CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS

AVANZADOS DEL INSTITUTO POLITÉCNICO NACIONAL

Unidad Zacatenco

Departamento de Matemáticas

Códigos Reed-Muller: familias y distancia mínima en términos algebraicos

TESIS

Que presenta

Fabiola Rodriguez Ortega

Para obtener el grado de

MAESTRA EN CIENCIAS

En la especialidad de

MATEMÁTICAS

Director de Tesis: Dr. Rafael Heraclio Villarreal Rodríguez

Ciudad de México Julio, 2017.

Índice general

Agradecimientos

A mi asesor el Dr. Rafael Heraclio Villarreal Rodríguez por el gran apoyo, conocimiento, paciencia y consejos transmitidos a lo largo de mis estudios de posgrado y realización de este trabajo. Mi agradecimiento también a mis sinodales el Dr. Carlos Valencia y Dr. Eliseo Sarmiento Rosales por el interés mostrado.

Agradezco al Departamento de Matemáticas del CINVESTAV-IPN por permitirme crecer académicamente así como al CONACYT por el recurso financiero que me otorgó.

A Raúl, Acapulco, My friend, Isaac y Rodo por los buenos ratos armando cursos y tardes de resolución problemas, al seminario de juegos. A mis amigas Ángela y Valentina por su apoyo moral y consejos.

Y sobre todo a mi abuelita, a mis papás y a mi hermano por darme la fuerza para hacer lo que me plazca.

Resumen

En esta tesis daremos un gran panorama de los códigos Reed-Muller generalizados. En los capítulos uno, dos y tres veremos su construcción vista como el cociente del anillo de polinomios en varias variables sobre el ideal anulador de un subconjunto del espacio proyectivo; la extracción de sus parámetros básicos a través del uso del álgebra conmutativa y por último abordaremos una serie de ejemplos de dichos códigos, dando fórmulas de sus parámetros así como el a-invariante y los generadores del ideal anulador asociado.

Los capítulos cuatro y cinco tratan dos temas independientes, en el primero generalizaremos el producto de códigos a través de la inmersión de Segre y como dicho producto hereda ciertas propiedades de cada uno de los elementos del producto. Por último daremos una definición alterna a la distancia mínima de un código la cual da lugar a una nueva manera de calcular dicho parámetro.

Abstract

In this thesis we will give a great overview of the generalized Reed-Muller codes. In chapters one, two and three we shall see its construction as the quotient of the ring of polynomials in several variables over the vanishing ideal of a subset of the projective space; the extraction of its basic parameters through the use of the commutative algebra. In chapter three we will view a series of examples of such codes giving formulas of their parameters, as well as the a-invariant and the generators of the associated vanishing ideal.

Chapters four and five deal with two independent themes, in the first we will generalize the product of codes through the Segre embedding and as that product inherits certain properties of each of the elements of the product. In the chapter five we will give an alternative definition to the minimum distance of a code, which gives rise to a new way of calculating this parameter.

Introducción

La Teoría de códigos es la rama de las matemáticas y de la computación que se ocupa de la transmisión de información y detección de errores en la información recibida. A grandes rasgos codificar es transformar información en una señal convenida para su comunicación. Así, un código algebraico es aquel donde la transformación está dada por cualquier transformación lineal inyectiva y la detección de errores está parametrizada por una métrica definida en el espacio ambiente de dicha transformación. Nosostros estudiaremos aquellos códigos dados por la siguiente estructura.

Definimos al $d-$ésimo código evaluación Reed-Muller generalizado $C_d(X)$ como la imagen de la siguiente función:

$$\mathrm{ev}_d \colon R_d = K[x_0, \ldots, x_n]_d \to K^{|X|}, \qquad f \mapsto (f(P_1), \ldots, f(P_{|X|})) \tag{1}$$

donde K es un campo finito, X un subconjunto del $n-$ésimo espacio proyectivo $\mathbb{P}^n$ y $P_1, \ldots, P_{|X|}$ la representación estándar de los puntos de X.

Este trabajo tiene tres objetivos principales.

El primero es definir y mostrar de una manera progresiva lo necesario para llegar a la ecuación anterior y que de manera natural tengamos noción de cuáles son las propiedades más importantes de $C_d(X)$: su longitud, dimensión y distancia mínima y qué herramientas usar para obtenerlas. Por herramientas nos referimos a conceptos y resultados de distintas áreas como el álgebra conmutativa, geometría algebraica y álgebra computacional.

El segundo objetivo es esclarecer con tres familias particulares de códigos evaluación Reed-Muller como obtener para cada d los parámetros básicos de $C_d(X)$ así como generadores del ideal anulador de X y el a-invariante asociado.

El tercer objetivo es lo que llamo ir de lo particular a lo general y un análisis alterno, pues generalizaremos el concepto de código asociado a la inmersión de Segre como producto directo de códigos y códigos proyectivos de Segre. Por otro lado atacaremos el

problema de encontrar la distancia mínima (el parámetro más difícil de entender) de un código Reed-Muller definiendo la distancia mínima de un ideal graduado, sus principales propiedades y la equivalencia entre ésta distancia y la distancia mínima de un código dando lugar a una nueva manera de calcular dicho parámetro y que pienso, es el resultado más fuerte que se expondrá en ésta tesis.

Para ti Cocolito

Capítulo 1

Códigos Lineales

Pensemos en la siguiente situación, el sujeto A quiere enviar un mensaje M al sujeto B, el mensaje viajará a través de un canal (red telefónica, internet, transmisión satelital, etc.) hasta llegar al sujeto B, la cuestión es la siguiente: ¿El mensaje enviado es el mismo que el mensaje recibido? existen distintos factores que pueden modificar el mensaje (montañas, tormentas o señales externas), a cualquier factor posible que evite que el mensaje M sea igual al mensaje recibido M' se le llama ruido.

Si A denota un alfabeto y P_A denota todas las posibles palabras con dicho alfabeto, los mensajes M y M' los podemos ver como subconjuntos de P_A, con estas condiciones el ruido modifica palabras de P_A en P_A. En lo siguiente, al alfabeto A lo encajaremos en un campo finito K y las palabras en K^n para algún $n \in \mathbb{N}$ por lo que una palabra x representa un elemento de K^n y un mensaje M representa un subconjunto de K^n.

En la primera sección de este capítulo nos enfocaremos en dar soluciones para aproximar el problema de recobrar M dado M'. Dichas soluciones se les conoce como Códigos Algebraicos, los cuales en principio deben contener cualquier posible palabra de M y mediante una métrica miden si las palabras de M' son lo suficientemente cercanas a las de M para decidir si alguna palabra $p' \in M'$ corresponde a una única palabra en M. La segunda sección es mucho más técnica pues sólo es una recopilación de conceptos y resultados que son necesarios en los siguientes capítulos.

1.1. Construcción de códigos lineales

Definición 1.1.1 Sea K^n un K-espacio vectorial con K un campo con q elementos. Un **código lineal** sobre un alfabeto K será un subespacio vectorial C de K^n.

Por lo que, si $|K^n| = q^n$ entonces $|C| = q^l$ con $l \leq n$. Si $\{\mathbf{g}_1, \ldots, \mathbf{g}_l\}$ es una base para C, entonces la matriz $G = \{\mathbf{g}_j\}_{j=1}^{l} \in M_{n\times l}(K)$ cuyas columnas son los vectores de la base, se dice generatriz del código C, así la transformación $G : K^l \to K^n$ tiene como imagen a C.

Si $m \in M$ es una palabra que se quiere enviar, $p = G(m)$ es la palabra codificada y es la palabra que se enviará, es decir, trabajaremos con $G(M)$ en vez de M. A continuación describiremos las herramientas necesarias para determinar cuando una palabra recibida p' pertenece o no a $G(M)$ o no hay manera de saberlo.

Definición 1.1.2 Sean $x, y \in K^n$, la **distancia de Hamming** entre x y y denotada por $d(x, y)$ es el número de posiciones en el cual x y y difieren. Es decir, si $x = (x_1, \ldots, x_n)$ y $y = (y_1, \ldots, y_n)$:

$$d(x, y) = |\{j : x_j \neq y_j\}| . \tag{1.1}$$

El **peso de Hamming** $w(x)$ de $x \in K^n$ es el número de coordenadas no cero de x y se tiene que $d(x, y) = w(x - y)$.

