x \in \mathbb{F}_q^n : x_i = 0\}$. Se tiene que $\dim(\mathrm{D}) = r$ y $\dim(V_i) = n - 1$. Utilizando la fórmula de las dimensiones y teniendo que cuenta que $\mathrm{D} \not\subset V_i$ se tiene que $\dim(\mathrm{D}_i) = \dim(\mathrm{D} \cap V_i) = \dim(\mathrm{D}) + \dim(V_i) - \dim(\mathrm{D} + V_i) = r + (n-1) - n = r - 1$. Además, es claro que $d_{r-1}(\mathrm{C}) \leq |\chi(\mathrm{D}_i)| \leq |\chi(\mathrm{D})| - 1 = d_r(\mathrm{C}) - 1 < d_r(\mathrm{C})$. □

Gracias a la monotonía de los pesos, podemos dar una versión generalizada de la cota de Singleton.

Corolario 1.17 (Cota de Singleton generalizada)**.** *Sea* C *un código lineal de tipo* $[n, k]$*, se cumple que*

$$d_r(\mathrm{C}) \leq n - k + r \text{ para todo } r = 1, \ldots, k.$$

Antes de comenzar la prueba, destaquemos que el caso $r = 1$ es la cota de Singleton, probada en el Teorema 1.9.

Demostración. Se tiene que $d_k(\mathrm{C}) \leq n = n - k + k$. Por la monotonía, $d_{k-1}(\mathrm{C}) \leq d_k(\mathrm{C}) - 1 = n - k + (k-1)$. Recursivamente se tiene que $d_r(\mathrm{C}) \leq n - k + r$. □

Como adelantamos anteriormente, vamos a dar ahora un teorema que nos permitirá calcular los pesos de Hamming de un código haciendo uso de una matriz de control.

Notación. C será un código lineal de tipo $[n, k]$. Consideremos una matriz de control, H, del código. Vamos a denotar por h_i con $i = 1, \ldots, n$ sus vectores columna y por $\langle h_i : i \in I \rangle$ el espacio generado por los vectores columna de H correspondientes a los índices de I, siendo I un subconjunto de $\{1, \ldots, n\}$.

Teorema 1.18. *Para cada $r = 1, \ldots, k$, se tiene que*

$$d_r(\mathrm{C}) = \min\{|I| : |I| - \dim(\langle h_i : i \in I \rangle) \geq r\}.$$

Demostración. Vamos a probar la igualdad probando las dos desigualdades. Para cada $I \subset \{1, \ldots, n\}$, sea $S = \langle h_i : i \in I \rangle$. Consideremos a su vez $S^\perp = \{\mathbf{x} : x_i = 0 \text{ para cada } i \notin I \text{ y } \sum_{i \in I} x_i h_i = 0\}$. Se tiene que $S^\perp$ es cerrado por combinaciones lineales y además $S^\perp \subset \mathrm{C}$ ya que si $x \in S^\perp$ y H es una matriz de control de C, $H \cdot x^T = 0$. Por tanto, $S^\perp$ es un subcódigo de C. Además, $\dim(S) + \dim(S^\perp) = |I|$.

Llamemos d_r a la expresión a la derecha de la igualdad en el enunciado del teorema. Sea $I \subset \{1, \ldots, n\}$ de modo que $|I| = d_r$ y que $|I| - \dim(S) = r$. Bajo estas condiciones, $\dim(S^\perp) = r$ y por tanto se tiene que

$$d_r(\mathrm{C}) \leq |\chi(S^\perp)| \leq |I| = d_r.$$

Veamos ahora la desigualdad contraria. Sea D un subcódigo de C de dimensión r tal que $d_r(\mathrm{C}) = |\chi(\mathrm{D})|$. Consideremos ahora $I = \chi(\mathrm{D})$. Si $x = (x_1, \ldots, x_n) \in \mathrm{D}$, se tiene que $x_j = 0$ para cada $j \notin I$ y además, por ser $\mathrm{D} \subset \mathrm{C}$, se cumple que $H \cdot x^T = 0$ para todo $x \in \mathrm{D}$. En consecuencia, $\mathrm{D} \subset S^\perp$.

Ahora, $\dim(S) = |I| - \dim(S^\perp) \leq |I| - \dim(\mathrm{D}) = d - r$, con lo que $|I| - \dim(S) \geq r$.

Hemos conseguido así un $I \subset \{1, \ldots, n\}$ tal que $|I| - \dim(S) \geq r$, por lo tanto, $d_r \leq |I| = d_r(\mathrm{C})$. □

Observación. De hecho, se tiene que

$$d_r(\mathrm{C}) = \mín\{|I| : \ |I| - \dim(\langle h_i : \ i \in I\rangle) = r\}.$$

En efecto, supongamos que $d_r(\mathrm{C}) = |I|$ con $|I| - \dim(\langle h_i : \ i \in I\rangle) = r' > r$. Por la definición de $d_r(\mathrm{C})$, existe un subcódigo D de dimensión r tal que $d_r(\mathrm{C}) = |\chi(\mathrm{D})|$. Por otra parte, $\dim(S^\perp) = r'$ con lo que $D \neq S^\perp$, y

$$d_r(\mathrm{C}) < d_{r'}(\mathrm{C}) \leq |\chi(S^\perp)| \leq |I|$$

Esta última cadena de desigualdades es una contradicción.

El Teorema 1.18 tiene como consecuencia directa el siguiente corolario, que da un modo de calcular la distancia mínima de un código.

Corolario 1.19. *Sea* C *un código lineal de tipo* $[n, k]$ *y sea* H *una matriz de control de* C*, entonces la distancia mínima del código es el menor entero* d *tal que* d *columnas de* H *son linealmente dependientes.*

1.4. Código dual

Damos en esta última sección del capítulo la noción de código dual. Vamos para ello a definir un producto interno en $\mathbb{F}_q^n$.

Definición 1.20. Consideremos el espacio vectorial $\mathbb{F}_q^n$. Dados $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, se define su **producto interno** como:

$$x \cdot y = x_1y_1 + \cdots + x_ny_n$$

Observación. El producto interno definido anteriormente es visto como aplicación con llegada en $\mathbb{F}_q$.

$$\begin{array}{rcl} \cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q \\ (x, y) & \longmapsto & x \cdot y \end{array}$$

La aplicación anterior es una forma bilineal simétrica no degenerada pero carece de la propiedad de ser definida ya que el producto de una palabra consigo misma puede ser nulo pese a que la palabra no lo sea.

Por ejemplo, la palabra $x = (1, 1) \in \mathbb{F}_2^2$ cumple que $x \cdot x = 0$ pese a que $x \neq 0$.

Con este producto interno vamos a definir el dual de un código lineal y vamos a poder dar una relación entre las matrices generatriz y de control de un código y su dual.

Definición 1.21 (Código dual)**.** Sea C un código lineal de tipo $[n, k]$ sobre $\mathbb{F}_q$. Se define su **código dual**, y se denota por $\mathrm{C}^\perp$ al conjunto:

$$\mathrm{C}^\perp = \{x \in \mathbb{F}_q^n : \ c \cdot x = 0 \text{ para cada } c \in \mathrm{C}\}$$

Es sencillo comprobar que efectivamente $\mathrm{C}^\perp$ es un código lineal, es decir, un subespacio vectorial de $\mathbb{F}_q^n$.

Proposición 1.22. *Sea* C *un código lineal de tipo* $[n, k]$ *con matriz generatriz* G*. Entonces* $\mathrm{C}^\perp$ *es un código lineal de tipo* $[n, n-k]$ *que tiene* G *como matriz de control.*

Demostración. Se tiene que $x \in \mathrm{C}^\perp \iff c \cdot x = 0$ para cada $c \in \mathrm{C}$. Como G es una matriz generatriz de C, $c \cdot x = 0$ para cada $c \in \mathrm{C} \iff mGx^T = 0$ para cada $m \in \mathbb{F}_q^k$, o equivalentemente $Gx^T = 0$. En consecuencia $\mathrm{C}^\perp$ es el núcleo de G. Puesto que G es una matriz $k \times n$, el espacio $\mathrm{C}^\perp$ tiene dimensión $n - k$ y G funciona como matriz de control. □

Observación. Este hecho permite demostrar que $\mathrm{C} = (\mathrm{C}^\perp)^\perp$. La contención $\mathrm{C} \subset (\mathrm{C}^\perp)^\perp$ es clara ya que $c \cdot x = 0$ para cada $x \in \mathrm{C}^\perp$. Además aplicando la proposición anterior, se tiene que C y $(\mathrm{C}^\perp)^\perp$ tienen la misma dimensión, luego se da la igualdad.

Finalmente, se tiene el siguiente resultado, fruto de la Proposición 1.22 y de la observación anterior:

Corolario 1.23. *Sea* C *un código lineal. Entonces:*

- G *es la matriz generatriz de* C *si y solo si* G *es la matriz de control de* $\mathrm{C}^\perp$*.*
- H *es la matriz de control de* C *si y solo si* H *es la matriz generatriz de* $\mathrm{C}^\perp$*.*

Capítulo 2

Matroides

En este capítulo vamos a definir el concepto de matroide, que generaliza el concepto de independencia lineal. El artículo considerado fundador de la teoría de matroides trata de aislar las propiedades abstractas más básicas asociadas a la dependencia, tanto en el ámbito de los grafos (que sean libres de ciclos) como en el del álgebra lineal (independencia lineal). Este artículo, debido a Hassler Whitney, se puede encontrar en [Whi92].

Las matroides presentan numerosas definiciones equivalentes. Hemos elegido como definición en este trabajo la relativa a conjuntos linealmente independientes. A partir de ella estudiaremos sus propiedades y definiremos conceptos tales como rango, circuitos, bases, etc. Estos conceptos se pueden usar para dar nuevas definiciones de matroides, equivalentes a la primera que ofrecemos. Vamos a desarrollar primero la teoría de conjuntos independientes, circuitos, bases y función de rango para posteriormente dar dos ejemplos fundamentales de matroides. Estudiaremos, para dichos ejemplos, su relación con los códigos lineales. La principal referencia que seguiremos para esta introducción es [Oxl06]

2.1. Conjuntos independientes y circuitos

Definición 2.1 (Matroide)**.** Una **matroide** M es un par $(E, \mathcal{I})$ donde E es un conjunto finito e $\mathcal{I}$ es una familia de subconjuntos de E que satisfacen las siguientes propiedades:

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

(I2) Si $I \in \mathcal{I}$ e $I' \subset I$, entonces $I' \in \mathcal{I}$.

(I3) Si I_1 e I_2 están en $\mathcal{I}$ y $|I_1| < |I_2|$, existe $e \in I_2 \setminus I_1$ tal que $I_1 \cup \{e\} \in \mathcal{I}$.

El conjunto E se llama **conjunto base** de la matroide M. Los elementos de $\mathcal{I}$ se llaman **conjuntos independientes** de M. Un subconjunto de E que no esté en $\mathcal{I}$ es un **conjunto dependiente**.

Definición 2.2. Sean $M_1 = (E_1, \mathcal{I}_1)$ y $M_2 = (E_2, \mathcal{I}_2)$ matroides. Una aplicación $\varphi\colon E_1 \to E_2$ es un **morfismo de matroides** si $\varphi(X) \in \mathcal{I}_2$ para cada $X \in \mathcal{I}_1$. Se dice que φ es un **isomorfismo** si además existe una aplicación $\phi\colon E_2 \to E_1$ que sea morfismo e inversa de φ.

Vamos a dar ahora la noción de circuito, la cual puede usarse como alternativa para dar una definición de matroide.

Definición 2.3 (Circuitos)**.** Sea M una matroide. Un **circuito** en M es un conjunto dependiente minimal, es decir, un conjunto dependiente de modo que cualquiera de sus subconjuntos propios es independiente. El conjunto de circuitos de una matroide M lo denotaremos por $\mathcal{C}_M$, o simplemente $\mathcal{C}$ cuando no sea necesario especificar M.

Si para una matroide $M = (E, \mathcal{I})$ tenemos determinado $\mathcal{I}$, los conjuntos dependientes serán los subconjuntos de E que no estén en $\mathcal{I}$. Al tomar solo los minimales obtenemos $\mathcal{C}$. Recíprocamente, si conocemos el conjunto de circuitos $\mathcal{C}$ de una matroide M, podemos determinar $\mathcal{I}$ ya que los conjuntos que están en $\mathcal{I}$ son los que no contienen ningún circuito. Por lo tanto, una matroide queda perfectamente caracterizada por su conjunto de circuitos.

De la definición de circuito se deducen las siguientes propiedades. La primera se debe a que $\mathcal{C}$ está formado por conjuntos dependientes y $\emptyset$ es independiente. La segunda se debe a la minimalidad.

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

(C2) Si C_1 y C_2 son dos circuitos y $C_1 \subset C_2$, entonces $C_1 = C_2$.

Además, se cumple una tercera propiedad:

Proposición 2.4. *Sea M una matroide. El conjunto de circuitos $\mathcal{C}$ de M satisface la siguiente propiedad:*

(C3) *Sean C_1 y C_2 son dos circuitos distintos y sea $e \in C_1 \cap C_2$, entonces existe un $C_3 \in C$ tal que $C_3 \subset (C_1 \cup C_2) \setminus e$.*

Demostración. Vamos a razonar por reducción al absurdo. Supongamos que $(C_1 \cup C_2) \setminus e$ no contiene ningún circuito. Se tiene entonces que $(C_1 \cup C_2) \setminus e$ es independiente. Como C_1 y C_2 son circuitos distintos, la propiedad **(C2)**

asegura la existencia de un $f \in C_2 \setminus C_1$. Como C_2 es un conjunto dependiente minimal, $C_2 \setminus f$ es independiente.

Vamos a escoger ahora un $I \subset C_1 \cup C_2$ maximal con la propiedad de que $C_2 \setminus f \subset I$. I es independiente, contiene a $C_2 \setminus f$ y C_2 es dependiente por lo que $f \notin I$. Como C_1 es también dependiente, existe un $g \in C_1$ tal que $g \notin I$. Además f y g son elementos distintos ya que $f \in C_2 \setminus C_1$. Por tanto,

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

Los conjuntos I y $(C_1 \cup C_2) \setminus e$ son independientes y $|I| < |(C_1 \cup C_2) \setminus e|$. Utilizando la propiedad (**I3**), podemos ampliar I a un conjunto independiente, contradiciendo la maximalidad. □

Vamos a probar a continuación que las propiedades (**C1**), (**C2**) y (**C3**) caracterizan las familias de conjuntos que pueden ejercer como conjunto de circuitos de una matroide.

Teorema 2.5. *Sea E un conjunto y sea $\mathcal{C}$ una familia de subconjuntos de E que cumplen las propiedades* (**C1**)*,* (**C2**) *y* (**C3**)*. Sea $\mathcal{I}$ la familia de subconjuntos de E que no contienen ningún conjunto de $\mathcal{C}$. Entonces $(E, \mathcal{I})$ es una matroide que tiene $\mathcal{C}$ como conjunto de circuitos.*

Demostración. Vamos a probar en primer lugar que se cumplen las condiciones (**I1**), (**I2**) y (**I3**). Como $\emptyset \notin \mathcal{C}$, se tiene que $\emptyset$ no contiene ningún elemento de $\mathcal{C}$ y, por tanto, $\emptyset \in \mathcal{I}$. Se verifica entonces (**I1**).

Veamos que se cumple (**I2**). Si $I \in \mathcal{I}$, entonces I no contiene ningún elemento de $\mathcal{C}$. Si $I' \subset I$, I' tampoco contiene ningún elemento de $\mathcal{C}$ y por tanto $I' \in \mathcal{I}$.

Probemos (**I3**). Vamos a razonar por reducción al absurdo suponiendo que existen dos elementos I_1 e I_2 de $\mathcal{I}$ tales que $|I_1| < |I_2|$ para los cuales no se cumpla la propiedad (**I3**). Consideremos el conjunto

$$A = \{I \in \mathcal{I} : \ I \subset I_1 \cup I_2 \text{ y } |I| > |I_1|\}.$$

Se tiene que $I_2 \in A$, luego no es vacío. Escojamos un subconjunto I_3 de A con la propiedad de que $|I_1 \setminus I_3|$ sea minimal. (**I3**) no se cumple, por tanto, $I_1 \cup e \notin \mathcal{I}$ para cualquier $e \in I_2 \setminus I_1$. Se tiene entonces que $I_1 \not\subset I_3$, es decir, $I_1 \setminus I_3 \neq \emptyset$. Podemos escoger así $e \in I_1 \setminus I_3$. Ahora, para cada elemento $f \in I_3 \setminus I_1$, consideramos $T_f = (I_3 \cup e) \setminus f$. Se tiene que $T_f \subset I_1 \cup I_2$, que $|T_f| = |I_3|$ y que $|I_1 \setminus T_f| < |I_1 \setminus I_3|$. Esta última desigualdad se debe a que al quitar T_f a I_1 estamos quitando todo I_3 y además el punto e. Por

consiguiente $T_f \notin \mathcal{I}$, así T_f un elemento C_f de $\mathcal{C}$, es decir, $C_f \subset (I_3 \cup e) \setminus f$. Además, $e \in C_f$ ya que de no ser así, $C_f \subset I_3$ pero $I_3 \in \mathcal{I}$.

Sea ahora $g \in I_3 \setminus I_1$. Si $C_g \cap (I_3 \setminus I_1) = \emptyset$, entonces $C_g \subset ((I_1 \cap I_3) \cup e) \setminus g \subset I_1$ pero $I_1 \in I$. Existe por tanto un $h \in C_g \cap (I_3 \setminus I_1)$. Además, $C_h \neq C_g$ ya que $h \notin C_h$. Se tiene que $e \in C_g \cap C_h$ y por (C3), $\mathcal{C}$ contiene un circuito C tal que $C \subset (C_g \cup C_h) \setminus e$. Pero tanto C_g como C_h son subconjuntos de $I_3 \cup e$, luego $C \subset I_3$. Esto es una contradicción ya que $I_3 \in \mathcal{I}$. Hemos probado por tanto que se cumplen (**I1**), (**I2**) y (**I3**) y que $M = (E, \mathcal{I})$ es una matroide.

