UNIVERSIDAD AUTÓNOMA DE ZACATECAS

UNIDAD ACADÉMICA DE MATEMÁTICAS

Aplicaciones a la teoría de códigos de los números de Betti de una matroide

TESIS

Que para obtener el título de:

Maestro en Matemáticas

PRESENTA

Aracely Isais Gómez

Asesor: Dr. Hernán de Alba Casillas

Zacatecas, Zacatecas, México
2019

Introducción

En teoría de la información uno de los problemas que existe es el detectar y corregir los errores en un mensaje enviado, donde el mensaje es enviado a través de un canal de información. Los códigos que más se estudian son los códigos lineales C, donde C es un subespacio lineal de $\mathbb{F}_q^n$, con $\mathbb{F}_q$ un campo finito con q elementos y $n \in \mathbb{N}$. Un invariante numérico de suma importancia para C (ver [17], [27]) es la mínima distancia de Hamming $d(C)$ que proporciona una solución al problema de detección y corrección de errores. En 1991, V.K. Wei generaliza el peso de Hamming y define para cada $i \in \{1, \ldots, k\}$ con k la dimensión del código, el i-ésimo peso generalizado de Hamming $d_i(C)$, donde $d_1(C) = d(C)$ y $1 \leq d_1(C) < d_2(C) < \cdots < d_k(C)$. Dichos pesos tienen relevancia por su estrecha relación con los problemas de códigos conocidos como wire-tap channel of type II ([25]) y las funciones t-resilientes ([8]).

El párrafo anterior pone en evidencia que la teoría de códigos está en estrecha relación con el álgebra lineal sobre campos finitos. Además, recientemente en [2], [15] y [16] se muestra que para estudiar los pesos de Hamming generalizados resultan de interés otras áreas de las matemáticas como lo son la topología, la combinatoria, el álgebra conmutativa, la teoría de matroides y el álgebra homológica. De hecho, el interés principal de esta tesis es estudiar la teoría de códigos y como se relaciona con las áreas antes mencionadas, principalmente con el álgebra conmutativa y el álgebra homológica (números de Betti); así como con la teoría de matroides.

A lo largo de esta tesis, vamos a considerar a $S := \mathbb{K}[x_1, \ldots, x_n]$ como el anillo de polinomios en n-indeterminadas con coeficientes en un campo $\mathbb{K}$. Sea C un código lineal, es decir, C es un subespacio vectorial de $\mathbb{F}_q^n$; por lo cual existe una matriz H, llamada de verificación de paridad de C, tal que representa a un sistema de ecuaciones homogéneo cuyo espacio solución es C. De esta forma, se puede construir una matroide a partir de H llamada la matroide vector asociada a H y denotada por $\mathcal{M}_C$. Además a $\mathcal{M}_C$ se le puede asociar un ideal $I_C \subset S$, tal que es generado por monomios. Del teorema de las sicigias de Hilbert, S/I_C tiene una resolución libre minimal graduada estándar, digamos:

$$0 \to F_\rho \to F_{\rho-1} \to \cdots \to F_1 \to S \to S/I_C \to 0,$$

tal que para todo $i \in \{1, \ldots, \rho\}$, F_i es un S-módulo libre, finitamente generado y graduado estándar; donde el número mínimo de generadores de grado j para F_i es denotado por $\beta_{i,j}(S/I_C)$ y es llamado el i-ésimo número de Betti de grado j. Así, los objetivos generales de esta tesis son:

1. Obtener una relación entre los números de Betti de S/I_C y los pesos generalizados de Hamming de C.

2. Caracterizar algunas familias de códigos en términos de sus números de Betti.

Para alcanzar los objetivos generales de está tesis, el contenido del presente trabajo se dividide en dos capítulos. El capítulo 1 está dedicado a la teoría de los números de Betti, principalmente a los números de Betti G-graduados, con G un grupo abeliano, a diferencia de la mayoría de los textos que abordan este tema, pero únicamente para el caso local o el caso graduado estándar. Nosotros adaptamos dichos resultados para los números de Betti G-multigraduados cuasi-positivos. Además se estudian los números de Betti para ideales monomiales, principalmente los que se obtienen a partir de matroides, por su relevancia en la teoría de códigos como se verá en el capítulo 2. Así, en la sección 1.1 adaptamos algunos resultados de anillos de polinomios con n-indeterminadas sobre un campo $\mathbb{K}$, G-multigraduados cuasi-positivos, donde G es un grupo abeliano. Primeramente se demuestra el lema de Nakayama (lema 1.1.9) usando algunas ideas que se encuentran en el libro de Atiyah para R-módulos con R un anillo local (ver proposicion 2.6, [3]). El lema de Nakayama será parte fundamental para mostrar la existencia de resoluciones libres minimales de S-módulos G-multigraduados cuasi-positivos finitamente generados (teorema 1.1.18). Una vez demostrado el teorema de existencia de las resoluciones libres minimales definiremos los números de Betti a partir de la proposición 1.1.20.

En la sección 1.2 se explica la tabla de los números de Betti de cualquier S-módulo graduado estándar. En la sección 1.3 se muestra la biyección que existe entre complejos simpliciales e ideales monomiales libres de cuadrados, a través del ideal de Stanley-Reisner de un complejo simplicial; la cual nos permitirá estudiar los números de Betti de un ideal monomial libre de cuadrados, de manera combinatoria; dando como resultado la fórmula de Hochster que se enunciará en el teorema 1.3.29.

El objetivo principal de la sección 1.4 es estudiar los números de Betti del ideal de Stanley-Reisner del complejo de independencia de una matroide $\mathcal{M}$, denotado por $\mathcal{I}_{\mathcal{M}}$. Es por eso, que en dicha sección se comienza estudiando brevemente la teoría de matroides usando como referencia principal [24]. Observaremos que una matroide $\mathcal{M}$ permite definir una retícula geométrica, la cual es llamada la retícula de cerrados de $\mathcal{M}$. La retícula geométrica que es relevante para el estudio de los números de Betti es la retícula de cerrados de la matroide dual de $\mathcal{M}$, la cual define una retícula $\mathcal{N}$ con objetos de $\mathcal{M}$ gracias a la proposición 1.4.20. En el teorema 1.4.30 se obtiene una fórmula combinatoria para calcular los números de Betti de $S/I_{\mathcal{M}}$ que depende exclusivamente de la retícula $\mathcal{N}$. Cabe señalar que el teorema 1.4.30 apareció primero en [15]; sin embargo, la demostración que aparece en ese artículo necesita definir un invariante numérico para una matroide, del cual nosotros prescindimos y únicamente usamos resultados clásicos de la teoría de matroides que aparecen en [24]. También la proposición 1.4.20 ya había aparecido en [2], pero para su demostración se requieren resultados de [15]. Al final de la sección 1.4 en el corolario 1.4.31 se obtiene la regularidad de Castelnuovo-Mumford de $S/I_{\mathcal{M}}$ en términos de la matroide; este resultado apareció en [20, lema 4.6] en el caso en que $\mathcal{M}$ es una matroide vector sobre un campo finito.

El segundo capítulo está dedicado a entender la relación entre los pesos generalizados de Hamming de cualquier código C y los números de Betti de S/I_C. Así, la sección 2.1 aborda brevemente los conceptos y propiedades básicas de la teoría de códigos; además se definen

los pesos de Hamming generalizados para un código lineal C. Gracias al teorema de Wei (teorema 2.1.12) se obtiene una definición equivalente para los pesos de Hammming generalizados en términos de la matroide $\mathcal{M}_C$. De hecho, se observa que los pesos de Hamming generalizados se pueden definir para cualquier matroide, aunque no provenga de un código; y a partir de lo obtenido en la sección 1.4 se obtiene una fórmula para calcular los pesos generalizados Hamming de cualquier matroide $\mathcal{M}$ en términos de sus números de Betti de su ideal de Stanley-Reisner $I_{\mathcal{M}}$ (proposición 2.1.13). De esta forma, en la sección 2.1 se alcanza el primer objetivo general de la tesis. En las siguientes dos secciones de este capítulo se busca alcanzar el segundo objetivo general. Así, en la seccion 2.2 determinamos la jerarquía de pesos generalizados de Hamming para los códigos de peso constante, que es el corolario 2.2.15. Ahora bien, en la sección 2.3 se da una caracterización de un código de peso constante C en términos de los números de Betti de $S/I_{\mathcal{M}_C}$ (ver el teorema 2.3.3 y su recíproco 2.3.5).

Índice general

Capítulo 1

Números de Betti

En todo este capítulo $\mathbb{K}$ denotará un campo cualquiera y $\mathbb{N}$ serán los números naturales, incluyendo al 0. Así, si R es una $\mathbb{K}$-álgebra y $A \subset R$, (A) denotará al ideal generado por A; y $< A >$ denotará el espacio vectorial sobre $\mathbb{K}$ generado por A. Además utilizaremos la letra S para denotar al anillo de polinomios con n indeterminadas con coeficientes en $\mathbb{K}$, es decir, $S := \mathbb{K}[x_1, \ldots, x_n]$. Sea $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotaremos por $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Además si $s \in \mathbb{N}$, $s \neq 0$, $[s] := \{1, \ldots, s\}$.

1.1. Resoluciones libres

En la presente sección se presenta la teoría necesaria para abordar los números de Betti, principalmente los números de Betti G-graduados, con G un grupo abeliano. Los resultados que aquí aparecen acerca de las graduaciones cuasi-positivas son adaptaciones del caso local o el caso graduado estándar que se pueden consultar en [6, capítulo 1.5] y [10, 1B]. El lema de Nakayama es parte fundamental para mostrar la existencia de resoluciones libres minimales, el cual es un resultado que adaptamos del caso local para el caso de S-módulos G-multigraduados cuasi-positivos finitamente generados. Una vez establecida la existencia de resoluciones libres minimales definiremos los números de Betti. A lo largo de este capítulo vamos a suponer algunos conceptos y resultados de álgebra conmutativa y de álgebra homológica que se encuentran en el libro de Atiyah [3] y en el libro de Rotman [28].

Sean G un grupo abeliano y R un anillo. Recordemos que R es un **anillo G-graduado** si existe una familia de subgrupos abelianos de R indexada por G, denotada por $\{R_g\}_{g\in G}$, tales que $R = \oplus_{g\in G} R_g$ y $R_g R_h \subset R_{g+h}$ para cualesquiera $g, h \in G$. Además si M es un R-módulo, diremos que M es un **módulo G-graduado** si existe una familia de subgrupos abelianos M_g de M tal que se satisface: $M = \oplus_{g\in G} M_g$ y $R_g M_h \subset M_{g+h}$ para cualesquiera $g, h \in G$. Un elemento $a \in M$ es llamado homogéneo si $a \in M_g$ para algún $g \in G$. Así diremos que el grado de a es g, simbólicamente, $\deg(a) = g$. Recordemos que como M se descompone en una suma directa se tiene que para cada $x \in M$ existe una única manera de expresarse, i.e., $x = \sum_{g\in G} a_g$, con $a_g \in M_g$ y todos los a_g son igual a cero, excepto por un número finito de ellos que son distintos de cero. Donde para cada $g \in G$, a_g se llama la componente homogénea de x de grado g. Sea N un submódulo de M, diremos que N es un **submódulo G-graduado** si es generado por elementos homogéneos de M. Así si $I \subset R$ es un ideal,

diremos que es G-graduado si es un submódulo graduado de R, con R módulo sobre si mismo.

Sean M y N dos R-módulos G-graduados y $\varphi : M \to N$ un R-homomorfismo. Diremos que φ es un **morfismo graduado** si para cada $g \in G$, $\varphi(M_g) \subset N_g$.

1.1.1 Proposición. *Sean R un anillo G-graduado, M, N, dos R-módulos G-graduados y $\varphi : M \to N$ un morfismo graduado. Entonces* $\ker(\varphi)$ *e* $\mathrm{im}(\varphi)$ *son G-submódulos graduados.*

Demostración. Sea $f \in \ker(\varphi) \subset M$, f tiene una única descomposición en suma de elementos homogéneos de M, digamos $f = f_{1_f} + \cdots + f_{n_f}$ con $f_{1_f}, \ldots, f_{n_f} \in M$ homogéneos. Así, para $f \in \ker(\varphi)$, $0 = \varphi(f) = \varphi(f_{1_f} + \cdots + f_{n_f}) = \varphi(f_{1_f}) + \cdots + \varphi(f_{n_f})$. Entonces $\varphi(f_{i_f}) = 0$, así concluímos que $f_{i_f} \in \ker(\varphi)$. Por lo tanto

$$\ker(\varphi) = (f \in M : f \in \ker(\varphi)) = (f_{i_f} \in M : f \in \ker(\varphi), 1 \leq i_f \leq n_f).$$

Por otro lado, sea $g \in \mathrm{im}(\varphi)$. Entonces existe $f \in M$ tal que $\varphi(f) = g$, pero como $f \in M$, f tiene una única descomposición en suma de elementos homogéneos de M, digamos $f = f_{1_f} + \cdots + f_{r_f}$ con $f_{1_f}, \ldots, f_{r_f} \in M$ homogéneos. Por lo que

$$g = \varphi(f) = \varphi(f_{1_f} + \cdots + f_{r_f}) = \varphi(f_{1_f}) + \cdots + \varphi(f_{r_f}), \text{ entonces cada } \varphi(f_{i_f}) \in \mathrm{im}(\varphi).$$

Así, $\mathrm{im}(\varphi) = (g \in N : g \in \mathrm{im}(\varphi)) = (\varphi(f_{i_f}) \in N : g \in \mathrm{im}(\varphi), 1 \leq i_f \leq r_f)$. ∎

En este trabajo estamos sobre todo interesados en graduaciones del anillo de polinomios $S := \mathbb{K}[x_1, \ldots, x_n]$ de n indeterminadas sobre el campo $\mathbb{K}$, por lo que a partir de este momento nos enfocaremos en ellas. Para tal fin haremos uso de una función grado, denotada por deg, que definiremos enseguida.

Sea G un grupo abeliano y consideremos que el $0 \in \mathbb{N}$. Diremos que $\deg : \mathbb{N}^n \to G$ es una **función de grado**, cuando deg es una función aditiva, i.e, $\deg(\alpha + \alpha') = \deg(\alpha) + \deg(\alpha')$ para cualesquiera $\alpha, \alpha' \in \mathbb{N}^n$. Obsérvese que $\deg(0) = 0$.

1.1.2 Observación. Toda función de grado nos induce una graduación en $S := \mathbb{K}[x_1, \ldots, x_n]$; pues si $\deg : \mathbb{N}^n \to G$ es una función de grado y definimos para cada $g \in G$,

$$S_g = \langle x^\alpha : \deg(\alpha) = g \rangle;$$

así $\mathbb{K}[x_1, \ldots, x_n] = \bigoplus S_g$; y como deg es una función aditiva, se tiene que $S_g S_h \subseteq S_{g+h}$ para cada $g, h \in G$; de esta forma S adquiere la estructura de anillo G-graduado. Diremos que S es un anillo G-**multigraduado** para hacer notar que existe una función $\deg : \mathbb{N}^n \to G$ que gradúa a S.

1.1.3 Ejemplos.

1. Sea $G = \mathbb{Z}$. La función de grado $\deg : \mathbb{N}^n \to \mathbb{Z}$ asociada al conjunto $\{b_1, \ldots b_n\} \subset \mathbb{Z}$ es: $\deg_{\{b_1,\ldots,b_n\}} : \mathbb{N}^n \to \mathbb{Z}$, $\deg_{\{b_1,\ldots,b_n\}}((\alpha_1, \ldots, \alpha_n)) = \alpha_1 b_1 + \cdots + \alpha_n b_n$. La función $\deg_{\{b_1,\ldots,b_n\}}$ induce una graduación sobre S, llamada la $(b_1, \ldots, b_n)$-graduación. Así

$$S_i = \langle x^\alpha : i = \deg_{\{b_1,\ldots,b_n\}}(\alpha) \rangle.$$

2. La **graduación estándar** en S es aquella donde la función de grado es $|\cdot| : \mathbb{N}^n \to \mathbb{Z}$ tal que $|(\alpha_1, \ldots, \alpha_n)| = \sum_{i=1}^{n} \alpha_i$. Así $S_i = \langle x^\alpha : i = |\alpha| \rangle$. Notemos que la graduación estándar es la $(1, \ldots, 1)$-graduación.

3. La **multigraduación** en S es aquella graduación que tiene función de grado $i : \mathbb{N}^n \to \mathbb{Z}^n$ (función inclusión). Así S es de la forma $S = \oplus_\alpha S_\alpha$ con $S_\alpha = \mathbb{K} \cdot x^\alpha$. □

1.1.4 Definición. Una función de grado $\deg : \mathbb{N}^n \to G$ es una función de **grado no negativa**, si para $g \in \mathrm{im}(\deg)$, $g \neq 0$, se tiene que $-g \notin \mathrm{im}(\deg)$. Diremos que la función $\deg : \mathbb{N}^n \to G$ es de **grado cuasi-positiva** si para cada $\alpha \in \mathbb{N}^n$, $\alpha \neq 0$, es tal que $\deg(\alpha) \neq 0$; y además es una función de grado no negativa. Así, nos referiremos a una **multigraduacion cuasi-positiva** para S como aquella G multigraduación de S cuya función de grado $\deg : \mathbb{N}^n \to G$ es cuasi-positiva.

En general, se dice que la función $\deg : \mathbb{N}^n \to G$ es una función de **grado positiva** si es función de grado cuasi-positiva y el grupo abeliano G es libre de torsión; esto para garantizar que todos los primos asociados en cualquier S-módulo sean multigraduados (ver proposición 8.11, [22]).

1.1.5 Ejemplos.

1. Consideremos la graduación estándar en S, la función de grado $|\cdot| : \mathbb{N} \to \mathbb{Z}$ es cuasi-positiva.

2. Consideremos la $(1, 1, \ldots, -1)$-graduación. La cual no es no-negativa, pues $\deg(1, 0, \ldots, 0) = 1$ y $\deg(0, \ldots, 0, 1) = -1$. Además, $\deg(1, 0, \ldots, -1) = 0$.

3. Consideremos la $(1, 0, \ldots, 0)$-graduación. De esta forma, $\deg(a_1, a_2, \ldots, a_n) = a_1$, tenemos que deg es no negativa. Pero como $\deg(0, 1, \ldots, 0) = 0$, entonces deg no es cuasi-positiva. □

1.1.6 Proposición. *Sean G un grupo abeliano y $\deg : \mathbb{N}^n \to G$ una función de grado. Entonces los siguientes enunciados son equivalentes:*

1. *La función* deg *es una función cuasi-positiva.*

2. *Para cada $\alpha \in \mathbb{N}^n$, $\alpha \neq 0$, $\deg(\alpha) \neq 0$.*

3. *Para cada $\alpha, \alpha' \in \mathbb{N}^n$, $\deg(\alpha) \neq -\deg(\alpha')$.*

Demostración.

1⇒2) Por definición.

2⇒3) Supongamos que existe $\alpha, \alpha' \in \mathbb{N}^n$ tal que $\deg(\alpha) = -\deg(\alpha')$, entonces $\deg(\alpha + \alpha') = 0$. Así $\alpha + \alpha' = 0$, $\alpha = 0 = \alpha'$.

3⇒2) Supongamos que $\alpha \neq 0$ con $\deg(\alpha) = 0$. Como $\deg(\alpha) = 0$, entonces $\deg(\alpha) = -\deg(0)$. Lo cual es una contradicción con 3.

3⇒1) Dado que cada $g := \deg(\alpha)$ se tiene que $g \neq -g$, entonces deg es no negativa. Además si existe $\alpha \neq 0$ con $\deg(\alpha) = 0$, se tiene de la demostración de 3⇒2) una contradicción con 3. ∎

1.1.7 Proposición. *Sea $S = \mathbb{K}[x_1, \ldots, x_n]$ G-multigraduado. Se tiene que $S_0 = \mathbb{K}$ si, y solo si, S es G-multigraduado cuasi-positivo.*

Demostración.

⇒) (Por contrapositiva) Supongamos que existe $\alpha \in \mathbb{N}^n$, $\alpha \neq 0$, tal que $\deg(\alpha) = 0$. Entonces $x^\alpha \in S_0$, por lo tanto $S_0 \neq \mathbb{K}$. Ahora bien, si existe $\alpha, \alpha' \in \mathbb{N}^n$, distintos de cero tal que $\deg(\alpha) = -\deg(\alpha')$, así $\deg(\alpha) + \deg(\alpha') = 0$ por lo cual $\deg(\alpha + \alpha') = 0$. Entonces $x^{\alpha+\alpha'} \in S_0$.

⇐) (Por contrapositiva) Supongamos que existe $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\alpha \neq (0, \ldots, 0)$, tal que $\deg(\alpha) = 0$. Así, existe $i \in \mathbb{N}$ tal que $\alpha_i \neq 0$ y $x^\alpha = x_i(x_1^{\alpha_1} \cdots x_i^{\alpha_i - 1} \cdots x_n^{\alpha_n})$. De esta forma, $\alpha' := (\alpha_1, \ldots, \alpha_i - 1, \ldots, \alpha_n) \in \mathbb{N}^n$ y $x^\alpha = x_i x^{\alpha'}$. Más aún, $0 = \deg(\alpha) = \deg(e_i) + \deg(\alpha')$, con e_i el vector canónico; entonces $\deg(e_i) = 0$ ó $\deg(e_i) = -\deg(\alpha')$. ∎

Denotemos a $\mathfrak{m} := (x_1, \ldots, x_n) \subset S$, al cual se le conoce como el **ideal irrelevante** de S.

1.1.8 Observación. De la proposición 1.1.7, si S es un anillo G-multigraduado cuasi-positivo, entonces $S_0 = \mathbb{K}$, por lo tanto el ideal irrelevante $\mathfrak{m} = (x_1, \ldots, x_n) = \oplus_{g \neq 0} S_g$ y además es el único ideal maximal G-homogéneo.

1.1.9 Lema. (**NAK**) *Sean G un grupo abeliano y supongamos que $S = \mathbb{K}[x_1, \ldots, x_n]$ es G-multigraduado cuasi-positivo. Sea M un S-módulo G-multigraduado finitamente generado e $I \subset \mathfrak{m}$ un ideal homogéneo de S. Entonces las siguientes afirmaciones son ciertas:*

1. *Si $M = IM$ entonces $M = 0$.*
2. *Si dado un submódulo G-multigraduado N de M, $M = IM + N$. Entonces $M = N$.*

Demostración.

1. Dado que M es finitamente generado y G-multigraduado, supongamos que es generado por $f_1, \ldots, f_p \in M$, donde cada $f_i = f_{i1} + \cdots + f_{ir_i}$ con f_{ij} homogéneo en M entonces podemos suponer que existe un sistema homogéneo de generadores para M, a decir, $\{m_1, \ldots, m_s\}$. Por hipótesis $M = IM$, de lo cual para cada $i \in [s]$, existen $m^{(i)} \in M$ y $\alpha_i \in I$ tal que $m_i = \alpha_i m^{(i)}$. Como $m^{(i)} \in M$, existen $a_{1i}, \ldots, a_{si} \in S$, $m^{(i)} = a_{1i}m_1 + \cdots + a_{si}m_s$ y así $m_i = \alpha_i(a_{1i}m_1 + \cdots + a_{si}m_s)$. Pero como S es un anilllo G-multigraduado e I es homogéneo, entonces para cada $i \in [s]$ y para cada $j \in [s]$ existen $a_{1_{ji}}^{(ji)}, \ldots, a_{r_{ji}}^{(ji)} \in S$ homogéneos y $\alpha_i^{(1)}, \ldots, \alpha_i^{(l_i)} \in I$ tales que:

$$\begin{aligned} m_i &= (\alpha_i^{(1)} + \cdots + \alpha_i^{(l_i)})[(a_{1_{1i}}^{(1i)} + \cdots + a_{r_{1i}}^{(1i)})m_1 + \cdots + (a_{1_{si}}^{(si)} + \cdots + a_{r_{si}}^{(si)})m_s] \\ &= \alpha_i^{(1)} a_{1_{1i}}^{(1i)} m_1 + \cdots + \alpha_i^{(1)} a_{r_{1i}}^{(1i)} m_1 + \cdots + \alpha_i^{(l_i)} a_{1_{1i}}^{(1i)} m_1 + \cdots + \alpha_i^{(l_i)} a_{r_{1i}}^{(1i)} m_1 + \\ &\cdots + \alpha_i^{(l_i)} a_{1_{s_i}}^{(si)} m_s + \cdots + \alpha_i^{(l_i)} a_{r_{s_i}}^{(si)} m_s. \end{aligned}$$

Como cada sumando de la parte derecha de la última ecuación es homogéneo y m_i es homogéneo de grado $\deg(m_i)$, entonces tenemos dos casos:

a) $\deg(\alpha_i^{(t)} a_{k_{ji}}^{(ji)} m_j) = \deg(m_i)$ y así $\deg(\alpha_i^{(t)} a_{k_{ji}}^{(ji)}) = \deg(m_i) - \deg(m_j)$.

b) $\deg(\alpha_i^{(t)} a_{k_{ji}}^{(ji)} m_j) \neq \deg(m_i)$ entonces para $\alpha_i^{(t)} a_{k_{ji}}^{(ji)} m_j$ existen sumandos tales que anulan a $\alpha_i^{(t)} a_{k_{ji}}^{(ji)} m_j$. Por lo cual, podemos omitir a dichos elementos.

Por lo tanto, sin pérdida de generalidad, podemos suponer que $m_i = b_{1i}m_1 + \cdots + b_{si}m_s$, tal que $\deg(b_{ji}) = \deg(m_i) - \deg(m_j)$, así pues, $\deg(b_{ii}) = 0$; pero como $b_{ii} \in I \subset \mathfrak{m}$, de la observación 1.1.8 se tiene que $\deg(b_{ii}) = 0$ si, y solo si, $b_{ii} = 0$. Así, $m_i = b_{1i}m_1 + \cdots + b_{(i-1)i}m_{i-1} + b_{(i+1)i}m_{i+1} + \cdots + b_{si}m_s$. Entonces

$$-b_{1i}m_1 - b_{2i}m_2 - \cdots + m_i - \cdots - b_{si}m_s = 0. \tag{1.1}$$

- Observemos que si para cada $B \in M_{s\times s}(S)$ definimos $Bm_i = [b_{1i}]m_i + \cdots + [b_{si}]m_i$, nos define una acción del grupo de matrices $M_{s\times s}(S)$ en M. Donde

  $$B \cdot m = B(b_1m_1 + \cdots + b_sm_s).$$

  Por lo cual $I_{s\times s} \cdot m = m$ con $I_{s\times s}$ la matriz identidad y $C \cdot (B \cdot m) = (C \times B) \cdot m$, donde $\times$ denota el producto matricial.

- De la ecuación 1.1 tenemos que $C \cdot m = 0$ para toda $m \in M$, donde

  $$C_{s\times s} = \begin{pmatrix} 1 & -b_{12} & \cdots & -b_{1i} & \cdots - b_{1s} \\ -b_{21} & 1 & \cdots & -b_{2i} & \cdots - b_{2s} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -b_{i1} & -b_{i2} & \cdots & 1 & \cdots - b_{is} \\ \vdots & \vdots & & \vdots & \vdots \\ -b_{s1} & -b_{s2} & \cdots & -b_{si} & \cdots 1 \end{pmatrix}.$$

  De esta forma, para toda $m \in M$,

  $$0 = (\mathrm{Adj}C)(C \cdot m) = \det(C) \cdot m \tag{1.2}$$

- Ahora bien, calculemos el $\det(C)$. Recordemos que si $A_{n\times n} = [a_{ij}]$, el $\det(A) = \sum_{\sigma\subset S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$ donde

  $$\mathrm{sign}(\sigma) = \begin{cases} 1 & \text{si } \sigma \text{ es producto de un número par de ciclos de longitud 2,} \\ -1 & \text{si } \sigma \text{ es producto de un número impar de ciclos de longitud 2.} \end{cases}$$

  Denotemos como $[A]_{ij} = a_{ij}$, por lo tanto,

  $$\det(C) = \sum_{\sigma\subset S_n} \mathrm{sign}(\sigma)[\mathrm{C}]_{1\sigma(1)}[\mathrm{C}]_{2\sigma(2)}\cdots[\mathrm{C}]_{\mathrm{s}\sigma(\mathrm{s})} \text{ (ver[[24], pp,83])}.$$

  Sea $\sigma \subset S_s$ e $i_1, \ldots, i_j$ los puntos fijos de σ con $j \leq s$. Sin pérdida de generalidad podemos suponer que $i_1 = 1, \ldots, i_j = j$. Entonces tenemos dos casos:

  - Si todos son puntos fijos de σ, $[C]_{1\sigma(1)}[C]_{2\sigma(2)}\cdots[C]_{s\sigma(s)} = 1$ y dado que $\mathrm{sign}(\sigma(i)) = 1$ pues $\sigma(i)$ es el producto de un número par de ciclos de longitud 2, $\mathrm{sign}(\sigma(i))[C]_{1\sigma(1)}\cdots = 1$.

- En caso contrario,

$$[C]_{j+1\sigma(j+1)} \cdots [C]_{s\sigma(s)} = (-b_{j+1\sigma(j+1)})(-b_{j+2\sigma(j+2)}) \ldots (-b_{s\sigma(s)}) \text{ y}$$

$$\begin{aligned} \deg((-b_{j+1\sigma(j+1)})(-b_{j+2\sigma(j+2)}) \ldots (-b_{s\sigma(s)})) &= \sum_{i=j+1}^{s} \deg(b_{i\sigma(i)}) \\ &= \sum_{i=j+1}^{s} \deg(m_{\sigma(i)}) - \deg(m_i) \\ &= 0, \end{aligned}$$

donde la última igualdad se sigue del hecho de que σ es biyectiva.

Así $\det(C) = 1$. Pero de la ecuación 1.2, para cada $m \in M$,

$$0 = \det(C) \cdot m = 1 \cdot m = m.$$

Por lo tanto, $M = 0$.

2. Consideremos el submódulo G-multigraduado M/N. Como $M = IM + N$, se tiene que $M/N = (IM + N)/N = IM/(N \cap IM) = I(M/N)$. Así, $M/N = 0$ del inciso 1 de este lema; por lo tanto $M = N$. ∎

1.1.10 Proposición. *Sean $S = \mathbb{K}[x_1, \ldots, x_n]$ G-multigraduado cuasi-positivo, M un S-módulo G-graduado cuasi-positivo finitamente generado, $Y := \{m_1, \ldots, m_s\} \subset M$ y $\overline{Y} := \{\overline{m_1}, \ldots, \overline{m_s}\} \subset M/\mathfrak{m}M$, donde $\overline{m_i} = m_i + \mathfrak{m}M$. Entonces se tienen las siguientes propiedades:*

1 El conjunto Y es un conjunto generador de M si, y solo si, $\overline{Y}$ es un conjunto generador de $M/\mathfrak{m}M$.