Teorema 1.1.3 *La distancia de Hamming $d : K^n \times K^n \to \mathbb{N}$ es una métrica, por lo tanto (K^n, d) es un espacio métrico.*

Demostración. Sólo demostraremos la desigualdad del triángulo ya que las demás propiedades son evidentes. Se tiene para cualesquiera $s, t \in K^n$ la siguiente propiedad.

$$w(s) \leq w(s - t) + w(t) \tag{1.2}$$

Sea s_j una coordenada de s con j fijo, si $s_j \neq 0$ entonces $s_j - t_j \neq 0$ o $s_j = t_j$ y en cualquier caso siempre se contribuye con un uno por lo tanto lo anterior se cumple, así poniendo a $s = x - y$ y $t = x - z$ tenemos: $w(x - y) \leq w(z - y) + w(x - z)$ por lo tanto

$$d(x, y) \leq d(x, z) + d(z, y). \tag{1.3}$$

■

Definición 1.1.4 La **distancia mínima** de un código $C \leq K^n$ se define como:

$$\delta(C) = min\ d(x, y) \tag{1.4}$$

tales que $x \neq y \in C$.

Si el código C es lineal y definimos el **peso mínimo** de un código C como

$$w(C) = min\ w(x - y) \tag{1.5}$$

tales que $x \neq y \in C$, entonces $\delta(C) = w(C)$. Un $(n, l, \delta(C))-$código es un código de longitud n, dimensíon l y distancia mínima $\delta(C)$.

Si p' es una palabra recibida y existe $p \in C$ tal que $d(p, p') \leq \lfloor \frac{\delta(C)-1}{2} \rfloor$ entonces la palabra que quiso ser enviada es p, es decir, p es el único elemento en C que satisface dicha desigualdad. En efecto, supongamos que existe $\exists z \in C$ tal que $d(p', z) \leq \lfloor \frac{\delta(C)-1}{2} \rfloor$ luego

$$d(p, z) \leq d(p, p') + d(p', z) \leq \lfloor \frac{\delta(C) - 1}{2} \rfloor + \lfloor \frac{\delta(C) - 1}{2} \rfloor \leq \delta(C) - 1 < \delta(C) \tag{1.6}$$

lo cual representa una contradicción.

Si $d(p, p') > \lfloor \frac{\delta(C)-1}{2} \rfloor \ \forall p \in C$ entonces el código no es capaz de saber que palabra se quiso enviar.

Corolario 1.1.5 *Un código es capaz de detectar y corregir* $\lfloor \frac{\delta(C)-1}{2} \rfloor$ *errores.*

Por lo que un buen código C debe tener distancia mínima lo más grande posible.

La siguiente proposición nos permite saber que tan grande puede ser $\delta(C)$ en términos de su longitud y dimensión.

Proposición 1.1.6 *Si C es un código lineal sobre K^n con $dim_K C = l$ y $\delta(C) = d$, entonces se cumple:*

$$d \leq n - l + 1 \tag{1.7}$$

Ésta cota es conocida como la cota de Singleton para la distancia mínima

Demostración. Consideremos el subespacio lineal $W \subseteq K^n$ definido por

$$W = \{(a_1, \ldots, a_n) : a_i = 0 \ \forall i \geq d\} \tag{1.8}$$

Notemos que si $a \in W$ entonces $w(a) \leq d - 1$ por lo que $W \cap C = \{0\}$ y se sigue

$$l+(d-1) = dim_K C + dim_K W = dim_K(C+W) + dim_K(W \cap C) = dim_K(C+W) \leq n \tag{1.9}$$

■

Definición 1.1.7 Los códigos en los que se cumple la igualdad $l + d = n + 1$ son llamados códigos de **distancia máxima separable** (DMS).

Un ejemplo de códigos con distancia máxima separable son los códigos de **Reed-Solomon**:

Ejemplo 1.1.8 Sea $n = q - 1$ y $\xi \in \mathbb{F}_q^*$ un elemento primitivo del grupo multiplicativo de $\mathbb{F}_q$, es decir $\mathbb{F}_q^* = \{\xi, \xi^2, \ldots, \xi^n = 1\}$. Para algún natural l con $1 \leq l \leq n$, consideremos el siguiente espacio vectorial sobre $\mathbb{F}_q$ de dimensión l

$$F_l = \{f \in \mathbb{F}_q[x] : \deg f \leq l - 1\} \tag{1.10}$$

y la función evaluación $ev : F_l \to {\mathbb{F}_q}^n$ dada por

$$ev(f) := (f(\xi), f(\xi^2), \ldots, f(\xi^n)) \tag{1.11}$$

Claramente ésta función es lineal e inyectiva porque un polinomio en F_l tiene a lo más $l - 1$ raíces y $l - 1 < n$. Por lo tanto

$$C_l = \big\{(f(\xi), f(\xi^2), \ldots, f(\xi^n)) : f \in F_l\big\} \tag{1.12}$$

es un código de dimensión l. El peso de una palabra codificada $c = ev(f) \in C_l$ con $c \neq 0$ es

$$\begin{aligned} w(c) &= n - \big|\big\{i \in \{1, \ldots, n\} : f(\xi^i) = 0\big\}\big| \\ &\geq n - \deg f \geq n - (l - 1) \end{aligned} \tag{1.13}$$

Por lo que $d \geq n+1-l$ pero por la proposición anterior se cumple $d \leq n+1-l$ por lo tanto $d = n + 1 - l$, así los códigos de Reed-Solomon son de distancia máxima separable sobre $\mathbb{F}_q$.

Hasta aquí nos hemos dado cuenta que la distancia mínima juega un papel muy importante dentro de los códigos lineales y ya se tienen ciertas sospechas sobre la complejidad de la misma. La naturaleza finita de los códigos hace que sus parámetros sean computables. Para la dimensión y longitud existen programas eficientes que los determinan (Macaulaey 2) pero para la distancia mínima se tiene otra historia. Mucho se ha trabajado en encontrar otras caracterizaciones de $\delta(C)$ y generar algoritmos eficientes que la calculen de manera directa como indirecta, ésta discusión la dejaremos pendiente por el momento. Enseguida generalizaremos la noción de distancia mínima.

Definición 1.1.9 Dado un subcódigo D de C (D es un subespacio lineal de C), el *soporte* de D, denotado por $\chi(D)$, es el conjunto de posiciones no cero de D, es decir,

$$\chi(D) := \{i : \exists\, (a_1, \ldots, a_s) \in D,\, a_i \neq 0\}.$$

El r-ésimo *peso generalizado de Hamming* de C, denotado por $\delta_r(C)$, es el tamaño del soporte más pequeño de un subcódigo r-dimensional, es decir,

$$\delta_r(C) := \text{mín}\{|\chi(D)| :\ D \text{ es un subcódigo lineal de } C \text{ con } \dim_K(D) = r\}.$$

La primera observación a esta definición es que $\delta_1(C) = \delta(C)$. Recordemos que los subespacios unidimensionales de C son aquellos generados por un elemento fijo de C y que $\forall \lambda \neq 0 \in K$ y $\forall c \in C$ $w(\lambda c) = w(c)$ por lo que $|\chi(c)| = w(c)$ $\forall c \in C$ y de esto se sigue que $\delta_1(C) = \delta(C)$.

La segunda observación es el siguiente teorema:

Teorema 1.1.10 *[36] Sea C un código (n,l,$\delta(C)$)-lineal. Entonces $\delta_r(C) \leq n - l + r$ para $r = 1, \ldots, l$ y además tenemos:*

$$1 \leq \delta(C) < \delta_2(C) < \ldots < \delta_r(C) \leq n. \tag{1.14}$$

Si $r = 1$ entonces recobramos la cota de Singleton para la distancia mínima. El peso generalizado de Hamming a recibido mucha atención; vea [6, 12, 33, 36, 37] y las referencias que se tienen en estas.

1.2. Anillos y módulos graduados

Ya que el objetivo principal de ésta tesis es hacer un análisis profundo de los códigos Reed-Muller. En ésta sección recordaremos algunos conceptos y resultados básicos de teoría de módulos graduados pues son fundamentales para definirlos y entenderlos.

De ahora en adelante cuando hablemos de un anillo nos referiremos a un anillo conmutativo con identidad y en esta sección K representa cualquier campo.

Definición 1.2.1 Una **graduación de un anillo** R es una familia $\{R_d\}_{d\in\mathbb{Z}}$ de subgrupos R_d del grupo aditivo de R tales que $R = \bigoplus_{d\in\mathbb{Z}} R_d$ y para todo $d,\ e \in \mathbb{Z}$ se tiene que $R_d R_e \subset R_{d+e}$. Un anillo R se dice **anillo graduado** si posee una graduación $\{R_d\}_{d\in\mathbb{Z}}$.

En particular se tiene que $R_0 R_0 \subset R_0$, por lo que R_0 es un anillo. Si para todo $d < 0$, $R_d = 0$ entonces se dice que R es un **anillo positivamente graduado**. Un elemento de R_d es llamado **elemento homogéneo de grado** d. Por lo tanto todo elemento de R se puede escribir de manera única como una suma finita de elementos homogéneos. Al conjunto de elementos homogéneos de R lo denotaremos por R^h

Ejemplo 1.2.2 Sea $R = K[x_0, \ldots, x_n]$ entonces R posee la siguiente graduación: Sea $d \geq 0$ definimos:

$$R_d := \{f \in R : f = \sum_i a_i x_0^{i_0} \cdots x_n^{i_n},\ i_0 + \cdots + i_n = d \text{ y } a_i \in K\ \forall i\} \cup \{0\}$$

y para $d < 0$ $R_d :=< 0 >$. A dicha graduación se le conoce como graduación estándar y es el anillo es la graduación con la que se trabajará a lo largo de esta tesis a menos que se diga lo contrario.