Ahora falta probar que $\mathcal{C}$ es el conjunto de circuitos de la matroide M. Sea C un circuito de M, esto es, un conjunto dependiente minimal. Se tiene que $C \notin \mathcal{I}(M)$ y que $C \setminus \{x\} \in \mathcal{I}$ para cada $x \in C$. Como $C \notin \mathcal{I}$, existe un $C' \in \mathcal{C}$ tal que $C' \subset C$. Es más, debe ser $C' = C$ ya que de no ser así, existe $x \in C \setminus C'$ y por ser C un circuito, $C \setminus \{x\} \in \mathcal{I}$. Esto es una contradcción ya que $C' \subset C \setminus \{x\} \in \mathcal{I}$. Entonces se tiene que $C = C'$ y por tanto, $C \in \mathcal{C}$. Sea ahora $C \in \mathcal{C}$, queremos probar que es un circuito de M, es decir, que es un conjunto dependiente minimal. Por una parte, es claro que $C \notin \mathcal{I}$ por cómo hemos definido $\mathcal{I}$. Además, C es minimal porque la familia $\mathcal{C}$ cumple la propiedad (**C2**). □

Combinando el Teorema 2.5 con las propiedades (**C1**), (**C2**) y (**C3**) que ya habíamos comprobado que satisfacía el conjunto de circuitos de una matroide M, se demuestra el siguiente resultado.

Corolario 2.6. *Sea $\mathcal{C}$ un conjunto de subconjuntos del conjunto E. $\mathcal{C}$ es la familia de circuitos de una matroide sobre E si y solo si satisface las propiedades* (**C1**)*,* (**C2**) *y* (**C3**)*.*

Para terminar esta sección vamos a dar dos definiciones sencillas que necesitaremos más adelante, así como un resultado de fácil demostración pero tremendamente útil en la argumentación con matroides.

Proposición 2.7. *Sea I un conjunto independiente en una matroide M y sea $e \in E$ tal que $I \cup e$ es dependiente. Entonces M tiene un único circuito contenido en $I \cup e$ y además, dicho circuito contiene a e.*

Demostración. Si $I \cup e$ es dependiente, contiene un circuito y claramente el circuito ha de contener a e. Veamos la unicidad. Sean C y C' dos circuitos distintos contenidos en $I \cup e$. Por (**C3**), $(C \cup C') \setminus e$ contiene un circuito, pero $(C \cup C') \setminus e \subset I$, lo cual es absurdo. □

Definición 2.8 (Bucles)**.** Sea M una matroide sobre un conjunto base E. Un **bucle** en M es un elemento $e \in E$ de forma que $\{e\}$ es un circuito de M.

Definición 2.9 (Elementos paralelos)**.** Sea M una matroide sobre un conjunto base E. Se dice que $f, g \in E$ son **paralelos** si $\{f, g\}$ es un ciruito de M. Una **clase paralela** de M es un subconjunto maximal $X \subset E$ tal que cualesquiera dos miembros de X son paralelos y X no contiene bucles.

2.2. Bases

Por el momento hemos visto que una matroide sobre un conjunto base E puede venir dada por la familia de conjuntos independientes o por sus circuitos. Al igual que ocurre en el caso de espacios vectoriales, las matroides van a poder ser determinadas por los conjuntos independientes maximales (las bases si hablamos en el ámbito del álgebra lineal). Nuestro siguiente propósito es definir las bases de una matroide y dar una caracterización con ellas.

Definición 2.10 (Bases)**.** Sea $M = (E, \mathcal{I})$ una matroide. Una **base**, B, de M es un conjunto independiente maximal, es decir, un conjunto tal que si le añadimos cualquier elemento deja de pertenecer a $\mathcal{I}$. Vamos a denotar por $\mathcal{B}_M$ al conjunto de bases de la matroide M, o simplemente $\mathcal{B}$ si no es necesario especificar.

Dar una matroide en función de sus bases es claramente más eficiente que darla especificando todos los conjuntos independientes. Vamos ahora a dar una serie de propiedades acerca de las bases de una matroide. Muchas de ellas recuerdan a las propiedades que cumplen las bases en los espacios vectoriales.

Proposición 2.11. *Sea M una matroide y sean B_1 y B_2 dos bases de M, entonces $|B_1| = |B_2|$.*

Demostración. Supongamos que $|B_1| < |B_2|$. Como ambos son conjuntos independientes, por (**I3**) existe un $e \in B_2 \setminus B_1$ tal que $B_1 \cup e \in \mathcal{I}$, en contra de la maximalidad de B_1. Hemos probado entonces que $|B_1| \geq |B_2|$. La desigualdad $|B_2| \geq |B_1|$ se prueba análogamente. □

Al igual que hicimos antes con las propiedades (**C1**), (**C2**) y (**C3**), vamos a desgranar cuáles son las propiedades que cumplen las bases, y que además caracterizan a los conjuntos que pueden ser bases de una matroide.

En primer lugar, si M es una matroide y $\mathcal{B}$ es su familia de bases se tiene que:

(B1) $\mathcal{B}$ es no vacío (por la propidad (**I1**)).

Proposición 2.12. *Sea $\mathcal{B}$ el conjunto de bases de una matroide M. Se verifica la siguiente propiedad:*

(B2) *Si B_1 y B_2 son elementos de $\mathcal{B}$ y $x \in B_1 \setminus B_2$, existe un elemento $y \in B_2 \setminus B_1$ tal que $(B_1 \setminus x) \cup y \in \mathcal{B}$.*

Demostración. Tanto B_2 como $B_1 \setminus x$ son conjuntos independientes. Además, por la proposición anterior se tiene que $|B_1 \setminus x| < |B_2|$. Por la propiedad (**I3**) existe entonces $y \in B_2 \setminus (B_1 \setminus x)$ tal que $(B_1 \setminus x) \cup y \in \mathcal{I}$. Como este conjunto es independiente, va a estar contenido en un conjunto independiente maximal B_1' y se cumple que $|B_1'| = |B_1| = |(B_1 \setminus x) \cup y|$. Entonces $B_1' = (B_1 \setminus x) \cup y$. Esto demuestra que $(B_1 \setminus x) \cup y \in \mathcal{B}$. □

Vamos a dar ahora el teorema que prueba que las condiciones (**B1**) y (**B2**) anteriores caracterizan las bases de una matroide.

Teorema 2.13. *Sea E un conjunto y sea $\mathcal{B}$ una familia de subconjuntos de E que satisfacen* (**B1**) *y* (**B2**)*. Sea $\mathcal{I}$ la el conjunto de subconjuntos de E que están contenidos en algún elemento de $\mathcal{B}$. Entonces $(E, \mathcal{I})$ es una matroide que tiene $\mathcal{B}$ como conjunto de bases*

Demostración. Nuestro objetivo es probar que se cumplen las propiedades (**I1**), (**I2**) e (**I3**). Puesto que $\mathcal{B}$ cumple (**B1**), se tiene $\emptyset \in \mathcal{I}$, verificándose así (**I1**). Ahora, si $I \in \mathcal{I}$, entonces existe $B \in \mathcal{B}$ tal que $I \subset B$. Si tenemos $I' \subset I$, se da que $I' \subset B$ y por lo tanto $I' \in \mathcal{I}$. Se cumple así (**I2**).

Para verificar que se cumple (**I3**) vamos a necesitar un resultado previo:

Lema 2.14. *Si $\mathcal{B}$ es un conjunto como en el teorema, todos sus elementos tienen el mismo cardinal.*

Demostración del lema. Vamos a razonar por reducción al absurdo. Sean B_1 y B_2 dos elementos de $\mathcal{B}$ tal que $|B_1| > |B_2|$. Los escogemos además tal que $|B_1 \setminus B_2|$ sea minimal. Como $B_1 \setminus B_2$ es no vacío, existe un $x \in B_1 \setminus B_2$. Puesto que $\mathcal{B}$ cumple (**B2**), podemos encontrar un $y \in B_2 \setminus B_1$ de forma que $(B_1 \setminus x) \cup y \in \mathcal{B}$. Se tiene que

$$|(B_1 \setminus x) \cup y| = |B_1| > |B_2|$$

y

$$|(B_1 \setminus x) \cup y| < |B_1 \setminus B_2|,$$

en contra de la minimalidad. □

Retomando la demostración del Teorema 2.13, nos falta probar que $\mathcal{I}$ cumple (**I3**). Vamos a suponer que no lo hace, es decir, que existen I_1 e I_2 en $\mathcal{I}$ con $|I_1| < |I_2|$ tal que para cada $e \in I_2 \setminus I_1$, el conjunto $I_1 \cup e \notin \mathcal{I}$. Como I_1 e I_2 están en $\mathcal{I}$, existen B_1 y B_2 de $\mathcal{B}$ tal que $I_1 \subset B_1$ e $I_2 \subset B_2$. Elijamos un B_2 de modo que $|B_2 \setminus (I_2 \cup B_1)|$ sea minimal.

Como $I_1 \cup e \notin \mathcal{I}$ para todo $e \in I_2 \setminus I_1$, se tiene que:

$$I_2 \setminus B_1 = I_2 \setminus I_1. \tag{2.1}$$

Supongamos que $B_2 \setminus (I_2 \cup B_1)$ es no vacío, es decir podemos coger x en dicho conjunto. Por (**B2**), existe $y \in B_1 \setminus B_2$ tal que $(B_2 \setminus x) \cup y \in \mathcal{B}$. Pero entonces $|((B_2 \setminus x) \cup y) - (I_2 \cup B_1)| < |B_2 \setminus (I_2 \cup B_1)|$, en contra de la elección de B_2. Por tanto, $B_2 \setminus (I_2 \cup B_1) = \emptyset$ y $B_2 \setminus B_1 = I_2 \setminus B_1$. Por 2.1,

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

Vamos a ver ahora que $B_1 \setminus (I_1 \cup B_2)$ es vacío. Si no lo fuera, existiría un x en dicho conjunto y por (**B2**), un $y \in B_2 \setminus B_1$ tal que $(B_1 \setminus x) \cup y \in \mathcal{B}$. Ahora, $I_1 \cup y \subset (B_1 \setminus x) \cup y$, luego $I_1 \cup y \in \mathcal{I}$. Puesto que $y \in B_2 \setminus B_1$, por 2.2, $y \in I_2 \setminus I_1$, en contra de la elección de I_1 e I_2. Por tanto tenemos que $B_1 \setminus (I_1 \cup B_2) = \emptyset$ y que $B_1 \setminus B_2 = I_1 \setminus B_2$. Así,

$$B_1 \setminus B_2 \subset I_1 \setminus I_2. \tag{2.3}$$

Por el Lema 2.14, $|B_1| = |B_2|$, luego $|B_1 \setminus B_2| = |B_2 \setminus B_1|$. Juntando 2.2 y 2.3 se llega a que $|I_1 \setminus I_2| \geq |I_2 \setminus I_1|$, o equivalentemente, $|I_1| \geq |I_2|$. Esto contradice la elección de I_1 e I_2 realizada al principio del argumento. Se cumple por tanto (**I3**).

Queda entonces probado que $(E, \mathcal{I})$ es una matroide. Es claro que $\mathcal{B}$ es el conjunto de bases de esta matroide. (Hemos definido los independientes como los conjuntos que están contenidos en algún miembro de $\mathcal{B}$, luego los elementos de $\mathcal{B}$ son independientes maximales). □

Si combinamos el Teorema 2.13 con las propiedades que ya conocíamos que habían de cumplir las bases obtenemos el siguiente resultado:

Corolario 2.15. *Sea E un conjunto y sea $\mathcal{B}$ un conjunto de subconjuntos de E. $\mathcal{B}$ es el conjunto de bases de una matroide sobre E si y solo si se satisfacen las propiedades* (**B1**) *y* (**B2**).

Damos un resultado que nos será útil a la hora de definir más adelante el dual de una matroide. El resultado es consecuencia inmediata de la Proposición 2.7.

Proposición 2.16. *Sea B una base de una matroide M. Si $e \in E \setminus B$, existe un único circuito contenido en $B \cup e$. Además, este circuito contiene a e.*

Definición 2.17. Para cada $e \in E$, el circuito único de la proposición anterior se llama circuito fundamental de e con respecto a B. Lo denotaremos por $C(e, B)$.

2.3. Rango

Vamos ahora a centrarnos en la función rango de una matroide, que generaliza el concepto de dimensión para un subespacio vectorial. Antes de empezar con la definición, vamos a dar una forma de construir una matroide a partir de otra ya conocida.

Sea $M = (E, \mathcal{I})$ una matroide sea $X \subset E$. Vamos a denotar por $\mathcal{I}|X$ al conjunto $\{I \subset X : I \in \mathcal{I}\}$. Es claro ver que $(X, \mathcal{I}|X)$ es una matroide:

- Se cumple (**I1**) ya que $\emptyset \subset X$ y $\emptyset \in \mathcal{I}$.
- Si $I \in \mathcal{I}|X$, se tiene que $I \subset X$ y que $I \in \mathcal{I}$. Sea $I' \subset I$. Es claro que $I' \subset X$ y como $(E, \mathcal{I})$ es una matroide, $I' \in \mathcal{I}$. Se cumple así (**I2**) para $(X, \mathcal{I}|X)$.
- Sean I_1 e I_2 dos elementos de $\mathcal{I}|X$ tales que $|I_1| < |I_2|$. Como ambos están en $\mathcal{I}$, existe un $e \in I_2 \setminus I_1$ tal que $I_1 \cup e \in \mathcal{I}$. Como $I_2 \subset X$, se tiene que $I_1 \cup e \subset X$ y por tanto $I_1 \cup e \in \mathcal{I}|X$. Hemos probado que se verifica (**I3**).

La matroide $(E, \mathcal{I}|X)$ se denomina **matroide restricción** de M a X y se denota por $M|X$. La Proposición 2.11 asegura que todas las bases de dicha matroide tienen el mismo cardinal. Vamos a definir el **rango** de X, como el cardinal de una base B de $M|X$. Es decir, el rango de X es el cardinal de cualquier conjunto independiente maximal contenido en X, es decir,

$$r(X) = \text{máx}\{|I| : I \subset X\,,\, I \in \mathcal{I}\}.$$

De la definición de rango es claro que se verifican las siguientes propiedades:

(R1) Si $X \subset E$, entonces $0 \leq r(x) \leq |X|$.

(R2) Si $X \subset Y \subset E$, entonces $r(X) \leq r(Y)$.

Se cumple además una tercera propiedad que, junto a las dos anteriores, caracterizan las funciones que pueden actuar con función rango de una ma-

troide. Nótese el parecido con la fórmula de las dimensiones, bien conocida para espacios vectoriales de dimensión finita.

Proposición 2.18. *La función rango de una matroide M sobre un conjunto E satisface la siguiente propiedad:*

(R3) *Si X e Y son dos subconjuntos de E, entonces*

$$r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

Demostración. Recordemos que habíamos definido el rango de $X \subset E$ como el cardinal de cualquier base de la matroide restricción $M|X$. Sea $B_{X\cap Y}$ una base de $X \cap Y$. Se tiene que $B_{X\cap Y}$ es un conjunto independiente de $M|(X \cup Y)$ y está, por tanto, contenido en una base $B_{X\cup Y}$ de dicha matroide. Además, $B_{X\cup Y} \cap X$ y $B_{X\cup Y} \cap Y$ son independientes en $M|X$ y en $M|Y$, respectivamente. Por la defínción de rango se tiene entonces que $r(X) \geq |B_{X\cup Y} \cap X|$ y $r(Y) \geq |B_{X\cup Y} \cap Y|$, por lo que:

$$\begin{aligned} r(X) + r(Y) &\geq |B_{X\cup Y} \cap X| + |B_{X\cup Y} \cap Y| \\ &= |(B_{X\cup Y} \cap X) \cup (B_{X\cup Y} \cap Y)| \\ &\quad + |(B_{X\cup Y} \cap X) \cap (B_{X\cup Y} \cap Y)| \\ &= |B_{X\cup Y} \cap (X \cup Y)| + |B_{X\cup Y} \cap (X \cap Y)|. \end{aligned}$$

Ahora, $B_{X\cup Y} \cap (X \cup Y) = B_{X\cup Y}$ y $B_{X\cup Y} \cap (X \cap Y) = B_{X\cap Y}$. Hemos probado por tanto que $r(X) + r(Y) \geq |B_{X\cup Y}| + |B_{X\cap Y}| = r(X \cup Y) + r(X \cap Y)$, como queríamos. □

Tal y como hicimos anteriormente con circuitos y bases, vamos a probar que las condiciones (**R1**), (**R2**) y (**R3**) caracterizan la función rango de una matroide. Necesitaremos el siguiente lema previo:

Lema 2.19. *Sea E un conjunto y sea $r : 2^E \longrightarrow \mathbb{N}$ una aplicación que satisface* (**R2**) *y* (**R3**)*. Si X e Y son subconjuntos de E tales que $r(X \cup y) = r(X)$ para cada $y \in Y \setminus X$, entonces $r(X \cup Y) = r(X)$.*

Demostración. Sea $Y \setminus X = \{y_1, \ldots, y_k\}$. Vamos a proceder por inducción sobre k. El caso $k = 1$ es inmediato. Supongamos que el resultado es cierto para n y veámoslo para $n + 1$.

Se tiene que:

$$\begin{aligned} r(X) + r(X) &= r(X \cup \{y_1, \dots y_n\}) + r(X \cup y_{n+1}) \\ &\geq r((X \cup \{y_1, \dots, y_n\}) \cup (X \cup y_{n+1})) \\ &\quad + r((X \cup \{y_1, \dots, y_{n+1}\}) \cap (X\ y_{n+1})) \\ &= r(X \cup \{y_1, \dots y_{n+1}) + r(X) \geq r(X) + r(X). \end{aligned}$$

En la expresión anterior, la primera igualdad se debe a la hipótesis de inducción junto con la hipótesis del enunciado, la siguiente desigualdad a la propiedad (**R2**) y la última desigualdad a (**R3**). De la cadena de desigualdades anterior se deduce que $r(X \cup \{y_1, \dots, y_{n+1}\}) = r(X)$. Queda así probado el lema por inducción. □

Teorema 2.20. *Sea E un conjunto y sea $r\colon 2^E \longrightarrow \mathbb{N}$ una función que satisface* (**R1**)*,* (**R2**) *y* (**R3**)*. Sea $\mathcal{I}$ la colección de subconjuntos X de E para los cuales $r(X) = |X|$. Entonces $(E, \mathcal{I})$ es una matroide con función de rango r.*

Demostración. Al igual que hicimos en las pruebas del Teorema 2.5 y el Teorema 2.13, nuestro objetivo va a ser probar que se cumplen las condiciones (**I1**), (**I2**) e (**I3**). Por (**R1**) se tiene que $0 \leq r(\emptyset) \leq |\emptyset| = 0$, por lo que $r(\emptyset) = 0 = |\emptyset|$ y $\emptyset \in \mathcal{I}$. Se satisface así (**I1**).