2 El conjunto Y es un conjunto minimal de generadores para M si, y solo si, $\overline{Y}$ es una base para el espacio vectorial $M/\mathfrak{m}M$.

Demostración.

1. Supongamos que Y es un conjunto generador para M, entonces $\overline{Y}$ genera a $M/\mathfrak{m}M$. Ahora supongamos que $\overline{Y}$ genera a $M/\mathfrak{m}M$. Sean M' el submódulo generado por $m_1, \ldots, m_s$ y $M'' = M/M'$; de esta forma se obtiene una sucesión exacta $0 \to M' \to M \to M'' \to 0$. La sucesión anterior la tensorizamos con $S/\mathfrak{m}$, $\cdots \to M' \otimes S/\mathfrak{m} \to M \otimes S/\mathfrak{m} \to M'' \otimes S/\mathfrak{m} \to 0$. Recordemos la siguiente propiedad: $M \otimes S/\mathfrak{m} \simeq M/\mathfrak{m}M$; y así la sucesión anterior exacta por la derecha se convierte en: $\cdots \to M'/\mathfrak{m}M' \xrightarrow{\bar{i}} M/\mathfrak{m}M \to M''/\mathfrak{m}M'' \to 0$. Dado que $m_1, \ldots, m_s \in M'$ y $\overline{m}_1, \ldots, \overline{m}_s$ generan a $M/\mathfrak{m}M$, se tiene que $\bar{i}$ es un epimorfismo, así $M''/\mathfrak{m}M'' = 0$; de lo cual $M'' = mM''$. Como M es finitamente generado y S es G-multigraduado cuasi-positivo, por el lema de Nakayama 1.1.9 se tiene que $M'' = 0$, pero $M'' = M/M'$; de aquí que $M' = M$.

2. Supongamos que $\overline{Y}$ no es linealmente independiente, por lo cual sin pérdida de generalidad $\{\overline{m_2}, \ldots, \overline{m_s}\}$ es un conjunto generador para $M/\mathfrak{m}M$. Pero del inciso 1 de esta proposición, $Y' := \{m_2, \ldots, m_s\}$ es un conjunto generador de M, lo cual es una contradicción, pues Y es minimal. Entonces $\overline{Y'}$ es linealmente independiente, por lo que $\overline{Y}$ es una base de $M/\mathfrak{m}M$. De manera similar si suponemos que Y no es minimal, entonces $\overline{Y}$ no es una base para $M/\mathfrak{m}M$. ∎

1.1.11 Observación. De la proposición 1.1.10, todos los conjuntos de generadores minimales de cualquier S-módulo G-multigraduado cuasi-positivo son del mismo tamaño.

1.1.12 Definición. Una **resolución libre G-multigraduada** sobre un S-módulo G-multigraduado M es una sucesión de S-morfismos graduados

$$\mathcal{F} : \cdots \to F_r \xrightarrow{\partial_r} F_{r-1} \to \cdots \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0, \tag{1.3}$$

tal que cada F_i es un S-módulo libre G-multigraduado, $\mathcal{F}$ es exacto y $\mathrm{M} \simeq \mathrm{F}_0/\mathrm{im}(\partial_1)$.

Cuando hablemos de una resolución libre G-multigraduada $\mathcal{F}$ de M, en algunas ocasiones la escribiremos como $\mathcal{F} : \cdots \to F_r \xrightarrow{\partial_r} F_{r-1} \to \cdots \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0$, donde la sucesión es exacta; esto se puede hacer dado que (1.3) es exacta y

$$\mathrm{coker}(\partial_1) = F_0/\mathrm{im}(\partial_1) = F_0/\ker(\partial_0) \simeq M.$$

Sea $S = \mathbb{K}[x_1, \ldots, x_n]$ G-multigraduado cuasi-positivo, definamos el **corrimiento** de S por $h \in G$ como $S(-h)$ donde $S(-h)_g := S_{g+h}$.

1.1.13 Proposición. *Sea M un S-módulo. Si M es G-multigraduado. Entonces tiene una resolución libre G-multigraduada.*

Demostración. Dado que M es graduado, i.e., $M = \oplus_{g\in G} M_g$. Definamos para cada $g \in G$, $S(-g)^{(M_g)} := \oplus_{m_g \in M_g} S \cdot e_{m_g}$, donde $\deg(e_{m_g}) = g$, de esta forma podemos definir el siguiente morfismo graduado sobreyectivo $\partial_0 : \oplus_{g\in G} S(-g)^{(M_g)} \to M$, donde $\partial_0(e_{m_g}) = m_g$ para cada $e_{m_g} \in S(-g)^{(M_g)}$ y para cada $m_g \in M_g$. Definimos a $F_0 := \oplus_{g\in G}(S(-g))^{(M_g)}$ y $K_0 := \ker(\partial_0)$, donde K_0 es G-multigraduado por la proposición 1.1.1. Entonces para K_0 podemos repetir lo anterior y así encontrar un módulo F_1 que sea G-multigraduado libre y un morfismo, $F_1 \xrightarrow{f_1} K_0$. Definamos $\partial_1 := i \circ f_i$, donde $i : K_0 \hookrightarrow F_0$ es el morfismo inclusión. Por lo tanto $F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0$ es exacta; y así sucesivamente podemos construir $\mathcal{F}$.∎

1.1.14 Definición. Una **resolución libre minimal** (G-multigraduada) de un S-módulo G-multigraduado finitamente generado M es una resolución libre G-multigraduada $\mathcal{F}$:

$$0 \longrightarrow F_r \xrightarrow{\partial_r} F_{r-1} \longrightarrow \cdots \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0,$$

tal que $\ker(\partial_i) = \partial_{i+1}(F_{i+1}) \subset \mathfrak{m}F_i$ para cada i $\in \mathbb{N}$.

1.1.15 Proposición. *Sean M un S-módulo G-multigraduado cuasi-positivo finitamente generado sobre S y*

$$\mathcal{F} : \cdots \to F_i \xrightarrow{\partial_i} \cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0$$

una resolución libre G-multigraduada de M. Entonces $\mathcal{F}$ es minimal si, y solo si, las entradas de cualquier matriz asociada a cada ∂_i son polinomios homogéneos no constantes o bien son nulos.

Demostración. Consideremos que $\{e_1, \dots e_{s_i}\}$ denota una base para F_i y $\{f_1 \dots f_{s_{i-1}}\}$ denota una base homogénea de F_{i-1}. Ahora recordemos que cualquier matriz A asociada a ∂_i en S es de la forma:

$$A = \begin{pmatrix} c_{11} & \dots & c_{1s_i} \\ \vdots & \vdots & \vdots \\ c_{s_{i-1}1} & \dots & c_{s_{i-1}s_i} \end{pmatrix},$$

donde $\partial_i(e_j) = c_{1j}f_1 + \cdots + c_{s_{i-1}j}f_{s_{i-1}}$.

Por definición $\mathcal{F}$ es minimal si, y solo si, $\operatorname{im}(\partial_i) \subset \mathfrak{m}F_{i-1}$ para todo $i \in \mathbb{N}$ donde $F_{-1} = M$. Así $\operatorname{im}(\partial_i) \subset \mathfrak{m}F_{i-1}$ si, y solo si, las entradas $c_{jk} \in \mathfrak{m}$ y además son homogéneos porque ∂_i es un morfismo homogéneo. ∎

1.1.16 Ejemplos.

- Sea $I = (x_1x_3, x_2x_4, x_3x_5, x_4x_5)$ un ideal de $S := \mathbb{K}[x_1, x_2, x_3, x_4, x_5]$. Ahora bien una resolución libre minimal de S/I es:

$$0 \to S(-4) \xrightarrow{\begin{pmatrix} 0 \\ -x_5 \\ x_3 \\ -x_2 \end{pmatrix}} S(-3)^4 \xrightarrow{\begin{pmatrix} -x_4 & 0 & 0 & 0 \\ 0 & -x_3 & -x_5 & 0 \\ x_1 & x_2 & 0 & -x_5 \\ 0 & 0 & x_2 & x_3 \end{pmatrix}} S(-2)^4$$

$$\xrightarrow{\begin{pmatrix} x_1x_3 & x_2x_4 & x_3x_5 & x_4x_5 \end{pmatrix}} S \longrightarrow S/I \to 0.$$

  Para obtener la resolución hicimos uso de las bases de Gröbner (ver [1]).

- Ahora bien consideremos la siguiente resolución libre para el ideal I del inciso anterior:

$$0 \to S(-4)^2 \xrightarrow{\begin{pmatrix} 0 & -x_2 \\ -x_5 & 0 \\ x_3 & 0 \\ -x_2 & 1 \end{pmatrix}} S(-3)^4 \oplus S(-4) \xrightarrow{A_2 = \begin{pmatrix} -x_4 & 0 & 0 & 0 & -x_2x_4 \\ 0 & -x_3 & -x_5 & 0 & x_1x_3 \\ x_1 & x_2 & 0 & -x_5 & 0 \\ 0 & 0 & x_2 & x_3 & 0 \end{pmatrix}}$$

$$S(-2)^4 \xrightarrow{\begin{pmatrix} x_1x_3 & x_2x_4 & x_3x_5 & x_4x_5 \end{pmatrix}} S \longrightarrow S/I \to 0.$$

De la proposición anterior se tiene que esta resolución no es minimal. De hecho, si e_1, e_2, e_3, e_4 es la base canónica de $S(-2)^4$,

$$\mathrm{im}(A_2) = (-x_4e_1 + x_1e_3, -x_3e_2 + x_2e_3, -x_5e_2 + x_2e_4, -x_5e_3 + x_3e_4);$$

y podemos observar que $x_2(-x_4e_1 + x_1e_3) - x_1(-x_3e_2 + x_2e_3) = -x_4x_2e_1 + x_1x_3e_2$. Así, el conjunto de generadores de $\mathrm{im}(A_2)$ no es minimal. En la proposición 1.1.19 estudiaremos esto que hemos observado. □

1.1.17 Lema. *Sean M un S-módulo G-multigraduado cuasi-positivo finitamente generado, $\{t_1, \ldots, t_s\}$ un sistema de generadores homogéneos minimal tal que $\deg(t_i) = a_i \in G$ y $\varphi : \oplus_{i=1}^s S(-a_i) \to M$ el morfismo de S-módulos G-graduados definido por $\varphi(e_i) = t_i$. Entonces $\ker(\varphi) \subset \mathfrak{m}(\oplus_{i=1}^s S(-a_i))$.*

Demostración. La proposición es equivalente a demostrar el siguiente enunciado: si $\sum_{i=1}^s c_it_i = 0$ con $c_i \in S$, entonces para cada $i \in [s]$ se tiene que $c_i \in \mathfrak{m}$.

Supongamos que existe $i \in [s]$ tal que $c_i \notin \mathfrak{m}$, por lo tanto, $c_i = p(x) + k$ con $k \in \mathbb{K}$, $k \neq 0$ y $p(x) \in \mathfrak{m}$. Sin pérdida de generalidad podemos suponer que $c_1 \notin \mathfrak{m}$, por hipótesis $\sum_{i=1}^s c_it_i = 0$, así $c_1t_1 = (p(x) + k)t_1 = -\sum_{j=2}^s c_jt_j$. Ahora bien, consideremos el morfismo cociente $\pi : M \to M/\mathfrak{m}M$, $\pi(t_i) = \overline{t_i}$ donde $\overline{t_i} = t_i + \mathfrak{m}M$. Así

$$\pi((p(x) + k)t_1) = \overline{(p(x) + k)t_1)} = k\overline{t_1}.$$

Por otra parte,

$$\pi(\sum_{j=2}^s c_jt_j) = \overline{\sum_{j=2}^s c_jt_j} = \sum_{j=2}^s \overline{c_jt_j} = \sum_{j=2}^s c_j\overline{t_j}.$$

De tal manera que $k\overline{t_1} = \sum_{j=2}^s c_j\overline{t_j}$, así $\overline{t_1} = -k^{-1}\sum_{j=2}^s c_j\overline{t_j}$. Entonces $\{\overline{t_1}, \ldots, \overline{t_s}\}$ no es una base para $M/\mathfrak{m}M$ y por la proposición 1.1.10 se tiene que $\{t_1, \ldots, t_s\}$ no es un conjunto de generadores homogéneos minimal. ■

1.1.18 Teorema (Existencia de resoluciones libres minimales). *Sea M un S-módulo G-multigraduado, cuasi-positivo y finitamente generado. Entonces existe una resolución libre minimal de M.*

Demostración. Dado que M es G-multigraduado y finitamente generado, existe un conjunto de generadores homogéneos minimal, digamos $\{m_1, \ldots, m_s\}$ con $\deg(m_i) = a_i \in G$ para cada $i \in \{1, \ldots, s\}$. Definamos el morfismo graduado $\partial_0 : \oplus_{i=1}^s S(-a_i) \to M$ dado por $\partial_0(e_i) = m_i$ para cada $i \in \{1, \ldots, s\}$. Dado que M es finitamente generado, ∂_0 es sobreyectiva. Por el lema 1.1.17, $\ker(\partial_0) \subset \mathfrak{m}(\oplus_{i=1}^s S(-a_i))$. Denotemos por $F_0 := \oplus_{i=1}^s S(-a_i)$ y $K_0 := \ker(\partial_0)$, donde K_0 es G-multigraduado por la proposición 1.1.1. Ahora bien, para K_0 podemos repetir lo anterior y así encontrar un módulo F_1 que sea G-multigraduado cuasi-positivo libre y un morfismo G-graduado $F_1 \xrightarrow{f_1} K_0$ y así $\ker(f_1) \subset \mathfrak{m}F_1$. Definamos $\partial_1 := i \circ f_1$, donde $i : K_0 \hookrightarrow F_0$ es el morfismo inclusión. Por lo tanto $F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0$ es exacta. Observemos además que $\ker(\partial_1) = \ker(i \circ f_1)$, pero i es inyectiva, así que $\ker(\partial_1) = \ker(f_1) =: K_1$; y así sucesivamente podemos construir $\mathcal{F}$. ■

1.1.19 Proposición. *Sea M un S-módulo G- multigraduado cuasi-positivo finitamente generado. Entonces una resolución libre G-multigraduada de M es minimal si, y solo si, en cada paso de la demostración de la proposición 1.1.13 se escoge un sistema de generadores homogéneos minimal del* $\ker(\partial_i)$.

$\Rightarrow$) Asumamos que para algún $i \geq -1$, escogemos un sistema de generadores homogéneo no mínimal del $\ker(\partial_i)$, digamos $l_1, \ldots, l_s$, por lo que sin pérdida de generalidad podemos suponer que $l_1 = \sum_{j=2}^{s} r_j l_j$ para $r_j \in S$; así definimos a $F_{i+1} = \oplus_{j=1}^{s} \mathbb{K} \cdot g_j$ con $\deg(g_j) = \deg(l_j)$ y $\partial_{i+1} : F_{i+1} \to \ker(\partial_i)$ dada por $\partial_{i+1}(g_j) = l_j$ para cada $j \in [s]$, entonces $\partial_{i+1}(g_1) = \sum_{j=2}^{s} r_j \partial_{i+1}(g_j)$, $\partial_{i+1}(g_1) - \sum_{j=2}^{s} r_j \partial_{i+1}(g_j) = 0$. Por lo tanto $g_1 - \sum r_j g_j \in \ker(\partial_{i+1}) = \mathrm{im}(\partial_{i+2})$. Dado que la resolución es minimal, se tiene que $\mathrm{im}(\partial_{i+2}) \subset \mathfrak{m}F_{i+1}$, así pues $g_1 - \sum r_j g_j \in \mathfrak{m}F_{i+1}$. Pero como $\{g_1, \ldots, g_s\}$ es una base de F_{i+1}, entonces $g_1 - r_2 g_2 - \cdots - r_s g_s = p_1 g_1 + \ldots p_s g_s$ con $p_1, \ldots, p_s \in \mathfrak{m}$. Entonces $(1 - p_1)g_1 - \sum_{j=2}^{s}(r_j + p_j)g_j = 0$; y por ser una base $\{g_1, \ldots, g_s\}$, $(1 - p_1) = 0$; y así $p_1 = 1$, lo cual es una contradicción al hecho de que $p_1 \in \mathfrak{m}$.

$\Leftarrow$) Es la demostración del teorema 1.1.18. ∎

Sean $\mathcal{F}$ una resolución libre y M cualquier S-módulo G-multigraduado. Recordemos que el producto tensorial de $\mathcal{F}$ y M se define como

$$\mathcal{F} \otimes M :\to \cdots \to F_r \otimes M \xrightarrow{\partial_r} F_{r-1} \otimes M \to \cdots \xrightarrow{\partial_2} F_1 \otimes M \xrightarrow{\partial_1} F_0 \otimes M.$$

Para la siguiente proposición usaremos el funtor Tor, el cual se puede consultar en [28, capítulo 7] y [6, capítulo 1.5].

1.1.20 Proposición. *Sea $\mathcal{F} : 0 \to F_\rho \xrightarrow{\partial_\rho} \cdots \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0$ una resolución libre minimal de un S-módulo G-multigraduado cuasi-positivo finitamente generado. Entonces cualquier conjunto minimal de generadores homogéneos de F_i tiene exactamente* $\dim_{\mathbb{K}}((\mathrm{Tor}_{\mathrm{i}}^{\mathrm{S}}(\mathrm{M}, \mathbb{K}))_{\mathrm{g}})$ *generadores de grado g.*

Demostración. Dado que $\mathcal{F}$ es minimal, $\partial_i(m) = am'$ con $m \in F_i$, $a \in \mathfrak{m}$ y $m' \in F_{i-1}$; al tensorizar $\mathcal{F}$ con $\mathbb{K}$, tenemos:

$$0 \to F_\rho \otimes \mathbb{K} \xrightarrow{\partial_\rho \otimes id} \cdots \xrightarrow{\partial_2} F_1 \otimes \mathbb{K} \xrightarrow{\partial_1 \otimes id} F_0 \otimes \mathbb{K} \xrightarrow{\partial_0 \otimes id} M \otimes \mathbb{K} \to 0.$$

Ahora bien, sean $m \in F_i$ y $k = (p + \mathfrak{m}) \in \mathbb{K} = S/\mathfrak{m}$ cualesquiera, se tiene que:

$$(\partial_i \otimes id)(m \otimes k) = \partial_i(m) \otimes k = (am') \otimes (p + \mathfrak{m}) = m' \otimes (ap + m) = m' \otimes 0 = 0.$$

Por otro lado, por una propiedad del producto tensorial y dado que $\ker(\partial_i) \subset \mathfrak{m}F_i$, se tiene que $\ker(\partial_i \otimes id) \subset F_i \otimes \mathbb{K}$. Entonces $\ker(\partial_i \otimes id) = F_i \otimes \mathbb{K}$ e $\mathrm{im}(\partial_i \otimes id) = 0$ para todo $i \in \mathbb{N} - \{0\}$. Como para cada $i \in \mathbb{N}$ el módulo F_i es libre, podemos escribir $F_i = \oplus_{g \in G} S(-g)^{\beta_{i,g}}$. Así, por definición del funtor Tor:

$$\begin{aligned}
\mathrm{Tor}_i^S(M, \mathbb{K})_g &= (\ker(\partial_i \otimes id)/\mathrm{im}(\partial_{i+1} \otimes id))_g \\
&= (F_i \otimes \mathbb{K}/0)_g \\
&= (F_i \otimes \mathbb{K})_g \\
&= ((\oplus_{g \in G} S(-g)^{\beta_{i,g}}) \otimes \mathbb{K})_g \\
&\simeq \oplus_{g \in G}(S(-g)^{\beta_{i,g}} \otimes \mathbb{K}))_g \\
&\simeq \mathbb{K}(-g)^{\beta_{i,g}};
\end{aligned}$$

y así $\dim_{\mathbb{K}}((\mathrm{Tor}_i^S(M,\mathbb{K}))_g) = \beta_{i,g}$. ∎

Sean M un S-módulo G-multigraduado cuasi-positivo y

$$\mathcal{F} : 0 \to F_d \xrightarrow{\partial_d} \cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} M \to 0$$

una resolución libre minimal de M, donde cada $F_i = \oplus_{g\in G} S(-g)^{\beta_{i,g}}$. De la proposición 1.1.20 el número $\beta_{i,g}$ no depende de la resolución libre minimal. Así, el número de generadores de grado g del i-ésimo módulo libre de una resolución libre minimal de M es llamado el i**-ésimo número de Betti** de grado g de M, el cual se denota como $\beta_{i,g}(M)$, de esta forma, $\beta_{i,g}(M) := \beta_{i,g}$. Por otro lado, se puede demostrar que toda resolución libre minimal de M es única salvo isomorfismo (ver teorema 7.5(2), [26]); así podemos definir de la resolución libre minimal $\mathcal{F}$ al $\ker(\partial_i)$ como la **i-ésima sicigia** de M, denotándose como $\mathrm{Syz}_i(M)$.

Recordemos que todo módulo proyectivo es sumando directo de un módulo libre. Por lo tanto, todo módulo proyectivo G-multigraduado es aquel que es sumando directo de un módulo libre G-multigraduado.

1.1.21 Proposición. *Si M es un S-módulo proyectivo G-multigraduado cuasi-positivo, finitamente generado, entonces M es libre.*

Demostración. Sean $\{y_1,\ldots,y_s\}$ un sistema minimal de generadores homogéneos y $\deg(y_i) = a_i$ para cada $i \in [s]$ y el morfismo sobreyectivo graduado $\varphi : \oplus_{i=1}^s S(-a_i) \to M$ tal que $\varphi(e_i) = y_i$. Solo resta demostrar que φ es inyectivo.

Por el lema 1.1.17 se tiene que $\ker(\varphi) \subseteq \mathfrak{m}(\oplus S(-a_i)))$. Por hipótesis se tiene que M es sumando directo de un módulo libre G-graduado cuasi-positivo H, entonces existe un submódulo G-multigraduado F de M tal que $H = F \oplus M$. Ahora bien, sean $g_1,\ldots,g_p$ una base de H y $\pi : H \to M$ el morfismo proyección, el cual es un morfismo G-graduado. Como φ es un morfismo sobreyectivo para cada $i \in [s]$ existe $f_i \in \oplus_{i=1}^s S(-a_i)$ tal que $\varphi(f_i) = \pi(g_i)$. Por lo tanto podemos definir un morfismo graduado $\gamma : H \to \oplus_{i=1}^s \oplus S(-a_i)$ dado por $\gamma(g_i) = f_i$. Si consideramos la restricción de γ en M, $\gamma_M : M \to \oplus_{i=1}^s S(-a_i)$. Ahora bien, para cada $m \in M$, existen $a_1,\ldots,a_p \in S$ tal que $m = a_1g_1 + \cdots + a_pg_p$; así:

$$\begin{aligned}
\varphi(\gamma_M(m)) &= \varphi(\gamma_M(a_1g_1 + \cdots + a_pg_p)) \\
&= \varphi(a_1f_1 + \cdots + a_pf_p) \\
&= a_1\pi(g_1) + \cdots + \pi(g_p) \\
&= \pi(a_1g_1 + \cdots + a_pg_p) \\
&= \pi(m) \\
&= m \\
&= id_M(m).
\end{aligned}$$

Por lo que

$$\oplus_{i=1}^s S(-a_i) = Im(\gamma_M) \oplus \ker(\varphi). \tag{1.4}$$

Como $\ker(\varphi) \subset \mathfrak{m}(\oplus_{i=1}^s S(-a_i))$, $\oplus_{i=1}^s \oplus S(-a_i) = \mathrm{im}(\gamma_M) + \mathfrak{m}(\oplus_{i=1}^s \oplus S(-a_i))$. Por el lema de Nakayama 1.1.9, $\oplus_{i=1}^s S(-a_i) = \mathrm{im}(\gamma_M)$ y así de la ecuación (1.3) $\ker(\varphi) = 0$. ∎

Sea R un anillo G-graduado, recordemos que la **dimensión proyectiva** de un R-módulo G-graduado M, la cual denotaremos como dimproj(M), es

$$\text{dimproj(M)} := \text{mín}\{\text{n : n es la longitud de una resolución proyectiva finita de M}\},$$

cuando existe una resolución proyectiva finita, si no dimproj(M) $= \infty$. Además, la **dimensión global proyectiva** del anillo G-graduado R se define como:

$$\text{gldimproj}(R) := \sup\{\text{dimproj}(M) : M \text{ es un R-módulo G-graduado finitamente generado}\}.$$

1.1.22 Proposición. *Sea M un S-módulo G-multigraduado cuasi-positivo finitamente generado. Entonces la dimensión proyectiva de M es igual a la longitud de la resolución libre minimal.*

Demostración. Si la dimproj$(M) = \infty$, entonces la longitud de la resolución libre minimal es infinita. Por otro lado, supongamos que dimproj$(M) < \infty$. Dado que todo módulo libre es proyectivo, entonces

$$\begin{aligned} \text{dimproj}(M) &\leq \text{mín}\{n : n \text{ es la longitud de una resolución libre minimal de M}\} \\ &= \sup\{n \in \mathbb{N} : \text{Tor}_n(M, \mathbb{K}) \neq 0\}. \end{aligned}$$

Donde la última igualdad de la ecuación se debe a la proposición 1.1.20. Sea $\mathcal{F}$ una resolución libre de M de tamaño dimproj(M), entonces por definición del funtor Tor,

$$\text{Tor}_{\text{dimproj(M)+j}}(M, \mathbb{K}) = 0$$

para todo $j \geq 1$. Por la proposición 1.1.20, $\sup\{n \in \mathbb{N} : \text{Tor}_{\text{n}}(M, \mathbb{K}) \neq 0\} \leq$ dimproj(M). Así, la dimproj$(M) = \text{mín}\{n : \text{n es la longitud de una resolución libre minimal de } M\}$. ∎

1.2. Números de Betti graduados

En esta sección se presentan la tabla de los números de Betti de un módulo graduado estándar finitamente generado sobre S como una manera de visualizar el número de generadores de grado $i + j$ del i-ésimo módulo libre de una resolución libre minimal de un módulo. Además se muestra que dicha tabla es finita. El teorema 1.2.8 es parte fundamental de la demostración del inciso 2 del teorema 2.3.3, dicho resultado es uno de los teoremas claves de está tesis.

1.2.1 Teorema. (**de las sicigias de Hilbert** (Teorema 1.1, [10])) *Sea $\mathbb{K}$ un campo y $S = \mathbb{K}[x_1, \ldots, x_n]$ graduado estándar. Entonces* gldimproj$(S) = n$.

1.2.2 Teorema. *Sea M un S-módulo graduado estándar finitamente generado y $\{\beta_{i,j}\}$ el conjunto de los números de Betti de M. Para algún $d \in \mathbb{N}$, si $\beta_{i,j}(M) = 0$ para cada $j < d$, entonces $\beta_{i+1,j+1}(M) = 0$ para cada $j < d$.*

Demostración. Consideramos la resolución libre minimal de M. Dado que $\beta_{i,j} = 0$ para cada $j < d$, se tiene que todos los generadores de F_i tienen grado mayor o igual que d. Entonces todos los elementos de $\mathfrak{m}F_i$ tienen grado mayor o igual a d+1. Por la minimalidad, los generadores de F_{i+1} mediante el morfismo ∂_i preservan el grado en $\mathfrak{m}F_i$, entonces su grado es mayor o igual a d+1, así $\beta_{i+1,j+1} = 0$ para $j < d$. ∎

Sea $\mathcal{F} : 0 \to F_s \to \cdots \to F_0 \xrightarrow{\partial_0} M$ una resolución libre minimal de un S-módulo M graduado estándar finitamente generado. Del teorema 1.2.2 podemos observar que para cualquier $i \in \mathbb{N}$ los grados de los generadores minimales del módulo libre F_i son mayores que los grados de los generadores minimales del módulo libre F_{i+1}. La tabla $B(M)$ de números de Betti de M, es $[B(M)]_{ij} = \beta_{i,i+j}(M)$.

Se define la **regularidad de Castelnuovo-Mumford** como

$$\text{reg}(M) := \text{máx}\{j \in \mathbb{N} : \beta_{i,i+j}(M) \neq 0, \text{ para algún i} \in \mathbb{N}\}.$$

Denotemos como $r = \text{reg}(M)$ y $\rho = \text{dimproj}(M)$; entonces por la definición de la regularidad de Castelnuovo-Mumford y por la proposición 1.1.20 la tabla de números de Betti de M se ve de la siguiente forma:

j\i	0	1	...	ρ
0	$\beta_{0,0}$	$\beta_{1,0+1}$	...	$\beta_{\rho,0+\rho}$
⋮	⋮	⋮	⋮	⋮
t	$\beta_{0,t}$	$\beta_{1,t+1}$	...	$\beta_{\rho,t+\rho}$
t+1	$\beta_{0,t+1}$	$\beta_{1,t+1+1}$	...	$\beta_{\rho,t+\rho+1}$
⋮	⋮	⋮	⋮	⋮
r	$\beta_{0,r}$	$\beta_{1,r+1}$	...	$\beta_{\rho,r+\rho}$.

Definamos el número de Betti total como $\beta_i := \sum_{j=0}^{r+i} \beta_{i,j}$.

1.2.3 Ejemplos.

1. Del ejemplo 1.1.16 se tiene que la tabla de números de Betti de S/I es:

$j\backslash i$	0	1	2	3
0	1	0	0	0
1	0	4	4	1

2. Sea $I = (x^2, xy, y^2)$ un ideal de $S := \mathbb{K}[x, y]$. La resolución libre minimal de S/I tiene la forma:

   $0 \to S(-3)^2 \to S(-2)^3 \to S \longrightarrow S/(x^2, xy, y^2) \longrightarrow 0$ y la tabla de números de Betti:

$j\backslash i$	0	1	2
0	1	0	0
1	0	3	2

3. Sea (x^2, y^2, z^2) un ideal de $S := \mathbb{K}[x, y, z]$. La resolución libre minimal de S/I tiene la forma

   $0 \to S(-6) \to S(-4)^3 \to S(-2)^3 \to S \to S/(x^2, y^2, z^2) \to 0$ y la tabla de los números de Betti se ve de la siguiente forma.