Definición 1.2.3 Sea R un anillo graduado. Un R-módulo M se llama **módulo graduado** si existe una sucesión $\{M_d\}_{d\in\mathbb{Z}}$ de subgrupos aditivos de M, tal que $M = \bigoplus_{d\in\mathbb{Z}} M_d$ y para todo d, l se cumple que $R_d M_l \subset M_{d+l}$.

Un submódulo N de M se llama **submódulo homogéneo** si $N = \bigoplus_{d\in\mathbb{Z}} N_d$ en donde $N_d = N \cap M_d$ para todo d; en particular un ideal I de R es un **ideal homogéneo** si $I = \bigoplus_{d=0}^{\infty} I \cap R_d$ o si es generado por elementos homogéneos de R.

Como R_0 es un anillo y $R_0 M_d \subset M_d$ $\forall d \in \mathbb{Z}$, entonces M_d es un R_0-módulo $\forall d \in \mathbb{Z}$, en particular si R_0 es un campo entonces M_d es un R_0-espacio vectorial $\forall d \in \mathbb{Z}$.

El módulo cociente M/N es también un $A-$módulo graduado con la siguiente graduación: $(M/N)_d = (M_d + N)/N \cong M_d/N_d$.

Si $M = \bigoplus_{d\in\mathbb{Z}} M_d$ y $N = \bigoplus_{d\in\mathbb{Z}} N_d$ son $R-$módulos graduados, entonces la suma directa (externa) $M \bigoplus N$ es un módulo graduado donde $(M \bigoplus N)_d = M_d \bigoplus N_d$ $\forall d \in \mathbb{Z}$, es una graduación.

Definición 1.2.4 Sea M un $R-$módulo graduado. Para $a \in \mathbb{Z}$ definamos el módulo con **corrimiento** a como $M(a) := M$, pero con graduación $(M(a))_d = M_{d+a}$

Definición 1.2.5 Sean M y N $R-$módulos graduados. Un **homomorfismo graduado** es un homomorfismo $\phi : M \to N$ tal que para todo d, $\phi(M_d) \subseteq N_d$

Lema 1.2.6 *Si ϕ en un homomorfismo graduado entonces* $\ker(\phi)$ *es un submódulo graduado del dominio de ϕ.*

Demostración. En efecto, sea $B = \ker(\phi)$ demostremos que $B = \bigoplus_{d\in\mathbb{Z}} B_d$ con $B_d = B \cap M_d$. Sea $b \in B$, como $M = \bigoplus_{d\in\mathbb{Z}} M_d$ entonces $a = \sum_{j=1}^{n} a_{i_j}$ $a_{i_j} \in M_{i_j}$ $\forall j = 1, \ldots, n$ y $\{i_1, \ldots, i_n\} \subseteq \mathbb{N}$ además $\phi(b) = \sum_{j=1}^{n} \phi(a_{i_j}) = 0$ y como $\phi(M_{i_j}) \subseteq N_{i_j}$ $\forall j = 1, .., n$ y $N = \bigoplus_{d\in\mathbb{Z}} N_d$ entonces $\phi(a_{i_j}) = 0$ $\forall j = 1, .., n$ luego $a_{i_j} \in B \cap M_{i_j}$ $\forall j = 1, .., n$, así $b \in \bigoplus_{d\in\mathbb{Z}} B_d$ y $B \subseteq \bigoplus_{d\in\mathbb{Z}} B_d$. Claramente $B \supseteq \bigoplus_{d\in\mathbb{Z}} B_d$, por lo tanto $\ker(\phi)$ es un submódulo graduado. ∎

Definición 1.2.7 Sea M un $R-$módulo graduado. Decimos que M tiene una **resolución libre graduada finita** (r.l.g.f) si existe la siguiente sucesión exacta:

$$0 \to M_t \xrightarrow{\phi_t} M_{t-1} \xrightarrow{\phi_{t-1}} \cdots \xrightarrow{\phi_2} M_1 \xrightarrow{\phi_1} M_0 \xrightarrow{\phi_0} M \to 0 \tag{1.15}$$

Donde los M_i's son $R-$módulos graduados libres finitamente generados, es decir, de la forma:

$$M_i \cong R(\alpha_{1i}) \oplus R(\alpha_{2i}) \oplus \cdots \oplus R(\alpha_{qi}), \quad \alpha_{ji} \in \mathbb{Z} \tag{1.16}$$

y los ϕ_i son homomorfismos graduados, donde $R(\alpha_{ji})$ es el R-módulo que se define como $R(\alpha_{ji})_k = R(\alpha_{ji+k})$, $R(\alpha_{ji}) = \bigoplus_{k\in\mathbb{Z}} R(\alpha_{ji})_k$.

Teorema 1.2.8 *[10] Cuando M es un módulo graduado sobre un álgebra graduada las cual es generada sobre un campo por sus elementos de grado positivo se tiene que M posee una r.l.g.f.*

Corolario 1.2.9 *Cuando $R = K[x_0, \ldots, x_n]$ e I es un ideal graduado el $R-$módulo R/I tiene una r.l.g.f .*

Capítulo 2

Códigos Reed-Muller Generalizados

Sea K cualquier campo y sea $R = K[x_0, \ldots, x_n]$ el anillo de polinomios en $n+1$ indeterminadas. Como en el ejemplo 1.2.2 para cada $d \geq 0$ definimos:

$$R_d := \{f \in R : f = \sum_i a_i x_0^{i_0} \cdots x_n^{i_n} \ , \ a_i \in K, \ i_0 + \cdots + i_n = d \ \forall i\} \cup \{0\}.$$

Es fácil ver que $\forall d \ R_d$ es un K-espacio vectorial de dimensión finita. Si I es un ideal de R generado por polinomios en $\bigcup_{d \in \mathbb{N}_0} R_d$ entonces para cada $d \in \mathbb{N}_0 \ I_d$ es un subespacio de R_d por lo que tiene sentido pensar en los K-espacios vectoriales R_d/I_d con $d \in \mathbb{N}_0$.

Recordemos que un código lo podemos pensar como un encaje lineal de un espacio vectorial en un espacio ambiente, con esto en mente resultaría interesante estudiar los espacios R_d/I_d bajo encajes en ciertos ambientes y ver que información relevante podemos obtener haciendo uso de la teoría que nos ofrece el álgebra conmutativa y computacional pues sabemos que los anillos de polinomios son fuertemente estudiados en éstas áreas.

Los códigos Reed-Muller generalizados que introduciremos en este capítulo son un tipo de familia $\{R_d/I_d\}_{d \in \mathbb{N}_0}$ donde I es el ideal anulador de un subconjunto de un espacio proyectivo. Mucho de lo que leeremos a continuación es un repaso de los conceptos necesarios tanto para definir como para obtener información de dicha familia.

2.1. Espacios proyectivos

Definición 2.1.1 Sea K un campo, definimos el $(n+1)-$espacio afín como

$$\mathbb{A}^{n+1} = \{(p_0, \ldots, p_n) : p_i \in K \ \forall i\}$$

y al $n-$espacio proyectivo $\mathbb{P}^n$ como $\mathbb{A}^{n+1}-\{0\}$ bajo la siguiente relación de equivalencia $(p_0,\ldots,p_n)\sim(\lambda p_0,\ldots,\lambda p_n)$ para todo $\lambda\in K$ distinta de cero. Para cada $P\in\mathbb{A}^{n+1}-\{0\}$, $[P]$ denota un elemento en $\mathbb{P}^n$.