Sea $I \in \mathcal{I}$ y sea $I' \subset I$. Entonces $r(I) = |I|$ y, por (**R3**),

$$r(I' \cup (I \setminus I')) + r(I' \cap (I \setminus I')) \leq r(I') + r(I \setminus I'),$$

o equivalentemente,

$$r(I) + r(\emptyset) \leq r(I') + r(I \setminus I').$$

Teníamos que $r(I) = |I|$ y $r(\emptyset) = 0$. Por (**R2**), $r(I') \leq |I'|$ y $r(I \setminus I') \leq |I \setminus I'|$. Por lo tanto,

$$|I| \leq r(I') + r(I \setminus I') \leq |I'| + |I \setminus I'| = |I|.$$

Así, hemos probado que $r(I') = |I'|$, por lo que $I' \in \mathcal{I}$, verificándose (**I2**).

Vamos a probar que se cumple (**I3**) razonando por reducción al absurdo. Sean pues I_1 e I_2 elementos de $\mathcal{I}$ con $|I_1| < |I_2|$ tal que para cada $e \in I_2 \setminus I_1$, $I_1 \cup e \notin \mathcal{I}$, es decir, $r(I_1 \cup e) \neq |I_1 \cup e| = |I_1| + 1$. Tenemos entonces la siguiente cadena de desigualdades:

$$|I_1| + 1 > r(I_1 \cup e) > r(I_1) = |I_1|,$$

por lo que $r(I_1 \cup e) = r(I_1)$. Para concluir, podemos aplicar el Lema 2.19 a I_1 e I_2, obteniendo así $r(I_1) = r(I_1 \cup I_2)$, pero $r(I_1) = |I_1|$ y $r(I_1 \cup I_2) > r(I_2) = |I_2|$, por lo que $|I_1| > |I_2|$, en contra de la elección de I_1 e I_2. Hemos probado así que $\mathcal{I}$ verifica (**I3**) y $(E, \mathcal{I})$ es una matroide.

Para acabar la demostración, falta probar que la función r definida en el enunciado es precisamente la función rango r_M de la matroide, es decir, hay que probar que $r(X) = r_M(X)$ para todo $X \subset E$. Supongamos en primer lugar que $X \in \mathcal{I}$, entonces por la definición de r, $r(X) = |X|$. Además, $r_M(X) = |X|$ ya que X es base de $M|X$. Veamos la igualdad para $X \notin \mathcal{I}$. Por una parte se tiene que $r_M(X) = |B|$, siendo B una base de $M|X$. Dicha base B es independiente maximal, luego $B \cup x \notin \mathcal{I}$ para cualquier $x \in X \setminus B$. Esto implica en términos de rango que:

$$|B| = r(B) \leq r(B \cup x) < |B \cup x| = |B| + 1.$$

Por tanto, $r(B \cup x) = r(B)$ para todo $x \in X \setminus B$. Aplicando el Lema 2.19 se llega a que $r(B \cup X) = r(B)$. Como $B \cup X = X$, tenemos que $r(X) = r(B) = |B| = r_M(X)$, como queríamos probar. □

Juntando el Teorema 2.20 junto con las propiedades que vimos que verificaba la función rango se tiene el siguiente resultado.

Corolario 2.21. *Sea E un conjunto. Una función $r\colon 2^E \longrightarrow \mathbb{N}$ es la función de rango de una matroide si y solo si satisface las propiedades* (**R1**)*,* (**R2**) *y* (**R3**)*.*

La función rango caracteriza además los conjuntos independientes, las bases y los circuitos.

Proposición 2.22. *Sea M una matroide sobre el conjunto base E con función de rango r y sea $X \subset E$. Entonces:*

- *X es independiente si y solo si $r(X) = |X|$.*
- *X es una base si y solo si $|X| = r(X) = r(M)$.*
- *X es un circuito si y solo si X es no vacío y $r(X \setminus x) = |X| - 1 = r(X)$ para cada $x \in X$.*

Demostración. Recordemos que el rango de un subconjunto X de E se define como el cardinal de una base de $M|X$ y que esta matroide tiene como familia de conjuntos independientes $\mathcal{I}|X = \{I \subset X : I \in \mathcal{I}\}$.

- Si X es independiente, entonces $X \in \mathcal{I}|X$. Además es maximal porque todos los elementos de $\mathcal{I}|X$ están contenidos en X. Es, por tanto, una base de $M|X$ y $r(X) = |X|$. Recíprocamente, $r(X) = |X|$ implica que X es una base de $\mathcal{I}|X$, en particular es un conjunto independiente.
- SI X es una base, también es un conjunto independiente y se tiene $r(X) = |X|$. Por la definición de rango se tiene también que $r(M) = |X|$. Recíprocamente, si $r(M) = |X|$, por la definición de rango, X es base de M.
- Si X es circuito, X es no vacío y es dependiente minimal, es decir, $X \setminus x \in \mathcal{I}$ para cada $x \in X$. Por lo tanto, $r(X \setminus x) = |X| - 1 = r(X)$ ya que $X \setminus x$ es una base de $M|X$. Recíprocamente, supongamos que X es no vacío y $r(X \setminus x) = |X| - 1 = r(X)$. Se tiene entonces que $X \setminus x$ es base de $M|X$ para cada $x \in X$, en particular $X \setminus x \in \mathcal{I}$ para cada $x \in X$. Puesto que además $X \neq \emptyset$, X es un circuito.

□

2.3.1. Función de nulidad.

Definición 2.23. Sea M una matroide sobre un conjunto base E con función de rango r_M. Sea $X \subset E$. La función de nulidad asociada a X es $n_M(X) = |X| - r_M(X)$.

La razón de dar esta definición es que en ocasiones nos va a interesar más trabajar con la función de nulidad de un subconjunto que con su rango, como veremos más adelante. Las propiedades asociadas a la función de nulidad se deducen inmediatamente de las que hemos probado para el rango. Resumimos las principales en los siguientes resultados.

Proposición 2.24. *Sea M una matroide sobre el conjunto base E con función de nulidad n. Entonces*

(N1) $0 \leq r(X) \leq |X|$.

(N2) *Si $X \subset Y \subset E$, entonces $n(X) \leq n(Y)$.*

(N3) *Si X e Y son subconjuntos de E, entonces*

$$n(X \cup Y) + n(X \cap Y) \leq n(X) + n(Y).$$

Además, la función de nulidad también caracteriza los conjuntos indepedientes y los circuitos. Esta caracterización se deduce inmediatamente de la Proposición 2.22.

Proposición 2.25. *Sea M una matroide sobre E con función de nulidad n_M. Sea $X \subset E$. Entonces:*

- *X es independiente si y solo si $n_M(X) = 0$.*
- *X es un circuito si y solo si X es no vacío y $n_M(X) = 1$.*

2.4. Algunas clases y ejemplos de matroides.

Vamos a explorar en esta sección una clase de matroides y a dar sus conjuntos independientes, circuitos, bases y función de rango.

Existen dos clases fundamentales de matroides, las matroides **gráficas** y las matroides **representables**. Las primeras surgen de la teoría de grafos mientras que las segundas del álgebra lineal. Vamos en este trabajo a particularizar en esta segunda clase.

Proposición 2.26. *Sea A una matriz de tamaño $m \times n$ con entradas en un cuerpo $\mathbb{K}$. Sea E el conjunto de índices de las columnas de A y sea $\mathcal{I}$ el conjunto de subconjuntos $X \subset E$ de forma que $X \in \mathcal{I}$ si los índices de X corresponden a columnas linealmente independientes en el espacio vectorial $\mathbb{K}^m$. Entonces $(E, \mathcal{I})$ es una matroide.*

En la prueba cometeremos un pequeño abuso de notación. Cuando hablemos de que $I \in \mathcal{I}$ y digamos que I es linealmente independiente, nos referiremos a que los vectores indexados por los elementos de I son linealmente independientes (en puridad I es un conjunto de índices).

Demostración. Hay que verificar que se cumplen las propiedades (**I1**), (**I2**) e (**I3**). Es claro que se verifican (**I1**) e (**I2**).

Veamos que se verifica (**I3**). Sean I_1 e I_2 dos conjuntos linealmente independientes tal que $|I_1| < |I_2|$. Consideremos el subespacio W de $\mathbb{K}^m$ generado por I_1 e I_2. Se tiene que $\dim(W) \geq |I_2|$. Razonemos por reducción al absurdo suponiendo que $I_1 \cup \{e\}$ es dependiente para todo $e \in I_2 \setminus I_1$, entonces se tiene que $W \subset \langle I_1 \rangle$ y por tanto que $|I_2| \leq \dim(W) \leq |I_1| < |I_2|$, una contradicción. Por tanto, existe un $e \in I_2 \setminus I_1$ tal que $I_1 \cup e$ es linealmente independiente. □

Definición 2.27. Las matroides obtenidas de una matriz A como en la Proposición 2.26 se denominan **matroides vectoriales** de A y se denotan por $M[A]$.

Una matroide M es **representable** sobre un cuerpo $\mathbb{K}$ si es isomorfa a la matroide vectorial de una matriz A con entradas en $\mathbb{K}$.

Ejemplo 2.28. Sea A la siguiente matriz sobre $\mathbb{R}$:

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

Con la notación de la proposición anterior se tiene que $E = \{1, 2, 3, 4, 5\}$. Los conjuntos independientes serán aquellos que correspondan a índices de columnas linealmente independientes en $\mathbb{R}^2$, luego:

$$\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{4\}, \{5\}, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}.$$

Podemos ahora determinar los conjuntos dependientes y los circuitos (que son los minimales). Los conjuntos dependientes son:

$$\{\{3\}, \{1, 4\}, \{1, 3\}, \{2, 3\}, \{3, 4\}, \{3, 5\}\} \cup \{X \subset E : \ |X| \geq 3\}.$$

Y los circuitos son $\mathcal{C} = \{\{3\}, \{1, 4\}, \{1, 2, 5\}, \{2, 4, 5\}\}$.

El conjunto de bases es

$$\mathcal{B} = \{\{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}.$$

$\diamond$

Sea $M[A]$ una matroide representable, con A una matriz $m \times n$ sobre un cuerpo $\mathbb{F}$. Dado un $X \subset E$, es claro que $r_M(X)$ es la dimensión del subespacio vectorial generado por las columnas que corresponden a los índices de X, o equivalentemente, al rango de la submatriz formada por las columnas de A correspondientes a los índices de X.

Ejemplo 2.29. Sean $m, n \in \mathbb{N}$ con $m \leq n$. Sea E un conjunto finito de n elementos y sea $\mathcal{B}$ la familia de subconjuntos de m elementos. Es claro que $\mathcal{B}$ cumple las propiedades **(B1)** y **(B2)** por lo que es el conjunto de bases de una matroide. Denotaremos esta matroide por $U_{m,n}$ y la llamaremos **matroide uniforme** de rango m sobre n elementos.

Es claro que

$$\mathcal{I}(U_{m,n}) = \{X \subset E : \ |X| \leq m\}$$

y por tanto los circuitos son

$$\mathcal{C}(U_{m,n}) = \begin{cases} \emptyset, & \text{si } m = n, \\ \{X \subset E : \ |X| = m + 1\}, & \text{si } m < n. \end{cases}$$

La función rango para la matroide uniforme es

$$r(X) = \begin{cases} |X|, & \text{si } |X| < m, \\ m, & \text{si } |X| \geq m. \end{cases}$$

◇

2.5. Matroide dual

Definimos brevemente en esta sección el concepto de matroide dual y relacionamos algunas de sus propiedades con las de la matroide original.

Consideremos una matroide $M = (E, \mathcal{I})$ y su conjunto de bases $\mathcal{B}_M$. Vamos a dar la definición de matroide dual proporcionando un conjunto de bases adecuado. Consideremos el conjunto siguiente:

$$\mathcal{B}_{\overline{M}} = \{E \setminus B : \ B \in \mathcal{B}_M\}.$$

Teorema 2.30. *El conjunto $\mathcal{B}_{\overline{M}}$ definido anteriormente es el conjunto de bases para una matroide sobre el conjunto base E.*

De acuerdo con el Corolario 2.15 es suficiente probar que el conjunto $\mathcal{B}_{\overline{M}}$ satisface las propiedades (**B1**) y (**B2**). Para ello, vamos a necesitar un lema previo, cuya demostración puede encontrarse en [Oxl06, Lemma 2.1.2].

Lema 2.31. *El conjunto de bases $\mathcal{B}$ de una matroide satisface la siguiente propiedad:*

- *Si B_1 y B_2 son dos bases y $x \in B_2 \setminus B_1$,existe un $y \in B_1 \setminus B_2$ tal que $(B_1 \setminus y) \cup x \in \mathcal{B}$.*

Demostración del Teorema 2.30. Como $\mathcal{B}_M$ es no vacío, también lo será $\mathcal{B}_{\overline{M}}$. Satisface por tanto **(B1)**. Sean ahora $\overline{B}_1 = E \setminus B_1, \overline{B}_2 = E \setminus B_2 \in \mathcal{B}_{\overline{M}}$ y sea $x \in \overline{B}_1 \setminus \overline{B}_2$. Se tiene que

$$\overline{B}_1 \setminus \overline{B}_2 = \overline{B}_1 \cap (E \setminus \overline{B}_2) = (E \setminus B_1) \cap B_2 = B_2 \setminus B_1.$$

Ahora, aplicando el Lema 2.31, existe un $y \in B_1 \setminus B_2$ tal que $(B_1 \setminus y) \cup x \in \mathcal{B}_M$. Se tiene que $y \in \overline{B}_2 \setminus \overline{B}_1$ y que $E \setminus ((B_1 \setminus y) \cup x) \in \mathcal{B}_{\overline{M}}$. ahora bien,

$$E \setminus ((B_1 \setminus y) \cup x) = ((E \setminus B_1) \setminus x) \cup y = (\overline{B}_1 \setminus x) \cup y.$$

Se cumple por tanto también **(B2)**. □

Definición 2.32 (Matroide dual)**.** La matroide sobre E con conjunto de bases $\mathcal{B}_{\overline{M}}$ se denomina **matroide dual** de M. La denotaremos por $\overline{M}$.

Observación. De la definición de matroide dual es claro que $\overline{(\overline{M})} = M$.

Vamos a dar a continuación una expresión que relaciona el rango de una matroide M con el rango de su matroide dual. La demostración se puede encontrar en [Oxl06, Prop. 2.1.9]. Vamos a denotar por r y r^*, respectivamente, a la función rango de la matroide M y de su matroide dual $\overline{M}$.

Proposición 2.33. *Sea M una matroide sobre un conjunto base E y sea $X \subset E$, se tiene que*

$$r^*(X) = |X| - r(M) + r(E \setminus X).$$

Corolario 2.34. *Con la notación anterior, se tiene que*

$$r^*(M) + r(M) = |E|.$$

2.6. Función de nulidad y circuitos no redundantes

Estudiaremos en esta sección una nueva propiedad de los circuitos de una matroide y demostraremos varios resultados que nos serán muy útiles en la posterior prueba de los dos teoremas fundamentales de este trabajo.

Definición 2.35. Sea M una matroide y sea $\Lambda \subset \mathcal{C}_M$. Se dice que los circuitos de Λ son **no redundantes** si para cada $D \in \Lambda$ se tiene que

$$\bigcup_{\mathcal{C} \in \Lambda \setminus D} \tau \subsetneq \bigcup_{C \in \Lambda} C.$$

De la definición se tiene que los circuitos de Λ son no redundantes si para cada $D \in \Lambda$ existe un $x \in D$ que no está en ningún otro circuito $C \in \Lambda$.

Definición 2.36. Sea $M = (E, \mathcal{I})$ una matroide y sea $X \subset E$. Se define el **grado de no redundancia** de X como el máximo número de circuitos no redundantes contenidos en X. Lo denotamos por $\deg(X)$.

Los siguientes resultados van encaminados a probar que la función de nulidad de un subconjunto $X \subset E$ es igual al grado de no redundancia del mismo.

Lema 2.37. *Sea M una matroide y sean $C_1, C_2, \ldots, C_s$ circuitos no redundantes. Entonces*

$$n\Big(\bigcup_{i=1}^{s} C_i\Big) \geq s.$$

Demostración. La prueba es por inducción. Para $s = 1$ el resultado es inmediato ya que la función de nulidad de un circuito es 1. Supongamos que el resultado es cierto para $s \geq 1$ y veámoslo para $s+1$. Tenemos por tanto que $C_1, \ldots, C_{s+1}$ son circuitos no redundantes y, por tanto, existe un $x \in C_{s+1}$ que no está en ninguno de los otros C_i. Aplicando la propiedad **(N3)** a los conjuntos $\bigcup_{i=1}^{s} C_i$ y a C_{s+1} se tiene que

$$n\Big(\bigcup_{i=1}^{s+1} C_i\Big) \geq s + 1 - n\Big(\bigcup_{i=1}^{s} C_i \cap C_{s+1}\Big) = s + 1,$$

donde la última igualdad se deduce de que $n\Big(\bigcup_{i=1}^{s} C_i \cap C_{s+1}\Big) = 0$ ya que está contenido en $C_{s+1} \setminus x$ y como C_{s+1} es circuito, al quitarle un elemento se obtiene un conjunto independiente. Queda probado así el resultado para $s + 1$. Queda probado el resultado por inducción. □

Corolario 2.38. *Sea M una matroide sobre E y sea $X \subset E$. Entonces*

$$n(X) \geq \deg(X).$$

Demostración. Pongamos $d = \deg(X)$. Sean $C_1, \ldots, C_d$ circuitos no redundantes contenidos en X. Se tiene que

$$n(X) \geq n\Big(\bigcup_{i=1}^{d} C_i\Big) \geq d.$$

La primera desigualdad se debe a la monotonía de la función de nulidad (propiedad **(N2)**) y la segunda al Lema 2.37. □

Lema 2.39. *Sea M una matroide y sean $C_1, \ldots, C_m$ circuitos no redundantes. Sea D otro circuito tal que $D \not\subset \bigcup_{i=1}^{m} C_i$ y sea $x \in D \setminus \bigcup_{i=1}^{m} C_i$. Entonces existe un circuito C_{m+1} que contiene a x tal que $C_1, \ldots, C_{m+1}$ son no redundantes.*

Demostración. Como los C_i son no redundantes, para cada $i = 1, \ldots, m$ podemos encontrar un $x_i \in C_i$ tal que $x_i \notin C_j$ para $j \neq i$. Vamos a considerar

$$\mathfrak{C} = \{C \in \mathcal{C}_M : x \in C\}.$$

Se tiene que $\mathfrak{C} \neq \emptyset$ ya que contiene a D. Sea C_{m+1} el elemento de $\mathfrak{C}$ que contiene el menor número de x_i. Queremos probar que dicho número es cero, razonando por reducción al absurdo. Supongamos que existe un $1 \leq i \leq m$ tal que $x_i \in C_{m+1}$. Entonces $x_i \in C_{s+1} \cap C_i$. Por **(C3)**, existe un circuito C tal que $C \subset (C_{m+1} \cup C_i) \setminus x_i$. Además, $x \in C$. Hemos encontrado por tanto un circuito contenido en $\mathfrak{C}$ con menos x_i que C_{m+1}, lo cual es absurdo. Por tanto, C_{m+1} no contiene ningún x_i. Además contiene a x, que no está en ninguno de los C_i, así, $C_1, \ldots, C_{m+1}$ son no redundantes. □

Corolario 2.40. *Sea M una matroide y sea $C_1, \ldots, C_m$ un conjunto maximal de circuitos no redundantes. Entonces*

$$\bigcup_{i=1}^{m} C_i = \bigcup_{C \in \mathcal{C}_M} C.$$

Demostración. La contención $\subset$ es inmediata. Para la contención $\supset$ hay que aplicar el Lema 2.39. Si no se diera $\supset$, existiría un circuito no contenido en la unión de los C_i y aplicando el lema podríamos encontrar un circuito C_{m+1} que, unido a los C_i, formase un conjunto de circuitos no redundantes, en contra de la maximalidad. □

Lema 2.41. *Sea M una matroide sobre E y sea $X \subset E$. Pongamos $d = n(X)$. Entonces existen d circuitos no redundantes en X y por tanto,* $\deg(X) \geq n(X)$.