$j\backslash i$	0	1	2	3
0	1	0	0	0
1	0	3	0	0
2	0	0	3	0
3	0	0	0	1

4. Sea $I = (x^2, yz, y)$ un ideal de $S := \mathbb{K}[x, y, z]$. La resolución libre minimal de S/I es de la forma

   $0 \to S(-3) \to S(-2) \oplus S(-1) \to S \longrightarrow S/(x^2, yz, y) \longrightarrow 0$ y la tabla de números de Betti:

$j\backslash i$	0	1	2
0	1	1	0
1	0	1	1

   Los números de Betti totales son: $\beta_0 = 1, \beta_1 = 2$ y $\beta_2 = 1$.

Las tablas de los números de Betti de los ideales de los ejemplos 2, 3 y 4 fueron calculadas usando Macaulay2 ([11]). □

1.2.4 Proposición. *Sean S un anillo G-multigraduado cuasi-positivo y M un R-módulo graduado finitamente generado. Entonces* $\beta_{i,\alpha}(\mathrm{Syz_j(M)}) = \beta_{\mathrm{i+j},\alpha}(\mathrm{M})$.

Demostración. Sea $\mathcal{F}$ una resolución libre minimal de M

$$\mathcal{F} : 0 \longrightarrow F_r \xrightarrow{\partial_r} F_{r-1} \longrightarrow \cdots \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0,$$

por definición $\mathrm{Syz_j(M)} = \ker(\partial_\mathrm{j}) = \partial_{\mathrm{j+1}}(\mathrm{F_{j+1}})$, así

$$\beta_{i,\alpha}(\mathrm{Syz_j(M)}) = \beta_{\mathrm{i,\alpha}}(\partial_{\mathrm{j+1}}(\mathrm{F_{j+1}})) = \beta_{\mathrm{i+j},\alpha}(\mathrm{M}).$$

■

1.2.5 Observación. De la proposición 1.2.4 se sigue que si I es un ideal de S, entonces $\beta_{i,\alpha}(I) = \beta_{i+1,\alpha}(S/I)$ pues $Syz_1(S/I) = I$.

La definición 1.2.6 y el teorema 1.2.8 se presentan en esta sección, serán de utilidad para determinar resultados en la sección 2.3.

1.2.6 Definición. Sean S con la graduación estándar e $I \subset S$ un ideal homogéneo. Una **resolución pura** de tipo $(d_1, d_2, \ldots, d_s)$ para S/I, es aquella en la que la resolución libre minimal $\mathcal{F}$ es de la forma

$$\mathcal{F} : 0 \to S(-d_s)^{\beta_s} \to \cdots \to S(-d_2)^{\beta_2} \to S(-d_1)^{\beta_1} \to S \to S/I.$$

Notemos que $d_1 < d_2 < \cdots < d_s$.

Recordemos que la dimensión de un R-Módulo M es $\dim(M) = \dim(R/\text{ann}(M))$.

1.2.7 Definición. Sean $S := \mathbb{K}[x_1, \ldots, x_n]$ y M un S-módulo. Decimos que M es **Cohen-Macaulay** si, y solo si, $\text{dimproj}(M) = n - \dim(M) =: \text{codim}(M)$.

1.2.8 Teorema. ([6, Teorema 4.1.15]) *Sea $S = [x_1, \ldots, x_n]$ G-multigraduado cuasi-positivo e I un ideal homogéneo. Si S/I es Cohen-Macaulay y este tiene una resolución pura del tipo $(d_1, \ldots, d_p)$, entonces $\beta_i = (-1)^{i+1} \prod_{j \neq i} \frac{d_j}{d_j - d_i}$.* ∎

1.3. Ideales monomiales y complejos simpliciales

En la presente sección se muestra la teoría necesaria (ver [12, capítulo 1] y [22, 1.3]) para comprender la fórmula de Hochster 1.3.29, esta fórmula nos permitirá obtener los números de Betti del ideal de Stanley-Reisner del complejo de independencia de una matroide, dicho resultado se encuentra en la sección 1.4. Además vamos a suponer algunos conocimientos acerca de ideales primos los cuales se pueden consultar en [21, capítulo 2].

Denotemos como M.C.D Y M.C.M a el minímo comun múltiplo y el máximo común divisor de dos o más números naturales, respectivamente. También denotemos como $\text{Mon}(S)$ al conjunto de monomios de $S = \mathbb{K}[x_1, \ldots, x_n]$. Como el conjunto $\text{Mon}(S)$ es una $\mathbb{K}$-base para S, para cada $f \in S$, $f = \sum_{u \in \text{Mon(s)}} a_u u$ con $a_u \in \mathbb{K}$. Llamemos a $\text{Supp}(f) := \{u \in \text{Mon}(S) \mid a_u \neq 0\}$, el **soporte** de f.

Un ideal $I \subset S$ es llamado **ideal monomial** si existe un conjunto generador de monomios para I (consultar [12] y [22] para más detalles de esta sección).

1.3.1 Proposición. *Sea I un ideal monomial. El conjunto N de monomios que pertenecen a I, forman una $\mathbb{K}$-base de I.*

Demostración. Los elementos de N son linealmente independientes, puesto que N es un subconjunto del $\text{Mon}(S)$. Sea $f \in I$ arbitrario; basta demostrar que $\text{Supp}(f) \subset N$, porque así N será un sistema de generadores para el $\mathbb{K}$-espacio vectorial I. Dado que $f \in I$, existen monomios $u_1, \ldots, u_m \in I$ y polinomios $f_1, f_2, \ldots, f_m \in S$ tales que $f = \sum_{i=1}^m f_i u_i$; por lo cual se tiene que $\text{Supp}(f) \subset \cup_{i=1}^m \text{Supp}(f_i u_i)$. Dado que para cada $v \in \text{Supp}(f_i u_i)$ es de la forma $w u_i$ con $w \in \text{Mon}(S)$; $\text{Supp}(f_i u_i) \subset N$ para todo $i \in [m]$. Así concluimos que $\text{Supp}(f) \subset N$. ∎

1.3.2 Corolario. *Sea $I \subset S$ un ideal, las siguientes condiciones son equivalentes:*

a) I es un ideal monomial.

b) Para cada $f \in S$ se tiene que, $f \in I$ si, y solo si, $\text{Supp}(f) \subset I$.

Demostración.

$a) \Rightarrow b)$ Supongamos que $f \in I$. Entonces por la demostración de la proposición 1.3.1, se tiene que $\text{Supp}(f) \subset I$.

$b) \Rightarrow a)$ Como S es noetheriano existe un conjunto generador $\{f_1, \ldots, f_m\}$. Dado que $\text{Supp}(f_i) \subset I$ para cada $i \in [m]$, entonces $\cup_{i=1}^m \text{Supp}(f_i)$ forman un conjunto generador para I. ∎

1.3.3 Proposición. *Sea $I \subset S$ un ideal monomial. Entonces existe $\{u_1, \ldots, u_s\} \subset \text{Mon}(S)$ finito que genera a I.*

Demostración. Dado que S es noetheriano (teorema de la base de Hilbert), I es finitamente generado. Entonces existen $p_1, \ldots, p_r \in I$ tales que $I = (p_1, \ldots, p_r)$; además cada $p_i = \sum_{j \in J_i} a_j x^{\alpha_j}$ con $x^{\alpha_j} \in \text{Mon}(S)$ y J_i un conjunto finito, así $\text{Supp}(p_i) = \{x^{\alpha_j} : j \in J_i\}$. Como I es monomial, $\text{Supp}(p_i) \subset I$. Así $G := \cup_{i=1}^r \text{Supp}(p_i) \subset I$; además $G \subset \text{Mon}(S)$, G es finito y $(G) \subset I$, como $p_i \in G$, entonces $I = (p_i)_{i=1}^r \subset (G)$. Por lo tanto, concluímos que $(G) = I$.

1.3.4 Proposición. *Sea $\{u_1, \ldots, u_m\}$ un sistema monomial de generadores del ideal monomial I. Entonces el monomio $v \in I$ si, y solo si, existe un monomio w tal que $v = wu_i$ para algún i.*

Demostración. Supongamos que $v \in I$ entonces existen polinomios $f_i \in S$ tal que $v = \sum_{i=1}^m f_i u_i$ y además $v \in \cup_{i=1}^m \text{Supp}(f_i u_i)$, es decir, $v \in \text{Supp}(f_i u_i)$ para algún $i \in [m]$. Lo que implica que $v = wu_i$ para algún $w \in \text{Supp}(f_i)$. El recíproco de la proposición 1.3.4 se sigue directamente. ∎

1.3.5 Proposición. *Cada ideal monomial tiene un único conjunto minimal de generadores monomiales.*

Demostración. Sean $G_1 = \{u_1, \ldots, u_p\}$ y $G_2 = \{v_1, \ldots, v_q\}$ conjuntos minimales de generadores monomiales del ideal I. Dado que $u_i \in I$, existe v_j tal que $u_i = w_1 v_j$ para algún monomio w_1. De manera similar, existe u_k y algún monomio w_2 tal que $v_j = w_2 u_k$. Se sigue que $u_i = w_1 w_2 u_k$. Dado que G_1 es un conjunto minimal de generadores monomiales de I, se tiene que $k = i$ y $w_1 w_2 = 1$. En particular $w_1 = 1$ y $u_i = v_j \in G_2$, por lo tanto $G_1 \subset G_2$. De manera similar se demuestra que $G_2 \subset G_1$. ∎

Notación: Al conjunto minimal único de generadores monomiales de I, lo denotaremos por $G(I)$.

1.3.6 Definición. Una presentación de un ideal I como una intersección de ideales, $I = \cap_{i=1}^m Q_i$, es llamada **irredundante** si ninguno de los ideales Q_i se puede omitir en esta presentación. Usamos el término **potencias puras** para describir a los monomios de la forma x_i^r.

1.3.7 Proposición. *Sea $I \subset S$ un ideal monomial. Entonces $I = \cap_{i=1}^m Q_i$, donde cada Q_i es generado por potencias puras de las variables, i.e, cada $Q_i = (x_{i_1}^{a_1}, x_{i_2}^{a_2}, \ldots, x_{i_k}^{a_k})$, más aún, cada representación irredundante de esta forma es única.*

Demostración. Sea $G(I) = \{u_1, \ldots, u_n\}$ y supóngase que algún u_i no es una potencia pura, digamos u_1, entonces podemos escribir $u_1 = vw$ donde v y w son monomios coprimos, i.e,

M.C.D$(v, w) = 1$ y $v \neq 1$ y $w \neq 1$.

Afirmación: $I = I_1 \cap I_2$, donde $I_1 = (v, u_2, \ldots, u_n)$ e $I_2 = (w, u_2, \ldots, u_n)$.

Se tiene que I esta contenida en la intersección. Recíprocamente, sea u un monomio en $I_1 \cap I_2$, si u es un múltiplo de algún u_i entonces $u \in I$. Si esto no ocurre, entonces u es múltiplo de v y w, y por lo tanto de u_1, puesto que u y v son coprimos. En cualquiera de los dos casos $u \in I$. Si algún $G(I_1)$ o $G(I_2)$ contiene un elemento, el cual no es una potencia pura, se procede como antes para obtener después de un número finito de pasos, una presentación de I como una intersección de ideales monomiales generados por potencias puras. Al omitir aquellos ideales que contienen la intersección de los otros, terminamos con una intersección irredundante.

Sean $Q_1 \cap \cdots \cap Q_r = Q_1' \cap \cdots \cap Q_s'$ dos intersecciones irredundantes de ideales generados por potencias puras e $i \in [r]$. Supongamos que $Q_i = (x_{i1}^{a_1}, \ldots, x_{i_k}^{a_k})$ y que $Q_j' \not\subset Q_i$ para cada $j \in [s]$. Entonces para cada j existe $x_{l_j}^{b_j} \in Q_j' - Q_i$. Se tiene así dos casos: $l_j \notin \{i_1, \ldots, i_k\}$ o bien $b_j < a_{l_j}$. Sea $u = \text{M.C.M}\{x_{l_1}^{b_1}, \ldots, x_{l_s}^{b_s}\}$. Entonces $u \in \cap_{j=1}^s Q_j' \subset Q_i$. Por lo tanto existe $i \in \{i_1, \ldots, i_k\}$ tal que $x_i^{a_i}$ divide a algún $x_{l_j}^{b_j}$, lo cual no es posible, así $Q_j' \subset Q_i$. Análogamente se demuestra que $Q_i \subset Q_j'$. Entonces $\{Q_1, \ldots, Q_r\} = \{Q_1', \ldots Q_s'\}$. ∎

1.3.8 Ejemplo. Sea $I = (x_1^2x_2, x_1^2x_3^2, x_2^2, x_2x_3^2)$ un ideal monomial y su descomposición irredundante es de la forma:

$$\begin{aligned}
I &= (x_1^2, x_1^2x_3^2, x_2^2, x_2x_3^2) \cap (x_2, x_1^2x_3^2, x_2^2, x_2x_3^2) \\
&= (x_1^2, x_1^2, x_2^2, x_2x_3^2) \cap (x_1^2, x_3^2, x_2^2, x_2x_3^2) \cap (x_2, x_1^2x_3^2, x_2x_3^2) \\
&= (x_1^2, x_1^2, x_2^2, x_2x_3^2) \cap (x_1^2, x_3^2, x_2^2, x_2x_3^2) \cap (x_2, x_1^2x_3^2, x_2) \cap (x_2, x_1x_3^2, x_3^2) \\
&= (x_1^2, x_2^2, x_2x_3^2) \cap (x_2, x_1^2x_3^2) \\
&= (x_1^2, x_2^2, x_2) \cap (x_1^2, x_2^2, x_3^2) \cap (x_2, x_1^2x_3^2) \\
&= (x_1^2, x_2^2, x_2) \cap (x_1^2, x_2^2, x_3^2) \cap (x_2, x_1^2) \cap (x_2, x_3^2) \\
&= (x_1^2, x_2) \cap (x_1^2, x_2^2, x_3^2) \cap (x_2, x_1^2) \cap (x_2, x_3^2) \\
&= (x_1^2, x_2^2, x_3^2) \cap (x_1^2, x_2) \cap (x_2, x_3^2).
\end{aligned}$$ □

Un ideal monomial que no se puede escribir como la intersección propia de dos ideales monomiales es llamado **irreducible**.

1.3.9 Corolario. *Un ideal monomial I es irreducible si, y solo si, es generado por potencias puras de las variables.*

Demostración.

⇐) Supongamos que $I = (x_{i1}^{a_1}, \ldots, x_{i_k}^{a_k})$ e $I = J_1 \cap J_2$, donde J_1 y J_2 son ideales monomiales que están propiamente contenidos en I. De la proposición 1.3.7, se tiene que $J_1 = \cap_{i=1}^r Q_i$ y $J_2 = \cap_{j=1}^s Q_j'$ para cada Q_i y Q_j' que son generados por potencias puras de las variables. Entonces se tiene la siguiente presentación de I:

$$I = (\cap_{i=1}^r Q_i) \cap (\cap_{j=1}^s Q_j').$$

De la unicidad de la presentación irredundante para I, entonces $I = Q_i$ o $I = Q_j'$ para algún i o j, lo cual es una contradicción.

⇒) Si $G(I)$ contiene un monomio $u = vw$ con M.C.D$(w, v) = 1$ y $v \neq 1 \neq w$, entonces por la demostración de 1.3.7, I se puede escribir como la intersección propia de dos ideales monomiales, donde v es un generador de uno y w es un generador del otro; así I es no irreducible. ∎

Sea $I \subset S$ un ideal. Recordemos que el **radical** de I es

$$\sqrt{I} := \{f \in S : f^k \in I \text{ para algún } k > 0\}.$$

1.3.10 Observación. La proposición 1.3.7 junto con el corolario 1.3.9 hacen concluir que cada ideal monomial tiene una única presentación como una intersección irredundante de ideales monomiales irreducibles. Más aún de la proposición 1.3.13 podremos concluir que la presentación como intersección irredundante de ideales irreducibles es una presentación de ideales primarios, cuya definición se encuentra en 1.3.12. Antes de demostrar la proposición 1.3.13 vamos a demostrar el siguiente resultado:

1.3.11 Lema. *Si I es un ideal monomial, entonces $\sqrt{I}$ es un ideal monomial.*

Demostración. Sea $f \in \sqrt{I}$, entonces existe $k \in \mathbb{N}$ tal que $f^k \in I$ y por el corolario 1.3.2, Supp$(f^k) \subset I$. Digamos que Supp$(f) = \{x^{a_1}, \ldots, x^{a_s}\}$, la envoltura convexa de $\{a_1, \ldots, a_s\}$ es un politopo en $\mathbb{R}^n$. Podemos asumir que a_1 es un vértice del politopo, es decir, a_1 no está en la envoltura convexa de $\{a_2, \ldots, a_s\}$. Supongamos que $(x^{a_1})^k = (x^{a_1})^{k_1}(x^{a_2})^{k_2} \cdots (x^{a_s})^{k_s}$ con $k = k_1 + k_2 + \cdots + k_s$ y $k_1 < k$. Entonces $a_1 k = a_1 k_1 + a_2 k_2 + \cdots + a_s k_s$,

$$a_1 k - a_1 k_1 = a_2 k_2 + \cdots + a_s k_s,$$

por lo tanto, $a_1 = \frac{a_2 k_2 + \cdots + a_s k_s}{k - k_1} = \sum_{i=2}^{s} \frac{k_i}{k-k_1} a_i$ con $\sum_{i=2}^{s} \frac{k_i}{k-k_1} = 1$. Entonces a_1 no es un vértice, lo cual es una contradicción. Así que $(x^{a_1})^k$ no se cancela con los otros términos de f^k y por lo tanto $(x^{a_1})^k \in$ Supp$(f^k) \subset I$, y por el corolario 1.3.2 se tiene que $x^{a_1} \in \sqrt{I}$. Como el Supp$(f) = \{x^{a_1}, \ldots, x^{a_s}\}$, existen $c_1, \ldots c_s \in \mathbb{K}$, tal que $f = c_1 x^{a_1} + \cdots + c_s x^{a_s}$. Como $f - c_1 x^{a_1} \in \sqrt{I}$, se tiene que Supp$(f - c_1 x^{a_1}) = \{x^{a_2}, \ldots, x^{a_s}\}$. Por un razonamiento similar podemos asumir la envoltura convexa de $\{a_2, \ldots, a_s\}$ es un politopo y a_2 es un vértice de politopo; y así $x^{a_2} \in \sqrt{I}$. Por lo tanto $f - c_1 x^{a_1} - c_2 x^{a_2} \in \sqrt{I}$. Entonces recursivamente tenemos que Supp$(f) \subset \sqrt{I}$; y por el corolario 1.3.2 tenemos que $\sqrt{I}$ es un ideal monomial. ∎

1.3.12 Definición. Sean R un anilo, $x, y \in R$ e $I \subset R$ un ideal de R. Recordemos que I es un **ideal primario** de R si $xy \in I$ entonces $x \in I$ o bien $y^n \in I$ para algún $n \in \mathbb{N}$.

1.3.13 Proposición. *Sea $I = (x_{i_1}^{a_{i_1}}, \ldots, x_{i_k}^{a_{i_k}}) \subset S$ un ideal generado por potencias puras. Entonces I es $(x_{i_1}, \ldots, x_{i_k})$-primario.*

Demostración. Del corolario 1.3.2 para mostrar que I es primario basta demostrar que si $m_1, m_2 \in$ Mon(S), $m_1 m_2 \in I$ y $m_1 \notin I$, entonces existe $s \in \mathbb{N}$ tal que $m_2^s \in I$. Sean $m_1, m_2 \in$ Mon(S) tales que $m_1 m_2 \in I$ y $m_1 \notin I$; por lo tanto existe i_j tal que existe

$u \in \text{Mon}(S)$ y $m_1 m_2 = x_{i_j}^{a_{i_j}} u$. Pero $m_1 \notin I$, entonces $x_{i_j}^{a^{i_j}} \not| m_1$; y así $x_{i_j} | m_2$. Sea $b \in \mathbb{N}$ la potencia máxima de x_{i_j} en m_2, es decir, existe $u' \in \text{Mon}(S)$ tal que x_{i_j}, u' son primos relativos, y $m_2 = x_{i_j}^b u'$. Así, sea d el mínimo común múltiplo de b y a_{i_j}, entonces $m_2^d = (x_{i_j}^b \cdot v')^d = x_{i_j}^{db} v'$ pero $x_i^{a_{i_j}} | x_{i_j}^{db}$, de lo cual $x_{i_j}^{a_{i_j}} | m_2^d$; y así $m_2^d \in I$.

Ahora bien, notemos que $(x_{i_1}, \ldots, x_{i_k}) \subset \sqrt{I}$. Por otro lado, dado que $\sqrt{I}$ es un ideal monomial por el lema 1.3.11, del corolario 1.3.2 basta mostrar que cada monomio $v \in \sqrt{I}$ es múltiplo de algún x_{i_j}. Sea $v \in \sqrt{I}$, entonces existe $n \in \mathbb{N}$ tal que $v^n \in I$, así que para algún $x_{i_j}^{a_{i_j}}$ y $w \in \text{Mon}(S)$ se tiene que $v^n = x_{i_j}^{a_{i_j}} w$. Entonces $\sqrt{(x_{i_1}^{a_{i_1}}, \ldots, x_{i_k}^{a_{i_k}})} = (x_{i_1}, \ldots, x_{i_k})$.

1.3.14 Definición. Un monomio x^a es **libre de cuadrados** si cada entrada de a es 0 o bien 1; así diremos que el vector $a \in \mathbb{N}^n$ es libre de cuadrados. Un ideal monomial I se dice **ideal monomial libre de cuadrados** si existe un conjunto generador de monomios libres de cuadrados para I.

Si I es un ideal monomial libre de cuadrados, el procedimiento del teorema 1.3.7 nos dice que los ideales monomiales irreducibles que aparecen en la intersección de I son de la forma $(x_{i_1}, \ldots, x_{i_k})$. Además observemos que los ideales monomiales primos en S son de la forma $(x_{i_1}, \ldots, x_{i_k})$. Así, los ideales primos asociados de I tienen la forma $(x_{i_1}, \ldots, x_{i_k})$; y como la descomposición de I obtenida por el teorema 1.3.7 es una descomposición primaria, todos los primos asociados son minimales. Por otro lado, de álgebra conmutativa sabemos que el conjunto de ideales minimales primos de I, denotado por $\text{Min}(I)$, está contenido en $\text{Ass}(I)$, donde $\text{Ass}(I)$ denota al conjunto de los primos asociados. Entonces:

1.3.15 Corolario. *Sea I un ideal monomial. Así I es un ideal monomial libre de cuadrados si, y solo si, $I = \bigcap_{P \in Min(I)} P$, además cada P es de la forma $(x_{i_1}, \ldots, x_{i_k})$.*

1.3.16 Definición. Decimos que la pareja $\Gamma := (E, \Delta)$ es un **complejo simplicial** (abstracto) si E es un conjunto finito y Δ es una familia de subconjuntos de E, tal que Δ satisface que si $F \in \Delta$ y $G \subset F$ entonces $G \in \Delta$, es decir, la familia de conjuntos Δ es cerrada bajo contención.

En la definición anterior como E es finito podemos pensar que E es igual a $[|E|] := \{1, \ldots, |E|\}$. Además, en este trabajo denotaremos al complejo simplicial por su familia de conjuntos Δ y obviaremos E por el contexto. Denotaremos como el conjunto potencia de E como $\mathcal{P}(E)$, así $\Delta \subset \mathcal{P}(E)$.

Sean Δ un complejo simplicial en E y $i \in [|E|]$. Un conjunto $\sigma \in \Delta$ se llama **simplejo** o **cara** de Δ. Si su cardinalidad es $i+1$ decimos que σ tiene dimensión i, la cual denotaremos por $\dim(\sigma) = \text{i}$. Si $\Delta \neq \emptyset$, la dimensión de Δ será la máxima de las dimensiones de sus simplejos, en caso contrario diremos que Δ es de dimensión $-\infty$. Un **vértice** de Δ es un simplejo de dimensión 0 y al conjunto de vértices lo denotaremos como $V(\Delta)$. Una **careta** es un simplejo maximal de Δ (respecto a la contención de conjuntos). Denotamos por $F(\Delta)$ al conjunto de las caretas de Δ. Como cualquier complejo simplicial Δ es cerrado bajo contención, si $F \in F(\Delta)$, entonces para cualquier $G \subset F$, $G \in \Delta$. De esta forma basta conocer de Δ a su conjunto de caretas $F(\Delta)$, y en este caso diremos que Δ está generado por $F(\Delta)$;

escribiendo así $\Delta = (F \in F(\Delta))$. Un complejo simplicial Δ es **puro** si todas sus caretas tienen la misma dimensión.

Sea Δ un complejo simplicial, una **no cara** de Δ es un subconjunto F de $\mathcal{P}(E)$ tal que F no pertenece a Δ. Definamos a $N(\Delta)$ como el conjunto minimal de no caras de Δ. Denotaremos como $f_i := f_i(\Delta)$ al número de simplejos o caras de Δ de dimensión $i-1$. Digamos que $d := \dim(\Delta)+1$, así, el polinomio $f_\Delta(t) := t^d + f_1 t^{d-1} + \cdots + f_d$ es llamado el **f-polinomio** de Δ. Definimos la **característica de Euler** (reducida) de un complejo simplicial Δ como $\widetilde{\chi}(\Delta) := (-1)^{d-1} f_\Delta(-1)$; notemos que:

$$\begin{aligned}\widetilde{\chi}(\Delta) := (-1)^{d-1} f_\Delta(-1) &= (-1)^{d-1}((-1)^d + f_1(-1)^{d-1} + \cdots + f_d) \\ &= (-1)^{2d-1} + f_1(-1)^{2d-2} + f_2(-1)^{2d-3} + \cdots + (-1)^{d-1} f_d. \\ &= -1 + f_1 - f_2 + \cdots + (-1)^{d-1} f_d.\end{aligned}$$

1.3.17 Ejemplo. El complejo simplicial $\Delta \subseteq \mathcal{P}([5])$ definido por

$$\Delta := (\{1,3\},\{2,4\},\{1,2,5\},\{3,4,5\}),$$

cuya realización geométrica (ver [23], capítulo 1) se puede observar en la figura 1.1.

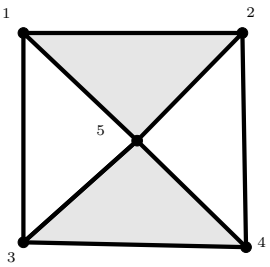

Figura 1.1: Realización geométrica de Δ.

Así, $F(\Delta) = \{\{1,3\},\{2,4\},\{1,2,5\},\{3,4,5\}\}$; $N(\Delta) = \{\{1,4\},\{2,3\},\{1,3,5\},\{2,4,5\}\}$; $f_\Delta(t) = t^3 + 5t^2 + 8t + 2$; $d = 3$ y $\widetilde{\chi}(\Delta) = (-1)^2(-1+5-8+2) = -2$. □

Sea Δ un complejo simplicial y $T \subseteq V(\Delta)$, definamos el complejo simplicial **inducido** por S como $\Delta|T := \{\sigma \subseteq T : \sigma \in \Delta\}$ y el **borrado** de un vértice $\{v\}$ del complejo simplicial Δ como $\Delta \setminus v := \Delta|(V(\Delta) - v)$.

Un complejo simplicial Δ es un **cono** si existe $v \in V(\Delta)$ tal que para cada $F \in F(\Delta)$, $v \in F$. Por otro lado, dado un complejo simplicial Δ y $v \notin \Delta$, definamos la **conificación** de Δ como $\Delta * \{v\} := \Delta \cup \{F \cup v : F \in \Delta\}$; el cual podemos ver que es un cono.

1.3.18 Proposición. *Sean Δ un complejo simplicial y $d := \dim(\Delta)+1$. Si Δ es un cono, entonces se tiene que $\widetilde{\chi}(\Delta) = 0$.*

Demostración. Dado que Δ es un cono existe $v \in V(\Delta)$ tal que $\Delta = \Delta' * v$, donde $\Delta' = \Delta \setminus v$. Ahora bien, $f_{\Delta'}(t) = t^d + f_1' t^{d-1} + \cdots + f_d$ y $f_\Delta(t) = t^d + (1+f_1')t^{d-1} + (f_1' + f_2')t^{d-2} + \cdots + f_d$, por lo que $\widetilde{\chi}(\Delta) = -1 + (1+f_1') - (f_1' + f_2') + (f_2' + f_3') - \cdots + (-1)^{d-1}(f_d) = 0$. ∎

1.3.19 Ejemplos.

1. Sea $\Delta \subseteq \mathcal{P}([4])$ el complejo simplicial definido por

$$\Delta := (\{1,2,3\},\{1,3,4\}).$$

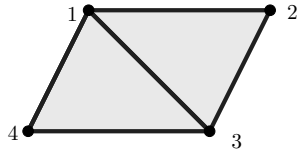

Figura 1.2: Realización geométrica de Δ.

Notemos que Δ es un cono donde $v = \{1\}$ ó $v = \{3\}$. Así $F(\Delta) = \{\{1,2,3\},\{1,3,4\}\}$; $f_\Delta(t) = t^3 + 4t^2 + 5t + 2$; $d = 3$ y $\widetilde{\chi}(\Delta) = (-1)^2(-1+4-5+2) = 0$.

2. Sea $\Delta_1 \subset \mathcal{P}([6])$ el complejo simplicial definido por

$$\Delta_1 := (\{1,2,3\},\{2,3,4\},\{4,5,6\}).$$

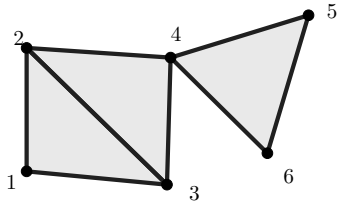

Figura 1.3: Realización geométrica de Δ.

Notemos que Δ_1 no es un cono. Así $F(\Delta_1) = \{\{1,2,3\},\{2,3,4\},\{4,5,6\}\}$; $f_{\Delta_1}(t) = t^3+6t^2+8t+3$; $d = 3$ y $\widetilde{\chi}(\Delta_1) = (-1)^2(-1+6-8+3) = 0$. □

Recordemos que cada monomio x^a en el anillo $S := \mathbb{K}[x_1, x_2, \ldots, x_n]$ se ve como $x^a = x_1^{a_1} \cdots x_n^{a_n}$, con $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$. Definamos para cada $\sigma \subset [n]$ la función $\text{vec} : \mathcal{P}([\text{n}]) \to \{0,1\}^{\text{n}}$ tal que $\text{vec}(\sigma) = (a_1^{(\sigma)}, \ldots, a_n^{(\sigma)})$ y

$$a_i^{(\sigma)} = \begin{cases} 0 & \text{si } i \notin \sigma; \\ 1 & \text{si i} \in \sigma, \end{cases}$$

de esta manera $x^\sigma := x^{\text{vec}(\sigma)} = \prod_{i\in\sigma} x_i$.