Observación 2.1.2 *Sea $R=K[x_0,\ldots,x_n]$, cada polinomio $g\in R$ define una función canónica $g:\mathbb{A}^{n+1}\to K$ la cual evalúa a cada punto de $\mathbb{A}^{n+1}$ en g, sin embargo esta función no pasa al proyectivo pues deja de estar bien definida. Sea $f\in R_d$ para algún $d>0$ entonces $\forall\lambda\in K$ y $\forall P\in\mathbb{A}^{n+1}$ se tiene que $f(\lambda a)=\lambda^d f(a)$, si $P\neq 0$ y p_i es la primera entrada no cero de P tenemos lo siguiente: $(f/x_i^d)(\lambda P)=\lambda^d f(P)/(\lambda p_i)^d=f(P)/p_i^d$ $\forall\lambda\neq 0$, si $p_i=1$ entonces $(f/x_i^d)(\lambda P)=f(P)$ $\forall\lambda\neq 0$.*

Proposición 2.1.3 *Sea $P'\in\mathbb{P}^n$. Existe un único representante $P\in\mathbb{A}^{n+1}$ con primer entrada $p_i=1$, es decir $P=(0,0,\ldots,p_i=1,p_{i+1},\ldots,p_n)$ con $p_j\in K$ $\forall j=i+1,\ldots,n$, a éste único representante se le conoce como la* ***representación estándar de*** *P'.*

Demostración. Sea $P'\in\mathbb{P}^n$ y $(p'_0,\ldots,p'_n)\in P'$, como sus entradas no son todas cero existe una primera entrada tal que $p'_i\neq 0$, multiplicando por ${p'_i}^{-1}$ a $(p'_0,\ldots,p'_n)$, tenemos el representante $P=(0,0,\ldots,p_i=1,p_{i+1},\ldots,p_n)\in P'$, ahora veamos que P es único: Sea $(0,..,1,b_{j+1},\ldots,b_n)$ otro representante de P' con dicha propiedad, entonces existe $\lambda\neq 0\in K$ tal que $(0,\ldots,0,p'_i=1,p'_{i+1},\ldots,p'_n)=(0,\ldots,0,\lambda,\lambda b_{j+1},\ldots,b_n)$. Si $j<i$ entonces $p_j=\lambda\neq 0$ lo cual contradice el hecho de que p_i es la primer i-ésima coordenada distinta de cero, si $i<j$ implica $b_i=0$, se sigue que $p_i=0$ lo cual no puede ser. Así $i=j$ y por lo tanto $\lambda=1$, es decir P es único. ■

Si f es un polinomio de R y $P\in\mathbb{A}^{n+1}$ la representación estándar de algún punto $P'\in\mathbb{P}^n$ evaluar f en P' se define como $f(P)$ lo cual es equivalente a evaluar P' en f/x_i^d, es decir, $f(P)=f/x_i^d(\lambda P)$ $\forall\lambda\neq 0$. Ésta equivalencia la hemos mencionado porque son usadas en los artículos que mencionaremos a lo largo de esta tesis; nosotros usaremos la evaluación en la representación estándar únicamente por que su notación es más corta.

Definición 2.1.4 Sea T un subconjunto de polinomios homogéneos de R. Definimos el conjunto de ceros de T en $\mathbb{P}^n$ como:

$$Z(T)=\{[P]\in\mathbb{P}^n : f(P)=0\ \forall f\in T\}.$$

Si I es el mínimo ideal homogéneo de R que contiene a T se tiene que: $Z(I)=Z(T)$ y existen $f_1,\ldots,f_r$ polinomios homogéneos que pertenecen a I tales que $Z(T)=Z(f_1,\ldots,f_r)$.

Lema 2.1.5 *[7] Si $V, W \subset \mathbb{P}^n$ son conjuntos algebraicos, entonces también lo son $V \cup W$ y $V \cap W$.*

Demostración. Supongamos que $V = V(f_1, ..., f_s)$ y $W = V(g_1, ..., g_t)$. Entonces afirmamos que

1. $V \cap W = V(f_1, ..., f_s, g_1, ..., g_t)$

2. $V \cup W = V(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$

La primera igualdad es trivial. Enfoquémonos en la segunda igualdad, si $[P] \in V$, entonces todos los f_i's se anulan en P y por consiguiente los productos $f_i g_j$'s se anulan en dicho punto, de esto se sigue que $V \subset V(f_i g_j)$, de manera análoga: $W \subset V(f_i g_j)$ por lo que $V \cup W \subset V(f_i g_j)$.

Sea $[P] \in V(f_i g_j)$. Si $[P] \in V$ hemos terminado, si no, existe i tal que $f_i(P) \neq 0$ y como $f_i([P])g_j([P]) = 0 \ \forall j$ se tiene que $[P] \in W$ luego $V(f_i g_j) \subset V \cup W$. ■

Del lema anterior se sigue que la colección de conjuntos algebraicos de $\mathbb{P}^n$ define una topología bajo conjuntos cerrados conocida como la Topología de Zariski.

Para cada ideal homogéneo de R hemos asociado un conjunto en $\mathbb{P}^n$ el cual es cerrado bajo la topología de Zariski. De igual manera, dado $X \subset \mathbb{P}^n$ definimos su ideal anulador I_X como el ideal generado por el conjunto $\left\{ f \in R^h : f(P) = 0 \ \forall [P] \in X \right\}$, al anillo graduado R/I_X se le conoce como el **anillo coordenado de** X.

En Geometría Algebraica Clásica se estudia el vínculo entre la estructura topológica de $\mathbb{P}^n$ y la estructura algebraica de $R = K[x_0, \ldots, x_n]$ (cuando K es un campo algebraicamente cerrado) bajo conjuntos algebraicos e ideales anuladores . Aunque este tema es bastante interesante, lamentablemente cuando K es un campo finito, la topología de Zariski resulta ser la topología discreta pues en general, los puntos resultan ser conjuntos algebraicos, de hecho para cualquier campo K y $[P] \in \mathbb{P}^n$ junto con su representación estándar $(p_0, \ldots, p_n)$:

$$\{[P]\} = V(p_j x_i - p_i x_j) \tag{2.1}$$

Así que no hay mucho de que hablar topológicamente cuando el campo es finito, sin embargo, En el Capítulo 3 y Secciones 3.2 y 3.3 veremos que los generadores de ideales anuladores de variedades proyectivas sobre sus cerraduras algebraicas nos dan información de los generadores de ciertos ideales sobre los campos iniciales.

2.2. Códigos evaluación Reed-Muller

Sea K un campo, X un subconjunto finito de $\mathbb{P}^n$, si $[P_1], \ldots, [P_{|X|}]$ son los puntos de X con $P_1, \ldots, P_{|X|}$ su representación estándar. La *función evaluación*

$$\mathrm{ev}_d \colon R_d = K[x_0, \ldots, x_n]_d \to K^{|X|}, \qquad f \mapsto (f(P_1), \ldots, f(P_{|X|})) \tag{2.2}$$

define una función lineal (ver la Observación(2.1.2) y Proposición (2.1.3)) de K-espacios vectoriales.

Definición 2.2.1 Cuando K es un campo finito la imagen de ev_d, denotada por $C_X(d)$, define un *código lineal* que llamaremos *código evaluación Reed-Muller generalizado* de orden d.

Como ya sabemos, por un *código lineal* nos referimos a un subespacio vectorial de $K^{|X|}$. El kernel de ev_d es precisamente $(I_X)_d$. Por lo que hay un isomorfismo entre los espacios vectoriales

$$(R/I_X)_d \simeq_K C_X(d). \tag{2.3}$$

Los elementos de $C_X(d)$ que no son cero pueden ser interpretados como polinomios homogéneos de grado d que no se anulan en todo X. Por eso estamos interesados en la estructura algebraica del ideal I_X, sus generadores, y la dimensión como $K-$espacio vectorial de cada una de sus componentes homogéneas, así como la cardinalidad de X; recordemos que los parámetros básicos de $C_X(d)$ son su longitud $|X|$, dimensión $dim_K C_X(d)$ y distancia mínima $\delta(C_X(d))$ la cual se denota también como $\delta_X(d)$.

Definición 2.2.2 Sea $R = K[x_0, \ldots, x_n]$ el anillo de polinomios e I un ideal homogéneo de R. La función de Hilbert de I es:

$$H_I(d) := dim_K R_d/I_d, \quad d = 0, 1, 2, \ldots$$

En estos términos, para cada $d \in \mathbb{N}$ el código Reed-Muller $C_X(d)$ tiene dimensión $H_I(d)$.

Proposición 2.2.3 *Consideremos a $R = K[x_0, \ldots, x_n]$, una base para R_d es:*

$$X_d = \{x_0^{i_0} \cdots x_n^{i_n} : i_j \in \mathbb{N} \ \ni \ i_0 + \cdots + i_n = d\} \tag{2.4}$$

y la dimensión de R_d es $\binom{n+d}{d}$.