Demostración. Vamos a ver primero qué ocurre con $n(X) = 0$ y $n(X) = 1$. Si $n(X) = 0$, X es independiente y no contiene ningún circuito. Si $n(X) = 1$, X es un circuito. En ambos casos se verifica el lema. Vamos ahora a razonar por reducción al absurdo. Sea X un conjunto minimal para la inclusión con la propiedad de que $\deg(X) < n(X)$. Tiene que ser $n(X) \geq 2$, por tanto, X es dependiente y contiene un circuito C. Como los circuitos son no vacíos, existe un $x \in C$. Consideremos $X' = X \setminus x$. El lema se verifica para este X' (por la minimalidad de X) y podemos por tanto encontrar al menos $n(X')$ circuitos no redundantes contenidos en X'. Como $d - 1 \leq n(X') \leq d$, encontramos al

menos $d-1$ circuitos no redundantes $C_1, \ldots, C_{d-1}$ contenidos en X', y por tanto, en X. Puesto que

$$x \in C \setminus \Big(\bigcup_{i=1}^{d-1} C_i \Big),$$

podemos aplicar el Lema 2.39 y obtener un circuito C_d que junto a los C_i forme un conjunto no redundante. Esto es absurdo ya que $C_1, \ldots, C_d$ son un conjunto de $d = n(X)$ circuitos contenidos en X. □

Juntando los resultados del Corolario 2.38 y el Lema 2.41 se tiene lo siguiente:

Proposición 2.42. *Sea M una matroide sobre E y sea $X \subset E$. Entonces*

$$\deg(X) = n(X).$$

2.7. Relación entre matroides y códigos

Vamos a ver en esta sección cómo asociar una matroide a un código lineal. Definiremos también los pesos de Hamming generalizados para una matroide en general y, en el caso de que sea la matroide asociada a la matriz de control de un código, veremos que coinciden con los que ya habíamos definido en 1.15. Estudiaremos las relaciones entre matroide dual asociada a un código y matroide asociada al código dual y caracterizaremos los códigos MDS por su matroide asociada.

Consideremos un código lineal C de tipo $[n, k]$ sobre $\mathbb{F}_q$ con matriz generatriz G (que será de tamaño $k \times n$). Se puede asociar una matroide M a dicho código como en la Proposición 2.26, esto es, el conjunto base es el conjunto $E = \{1, \ldots, n\}$ y los conjuntos independientes son los subconjuntos de E que corresponden a índices tales que las columnas de G asociadas son linealmente independientes, vistas como vectores en $\mathbb{F}_q^k$. Denotaremos dicha matroide por M_G.

Debemos ver que dicha matroide no depende de la matriz generatriz elegida para C, es decir, que si G_1 y G_2 son dos matrices generatrices de C, entonces $M_{G_1} = M_{G_2}$. Como son dos matrices del mismo código, su forma escalonada reducida es la misma. Es un hecho conocido de álgebra lineal que el rango se mantiene por tranformaciones por filas, de modo que si $I = \{i_1, \ldots, i_t\}$ es un conjunto independiente de M_{G_1}, es decir, las columnas correspondientes a esos índices son linealmente independientes; al llegar a la forma escalonada

reducida, se tiene que dichas columnas son también independientes. Realizando de nuevo operaciones por filas desde la matriz escalonada reducida se llega a G_2, de modo que las columnas de G_2 correspondientes a los índices de I también son linealmente independientes.

Dado un código lineal C, denotaremos por M_C a la matroide asociada a cualquiera de sus matrices generatrices.

En esta memoria, vamos a trabajar con la matroide asociada a una de las matrices de control H de un código. Puesto que una matriz de control de C es una matriz generatriz del código dual, la matroide no depende de la elección de H.

Definición 2.43. Sea $M = (E, \mathcal{I})$ una matroide. Los pesos de Hamming generalizados de M se definen como

$$d_i = \text{mín}\{|X| : X \subset E\ ,\ |X| - r(X) = i\},\ \text{para}\ i = 1, \ldots, |E| - r(E).$$

Claramente, para una matroide asociada a la matriz de control de un código, esta expresión coincide con la dada en el Teorema 1.18.

Nuestro siguiente objetivo es probar que los códigos MDS son precisamente aquellos para los cuales la matroide asociada es la matroide uniforme. Para ello necesitamos el siguiente resultado previo. La demostración puede encontrarse en [PWBJ17, Prop 2.2.5].

Proposición 2.44. *Sea* C *un código de tipo* $[n, k, d]$ *sobre* $\mathbb{F}_q$. *Sean* G *y* H *una matriz generatriz y de control, respectivamente, de* C. *Las siguientes afirmaciones son equivalentes:*

1. C *es un código MDS.*
2. *Cada* $(n - k)$ *columnas de* H *son linealmente independientes.*
3. *Cada* k *columnas de* G *son linealmente independientes.*

Proposición 2.45. *Sea* C *un código de tipo* $[n, k]$ *con matriz generatriz* G. C *es un código MDS si y solo si la matroide asociada* $M[G]$ *es la matroide uniforme* $U_{k,n}$.

Demostración. Por la Proposición 2.44, el código C es MDS si y solo si cada k columnas de una matriz generatriz son linealmente independientes. Esto es equivalente a que todos los conjuntos de j elementos con $j \leq k$ dentro de $M[G]$ sean independientes, de hecho, solamente estos conjuntos son los independientes. Esta matroide es precisamente $U_{k,n}$. □

A continuación, vamos a estudiar la relación existente entre la matroide dual asociada a un código y la matroide asociada al dual de un código. Para ello, necesitamos estudiar en primer lugar dos tipos de códigos que se construyen a partir de uno dado.

Definición 2.46. Sea C un código lineal de tipo $[n, k]$ sobre $\mathbb{F}_q$. Sea $J \subset \{1, \ldots, n\}$. Se define el **código punteado**, C_J, como la imagen de la proyección $\pi_{[n]\setminus J} : \mathbb{F}_q^n \to \mathbb{F}_q^{n-|J|}$, es decir, es el código obtenido al restringirnos a las coordenadas en el complementario de J.

Definición 2.47. Sea C un código lineal de tipo $[n, k]$ y sea $J \subset \{1, \ldots, n\}$. Sea $\mathrm{C}(J)$ el subcódigo de C formado por aquellas palabras tales que $c_i = 0$ si $i \in J$. Se define el **código acortado**, C^J, como el código punteado $\mathrm{C}(J)_J$.

Vamos a necesitar el siguiente lema previo, cuya demostración puede encontrarse en [PWBJ17, Prop. 2.1.7].

Lema 2.48. *Sea* C *un código de tipo* $[n, k]$ *y sea* $J \subset \{1, \ldots, n\}$ *. Entonces se tiene*

$$(\mathrm{C}^J)^\perp = (\mathrm{C}^\perp)_J.$$

Proposición 2.49. *Sea* C *un código de tipo* $[n, k]$ *con matriz generatriz* G *y matriz de control* H*, entonces las matroides* $\overline{M_C}$ *y* $M_{C^\perp}$ *coinciden.*

Demostración. La prueba se basa en demostrar que la matroide $M_{C^\perp} = M_H$ tiene la misma función rango que la matroide $\overline{M_C} = \overline{M_G}$ ya que, por el Teorema 2.20, la función rango caracteriza a una matroide. Recodermos que la función rango para la matroide dual viene dada por la expresión de la Proposición 2.33. Dado un $J \subset \{1, \ldots, n\}$, vamos a denotar por H_J la submatriz de H correspondiente a tomar las columnas de J y por $[n] \setminus J$ al complementario del conjunto J. Nuestro objetivo es probar que

$$r(H_{[n]\setminus J}) = |[n] \setminus J| - k + r(G_J), \text{ para todo } J \subset \{1, \ldots, n\}.$$

Por el lema anterior, se tiene que

$$\dim(\mathrm{C}^\perp)_J = \dim((\mathrm{C}^J)^\perp) = |[n] \setminus J| - \dim(\mathrm{C}^J).$$

La primera igualdad se debe al lema y la segunda es una propiedad conocida del dual de un código. Además, se tiene que $\dim(\mathrm{C}^J) = k - \dim(\mathrm{C}_{[n]\setminus J})$. En efecto, consideremos la proyección sobre J,

$$\pi_J : \mathrm{C} \longrightarrow \mathrm{C}_{[n]\setminus J}.$$

Se tiene que π_J es sobreyectiva y $\ker(\pi_J) = \mathrm{C}(J) \cong \mathrm{C}^J$, por lo que $\dim(\mathrm{C}_{[n]\setminus J})+\dim(\mathrm{C}^J) = \dim(\mathrm{C}) = k$. Para finalizar, observemos que $\dim(\mathrm{C}^\perp)_J = r(H_{[n]\setminus J})$ y $\dim(\mathrm{C}_{[n]\setminus J}) = r(G_J)$. □

Capítulo 3

Resoluciones libres

Este capítulo, cuyo contenido es puramente algebraico, tiene como objetivo explicar en qué consiste la resolución libre de un módulo y poder definir con ello los números de Betti. La Sección 3.1 y la Sección 3.2 presentan los conceptos de anillo y módulo graduados, respectivamente. En la Sección 3.3, damos la definición de resolución libre graduada para un módul y definimos los números de Betti asociados a una resolución libre minimal. Finalmente, en la Sección 3.4 nos centramos en los complejos simpliciales, veremos cómo asociar a éstos una estructura de anillo, el llamado anillo de Stanley-Reisner, y estudiaremos algunas de sus propiedades. También definimos en esta última sección la homología simplicial.

3.1. Anillos graduados

Definición 3.1 (Anillo graduado)**.** Sea R un anillo. Se dice que R es un **anillo graduado** si existe una familia $\{R_i\}_{i\in\mathbb{N}}$ de subgrupos aditivos de R tales que:

- $R = \bigoplus_{i\in\mathbb{N}} R_i$ (como grupos),
- $R_i R_j \subset R_{i+j}$ para cada $i, j \in \mathbb{N}$.

El subgrupo R_i se denomina **componente homogénea de grado** i. Si $f \in R_i$ se dice que f es un elemento homogéneo de grado i y se denota por $\deg(f) = i$.

De la descomposición del anillo como suma directa de subgrupos aditivos se deduce que si $f \in R$, entonces se puede escribir de forma única como suma

de sus componentes homogéneas $f = \sum_{i\in\mathbb{N}} f_i$, con $f_i = 0$ salvo una cantidad finita.

La definición anterior se puede generalizar y se pueden considerar graduaciones donde el conjunto de grados sea un semigrupo S. Si este es el caso, se dice que el anillo R está S-graduado.

Ejemplo 3.2. El anillo de polinomios en una variable con coeficientes en un cuerpo $\mathbb{K}[t]$ tiene estructura de anillo graduado tomando como R_i el conjunto de polinomios de grado i. ◇

Observación. Vamos a introducir una graduación en $S = \mathbb{K}[x_1, x_2, \ldots, x_n]$, el anillo de polinomios en varias variables sobre un cuerpo $\mathbb{K}$. Diremos que un monomio $x_1^{c_1} \cdots x_n^{c_n}$ tiene grado $c_1 + \cdots + c_n$ y denotaremos por S_i el $\mathbb{K}$-espacio vectorial generado por los monomios de grado i. En particular, se tiene que $S_0 = \mathbb{K}$. Con esta graduación introducida es claro que $S = \bigoplus_{i\in\mathbb{N}} S_i$ y $S_i S_j \subset S_{i+j}$. Esta graduación recibe el nombre de **graduación estándar**.

Ejemplo 3.3. Consideremos el anillo $S = \mathbb{K}[x, y]$. Se tiene que $S_0 = \mathbb{K}$, S_1 es el espacio vectorial de polinomios homogéneos de grado 1, S_2 el espacio vectorial de polinomios homogéneos de grado 2, y así sucesivamente. El polinomio $f = xy^2 + x^3 + x^4y + x^2y^3$ tiene dos componentes homogéneas, una de grado 3 que es $xy^2 + x^3$ y otra de grado 5 que es $x^4y + x^2y^3$. ◇

Vamos a ver a continuación cómo se traslada esta estructura graduada del anillo a los ideales propios de éste.

Definición 3.4. Sea R un anillo graduado. Un ideal $I \subset R$ se dice que es **homogéneo** (o graduado) si para cada $f \in I$, las componentes homogéneas de f están también en I.

Proposición 3.5. *Sea I un ideal de un anillo graduado $R = \bigoplus_{i\in\mathbb{N}} R_i$. Las siguientes condiciones son equivalentes:*

1. *I es un ideal homogéneo.*
2. *$I = \bigoplus_{i\in\mathbb{N}} I_i$ donde $I_i = I \cap R_i$.*
3. *Si $\tilde{I}$ es el ideal generado por los elementos homogéneos de I, entonces $\tilde{I} = I$.*
4. *I tiene un sistema de generadores homogéneos.*

Demostración. $1 \Rightarrow 2$. Sea $f \in I$. Como $f \in R$, f se puede descomponer en sus componentes homogéneas $f = \sum_{i\in\mathbb{N}} f_i$ con $f_i \in R_i$. Por ser I homogéneo,

$f_i \in I$ para cada $i \in \mathbb{N}$. Se tiene entonces que $f_i \in I \cap R_i$ y que $f = \sum_{i\in\mathbb{N}} f_i$ de forma única, luego $I = \bigoplus_{i\in\mathbb{N}} I_i$.

$2 \Rightarrow 3$. Claramente se tiene que $\tilde{I} \subset I$, veamos la contención contraria. Sea $f \in I$, por hipótesis se tiene que $f = \sum_{i\in\mathbb{N}} f_i$ donde $f_i \in I \cap R_i$, es decir, las f_i son elementos homogéneos de I y por tanto $f \in \tilde{I}$.

$3 \Rightarrow 4$. Es inmediato.

$4 \Rightarrow 1$. Dado $f \in I$, se puede escribir como $f = \sum_j r_j g_j$ donde $r_j \in R$ y los g_j son los generadores homogéneos de I. La componente homogénea de grado i de f será por tanto la correspondiente a sumar las componentes homogéneas de $r_j g_j$ que son elementos de I. Por tanto, $f_i \in I$ para cada i. □

Observación. Si I es un ideal homogéneo de S se tiene que $S_i I_j \subset I_{i+j}$ para cada $i, j \in \mathbb{N}$. Esto es claro ya que en particular se tiene que $I_j \subset S_j$ y la condición de ideal.

Vamos a explicar ahora cómo se traslada la graduación de un anillo S a un anillo cociente $R = S/I$ por un ideal homogéneo I de S. Esto será interesante ya que muchos de los anillos con los que vamos a trabajar, en particular el anillo de Stanley-Reisner sobre un complejo simplicial (que definiremos posteriormente), son anillos cociente de $S = \mathbb{K}[x_1, \ldots, x_n]$.

Proposición 3.6. *Sea S un anillo graduado y sea I un ideal homogéneo de S. El anillo cociente $R = S/I$ hereda de forma natural la graduación de S por $R_i = S_i/I_i$. Es decir, el anillo cociente R tiene la siguiente descomposición:*

$$R = S/I = \bigoplus_{i\in\mathbb{N}} R_i = \bigoplus_{i\in\mathbb{N}} (S/I)_i \cong \bigoplus_{i\in\mathbb{N}} S_i/I_i.$$

Demostración. Recordemos que la condición de suma directa en los anillos graduados se entiende como suma directa de grupos. Se tiene que I_i y S_i son grupos conmutativos para cada $i \in \mathbb{N}$ (son por tanto normales) y tiene sentido considerar S_i/I_i. Es un resultado conocido de teoría de grupos que $\bigoplus_{i\in\mathbb{N}} S_i / \bigoplus_{i\in\mathbb{N}} I_i \cong \bigoplus_{i\in\mathbb{N}} (S_i/I_i)$. Para obtener el resultado, basta tomar como $(S/I)_i$ la contraimagen de R_i/I_i por tal isomorfismo. □

Notación. En el resto del capítulo, S denotará el anillo de polinomios en n variables con coeficientes en un cuerpo $\mathbb{K}$, esto es, $S = \mathbb{K}[x_1, \ldots, x_n]$, I denotará un ideal homogéneo propio de dicho anillo y $R = S/I$ el anillo cociente correspondiente.