1.3.20 Definición. El **ideal de Stanley-Reisner** del complejo simplicial Δ es el ideal monomial libre de cuadrados generado por los monomios x^σ tal que σ es una no cara, esto es, $I_\Delta := (x^\sigma : \sigma \subset [n], \sigma \notin \Delta)$. **El anillo de Stanley-Reisner** de Δ es el anillo cociente S/I_Δ.

Observemos que dado un complejo simplicial Δ, si $\tau \notin \Delta$; entonces existe $\sigma \in N(\Delta)$ tal que $\sigma \subset \tau$ y así $x^\sigma | x^\tau$, entonces $I_\Delta = (x^\tau : \tau \in N(\Delta))$.

Sea $\rho \subseteq \mathcal{P}([n])$, denotemos como $\mathfrak{m}^\rho := (x_i \mid i \in \rho)$ al **ideal monomial primo correspondiente a** ρ . Además denotaremos por $\overline{\rho}$ al complemento de ρ sobre $[n]$, es decir, $\overline{\rho} := [n] - \rho$.

1.3.21 Proposición. *Sea Δ un complejo simplicial. Entonces la descomposición primaria de I_Δ está dada por $I_\Delta = \cap_{\sigma\in F(\Delta)}\mathfrak{m}^{\overline{\sigma}}$.*

Demostración. Como I_Δ es un ideal monomial libre de cuadrados y por el corolario 1.3.15 $\cap_{\sigma\in F(\Delta)}\mathfrak{m}^{\overline{\sigma}}$ también es un ideal monomial libre de cuadrados, entonces para demostrar que I_Δ y $\cap_{\sigma\in F(\Delta)}\mathfrak{m}^{\overline{\sigma}}$ son iguales hay que ver que contienen a los mismos monomios libres de cuadrados. Así pues, sea $F \subset [n]$, $x^F \in \cap_{\sigma\in F(\Delta)}\mathfrak{m}^{\overline{\sigma}}$ si, y solo si, $x^F \in \mathfrak{m}^{\overline{\sigma}}$ para toda $\sigma \in F(\Delta)$ si, y solo si, para toda $\sigma \in F(\Delta)$, existe $j_\sigma \in \overline{\sigma}$ tal que $j_\sigma \in F$ si, y solo si, para toda $\sigma \in F(\Delta)$, $F \not\subset \sigma$ si, y solo si, F es no cara. De aquí que $\cap_{\sigma\in F(\Delta)}\mathfrak{m}^{\overline{\sigma}} = I_\Delta$. ∎

1.3.22 Teorema. *Sea Δ un complejo simplicial. La correspondencia $\Delta \rightsquigarrow I_\Delta$ es una biyección.*

Demostración. Como $I_\Delta = (x^\sigma : \sigma \in N(\Delta))$, la correspondencia es inyectiva. Por otro lado, sea I un ideal monomial libre de cuadrados en $\mathbb{K}[x_1, \ldots, x_n]$, el cual por el corolario 1.3.15 se tiene que $I = \cap_{\sigma\subset[n], m^\sigma\in \mathrm{Min}(I)} m^\sigma$. Definamos $\Delta = (\overline{\sigma} : \mathfrak{m}^\sigma$ aparece en la descomposición primaria de $I)$. ∎

1.3.23 Ejemplo. Del complejo simplicial del ejemplo 1.3.17 tenemos que su ideal de Stanley-Reisner es $I_\Delta = (x_1x_4, x_2x_3, x_1x_3x_5, x_2x_4x_5) = (x_2x_4x_5)\cap(x_1x_3x_5)\cap(x_3x_4)\cap(x_1x_2)$. □

Recordemos que la altura de un ideal primo $\mathfrak{p} \subset R$, denotada por $\mathrm{ht}(\mathfrak{p})$, se define como $\mathrm{ht}(\mathfrak{p}) = \sup\{r : \text{existe una cadena } \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p} \text{ en } R\}$. También recordemos que $\mathcal{V}(I) = \{\mathfrak{p} \in \mathrm{Spec}(I) : I \subset \mathfrak{p}\}$ y la **altura** de un ideal $I \subset R$ es $\mathrm{ht}(I) = \text{ínf}\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \in \mathcal{V}(I)\}$.

1.3.24 Proposición. *Sea Δ un complejo simplicial. Entonces* $\dim(S/I_\Delta) = \dim(\Delta) + 1$.

Demostración. Recordemos que dado que S es un anillo graduado estándar regular, $\dim(S/I_\Delta) = \dim(S) - \mathrm{ht}(I_\Delta)$. Entonces,

$$\dim(S/I_\Delta) = \dim(S) - \mathrm{ht}(I_\Delta) = n - \text{mín}\{\mathrm{ht}(\mathfrak{p}) : \mathfrak{p} \in \mathcal{V}(I_\Delta)\} = n - \text{mín}\{\mathrm{ht}(\mathfrak{m}^{\overline{\sigma}}) : \sigma \in F(\Delta)\}.$$

Donde la última igualdad es por la descomposición primaria de I_Δ en la proposición 1.3.21. Ahora bien, si $\sigma = (i_1, \ldots, i_{|\sigma|})$ entonces $S/m^{\overline{\sigma}} \simeq \mathbb{K}[x_{i_1}, \ldots, x_{i_{|\sigma|}}]$; y así

$$\mathrm{ht}(\mathfrak{m}^{\overline{\sigma}}) = \dim(S) - \dim(S/\mathfrak{m}^{\overline{\sigma}}) = n - \dim(\mathbb{K}[x_{i_1}, \ldots, x_{i_{|\sigma|}}]) = n - |\sigma|, \text{ por lo tanto,}$$

$$\begin{aligned}\dim(S/I_\Delta) &= n - \text{mín}\{n - |\sigma| : \sigma \in F(\Delta)\}\\ &= n - (n + \text{mín}\{-|\sigma| : \sigma \in F(\Delta)\})\\ &= \text{máx}\{|\sigma| : \sigma \in F(\Delta)\}\\ &= \dim(\Delta) + 1.\end{aligned}$$

∎

Sean Δ un complejo simplicial sobre $[n]$ y $F_i(\Delta) := \{\sigma \in \Delta : \dim(\sigma) = i\}$ el conjunto de los simplejos de Δ de dimensión i. Definimos $\mathbb{K}^{F_i(\Delta)} := \oplus_{\sigma\in F_i(\Delta)}\mathbb{K}\cdot e_\sigma$. Observemos que $\mathbb{K}^{F_i(\Delta)} \simeq \mathbb{K}^{|F_i(\Delta)|}$.

1.3.25 Definición. Sean Δ un complejo simplicial, $d := \dim \Delta$ y $\mathbb{K}$ un campo cualquiera. Definamos $C.(\Delta, \mathbb{K})$ como la sucesión de morfismos (transformaciones lineales):

$$C.(\Delta, \mathbb{K}) : 0 \to \mathbb{K}^{F_d(\Delta)} \xrightarrow{\partial_d} \cdots \to \mathbb{K}^{F_i(\Delta)} \xrightarrow{\partial_i} \mathbb{K}^{F_{i-1}(\Delta)} \xrightarrow{\partial_{i-1}} \cdots \xrightarrow{\partial_0} \mathbb{K}^{F_{-1}(\Delta)} \to 0,$$

donde los morfismos ∂_i estan definidas como $\partial_i(e_\sigma) = \sum_{j\in\sigma} \mathrm{sign(j,\sigma)e_{\sigma-\{j\}}}$. Si $i < -1$ o $i > d$, entonces $\mathbb{K}^{F_i(\Delta)} = 0$ y $\partial_i = 0$. El $\mathrm{sign(j,\sigma)} = (-1)^{\mathrm{r-1}}$ si j es el r-ésimo elemento en $\sigma \subseteq [n]$ (donde σ está ordenado con el orden natural).

1.3.26 Proposición. *La sucesión de morfismos $C.(\Delta, \mathbb{K})$ es un complejo de cadena, i.e., $\partial_i \circ \partial_{i-1} = 0$.*

Demostración. Sea $\sigma \in \Delta$,

$$\begin{aligned}
\partial_i(\partial_{i-1}(e_\sigma)) &= \partial_i(\textstyle\sum_{j\in\sigma} \mathrm{sign(j,\sigma)e_{\sigma-j}}) \\
&= \textstyle\sum_{j\in\sigma} \mathrm{sign(j,\sigma)}\partial_{\mathrm{i}}(\mathrm{e_{\sigma-j}}) \\
&= \textstyle\sum_{j\in\sigma} \mathrm{sign(j,\sigma)}(\sum_{\mathrm{k}\in(\sigma-\mathrm{j})} \mathrm{sign(k,(\sigma-j))e_{(\sigma-j)-k}}) \\
&= \textstyle\sum_{j,k\in\sigma} (\mathrm{sign(j,\sigma)sign(k,\sigma-j)e_{(\sigma-j)-k}}.
\end{aligned}$$

Afirmación: Se tiene que $\mathrm{sign(j,\sigma)sign(k,\sigma-j)} = -\mathrm{sign(k,\sigma)sign(j,\sigma-k)}$.

Supongamos que $j < k$, entonces $\mathrm{sign(k,\sigma-j)} = -\mathrm{sign(k,\sigma)}$, pero $\mathrm{sign(j,\sigma)} = \mathrm{sign(j,\sigma-k)}$. Y así $\mathrm{sign(j,\sigma)sign(k,\sigma-j)} = -\mathrm{sign(k,\sigma)sign(j,\sigma-k)}$. De manera similar para cuando $j > k$ se tiene que $\mathrm{sign(j,\sigma)sign(k,\sigma-j)} = -\mathrm{sign(k,\sigma)sign(j,\sigma-k)}$. Entonces $\partial_i(\partial_{i-1}(e_\sigma)) = 0$. ∎

1.3.27 Definición. Sean Δ un complejo, $d := \dim \Delta$, $\mathbb{K}$ un campo cualquiera y

$$C.(\Delta, \mathbb{K}) : 0 \to \mathbb{K}^{F_d(\Delta)} \xrightarrow{\partial_d} \cdots \to \mathbb{K}^{F_i(\Delta)} \xrightarrow{\partial_i} \mathbb{K}^{F_{i-1}(\Delta)} \xrightarrow{\partial_{i-1}} \cdots \xrightarrow{\partial_0} \mathbb{K}^{F_{-1}(\Delta)} \to 0,$$

la **homología simplicial reducida** de grado i de Δ es el espacio vectorial sobre $\mathbb{K}$ definido por:

$$\widetilde{H}_i(\Delta, \mathbb{K}) = \ker(\partial_i)/\mathrm{im}(\partial_{i+1}).$$

1.3.28 Ejemplo. Consideremos el complejo simplicial $\Delta = (\{1,3\},\{2,4\},\{1,2,5\},\{3,4,5\})$.

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

Por lo tanto, $\partial_2(e_{\{1,2,5\}}) = e_{\{2,5\}} - e_{\{1,5\}} + e_{\{1,2\}}$, $\partial_1(e_{\{1,2\}}) = e_{\{2\}} - e_{\{1\}}$, de manera similar para los otros elementos. Así Δ tiene el siguiente complejo de cadena:

$$0 \to \mathbb{K}^2 \xrightarrow[\partial_2]{\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ -1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & -1 \\ 0 & 1 \end{pmatrix}} \mathbb{K}^8 \xrightarrow[\partial_1]{\begin{pmatrix} -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}} \mathbb{K}^5 \xrightarrow[\partial_0]{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}} \mathbb{K} \to 0.$$

Las matrices asociadas a los morfismos $\partial_2, \partial_1, \partial_0$ tienen rango 1,4,2 respectivamente, ∂_0 es inyectivo y ∂_2 es sobreyectivo. Entonces $\widetilde{H}_0 = \mathbb{K}^4/\mathbb{K}^4 \simeq 0$, $\widetilde{H}_1 = \mathbb{K}^4/\mathbb{K}^2 \simeq \mathbb{K}^2$ y los otros grupos de homología son cero. □

Antes de proceder al siguiente teorema definamos para cada $\sigma \in \{0,1\}^n$, $\text{conj}(\sigma) := \text{vec}^{-1}(\sigma)$. Además, cabe señalar que el siguiente teorema nos ayudará para calcular los números de Betti del ideal de Stanley-Reisner del complejo de independencia de una matroide (ver el teorema 1.4.30).

1.3.29 Teorema. (Fórmula de Hochster, [13]) *Sean $\Delta \subset \mathcal{P}([n])$ un complejo simplicial. Entonces el número de Betti multigraduado $\beta_{i,\sigma}$ de I_Δ es cero si σ no es libre de cuadrados, pero si σ es libre de cuadrados*

$$\beta_{i,\sigma}(I_\Delta) = \dim_{\mathbb{K}} \widetilde{\mathrm{H}}_{|\sigma|-\mathrm{i}-2}(\Delta|\text{conj}(\sigma), \mathbb{K}).$$

Así de la observación 1.2.5 obtenemos que $\beta_{i,\sigma}(S/I_\Delta) = \dim_{\mathrm{k}} \widetilde{\mathrm{H}}_{|\sigma|-\mathrm{i}-1}(\Delta|\text{conj}(\sigma), \mathbb{K})$. Entonces podemos ver que por la fórmula de Hochster (teorema 1.3.29):

$$\beta_{i,j}(S/I_\Delta) = \sum_{\substack{\sigma \in \{0,1\}^n, \\ |\sigma| = j}} \beta_{i,\sigma}(S/I_\Delta) = \sum_{\substack{\sigma \in \{0,1\}^n, \\ |\sigma| = j}} \dim_{\mathrm{k}} \widetilde{\mathrm{H}}_{|\sigma|-\mathrm{i}-1}(\Delta|\sigma, \mathbb{K}). \tag{1.5}$$

1.4. Matroides

En esta sección comenzaremos dando una breve introducción a la teoría de matroides las cuales se pueden consultar principalmente en el libro de Oxley, [24]). También algunas de las demostraciones de las siguientes proposiciones de matroides van a ser omitidas y pueden ser consultadas en dicho libro. Después de un resumen de la teoría de matroides, demostraremos el teorema 1.4.30, el cual calcula los números de Betti del ideal de Stanley-Reisner del complejo de independencia de una matroide. Dicho teorema aparece en el artículo de T. Johnsen y H. Verdure [15, teorema 1], el cual nosotros demostramos de manera diferente usando resultados básicos de Oxley [24] a diferencia que ellos lo hicieron a través de circuitos irredundantes. Nuestra manera de trabajar nos permitirá calcular los números de Betti en términos de la retícula de cerrados del matroide dual, que aparece en la tesis [2] y ahí es demostrado a partir del teorema de T. Johnsen y H. Verdure, pero nosotros mostramos que es independiente de dicho resultado.

Por abuso de notación, los conjuntos de un solo elemento $\{a\}$ (**singleton**) se denotarán por su elemento a.

1.4.1 Definición. Una **matroide** $\mathcal{M}$ es un par ordenado $\mathcal{M} = (E, \mathcal{I})$, con E un conjunto finito (llamado **conjunto subyacente**) e $\mathcal{I}$ un complejo simplicial no vacío sobre E, tal que se satisface la siguiente propiedad: si $I_1, I_2 \in \mathcal{I}$ y $|I_1| < |I_2|$, entonces existe $a \in I_2 - I_1$, tal que $I_1 \cup a \in \mathcal{I}$.

Los elementos de $\mathcal{I}$ son llamados los conjuntos **independientes** de $\mathcal{M}$ y a las caretas de $\mathcal{I}$ se les llama **bases** de $\mathcal{M}$. De esta forma, si $\mathcal{B}$ es el conjunto de bases de $\mathcal{M}$, entonces $\mathcal{I} = \langle B \in \mathcal{B} \rangle$. Además se demuestra en [24, lema 1.2.1] que todas las bases son equicardinales, por lo que $\mathcal{I}$ es un complejo simplicial puro.

1.4.2 Ejemplo. Sean $A \in M_{m\times n}(\mathbb{K})$, E el conjunto de etiquetas de las columnas de la matriz A e $\mathcal{I}$ la colección de subconjuntos de E tales que representan conjuntos de columnas linealmente independientes de A. Esta matroide es llamada la **matroide vector** de A y la denotaremos como $\mathcal{M}[A]$. Más adelante, en el ejemplo 1.4.11 se va presentar una matroide vector para una matriz específica. □

Sean $\mathcal{M} = (E, \mathcal{I})$ y $\mathcal{M}' = (E', \mathcal{I}')$ dos matroides. Un isomorfismo de $\mathcal{M}$ a $\mathcal{M}'$ es una función biyectiva $\varphi : E \to E'$ tal que:

1. Para cada $I \in \mathcal{I}$, $\varphi(I) \in \mathcal{I}'$.

2. Para cada $I' \in \mathcal{I}'$, $\varphi^{-1}(I') \in \mathcal{I}$.

Así, decimos que $\mathcal{M}$ y $\mathcal{M}'$ son **isomorfos** si existe un isomorfismo entre ellos.

1.4.3 Observación. Si la matroide $\mathcal{M}$ es isomorfa a la matroide vector de una matriz D sobre un campo $\mathbb{K}$, diremos que $\mathcal{M}$ es **representable sobre** $\mathbb{K}$. Es importante decir que dado un campo $\mathbb{K}$ no toda matroide es representable sobre $\mathbb{K}$ (ver [24, capítulo 6]).

1.4.4 Proposición. ([24, lema 1.2.1,]) *Sea $\mathcal{M}$ una matroide y $\mathcal{B}$ la colección de bases de $\mathcal{M}$. Entonces se satisface que:*

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

(B2) Sea $B_1, B_2 \in \mathcal{B}$ *y* $x \in B_1 - B_2$. *Entonces existe un elemento* $y \in B_2 - B_1$ *tal que* $(B_1 - x) \cup y \in \mathcal{B}$.

1.4.5 Proposición. ([24, corolario 1.2.5]) *Sea $\mathcal{B}$ la colección de subconjuntos de E. Entonces $\mathcal{B}$ es la colección de bases de una matroide en E si, y sólo si, se satisfacen $(B1)$ y $(B2)$.*

1.4.6 Definición. Sea $D \subset E$, si $D \notin \mathcal{I}$ entonces diremos que D es un conjunto **dependiente**. Un **circuito** es un conjunto dependiente minimal, i.e., sus subconjuntos propios son independientes. Además a la colección de circuitos de $\mathcal{M}$ la denotaremos como $\mathcal{C}(\mathcal{M})$ o simplemente $\mathcal{C}$, cuando no exista confusión sobre $\mathcal{M}$. Si $\{e\} \in \mathcal{C}$, se dice que e es un **lazo**.

1.4.7 Proposición. ([24, teorema 1.1.4]) *Sean E un conjunto, $\mathcal{C}$ una familia de subconjuntos de E tal que satisface:*

1. $\emptyset \notin \mathcal{C}$;

2. *Si* $C_1 \in \mathcal{C}$ *y* $C_2 \in \mathcal{C}$ *tales que* $C_1 \subseteq C_2$, *entonces* $C_1 = C_2$;

3. *Si* $C_1, C_2 \in \mathcal{C}$ *y* $e \in C_1 \cap C_2$, *entonces existe* $C_3 \in \mathcal{C}$ *tal que* $C_3 \subseteq (C_1 \cup C_2) - e$.

Sea $\mathcal{I}$ la familia de subconjuntos de E que no contienen ningún miembro de $\mathcal{C}$. Entonces $(E, \mathcal{I})$ es una matroide, cuya familia de circuitos es $\mathcal{C}$.

Sean $\mathcal{M} = (E, \mathcal{I})$ una matroide y $X \subseteq E$. **La matroide restricción** de $\mathcal{M}$ en X es el par $(X, \mathcal{I}|X)$. El cual lo vamos a denotar como $\mathcal{M}|X$. Como $\mathcal{M}|X$ es una matroide y dado que todas las bases son equicardinales, definimos el rango $r(X)$ de X como el tamaño de una base B de $\mathcal{M}|X$. La función $r : 2^E \to \mathbb{Z}^+ \cup \{0\}$, es llamada la **función rango** de $\mathcal{M}$; y así definimos el rango de $\mathcal{M}$ como el tamaño de una base de $\mathcal{M}$ y lo denotaremos por $r(\mathcal{M})$; además notemos que $r(\mathcal{M}) = r(E)$. La función r tiene las siguientes propiedades:

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

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

(R3) Si X y Y son subconjuntos de E, entonces $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

1.4.8 Proposición. ([24, teorema 1.3.2]) *Sean E un conjunto, $r : 2^E \to \mathbb{Z}^+ \cup \{0\}$ una función tal que se satisface* (R1)-(R3)*, $\mathcal{I}$ la colección de subconjuntos X de E para los cuales $r(X) = |X|$. Entonces la pareja $(E, \mathcal{I})$ es una matroide con función rango r.*

1.4.9 Observaciones.

1. Sean E un conjunto y $r : 2^E \to \mathbb{Z}^+ \cup \{0\}$ una función. La función r es la función rango de una matroide en E si, y solo si, r satisface $(R1)$-$(R3)$.
2. Sean $\mathcal{M}$ una matroide con función rango r y $X \subseteq E$. Se tiene que X es independiente si, y solo si, $|X| = r(X)$.
3. X es una base si, y solo si, $|X| = r(X) = r(\mathcal{M})$.
4. X es un circuito si, y solo si, $X \neq \emptyset$ y $r(X - x) = |X| - 1 = r(X)$ para cada $x \in X$.

1.4.10 Proposición. ([24, teorema 1.4.14(R2)]) *Sea E un conjunto y r la función rango de una matroide en E. Si $X \subseteq E$ y $x \in E$, entonces $r(X) \leq r(X \cup x) \leq r(X) + 1$.*

1.4.11 Ejemplo. Sea

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in M_{3\times 6}(\mathbb{F}_2),$$

la matroide asociada $M[A]$ tiene como conjunto subyacente a $E = \{1, 2, 3, 4, 5, 6\}$ e $\mathcal{I}(\mathcal{M}[A])$ de la manera siguiente:

$$\begin{aligned}
\mathcal{I}(\mathcal{M}[A]) &= A_0 \cup A_1 \cup A_2 \cup A_3 \text{ con } A_0, A_1, A_2, A_3 \text{ subfamilias de conjuntos de } E. \\
A_0 &= \emptyset, \\
A_1 &= \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}, \\
A_2 &= \{\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{1,6\}, \{2,4\}, \{2,5\}, \{2,6\}, \{3,4\}, \{3,5\}, \{3,6\}, \\
&\quad \{4,5\}, \{4,6\}, \{5,6\}\}, \\
A_3 &= \{\{1,2,4\}, \{1,2,5\}, \{1,2,6\}, \{1,3,4\}, \{1,3,5\}, \{1,3,6\}, \{1,4,5\}, \{1,5,6\}, \\
&\quad \{2,4,6\}, \{2,5,6\}, \{3,4,6\}, \{3,5,6\}, \{4,5,6\}\} \\
&= \mathcal{B}(\mathcal{M}[A]) \\
\mathcal{C}(M[A]) &= \{\{2,3\}, \{1,4,6\}, \{2,4,5\}, \{3,4,5\}, \{1,2,5,6\}, \{1,3,5,6\}\}.
\end{aligned}$$

□

1.4.12 Proposición. ([24, teorema 2.1.1]) *Sean $\mathcal{M}$ una matroide en E y $\mathcal{B}^* = \{E - B : B \in \mathcal{B}(\mathcal{M})\}$. Entonces $\mathcal{B}^*(\mathcal{M})$ es el conjunto de bases de una matroide en $E(\mathcal{M})$.*

A la matroide de la proposición 1.4.12 se le conoce como la **matroide dual** de $\mathcal{M}$, la cual denotaremos como $\mathcal{M}^*$. Todas las definiciones son válidas para esta nueva matroide y son llamadas igual, excepto con el prefijo co, así por ejemplo colazo, cocircuito y coindependiente denotan a un lazo, circuito e independiente de $\mathcal{M}^*$ respectivamente. Además, para cada $X \subseteq E$ se tiene que la función corango, es decir, r^* denota la función rango de $\mathcal{M}^*$ y satisface que (ver [24, proposición 2.19]):

$$r^*(X) = |X| - r(\mathcal{M}) + r(E - X). \tag{1.6}$$

Recordemos de álgebra lineal que mediante una secuencia de operaciones elementales podemos llevar una matriz $A \in M_{n\times m}(\mathbb{F}_q)$ a la forma $[I_n|D]$ donde $I_n \in M_{n\times n}(\mathbb{F}_q)$ es la matriz identidad y $D \in M_{n\times(m-n)}(\mathbb{F}_q)$.

1.4.13 Proposición. ([24, teorema 2.2.8]) *Sean $A = [I_n|D] \in M_{n\times m}(\mathbb{F}_q)$ y $\mathcal{M}[I|D]$ la matroide vector de A. Entonces la matroide $(\mathcal{M}[A])^*$ es la matroide vector de $[-D^T|I_{m-n}]$.*

1.4.14 Ejemplo. La matroide dual de la matroide $\mathcal{M}[A]$ del ejemplo 1.4.11 es $(\mathcal{M}[A])^* = (E, \mathcal{B}^*(\mathcal{M}[A]))$ con

$$\begin{aligned}\mathcal{B}^*(\mathcal{M}[A])) \;=\; &\{\{3,5,6\},\{3,4,6\},\{3,4,5\},\{2,5,6\},\{2,4,6\},\{2,4,5\},\{2,3,6\},\{2,3,4\},\\ &\{1,3,5\},\{1,3,4\},\{1,2,5\},\{1,2,4\},\{1,2,3\}\}.\end{aligned}$$ □

Sean $\mathcal{M}$ una matroide en E y $T \subseteq E$. La operación **borrado** de T en $\mathcal{M}$ se define como $\mathcal{M}|(E-T)$, a dicha matroide la denotamos como $\mathcal{M}\backslash T$; la **contracción** de T a $\mathcal{M}$ denotada por $\mathcal{M}/T$ se define como $\mathcal{M}/T := (\mathcal{M}^*\backslash T)^*$, la cual tiene conjunto subyacente a $E - T$.

1.4.15 Proposición. ([24, proposición 3.1.7]) *Sea $T \subseteq E$. Entonces*

$$r(\mathcal{M}/T) = r_{\mathcal{M}}(X \cup T) - r_{\mathcal{M}}(T), \text{ para cada } X \subseteq E - T.$$

Sean $\mathcal{M}$ una matroide en E y r su función rango. Definamos la función $\mathrm{cl}_{\mathcal{M}} : 2^{\mathrm{E}} \to 2^{\mathrm{E}}$ como $\mathrm{cl}_{\mathcal{M}}(X) := \{x \in E : r(X \cup x) = r(X)\}$, cuando no exista confusión escribiremos cl. Esta función es llamada operador **clausura** de $\mathcal{M}$, así llamamos $\mathrm{cl}(X)$ la clausura de X en $\mathcal{M}$. Diremos que $X \subseteq E$ es un **cerrado** si $X = \mathrm{cl}(X)$, a la familia de cerrados de $\mathcal{M}$ la denotaremos como $\mathcal{F}(\mathcal{M})$ y $\mathcal{F}(\mathcal{M})_i := \{\sigma \subset E : \sigma \in \mathcal{F}(\mathcal{M}), r(\sigma) = i\}$. Un **hiperplano** de $\mathcal{M}$ es un cerrado de rango $r(\mathcal{M}) - 1$. Además para cada $\sigma \subset E$ se define la función **nulidad** denotada por $n_{\mathcal{M}} : 2^E \to \mathbb{Z}$ como $n_{\mathcal{M}}(\sigma) = |\sigma| - r(\sigma)$ y definamos para cada $i \in \{1, \ldots, n_M(E)\}$,

$$\mathcal{N}_i := \{\sigma \subset E : n_{\mathcal{M}}(\sigma) = i, \sigma \text{ minimal respecto a esta propiedad}\}.$$

En el artículo de T. Johnsen y H. Verdure [15] se define $\mathcal{N}_i$ igual que aquí, pero sin pedir la minimalidad, sin embargo veremos que en el teorema 1.4.30 que la minimalidad es importante para determinar cuando los números de Betti del anillo de Stanley-Reisner asociado a una matroide son distintos de cero. Además al pedir minimalidad en el teorema 1.4.22 obtenemos que $\mathcal{N} = \cup\mathcal{N}_i$ es una retícula (ver proposición 1.4.20).

1.4.16 Observación. De la proposición 1.4.10 se tiene que para cada $X \subseteq E$ y $x \in E$, $n_{\mathcal{M}}(X) \geq n_{\mathcal{M}}(X - x) \geq n_{\mathcal{M}}(X) - 1$.

1.4.17 Proposición. ([24, proposición 2.1.6 (iv)]) *Sea $\mathcal{M} = (E, \mathcal{I})$ una matroide y supongamos que $X \subseteq E$. Entonces X es un circuito si, y solo si, $E - X$ es un cohiperplano.*

Las siguientes proposiciones van a ser de gran utilidad para la demostración del teorema 1.4.30, donde la siguiente proposición resulta ser el ejercicio 5 de [24, pp.110].

1.4.18 Proposición. *Sean $\mathcal{M}$ una matroide y $T \subset E(\mathcal{M})$. La matroide $\mathcal{M}/T$ no tiene lazos si, y solo si, T es un cerrado de $\mathcal{M}$.*

Demostración.

$\Leftarrow$) Si e es un lazo de $\mathcal{M}/T$ entonces e está en todas las bases de $(\mathcal{M}/T)^*$. Notemos que $(\mathcal{M}/T)^* = ((\mathcal{M}^* \backslash T)^*)^* = \mathcal{M}^* \backslash T$. Pero las bases de $M^* \backslash T$ son de la forma $B^* - T$ con $B^* \in \mathcal{B}^*(\mathcal{M})$. Recordemos que $\mathcal{B}^*(\mathcal{M}) = \{E(\mathcal{M}) - B : B \in \mathcal{B}\}$, entonces para toda $B \in \mathcal{B}(\mathcal{M})$ se tiene que $e \in (E - B) - T$, así que $e \notin B$ para toda $B \in \mathcal{B}(\mathcal{M})$. Por lo tanto e es un lazo de $\mathcal{M}$. Así $e \in \mathrm{cl}(T)$ y por consiguiente T no es cerrado en $\mathcal{M}$.