Demostración. Sea $x_0^{i_0}\cdots x_n^{i_n} \in X_d$, asociándole la $d-$tupla

$$a_d = (\underbrace{0,\ldots,0}_{i_0},\ldots,\underbrace{n,\ldots,n}_{i_n})$$

y a su vez asociándole a a_d la $d-$tupla:

$b_d = (0+1, 0+2, \ldots, 0+i_0, \ldots, j+(i_0+\cdots+i_{j-1}+1), \ldots, j+(i_0+\cdots+i_j), \ldots, n+(i_0+\cdots+i_{n-1}+1), \ldots, n+(i_0+\cdots+i_n = d))$

Obtenemos que la cantidad de elementos de la forma b_d son todas las combinaciones posibles de tomar d elementos de $d+n$ elementos, es decir $\binom{n+d}{d}$. ■

Proposición 2.2.4 *Sea*

$$0 \to M_t \xrightarrow{\phi_t} M_{t-1} \xrightarrow{\phi_{t-1}} \cdots \xrightarrow{\phi_2} M_1 \xrightarrow{\phi_1} M_0 \to 0 \tag{2.5}$$

una sucesión exacta de K-espacios vectoriales de dimensión finita, entonces

$$\sum_{i=0}^{t}(-1)^i dim_K(M_i) = 0 \tag{2.6}$$

Demostración. Procedamos por inducción sobre el número $n = t+1$ de K-espacios vectoriales involucrados en la sucesión.

a. Para $t = 1$ y $n = 2$ tenemos la sucesión $0 \to M_1 \xrightarrow{\phi_1} M_0 \to 0$ Donde $\ker(\phi_1) = 0$ y $Im(\phi_1) = M_0$, luego $M_1 \cong M_0$ por lo que

$$dim_K(M_0) - dim_K(M_0) = 0 \tag{2.7}$$

Supongamos que la fórmula se cumple para $n = t$ espacios, es decir

$$0 \to M_{t-1} \xrightarrow{\phi_{t-1}} \cdots \xrightarrow{\phi_2} M_1 \xrightarrow{\phi_1} M_0 \to 0 \tag{2.8}$$

b. Demostremos que se cumple para $n = t+1$ espacios. Sea

$$0 \to M_t \xrightarrow{\phi_t} M_{t-1} \xrightarrow{\phi_{t-1}} \cdots \xrightarrow{\phi_2} M_1 \xrightarrow{\phi_1} M_0 \to 0 \tag{2.9}$$

Haciendo $M = \phi_2(M_2) = \ker(\phi_1)$ obtenemos la sucesión exacta

$$0 \to M_t \xrightarrow{\phi_t} M_{t-1} \xrightarrow{\phi_{t-1}} \cdots M_2 \xrightarrow{\phi_2} M \to 0 \tag{2.10}$$

con t espacios, luego por hipótesis de inducción: $\sum_{i=2}^{t}(-1)^i dim_K(M_i) = dim_K(M)$, pero $M_1/M \cong \phi_1(M_1) = M_0$, por lo que $dim_K(M) = dim_K(M_1) - dim_K(M_0)$ luego

$$\sum_{i=0}^{t}(-1)^i dim_K(M_i) = 0 \tag{2.11}$$

■

La fórmula anterior se conoce como la ***fórmula de Poincaré*** *y nos dice que que la dimensión de espacios vectoriales es una función aditiva.*

Definición 2.2.5 Sea R cualquier anillo y $Spec(R) = \{P \subset R : P \text{ es ideal primo de} R\}$ el espectro R. Una cadena de $Spec(R)$ es una sucesión ordenada (bajo la inclusión) de elementos de $Spec(R)$, la longitud de una cadena finita es su número de elementos. La dimensión de Krull de R se define como:

$$dimR := sup\{longitudes\ de\ cadenas\ de\ Spec(R)\}$$

Teorema 2.2.6 ***(Hilbert)****[29] Sea $R = K[x_0, \ldots, x_n]$ e I un ideal homogéneo de R tal que $dim(R/I) = k$. Entonces existe un polinomio $h_I(x) \in \mathbb{Q}[t]$ de grado $k-1$ (el grado del polinomio cero es -1) tal que $H_I(d) = h_I(d)$ para $d \gg 0$.*

Observación 2.2.7 *Dado X un subconjunto no vacío de $\mathbb{P}^n$, hemos definido una sucesión de códigos $\{C_X(d)\}_{d\in\mathbb{N}_0}$, la cual a su vez define una sucesión de enteros $\{H_X(d)\}_{d\in\mathbb{N}_0}$ donde $H_X(d) := H_{I_X}(d)$. Por el teorema de Hilbert-Serre la sucesión $\{H_X(d)\}_{d\in\mathbb{N}_0}$ diverge si $dimR/I > 1$ o es constante a partir de d suficientemente grande, como $C_X(d) \leq K^{|X|}\ \forall d$ entonces $H_X(d) \leq |X|\ \forall d$ luego $0 \leq dim(R/I_X) \leq 1$.*

Proposición 2.2.8 *[1, 25, 20, 23, 5] Sea $I = I_X$ entonces $I = \oplus_{r=\gamma_X}^{\infty} I_r$ con $I_{\gamma_X} \neq 0$ y γ_X es el grado más pequeño de las componentes homogéneas no triviales de I. Existe un elemento llamado el a- invariante de X (o el a-invariante del ideal I_X) denotado por a_X que satisface lo siguiente:*

1. $H_X(d) = \dim_K R_d = \binom{n+d}{d}$ *si y sólo si* $d < \gamma_X$.
2. $1 = H_X(0) < H_X(d) < H_X(d+1) < |X|$ *para* $0 \leq d < a_X$.
3. $1 < \delta(C_X(d+1)) < \delta(C_X(d))$ *para* $0 \leq d < a_X$.
4. $H_X(d) = |X|$ *para* $d > a_X$.
5. *El anillo R/I es un anillo Cohen-Macaulay cuya dimensión de Krull es* 1.

El número $\text{reg}(R/I) := a_X + 1$ es llamado el *índice de regularidad* o regularidad de R/I_X y es el mínimo entero tal que $H_X(d) = h_X(d) = |X|$.

Corolario 2.2.9 *$dim(R/I_X) = 1$ si X es no vacío.*

La utilidad del inciso 3 en nuestro caso particular: $\{C_X(d)\}_{d\in\mathbb{N}_0}$, es que estudia su eficiencia, pues para $d \geq a_X + 1$: $C_X(d) = K^{|X|}$ y por la cota de Singleton (ver Ec.(1.1.6)): $C_X(d)$ es un código de distancia mínima $\delta(C_X(d)) = 1$, el cual es inservible pues no detecta ni corrige errores. Por otro lado, debido a la naturaleza computacional de los códigos evaluación, a_X nos da una cota para generarlos.

Recordemos que una resolución graduada libre de R/I_X es una sucesión exacta de la forma:

$$0 \to \oplus R(-\alpha_{ir})^{\beta_{ir}} \to \cdots \to \oplus R(-\alpha_{i1})^{\beta_{i1}} \to R \to R/I_X \to 0$$

restringiendo a la componente d de la sucesión y usando la fórmula de Poincaré obtenemos la fórmula general para la función de Hilbert de I_X:

$$H_X(d) = \binom{m-1+d}{d} + \sum_{j=1}^{r}(-1)^j \sum_i \beta_{ij}\binom{m-1+d-\alpha_{ij}}{d-\alpha_{ij}} \tag{2.12}$$

Es decir, en términos de una resolución libre graduada finita (r.l.g.f) podemos recobrar la dimensión de $C_X(d)$. Macaulay 2 es un programa computacional que entre muchas cosas calcula una resolución libre graduada finita (r.l.g.f) cuando se conocen los generadores de I_X, por lo que es muy importante esta ecuación a la hora de generar códigos.

2.3. Bases de Gröbner

Como ya sabemos $K[x]$ es un $D.I.P$ y por el algoritmo de la división saber si $f \in K[x]$ pertenece a un ideal dado I, es equivalente a saber si el residuo de dividir a f por el polinomio generador de I es cero o no. Estos resultados son valiosos para el anillo $R = K[x_0, \ldots, x_n]$, pues aunque R no es D.I.P y por lo tanto no es Dominio Euclideano, si que es finitamente generado y preguntarnos si dado $f \in R$ y un conjunto finito de polinomios $\{f_1, \ldots, f_m\}$ ¿es siempre posible escribir a f como combinación de $\{f_1, \ldots, f_m\}$ más un polinomio r tal que si es distinto de cero, entonces f no pertenece a I (análogo a como pasa con el algoritmo de la división en $K[x]$)?. La respuesta es si, si el conjunto $\{f_1, \ldots, f_m\}$ satisface ciertas propiedades. [1]Ésta sección esta dedicada a mostrar los resultados más

[1]Para todos los detalles de esta sección vea la referencia [7]

importantes de la generalización del Algoritmo de la División en el anillo de polinomios en varias variables y como dicho algoritmo nos ayuda a saber si dado un polinomio $f \in K[x_0, \ldots, x_n]$ pertenece o no, a un ideal fijo I.

En esta sección R siempre denota el anillo de poliniomios $K[x_0, \ldots, x_n]$ y para cada $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^{n+1}$, x^α denota al monomio $x_0^{\alpha_0} \cdots x_n^{\alpha_n} \in R$.

Definición 2.3.1 Un orden monomial $\prec$ en R es cualquier relación $\prec$ en $\mathbb{Z}_{\geq 0}^{n+1}$, o equivalentemente, cualquier relación en el conjunto de monomios x^α, $\alpha \in \mathbb{Z}_{\geq 0}^{n+1}$, satisfaciendo:

- $\prec$ es un orden total en $\mathbb{Z}_{\geq 0}^{n+1}$.
- Si $\alpha \prec \beta$ y $\gamma \in \mathbb{Z}_{\geq 0}^{n+1}$, entonces $\alpha + \gamma \prec \beta + \gamma$.
- $\prec$ es un buen orden en $\mathbb{Z}_{\geq 0}^{n+1}$.