Denotaremos por $\mathfrak{m}$ al ideal $\langle x_1, \dots x_n \rangle$ generado por las n indeterminadas del anillo S. Este ideal es maximal y homogéneo. Una observación relevante es que cualquier ideal I propio homogéneo de S está contenido en $\mathfrak{m}$.

Merece la pena detenerse a comprender algo mejor la estructura de S y R como anillos graduados. Resumimos en la siguiente proposición algunas de las propiedades que usaremos más adelante. Vamos a denotar por $\bar{\mathfrak{m}}$ al ideal $\mathfrak{m}/I$ del anillo cociente R.

Proposición 3.7. *Sea $S = \mathbb{K}[x_1, \dots, x_n]$, I un ideal homogéneo propio de este anillo y sea $R = S/I$ el anillo cociente. Consideremos en S la graduación estándar. Se verifica:*

1. *R es noetheriano.*
2. *$R_0 \cong \mathbb{K}$ y por lo tanto, R_i es un k-espacio vectorial de dimensión finita para cada $i \in \mathbb{N}$.*
3. *$\bigoplus_{i \geq 1} R_i = \bar{\mathfrak{m}}$*
4. *$R = R_0 \oplus \bar{\mathfrak{m}}$*

Demostración.

1. S es un anillo noetheriano por el Teorema de la Base de Hilbert (ver [Eis13, Th. 1.2]). Como los ideales de R están en correspondencia con los ideales de S que contienen a I, los ideales de R serán también finitamente generados.

2. Observemos que la componente homogénea de grado 0 en R es S_0/I_0, con la graduación estándar se tiene que $S_0 = \mathbb{K}$ y como I_0 es ideal propio de S e $I_0 \subset \mathbb{K}$, que es cuerpo, $I_0 = \{0\}$. Por tanto, $R_0 \cong S_0/I_0 \cong \mathbb{K}/\{0\} \cong \mathbb{K}$.

3. Para el anillo S se tiene la siguiente descomposición

$$S = S_0 \oplus \Big(\bigoplus_{i \geq 1} S_i \Big) = k \oplus \mathfrak{m}.$$

   Al pasar al anillo cociente por el ideal I se tiene que $\bigoplus_{i \geq 1} R_i = \bar{\mathfrak{m}}$.

4. Es inmediato de 2 y 3.

□

3.2. Módulos graduados

Ya hemos definido el concepto de graduación para anillos y para ideales. Puesto que el concepto de ideal de un anillo se puede extender al de módulo, resulta también natural extender el concepto de graduación a los módulos sobre anillos.

Definición 3.8 (Módulo graduado)**.** Sea M un R-módulo. Se dice que M es **graduado** si existe una familia de subgrupos $\{M_i\}_{i\in\mathbb{N}}$ tal que:

- $M = \bigoplus_{i\in\mathbb{N}} M_i$,
- $R_i M_j \subset M_{i+j}$ para cada $i, j \in \mathbb{N}$.

Los subgrupos $\{M_i\}_{i\in\mathbb{N}}$ son las **componentes homogéneas de grado** i. Un elemento m se dice que es homogéneo si $m \in M_i$ para algún $i \in \mathbb{N}$. La condición de suma directa implica que todo elemento $m \in M$ se escribe de forma única como $m = \sum_{i\in\mathbb{N}} m_i$ siendo todos los sumandos nulos salvo una cantidad finita de ellos.

Observación. Se tiene que $R_0 = \mathbb{K}$ y como $R_0 M_i \subset M_i$ se tiene que M_i es un $\mathbb{K}$-espacio vectorial y por tanto la suma directa es como espacios vectoriales.

Al igual que vimos para ideales homogéneos se tiene lo siguiente.

Proposición 3.9. *Sea N un R-módulo graduado. Existe un sistema de generadores homogéneo de N. Los grados de los elementos en un sistema de generadores homogéneos determinan la graduación de N*

Demostración. Basta tomar las componentes homogéneas de los elementos de un sistema de generadores de N. □

Definición 3.10 (Graduación desplazada)**.** Sea $M = \bigoplus_{i\in\mathbb{N}} M_i$ un R-módulo graduado. Se define la **graduación desplazada** de M como el módulo $M(p)$ donde $M(p)_i = M_{p+i}$.

Observación. En las resoluciones de módulos que trataremos más adelante nos aparecen fundamentalmente desplazamientos del tipo $R(-p)$ con $p > 0$. Notemos que $R(-p)_p = R_{p-p} = R_0$, es decir, los elementos homogéneos de $R(-p)$ tienen grados mayores o iguales que p.

Nuestro objetivo va a ser probar que todo R-módulo graduado finitamente generado será isomorfo al cociente de una suma directa de módulos del tipo $R(-p)$. Para ello necesitamos la noción de homomorfismo graduado y de submódulo graduado.

Las demostraciones para submódulos graduados son análogas a las de ideales, con lo que las omitiremos en pos de una redacción más concisa.

Definición 3.11 (Submódulo homogéneo)**.** Sea M un R-módulo graduado. Se dice que N es un **submódulo homogéneo** o graduado si para cada $f \in N$, las componentes homogéneas de f están también en N.

Proposición 3.12. *Sea N un submódulo de un R-módulo graduado M. Son equivalentes:*

1. *N es homogéneo.*
2. *$N = \bigoplus_{i\in\mathbb{N}} N_i$ donde $N_i = M_i \cap N$.*
3. *Si $\tilde{N}$ es el submódulo generado por los elementos homogéneos de N entonces $N = \tilde{N}$.*
4. *N tiene un sistema de generadores homogéneos.*

Definición 3.13 (Grado de un homomorfismo)**.** Sean M y N dos R-módulos graduados. Diremos que un homomorfismo $\varphi : M \longrightarrow N$ tiene grado i si $deg(\varphi(m)) = i + deg(m)$ para cada elemento homogéneo $m \in M \setminus \ker(\varphi)$. El conjunto de homomorfismos de grado i de M en N se denota por $Hom_i(M, N)$. Un homomorfismo $\varphi : M \longrightarrow N$ se llama graduado u homogéneo (u homomorfismo de módulos graduados) si $\varphi \in Hom_i(M, N)$ para algún i.

Si $\varphi : M \longrightarrow N$ es un homomorfismo de R-módulos graduados y $f = f_1 + \cdots + f_p$ es la descomposición de f en sus componentes homogéneas entonces $\varphi(f_1), \ldots, \varphi(f_p)$ son las componentes homogéneas de $\varphi(f)$. Este hecho es consecuencia de la linealidad de φ y de que es un homomorfismo de grado i.

Si M y N son dos módulos graduados, definimos el grupo de homomorfismos graduados de M en N como $\mathcal{H}(M, N) = \bigoplus_{i\in\mathbb{N}} Hom_i(M, N)$. En general $\mathcal{H}(M, N)$ será un submódulo de $Hom(M, N)$ y van a coincidir cuando el módulo de partida sea finitamente generado. Una demostración de este aserto puede encontrarse en [Pee10, 2.7].

Proposición 3.14. *Sea $\varphi : M \longrightarrow N$ un homomorfismo de R-módulos graduados, entonces* $\ker(\varphi)$ *e* $\mathrm{im}(\varphi)$ *son submódulos graduados.*

Demostración. Veamos que el núcleo es graduado. Sea $f \in \ker(\varphi)$, como M es un módulo graduado se puede escribir $f = f_1 + \cdots + f_p$ como suma de sus componentes homogéneas. Si $\varphi(f_i) \neq 0$ para algún $i = 1, \ldots, p$ entonces

$\varphi(f_i)$ es una componente homogénea de $\varphi(f)$. Puesto que $\varphi(f) = 0$ sus componentes homogéneas han de ser también nulas luego $\varphi(f_i) = 0$ para todo $i = 1, \ldots, p$, es decir, $f_i \in \ker(\varphi)$ para todo $i = 1, \ldots, p$.

Veámoslo ahora para la $\mathrm{im}(\varphi)$. Sea $g \in \mathrm{im}(\varphi)$, existe un $f \in M$ tal que $g = \varphi(f)$. Sea $f = f_1 + \cdots + f_p$ la descomposición de f en sus componentes homogéneas, se tiene que $\varphi(f_i)$ son las componentes homogéneas de $\varphi(f) = g$ luego todas las componentes homogéneas de g están en $Im(\varphi)$ como queríamos probar. □

Podemos ahora probar un resultado de estructura para R-módulos graduados finitamente generados:

Teorema 3.15. *Las condiciones siguientes son equivalentes:*

1. *U es un R-módulo finitamente generado.*
2. *$U \cong W/T$, donde W es una suma directa finita de módulos libres desplazados, T es un submódulo graduado de W y el isomorfismo conserva los grados.*

Demostración. La implicación recíproca es inmediata, si $U \cong W/T$ y W es suma directa finita de módulos libres, W es finitamente generado y U también. Probemos pues la implicación directa.
Como U es un R-módulo graduado finitamente generado, tiene un sistema finito de generadores homogéneos $\{m_1, ..., m_j\}$. Sean $a_1, ..., a_j$ sus respectivos grados. Consideremos $W = R(-a_1) \oplus R(-a_2) \oplus \cdots \oplus R(-a_j)$. Para cada $1 \leq i \leq j$, vamos a denotar por e_i el generador de W de la forma $(0, \ldots, 1, \ldots, 0)$, con un 1 en la posición i-ésima. Consideremos ahora el homomorfismo siguiente (extendido por linealidad):

$$\begin{array}{rccc} \varphi\colon W = R(-a_1) \oplus R(-a_2) \oplus ... \oplus R(-a_j) & \longrightarrow & U \\ e_i & \longmapsto & m_i \end{array}$$

La aplicación φ es sobreyectiva. En efecto, si tomamos $u \in U$ se puede escribir como $\sum_i m_i$ y se tiene que $u = \sum_i \varphi(e_i) = \varphi(\sum_i e_i)$ y por tanto $u \in Im(\varphi)$. Si consideramos $T = \ker(\varphi)$, ya sabemos que T es graduado y el teorema de isomorfía nos dice que $U \cong W/T$. Es claro que el isomorfimo conserva los grados. □

Damos a continuación un lema que nos resultará fundamental a la hora de establecer relaciones entre los generadores. El resultado que nosotros necesitamos está adaptado para el caso de módulos graduados. La versión general para anillos locales del lema de Nakayama se puede consultar en [Mat89].

Proposición 3.16 (Lema de Nakayama)**.** *Sea J un ideal propio graduado en R y sea U un R-módulo finitamente generado. Se tiene que:*

1. *Si $U = JU$ entonces $U = 0$.*
2. *Si W es un R-submódulo graduado de U tal que $U = W + JU$, entonces $U = W$.*

Demostración. Vamos a razonar por reducción al absurdo para probar 1. Supongamos que $U \neq 0$, entonces existe un elemento $m \neq 0$ de U de grado mínimo, es decir, $U_j = 0$ para todo $j < deg(m)$. Como J es un ideal propio y R está graduado por $\mathbb{N}$ se tiene que todo elemento homogéneo de JU tiene grado estrictamente mayor que $deg(m)$. Esto es porque los elementos de JU son de la forma ab donde $a \in J$ y $b \in U$ y por tanto $deg(ab) \geq deg(a) + deg(m)$; puesto que J es propio, todos los elementos de J tienen grado mayor estrictamente que 0 y por tanto $deg(ab) > deg(m)$. Ahora bien, $m \in U$ y, por hipótesis, $U = JU$ luego $m \in JU$. Con consecuencia se llega a que $\deg(m) > deg(m)$. Esto es absurdo. Se tiene entonces que $U = 0$.

Apliquemos el apartado 1 a U/W. Más precisamente, por hipótesis se tiene que $U = W + JU$, luego $U/W = W/W + JU/W = J(U/W)$. Por el apartado 1 se tiene que $U/W = 0$ y por tanto $U = W$. □

El resultado anterior es de capital relevancia para probar el siguiente teorema, que nos caracteriza los conjuntos de generadores homogéneos minimales de un R-módulo graduado finitamente generado U. Un **sistema de generadores homogéneos minimal** es un sistema generador homogéneo de modo que ninguno de sus subconjuntos propios es sistema generador.

Recordemos que $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$. Si U es un R-módulo graduado finitamente generado y consideramos $\tilde{U} = U/\mathfrak{m}U$ se tiene que $\tilde{U}$ es un espacio vectorial sobre k (Recordemos que $R = k[x_1, \ldots, x_n]/I$ y lo que estamos haciendo es eliminar las variables). Además $\tilde{U}$ tiene dimensión finita como k-espacio vectorial porque U es finitamente generado.

Teorema 3.17. *Sea U un R-módulo graduado finitamente generado. Consideremos $\tilde{U}$ como antes y denotemos por p su dimensión.*

1. *Si $\{\tilde{u_1}, \ldots, \tilde{u_p}\}$ es una base homogénea de $\tilde{U}$ (como k-espacio vectorial), entonces $\{u_1, \ldots, u_p\}$ es un sistema minimal de generadores homogéneos.*
2. *Todo sistema minimal de generadores homogéneos de U se obtiene de la forma anterior.*

3. Todo sistema minimal de generadores homogéneos tiene p elementos.

Demostración. Vamos a probar 1. Puesto que $\{\tilde{u_1}, \ldots, \tilde{u_p}\}$ son base de $U/\mathfrak{m}U$ podemos escribir $U = \mathfrak{m}U + Ru_1 + \cdots + Ru_p$, donde Ru_i denota el R-módulo generado por u_i, para cada $i = 1, \ldots, p$. Por el Lema de Nakayama se tiene que $U = Ru_1 + \cdots + R_up$. Esto prueba que $\{u_1, \ldots, u_p\}$ es sistema generador homogéneo. Falta ver la minimalidad. Razonemos por reducción al absurdo suponiendo que $\{u_1, \ldots, u_p\}$ no es minimal; en este caso puede escribirse (tras quizá un reordenamiento) $u_1 = \sum_{i=2}^{p} a_i u_i$ para algunos $a_i \in R$. Al pasar al cociente por $\mathfrak{m}$ se tendría que $\tilde{u_1} = \sum_{i=2}^{p} \tilde{a_i}\tilde{u_i}$, en contra de que $\{\tilde{u_1}, \ldots, \tilde{u_p}\}$ es una base.

Veamos 2. Supongamos que $\{u_1, \ldots, u_p\}$ es un sistema minimal de generadores homogéneos. Entonces se tiene que $\{\tilde{u_1}, \ldots, \tilde{u_p}\}$ generan $\tilde{U}$. Queremos ver que, de hecho, son una base. Razonemos por reducción al absurdo y supongamos que son linealmente dependientes. Entonces, existen $\tilde{u_{i_1}}, \ldots, \tilde{u_{i_l}} \in \{\tilde{u_1}, \ldots, \tilde{u_p}\}$ que forman una base de $\tilde{U}$. Por el apartado 1, $\{u_{i_1}, \ldots, u_{i_l}\}$ serían un sistema de generadores de U en contra de la minimalidad de $\{u_1, \ldots, u_p\}$.

El apartado 3 es consecuencia de 1 y 2. □

Una vez abordados los conceptos básicos acerca de anillos y módulos graduados, vamos a tratar ahora los complejos de cadena graduados, que nos llevarán a la definición de resolución libre. Daremos un modo de calcular la resolución libre de un módulo, definiremos resolución minimal y podremos definir los números de Betti en base a una resolución minimal.

3.3. Complejos graduados y resoluciones libres

Definición 3.18 (Complejo de cadena)**.** Sea R un anillo. Un **complejo de cadena** es una sucesión de R-módulos $\{M_i\}_{i\in\mathbb{Z}}$ y homomorfismos $\{d_i\}_{i\in\mathbb{Z}}$

$$\cdots \longrightarrow M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots \longrightarrow M_1 \xrightarrow{d_1} M_0 \longrightarrow \cdots$$

tal que $d_{i-1} \circ d_i = 0$ para cada $i \in \mathbb{Z}$. Esta condición es equivalente a que $\mathrm{im}(d_i) \subset \ker(d_{i-1})$. Los homomorfismos d_i reciben el nombre de **diferenciales** y la familia $\{d_i\}_{i\in\mathbb{Z}}$ se llama **diferencial**. Se dice que el complejo es

exacto en la posición i si $(d_{i+1}) = \ker(d_i)$. Se dice que el complejo es **graduado** si los módulos M_i son graduados y cada d_i es un homomorfismo de grado 0. En este caso cada uno de los módulos M_i lo podemos escribir como $M_i = \bigoplus_{j\in\mathbb{Z}} M_{i,j}$. Vamos a decir que un elemento en $M_{i,j}$ tiene **grado de homología** i y **grado interno** j.

Definición 3.19 (Morfismo de complejos)**.** Si tenemos dos complejos de cadena, esto es, dos sucesiones de R-módulos $\{M_i\}_{i\in\mathbb{Z}}$, $\{N_i\}_{i\in\mathbb{Z}}$ y respectivos homomorfismos $\{d_i\}_{i\in\mathbb{Z}}$, $\{\delta_i\}_{i\in\mathbb{Z}}$, un **homomorfismo de complejos** es una familia de homomorfismos $\varphi_i\colon M_i \longrightarrow N_i$ que hacen conmutativo el siguiente diagrama:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & M_i & \xrightarrow{d_i} & M_{i-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_{i-1}} & & \\ \cdots & \longrightarrow & N_i & \xrightarrow{\delta_i} & N_{i-1} & \longrightarrow & \cdots \end{array}$$

esto es, $\delta_i \circ \varphi_i = \varphi_{i-1} \circ d_i$ para todo $i \in \mathbb{Z}$.

Definición 3.20 (Resolución libre)**.** Sea U un R-módulo finitamente generado. Una **resolución libre** del módulo U es un complejo de cadena

$$\cdots \longrightarrow F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0$$

tal que

1. F_i es un módulo libre finitamente generado para cada $i \in \mathbb{N}$
2. El complejo es exacto en cada posición.
3. $U \cong F_0/Im(d_1)$

Precisamente por esta última condición, unido al hecho de que pedimos la exactitud en el complejo, la resolución suele escribirse de la forma siguiente:

$$\cdots \longrightarrow F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} U \longrightarrow 0\,.$$

Para finalizar, diremos que la resolución es **graduada** si U es un R-módulo graduado, el complejo es graduado y el isomorfismo $U \cong F_0/Im(d_1)$ tiene grado 0.

Supomgamos ahora que tenemos U un R-módulo graduado finitamente generado. Vamos a construir de forma recursiva una resolución libre graduada sobre U.