$\Rightarrow$) Supongamos que T no es cerrado en $\mathcal{M}$, i.e., $\mathrm{cl}(T) \neq T$. Así $\mathrm{cl}(T) - T \neq \emptyset$; ahora bien, calculemos el rango de $\mathrm{cl}(T) - T$:

$$\begin{aligned}
\mathrm{r}_{\mathcal{M}/\mathrm{T}}(\mathrm{cl(T)} - \mathrm{T}) &= r_{(\mathcal{M}^* \backslash T)^*}(\mathrm{cl(T)} - \mathrm{T}) \\
&= |(\mathrm{cl(T)} - \mathrm{T})| + \mathrm{r}_{(\mathcal{M}^* \backslash \mathrm{T})}((\mathrm{E} - \mathrm{T}) - (\mathrm{cl(T)} - \mathrm{T})) - \mathrm{r}_{(\mathcal{M}^* \backslash \mathrm{T})}(\mathrm{E} - \mathrm{T}) \\
&= |(\mathrm{cl(T)} - \mathrm{T})| + \mathrm{r}_{(\mathcal{M}^* \backslash \mathrm{T})}((\mathrm{E} - (\mathrm{cl(T)}) - \mathrm{r}_{(\mathcal{M}^* \backslash \mathrm{T})}(\mathrm{E} - \mathrm{T}) \\
&= |(\mathrm{cl(T)} - \mathrm{T})| + \mathrm{r}_{\mathcal{M}^*}((\mathrm{E} - (\mathrm{cl(T)}) - \mathrm{r}_{\mathcal{M}^*}(\mathrm{E} - \mathrm{T}) \\
&= |(\mathrm{cl(T)} - \mathrm{T})| + |\mathrm{E} - (\mathrm{cl(T)}| + \mathrm{r}(\mathrm{E} - (\mathrm{E} - (\mathrm{cl(T)}))) - \mathrm{r(E)} \\
&\quad -|E - T| - r(E - (E - T)) + r(E) \\
&= (|(\mathrm{cl(T)} - \mathrm{T})| + |\mathrm{E} - \mathrm{cl(T)}| - |\mathrm{E} - \mathrm{T}|) + [\mathrm{r}(\mathrm{E} - (\mathrm{E} - \mathrm{cl(T)})) \\
&\quad -r(E - (E - T)) + r(E) - r(E)] \\
&= (|(\mathrm{cl(T)} - \mathrm{T})| + |\mathrm{E} - \mathrm{cl(T)}| - |\mathrm{E} - \mathrm{T}|) + (\mathrm{r(cl(T))} - \mathrm{r(T)}) \\
&\quad +(r(E) - r(E)) \\
&= 0 + 0 + 0 \\
&= 0.
\end{aligned}$$

Entonces los elementos de $\mathrm{cl}(T) - T$ son lazos de $\mathcal{M}/T$. ∎

1.4.19 Observación. Sean $\mathcal{M}$ una matroide en E y $X \subset E$. Aplicando la ecuación (1.6) en $E - X$, se tiene que:

$$\begin{aligned}
r^*(E - X) &= |E - X| + r(E - (E - X)) - r(\mathcal{M}) \\
&= |E - X| + r(X) - r(\mathcal{M}) \\
&= |E| - |X| + r(X) - r(\mathcal{M}) \\
&= |E| + r(E) - (|X| - r(X)) \\
&= r^*(E) - n_{\mathcal{M}}(X).
\end{aligned}$$

Por lo tanto $r^*(E - X) = r^*(E) - n_{\mathcal{M}}(X)$.

1.4.20 Proposición. *Sean $\mathcal{M}$ una matroide en E, r^* el rango de $\mathcal{M}^*$ y $\sigma \subset E$. Entonces $\sigma \in \mathcal{N}_i$ si, y solo si, $E - \sigma \in \mathcal{F}(\mathcal{M}^*)_{r^* - i}$.*

Demostración.

$\Rightarrow$) Se tiene de la observación 1.4.19 que $r^*(E-\sigma) = r^*(E) - n_{\mathcal{M}}(\sigma) = r^*(E) - i$. Ahora bien, para cualquier $x \in \sigma$,

$$r^*((E-\sigma)\cup x) = r^*(E-(\sigma - x)) = r^*(E) - n_{\mathcal{M}}(\sigma - x) = r^*(E) - (n_{\mathcal{M}}(\sigma) - 1),$$

pero $r^*(E) - (n_{\mathcal{M}}(\sigma) - 1) = r^*(E-\sigma) + 1$. Así que $\mathrm{cl}^*(E-\sigma) = E - \sigma$, donde cl^* denota la clausura de $\mathcal{M}^*$.

$\Leftarrow$) Solo resta demostrar que σ es minimal en $\mathcal{N}_i$. Supongamos que existe $\sigma' \subset \sigma$ tal que $n_{\mathcal{M}}(\sigma') = i$. De lo cual $r^*(E-\sigma') = r^*(E) - n_{\mathcal{M}}(\sigma') = r^*(E) - i$. Por otro lado, $E - \sigma \subset E - \sigma'$, y como $E - \sigma \in \mathcal{F}(\mathcal{M}^*)_{r^*-i}$, $E - \sigma = E - \sigma'$. De lo cual concluímos que $\sigma = \sigma'$. ∎

1.4.21 Observación. Para cada $\sigma \in \mathcal{C}(\mathcal{M})$, se tiene de la proposición 1.4.17 y de la proposición 1.4.20 que $\sigma \in \mathcal{N}_1$ si, solo si $\sigma \in \mathcal{C}(\mathcal{M})$. Así, $\mathcal{C}(\mathcal{M}) = \mathcal{N}_1$.

Un **poset** es un conjunto P sobre el cual existe un orden parcial " $\leq$ ". Una **retícula** (finita) es un poset finito $\mathcal{L}$, tal que para cada par de elementos $x, y \in \mathcal{L}$ existe una menor cota ruperior y una mayor cota inferior, las cuales denotaremos como $x \vee y$ y $x \wedge y$ respectivamente. Además, si exite $z \in P$ tal que $z \leq x$ para todo $x \in P$, entonces a z se le llama **elemento cero** de P. Por otra parte, si existe un elemento $y \geq x$ para todo $x \in P$, a y se le llama **elemento uno**. Si $x < y$, decimos que x **cubre** a y si no existe un z tal que $x < z < y$. Sea x_0 y $x_n \in \mathcal{L}$, una **cadena** de x_0 a x_n es un subconjunto $\{x_0, x_1, \ldots, x_n\}$ de $\mathcal{L}$ tal que $x_0 < x_1 < \cdots < x_n$ y x_i cubre a x_{i-1} para todo $i \in [n]$. La **longitud** de tal cadena es n. Para cualquier par de elementos x y y si todas las cadenas de x a y tienen la misma longitud entonces decimos que $\mathcal{L}$ satisface la **condición de Jordan-Dedekind**. Además para cualquier $x \in \mathcal{L}$, la **altura** de x es la máxima longitud de una cadena de 0 a x, que denotaremos como $h(x)$. Así, una **retícula geométrica** es aquella retícula $\mathcal{L}$ donde cada elemento es unión de elementos que cubren al 0, $\mathcal{L}$ satisface la condición de Jordan-Dedekind y para cualquier par de elementos $x, y \in \mathcal{L}$ se tiene que

$$h(x \vee y) + h(x \wedge y) \leq h(x) + h(y). \tag{1.7}$$

Por ejemplo, para cualquier matroide $\mathcal{M}$ sobre E se tiene que los cerrados forman una retícula con el orden " $\subseteq$ ", la cual denotaremos por abuso de notación por $\mathcal{F}(\mathcal{M})$. Donde el elemento cero es $\mathrm{cl}_{\mathcal{M}}(\emptyset)$ y el elemento uno es E. Más aún, para cada $F_1, F_2 \in \mathcal{F}(\mathcal{M})$ se tiene que $F_1 \vee F_2 = \mathrm{cl}(F_1 \cup F_2)$ y $F_1 \wedge F_2 = F_1 \cap F_2$ (ver [24, lema 1.7.3]). Por otro lado, podemos observar que los elementos de $\mathcal{F}(\mathcal{M})_1$ son los elementos que cubren a $\mathrm{cl}(\emptyset)$, y además es fácil ver que cualquier otro elemento de $\mathcal{F}(\mathcal{M})$ es unión de los cerrados de rango 1. Del lema 1.7.6 en [24], se tiene que $\mathcal{F}(\mathcal{M})$ satisface la condición de Jordan-Dedekind. Más aún, para cada $F \in \mathcal{F}(\mathcal{M})$, $h(F) = r(F)$. Por lo tanto se satisface (1.7). De esta forma $\mathcal{F}(\mathcal{M})$ es una retícula geométrica. De hecho, en el siguiente teorema podemos ver que las únicas retículas geométricas, salvo isomorfismo, son las retículas de cerrados de matroides:

1.4.22 Teorema. ([24, teorema 1.7.5]) *Una retícula $\mathcal{L}$ es una retícula geométrica si, y solo si, es la retícula de cerrados de una matroide.*

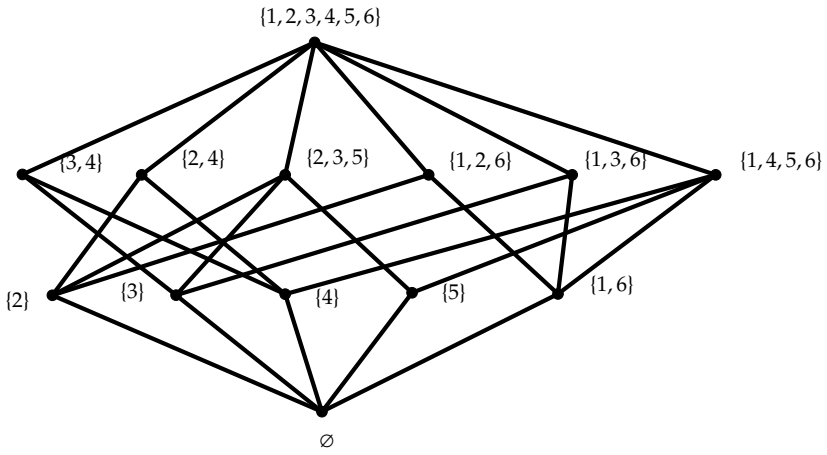

Figura 1.4:

Para tener una representación gráfica de una retícula, podemos utlizar un diagrama de Hasse, que es una gráfica simple, donde los vértices son los elementos de la retícula; y existe una arista entre dos elementos x y y, si x cubre a y. Así para cualquiera matroide $\mathcal{M}$, el diagrama de Hasse de la retícula $\mathcal{F}(\mathcal{M})$ esta por niveles, es decir, si F_1 y F_2 están en el mismo nivel entonces $r(F_1) = r(F_2)$.

1.4.23 Observación. Dada una retícula $\mathcal{L}$ su retícula dual es aquella en la que se invierte el orden, es decir, se considera el orden " $\geq$ ". Así, por la proposición 1.4.20 el conjunto $\mathcal{N}(\mathcal{M}) = \{\sigma \subset E : \exists i \in [r^*], \sigma \in \mathcal{N}_i\}$ con el orden " $\supseteq$ " resulta isomorfo a la retícula dual $\mathcal{F}(\mathcal{M}^*)$, por lo que $\mathcal{N}(\mathcal{M})$ es una retícula geométrica. Así que los niveles del diagrama de Hasse de la retícula $\mathcal{N}(\mathcal{M})$ están dados por la función nulidad del matroide.

1.4.24 Ejemplo. Del ejemplo 1.4.11, la retícula de cerrados de $(\mathcal{M}[A])^*$ y su retícula dual $\mathcal{N}(\mathcal{M}[A])$ están representadas en la figura 1.4 y 1.5, respectivamente.

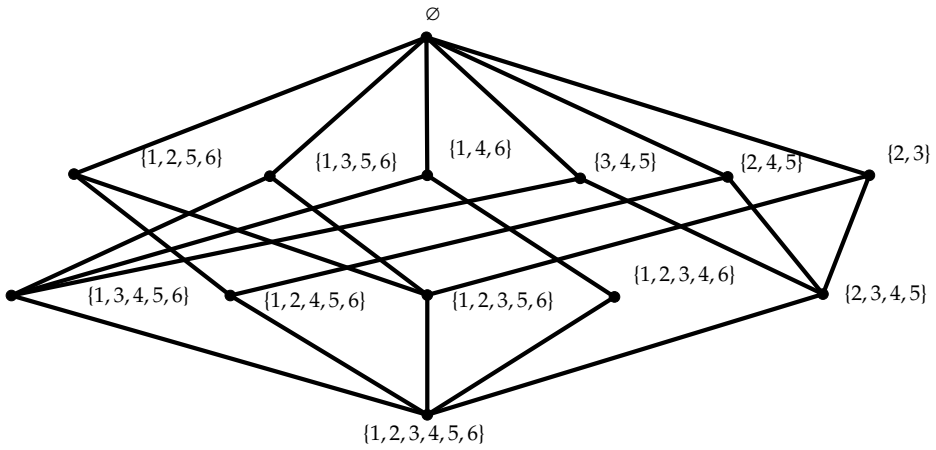

Figura 1.5:

□

Para una matroide $\mathcal{M} = (E, \mathcal{I})$, $W \subset E$, $F \in \mathcal{F}(\mathcal{M})$, definimos la función **de Möbius** como:

$$\mu_{\mathcal{M}}(W, F) := \sum_{\substack{W \subseteq X \subseteq F \\ \mathrm{cl}(X) = F}} (-1)^{|X-W|}. \tag{1.8}$$

1.4.25 Proposición. ([32, teorema 7.18]) *Sea $\mathcal{M}$ una matroide y $\mathcal{F}(\mathcal{M})$ su retícula de cerrados. Entonces para cualesquiera $F_1, F_2 \in \mathcal{F}(\mathcal{M})$ y $F_1 \subseteq F_2$, $\mu_{\mathcal{M}}(F_1, F_2) \neq 0$.*

Definimos:

$$\mu(\mathcal{M}) := \begin{cases} |\mu_{\mathcal{M}}(\mathrm{cl}(\emptyset), E)| & \text{si } \mathcal{M} \text{ no tiene lazos,} \\ 0 & \text{en otro caso.} \end{cases} \tag{1.9}$$

En la siguiente proposición relacionemos la característica de Euler.

1.4.26 Proposición. ([5, teorema 7.4.7]) *Sea $\mathcal{M}$ una matroide con rango r y sin lazos. Entonces*

$$\widetilde{\chi}(\mathcal{I}(\mathcal{M})) = (-1)^{r-1}\mu(\mathcal{M}^*). \tag{1.10}$$

1.4.27 Lema. ([5, teorema 7.8.1]) *Sean $\mathcal{M}$ una matroide de rango r y $\Delta = \mathcal{I}(\mathcal{M})$. Entonces*

$$\widetilde{H}_i(\Delta, \mathbb{Z}) \simeq \begin{cases} \mathbb{Z}^{(-1)^{r-1}\widetilde{\chi}(\Delta)} & \text{si } i = r-1 \\ 0 & \text{en otro caso.} \end{cases}$$

1.4.28 Proposición. ([28, corolario 7.58]) *Sean X un espacio topológico y G un grupo abeliano. Si $\widetilde{H}_{n-1}(X)$ o G es libre de torsión, entonces*

$$\widetilde{H}_n(X, G) \simeq \widetilde{H}_n(X) \otimes_{\mathbb{Z}} G.$$

De la proposición 1.4.27 y 1.4.28 se sigue quien es la homología de $\Delta = \mathcal{I}(\mathcal{M})$ sobre cualquier campo $\mathbb{K}$ con r el rango de $\mathcal{M}$, y es:

$$\widetilde{H}_i(\Delta, \mathbb{K}) \simeq \begin{cases} \mathbb{K}^{(-1)^{r-1}\widetilde{\chi}(\Delta)} & \text{si } i = r-1 \\ 0 & \text{en otro caso.} \end{cases} \tag{1.11}$$

1.4.29 Proposición. *Sea $\mathcal{M}$ una matroide en E. Entonces $\widetilde{\chi}(\mathcal{I}(\mathcal{M})) = 0$ si, y solo si, $\mathcal{M}^*$ tiene un lazo.*

Demostración.

⇒) Si $\widetilde{\chi}(\mathcal{I}(\mathcal{M})) = 0$ se tiene por la ecuación 1.10, $\mu(\mathcal{M}^*) = 0$, entonces de la proposición 1.4.25 y de la definición de $\mu(\mathcal{M})$ (ver 1.9) se tiene que M^* tiene un lazo.

⇐) La matroide $\mathcal{M}^*$ tiene un lazo e si, y solo si, $E - \{e\}$ es un hiperplano si, y solo si, e está en cada base de $\mathcal{M}$ entonces $\mathcal{I}(M)$ es un cono. Así de la proposición 1.3.18 se tiene que $\widetilde{\chi}(\mathcal{I}(\mathcal{M})) = 0$. ∎

El siguiente teorema lo demostramos de manera diferente a la que se puede consultar en [15, teorema 1]. Sea $\mathcal{M} = (E, \mathcal{I})$ una matroide, recordemos que dado que $\mathcal{I}$ es un complejo simplicial, podemos asociarle el anillo de Stanley-Reisner, y así calculamos los números de Betti, dicho cálculo es posible gracias a la fórmula de Hochster 1.3.29.

El resto de la demostración del teorema 1 en [15] para mostrar que los números de Betti $\beta_{i,\sigma}$ del anillo de Stanley-Reisner asociado a $\mathcal{I}$ son distintos de cero si y solo si σ tiene nulidad i y es minimal respecto a esta propiedad, se introduce el concepto de circuitos irredundantes y sus propiedades para mostrar que cualquier subconjunto σ de nulidad i es minimal si, y solo si, σ es la union de circuitos irredundantes maximales. Recordemos que la definición de $\mathcal{N}_i$ que nosotros consideramos incluye la propiedad de minimalidad, dicha propiedad nos permite tener una retícula $\mathcal{N}(\mathcal{M}) = \cup\mathcal{N}_i$ y así demostramos el teorema con el estudio de retículas sin tener que pasar por los circuitos irredundantes. Cabe señalar que del estudio de las retículas de una matroide $\mathcal{M}$, las cuales son la retículas $\mathcal{N}(\mathcal{M})$ y $\mathcal{F}(M^*)$ se desprenden las ideas para calcular la regularidad de Castelnuovo-Mumford del anillo de Stanley-Reisner asociado a una matroide, el cual generaliza al lema 4.6 que recientemente apareció en [20].

Sea $\mathcal{M} = (E, \mathcal{I})$ una matroide, $I_{\mathcal{I}}$ el anillo de Stanley-Reisner asociado al complejo de independencia $\mathcal{I}$, el cual denotaremos por $I_{\mathcal{M}}$; y $S/I_{\mathcal{M}}$ el anillo de Stanley-Reisner asociado al complejo de independencia $\mathcal{I}$ de $\mathcal{M}$ donde S es el anillo de polinomios en las variables indexadas por E con coeficientes en el campo $\mathbb{K}$.

1.4.30 Teorema. *Sean $M = (E, \mathcal{I})$ una matroide y $\sigma \subset E$. Entonces $\beta_{i,\sigma}(S/I_{\mathcal{M}}) \neq 0$ si, y solo si, $\sigma \in \mathcal{N}_i$. Más aún, si $\sigma \in \mathcal{N}_i$, $\beta_{n_{\mathcal{M}}(\sigma),\sigma}((S/I_{\mathcal{M}})) = (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma) \neq 0$ y $\beta_{i,\sigma}(S/I_{\mathcal{M}}) = 0$ si $i \neq n_{\mathcal{M}}(\sigma)$.*

Demostración. Por la fórmula de Hochster se tiene que $\beta_{i,\sigma}(S/I_{\mathcal{M}}) = \dim \widetilde{H}_{|\sigma|-i-1}(\mathcal{I}|\sigma, \mathbb{K})$. Además de la ecuación (1.11),

$$\dim \widetilde{H}_{|\sigma|-i-1}(\mathcal{I}|\sigma, \mathbb{K}) \simeq \begin{cases} (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma) & \text{si } |\sigma| - i - 1 = r(\mathcal{M}|\sigma) - 1, \\ 0 & \text{en otro caso.} \end{cases} \tag{1.12}$$

Entonces $\beta_{i,\sigma}(S/I_{\mathcal{M}}) \neq 0$ si, y solo si, $|\sigma| - i - 1 = r(\mathcal{M}|\sigma) - 1$ y $\widetilde{\chi}(\mathcal{I}|\sigma) \neq 0$. Si $|\sigma| - i - 1 = r(\mathcal{M}|\sigma) - 1$ obtenemos que $i = r(\mathcal{M}|\sigma) - |\sigma| = r(\sigma) - |\sigma| = n_{\mathcal{M}}(\sigma)$. Usando la proposición 1.4.29 se deduce que $n_{\mathcal{M}}(\sigma) = i$ y $\widetilde{\chi}(\mathcal{I}|\sigma) \neq 0$ si, y solo si, $(\mathcal{M}|\sigma)^*$ no tiene lazos y $n_{\mathcal{M}}(\sigma) = i$. Por otro lado, $(\mathcal{M}|\sigma)^* = (\mathcal{M}\backslash(E - \sigma))^* = \mathcal{M}^*/(E - \sigma)$. Por lo tanto de la proposición 1.4.18, $(\mathcal{M}|\sigma)^*$ no tiene lazos si, y solo si, $E - \sigma \in \mathcal{F}(\mathcal{M}^*)$. Más aún, de la observación 1.4.19 se tiene que $r^*(E - \sigma) = r^*(E) - n_{\mathcal{M}}(\sigma)$. De esta forma $(\mathcal{M}|\sigma)^*$ no tiene lazos y $n_{\mathcal{M}}(\sigma) = i$ si, y solo si, $E - \sigma \in \mathcal{F}(\mathcal{M}^*)$ y $r(E - \sigma) = r^*(E) - i$, es decir, $E - \sigma \in \mathcal{F}(\mathcal{M}^*)_{r^*(E)-i}$. Más aún de la proposición 1.4.20, $(E - \sigma) \in \mathcal{F}(\mathcal{M}^*)_{r^*-n_{\mathcal{M}}(\sigma)}$ si, y solo si, $\sigma \in \mathcal{N}_i$. Por lo que hemos demostrado que $\beta_{i,\sigma}(S/I_{\mathcal{M}}) \neq 0$ si, y solo si, $\sigma \in \mathcal{N}_i$. Además de lo anterior y usando la ecuación 1.12 obtenemos que si $\sigma \in \mathcal{N}_i$, $\beta_{n_{\mathcal{M}}(\sigma),\sigma}((S/I_{\mathcal{M}})) = (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma) \neq 0$; y si $i \neq n_{\mathcal{M}}(\sigma)$, entonces $\beta_{n_{\mathcal{M}}(\sigma),\sigma}((S/I_{\mathcal{M}})) = 0$. ∎

1.4.31 Corolario. *Sean $\mathcal{M} = (E, \mathcal{I})$ una matroide. Entonces se cumplen los siguientes enunciados:*

1.

$$\begin{aligned}\beta_{i,j}(S/I_{\mathcal{M}}) &= \sum_{\substack{\sigma \in \mathcal{N}_i \\ |\sigma| = j}} \beta_{i,\sigma}(S/I_{\mathcal{M}}) \\ &= \sum_{\substack{\sigma \in \mathcal{N}_i \\ |\sigma| = j}} (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma) \\ &= \sum_{\substack{\gamma \in (\mathcal{F}(\mathcal{M}^*))_{r^*(\mathcal{M})-i} \\ |\gamma| = |E| - j}} (-1)^{r(E-\gamma)-1}\widetilde{\chi}(\mathcal{I}|E-\gamma).\end{aligned}$$

2. $\operatorname{dimproj}(S/I_{\mathcal{M}}) = |E| - r(\mathcal{M})$.

3. $S/I_{\mathcal{M}}$ *es un álgebra de nivel.*

4. $\operatorname{reg}(S/I_{\mathcal{M}}) = r(\mathcal{M}) - |\mathrm{cl}^*(\emptyset)|$.

Demostración.

1. De la ecuación (1.5) se tiene que $\beta_{i,j}(S/I_{\mathcal{M}}) = \sum_{\sigma\in\mathbb{N}^n,|\sigma|=j} \beta_{i,\sigma}(S/I_{\mathcal{M}})$. Pero del teorema 1.4.30 $\beta_{i,\sigma}(S/I_{\mathcal{M}}) \neq 0$ si, y solo si, $\sigma \in \mathcal{N}_i$. Así,

$$\beta_{i,j}(S/I_{\mathcal{M}}) = \sum_{\substack{\sigma \in \mathcal{N}_i \\ |\sigma| = j}} \beta_{i,\sigma}(S/I_{\mathcal{M}}) = \sum_{\substack{\sigma \in \mathcal{N}_i \\ |\sigma| = j}} (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma).$$

   Más aún, de la proposición 1.4.20,

$$\begin{aligned}\sum_{\substack{\sigma \in \mathcal{N}_i \\ |\sigma| = j}} (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma) &= \sum_{\substack{E-\sigma \in (\mathcal{F}(\mathcal{M}))_{r^*(\mathcal{M})-i} \\ |E-\sigma| = |E| - j}} (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{I}|\sigma) \\ &= \sum_{\substack{\gamma \in (\mathcal{F}(\mathcal{M}))_{r^*(\mathcal{M})-i} \\ |\gamma| = |E| - j}} (-1)^{r(E-\gamma)-1}\widetilde{\chi}(\mathcal{I}|E-\gamma)\end{aligned}.$$

2. Recordemos que $\operatorname{dimproj}(S/I_{\mathcal{M}}) = \max\{i : \beta_{i,j}(S/I_{\mathcal{M}}) \neq 0\}$. Del inciso *1.* de este corolario se tiene que $\beta_{i,j}(S/I_{\mathcal{M}}) = \sum_{\sigma\in\mathcal{N}_i,|\sigma|=j} \beta_{i,\sigma}(S/I_{\mathcal{M}})$. Así

$$\operatorname{dimproj}(S/I_{\mathcal{M}})) = n_{\mathcal{M}}(\mathcal{M}) = r^*(\mathcal{M}) = |E| - r(\mathcal{M}).$$

3. Recordemos que si $\rho = \operatorname{dimproj}(S/I_{\mathcal{M}}))$, decimos que $S/I_{\mathcal{M}}$ es una álgebra de nivel si $\beta_\rho(S/I_{\mathcal{M}}) = \beta_{\rho,j}(S/I_{\mathcal{M}})$ para algún $j \in \mathbb{N}$ y $S/I_{\mathcal{M}}$ es Cohen-Macaulay. Del inciso 2 de este corolario $\rho = |E| - r(\mathcal{M}) = r^*(\mathcal{M}) = \operatorname{codim}(S/I_{\mathcal{M}})$; por lo que $S/I_{\mathcal{M}}$ es Cohen-Macaulay y del inciso 1:

$$\beta_{\rho,j}(S/I_{\mathcal{M}}) = \sum_{\substack{\sigma \in \mathcal{N}_{r^*(\mathcal{M})} \\ |\sigma| = j}} (-1)^{r(\sigma)-1}\widetilde{\chi}(\mathcal{M}|_\sigma),$$

para cada $j \in \mathbb{N}$. Pero de la proposición 1.4.20 se tiene que:

$$\begin{aligned}\mathcal{N}_{r^*(\mathcal{M})} &= \{\sigma \subset E : n_{\mathcal{M}}(\sigma) = r^*(\mathcal{M})\} \\ &= \{E - \sigma \in \mathcal{F}(\mathcal{M}^*)_{r^*(\mathcal{M})-r^*(\mathcal{M})}\} \\ &= \{E - \sigma \in \mathcal{F}(\mathcal{M}^*)_0\};\end{aligned}$$

sin embargo $(\mathcal{F}(\mathcal{M}^*))_0 = \{\mathrm{cl}^*(\emptyset)\} := \mathcal{A}(\mathcal{M})$, donde cl^* denota el operador clausura en $\mathcal{M}^*$. Así $\mathcal{N} = \{E - \mathcal{A}(\mathcal{M})\}$. Entonces

$$\begin{aligned}\beta_\rho(S/I_{\mathcal{M}}) &= \beta_{r^*(\mathcal{M})}(S/I_{\mathcal{M}})) \\ &= \beta_{r^*(\mathcal{M}),|E-\mathcal{A}(\mathcal{M})|}(S/I_{\mathcal{M}})\end{aligned} \tag{1.13}$$

De lo cual concluimos que $S/I_{\mathcal{M}}$ es una álgebra de nivel.