Si $\prec$ es un orden monomial y $\alpha, \beta \in \mathbb{Z}_{\geq 0}^{n+1}$ escribiremos $x^\alpha \prec x^\beta$ si $\alpha \prec \beta$.

Ejemplo 2.3.2 (Orden Lexicográfico). Sean $\alpha, \beta \in \mathbb{Z}_{\geq 0}^{n+1}$. Decimos que $\alpha \prec_{lex} \beta$ si la entrada no cero más a la izquierda del vector $\beta - \alpha \in \mathbb{Z}^{n+1}$ es positiva. Ésta relación se conoce como orden lexicográfico y es un orden monomial para R.

Ejemplo 2.3.3 (Orden Lexicográfico Inverso Graduado). Sean $\alpha, \beta \in \mathbb{Z}_{\geq 0}^{n+1}$. Decimos que $\alpha \prec_{grevlex} \beta$ si

$$|\alpha| = \sum_{i=0}^{n} \alpha_i < |\beta| = \sum_{i=0}^{n} \beta_i, \quad o$$

$|\alpha| = |\beta|$ y la entrada no cero más a la derecha de $\beta - \alpha \in \mathbb{Z}^{n+1}$ es negativa

Ésta relación se conoce como Orden Lexicográfico Inverso Graduado (grevlex) y es un orden monomial en R.

Sea $\prec$ un orden monomial en R, si $f \in R$ es un polinomio distinto de cero, $f = \sum_{i=1}^{r} a_1 x^{\alpha_i}$ con $a_i \in K^*$ y $x^{\alpha_r} \prec \ldots \prec x^{\alpha_1}$, al *monomio líder* x^{α_1} *de* f *se le denota por* $in_\prec(f)$ *y a* α_1 *se le conoce como el grado de* f.

Teorema 2.3.4 (Algoritmo de la División en $K[x_0, \ldots, x_n]$***).***
Sea $\prec$ *un orden monomial en* R *y* $F = \{f_1, \ldots, f_s\}$ *una* $s-$*tupla ordenada de polinomios. Entonoces cada* $f \in R$ *puede escribirse como*

$$f = h_1 f_1 + \cdots + h_s f_s + r,$$

tal que

- $h_i \in R$ *y* $in_\prec(h_i f_i) \preceq in_\prec(f)\ \forall i = 1, \ldots, s$.
- $r \in R$ *y* $r = 0$ *o* r *es combinación lineal de monomios con coeficientes en* K*, tal que ningún monomio es divisible por ningún* $in_\prec(f_1), \ldots, in(f_s)$.

A r *se le llama el residuo de dividir* f *por* F.

Como veremos en el siguiente ejemplo, r no siempre es único:

Ejemplo 2.3.5 Sea $f_1 = xy + 1$, $f_2 = y^2 - 1 \in K[x, y]$ con el orden lexicográfico. Dividir a $f = xy^2 - x$ por $F = \{f_1, f_2\}$ resulta:

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

Pero

$$xy^2 - x = x(y^2 - 1) = xf_2 \tag{2.13}$$

Recordemos que la información que queremos obtener del algoritmo de la división es, si dado $f \in R$ e I un ideal de R junto con un conjunto de generadores de I: $\{f_1, \ldots, f_s\}$ ¿es posible saber si f no está en I si y solo si el residuo de dividir a f por $\{f_1, \ldots, f_s\}$ es no cero?. En el Ejemplo 2.3.5 la ecuación 2.13 muestra que $f \in \langle f_1, f_2 \rangle$ aunque el residuo de dividir a f por $\{f_1, f_2\}$ sea distinto de cero y a simple vista este ejemplo puede destrozar el objetivo que buscamos, pero no perdamos la calma, esto sólo quiere decir que no todos las conjuntos generadores de un ideal I son buenos en este sentido. Por lo que nuestro siguiente objetivo es encontrar buenos conjuntos generadores de I.

Definición 2.3.6 Sea I un ideal de R junto con un orden monomial $\prec$. Definimos el ideal inicial de I como:

$$in_\prec(I) = \langle in_\prec(f) : f \in I \rangle$$

Proposición 2.3.7 *Sea* I *un ideal de* R.

- $in_\prec(I)$ *es un ideal monomial (un ideal generado por monomios).*
- *Existen* $g_1, \ldots, g_t \in I$ *tales que* $in_\prec(I) = \langle in_\prec(g_1), \ldots, in_\prec(g_t) \rangle$.

Definición 2.3.8 A un subconjunto de I como en la proposición anterior se le conoce como base de Gröbner.

Corolario 2.3.9 *Sea* $\mathcal{G} = \{g_1, \ldots, g_t\}$ *una base de Gröbner de un ideal I. Entonces* $I = \langle \mathcal{G} \rangle$.

Demostración. Es una consecuencia de la proposición anterior y del algoritmo de la división. ■

El corolario anterior nos dice que todo ideal I de R contiene una base de Gröbner y que dicho conjunto es un conjunto generador de I, y bueno, resulta que las bases de Gröbner de I son conjuntos generadores que se comportan bien bajo el algoritmo de la división:

Teorema 2.3.10 *Sea $\mathcal{G} = \{g_1, \ldots, g_t\}$ una base de Gröbner de un ideal $I \subset R$ y sea $f \in R$. Entonces existe un único $r \in R$ que satisface lo siguiente*

- *Ningún monomio de r es divisible por ningún elemento de $\{in_\prec(g_1), \ldots, in_\prec(g_t)\}$.*
- *Existe $g \in I$ tal que $f = g + r$*

En particular, r es el residuo de dividir a f por $\mathcal{G}$ no importando el orden que se le de a los elementos de $\mathcal{G}$. Por lo que $f \in I$ si y solo si el residuo de dividir a f por $\mathcal{G}$ es cero.

Lema 2.3.11 *Si I es un ideal de $K[x_0, \ldots, x_n]$ tal que $in_\prec(I)$ es primo, entonces I también es primo.*

Demostración. Para esta prueba utilizaremos fuertemente el Teorema 2.3.10.

Sean $f, g \in K[x_0, \ldots, x_n]$ no cero tales que $fg \in I$. Sí $\mathcal{G} = \{g_1, \ldots g_t\}$ es una base de Gröbner de I entonces $r_f r_g \in I$ donde r_f y r_g son los residuos de dividir a f y g por $\mathcal{G}$ respectivamente. Si $r_f r_g = 0$ es claro que $f \in I$ o $g \in I$, si $r_f r_g \neq 0$ el monomio $in_\prec(r_f r_g)$ pertenece a $in_\prec(I)$ pero sabemos que existen m_f y m_g monomios pertenecientes a la combinaciones lineales que definen a r_f y r_g respectivamente tales que $in_\prec(r_f r_g) = m_f m_g$ y como $in_\prec(I)$ es un ideal primo $m_f \in in_\prec(I)$ o $m_g \in in_\prec(I)$ lo cual contradice que r_f sea el residuo de dividir a f por $\mathcal{G}$ o que r_g sea el residuo de dividir a g por $\mathcal{G}$. ■

Definición 2.3.12 Sean f, $g \in K[x_0, \ldots, x_n]$ polinomios no cero

- Si el grado de f es α y el grado de g es β, entonces sea $\gamma = (\gamma_1, \ldots, \gamma_n)$ con $\gamma_i = max(\alpha_i, \beta_i)$. Definimos el mínimo común múltiplo de $in_\prec(f)$ y $in_\prec(g)$ como x^γ y para referirnos a el usamos la siguiente notación: $LCM(LM(f), LM(g)) := x^\gamma$.
- El S-polinomio de f y g es la combinación

$$S(f, g) = \frac{x^\gamma}{in_\prec(f)} \cdot f - \frac{x^\gamma}{in_\prec(g)} \cdot g \tag{2.14}$$

Teorema 2.3.13 *(Criterio de Buchberger's). Sea I un ideal de $K[x_0, \ldots, x_n]$ entonces un conjunto generador de I $\mathcal{G} = \{g_1, \ldots g_t\}$ es base de Gröbner de I si y sólo si, para cualesquiera pares disjuntos (g_i, g_j) el residuo de dividir a su correspondiente $S-$polinomio $S(g_i, g_j)$ por $\mathcal{G}$ (en algún orden) es igual a cero.*

En la sección anterior definimos para un subconjunto $X \subseteq \mathbb{P}^n$ la familia de códigos Reed-Muller generalizados $\{C_d(X)\}_{d\in\mathbb{N}_0}$ e hicimos la observación de que los elementos no cero de $C_d(X)$ pueden ser interpretados como polinomios que no se anulan en todo X, por el Teorema 2.3.10, es suficiente estudiar los residuos de dichos polinomios bajo alguna base de Gröbner $\mathcal{G}$. Más aún, si se conocen los generadores de I_X, bajo el algoritmo de la división se puede extraer una base de Gröbner de I_X y así encontrar una base para cada $C_X(d)$. Por lo cual ésta sección es tan importante, las bases de Gröbner son el método computacional para generar dichos códigos.