- **Paso 0:** Escojamos $m_1, ..., m_r$ generadores homogéneos de U. Esto puede hacerse ya que U es graduado y finitamente generado. Sean $a_1, \ldots, a_r$ sus respectivos grados. Consideremos ahora $F_0 = R(-a_1) \oplus ... \oplus R(-a_r)$. Tomamos f_j, $1 \leq j \leq r$ el elemento de la base canónica de F_0, que es de la forma $(0, \ldots, 1, \ldots, 0)$ con un 1 en la posición j-ésima. Definimos el morfismo siguiente:

$$\begin{array}{rccc} d_0 \colon & F_0 & \longrightarrow & U \\ & f_j & \longmapsto & m_j \end{array}$$

  Se tiene que F_0 es un módulo libre y el homomorfismo φ conserva los grados (es de grado 0). Además es sobreyectivo.

  Supongamos que hemos construido recursivamente los módulos F_i con los respectivos homomorfismos d_i de tal forma que el complejo sea exacto.

- **Paso i + 1**: Consideremos $\ker(d_i) \subset F_i$ y escojamos generadores homogéneos $l_1, \ldots, l_s$ de dicho núcleo. Sean $\alpha_1, \ldots, \alpha_s$ sus respectivos grados. Consideramos $F_{i+1} = R(-\alpha_1) \oplus ... \oplus R(-\alpha_s)$. Para cada $1 \leq j \leq s$, escogemos g_j el generador de $R(-\alpha_j)$ (se tiene que $deg(g_j) = \alpha_j$).

  Definimos el morfismo siguiente:

$$\begin{array}{rccc} d_{i+1} \colon & F_{i+1} & \longrightarrow & \ker(d_i) \\ & g_j & \longmapsto & l_j \end{array}$$

  Este homomorfimo es sobreyectivo, claramente $Im(d_{i+1}) = \ker(d_i)$ y conserva grados (es de grado 0).

Observación. El Teorema de las Sicigias de Hilbert (en inglés, *Hilbert´s Syzygy Theorem*) garantiza que todo $\mathbb{K}[x_1, \ldots, x_n]$-módulo finitamente generado tiene una resolución libre finita y de tamaño a lo sumo n. Una demostración de este teorema se puede consultar [Eis13]. Por lo tanto, en la construcción anterior existe una forma de escoger los generadores homogéneos para acabar en a lo sumo n pasos.

3.3.1. Resoluciones minimales y números de Betti

En esta sección vamos a estudiar el concepto de resolución minimal y a definir los **números de Betti**.

La notación en las siguientes definiciones y teoremas es la utilizada en la sección anterior a la hora de definir y construir la resolución libre de un módulo.

Definición 3.21 (Resolución minimal)**.** Una resolución libre graduada de un R-módulo U finitamente generado es **minimal** si

$$d_{i+1}(F_{i+1}) \subset (x_1, \ldots, x_n)F_i$$

para cada $i \geq 0$

En una resolución libre cada uno de los F_i son módulos libres de modo que podemos fijar una base de elementos homogéneos en cada uno de ellos. De este modo, los homomorfismos d_i se pueden representar por matrices en dichas bases, cuyas entradas son elementos homogéneos de R. De la definición se deduce que una resolución minimal es aquella en la que no aparecen elementos invertibles en dichas matrices.

La definición que hemos dado de resolución minimal es algo oscura, pues no da una idea intuitiva de la minimalidad que hay detrás. Los teoremas que probaremos a continuación resuelven este problema y dan una idea de lo que significa realmente la minimalidad de una resolución.

Recordemos que en la sección anterior hemos construido de manera recursiva una resolución libre graduada.

Proposición 3.22. *La resolución libre graduada construida en la sección anterior es minimal si y solo si escogemos un sistema de generadores homogéneos minimal del núcleo de las diferenciales en cada paso.*

En la demostración usamos idéntica notación que en la sección anterior cuando explicamos la construcción de la resolución. Así, si $\{l_1, \ldots, l_s\}$ son generadores homogéneos de $\ker(d_i)$ su contraimagen por la aplicación d_{i+1} será $\{g_1, \ldots, g_s\}$ y dichos g_j generan F_{i+1}.

Demostración. Supongamos en primer lugar que la resolución es minimal (en el sentido de la Definición 1.19). Vamos a razonar por reducción al absurdo suponiendo que en algún paso $i \geq 0$ hemos tomado un sistema de generadores homogéneos $\{l_1, \ldots, l_s\}$ no minimal de $\ker(d_i)$. Entonces (salvo reordenamiento) podemos escribir $l_1 = \sum_{j=2}^{s} r_j l_j$ con $r_j \in R$. Se tiene entonces que $d_{i+1}(g_1) = \sum_{j=2}^{s} r_j d_{i+1}(g_j)$. Por lo tanto,

$$g_1 - \sum_{j=2}^{s} r_j g_j \in \ker(d_{i+1}) = \mathrm{im}(d_{i+2}).$$

Como la resolución es minimal se tiene que $\mathrm{im}(d_{i+2}) \subset \mathfrak{m}F_{i+1}$ por lo que $g_1 - \sum_{j=2}^{s} r_j g_j \in \mathfrak{m}F_{i+1}$. Esta pertenencia es una contradicción ya que los g_j generan F_{i+1} y son homogéneos.

Supongamos ahora que en cada paso hemos escogido un sistema minimal de generadores homogéneos de los núcleos, queremos ver que la resolución es minimal. De nuevo razonaremos por reducción al absurdo. Supongamos que existe $i \geq 0$ tal que $\mathrm{im}\,(d_{i+2}) \not\subset \mathfrak{m}F_{i+1}$. Entonces, $\mathrm{im}(d_{i+2}) = \ker(d_{i+1})$ contiene un elemento homogéneo que no pertenece a $\mathfrak{m}F_{i+1}$. Tras un reordenamiento podemos suponer que $g_1 - \sum_{j=2}^{s} r_j g_j \in \ker(d_{i+1})$ con $r_j \in R$. Por tanto, $d_{i+1}(g_1) = \sum_{j=2}^{s} r_j d_{i+1}(g_j)$. Recordemos que $d_{i+1}(g_i) = l_i$ para cada $i = 1, \ldots, s$, luego se tiene que

$$l_1 = \sum_{j=2}^{s} r_j l_j,$$

contradiciendo que $\{l_1, \ldots l_s\}$ eran un sistema de generadores minimal de $\ker(d_i)$. □

Un **complejo trivial corto** es un complejo de la forma siguiente, donde Id es la aplicación identidad.

$$0 \longrightarrow R(-p) \xrightarrow{\mathrm{Id}} R(-p) \longrightarrow 0\ .$$

Vamos a utilizar la notación (**F**,d) para referirnos a un complejo como el definido en la Definición 1.14. Si (**F**,d) y (**G**,∂) entonces su suma directa es el complejo $\mathbf{F} \oplus \mathbf{G}$, que tiene como sucesión de módulos la suma directa de los módulos de (**F**,d) y (**G**,∂) y como diferencial $d \oplus \partial$. Una suma directa de complejos triviales cortos (admitiendo que estén situados en grados de homología diferentes) recibe el nombre de **complejo trivial**.

El siguiente resultado, de capital importancia, garantiza la unicidad salvo isomorfismo de la resolución minimal de un R-módulo finitamente generado. La demostración del teorema consiste fundamentalmente en probar el segundo apartado ya que el apartado 1 del teorema es consecuencia de la Proposición 3.22 y el apartado 3 es consecuencia del 2. La prueba del apartado 2 es demasiado técnica y no aporta demasiado al objetivo global del trabajo, con lo que la omitiremos. No obstante, puede encontrarse en [Pee10, Section 9]

Teorema 3.23. *Sea U un R-módulo graduado finitamente generado.*

1. *Existe una resolución graduada libre minimal de U.*

2. *Sea* $\boldsymbol{F}$ *una resolución graduada libre minimal de* U*. Si* $\boldsymbol{G}$ *es otra resolución libre graduada de* U*, entonces* $\boldsymbol{G} \cong \boldsymbol{F} \oplus \boldsymbol{T}$ *donde* $\boldsymbol{T}$ *es un complejo trivial.*

3. *La resolución graduada libre minimal de* U *es única salvo isomorfismo.*

En virtud del teorema anterior, dado un R-módulo finitamente generado podremos hablar de *la* resolución minimal libre graduada.

Definición 3.24 (Módulo de sicigias)**.** Sea $\mathbf{F}$ la resolución minimal libre graduada de un R-módulo finitamente generado U. Para cada $i \geq 1$ el submódulo $\mathrm{im}(d_i) = \ker(d_{i-1}) \subset F_{i-1}$ se denomina ***i*-ésimo módulo de sicigias** de U y se representa por $Syz_i(U)$.

Recordemos que una resolución minimal libre graduada de U es de la forma

$$\mathbf{F}: \cdots \longrightarrow F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} U \longrightarrow 0\,,$$

donde los F_i son módulos libres.

Definición 3.25 (Números de Betti)**.** Con la notación anterior, el ***i*-ésimo número de Betti** de U es $\beta_i(U) = \dim(F_i)$. Por el Teorema 3.23, los números de Betti están bien definidos.

Como las resoluciones con las que estamos trabajando son graduadas podemos refinar un poco la definición anterior. Recordemos que los módulos libres F_i son suma directa de módulos de la forma $R(-p)$.

Definición 3.26 (Números de Betti graduados)**.** Con la notación anteriormente introducida, se definen los **números de Betti graduados** de U como $\beta_{i,p}(U) =$ número de sumandos en F_i de la forma $R(-p)$.

Ya hemos hablado de la graduación estándar para el anillo de polinomios $S = k[x_1, \ldots, x_n]$. Sin embargo, podemos definir una graduación un poco más fina, utilizando $\mathbb{N}^n$. De esta forma, dado un monomio $\mathbf{x^c} = x_1^{c_1} \cdots x_n^{c_n}$, diremos que tiene multigrado $c = (c_1, \ldots, c_n)$. Denotamos $|c| = c_1 + \cdots + c_n$. La forma usual de ordenar estos multigrados es utilizar un orden monomial. Podemos por tanto, considerar el anillo de polinomios multigraduado

$$S = \bigoplus_{\alpha \in \mathbb{N}^n} S_\alpha,$$

donde S_α es el k-espacio vectorial generado por los monomios de multigrado α. Para esta graduación podemos definir también una resolución graduada libre minimal de la forma

$$\mathbf{F}: \cdots \longrightarrow F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} U \longrightarrow 0\,.$$

En esta resolución, al igual que cuando consideramos la graduación con $\mathbb{N}$, el Teorema 3.15 afirma que cada F_i es de la forma

$$F_i = \bigoplus_{\alpha \in \mathbb{N}^n} S(-\alpha)^{\beta_{i,\alpha}}.$$

Definición 3.27. Los exponentes $\beta_{i,\alpha}$ de la resolución anterior reciben el nombre de **números de Betti multigraduados**.

Observación. La relación entre los números de Betti globales, los graduados y los multigraduados viene dada por la siguientes expresiones:

$$\beta_i = \sum_p \beta_{i,p},$$

$$\beta_{i,p} = \sum_{|\alpha|=p} \beta_{i,\alpha}.$$

3.4. Complejos simpliciales

En esta sección daremos una breve introducción a la teoría de complejos simpliciales. A partir de la definición, vamos a definir un anillo sobre el que poder poder aplicar las técnicas de la Sección 3.3. También estudiaremos la similitud del concepto de complejo simplicial con el de matroide.

Definición 3.28 (Complejo simplicial)**.** Sea E un conjunto finito. Un **complejo simplicial** Δ sobre E es una colección de subconjuntos de E que verifican la siguiente propiedad:

- Si $\sigma \in \Delta$ y $\tau \subset \sigma$, entonces $\tau \in \Delta$.

Los subconjuntos de E que forman el complejo simplicial se llaman **caras**. La **dimensión** de una cara $\sigma \in \Delta$ de cardinal $|\sigma| = i + 1$ es $\dim(\sigma) = i$ y se dice que es una i-cara. La dimensión del complejo, $\dim(\Delta)$, se define como el máximo de las dimensiones de sus caras. Para determinar un complejo simplicial es suficiente dar el conjunto de **caras maximales**, que son áquellas a las cuales al añadirle cualquier elemento dejan de ser una cara del complejo.

El complejo simplicial que no tiene caras se llama **complejo vacío** y tiene dimensión $-\infty$.

Puesto que E es un conjunto finito, a menudo se identifica con $\{1, \ldots, |E|\}$. También es común identificarlo con las variables $\{x_1, \ldots, x_{|E|}\}$.

Observación. Volviendo a la Definición 2.1, podemos ver las matroides como un caso particular de complejos simpliciales no vacíos, cumpliendo además la propiedad **(I3)**. Las caras de un complejo simplicial se corresponden así con los conjuntos independientes de una matroide, y las caras maximales con las bases. La estructura de anillo asociada a un complejo simplicial, que posteriormente explicaremos, se puede asociar así también al complejo simplicial que forman los conjuntos independientes de una matroide.

Dado un complejo simplicial, Δ, vamos a denotar por f_i al número de caras de cardinal i. De este modo tenemos que $f_0 = 1$, $f_1 = |E|$ y $f_k = 0$ para $k > r = \dim(\Delta)+1$. Se define la **característica de Euler** del complejo simplicial como

$$\chi(\Delta) = -f_0 + f_1 - f_2 + \cdots + (-1)^{k-1} f_k.$$

3.4.1. Anillos de Stanley-Reisner

Vamos a ver cómo asociar una estructura de anillo a un complejo simplicial.

Sea Δ un complejo simplicial y sea $\sigma \in \Delta$ una de sus caras. Vamos a identificar cada cara de Δ con un vector de $\{0,1\}^{|E|}$ que tiene como coordenada i un 1 si $i \in \sigma$ y un 0 en caso contrario. Así, denotaremos por $\mathbf{x}^\sigma$ a $\Pi_{i\in\sigma} x_i$. Estamos haciendo corresponder cada cara de un complejo simplicial con un monomio cuyos exponentes son todos 0 o 1. Tales monomios se dice que son **libres de cuadrados**.

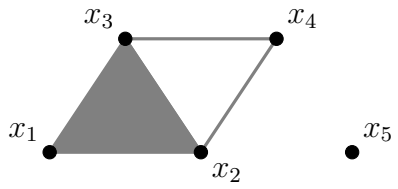
Definición 3.29. Sea Δ un complejo simplicial sobre un conjunto base E (que se puede identificar con $\{1,\ldots,n\}$) y sea $\mathbb{K}$ un cuerpo. Consideremos $S = \mathbb{K}[x_1,\ldots,x_n]$ el anillo de polinomios en $|E|$ variables. Se define el **ideal de Stanley-Reisner** de Δ como el ideal monomial libre de cuadrados generado por las no caras de Δ, esto es,

$$I_\Delta = \langle x^\tau : \tau \notin \Delta \rangle.$$

El **anillo de Stanley-Reisner** de Δ es el anillo cociente $R = S/I_\Delta$.

Observación. Notemos que el ideal de Stanley-Reisner de un complejo simplicial Δ se puede escribir como el ideal monomial generado por las no caras minimales de Δ. Cuando hablemos del ideal de Stanley-Reisner asociado a una matroide M, nos referimos entonces al ideal generado por el conjunto de circuitos de M.

Ejemplo 3.30. Consideremos $E = \{1,2,3,4,5\}$ y Δ el complejo simplicial que tiene como caras maximales los conjuntos $\{1,2,3\}$, $\{2,4\}$, $\{3,4\}$ y $\{5\}$. Una posible representación es:



Hemos realizado aquí la identificación natural de $\{1,2,3,4,5\}$ con las variables $\{x_1,x_2,x_3,x_4,x_5\}$. Notemos que los subconjuntos minimales que no son caras del complejo Δ son $\{1,4\},\{2,3,4\},\{1,5\},\{2,5\},\{3,5\},\{4,5\}$. Por lo tanto,

$$I_\Delta = \langle x_1x_5, x_2x_5, x_3x_5, x_4x_5, x_1x_4, x_2x_3x_4\rangle.$$

$\diamond$

Ejemplo 3.31. Consideremos la siguiente matriz

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

La matroide $M[H]$ asociada a dicha matriz tiene como conjunto de bases el siguiente:

$$\mathcal{B} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}.$$

El conjunto de circuitos de dicha matroide son:

$$\mathcal{C} = \{\{1,2,3\},\{1,2,4\},\{3,4\}\}.$$

Por lo tanto, el ideal de Stanley-Reisner asociado al complejo simplicial que forman los conjuntos independientes de $M[H]$ es:

$$I_\Delta = \langle x_1x_2x_3, x_1x_2x_4, x_3x_4\rangle.$$

$\diamond$

Vamos a asociar a este anillo una resolución graduada libre minimal y a considerar sus correspondientes números de Betti. Este anillo tiene una resolución libre minimal, visto como $\mathbb{N}^{|E|}$-módulo graduado:

$$0 \longrightarrow F_l \xrightarrow{d_l} F_{l-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} R \longrightarrow 0\,.$$

Como vimos en el Teorema 3.15, cada uno de los F_i es de la forma

$$F_i = \bigoplus_{\alpha\in\mathbb{N}^{|E|}} S(-\alpha)^{\beta_{i,\alpha}}.$$

Los exponentes $\beta_{i,\alpha}$ son los números de Betti $\mathbb{N}^{|E|}$-graduados.

Observación. Puesto que I_Δ es un ideal monomial libre de cuadrados los números de Betti multigraduados cumplen que

$$\beta_{i,\alpha} = 0, \text{ si } \alpha \in \mathbb{N}^{|E|} \setminus \{0,1\}^E.$$

Este es el contenido de [Pee10, Corollary 26.10]. Como cuestíón de notación, si σ es una cara de un complejo simplicial Δ sobre E, denotamos por $\beta_{i,\sigma}$ al número de Betti $\beta_{i,\alpha}$, donde $\alpha \in \mathbb{N}^{|E|}$ es el vector que tiene un 1 en la coordenada j si $j \in \sigma$ y un 0 en caso contrario. Denotamos también por $|\alpha|$ a la suma de sus coordenadas.

Los números de Betti $\mathbb{N}$-graduados para el complejo simplicial Δ y los números de Betti globales son, respectivamente,

$$\beta_{i,d} = \sum_{|\alpha|=d} \beta_{i,\alpha},$$

$$\beta_i = \sum_d \beta_{i,d}.$$

3.4.2. Homología simplicial

Vamos ahora a definir lo que es un complejo de cadena para un complejo simplicial. Esta definición nos llevará al concepto de homología simplicial. Utilizando herramientas de homología se puede llegar a una expresión de los numeros de Betti que nos será útil para trabajar con ellos.