4. Recordemos que $\mathrm{reg}(S/I_{\mathcal{M}}) = \mathrm{máx}\{j \in \mathbb{N} : \beta_{i,i+j}(S/I_{\mathcal{M}}) \neq 0 \text{ para algún } i \in \mathbb{N}\}$. De (1.13) $\beta_{r^*(\mathcal{M}),|E-\mathcal{A}(\mathcal{M})|}(S/I_{\mathcal{M}}) \neq 0$, de aquí que

$$(|E - \mathcal{A}(\mathcal{M})| - r^*(\mathcal{M})) \in \{j \in \mathbb{N} : \beta_{i,i+j}(S/I_{\mathcal{M}}) \neq 0\}, \text{ pero}$$

$$|E - \mathcal{A}(\mathcal{M})| - r^*(\mathcal{M}) = (|E| - |\mathcal{A}(\mathcal{M})|) - (|E| - r(\mathcal{M})) = r(\mathcal{M}) - |\mathcal{A}(\mathcal{M})|.$$

Del inciso 1 se tiene que para cualesquiera $i, j \in \mathbb{N}$:

$$\beta_{i,i+j}(S/I_{\mathcal{M}}) = \sum_{\substack{\gamma \in (\mathcal{F}(\mathcal{M}^*))_{r^*(\mathcal{M})-i} \\ |\gamma| = |E| - (i+j)}} (-1)^{r(E-\gamma)-1}\widetilde{\chi}(\mathcal{M}|E-\gamma).$$

Así, sea $i \in \mathbb{N}$, $\gamma \in (\mathcal{F}(\mathcal{M}^*))_{r^*(\mathcal{M})-i}$ y $j = |E| - i - |\gamma|$. Dado que $r^*(\gamma) = r^*(\mathcal{M}) - i$ se tiene que:

$$j = |E| - i - |\gamma| = |E| - (r^*(\mathcal{M}) - r^*(\gamma)) - |\gamma| = (|E| - r^*(\mathcal{M})) + r^*(\gamma)) - |\gamma|.$$

Pero $r^*(\gamma) = r^*(\gamma - \mathcal{A}(\mathcal{M}) \cup \mathcal{A}(\mathcal{M})) \leq r^*(\gamma - \mathcal{A}(\mathcal{M})) + r^*(\mathcal{A}(\mathcal{M})) - r^*(\gamma - \mathcal{A}(\mathcal{M}) \cap \mathcal{A}(\mathcal{M}))$, donde la desigualdad está dada por la propiedad $(R3)$. Como $\mathcal{A}(\mathcal{M})$ es el conjunto de los lazos de $\mathcal{M}^*$ entonces $r^*(\mathcal{A}(\mathcal{M})) = 0$, así

$$\begin{aligned}j &\leq (|E| - r^*(\mathcal{M})) + (r^*(\gamma - \mathcal{A}(\mathcal{M})) - |\gamma - \mathcal{A}(\mathcal{M})| - |\mathcal{A}(\mathcal{M})|)) \\ &= (r(\mathcal{M}) - |\mathcal{A}(\mathcal{M})|) - (|\gamma - \mathcal{A}(\mathcal{M})| - r^*(\gamma - \mathcal{A}(\mathcal{M}))).\end{aligned} \tag{1.14}$$

Y como $|\gamma - \mathcal{A}(\mathcal{M})| - r^*(\gamma - \mathcal{A}(\mathcal{M})) \geq 0$, dado que $r^*(\gamma - \mathcal{A}(\mathcal{M})) \leq |\gamma - \mathcal{A}(\mathcal{M})|$. Así de 1.14, $j \leq r(\mathcal{M}) - |\mathcal{A}(\mathcal{M})| - (r^*(\gamma - \mathcal{A}(\mathcal{M})) + |\gamma - \mathcal{A}(\mathcal{M})|) \leq r(\mathcal{M}) - |\mathcal{A}(\mathcal{M})|$. Por lo tanto, $\mathrm{reg}(S/I_{\mathcal{M}}) = r(\mathcal{M}) - |\mathcal{A}(\mathcal{M})|$. ∎

El inciso 2 del corolario 1.4.31 se puede demostrar del hecho de que el conjunto de independencia de un matroide es escalonado (es decir, shellable) y el anillo de Stanley-Reisner de todo complejo simplicial escalonado es Cohen-Macaulay (ver [6] y [30, capítulo 3]); así

$$\mathrm{dimproj}(S/I) = \mathrm{codim}(S/I) = n - \dim(S/I) = n - r,$$

la última igualdad se debe a la proposición 1.3.24. Además, el inciso 3 del corolario 1.4.31 se puede demostrar del hecho de que dado una matroide $\mathcal{M} = (E, \mathcal{I})$, $\mathcal{I}$ es un complejo simplicial y cualquier subcomplejo inducido es puro. Tambien se sabe que todo subcomplejo inducido puro es escalonado ([30, proposición 3.1]) y el anillo de Stanley-Reisner de todo complejo simplicial escalonado es Cohen-Macaulay. Así solo resta usar [30, proposición 3.2] para demostrar que $S/I_{\mathcal{M}}$ es de nivel.

1.4.32 Ejemplo. Sea $\mathcal{M}[B]$ la matroide vector asociada a la matriz:

$$B = \begin{pmatrix} 0 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 0 & 2 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & 2 & 2 & 0 & 2 \end{pmatrix} \in M_{4\times 4}(\mathbb{F}_3).$$

La tabla de los números de Betti es:

$j\backslash i$	0	1
0	1	2

Así por definición de regularidad de Castelnuovo-Mumford, $\operatorname{reg}(S/I_{\mathcal{M}[B]}) = 0$. Por otro lado, el rango de $\mathcal{M}[B]$ es 3, entonces del inciso 4 del corolario 1.4.31 y dado que

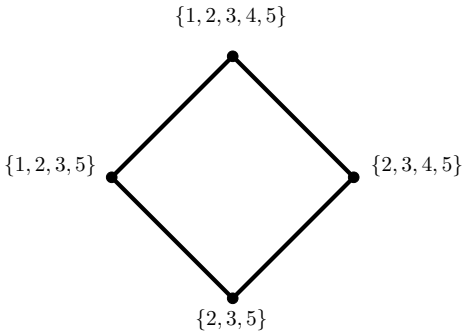

Figura 1.6: La retícula $\mathcal{F}((\mathcal{M}[B])^*)$.

$\mathcal{A}(\mathcal{M}) = \{\{2, 3, 5\}\}$ (ver figura 1.6), se tiene que $\operatorname{reg}(S/I_{\mathcal{M}[B]}) = 3-|\{2, 3, 5\}| = 0$. □

Una matroide $\mathcal{M}$ es un **diseño matroidal perfecto** si todos los cerrados de $(\mathcal{F}(\mathcal{M}))_i$ tienen el mismo tamaño. Así, estamos en condiciones para enunciar el siguiente corolario que es consecuencia directa del inciso 1 del corolario 1.4.31:

1.4.33 Corolario. *Sean $\nu \in \mathbb{N}$, $1 \leq d_1 < \cdots < d_\nu \in \mathbb{N}$ y $\mathcal{M} = (E, \mathcal{I})$ una matroide de nulidad ν. Entonces $S/I_{\mathcal{M}}$ tiene una resolución $(0, d_1, \ldots, d_\nu)$-pura si, y solo si, $\mathcal{M}^*$ es un diseño matroidal perfecto; además si $\sigma \in \mathcal{N}_i$, $|\sigma| = d_i$.*

■

Capítulo 2

Jerarquía de pesos generalizados de Hamming

Fijando un poco de notación, $\mathbb{F}_q$ denotará un campo finito de tamaño q. Dado $n \in \mathbb{N}$, los elementos $x \in \mathbb{F}_q^n$ se consideraran que son vectores renglón, salvo se indique lo contrario, es decir, $x = (x_1, \ldots, x_n)$ con $x_1, \ldots, x_n \in \mathbb{F}_q$; además x^T será la transpuesta de x, esto es, x^T es un vector columna. Dado $m, n \in \mathbb{N}$, usaremos $M_{m\times n}(\mathbb{F}_q)$ para denotar el conjunto de matrices con entradas en $\mathbb{F}_q$ con m renglones y n columnas. Además los elementos $M_{m\times n}(\mathbb{F}_q)$ se denotarán por letras mayúsculas seguidas por el subíndice $m \times n$ o no, cuando el contexto lo permita; por ejemplo: escribiremos $A_{m\times n}$ o A para denotar a una matriz. Dada una matriz $A \in M_{m\times n}(\mathbb{F}_q)$, $\operatorname{rank}(A)$ indica el rango de la matriz A; y además $A^{\perp} = \{x \in \mathbb{F}_q^n : Ax^T = 0\}$.

2.1. Teoría de códigos

La presente sección comienza introduciendo los conceptos y propiedades básicas de la teoría de códigos, así como también se definen los pesos de Hamming generalizados para un código. Una parte fundamental para la obtención de una definición equivalente para los pesos de Hamming generalizados de una matroide es el teorema de Wei. Gracias a esto último y a los resultados de la sección 1.4 obtenemos una fórmula para calcular los pesos generalizados de Hamming de cualquier matroide en términos de sus números de Betti de su ideal de Stanley-Reisner.

Un **código lineal** C es un subespacio lineal de $\mathbb{F}_q^n$ (con $\mathbb{F}_q$ el campo finito de q elementos), donde $q = p^m$ con p primo (para saber más acerca de campos finitos, ver capítulo 10 de [29]). La **dimensión** de un código lineal es su dimensión como un espacio vectorial en $\mathbb{F}_q^n$. Denotemos a un código lineal $C \subset \mathbb{F}_q^n$ de dimensión k como $[n, k]_q$, código de tipo $[n, k]_q$ o simplemente como $[n, k]$, cuando el campo pueda obviarse por el contexto. Para un código lineal C de tipo $[n, k]$ en $\mathbb{F}_q^n$, definimos la **codimensión** (redundancia en algunos textos como [17]) como $r := n - k$. Los elementos en un código C de tipo $[n, k]_q$ son llamados **palabras código**. El **tamaño** de un código C es $M = q^k$ dado que $C \simeq \mathbb{F}_q^k$, es decir, C contiene M palabras código.

2.1.1 Observación. Hay dos maneras de describir a un subespacio vectorial, las cuales son dando una base y por el espacio solución de un conjunto de ecuaciones lineales homógeneas.

Así, existen dos maneras de describir a un código lineal, que describiremos en las siguientes líneas.

Sea C un código lineal de tipo $[n,k]_q$. Dado que C es un subespacio k-dimensional lineal de $\mathbb{F}_q^n$, existe una base para C que consiste de k palabras código. Así, una matriz $G_{k\times n}$ cuyos renglones son una base para C se llama una **matriz generadora** para C.

2.1.2 Observación. Sea G una matriz generadora para el código C de tipo $[n,k]_q$. Así $C = ER(G)$, donde $ER(G)$ denota al espacio renglón de G. De aquí que $c \in C$ si, y solo si, existe $x \in \mathbb{F}_q^k$ tal que $c = xG$. Por lo tanto $C = \{xG : x \in \mathbb{F}_q^k\}$. Además, por Gauss-Jordan, se tiene que cualquier matriz generadora se puede reducir a una matriz de la forma $(I_{k\times k}|P_{k\times(n-k)})$. Así cuando hablemos de la matriz generadora para C estaremos pensando en una de la forma $(I_{k\times k}|P_{k\times(n-k)})$.

2.1.3 Lema. *Todo subespacio vectorial de $\mathbb{K}^n$ de dimensión finita sobre un campo $\mathbb{K}$ es una sicigia.*

Demostración. Sea C cualquier subespacio de dimensión k. Por lo que C tiene una base, supongamos $\{c_1,\ldots,c_k\}$ y podemos completarla a una base de $\mathbb{K}^n$ digamos $\{c_1,\ldots,c_k,c_{k+1},\ldots,c_n\}$. Además sea $e_1,\ldots,e_{n-k}$ la base canónica para $\mathbb{K}^{n-k}$; así definimos la transformación lineal $T:\mathbb{K}^n\to\mathbb{K}^{n-k}$ dada por

$$T(c_i) = \begin{cases} 0 & \text{si } i \in [k], \\ e_{i-k} & \text{si } i \in \{k+1,\ldots,n\}. \end{cases}$$

Observemos que $C = \ker(T)$. ∎

Como C es un subespacio vectorial de $\mathbb{F}_q^n$, del lema 2.1.3, existe una transformación $T:\mathbb{F}_q^n\to\mathbb{F}_q^{n-k}$. Así, tomemos a H como la matriz asociada a T con respecto a las bases canónicas, entonces $c\in C$ si, y solo si, $Hc^T = 0$. De esta forma una matriz $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ se dice **matriz de verificación de paridad** si representa un sistema de ecuaciones homogéneo cuya solución es C, es decir, si sucede que $c\in C$ si, y solo si, $Hc^T = 0$, es decir, $c \in H^\perp$.

2.1.4 Proposición. *Supongamos que C es un $[n,k]$ código. Entonces $G := (I_k|P)$ es una matriz generadora de C si, y solo si, $H := (-P^T|I_{n-k})$ es una matriz de verificación de paridad para C.*

Demostración. Para cada palabra código $c\in C$ se tiene que $c = xG$, con $x\in\mathbb{F}_q^k$. Así,

$$c = xG = (x_1,\ldots,x_k)\left(I_{k\times k}|P_{k\times(n-k)}\right) = ((x_1,\ldots,x_k)|(x_1,\ldots,x_k)P_{k\times(n-k)}) = (x,xP).$$

De esta forma para $m\in\mathbb{F}_q^k$ y $r\in F_q^{n-k}$ cualquiera:

$$\begin{aligned} c=(m,r)\in C &\iff mP = r \\ &\iff mP - r = 0 \\ &\iff (mP-r)^T = 0 \\ &\iff P^Tm^T - r^T = 0 \\ &\iff -P^Tm^T + r^T = 0 \\ &\iff -P^Tm^T + I_{n-k\times n-k}(r^T) = (-P^T,I)(m,r)^T = 0 \\ &\iff (-P^T|I_{n-k})c^T = 0. \end{aligned}$$

∎

2.1.5 Definición. Para un código C de tipo $[n,k]_q$ definimos el **código dual** como:

$$C^{\perp} := \{x \in \mathbb{F}_q^n : c \cdot x = 0, \forall\ c \in C\},$$

donde $c \cdot x$ denota al producto interno usual.

2.1.6 Teorema. *Si C es un código lineal con G una matriz generadora, entonces G es una matriz de verificación de paridad para $C^{\perp}$.*

Demostración. Por definición de código dual, $x \in C^{\perp}$ si, y solo si, $c \cdot x = 0$ para cada $c \in C$. Pero $c \in C$ si, y solo si, existe $m \in \mathbb{F}_q^k$ tal que $c = mG$, así $0 = c \cdot x = (mG)x^T$ si, y solo si, $Gx^T = 0$. ∎

Una medida natural usada en teoría de códigos es la distancia de Hamming, que mide la diferencia entre dos palabras.

Definamos $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{N}$ dada por $d((x,y)) := |\{i : x_i \neq y_i, i \in [n]\}|$, para $x = (x_1, x_2, \ldots, x_n)$ y $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$. A $d(x,y)$ se le conoce como la **distancia de Hamming**. **La mínima distancia de Hamming** de un código C de longitud n y tamaño M, se define como:

$$d(C) := \begin{cases} \text{mín}\{d(x,y) : x, y \in C, x \neq y\} & \text{si } M > 1 \\ n+1 & \text{si } M = 1. \end{cases} \tag{2.1}$$

Si agregamos la mínima distancia $d(C)$ a los parámetros del código, entonces un código $C \subset \mathbb{F}_q^n$ se denotará por $[n,k,d]_q$, donde $n, k, d \in \mathbb{N}$ y q es una potencia de un primo $p \in \mathbb{N}$ y n es la longitud, k la dimensión y d la mínima distancia de Hamming de C ; o bien cuando el campo pueda obviarse se denotará por $[n,k,d]$.

2.1.7 Definición. Para una palabra $x \in \mathbb{F}_q^n$, se define el **soporte** de x como $\text{supp}(x) := \{i : x_i \neq 0\}$ y además el **peso** de x se define como $\text{w}(x) = |\text{supp}(x)|$. El **peso mínimo** de un código C, se define como:

$$\text{mín w}(C) := \begin{cases} \text{mín}\{\text{w}(x)\} & \text{si } x \in C, x \neq 0 \\ n+1 & \text{si } x = 0. \end{cases} \tag{2.2}$$

2.1.8 Proposición. *Sea C un código lineal de dimensión $k > 0$ y $d(C)$ la mínima distancia de Hamming. Entonces $d(C) = \text{mín w}(C)$.*

Demostración. Dado que C es un código lineal, se tiene que $0 \in C$ y para cualesquiera $x, y \in C$, se tiene que $x - y \in C$, además $d(x,y) = \text{w}(x-y)$. Ahora bien,

$$d(C) = \text{mín}\, d(x,y) = \text{mín w}(x-y) = \text{mín w}(C).$$

∎

Sea C un código de tipo $[n,k]_q$, un **subcódigo** D es un subespacio lineal de C. Definamos el soporte de D como

$$\text{Supp}(D) := \{i \in [n] : \exists (x_1, x_2, \ldots, x_n) \in D, x_i \neq 0\}$$

y definimos el peso de D como $w(D) := |\text{Supp}(D)|$.

2.1.9 Definición. Dado C un código de tipo $[n,k]_q$ e $i \in [k]$, se define el **i-ésimo peso generalizado de Hamming** denotado por $d_i(C)$ como

$$d_i(C) := \text{mín}\{w(D) : D \subseteq C \text{ subcódigo}, \dim(\text{D}) = \text{i}\}.$$

Cuando el contexto lo permita d_i denotará a $d_i(C)$.

2.1.10 Observación. Si $D \subset C$ es un subcódigo, con $\dim(D) = 1$, existe $c \in C$ tal que $D =< c >$, más aún $w(D) = w(c)$.

Notemos que $d_1(C)$ es la mínima distancia de un código C, pues:

$$\text{mín } w(C) = \min_{x \in C, x \neq 0} w(x) = \min_{x \in C, x \neq 0} |\{i : x_i \neq 0\}| = \min_{<x>, x \in C} |\{i : x_i \neq 0\}| = d_1(C).$$

2.1.11 Proposición. *Para un código $C \neq 0$ de tipo $[n,k]_q$ se tiene que:*

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

Demostración. Como $C \neq 0$, $d_1(C) \geq 1$. Sea $D \subset C$ con $\dim(D) = i$, $i \geq 2$ y $w(D) = d_i(C)$. Consideremos $j \in Supp(D)$ y definamos $D_j := \{x = (x_1, \ldots, x_n) \in D : x_j = 0\}$ entonces $\dim(D_j) = i - 1$ y $d_{i-1}(C) \leq w(D_j) \leq w(D) - 1 = d_i(C) - 1$. ∎

Así, de la proposición 2.1.11 podemos llamar al conjunto $\{d_i(C) : i \in [k]\}$ como la **jerarquía de pesos de Hamming** del código C de tipo $[n,k]_q$.

Sean $A \in M_{n \times m}(\mathbb{F}_q)$ y $S \subset \text{Col}(A)$. Entonces A_S es la matriz cuyas columnas son aquellas en S.

2.1.12 Teorema. (**Wei**) *Sean C un $[n,k]_q$ código y H una matriz de verificación de paridad de C. Entonces para cada $i \in [k]$:*

$$d_i(C) = \text{mín}\{|S| \in \{1, \ldots, n\} : S \subset Col(H), |S| - rank(H_S) = i\}.$$

Demostración. Definamos $H_S^{\perp} := \{x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n : \forall i \notin S, x_i = 0 \text{ y } Hx^T = 0\}$. Por la definición de $H_S^{\perp}$ tenemos que $H_S^{\perp} \subset C$. Recordemos del teorema de la dimensión que:

$$rank(H_S) + rank(H_S^{\perp}) = |S|. \tag{2.3}$$

Denotemos por $d := \text{mín}\{|S| \in \{1, \ldots, n\} : |S| - rank(H_S) = i\}$. Sea $S \subset [n]$, con $d = |S|$ y $|S| - rank(H_S) = i$; pero $rank(H_S^{\perp}) = |S| - rank(H_S) = i$. Como $H_S^{\perp} \subset C$,

$$d_i(C) \leq w(H_S^{\perp}) \leq |S| = d. \tag{2.4}$$

Por otro lado, sea $D \subset C$ tal que $dim_{\mathbb{F}_q}(D) = i$ y $w(D) = d_i(C)$. Definamos $S := Supp(D)$, entonces $D \subseteq H_S^{\perp}$ y así $\dim(D) \leq \dim(H_S^{\perp}) = |S| - rank(H_s)$. Supongamos que $i' := \dim(H_S^{\perp}) > \dim(D) = i$. Observemos que $H_S^{\perp} \subset C$ y $\dim(H_S^{\perp})$, entonces $d_{i'} \leq |Supp(D)| = d_i(C)$. Ahora bien, de la proposición 2.1.11, $d_i(C) < d_i'(C)$. Por lo tanto $\dim(D) = \dim(H_S^{\perp})$, pero $D \subset H_S^{\perp}$, así que $D = H_S$ y $d \leq d_i(C)$; sin embargo de 2.4

obtenemos que $d = d_i(C)$. ∎

Sea C un $[n,k]_q$ código con matriz de verificación de paridad H_C, la matroide asociada a C es la matroide vector de H_C, la cual denotaremos como $\mathcal{M}_C$. Además, el ideal de Stanley-Reisner asociado al complejo de independencia de $\mathcal{M}_C$(ver definición 1.3.20), lo denotaremos como I_C y así

$$I_C = (x^\sigma : \sigma \in \mathcal{C}(\mathcal{M}_C)),$$

donde $\mathcal{C}(\mathcal{M}_C)$ son los circuitos de $\mathcal{M}_C$. Por el teorema de Wei se tiene que

$$d_i(C) = \text{mín}\{|\sigma| : \sigma \subset [n], n_{\mathcal{M}_C}(\sigma) = i\}$$

para cada $i \in [k]$, donde $n_{\mathcal{M}_C}$ es la función nulidad de la matroide $\mathcal{M}_C$; recordemos que si $r_{\mathcal{M}_C}$ es la función rango de $\mathcal{M}_C$, entonces para cada $\sigma \subset [n]$, $n_{\mathcal{M}_C}(\sigma) = |\sigma| - r_{\mathcal{M}_C}(\sigma)$ (ver sección 1.4). Así cuando $\mathcal{M} = (E, \mathcal{I})$ es una matroide y para cada $i \in [n_{\mathcal{M}}(E)] \cup \{0\}$, podemos definir

$$d_i(\mathcal{M}) := \text{mín}\{|\sigma| : \sigma \subset E, n_{\mathcal{M}}(\sigma) = i\}.$$

La definición de los pesos de Hamming generalizados para matroides apareció por primera vez en [15] y es la definición 1 de dicho artículo. Recordando de la sección 1.4 que para cada $i \in ([r(\mathcal{M}^*)]) \cup \{0\}$

$$\mathcal{N}_i := \{\sigma \subset E : n_{\mathcal{M}}(\sigma) = i,\ \sigma \text{ es minimal con respecto a esta propiedad}\},$$

de esta forma si $\sigma \subset E$ es tal que $n_{\mathcal{M}}(\sigma) = i$ y $|\sigma| = d_i$, se tiene que $\sigma \in \mathcal{N}_i$ y así

$$d_i(\mathcal{M}) = \text{mín}\{|\sigma| : \sigma \in \mathcal{N}_i\}. \tag{2.5}$$

Observemos que la definición anterior de $d_i(\mathcal{M})$ comparada con la que aparece en [15] cambia solo en la propiedad de que σ sea minimal, además no afecta en nada la nueva definición puesto $d_i(\mathcal{M})$ se alcanza cuando σ es minimal. Además recordemos por el teorema 1.4.30 que los números de Betti $\beta_{i,\sigma}$ son distintos de cero si, y sólo si, $\sigma \in \mathcal{N}_i$. En la proposición 2.1.13 se muesta más a detalle lo anterior. Recordemos que la condición de minimalidad que agregamos nos permite trabajar con retículas y en el caso del artículo [15] la minimalidad aparece de manera implícita en los circuitos irredundantes que definen en dicho artículo.

Como $\mathcal{N} = \cup_{i=0}^{n_{\mathcal{M}}(E)} \mathcal{N}_i$ forma una retícula geométrica donde el orden es la contención (ver observación 1.4.23)y así para estudiar los $d_i(\mathcal{M})$ podemos hacer uso de propiedades de las retículas geométricas, por ejemplo del hecho de que $\mathcal{N}$ es retícula geométrica deducimos de manera inmediata que $0 = d_0(\mathcal{M}) \leq d_1(\mathcal{M}) < \cdots < d_{n_{\mathcal{M}}(E)}(\mathcal{M})$. De esta forma, si C es un código, $d_0(C) = d_0(\mathcal{M}_C) = 0$.

2.1.13 Proposición. *Sea $\mathcal{M} = (E, \mathcal{I})$ una matroide y $S/I_{\mathcal{M}}$ el anillo de Stanley-Reisner asociado al complejo de independencia de $\mathcal{M}$. Entonces el peso generalizado de Hamming está dado por:*

$$d_i(\mathcal{M}) = \text{mín}\{d : \beta_{i,d}(S/I_{\mathcal{M}}) \neq 0\}.$$

Demostración. Por la ecuación 2.5, $d_i(\mathcal{M}) = \text{mín}\{|\sigma| : \sigma \in \mathcal{N}_i\}$. Además del inciso 1 del corolario 1.4.31 se tiene que para cada $d \in \mathbb{N}$, $\beta_{i,d}(S/I_{\mathcal{M}}) = \sum_{\sigma \in \mathcal{N}_i, |\sigma| = d} \beta_{i,\sigma}(S/I_{\mathcal{M}})$. Pero del teorema 1.4.30, $\beta_{i,\sigma} \neq 0$ si, y solo si, $\sigma \in \mathcal{N}_i$. Así $d_i(\mathcal{M}) = \text{mín}\{d \in \mathbb{N} : \beta_{i,d}(S/I_{\mathcal{M}}) \neq 0\}$. ∎

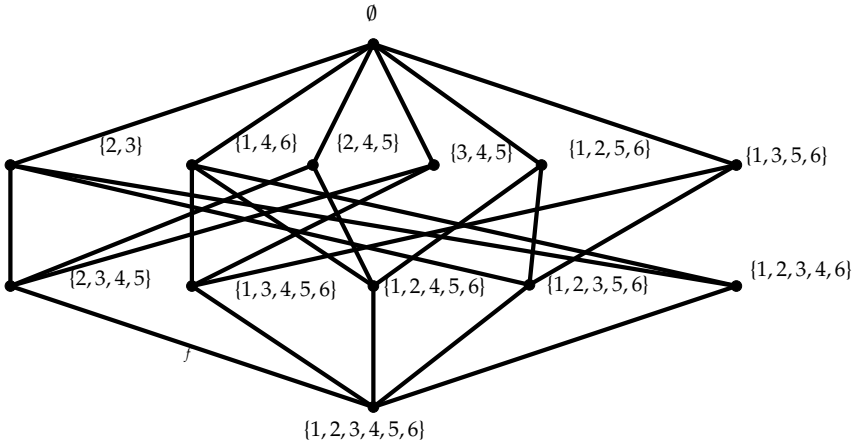

Figura 2.1:

2.1.14 Ejemplo. Sea C el código con matriz de verificación de paridad

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

Entonces, $\mathcal{C}_{\mathcal{M}_C} = \{\{2,3\},\{2,4,5\},\{3,4,5\},\{1,4,6\},\{1,2,5,6\},\{1,3,5,6\}\}$.

Ahora bien, el ideal de Stanley-Reisner y la tabla de los números de Betti de $S/I_{\mathcal{M}_C}$ son:

$$I_C = (x_2x_3, x_3x_4x_5, x_2x_4x_5, x_1x_4x_6, x_1x_2x_5x_6, x_1x_3x_5x_6),$$

$j\backslash i$	0	1	2	3
0	1	0	0	0
1	0	1	0	0
2	0	3	2	0
3	0	2	7	4

Como $d_i = \min\{i+j : \beta_{i,i+j}(S/I_{\mathcal{M}_C}) \neq 0\}$, por lo tanto $d_1(\mathcal{M}) = \min\{1+j : \beta_{1,1+j} \neq 0\}$=1+1= 2, $d_2(\mathcal{M}) = 2+2 = 4$ y $d_3(\mathcal{M}) = 3+3 = 6$. Por otro lado, de la definición de $d_i(\mathcal{M})$ (ver ecuación 2.5), es suficiente observar cada nivel del diagrama de Hasse de la retícula $\mathcal{N}(\mathcal{M}_C)$(figura 2.1), para así, obtener los valores $d_i(\mathcal{M})$. De la proposición 1.4.20 obtenemos dicha retícula a partir de calcular los cerrados de $\mathcal{M}_C^*$. Así, $d_1(\mathcal{M}) = \min\{|\sigma| : \sigma \in \mathcal{N}_1\} = |\{2,3\}| = 2$, $d_2(\mathcal{M}) = |\{2,3,4,5\}| = 4$ y $d_3(\mathcal{M}) = |\{1,2,3,4,5,6\}| = 6$. Para la tabla de los números de Betti y los cerrados de $\mathcal{M}_C^*$, hicimos uso del programa computacional Macaulay2 [11]. □

2.1.15 Proposición. *Sea C un código de tipo $[n,k]_q$ e $i \in [k]$. Entonces $d_i(C) \leq n-k+i$.*

Demostración. Supogamos que $d_i(C) > n-k+i$, como los $d_i(C)$ son una jerarquía (ver proposición 2.1.11), se tiene que $d_k(C) > n$, lo cual es una contradicción al hecho de que

$d_k(C) \leq n$. ∎

Sea C un $[n, k, d]_q$-código. Si en la proposición 2.1.15, $i = 1$, entonces $d_1(C) \leq n - k + 1$, el valor $n - k + 1$ se llama **cota de Singleton**. Ahora bien, si $d = d_1 = n - k + 1$, C es llamado un **código de distancia máxima separable** (o bien por sus siglas en inglés un **código MDS**). De hecho, si C es un código MDS, entonces para cada $i \in [k]$ se tiene que se alcanza la cota de la proposición 2.1.15, esto es, $d_i(C) = n - k + i$.

2.1.16 Proposición. *Sea C un $[n, k, d]_q$-código. Entonces C es un código MDS si, y solo si, cada k columnas de una matriz generadora G de C son linealmente independientes.*

Demostración. La matriz $G_{k\times n}$ es una matriz generadora para un código MDS si, y solo si, para cada $m \in \mathbb{F}_q^k$, mG tiene a lo más $n - d = k - 1$ coordenadas cero si, y solo si, para cada submatriz $G'_{k\times k}$ de G y $m \in \mathbb{F}_q^k$ se tiene que $mG' \neq 0$ si, y solo si, cada submatriz $G'_{k\times k}$ de G tiene rango k si, y solo si, las columnas de cada submatriz G' son linealmente independientes. ∎

2.1.17 Proposición. *Sea C un código de tipo $[n, k]_q$. Si C es un código* MDS*, entonces el código dual de C es un código MDS.*

Demostración. Se tiene que C es del tipo $[n, k, n - k + 1]$ porque C es un código MDS. Del hecho que $\dim(C^\perp) = n - \dim(C) = n - k$ y de la proposición 2.1.15 se tiene que $d(C^\perp) \leq n - \dim(C^\perp) + 1 = k + 1$. Ahora bien, supongamos que $d(C^\perp) \leq k$; entonces existe $x \in C^\perp$, $x \neq 0$, tal que $\mathrm{w}(x) \leq k$. Sea G una matriz generadora para C; por el teorema 2.1.12 existen k columnas linealmente dependientes que corresponden a las palabras x, lo cual no es posible por la proposición 2.1.16 pues C es un código MDS. De esta forma concluimos que $d(C^\perp) = n - \dim(C^\perp) + 1$. ∎

2.2. Multiplicidad

En la presente sección vamos a calcular la jerarquía de pesos de Hamming de una familia de códigos mediante la multiplicidad que sera definida posteriormente. Cabe señalar que el concepto de multiplicidad apareció como un caso particular del concepto de función de valor estudiado en el artículo de Z. Liu y W. Chen ([19]). De dichos resultados en [19] las demostraciones son omitidas o solo bosquejadas, por lo que en está sección presentamos las demostraciones para dar claridad , así como agregamos algunas proposiciones y lemas que en [19] se omitieron, pero nosotros consideramos que eran útiles para facilitar la comprensión de los conceptos y resultados aquí tratados.