Capítulo 3

Familias de Códigos Reed-Muller Generalizados

Sea $X \subseteq \mathbb{P}^n$ junto con I_X su ideal anulador, en el capítulo anterior dejamos claro que la información que define a cada elemento de la familia $\{C_X(d)\}_{d\in\mathbb{N}_0}$ es:

1. La longitud de $C_X(d)$, es decir, el número de elementos de X.

2. Un conjunto generador de I_X y la fórmula general para la función de Hilbert de I_X (vea Eq.(2.12)), ambas para encontrar una base de $C_X(d)$ y su dimensión.

3. El índice de regularidad de I_X: $\mathrm{reg}(R/I_X)$, el cual da una cota para generar códigos detectores de errores.

4. La distancia mínima $\delta(C_X(d))$ cuando $d < \mathrm{reg(R/I_X)}$.

En este capítulo mostraremos fórmulas de los parámetros básicos e índice de regularidad de tres familias de códigos Reed-Mulller generalizados en términos de los parámetros de una familia ya muy estudiada: $\{C_{\mathbb{P}^n}(d)\}_{d\in\mathbb{N}_0}$. Para cada $d \in \mathbb{N}_0$, a $C_{\mathbb{P}^n}(d)$ se le conoce como Código Reed Muller Clásico de orden d.

3.1. Códigos Reed-Muller clásicos

En esta sección recordaremos cuales son los parámetros básicos de los códigos Reed-Muller clásicos. Los detalles del siguiente teorema se encuentran en la referencia [34].

Teorema 3.1.1 *Sea $K = \mathbb{F}_q$ un campo finito y sea $C_{\mathbb{P}^n}(d)$ el código clásico Reed-Muller de grado d en el conjunto $\mathbb{P}^n$. Entonces*

1. *Su longitud es:* $|\mathbb{P}^n| = \frac{q^{n+1}-1}{q-1}$

2. *Su dimensión esta dada por la fórmula general de la función de Hilbert:*

$$H_{\mathbb{P}^n}(d) = \sum_{\substack{i=d \bmod q-1 \\ 0<i\leq d}} \left(\sum_{j=0}^{n+1} (-1)^j \binom{n+1}{j} \binom{i-jq+n}{i-jq} \right) \tag{3.1}$$

y el ideal anulador de $\mathbb{P}^n$ *esta dado por:*

$$I_{\mathbb{P}^n} = \left\langle x_i^q x_j - x_i x_j^q,\ i<j:\ i,j=0,1,\ldots,n \right\rangle \subseteq K[x_0,\ldots,x_n] \tag{3.2}$$

3. *El índice de regularidad es*

$$\mathrm{reg(R/I_{\mathbb{P}^n})} = \mathrm{n(q-1)+1} \tag{3.3}$$

4. *Su distancia mínima:*

$$\delta_{\mathbb{P}^n}(d) = \begin{cases} (q-\ell+1)\, q^{n-k-1} & \text{if } d \leq n(q-1), \\ 1 & \text{if } d \geq n(q-1)+1, \end{cases} \tag{3.4}$$

donde $0 \leq k \leq n-1$ *y* ℓ *son los únicos enteros que satisfacen* $d = k(q-1)+\ell$ *con* $1 \leq \ell \leq q-1$.

Demostración. Vea [34] para las otras partes. Nosotros sólo vamos a probar la parte 1.

Recordemos que $\mathbb{P}^n$ se definió como $K^{n+1} - \{0\}$ bajo la relación de equivalencia $\sim$ (Definición 2.1.1). Así que $K^{n+1} - \{0\}$ se puede ver como la unión disjunta de todas las clases de equivalencia bajo $\sim$. Si K es un campo finito con q elementos se tiene que:

$q^{n+1} - 1 = |K^{n+1} - \{(0,\ldots,0)\}|$

$= \left| \bigcup_{P\in\mathbb{P}^n} P \right| = \sum_{P\in\mathbb{P}^n} |\{(Q_0,\ldots,Q_n):\ \exists \lambda \in K^* \text{ tal que } (Q_0,\ldots,Q_n) = \lambda(P_0,\ldots,P_n)\}|$

$= |\mathbb{P}^n|(q-1)$

y se sigue que $|\mathbb{P}^n| = \frac{q^{n+1}-1}{q-1}$. ■

Ejemplo 3.1.2 Sea K el campo $\mathbb{F}_8$. Si $\mathbb{X} = \mathbb{P}^2$, entonces los parámetros del código clásico Reed-Muller $C_{\mathbb{X}}(d)$ de grado d están dados por

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\lvert\mathbb{X}\rvert$	73	73	73	73	73	73	73	73	73	73	73	73	73	73	73
$H_{\mathbb{X}}(d)$	3	6	10	15	21	28	36	45	52	58	63	67	70	72	73
$\delta_{\mathbb{X}}(d)$	64	56	48	40	32	24	16	8	7	6	5	4	3	2	1

La regularidad de $S/I_{\mathbb{X}}$ es 15 y el a-invariante es 14.

Definición 3.1.3 Usando la notación del teorema anterior definimos el toro proyectivo como el subconjunto $\mathbb{T}^n$ de $\mathbb{P}^n$ dado por

$$\mathbb{T}^n = \{[P_0, \ldots, P_n] \in \mathbb{P}^n : P_0 \cdots P_n \neq 0\} \tag{3.5}$$

Observación 3.1.4 *El toro proyectivo $\mathbb{T}^n$ es un grupo abeliano bajo la multiplicación entrada a entrada e isomorfo a $(K^*)^n$.*

Enseguida recordaremos quienes son los parámetros básicos del código Reed-Muller generalizado sobre un toro proyectivo.

Proposición 3.1.5 *[9][24][30] Si $\mathbb{T}^n$ es el toro proyectivo en $\mathbb{P}^n$ y $C_{\mathbb{T}^n}(d)$ es el código clásico Reed-Muller de grado d asociado a $\mathbb{T}^n$ entonces para $C_{\mathbb{T}^n}(d)$ tenemos los siguiente:*

1. *Su longitud es: $|(K^*)^n| = (q-1)^n$*

2. *Su dimensión esta dada por la fórmula general de la función de Hilbert:*

$$H_{\mathbb{T}^n} = \sum_{j=0}^{\lfloor d/(q-1) \rfloor} (-1)^j \binom{n}{j} \binom{n+d-j(q-1)}{n} \tag{3.6}$$

   y el ideal anulador de $\mathbb{T}^n$ esta dado por:

$$I_{\mathbb{P}^n} = \left\langle x_i^{q-1} - x_0^{q-1} : \ i = 1, \ldots, n \right\rangle \subseteq K[x_0, \ldots, x_n] \tag{3.7}$$

3. *El índice de regularidad es*

$$\mathrm{reg}(\mathrm{R}/\mathrm{I}_{\mathbb{T}^n}) = \mathrm{n}(\mathrm{q}-2) \tag{3.8}$$

4. *Su distancia mínima:*

$$\delta_{\mathbb{T}^n}(d) = (q-1)^{n+1-(k-2)}(q-1-l) \tag{3.9}$$

   para todo $d < \mathrm{reg}(\mathrm{R}/\mathrm{I}_{\mathbb{T}^n})$ donde $0 \leq k$ y $1 \leq l \leq q-2$ son los únicos enteros tales que $d = k(q-2)+l$.

3.2. Código asociado a la inmersión de Veronese

Definición 3.2.1 Para $m, n > 0$ dados, sean $M_0, M_1, \ldots, M_N$ $(N = \binom{m+n}{m} - 1)$ todos los monomios de grado n que pertenecen $K[X_0, \ldots, X_m]$ con K un campo. Definimos la inmersión n-ésima de Veronese como la función

$$\rho_n : \mathbb{P}^m \longrightarrow \mathbb{P}^N$$
$$P = [p_0, \ldots, p_m] \mapsto [M_0(P), \ldots, M_N(P)]$$

Proposición 3.2.2 *La inmersión n-ésima de Veronese está bien definida y es inyectiva. En particular, si K es un campo con q elementos entonces* $|\rho_n(\mathbb{P}^m)| = |\mathbb{P}^m| = \frac{q^{m+1}-1}{q-1}$.