Notación. Sea Δ un complejo simplicial sobre un conjunto finito E de tamaño n, que identificamos con $\{1,\dots,n\}$, y sea $\mathbb{K}$ un cuerpo. Para cada $i \in \mathbb{Z}$, vamos a denotar por $F_i(\Delta)$ el conjunto de caras de dimensión i de Δ y $V_i = \mathbb{K}^{F_i(\Delta)}$ el espacio vectorial de dimensión $|F_i|$ que tiene como base los elementos e_σ, donde $\sigma \in F_i(\Delta)$.

Notación. Dada $\sigma \in \Delta$ una cara del complejo simplicial, es decir, $\sigma \subset \{1,\dots,n\}$, y dado $j \in \sigma$, vamos a denotar por $\text{signo}(j,\sigma) = (-1)^{r-1}$ si j es el r-ésimo elemento de σ donde ordenamos los elementos de σ de modo creciente.

Definición 3.32. El complejo de cadena de Δ sobre el cuerpo $\mathbb{K}$ es el complejo, entendido como en la Definición 3.18, siguiente:

$$0 \longrightarrow V_{n-1} \xrightarrow{\partial_{n-1}} \cdots \longrightarrow \cdots \longrightarrow V_1 \xrightarrow{\partial_1} V_0 \xrightarrow{\partial_0} V_{-1} \longrightarrow 0\,.$$

Las diferenciales del complejo de cadena se definen como

$$\partial_i(e_\sigma) = \sum_{j\in\sigma} \text{signo}(j,\sigma)\, e_{\sigma\setminus j}.$$

Observación. Notemos que si $|E| = n$, para $i > n-1$ o $i < -1$ se tiene que $V_i = 0$ y $\partial_i = 0$. Es un cálculo sencillo comprobar que $\partial_{i+1} \circ \partial_i = 0$, por lo que el complejo está bien definido.

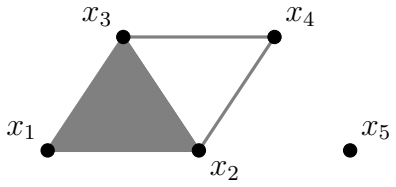
Definición 3.33. Para cada $i \in \mathbb{Z}$, el $\mathbb{K}$-espacio vectorial

$$\tilde{H}_i(\Delta) = \ker(\partial_i)/\text{im}(\partial_{i+1})$$

recibe el nombre de **módulo i-ésimo de homología** de Δ. Vamos a denotar por $\tilde{h}_i$ a la dimensión como $\mathbb{K}$-espacio vectorial de $\tilde{H}_i$, es decir,

$$\tilde{h}_i = \dim(\tilde{H}_i).$$

Ejemplo 3.34. Consideremos de nuevo el complejo simplicial Δ:



Para este complejo se tiene

$$\begin{aligned} F_2(\Delta) &= \{\{1,2,3\}\},\\ F_1(\Delta) &= \{\{1,2\},\{1,3\},\{2,3\},\{2,4\},\{3,4\}\},\\ F_0(\Delta) &= \{\{1\},\{2\},\{3\},\{4\},\{5\}\},\\ F_{-1}(\Delta) &= \{\emptyset\}. \end{aligned}$$

El complejo de cadena asociado a Δ es entonces

$$0 \longrightarrow \mathbb{K} \xrightarrow{\partial_2} \mathbb{K}^5 \xrightarrow{\partial_1} \mathbb{K}^5 \xrightarrow{\partial_0} \mathbb{K} \longrightarrow 0\,.$$

Cada una de las aplicaciones ∂_i viene dada por una matriz en cuyas columnas están las imágenes de los elementos de la base. Por ejemplo, ∂_2 se puede representar por una matriz de tamaño (5×1) que tiene como columna $\partial_2(e_{\{1,2,3\}}) = e_{\{2,3\}} - e_{\{1,3\}} + e_{\{1,2\}}$, que identificamos con el vector $(1,-1,1,0,0)$. $\diamond$

El siguiente teorema da una expresión que relaciona los números de Betti multigraduados con las dimensiones de los módulos de homología asociados a un determinado complejo simplicial. La expresión, conocida como fórmula de Hochster fue probada por primera vez en [Hoc77]. Omitiremos la demostración ya que precisa nociones importantes de homología simplicial, no obstante, se puede encontar bien en el artículo original, bien en [MS05, Cor. 5.12]

Teorema 3.35 (fórmula de Hochster)**.** *Sea Δ un complejo simplicial sobre E y sea $\sigma \subset E$. Denotaremos por Δ_σ la restricción de Δ a σ, esto es, el complejo simplicial que tiene como caras $\{\tau \cap \sigma : \tau \in \Delta\}$. Se tiene la siguiente expresión para los números de Betti muligraduados:*

$$\beta_{i,\sigma} = \tilde{h}_{|\sigma|-i-1}(\Delta_\sigma).$$

En la fórmula anterior, $\beta_{i,\sigma}$ denota el $\beta_{i,\alpha}$ donde α es el vector de $\mathbb{N}^{|E|}$ que tiene un 1 en la coordenada j si $j \in \sigma$ y un 0 en caso contrario.

Capítulo 4

Números de Betti y pesos generalizados

Este último capítulo ofrece los dos resultados principales de la memoria. Dichos resultados permiten calcular los pesos de Hamming generalizados de una matroide (y por tanto de un código lineal) a partir de los números de Betti $\mathbb{N}$-graduados del complejo simplicial asociado. Veremos también algún ejemplo de cálculo de los pesos de Hamming de un código utilizando resoluciones, junto a otros ejemplos que permiten ver que los pesos de Hamming no determinan los números de Betti. También exploraremos algunas de las consecuencias de los teoremas principales, en particular, daremos una caracterización de los códigos MDS utilizando la resolución libre minimal asociada.

Los teoremas que vamos a probar sirven para relacionar los números de Betti con los pesos de Hamming generalizados de cualquier matroide, definidos como en 2.43. Podremos entonces particularizar el resultados a las matroides asociadas a (la matriz de control de) un código lineal. Estos resultados vienen motivados por la existencia de algoritmos para el cálculo de números de Betti, por ejemplo utilizando bases de Gröbner, de una resolución. Estos algoritmos, pese a que en su mayoría son de complejidad exponencial, suponen una gran mejora con respecto al cálculo de los pesos generalizados por fuerza bruta.

Notación. En este capítulo, M será una matroide definida sobre un conjunto finito E, con $|E| = n$. Denotaremos por $\mathcal{I}_M$, $\mathcal{C}_M$, $\mathcal{B}_M$, r_M y n_M la familia de conjuntos independientes, circuitos, bases, función rango y función de nulidad de M, respectivamente. Con S, denotamos el anillo de polinomios con n variables sobre un cuerpo $\mathbb{K}$, $S = \mathbb{K}[x_1, \ldots, x_n]$.

Recordemos que dado un complejo simplicial Δ, podemos definir su anillo de Stanley-Reisner S/I_Δ como en la Sección 3.4. Ya hemos estudiado que este anillo tiene una resolución graduada (con la graduación de $\mathbb{N}^n$) libre minimal de la forma siguiente:

$$0 \longrightarrow F_l \xrightarrow{d_l} F_{l-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} R \longrightarrow 0, \tag{4.1}$$

donde cada F_i es de la forma:

$$F_i = \bigoplus_{\alpha \in \mathbb{N}^{|E|}} S(-a)^{\beta_{i,\alpha}}.$$

Como recordatorio, los exponentes $\beta_{i,\alpha}$ son los números de Betti multigraduados. Los números de Betti $\mathbb{N}$-graduados para el complejo simplicial Δ y los números de Betti globales son, respectivamente,

$$\beta_{i,d} = \sum_{|a|=d} \beta_{i,a},$$

$$\beta_i = \sum_{d} \beta_{i,d}.$$

Notación. Generalmente, los números de Betti se dan en una tabla, de modo que la entrada en la i-ésima columna y la p-ésima fila es el número de Betti $\beta_{i,i+p}$. Existe una fila adicional, encima de la tabla y separada por una línea horizontal que contiene los números de Betti globales (que se obtienen de sumar los números de Betti de esa columna). La i-ésima columna da entonces la información en el paso i de la resolución libre graduada minimal. Estas tablas reciben el nombre de **diagramas de Betti**. En nuestro caso, al calcular el primer módulo libre de la resolución, vamos a tener $F_0 = S$ por lo que vamos a omitir la parte del diagrama que corresponde a $\beta_{0,j}$ ya que $\beta_{0,0} = 1$ y $\beta_{0,j} = 0$ en el resto de casos. Es importante tener esto en cuenta ya que el primer número de Betti global, β_0, siempre va a ser igual a 1.

	β_1	β_2	β_3	$\cdots$
0	$\beta_{1,1}$	$\beta_{2,2}$	$\beta_{3,3}$	$\cdots$
1	$\beta_{1,2}$	$\beta_{2,3}$	$\beta_{3,4}$	$\cdots$
2	$\beta_{1,3}$	$\beta_{2,4}$	$\beta_{3,5}$	$\cdots$
3	$\beta_{1,4}$	$\beta_{2,5}$	$\beta_{3,6}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Cuadro 4.1: Ejemplo diagrama de Betti

Notación. Sea M una matroide sobre E con función de rango r y función de nulidad n. Para cada $d = 0, \ldots, |E| - r(M)$ vamos a denotar por $N_d = n^{-1}(d)$. En particular, $\mathcal{I} = N_0$.

El siguiente teorema da una expresión para los números de Betti utilizando la caracteríctica de Euler de una matroide. Recordemos que la familia de conjuntos independientes de una matroide es un complejo simplicial, por lo que tiene sentido hablar de la característica de Euler de una matroide.

Previo a su demostración, necesitaremos un lema básico sobre matroides y varios resultados acerca de la homología de matroides, desarrollados en [Bjö92]. Además, en el teorema también usaremos la expresión de los números de Betti multigraduados que da la fórmula de Hochster.

Definición 4.1. Sea M una matroide sobre un conjunto base E. Se dice que $x \in E$ es un **istmo** si x está en todas las bases de M.

Lema 4.2. *Sea M una matroide sobre E y sea $\overline{M}$ su matroide dual. Se tienen las siguientes equivalencias.*

1. *M tiene un istmo.*
2. *$\overline{M}$ tiene un bucle.*
3. *Existe un elemento que no está en ninguna base de $\overline{M}$.*
4. *Existe un elemento que está en todas las bases de M.*
5. *Existe un elemento que no está en ningún circuito de M.*
6. *El conjunto base de M no es igual a la unión de sus circuitos.*

Demostración. $1 \Rightarrow 2$. Supongamos que existe un $x \in E$ que está en todas las bases de M. Las bases de $\overline{M}$ son exactamente los complementarios de las bases de M, por lo que x no está en ninguna base de $\overline{M}$. En conclusión, x no es independiente en $\overline{M}$ y por tanto es un circuito.

$2 \Rightarrow 3$. Sea x un bucle de $\overline{M}$, entonces x es un conjunto dependiente y no puede estar ninguna base de $\overline{M}$, ya que estas son los conjuntos independientes maximales.

$3 \Rightarrow 4$. Es inmediato ya que las bases de $\overline{M}$ son los complementarios de las bases de M.

$4 \Rightarrow 5$. Sea $x \in E$ tal que x está en todas las bases de M. Supongamos que x está en un circuito C. Entonces $C \setminus x$ es un conjunto independiente.

Podemos ampliar dicho conjunto a una base B, pero dicha base tiene que contener a x. Tenemos por tanto $C \subset B$, absurdo pues C era un circuito.

$5 \Rightarrow 6$. Es inmediato.

$6 \Rightarrow 1$. Existe un $x \in E$ que no está en ningún circuito. Supongamos que existe una base B que no contiene a x. Por la proposición 2.16, existe un circuito que contiene a x contenido en $B \cup x$. Esto es una contradicción ya que x no puede estar en ningún circuito. □

Definición 4.3. Sea Δ un complejo simplicial sobre E. Se dice que Δ es un **cono** de vértice X si existe un $X \in E$ tal que X está en todas las caras maximales.

Observación. En caso de que Δ sea el complejo simplicial cuyas caras son los conjuntos independientes de una matroide M, es claro que Δ es un cono $\iff M$ tiene un istmo.

Recordemos que con $\beta_{i,X}$ denotamos el número de Betti multigraduado $\beta_{i,\alpha}$, donde $\alpha \in \mathbb{N}^{|E|}$ es el vector que tiene un 1 en la coordenada j si $j \in X$ y un 0 en caso contrario. Además, $\beta_{i,\alpha} = 0$ si $\alpha \in \mathbb{N}^{|E|} \setminus \{0,1\}^{|E|}$.

Teorema 4.4. *Sea M una matroide sobre el conjunto base E y sea $X \subset E$. Entonces*

$$\beta_{i,X} \neq 0 \iff X \text{ es minimal en } N_i \text{ para la inclusión.}$$

Además,

$$\beta_{n_M(X),X} = (-1)^{r(X)-1}\, \chi(M|X).$$

Demostración. La matroide restricción $M|X$ tiene rango $r(X)$. Por [Bjö92, Th. 7.8.1] sabemos que solo tiene homología en grado $r(X) - 1$. Por otra parte, la fórmula de Hochster dice que $\beta_{i,X} = \tilde{h}_{|X|-i-1}(M|X)$. De este modo, $\beta_{i,X} = 0$ excepto cuando $i = n_M(X)$. En este caso, combinando [Bjö92, Th. 7.4.7] y [Bjö92, Th. 7.8.1] se tiene la siguiente expresión.

$$\beta_{n_M(X),X} = \tilde{h}_{r(X)-1}(M|X) = (-1)^{r(X)-1}\, \chi(M|X).$$

Esto da la expresión del teorema. Solo faltaría probar que dicha expresión es no nula si y solo si X es minimal en N_i para la inclusión. En primer lugar se observa que $\beta_{i,X} = 0 \iff \chi(M|X) = 0$. Por [Bjö92, Th. 7.4.7], dada una matroide M se tiene que $\chi(M) = 0$ si y solo si M tiene un itsmo. Por el Lema 4.2 sabemos que M tiene un itsmo si y solo si el conjunto base de M no es igual a la unión de sus circuitos. Ahora bien, los resultados que estudiamos

en la Sección 2.6 permiten afirmar que X es minimal en N_i si y solo si es igual a la unión de sus circuitos. Más concretamente, supongamos que X es minimal en N_i, entonces $\deg(X) = i$, y por tanto existe un conjunto maximal de i circuitos no redundantes en X cumpliendo además que

$$n(X) \geq n\Big(\bigcup_{j=1}^{i} C_j\Big) \geq deg(X) = n(X).$$

La primera desigualdad se debe a la monotonía de la nulidad, la segunda es el contenido del Lema 2.37 y la última igualdad se cumple por la Proposición 2.42. Por lo tanto, $\bigcup_{j=1}^{i} C_j \subset X$ y tienen la misma nulidad. Por la minimalidad de X en N_i, debe ser $X = \bigcup_{j=1}^{i} C_j$. El Corolario 2.40 afirma que esta última unión es igual a la unión de todos los circuitos en X.

Recíprocamente, sea $X \subset N_i$ tal que X es igual a la unión de sus circuitos. Entonces, $\deg(X) = i$ y existe un conjunto maximal de i circuitos no redundantes en X tal que

$$\bigcup_{j=1}^{i} C_j = \bigcup_{C \in \mathcal{C}_{M|X}} C = X.$$

Si X no fuese minimal en N_i, existiría un $Y \subsetneq X$ con $n(Y) = i = \deg(Y)$. Existen por tanto i circuitos no redundantes $\{C'_1, \ldots, C'_i\}$ en Y (y por tanto también en X) tal que

$$Y = \bigcup_{j=1}^{i} C'_j.$$

Los C'_j son un sistema maximal de circuitos no redundantes en X y aplicando el Corolario 2.40 se tiene que

$$Y = \bigcup_{j=1}^{i} C'_j = \bigcup_{C \in \mathcal{C}_{M|X}} C = X.$$

Esto es una contradicción ya que $Y \neq X$. Hemos probado por tanto que X es minimal en N_i. □

Recogemos algunas de las consecuencias inmediatas de este teorema en los siguientes corolarios.

Corolario 4.5. *Sea M una matroide sobre el conjunto base E y sea $X \subset E$. Entonces*

$$\beta_{0,X} = \begin{cases} 1, & si\ X = \emptyset, \\ 0, & en\ caso\ contrario \end{cases} \tag{I}$$

y

$$\beta_{1,X} = \begin{cases} 1, & si\ X\ es\ un\ circuito, \\ 0, & en\ caso\ contrario. \end{cases} \tag{II}$$

Además, la resolución tiene exactamente longitud $k = |E| - r(M)$, es decir, $N_k \neq \emptyset$ pero $N_i = \emptyset$ para $i > k$.

Demostración. Las expresiones (I) y (II) son inmediatas del Teorema 4.4. Además, existe un $X \subset E$ tal que $|X| - r(X) = |E| - r(M)$, en particular basta tomar $X = E$, por lo tanto $N_k \neq \emptyset$ pero no existe ningún $X \subset E$ tal que $n(X) > |E| - r(M)$, ya que la función de nulidad es monótona creciente, luego $N_i = \emptyset$ para $i > k$. □

Corolario 4.6. *El conjunto de circuitos de una matroide M sobre E queda determinado por los números de Betti $\mathbb{N}^{|E|}$-graduados en grado de homología 1. Más precisamente, se tiene que*

$$\mathcal{C}_M = \{X \subset E : \beta_{1,X} \neq 0\}.$$

Probamos ahora el resultado anunciado al principio de este trabajo. El siguiente teorema da la relación que existe entre los pesos de Hamming generalizados que hemos definido para una matroide y los números de Betti $\mathbb{N}$-graduados que aparecen en la resolución del anillo de Stanley-Reisner asociado.