2.2.1 Lema. *Sea V un espacio lineal de dimensión k en un campo $\mathbb{F}_q$. Entonces el número de subespacios de V, de dimensión r, con $0 \leq r \leq k$ es:*

$$\begin{bmatrix} k \\ r \end{bmatrix}_q := \frac{(q^k - 1)(q^k - q)(q^k - q^2)\cdots(q^k - q^{r-1})}{(q^r - 1)(q^r - q)\cdots(q^r - q^{r-1})}$$

Demostración. Construyamos una base $\beta := \{v_1, v_2, \ldots, v_r\}$ de tamaño r para V. Dado que $|V| = q^k$ y $0 \in V$ no es linealmente independiente, tenemos $q^k - 1$ maneras de elegir a v_1. Dado que $v_2 \neq \alpha v_1$ con $\alpha \in \mathbb{F} - \{0\}$, tenemos $q^k - q$ maneras de elegir a v_2 pues existen q múltiplos de v_1 ; tenemos $q^k - q^2$ maneras de elegir a v_3, dado que existen q^2 combinaciones lineales de v_1 y v_2. Y así sucesivamente podemos concluir que tenemos $q^k - q^i$ maneras de elegir a v_i. De esta forma obtenemos que existen $(q^k - 1)\cdots(q^k - q^{r-1})$ bases de tamaño r. Sin embargo no todas las bases que hemos contado nos dan un subespacio vectorial distinto; de hecho, por un argumento similar al anterior obtenemos que por cada subespacio de dimensión r existen $(q^r - 1)(q^r - q)\cdots(q^r - q^{r-1})$ bases. Aplicando la regla de la división obtenemos la conclusión del lema 2.2.1. ∎

Sea V un espacio vectorial de dimensión finita sobre un campo $\mathbb{F}_q$. Definamos la relación de equivalencia $\sim$ en $V - 0$ como:

$$u \sim v \Longleftrightarrow \exists\ \lambda \in \mathbb{F}_q - 0 \ \text{ tal que } \ u = \lambda v.$$

2.2.2 Definición. El **espacio proyectivo** asociado a V (o la proyectivización de V) es $\mathbb{P}(V) := (V - 0)/\sim$. Además $\dim(\mathbb{P}(V)) := \dim V - 1$. Sea $\mathbb{P}^{k-1}(\mathbb{F}_q)$ el espacio proyectivo de dimensión $k-1$ en el campo $\mathbb{F}_q$, es decir, $\mathbb{P}^{k-1}(\mathbb{F}_q) := \mathbb{P}(\mathbb{F}_q^k)$. Un **subespacio proyectivo** de $\mathbb{P}(V)$ es un subconjunto de la forma $\mathbb{P}(W)$ con $W \subset V$ subespacio vectorial de V.

Para un r fijo, $0 \leq r \leq k-1$, denotemos por P_r a cualquier subespacio proyectivo de $\mathbb{P}^{k-1}(\mathbb{F}_q)$ de dimensión r. Definamos N_r es el número de subespacio proyectivos de dimensión r. Así, del lema 2.2.1 y de la definición de espacio proyectivo se obtiene:

2.2.3 Proposición. *Sea $k \in \mathbb{N}$, entonces el número de subespacios proyectivos de dimensión r en $\mathbb{P}^{k-1}(\mathbb{F}_q)$ con $0 \leq r \leq k-1$ es:*

$$N_r = \frac{(q^k - 1)(q^k - q)(q^k - q^2)\cdots(q^k - q^r)}{(q^{r+1} - 1)(q^{r+1} - q)\cdots(q^{r+1} - q^r)}.$$

∎

Sea $p \in \mathbb{P}^{k-1}(\mathbb{F}_q)$ fijo. Definamos $N_{r,1} := |\{P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q) : \ \dim(P_r) = r, \mathfrak{p} \in P_r\}|$. Por la proposición 2.2.3 se tiene que:

$$N_{r,1} = \frac{(q^k - q)(q^k - q^2)\cdots(q^k - q^r)}{(q^{r+1} - q)\cdots(q^{r+1} - q^r)}. \tag{2.6}$$

También notemos que para $p_1 \in \mathbb{P}^{k-1}(\mathbb{F}_q)$, $p_1 \neq p$ se tiene de la proposición 2.2.3, que el número de subespacios de dimensión r que pasan por p y p_1 es:

$$N_{r,2} = \frac{(q^k - q^2)\ldots(q^k - q^r)}{(q^{r+1} - q^2)\ldots(q^{r+1} - q^r)}. \tag{2.7}$$

2.2.4 Observación. Sea C un código de tipo $[n,k]_q$, observemos que podemos definir una correspondencia 1-1 entre los subcódigos $D \subset C$ y los subespacios proyectivos del espacio proyectivo $\mathbb{P}^{k-1}(\mathbb{F}_q)$, denotada por g y definida por $g(D) := \mathbb{P}(D^\perp)$. Notemos que si $i \in [k] \cup \{0\}$ y $D \subset C$ con $\dim(D) = i$, entonces

$$\dim(g(D)) := \dim(\mathbb{P}(D^\perp)) = \dim(D^\perp) - 1 = (k - i) - 1.$$

Sea G una matriz generadora de un código C de tipo $[n,k]_q$. Para cada $x \in \mathbb{F}_q^k$, definimos la G-**multiplicidad** de $x \in C$ como el número de veces que x o un múltiplo $m \neq 0$ (existe $a \in \mathbb{F}_q$, tal que $m = ax$) de x aparece en las columnas de G, la cual denotaremos como $m_G(x)$. Así si $P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$, definimos $m_G(P_r) := \sum_{x \in P_r} m_G(x)$.

2.2.5 Observaciones. Sea C un código de tipo $[n,k]_q$ y G una matriz generadora para C, entonces:

1. Si G' es una matriz equivalente a G (G' se obtuvo por medio de operaciones elementales en los renglones y permutación de columnas), entonces $m_G(0) = m_{G'}(0)$.

2. $w(C) = n - m_G(0)$, pues:

$$\begin{aligned} w(C) &:= |Supp(C)| \\ &= |\{i \in [n] : \exists x = (x_1, x_2, \ldots, x_n) \in C, x_i \neq 0\}| \\ &= n - |\{i \in [n] : \forall x = (x_1, \ldots, x_n) \in C, x_i = 0\}| \\ &= n - m_G(0). \end{aligned}$$

   De esta forma obtenemos que

$$d_k := \text{mín}\{w(D) : D \subseteq C, \dim(D) = k\} = w(C) = n - m_G(0) = m_G(\mathbb{P}^{k-1}(\mathbb{F}_q)). \quad (2.8)$$

2.2.6 Lema. *Sea C un código de tipo $[n,k]_q$ y $G \in M_{k\times n}(\mathbb{F}_q)$ una matriz generadora para C. Entonces:*

1. *Si D es un subcódigo de C, tal que $\dim(D) = r \leq k$, entonces existe una matriz $B \in M_{r\times k}(\mathbb{F}_q)$ de rango r tal que $G_D = BG$ es una matriz generadora de D.*

2. *Recíprocamente, para cualquier matriz $B \in M_{r\times k}(\mathbb{F}_q)$ de rango r, entonces $D := ER(BG)$ es un subcódigo de C de dimensión r.*

Demostración.

1. Dado que $D \subset C$ es un subcódigo de $\dim(D) = r$, existe una base $\{w_1, \ldots, w_r\}$ de D tal que una matriz generadora de D es

$$G_D = \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix}_{r\times k}.$$

   Supongamos que $\{v_1, \ldots, v_k\}$ es una base para C, entonces

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & \ldots & v_{1n} \\ \vdots & & \vdots \\ v_{k1} & \cdots & v_{kn} \end{pmatrix}.$$

   Además si $e_1, \ldots, e_n$ es la base canónica de $\mathbb{F}_q^n$, entonces $v_i = v_{i1}e_1 + \cdots + v_{in}e_n$.

Como $D \subset C$, existen para cada $i \in [r]$ $b_{i1}, \ldots, b_{ik}$ tal que $w_i = b_{i1}v_1 + \cdots + b_{ik}v_k$. Definamos

$$B = \begin{pmatrix} b_{11} & \ldots & b_{1k} \\ \vdots & & \vdots \\ b_{r1} & \ldots & b_{rk} \end{pmatrix},$$

así

$$\begin{aligned} BG &= \begin{pmatrix} b_{11} & \ldots & b_{1k} \\ \vdots & & \vdots \\ b_{r1} & \ldots & b_{rk} \end{pmatrix} \begin{pmatrix} v_{11} & \ldots & v_{1n} \\ \vdots & & \vdots \\ v_{k1} & \cdots & v_{kn} \end{pmatrix} \\ &= \begin{pmatrix} b_{11}v_{1n} + \cdots + b_{1k}v_{k_1} & \ldots & b_{11}v_{1n} \cdots + b_{1k}v_{kn} \\ \vdots & & \vdots \\ b_{r1}v_{11} + \cdots + b_{rk}v_{k_1} & \cdots & b_{r1}v_{1n} + \cdots + b_{rk}v_{kn} \end{pmatrix} \\ &= \begin{pmatrix} b_{11}v_{1n}e_1 + \cdots + b_{1k}v_{k_1}e_1 + \cdots + b_{11}v_{1n}e_n \cdots + b_{1k}v_{kn}e_n \\ \vdots \\ b_{r1}v_{11}e_1 + \cdots + b_{rk}v_{k_1}e_1 + \cdots + b_{r1}v_{1n}e_n + \cdots + b_{rk}v_{kn}e_n \end{pmatrix} \\ &= \begin{pmatrix} b_{11}(v_{11}e_1 + \cdots + v_{1n}e_n) + \cdots + b_{1k}(v_{k1}e_1 + \cdots + v_{k_n}e_n) \\ \vdots \\ b_{r_1}(v_{11}e_1 + \cdots + v_{1_n}e_n) + \cdots + b_{r_k}(v_{k1}e_1 + \cdots + v_{k_n}e_n) \end{pmatrix} \\ &= \begin{pmatrix} b_{11}v_1 + \cdots + b_{1k}v_k \\ \vdots \\ b_{r_1}v_1 + \cdots + b_{r_k}v_k \end{pmatrix} \\ &= \begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix}. \end{aligned}$$

Ahora, se tiene de [14, 0.4.5(c)] que $\text{rank}(BG) \leq \text{mín}\{\text{rank}(B), \text{rank}(G)\}$. Por hipótesis $\text{rank}(BG) = r$, así $r \leq \text{rank}(B)$; pero $\text{rank}(B) \leq r$. Por lo tanto, rank(B) $= r$.

2. Sean

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & \ldots & v_{1n} \\ \vdots & & \vdots \\ v_{k1} & \cdots & v_{kn} \end{pmatrix} \text{ y } B = \begin{pmatrix} b_{11} & \ldots & b_{1k} \\ \vdots & & \vdots \\ b_{r1} & \ldots & b_{rk} \end{pmatrix}.$$

Así de los cálculos hechos en la demostración del inciso 1 de este lema se tiene que:

$$BG = \begin{pmatrix} b_{11} & \ldots & b_{1k} \\ \vdots & & \vdots \\ b_{r1} & \ldots & b_{rk} \end{pmatrix} \begin{pmatrix} v_{11} & \ldots & v_{1n} \\ \vdots & & \vdots \\ v_{k1} & \cdots & v_{kn} \end{pmatrix} = \begin{pmatrix} b_{11}v_1 + \cdots + b_{1k}v_k \\ \vdots \\ b_{r_1}v_1 + \cdots + b_{r_k}v_k \end{pmatrix}.$$

Para cada $i \in [r]$, sea w_i el i-ésimo vector renglón de la matriz BG. Observemos que $w_i \in C$, porque $v_1, \ldots, v_k$ es una base para C, pues son los renglones de la matriz generadora G de C. Supongamos que $a_1 w_1 + \cdots + a_r w_r = 0$ con $a_1, \ldots, a_r \in \mathbb{F}_q$.

$$a_1(b_{11}v_1 + \cdots + b_{1k}v_k) + \cdots + a_r(b_{r_1}v_1 + \cdots + b_{r_k}v_k) = 0$$

$$(a_1 b_{11} + \cdots + a_r b_{r_1})v_1 + \cdots + (a_1 b_{1k} + \cdots + a_r b_{rk})v_k = 0.$$

Como $v_1, \ldots, v_k$ son linealmente independientes por ser base de G,

$$\begin{aligned} a_1 b_{11} + \cdots + a_r b_{r_1} &= 0 \\ &\vdots \\ a_1 b_{1k} + \cdots + a_r b_{rk} &= 0. \end{aligned}$$

Pero como B es de rango r, $a_1 = \cdots = a_r = 0$. Entonces $w_1, \ldots, w_r$ son linealmente independientes. De esta forma hemos demostrado que BG es una matriz generadora para el subcódigo $D := ER(BG) \subset C$. ∎

2.2.7 Lema. *Sean C un código de tipo $[n,k]_q$, G una matriz generadora de C e $i \leq k$. Si $D \subset C$ es un subcódigo, entonces $w(D) = d_k - m_G(\mathbb{P}(D^\perp))$; y así*

$$d_i = d_k - \text{máx}\{m_G(P_{k-i-1}) : P_{k-i-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q)\}.$$

Demostración. Del lema 2.2.6 existe $B \in M_{r\times k}(\mathbb{F}_q)$, tal que $G_D := BG$ es una matriz generadora para D. Así, del inciso 2 de las observaciones 2.2.5 $w(D) = n - m_{G_D}(0)$. Ahora bien,

$$\begin{aligned} m_{G_D}(0) &:= |\{i \in [n] : v_i \in \text{Col}(G_D), v_i = 0\}| \\ &= |\{i \in [n] : v_i \in \text{Col}(G_D), Bv_i = 0\}| \\ &= \sum_{\substack{p \in \mathbb{P}^{k-1}(\mathbb{F}_q), \\ Bp^T = 0}} m_G(p) + m_G(0) \\ &= \sum_{p \in \mathbb{P}(B^\perp)} m_G(p) + m_G(0) \\ &= \sum_{p \in \mathbb{P}(D^\perp)} m_G(p) + m_G(0) \\ &= m_G(\mathbb{P}(D^\perp)) + m_G(0). \end{aligned}$$

Entonces $w(D) = n - (m_G(\mathbb{P}(D^\perp)) + m_G(0)) = (n - m_G(0)) - m_G(\mathbb{P}(D^\perp)) = d_k - m_G(\mathbb{P}(D^\perp))$, donde la útlima igualdad se tiene de 2.8. Por otra parte,

$$\begin{aligned} d_i &= \text{mín}\{w(D) : D \subset C, \dim(D) = i\} \\ &= \text{mín}\{d_k - m_G(\mathbb{P}(D^\perp)) : D \subset C, \dim(D) = i\} \\ &= d_k - \text{máx}\{m_G(\mathbb{P}(D^\perp)) : D \subset C, \dim(D) = i\}. \end{aligned}$$

De la observación 2.2.4, dado un subcódigo $D \subset C$ de $\dim(D) = i$, la asignación $g(D) = \mathbb{P}(D^\perp)$ define una biyección entre los subcódigos de dimensión i de C con los subespacios proyectivos de dimensión $k - i - 1$ de $\mathbb{P}^{k-1}(\mathbb{F}_q)$, entonces

$$\begin{aligned} d_i &= d_k - \text{máx}\{m_G(\mathbb{P}(D^\perp)) : D \subset C, \dim(D) = i\} \\ &= d_k - \text{máx}\{m_G(P_{k-i-1}) : P_{k-i-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q)\}. \end{aligned}$$

■

Del lema 2.2.7, para $i \leq k$, se tiene que:

$$d_k - d_{k-i-1} = \text{máx}\{m_G(P_i) : P_i \subset \mathbb{P}^{k-1}(\mathbb{F}_q), \dim(P_i) = i\}. \tag{2.9}$$

Sean C un código de tipo $[n,k]_q$ y G una matriz generadora para C. Definamos lo siguiente:

1. $B_s^j := |\{D \subset C | \dim(D) = s \ , w(D) = j\}|$ para $s \in [k] \cup \{0\}$ y $j \in [n+1]$;

2. $\gamma_r := \text{mín}\{m_G(P_r) | P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q), \dim(P_r) = r\}$ para $r \in [k-1] \cup \{0\}$;

3. $\Gamma_r := \text{máx}\{m_G(P_r) | P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q)\}$ para $r \in [k-1] \cup \{0\}$;

4. $A_r^i := |\{P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q) : m_G(P_r) = i\}|$ para para $r \in [k-1] \cup \{0\}$ e $i \in [n] \cup 0$.

2.2.8 Observación. Por la correspondencia 1-1 que existe entre los subcódigos D de C con $\dim(D) = s$ y los subespacios proyectivos de $\mathbb{P}^{k-1}(\mathbb{F}_q)$ de dimensión $k-s-1$ (ver observación 2.2.4); y además del lema 2.2.7, $m_G(\mathbb{P}(D^\perp)) = d_k - w(D)$, donde G es una matriz generadora para C, se tiene:

$$\begin{aligned} B_s^j &= |\{D \subset C | \dim(D) = s \ , w(D) = j\}| \\ &= |\{P_{k-s-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q) : m_G(P_{k-s-1}) = d_k - j\}| \\ &= A_{k-s-1}^{d_k - j}. \end{aligned}$$

2.2.9 Lema. ([19, lema 1]) *Sean C un código de tipo $[n,k]_q$ y G una matriz generadora para C. Dado $r \in [k-1] \cup \{0\}$, se tiene que:*

$$\sum_{i=\gamma_r}^{\Gamma_r} A_r^i = N_r \ y \ \sum_{i=\gamma_r}^{\Gamma_r} i A_r^i = N_{r,1} m_G(\mathbb{P}^{k-1}(\mathbb{F}_q)) = N_{r,1} d_k.$$

En particular, si $\gamma_r = \Gamma_r$, $\gamma_r A_r^{\gamma_r} = \gamma_r N_r = N_{r,1} d_k$ y así, $d_k = \dfrac{q^k - 1}{q^{r+1} - 1} \gamma_r$.

Demostración. De la definición de A_r^i se sigue que $\displaystyle\sum_{i=\gamma_r}^{\Gamma_r} A_r^i = N_r$. Ahora bien,

$$\begin{aligned} \sum_{i=\gamma_r}^{\Gamma_r} i A_r^i &= \sum_{i=\gamma_r}^{\Gamma_r} i(|\{P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q) : m_G(P_r) = i\}|) \\ &= \sum_{i=\gamma_r}^{\Gamma_r} \sum_{\substack{P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q), \\ m_G(P_r) = i}} m_G(P_r) \end{aligned}$$

$$\begin{aligned}
\sum_{i=\gamma_r}^{\Gamma_r} iA_r^i &= \sum_{i=\gamma_r}^{\Gamma_r} \sum_{\substack{P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q) \\ m_G(P_r)=i}} m_G(P_r) \\
&= \sum_{i=\gamma_r}^{\Gamma_r} \sum_{\substack{P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q) \\ m_G(P_r)=i}} \sum_{p\in P_r} m_G(p) \\
&= \sum_{P_r\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} \sum_{p\in P_r} m_G(p) \\
&= N_{r,1} \sum_{p\in\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(p) \\
&= N_{r,1} \sum_{p\in\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(p) \\
&= N_{r,1}(m_G(\mathbb{P}^{k-1}(\mathbb{F}_q))) \\
&= N_{r,1}d_k,
\end{aligned}$$

donde la última igualdad se debe al inciso 2. de la observación 2.2.5. En particular, si $\gamma_r = \Gamma_r$, $\gamma_r A_r^{\gamma_r} = \gamma_r N_r = N_{r,1}d_k$. Así,

$$d_k = \frac{\gamma_r N_r}{N_{r,1}} = \gamma_r \frac{\dfrac{(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^r)}{(q^{r+1}-1)(q^{r+1}-q)\cdots(q^{r+1}-q^r)}}{\dfrac{(q^k-q)(q^k-q^2)\cdots(q^k-q^r)}{(q^{r+1}-q)\cdots(q^{r+1}-q^r)}} = \gamma_r \frac{q^k-1}{q^{r+1}-1}.$$

Donde la última igualdad se debe a la proposición 2.2.3 y a la ecuación 2.6. ∎

2.2.10 Proposición. ([19, lema 2]) *Sea C un código de tipo $[n,k]_q$ y G una matriz generadora para C. Para algún $i \in [k-2]\cup\{0\}$, supongamos que $m_G(P_i) = \gamma_i$ para cada subespacio proyectivo de dimensión i. Entonces $m_G(p) = \frac{q-1}{q^{i+1}-1}\gamma_i$ para cada $p \in \mathbb{P}^{k-1}(\mathbb{F}_q)$.*

Demostración. Si $i = 0$, por hipótesis $m_G(P_0) = \gamma_0$, pero los subespacios de dimensión cero son los puntos $p \in \mathbb{P}^{k-1}(\mathbb{F}_q)$, por lo tanto, $m_G(p) = \gamma_0 = \frac{q-1}{q^{0+1}-1}\gamma_0$ para cada $p \in \mathbb{P}^{k-1}(\mathbb{F}_q)$. Ahora bien, si $i = 1$, recordemos N_1 y $N_{1,1}$ de la proposición 2.2.3 y la ecuación 2.6. Entonces se tiene que

$$\begin{aligned}
N_{1,1}\gamma_1 &= N_{1,1}m_G(P_1) \\
&= \textstyle\sum_{p\in P_1, P_1\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(P_1) \\
&= \textstyle\sum_{p\in P_1, P_1\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} (m_G(p) + \sum_{p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q), p_1\neq p} m_G(p_1)).
\end{aligned}$$

Entonces:

$$N_{1,1}\gamma_1 = \sum_{p\in P_1,\ P_1\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} (m_G(p) + \sum_{p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q),\ p_1\neq p} m_G(p_1)) = N_{1,1}m_G(p) + \sum_{p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q),\ p_1\neq p} m_G(p_1).$$

Así $(N_{1,1}-1)m_G(p)+\sum_{p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(p_1) = N_{1,1}\gamma_1$. Del lema 2.2.9 se tiene que $\frac{\gamma_1 N_1}{N_{1,1}} = d_k = \sum_{p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(p_1) = N_{1,1}d_k$ y $d_k = \dfrac{q^k-1}{q^2-1}\gamma_1$. Por lo tanto,

$$
\begin{aligned}
m_G(p) &= \frac{N_{1,1}\gamma_1 - \left(\dfrac{\gamma_1 N_1}{N_{1,1}}\right)}{(N_{1,1}-1)} \\
&= \frac{\dfrac{q^k-q}{q^2-q}\gamma_1 - \dfrac{q^k-1}{q^2-1}\gamma_1}{\dfrac{q^k-q}{q^2-q}-1} \\
&= \left(\frac{\dfrac{q^k-q}{q^2-q} - \dfrac{q^k-1}{q^2-1}}{\dfrac{q^k-q}{q^2-q}-1}\right)\gamma_1 \\
&= \left(\frac{\dfrac{(q^2-1)(q^k-q)-(q^2-q)(q^k-1)}{(q^2-q)(q^2-1)}}{\dfrac{(q^k-q)-(q^2-q)}{(q^2-q)}}\right)\gamma_1 \\
&= \left(\frac{(q^2-1)(q^k-q)-(q^2-q)(q^k-1)}{(q^2-1)(q^k-q^2)}\right)\gamma_1 \\
&= \left(\frac{q^2q^k-q^3-q^k+q-q^2q^k+q^2+qq^k-q}{(q^2-1)(q^k-q^2)}\right)\gamma_1 \\
&= \left(\frac{-q^3-q^k+q^2+qq^k}{(q^2-1)(q^k-q^2)}\right)\gamma_1 \\
m_G(p) &= \left(\frac{(q-1)(q^k-q^2)}{(q^2-1)(q^k-q^2)}\right)\gamma_1 \\
&= \left(\frac{q-1}{q^2-1}\right)\gamma_1.
\end{aligned}
$$

Si $i\geq 2$, recordemos a $N_{i,1}$ y $N_{i,2}$ de la ecuación 2.6 y de la ecuación 2.7. Así,

$$
\begin{aligned}
N_{i,1}\gamma_i &= N_{i,1}m_G(P_i) \\
&= \textstyle\sum_{p\in P_i, P_i\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(P_i) \\
&= \textstyle\sum_{p\in P_i, P_i\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} \sum_{p_1\in P_i} m_G(p_1) \\
&= \textstyle\sum_{p\in P_i, P_i\subset\mathbb{P}^{k-1}(\mathbb{F}_q)} \left(m_G(p) + \sum_{p_1\neq p, p_1\in P_i} m_G(p_1)\right) \\
&= N_{i,1}m_G(p) + N_{i,2}\textstyle\sum_{p_1\neq p, p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q)} m_G(p_1).
\end{aligned}
$$

Por lo tanto, $N_{i,1}\gamma_i = (N_{i,1} - N_{i,2})m(p) + N_{i,2}\sum_{p_1\in\mathbb{P}^{k-1}}(\mathbb{F}_q)m(p_1)$. Del lema 2.2.9 se tiene que $\frac{\gamma_i N_i}{N_{i,1}} = d_k = \sum_{p_1\in\mathbb{P}^{k-1}(\mathbb{F}_q)} m(p_1) = N_{r,1}d_k$ y $d_k = \dfrac{q^k-1}{q^{i+1}-1}\gamma_i$. Entonces

$$(N_{i,1} - N_{i,2})m(p) + \gamma_i\frac{N_{i,2}N_i}{N_{i,1}} = N_{i,1}\gamma_i, \text{ así,}$$

$$\begin{aligned}
m(p) &= \left(\frac{N_{i,1} - N_{i,2}\frac{N_i}{N_{i,1}}}{(N_{i,1} - N_{i,2})}\right)\gamma_i \\
&= \left(\frac{\dfrac{(q^k-q)\dots(q^k-q^i)}{(q^{i+1}-q)\dots(q^{i+1}-q^i)} - \dfrac{(q^k-q^2)\dots(q^k-q^i)}{(q^{i+1}-q^2)\dots(q^{i+1}-q^i)}\left(\dfrac{q^k-1}{q^{i+1}-1}\right)}{\dfrac{(q^k-q)(q^k-q^2)\dots(q^k-q^i)}{(q^{i+1}-q)\dots(q^{i+1}-q^i)} - \dfrac{(q^k-q^2)\dots(q^k-q^i)}{(q^{i+1}-q^2)\dots(q^{i+1}-q^i)}}\right)\gamma_i \\
&= \left(\frac{\dfrac{(q^i+1)(q^k-q)\dots(q^k-q^i) - (q^{i+1}-q)(q^k-1)(q^k-q^2)\dots(q^k-q^i)}{(q^{i+1}-1)(q^{i+1}-q)\dots(q^{i+1}-q^i)}}{\dfrac{(q^k-q)(q^k-q^2)\dots(q^k-q^i) - (q^{i+1}-q)(q^k-q^2)\dots(q^k-q^i)}{(q^{i+1}-q)\dots(q^{i+1}-q^i)}}\right)\gamma_i \\
&= \left(\frac{(q^i+1)(q^k-q)\dots(q^k-q^i) - (q^{i+1}-q)(q^k-1)(q^k-q^2)\dots(q^k-q^i)}{(q^{i+1}-1)\left((q^k-q)(q^k-q^2)\dots(q^k-q^i) - (q^{i+1}-q)(q^k-q^2)\dots(q^k-q^i)\right)}\right)\gamma_i \\
&= \left(\frac{(q^k-q^2)\dots(q^k-q^i)\left[(q^{i+1}-1)(q^k-q) - (q^{i+1}-q)(q^k-1)\right]}{(q^k-q^2)\dots(q^k-q^i)\left[(q^{i+1}-1)(q^k-q) - (q^{i+1}-1)(q^{i+1}-q)\right]}\right)\gamma_i \\
&= \left(\frac{(q^k-q^{i+1})(q-1)}{(q^{i+1}-1)(q^k-q^{i+1})}\right)\gamma_i \\
&= \left(\frac{(q-1)}{(q^{i+1}-1)}\right)\gamma_i.
\end{aligned}$$

■

2.2.11 Corolario. ([19, corolario 2]) *Sea C un código de tipo $[n,k]_q$ y G una matriz generadora para C. Supongamos que existe un $r \in [k-2]\cup\{0\}$ tal que para cada $P_r \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$, $m(P_r) = \gamma_r$. Entonces para cada subespacio proyectivo P_s con $\dim(P_s) = s$, $m_G(P_s) = \dfrac{q^{s+1}-1}{q^{r+1}-1}(\gamma_r)$, para $s \in [k-1]\cup\{0\}$.*

Demostración. Por definición $m_G(P_s) = \sum_{p\in P_s} m_G(p)$. El número de puntos $p \in P_s$, por la proposición 2.2.3 es $\frac{q^{s+1}-1}{q-1}$; y de la proposición 2.2.10, $m_G(p) = \frac{q-1}{q^{r+1}-1}\gamma_r$. Así

$$m_G(P_s) = \sum_{p\in P_s} m_G(p) = \left(\frac{q^{s+1}-1}{q-1}\right)\left(\frac{q-1}{q^{r+1}-1}\gamma_r\right) = \frac{q^{s+1}-1}{q^{r+1}-1}\gamma_r.$$

■

2.2.12 Proposición. ([19, corolario 3]) *Sea C un código de tipo $[n,k]_q$ y G una matriz generadora para C. Entonces*

$$\sum_{j=d_s}^{d_k}(d_k-j)B_s^j = N_{k-s-1,1}d_k \text{ y } \sum_{j=d_s}^{d_k}B_s^j = N_{k-s-1}.$$

Demostración. Del lema 2.2.7 se tiene que para cada $j \in [k]$

$$d_j = d_k - \text{máx}\{m_G(\mathbb{P}(D^\perp) : D \subset C, \dim(D) = j\}.$$

Por lo tanto,

$$\Gamma_{k-j-1} = \text{máx}\{m_G(P_{k-j-1})|P_{k-j-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q), \dim(P_{k-s-1}) = k-s-1\} = d_k - d_j. \quad (2.10)$$

De esta forma, de la ecuación (2.10) y de la observación 2.2.8

$$\begin{aligned}\sum_{j=d_s}^{d_k}(d_k-j)B_s^j &= \sum_{j=d_s}^{d_k}(d_k-j)A_{k-s-1}^{dk-d_j}\\ &= \sum_{i=0}^{d_k-d_s} iA_{k-s-1}^i\\ &= \sum_{i=\gamma_{k-s-1}}^{\Gamma_{k-s-1}} iA_{k-s-1}^i.\end{aligned}$$

Del lema 2.2.9 se tiene que $\sum_{j=d_s}^{d_k}(d_k-j)B_s^j = N_{k-s-1,1}(d_k)$. Por otro lado, de la observación 2.2.8 y de la ecuación 2.10 se tiene que:

$$\begin{aligned}\sum_{j=d_s}^{d_k}B_s^j &= \sum_{j=d_S}^{d_k}A_{k-s-1}^{d_k-j}.\\ &= \sum_{i=\gamma_{k-s-1}}^{\Gamma_{k-s-1}}A_{k-s-1}^i.\end{aligned}$$

Por lo tanto, del lema 2.2.9, $\sum_{j=d_s}^{d_k}B_s^j = N_{k-s-1}$. ∎

2.2.13 Teorema. ([19, teorema 1]) *Sea C un código de tipo $[n,k]_q$. Supongamos que para algún $s \in [k-1]$, cada $D_s \subseteq C$ con $\dim(D_s) = s$, $w(D_s) = d_s$. Entonces para cada $t \in [k] \cup \{0\}$, subcódigo $D_t \subset C$ con $\dim(D) = t$ se tiene que $w(D_t) = d_t$. Mas aún*

$$w(D_t) = d_t = \frac{q^k - q^{k-t}}{q^k - q^{k-s}}(w(D_s)) = \frac{q^k - q^{k-t}}{q^k - q^{k-s}}(d_s).$$

Demostración. Sea G una matriz generadora para C. Del lema 2.2.7,

$$d_k - m_G(\mathbb{P}(D_s^\perp)) = w(D_s) = d_s.$$

Así de la observación 2.2.4 todos los subespacios proyectivos $P_{k-s-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$ tienen la misma multiplicidad, es decir, $m_G(P_{k-s-1}) = d_k - d_s$. Además de la observación 2.2.8 y de la definición de B_s^j se tiene que $B_s^{d_s} = N_{k-s-1}$ y $B_s^j = 0$, para cada $j \neq d_s$. Ahora bien, por la proposición 2.2.12, $(d_k - d_S)N_{k-s-1} = N_{k-s-1,1}(d_k)$.