Notación. Recordemos que dada una matroide M sobre un conjunto base E, habíamos definido sus pesos de Hamming generalizados como:

$$d_i = \text{mín}\{|X| : X \subset E\ ,\ |X| - r(X) = i\}$$

Teorema 4.7. *Sea M una matroide sobre el conjunto base E. Los pesos de Hamming generalizados vienen dados por*

$$d_i = \text{mín}\{d : \beta_{i,d} \neq 0\}\ \ para\ i = 1, \ldots, |E| - r(M).$$

Demostración. Sea X minimal tal que $n(X) = i$. Por el Teorema 4.4 se tiene que $\beta_{i,X} \neq 0$, lo cual implica que $\beta_{i,d_i} = \beta_{i,|X|} \neq 0$. Se tiene por tanto que

$$d_i \geq \text{mín}\{d : \ \beta_{i,d} \neq 0\}.$$

Sea ahora d el mínimo tal que $\beta_{i,d} \neq 0$. Existe un $X \subset E$ tal que $|X| = d$ con $\beta_{i,X} \neq 0$. Por el Teorema 4.4, X es minimal en N_i, en particular, $n(X) = |X| - r(X) = i$. Se tiene por tanto que

$$d_i \leq |X| = d = \text{mín}\{d : \ \beta_{i,d} \neq 0\}.$$

□

4.1. Ejemplos de cálculo

Esta sección está íntegramente dedicada a ejemplos de cálculo. En primer lugar, veremos un ejemplo de cómo aplicar el Teorema 4.7 para calcular los pesos de un código C. Posteriormente, veremos que el recíproco de dicho teorema no es cierto, en el sentido que pueden existir matroides con la misma jerarquía de pesos pero sus números de Betti sean distintos. Finalmente, estudiaremos un ejemplo donde quedará también patente que los pesos generalizados no pueden deducirse de los números de Betti globales.

Ejemplo 4.8. En este primer ejemplo vamos simplemente a calcular los pesos de Hamming generalizados de un código C dado utilizando los números de Betti.

Consideremos el código C de tipo $[6, 3]$ que tiene como matriz de control

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

La matroide M asociada a dicha matriz de control tiene como conjunto de bases y circuitos, respectivamente,

$$\mathcal{B}_M = \{\{1,2,4\},\{1,2,5\},\{1,2,6\},\{1,3,4\},\{1,3,5\},\{1,3,6\},\{1,4,5\},\{1,4,6\},\{2,3,4\},\{2,3,5\},\{2,3,6\},\{2,4,5\},\{2,4,6\}\},$$

$$\mathcal{C}_M = \{\{5,6\},\{3,4,6\},\{3,4,5\},\{1,2,3,4\}\}.$$

Por tanto el ideal de Stanley-Reisner asociado es

$$I_M = \langle x_1x_2x_3x_4, x_3x_4x_5, x_3x_4x_6, x_5x_6\rangle.$$

Utilizando SageMath, podemos calcular la resolución minimal para el anillo de Stanley-Reisner así como los números de Betti, obteniendo así

$$0 \longrightarrow S(-6) \longrightarrow S(-4)^2 \oplus S(-5)^2 \longrightarrow S(-2) \oplus S(-3)^2 \oplus S(-4)$$

$$\longrightarrow S \longrightarrow S/I_M \longrightarrow 0.$$

	4	4	1
1	1	-	-
2	2	2	-
3	1	2	1

Cuadro 4.2: Diagrama de Betti de M.

Observando el diagrama de Betti podemos concluir que

$$(d_1, d_2, d_3) = (2, 4, 6).$$

$\diamond$

Ejemplo 4.9. Este ejemplo permite ver que pese a que dos matroides tengan la misma jerarquía de pesos, sus números de Betti pueden ser diferentes.

Consideremos los códigos C_1 y C_2 sobre $\mathbb{F}_2$ de tipo $[4, 2]$ con matrices de control, respectivamente,

$$H_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \; ; \; H_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Las matroides M_1 y M_2 asociadas a dichas matrices de control tienen como conjunto de bases, respectivamente,

$$\mathcal{B}_{M_1} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\},$$

$$\mathcal{B}_{M_2} = \{\{1, 2\}, \{1, 3\}, \{2, 4\}, \{3, 4\}\}.$$

Para cada una de ellas, el conjunto de circuitos es

$$\mathcal{C}_{M_1} = \{\{1, 2, 3\}, \{1, 2, 4\}, \{3, 4\}\},$$

$$\mathcal{C}_{M_2} = \{\{1,4\},\{2,3\}\}.$$

Los ideales de Stanley-Reisner asociados son por tanto

$$I_{M_1} = \langle x_1x_2x_3, x_1x_2x_4, x_3x_4\rangle,$$

$$I_{M_2} = \langle x_1x_4, x_2x_3\rangle.$$

Utilizando SageMath, podemos calcular los diagramas de Betti para las dos resoluciones.

$$\mathbf{F_1}:\ 0 \longrightarrow S(-4)^2 \longrightarrow S(-2)\oplus S(-3)^2 \longrightarrow S \longrightarrow S/I_{M_1} \longrightarrow 0\ ,$$

$$\mathbf{F_2}:\ 0 \longrightarrow S(-4) \longrightarrow S(-2)^2 \longrightarrow S \longrightarrow S/I_{M_2} \longrightarrow 0\ .$$

	3	2
1	1	-
2	2	2

Cuadro 4.3: Diagrama de Betti M_1.

	2	1
1	2	-
2	-	1

Cuadro 4.4: Diagrama de Betti M_2.

Podemos ver en los diagramas de Betti que los números de Betti $\mathbb{N}$-graduados no coinciden, pese a que la jerarquía de pesos es la misma, en este caso, $(d_1, d_2) = (2, 4)$. ◇

Ejemplo 4.10. El ejemplo que vamos a poner a continuación permite observar que dos códigos diferentes con los mismos números de Betti globales pueden tener jerarquías de pesos distintas.

Consideremos los códigos C_1 y C_2 sobre $\mathbb{F}_5$ que tienen como matrices de control, respectivamente,

$$H_1 = \begin{pmatrix} 1 & 4 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}\ ;\ H_2 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 3 \end{pmatrix}.$$

Las matroides M_1 y M_2 asociadas a dichas matrices de control tienen los siguientes conjuntos de circuitos:

$$\mathcal{C}_{M_1} = \{\{1,4\},\{1,2,3\},\{2,3,4\}\},$$

$$\mathcal{C}_{M_2} = \{\{2,3\},\{2,4\},\{3,4\}\}.$$

Los ideales de Stanley-Reisner asociados son

$$I_{M_1} = \langle x_1x_4, x_1x_2x_3, x_2x_3x_4\rangle,$$

$$I_{M_2} = \langle x_2x_3, x_2x_4, x_3x_4\rangle.$$

Utilizando SageMath, podemos calcular los diagramas de Betti para las resoluciones correspondientes, obteniendo

	3	2
1	1	-
2	2	2

Cuadro 4.5: Diagrama de Betti M_1

	3	2
1	3	2
2	-	-

Cuadro 4.6: Diagrama de Betti M_2

Podemos ver que ambos códigos tienen como números de Betti globales $(1,3,2)$, sin embargo, la jerarquía de pesos es diferente. C_1 tiene como pesos $(2,4)$ mientras que C_2 tiene $(2,3)$. ◇

4.2. Caracterización de los códigos MDS

Los teoremas de este capítulo no solamente ofrecen un algoritmo para el cálculo de los pesos de Hamming generalizados de un código, sino que también conllevan numerosas consecuencias de carácter más teórico. En esta sección nos gustaría destacar el hecho de que estudiando la resolución del anillo de Stanley-Reisner asociado al complejo simplicial formado por los conjuntos independientes de la matroide asociada a un código podemos determinar si el código es MDS.

Sea C un código lineal de tipo $[n, k]$. Recordemos que los códigos satisfacen la siguiente cota, como ya vimos en 1.17.

Teorema 4.11. *Sea* C *un código lineal de tipo* $[n, k]$*, se cumple que*

$$d_r(\mathrm{C}) \leq n - k + r \text{ para todo } r = 1, \ldots, k.$$

Definición 4.12. Se dice que un código C es r-MDS si $d_r = n - k + r$.

Observación. Si un código es r-MDS, entonces también es i-MDS para todo $i = r, \ldots, k$. En efecto, supongamos que C es un código r-MDS. Se tiene entonces que $d_r = n - k + r$. Ahora, por la monotonía de los pesos (1.16) y la cota de Singleton generalizada (1.17), se tiene que

$$n - k + r = d_r < d_{r+1} \leq n - k + r + 1,$$

por lo que $d_{r+1} = n - k + r + 1$.

Antes de dar el resultado de caracterización de códigos MDS vamos a dar algunas definiciones que se enmarcan dentro de la teoría de resoluciones de módulos.

Notación. Consideremos $\mathbf{F}$ una resolución libre graduada de U, un R-módulo graduado finitamente generado,

$$\mathbf{F}: \cdots \longrightarrow F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} U \longrightarrow 0\,.$$

Vamos a denotar por $c_{i,p}$ el número de copias de $R(-p)$ que hay en F_i. Notemos que si la resolución es minimal, $c_{i,p}$ coincide con los números de Betti, $\beta_{i,p}$.

El conjunto de desplazamientos i-ésimos es $\{p : \ c_{i,p} \neq 0\}$. Vamos a denotar por ν_i y μ_i, respectivamente, a:

$$\nu_i = \text{mín}\{p : \ c_{i,p} \neq 0\} \quad \text{y} \quad \mu_i = \text{máx}\{p : \ c_{i,p} \neq 0\}.$$

Definición 4.13. Con la notación anterior, se dice que $\mathbf{F}$ es una **resolución pura** si para cada i, el número de desplazamientos i-ésimos es un único número, que denotamos p_i, es decir, $\nu_i = \mu_i = p_i$.

Una resolución pura $\mathbf{F}$ es **q-lineal** si existe un número q tal que $p_i = q + i$, para cada i.

Las definiciones dadas en 4.13 se pueden expresar en términos de anulación de los números de Betti en el sentido de la siguiente proposición. (Ver [Pee10, Prop. 17.5]).

Proposición 4.14. *Sea* $\mathbf{F}$ *una resolución libre graduada de un* R*-módulo graduado finitamente generado.*

- $\mathbf{F}$ *es pura si y solo si para cada* i *existe un número* p_i *tal que* $c_{i,j} = 0$ *para* $j \neq p_i$*.*
- $\mathbf{F}$ *es* q*-lineal si y solo si* $c_{i,j} = 0$ *para cada* $j \neq q + i$*.*

Notemos que si $\mathbf{F}$ *es minimal, el resultado es válido intercambiando* $c_{i,j}$ *por los números de Betti,* $\beta_{i,j}$*.*

Lema 4.15. *Sea* C *un código lineal de tipo* $[n, k]$*. Consideremos* $M[H]$ *la matroide asociada a una matriz de control* H *de* C*. Entonces* $M[H]$ *no tiene itsmos si y solo si el código* C *es no degenerado.*

Demostración. Denotemos por $M = M[H]$ la matroide asociada a una matriz de control. Sabemos entonces que $\overline{M}$ se corresponde con la matroide asociada a una matriz de control del código dual, o equivalentemente, a una matriz generatriz de C. Por otra parte, por el lema 4.2, M tiene un itsmo si y solo si $\overline{M}$ tiene un bucle. Un bucle en la matroide asociada a una matriz generatriz se corresponde con una columna de ceros, luego existe una posición en la que todas las palabras de C son nulas, esto es, C es degenerado. □

Observación. Observemos que un código de tipo $[n, k]$ es k-MDS, es decir, $d_k = n$, si y solo si C es no degenerado, o equivalentemente, si y solo si M no tiene itsmos.

Teorema 4.16. *Para la resolución* (4,1)*, y considerando la matroide* M *asociada a una matriz de control* H *de un código lineal* C *de tipo* $[n, k]$*, se tiene que* C *es* h*-MDS si y solo si la parte*

$$0 \longrightarrow F_k \xrightarrow{d_k} F_{k-1} \longrightarrow \cdots \xrightarrow{d_{h+1}} F_h$$

de la resolución es $(n - k)$*-lineal y* M *no tiene itsmos.*

Demostración. En primer lugar, el Corolario 4.5 afirma que $N_i = \emptyset$ para cada $i > k = |E| - r(M)$, por lo tanto, $\beta_{i,j} = 0$ para todo j y para $i > k$. Por otra parte, el Teorema 4.7 establece que $d_h = n - k + h$ si y solo si $\beta_{i,j} = 0$ para $j < n - k + h$, y $\beta_{i,n-k+h} \neq 0$. Sabemos que si un código es h-MDS lo es también para los pesos de órdenes más altos luego $\beta_{i,j} \neq 0$ para

$j = n-k+h, \ldots, n-k+k = n$. Puesto que no existe ninguna base con más de n elementos, se tiene además que $\beta_{k,j} = 0$ para $j > n$. Pongamos

$$\nu_i = \text{mín}\{j : \beta_{i,j} \neq 0\} \quad \text{y} \quad \mu_i = \text{máx}\{j : \beta_{i,j} \neq 0\}.$$

Por el Teorema 4.7, $\nu_i = d_i$. Hemos probado que $\nu_k = \mu_k = n$ si y solo si $d_k = n$. Por [Sta07, Th. 3.4, page 92] y [BH95, Prop. 1.1], los μ_i son una sucesión estrictamente creciente. Si M no tiene itsmos, $d_k = n$ y, por tanto, $\mu_i \leq \mu_k - (k-i) = n-k+i$ y por tanto $\beta_{i,j} = 0$ para $j > n-k+i$. Queda así probado el resultado gracias a la caracterización para resoluciones lineales que explicamos en la Proposición 4.14. □

Corolario 4.17. *Con la notación del teorema anterior,* C *es un código MDS si y solo si la resolución completa es* $(n-k)$*-lineal y* C *es no degenerado.*

Demostración. Es un caso particular del teorema anterior tomando $h = 1$. □

4.2.1. Ejemplos

Para finalizar, dedicamos esta sección a estudiar algún ejemplo de código MDS utlizando el Teorema 4.16.

Ejemplo 4.18. Vamos a considerar el código C de tipo $[5, 3]$ sobre $\mathbb{F}_5$ que tiene como matriz de control

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

La matroide M asociada tiene como conjunto de circuitos los 10 subconjuntos que tienen 3 elementos de entre $E = \{1, 2, 3, 4, 5\}$.

Utilizando SageMath, podemos obtener el diagrama de Betti de la resolución

	10	15	6
1	-	-	-
2	10	15	6
3	-	-	-

Cuadro 4.7: Diagrama de Betti de M.

La jerarquía de pesos dada por los números de Betti $\mathbb{N}$-graduados es $(d_1, d_2, d_3) = (3, 4, 5)$. El código es por tanto MDS. Si nos fijamos en el diagrama de Betti, podemos observar que la resolución es $(n - k) = 2$-lineal en el sentido de la Definición 4.13.

Conclusiones

Hemos visto que a cada código lineal de tipo $[n, k]$ le podemos asociar la matroide correspondiente a una de sus matrices de control. La familia de conjuntos independientes de dicha matroide forman un complejo simplicial Δ, para el cual podemos definir su anillo de Stanley-Reisner, S/I_Δ. Este anillo tiene una resolución libre minimal como $\mathbb{N}^n$-módulo graduado. Para esta graduación existen tres conjuntos de números de Betti: los números de Betti globales, los $\mathbb{N}$-graduados y los $\mathbb{N}^n$-graduados.

Los números de Betti $\mathbb{N}^n$-graduados determinan M ya que $\beta_{i,X} \neq 0$ si y solo si X es un circuito de la matroide. Este es el contenido del Corolario 4.6.

Los números de Betti $\mathbb{N}$-graduados determinan la jerarquía de pesos de la matroide M en el sentido del Teorema 4.7, resultado principal de la presente memoria. Como ejemplo de cálculo hemos aportado 4.8.

Por último, los números de Betti globales no determinan la jerarquía de pesos de la matroide. En el Ejemplo 4.10 presentamos dos códigos con los mismos números de Betti globales pero distinta jerarquía de peso. No es cierto tampoco que la jerarquía de pesos determine los números de Betti globales, como se puede ver en el Ejemplo 4.9.

Los resultados mostrados en este trabajo permiten construir un algoritmo para calcular los pesos de Hamming generalizados de un código, en particular, permiten calcular su distancia mínima, el cual es unos de los principales problemas que aborda la teoría de códigos. Este algoritmo se divide fundamentalmente en los siguientes pasos.

- **Paso 1.** Determinar la matroide asociada a la matriz de control del código. En particular, necesitaremos los conjuntos dependientes minimales ya que con ellos podemos formar el ideal de Stanley-Reisner.
- **Paso 2.** Determinar el anillo de Stanley-Reisner a partir de la matroide obtenida en el paso 1.

- **Paso 3.** Calcular los números de Betti $\mathbb{N}$-graduados del anillo de Stanley-Reisner.
- **Paso 4.** Encontrar la distancia mínima a partir de los números de Betti obtenidos utilizando el Teorema 4.7.

Bibliografía

[BH95] Winfried Bruns and Takayuki Hibi. Stanley–Reisner rings with pure resolutions. *Communications in Algebra*, 23(4):1201–1217, 1995.

[Bjö92] Anders Björner. The homology and shellability of matroids and geometric lattices. *Matroid applications*, 40:226–283, 1992.

[Eis13] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[Hoc77] Melvin Hochster. Cohen-Macaulay rings, combinatorics, and simplicial complexes, in *Ring Theory II. Lect. Notes in Pure Appl. Math.*, (26):171–223, 1977.

[JV13] Trygve Johnsen and Hugues Verdure. Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids. *Applicable Algebra in Engineering, Communication and Computing*, 24(1):73–93, 2013.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*. Number 8. Cambridge University Press, 1989.

[MS05] Ezra Miller and Bernd Sturmfels. *Combinatorial commutative algebra*, volume 227. Springer, 2005.

[Oxl06] James G Oxley. *Matroid theory*, volume 3. Oxford University Press, USA, 2006.

[Pee10] Irena Peeva. *Graded syzygies*, volume 14. Springer Science & Business Media, 2010.

[PWBJ17] Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin, and Relinde Jurrius. *Codes, cryptology and curves with computer algebra*. Cambridge University Press, 2017.

[Sta07] R.P. Stanley. *Combinatorics and commutative algebra*, volume 41. Springer Science & Business Media, 2007.

[Wei91] Victor K Wei. Generalized Hamming weights for linear codes. *IEEE Transactions on information theory*, 37(5):1412–1418, 1991.

[Whi92] Hassler Whitney. On the abstract properties of linear dependence. *Hassler Whitney Collected Papers*, pages 147–171, 1992.