Por otra parte, como $m(\mathbb{P}^{k-1}(\mathbb{F}_q)) = d_k$ y por el lema 2.2.9,

$$d_k = \frac{q^k - 1}{q^k - q^{k-s}}(d_s). \tag{2.11}$$

Ahora bien, dado que cada subespacio proyectivo $P_{k-s-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$ tiene la misma multiplicidad, es decir, $m_G(P_{k-s-1}) = d_k - d_s$, se tiene del corolario 2.2.11 que para cada cada subespacio proyectivo $P_{k-t-1} \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$, donde $t \in [k-1] \cup \{0\}$:

$$d_k - d_t = m_G(P_{k-t-1}) = \frac{q^{k-t} - 1}{q^{k-s} - 1}(d_k - d_s). \tag{2.12}$$

De 2.11 y 2.12 se tiene que:

$$\begin{aligned}
d_t &= d_k - \frac{q^{k-t} - 1}{q^{k-s} - 1}(d_k - d_s) \\
&= \frac{q^k - 1}{q^k - q^{k-s}}(d_s) - \frac{q^{k-t} - 1}{q^{k-s} - 1}\left(\frac{q^k - 1}{q^k - q^{k-s}}(d_s) - d_s\right) \\
&= \left(\frac{q^k - 1}{q^k - q^{k-s}} - \frac{q^{k-t} - 1}{q^{k-s} - 1}\left(\frac{q^k - 1}{q^k - q^{k-s}}\right) + \frac{q^{k-t} - 1}{q^{k-s} - 1}\right) d_s \\
&= \left(\frac{q^{k+k-s} + q^{k-t} - q^{k-t+k-s} - q^k}{(q^k - q^{k-s})(q^{k-s} - 1)}\right) d_s \\
&= \left(\frac{(q^k - q^{k-t})(q^{k-s} - 1)}{(q^k - q^{k-s})(q^{k-s} - 1)}\right) d_s \\
&= \left(\frac{(q^k - q^{k-t})}{(q^k - q^{k-s})}\right) d_s.
\end{aligned}$$

■

De la observación 2.1.10; notemos que todos los subcódigos $D \subset C$, con $\dim(D) = 1$, tienen $w(D) = d_1$ si, y solo si, todas las palabras código $c \in C$, $c \neq 0$, $w(c) = d_1$.

2.2.14 Definición. *Sea C un código, si para cada $c \in C$, $c \neq 0$ se tiene que $w(c) = d \in \mathbb{N}$, decimos que C es un* ***código de peso constante****.*

2.2.15 Corolario. ([16, corolario 1]) *Sea C un $[n,k]_q$-código, si C es un código de peso constante d, entonces $d_i = d\dfrac{q^i - 1}{q^{i-1}(q-1)}$ para $i \in [k]$.*

Demostración. Como para cada $c \in C$, $w(c) = d$ y el espacio generado por c es un subespacio de dimensión 1, por lo que del teorema 2.2.13 para $i \in [k]$, se tiene que:

$$\begin{aligned} d_i &= d\frac{q^k - q^{k-i}}{q^k - q^{k-1}} \\ &= d\frac{q^k(1-q^{-i})}{q^k(1-q^{-1})} \\ &= d\frac{(1-\frac{1}{q^i})}{(1-\frac{1}{q})} \\ &= d\left(\frac{\frac{q^i-1}{q^i}}{\frac{q-1}{q}}\right) \\ &= d\frac{q(q^i-1)}{(q-1)q^i} \\ &= d\frac{q(q^i-1)}{q(q^i-q^{i-1})} \\ &= d\frac{q^i-1}{q^{i-1}(q-1)}. \end{aligned}$$

■

Sean $n = (q^r - 1)/(q-1)$ y $H_r^q \in M_{r\times n}(\mathbb{F}_q)$ con columnas no cero para cada $q \in \mathbb{N}$ y $r \in \mathbb{N}$, tal que no existen dos columnas dependientes. Al código que tiene a H_r^q como matriz de verificación de paridad es llamado **código q-ario de Hamming** y lo denotamos como $\mathcal{H}_r^q$ y al código que tiene a H_r^q como matriz generadora se le conoce como **código q-ario simple,** el cual denotamos como S_r^q. Notemos que los códigos $\mathcal{H}_r^q$ y S_r^q, son duales, por definición.

2.2.16 Proposición. ([17, proposición 5.7]) *Sean $r \geq 2$ y $n = (q^r - 1)/(q-1)$. Entonces el código de Hammming $\mathcal{H}_r^q$ es un $[n, n-r, 3]$ código.*

Demostración. El rango de la matriz H_r^q es r, por lo tanto $H_r(q)$ es la matriz de verificación de paridad de un código de codimensión r; además, por definición $r = n - \dim(H_r^q)$, así tenemos que $k := \dim(H_r^q) = n - r$. Por definición $r = n - k$, por lo tanto, $k = n - r$. Ahora bien por definición cualesquiera dos columnas son linealmente independientes y una columna de peso 2 es una combinación lineal de dos columnas de peso 1, por lo que existen tales tres columnas puesto que $r \geq 2$. La mínima distancia es 3 por el teorema 2.1.12. ■

2.2.17 Ejemplo. Sea $\mathcal{H}_2^3$ un código q-ario de Hamming del tipo $[4, 2]$; así una matriz de verificación de paridad es:

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

Por ser un código de q-ario de Hamming, $d_1 = 3$. Ahora bien, como $c \in H_2^3$ si, y solo si, $Hc^T = 0$, entonces las palabras del código H_2^3 son: $(0,0,0,0), (0,1,1,1), (0,2,2,2), (1,0,1,2)$, $(2,0,2,1), (1,1,2,0), (2,2,1,0), (1,2,0,1), (2,1,0,2)$. Notemos que el peso de todas las palabras distintas de cero es 3, por lo tanto $\mathcal{H}_2^3$ es un código de peso constante. Así, por el corolario 2.2.15, $d_2 = 3(\frac{3^2-1}{3^{2-1}(3-1)}) = 3(\frac{8}{6}) = 4$. □

El siguiente resultado nos da un ejemplo de una familia de códigos de peso constante.

2.2.18 Proposición. ([17, proposición 5.8]) *Sean* $n = \frac{q^r-1}{q-1}$ *y* $r \in \mathbb{N}$*, el código* S_r^q *de tipo* $[n, r]_q$ *es un código de peso constante.*

Demostración. Sea $c = (c_1, \ldots, c_j, \ldots, c_n) \in S_r^q$, $c \neq 0$ si, y solo si, existe $m \in \mathbb{F}_q^r$ tal que $c = mH_r^q$. Ahora bien, $c_j = 0$ si, y solo si, $mh_j = 0$, donde h_j es la j-ésima columna de H_r^q. Así buscamos el número de soluciones de x en la ecuación $mx = 0$. Notemos que $mx = 0$ es una ecuación homogénea y no trivial (no hay columna cero). La ecuación $mx = 0$ tiene q^{r-1} soluciones puesto que se necesitan q^{r-1} soluciones para determinar a las otras. Pero como no hay columna cero entonces exiten $q^{r-1}-1$ soluciones. Ahora bien, hay que quitar aquellas que sean linealmente dependientes, entonces existe $\frac{q^{r-1}-1}{q-1}$ soluciones. Como para cada $c = (c_1, \ldots, c_n)$, $w(c) = |j : c_j \neq 0| = n - |j : c_j = 0|$ y $n = \frac{q^r-1}{q-1}$. Entonces cada $c = (c_1, \ldots, c_n) \in S_r^q$ tiene peso q^{r-1}, puesto que $n - \frac{q^{r-1}-1}{q-1} = \frac{q^r-1-q^{r-1}-1}{q-1} = \frac{q^r-q^{r-1}}{q-1} = \frac{q^{r-1}(q-1)}{q-1} = q^{r-1}$. ∎

Por la proposición anterior 2.2.18 se tiene que un código S_r^q simple de tipo $[n, r]_q$ es un código de peso constante $d = q^{r-1}$, por lo tanto, S_r^q es un código de tipo $[\frac{q^r-1}{q-1}, r, q^{r-1}]_q$. Así, del corolario 2.2.15 se tiene que la jerarquía de pesos generalizados de Hammming es

$$d_i(S_r^q) = (q^{r-1})\frac{q^i - 1}{q^{i-1}(q-1)} \text{ para } i \in [k].$$

2.3. Resoluciones libres minimales de códigos de peso constante

En esta sección daremos una caracterización de un código de peso constante C a través de los números de Betti de $S/I_{\mathcal{M}}$, el cual es el teorema 2.3.3, así como también el recíproco que esta enunciado en la proposición 2.3.5. Recordemos que para cualquier código C existe una matroide $\mathcal{M}_C$, la cual es la asociada a la matriz de verificación de paridad del código, además $r(\mathcal{M}_C^*)$ denota el rango de la matroide dual de $\mathcal{M}$ y para cada $i \in ([r(\mathcal{M}_C^*)]) \cup \{0\}$,

$$\mathcal{N}_i := \{\sigma \subset E : n_{\mathcal{M}_C}(\sigma) = i,\ \sigma \text{ es minimal con respecto a esta propiedad}\}.$$

Cabe señalar que en el teorema 2.3.3 la diferencia de la demostración en gran parte radica en el hecho de la diferencia de la definición $\mathcal{N}_i$ cuando agregamos minimalidad. La siguiente proposición la demostramos de manera diferente a la que se puede consultar en el ([16, lema 1]), dicha diferencia como se ha estado diciendo se debe a la minimalidad de $\sigma \in \mathcal{N}_i$, dado que ellos la minimalidad la manejan implícitamente en los circuitos irredundantes y nosotros como se puede consultar en la demostración de la proposición 2.3.1 .

2.3.1 Proposición. *Sean* C *un código de tipo* $[n, k]_q$*,* $\sigma \in \mathcal{N}_i$ *con* $i \in [k]$ *y* H *una matriz de verificación de paridad de* C*. Entonces existe un subcódigo* $C' \subset C$ *con* $\dim(C') = i$ *tal que* $\sigma = supp(C')$*.*

Demostración.

$$H_\sigma^\perp := \{v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n : v_i = 0 \text{ si } i \notin \sigma, Hv^T = 0\}.$$

Pero $i = n_{\mathcal{M}}(\sigma) = \dim(H_\sigma^\perp)$. Entonces $H_\sigma^\perp \subset C$, $\dim(H_\sigma^\perp) = i$ y $Supp(H_\sigma^\perp) \subset \sigma$. Llamemos $\gamma := Supp(H_\sigma^\perp)$, por lo tanto, $\gamma \subseteq \sigma$. Observemos que $H_\gamma^\perp = H_\sigma^\perp$, así:

$$n_{\mathcal{M}}(\gamma) = n_{\mathcal{M}}(H_\gamma^\perp) = n_{\mathcal{M}}(H_\sigma^\perp) = n_{\mathcal{M}}(\sigma) = i. \text{ Como } \sigma \in \mathcal{N}_i, \gamma = \sigma.$$

■

2.3.2 Corolario. *Sea C un código, H una matriz de verificación de paridad y $\mathcal{M}_C = \mathcal{M}[H]$ la matroide asociada a C. Entonces para cada $\sigma \in \mathcal{C}(\mathcal{M}_C)$, existe $c \in C$ tal que $\sigma = supp(c)$.*

Demostración. Como de la observación 1.4.21, $\mathcal{C}(\mathcal{M}_C) = \mathcal{N}_1(\mathcal{M}_C)$, por la proposición 2.3.1 se obtiene el resultado deseado. ■

Recordemos que el peso generalizado de una matroide esta dado por $d_i = \text{mín}\{|\sigma| : \sigma \in \mathcal{N}_i\}$ para $i \in [r^*(\mathcal{M})] \cup \{0\}$.

El siguiente teorema es una serie de resultados presentados por T. Johnsen y H. Verdure, los cuales son el corolario 3 y el teorema 2 de [16]. En está tesis lo demostramos de manera diferente, sin la necesidad de usar circuitos irredundantes. Dado que el corolario 3 dice que todos los elementos de nulidad i tienen la misma cardinalidad d_i, así pues el inciso 1 esta justificado, puesto que de manera particular los elementos minimales con dicha nulidad cumplen esa condición. La demostración que nosotros presentamos del inciso 2 del siguiente teorema se basa en resultados del álgebra conmutativa como lo son la dimensión proyectiva y el ser Cohen-Macaulay, así como el teorema 1.2.8 (ver [6]). Por otro lado, la demostración en [16] parte de parametrizar a partir de una Grassmaniana todos los subcódigos de cierta dimensión de un código.

2.3.3 Teorema. ([16, corolario 3] y [16, teorema 2]) *Sea C un $[n,k]_q$-código de peso constante. Entonces:*

1. *Todos los elementos en $\mathcal{N}_i$ tienen la misma cardinalidad d_i.*

2. *La resolución libre minimal graduada estándar de $S/I_{\mathcal{M}_C}$ es pura y es de la forma*

$$0 \to \cdots \to S(-d_i)^{\begin{bmatrix} k \\ i \end{bmatrix}_q^{(q^{\frac{i(i-1)}{2}})}} \to \cdots \to S \to S/\mathcal{I}_{\mathcal{M}} \to 0,$$

donde $d_i = d\frac{q^i-1}{q^{i-1}(q-1)}$.

Demostración.

1. Para cada $\sigma \in N_i$ se tiene por la proposición 2.3.1 que existe un subcódigo $C'_\sigma \subset C$ de $\dim(C'_\sigma) = i$ tal que $|\sigma| = |Supp(C'_\sigma)| = w(C'_\sigma)$. Pero del teorema 2.2.13 se tiene que todos los subcódigos de dimensión i tienen peso constante, digamos $w(C') = w$. Así en particular $w = w(C'_\sigma) = |\sigma|$.

2. Del teorema 1.4.30 se tiene que la resolución es pura, además $S/I_{\mathcal{M}}$ es Cohen-Macaulay dado que por 1.4.31(2), $\text{dimproj}(S/I_M) = |E| - r(\mathcal{M})$. Entonces, del teorema 1.2.8 se

tiene:

$$\begin{aligned}
\beta_i &= (-1)^{i+1}\prod_{j\neq i}\frac{d_j}{d_j-d_i}\\
&= (-1)^{i+1}\prod_{j\neq i}\frac{d_{\frac{q^j-1}{q^{j-1}(q-1)}}}{d_{\frac{q^j-1}{q^{j-1}(q-1)}}-d_{\frac{q^i-1}{q^{i-1}(q-1)}}}\\
&= (-1)^{i+1}\prod_{j=1}^{i-1}\frac{\frac{q^j-1}{q^{j-1}(q-1)}}{\frac{(q^j-1)q^{i-j}-(q^i-1)}{q^{i-1}(q-1)}}\prod_{j=i+1}^{k}\frac{\frac{q^j-1}{q^{j-1}(q-1)}}{\frac{(q^j-1)-(q^i-1)q^{j-i}}{q^{j-1}(q-1)}},\\
&= (-1)^{i+1}\prod_{j=1}^{i-1}\frac{(q^j-1)q^{i-j}}{(q^j-1)q^{i-j}-(q^i-1)}\prod_{j=i+1}^{k}\frac{q^j-1}{(q^j-1)-(q^i-1)q^{j-i}}\\
&= (-1)^{i+1}\prod_{j=1}^{i-1}\frac{(q^j-1)}{(q^j-1)q^{i-j}-(q^i-1)}\prod_{j=1}^{i-1}q^j\prod_{j=i+1}^{k}\frac{q^j-1}{(q^j-1)-(q^i-1)q^{j-i}}\\
&= (-1)^{i+1}\prod_{j=1}^{i-1}\frac{(q^j-1)}{(q^j-1)q^{i-j}-(q^i-1)}\prod_{j=1}^{i-1}q^j\prod_{j=i+1}^{k}\frac{q^j-1}{(q^j-1)-(q^i-1)q^{j-i}}\\
&= (-1)^{i+1}\prod_{j=1}^{i-1}\frac{(q^j-1)}{q^i-q^{i-j}-q^i+1}\prod_{j=i+1}^{k}\frac{q^j-1}{q^j-1-q^j+q^{j-i}}\prod_{j=1}^{i-1}q^j\\
&= (-1)^{i+1}\prod_{j=1}^{i-1}\frac{q^j-1}{1-q^{i-j}}\prod_{j=i+1}^{k}\frac{q^j-1}{q^{j-i}-1}(q^{\sum_{j=1}^{i-1}j})\\
&= (-1)^{i-1}\prod_{j=1}^{i-1}\frac{q^j-1}{1-q^{i-j}}\prod_{j=i+1}^{k}\frac{q^j-1}{q^{j-i}-1}(q^{\frac{i(i-1)}{2}})\\
&= \prod_{j=1}^{i-1}\frac{q^j-1}{q^{i-j}-1}\prod_{j=i+1}^{k}\frac{q^j-1}{q^{j-i}-1}(q^{\frac{i(i-1)}{2}})\\
&= \frac{(q-1)(q^2-1)\dots(q^{i-2}-1)(q^{i-1})}{(q^{i-1}-1)(q^{i-2}-1)\dots(q^2-1)(q-1)}\prod_{j=i+1}^{k}\frac{q^j-1}{q^{j-i}-1}(q^{\frac{i(i-1)}{2}})\\
&= \prod_{j=i+1}^{k}\frac{q^j-1}{q^{j-i}-1}(q^{\frac{i(i-1)}{2}})\\
&= \begin{bmatrix} k \\ k-i \end{bmatrix}_q (q^{\frac{i(i-1)}{2}})\\
&= \begin{bmatrix} k \\ i \end{bmatrix}_q (q^{\frac{i(i-1)}{2}}).
\end{aligned}$$

Donde la última igualdad se debe al hecho de que $\begin{bmatrix} k \\ k-i \end{bmatrix}_q = \begin{bmatrix} k \\ i \end{bmatrix}_q$ (ver [24, ejercicio 2]).

■

2.3.4 Ejemplo. Tomemos el ejemplo 2.2.17. Como el código q-ario de Hamming y el código q-ario simple son códigos duales, entonces de la proposición 2.1.4 obtenemos la siguiente matriz de verificación de paridad para S_2^3:

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

Así, del corolario 2.2.15 se tiene que $d_1 = 3$ y $d_2 = 4$. Ahora bien, de la figura 2.2, donde la retícula de la izquierda es $\mathcal{F}(\mathcal{M}^*[G])$ y la otra es $\mathcal{N}(\mathcal{M}[G])$, podemos observar que para cada $i \in \{1, 2\}$, todos los elementos de $\mathcal{N}_i$ tienen el mismo tamaño.

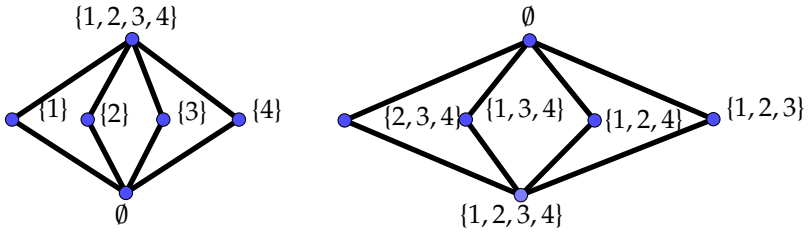

Figura 2.2:

Por otro lado, la resolución libre minimal graduada estándar de $S/I_{\mathcal{M}_{S_2^3}}$ tiene la forma:

$$0 \to S(-4)^{3\begin{bmatrix} 2 \\ 2 \end{bmatrix}_3} \to S(-3)^{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_3} \to S \to S/I_{\mathcal{M}_{S_2^3}} \to 0,$$

es decir,

$$0 \to S(-4)^3 \to S(-3)^4 \to S \to S/I_{\mathcal{M}_{S_2^3}} \to 0.$$

□

Para el inciso 2. del teorema 2.3.3 se tiene un resultado recíproco, el cual es la siguiente proposición:

2.3.5 Proposición. ([16, proposición 4]) *Sea C un $[n, k, d]_q$ código, si la resolución libre minimal asociada a C comienza como:*

$$\cdots \to S(-d)^{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} \to S \to S/I_{\mathcal{M}_C} \to 0.$$

Entonces C es un código de peso constante.

Demostración. Observemos que $\beta_1(S/I_{\mathcal{M}_C}) = \beta_{1,d}(S/I_{\mathcal{M}_C})$. Por otro lado, $\beta_1(S/I_{\mathcal{M}_C})$ es el número de generadores de $I_{\mathcal{M}_C}$ e $I_{\mathcal{M}_C} = \{x^\sigma : \sigma \in \mathcal{C}(\mathcal{M})\}$, así que

$$|\mathcal{C}(\mathcal{M}_C)| = \beta_1(S/I_{\mathcal{M}_C}) = \beta_{1,d}(S/I_{\mathcal{M}_C}) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q.$$

Ahora bien, de la proposición 2.3.2 se tiene que para cualquier $\sigma \in \mathcal{C}(\mathcal{M}_C)$ existe $c \in C$, tal que $\sigma = supp(c)$; y como $d = |\sigma| = |supp(c)|$ se tiene que dichas palabras código tienen

peso d. Así, hay al menos $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ subespacios generados por una palabra de peso d. Pero existen $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ subespacios de dimensión 1. Entonces todos los subespacios de dimensión 1 son generados por una palabra de peso d; así concluimos que toda palabra $c \in C$, $c \neq 0$ tiene peso d. ∎

2.3.6 Ejemplo.

1. Sea $\mathcal{H}_3^2$ un código q-ario de Hamming con matriz de verificación de paridad:

$$\mathcal{H} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in M_{3\times 7}(\mathbb{F}_3).$$

   La tabla de números de Betti de $S/I_{\mathcal{M}_{\mathcal{H}_3^2}}$ es:

	0	1	2	3	4
0	1	0	0	0	0
1	0	0	0	0	0
2	0	6	0	0	0
3	0	11	48	46	14

   Por lo tanto el código $\mathcal{H}_3^2$ no es un código de peso constante.

2. Recordemos que $\mathbb{F}_4 \simeq \mathbb{F}_2[w]/w^2 + w + 1$. Sea $\mathcal{H}_2^4$ un código q-ario de Hamming con matriz de verificación de paridad:

$$\mathcal{H} = \begin{pmatrix} 1 & 0 & w & 1 & w+1 \\ 0 & 1 & 1 & w & w+1 \end{pmatrix} \in M_{2\times 5}(\mathbb{F}_4).$$

   La tabla de números de Betti de $S/I_{\mathcal{M}_{\mathcal{H}_2^4}}$ es:

	0	1	2	3
0	1	0	0	0
1	0	0	0	0
2	0	10	15	6

   Por lo tanto $\beta_{1,3} = 10$. Por otro lado, de la proposición 2.3.5 se tiene que $\beta_{1,3} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q = 21$. Pero $10 \neq 21$ por lo tanto los códigos q-ario de Hamming $\mathcal{H}_r^q$ no son códigos de peso constante. □

2.3.7 Observación. En la proposición 2.2.18 vimos que el código q-ario simple $\mathcal{S}_r^q$ es un código de peso constante. Recordemos que por definición el código q-ario de Hamming $\mathcal{H}_r^q$ es el código dual de $\mathcal{S}_r^q$. Así, del inciso 1 de los ejemplo 2.3.6 se muestra que la propiedad de ser un código de peso constante es una propiedad que no se conserva bajo dualidad. Sin embargo existen propiedades que si se corservan bajo dualidad, una de ellas es la de ser un código MDS, como se vió en la proposición 2.1.17.

Bibliografía

[1] W. W. Adams y P. Loustaunau, An introduction to Gröbner bases, Graduate studies in mathematics, vol. 3, American Mathematical Society, **289**, 1994.

[2] N.D Armenoff (2015). Free resolutions associated to representable matroids (tesis doctoral). Universidad de Kentucky.

[3] M. F. Atiyah, I. G. MacDonald, Introduction to commutative algebra, Avalon Publishing, 1994.

[4] J.Atwood y J. Spoisky, 2009, a network of question-and-answer websites on math, disponible en https://math.stackexchange.com.

[5] A. Bjorner, *The homology and shellability of matroids and geometric lattices*. Matroid Applications, Encyclopedia Math. Appl.,**40**, Cambridge Univerity Press. Cambridge(1992).

[6] W. Bruns, J. Herzog, Cohen-Macaulay rings, Cambridge University Press, 1998.

[7] W. Chen y T. Kløve, *The weight hierarchies of q-ary codes of dimension 4*, IEEE Trans. Inform. Theory, **42**(5), Nov 1996.

[8] B. Chor, O. Goldreich, J. Hastad, J. Friedmann, S. Rudich y R. Smolenky, *The bit extraction problem of t-resilient functions*, en proc. 26 symp. found compu. sci., 1985.

[9] D. Eisenbud, Commutative algebra with a view toward Algebraic Geometry, Graduate Texts in Mathematics, **150**, Springer Berlin Heidelberg New York, 1995, Springer, New York (2005).

[10] D. Eisenbud, The geometry of syzygies, A Second Course in Algebraic Geometry and Commutative Algebra, Grad. texts in Mathematics, **229**, Springer-Verlag New York, 2005.

[11] D. Grayson y M.Stillman, 1992. Macaulay2, a software system for research in algebraic geometry, disponible en http://www2.macaulay2.com.

[12] J.Herzog y T. Hibi, Monomial ideals, Graduate texts in Mathematics, Springer-Verlag London, **260**, (2011).

[13] M., Hochster, *Cohen-Macaulay rings, combinatorics and simplicial complexes*, in "Ring Theory II", pp. 171-223, Dekker, New York, 1977.

[14] R. A. Horn y C.R, Johnson, Matrix analysis, Cambridge university press, segunda edición, (2013).

[15] T. Johnsen y H. Verdure, *Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids*. Appl. Algebra in Engineering, Communication and Computing. **24**(1), 2013.

[16] T. Johnsen y H. Verdure, *Stanley-Reisner resolution of constant weight linear codes.* Designs, Codes and Cryptography 2014; **72** (2).

[17] R. Jurrius, y R. Pellikaan, *Codes, arrangements and matroids*, DOI: 10,1142/9789814335768_0006, Feb 2013.

[18] T. Kløve, *Generalized Hamming weights of linear Codes*, IEEE Trans. Inform. Theory, **38**(3), May 1992.

[19] Z. Liu y W. Chen. *Notes on the value function.* Des. Codes Cryptogr., **54**, 11-19 (2010).

[20] J. Martínez-Bernal, M. A. Valencia-Bucio y R. H. Villarreal, Linear codes over signed graphs. Preprint, 2019, arXiv:1904.09487.

[21] H. Matsumura, Commutative ring theory, Cambridge studies in advanced mathematics, Cambridge University Press, pp. 320, 1989.

[22] E. Miller y B. Sturmfels, Combinatorial commutative algebra, Graduate Texts in Mathematics, **227**, (2015).

[23] J. Munkres, Elements Of Algebraic Topology, Addison-Wesley, 1984.

[24] J.G. Oxley. Matroid theory, Oxford University Press, Oxford, 1992.

[25] L.H. Ozarow y A.D. Wyner, *Wire-tap-channel II*, AT&T bell labs tech. J., **63**, 1984.

[26] I. Peeva, Graded syzygies, Algebra and aplications Volume 14, Springer Berlin Heidelberg New York, 2011.

[27] S. Roman, Coding and information theory, Graduate texts in mathematics, 134, Springer-Verlag New York, pp- 488.

[28] J. Rotman, An introduction to homological algebra, Universitext, Springer-Verlag New York, 2009.

[29] J. Rotman, Galois theory, Universitext, Springer-Verlag New York, 1998.

[30] R. P. Stanley, Combinatorics and commutative algebra, segunda ed., Progress in Mathematics, **41**, Birkhauser, Boston, MA, 1996.

[31] V.K. Wei, *Generalized Hamming weigths for linear codes*. IEEE Trans. Inform. Theory, **37**(5), (1991).

[32] N. White, Combinatorial geometries, Cambridge University Press, 1987.

Índice alfabético