***Demostración*.** Sean $P = [p_0, \ldots, p_m], Q = [q_0, \ldots, q_m] \in \mathbb{P}^m$.

a) Como $\exists l$ tal que $p_l \neq 0$ entonces $X_l^n(P) = p_l^n \neq 0$, así no todas las entradas de $\rho_n(P)$ son cero. Ahora supongamos que $P = Q$, entonces existen $P', Q' \in \mathbb{A}^{m+1}$ y $\lambda \neq 0$ tales que $Q' = (q'_0, \ldots, q'_m) = \lambda(p'_0, \ldots, p'_m) = \lambda P'$ con $\lambda \in K^*$, se sigue que $\rho_n(Q) = \lambda^n \rho_n(P) = \rho_n(P)$.

b) Sean $P, Q \in \mathbb{P}^m$ tales que $\rho_n(P) = \rho_n(Q)$ entonces existe $\exists \lambda \neq 0$ tal que

$$p_0{}^{i_0} \cdots p_m{}^{i_m} = \lambda q_0{}^{i_0} \cdots q_m{}^{i_m}$$

con $i_0 + \cdots + i_m = n$.

Sin pérdida de generalidad supongamos que $p_0 \neq 0$ entonces $p_0^n = \lambda q_0^n$ implica $q_0 \neq 0$. Sea $\lambda' = \frac{q_0}{p_0} \in K^*$ entonces $q_0 = \lambda' p_0$ y

$$p_0^{n-1} = \lambda \lambda' q_0^{n-1} \tag{3.10}$$

Por hipótesis

$$p_0^{n-1} p_i = \lambda q_0^{n-1} q_i \quad \forall i = 0, \ldots, m$$

usando la ecuación (3.10) se tiene

$\lambda \lambda' q_0^{n-1} p_i = \lambda q_0^{n-1} q_i \ \ \forall i = 0, \ldots, m$. Por lo que $q_i = \lambda' p_i \ \forall i = 0, \ldots, m$, demostrando que $P = Q$.

■

Teorema 3.2.3 *Sea* $\mathbb{S} = \rho_n(\mathbb{P}^m)$ *un subconjunto de el espacio proyectivo* $\mathbb{P}^N$ *sobre un campo K con q elementos. Si* $C_{\mathbb{S}}(d)$ *denota el código Reed-Muller generalizado de grado d asociado a* $\mathbb{S}$*, entonces lo siguiente se satisface.*

1. *La longitud del código* $C_{\mathbb{S}}(d)$ *es* $\frac{q^{m+1}-1}{q-1}$.

2. *Para cada* $d \geq 0$, *la dimensión de* $C_X(d)$ *es*

$$H_{\mathbb{S}}(d) = H_{\mathbb{P}^m}(nd) \tag{3.11}$$

y si $n \leq q$ *el ideal anulador de* $\mathbb{S}$ *esta dado por*

$$I_{\mathbb{S}} = \langle I_{\mathbb{S}}(2), I_{\mathbb{S}}(r+1) \rangle \subset K[Y_0, \ldots, Y_N] \tag{3.12}$$

Donde $r = \frac{q-l}{n}$ *y* $l \in [0, n-1]$ *es tal que* $l \equiv q \ mod \ n$.

3. *El índice de regularidad asociado a* $C_X(d)$ *es*

$$\mathrm{reg}(\mathrm{R_N}/\mathrm{I_{\mathbb{S}}}) = \begin{cases} \frac{a_m+1-j}{n} + 1 & si \ a_m + 1 \equiv j \ mod \ n \ y \ j > 0 \\ \frac{a_m+1}{n} & si \ a_m + 1 \equiv 0 \ mod \ n \end{cases} \tag{3.13}$$

Donde a_m *denota el* $a-$*invariante de* $R_m/I_{\mathbb{P}^m}$.

4. *la distancia mínima es* $\delta_{\mathbb{S}}(d) = \delta_{\mathbb{P}^m}(nd) \ \forall d \geq 0$.

Demostración.

El inciso 1 se sigue de la proposición anterior.

Para probar 2 es suficiente ver que $(R_N/I_{\mathbb{S}})_d \cong_K (R_m/I_{\mathbb{P}^m})_{nd}$. Sea $f \in (R_N)_d$, definimos el $K-$morfismo

$$\varphi : (R_N)_d \to (R_m)_{nd}$$
$$f \mapsto \varphi_f := f(M_0, \ldots, M_N)$$

Notemos que si $x_0^{i_0} \cdots x_m^{i_m}$ es de grado nd podemos reescribirlo como producto de d monomios de grado n, luego φ es epimorfismo. Sea f un polinomio homogéneo tal que $f \in (I_{\mathbb{S}})_d$ y $[Q] \in \mathbb{P}^m$ entonces $\varphi_f([Q]) = f(M_0([Q]), \ldots, M_N([Q])) = f(\rho_n([Q])) = 0$ por lo que φ induce un $K-$isomorfismo

$$\varphi_d : (R_N/I_{\mathbb{S}})_d \to (R_m/I_{\mathbb{P}^m})_{nd}$$

φ_d es epimorfismo pues φ es epimorfismo. Para ver que φ_d es un monomorfismo, sea $f \in (R_N)_d$ tal que $\varphi_f \in (I_{\mathbb{P}^m})_{nd}$ y sea $[P'] \in \mathbb{S}$ entonces $\exists [P] \in \mathbb{P}^m$ tal que $\rho_n([P]) = [P']$ luego $f([P']) = f(\rho_n([P])) = \varphi_f([P]) = 0$. Por lo que $f \in (I_{\mathbb{S}})_d$.

Ahora probaremos que la Ecuación (3.12) se satisface. Sea $\overline{K}$ la cerradura algebraica de K y sea $\overline{\mathbb{S}}$ la cerradura algebraica de la variedad de Veronese, i.e., la imagen de $\mathbb{P}^m(\overline{K})$ bajo la función $\rho_n : \mathbb{P}^m(\overline{K}) \to \mathbb{P}^N(\overline{K})$, y sea $I_{\overline{\mathbb{S}}}$ el ideal anulador de $\overline{\mathbb{S}}$.

Este resultado es una generalización del caso $m = 1$

Ya que $I_{\mathbb{S}} = \oplus_{d\geq 2}(I_{\mathbb{S}})_d$, con el fin de probar la afirmación del teorema es suficiente demostrar que

$$(I_{\mathbb{S}})_d = \sum_{i=0}^{N} Y_i (I_{\mathbb{S}})_{d-1} \tag{3.14}$$

para todo $d \geq 3$ y $d \neq r+1$. Donde $Y_i(I_{\mathbb{S}})_{d-1} := \{Y_i f | f \in (I_{\mathbb{S}})_{d-1}\}$ es subgrupo de $(I_{\mathbb{S}})_d$. Consideraremos dos casos: a) $3 \leq d \leq r$ y b) $d \geq r+2$.

Pero primero haremos un paréntesis para explicar una serie de resultados necesarios para la prueba.

Si d es cualquier entero tal que $nd < q+1$, desde que $I_{\mathbb{P}^m} =< (I_{\mathbb{P}^m})_{q+1} >$ entonces $\varphi_f = 0$ para todo $f \in (I_{\mathbb{S}})_d$ por lo que $\varphi_f \in (I_{\mathbb{P}^m(\overline{K})})_{nd}$ luego $f \in (I_{\overline{\mathbb{S}}})_d$ (donde φ_f fué definida algunos párrafos antes), demostrando que $(I_{\mathbb{S}})_d \subseteq (I_{\overline{\mathbb{S}}})_d$.

Ya que $I_{\overline{\mathbb{S}}} =< (I_{\overline{\mathbb{S}}})_2 >$ entonces para todo $d \geq 3$, se tiene $(I_{\overline{\mathbb{S}}})_d = \sum_{i=0}^{N} Y_i (I_{\overline{\mathbb{S}}})_{d-1}$.

- $d = 3$. Sea $f \in (I_{\overline{\mathbb{S}}})_3$, ya que $f \in < (I_{\overline{\mathbb{S}}})_2 >$: $f = \sum_i g_{1,i} f_{2,i}$ con $g_{1,i} \in (R_N)_1$, $f_{2,i} \in (I_{\overline{\mathbb{S}}})_2$. Así

$$f = \sum_{i=0}^{N} Y_i f'_{2,i} \quad f'_{2,i} \in (I_{\overline{\mathbb{S}}})_2 \ \forall i \in 0, \ldots, N \tag{3.15}$$

  es decir, $f \in \sum_{i=0}^{N} Y_i (I_{\overline{\mathbb{S}}})_2$

- $d = 4$. Sea $g \in (I_{\overline{\mathbb{S}}})_4$

$$f = \sum_{i=0,j=0}^{N} Y_i Y_j g_{2,(i,j)} = \sum_{i=0}^{N} Y_i (\sum_{j=0}^{N} Y_j g'_{2,(i,j)}) \quad g_{2,(i,j)}, g'_{2,(i,j)} \in (I_{\overline{\mathbb{S}}})_2 \ \forall i,j \in [0,N] \tag{3.16}$$

  Como $\sum_{j=0}^{N} Y_j g'_{2,(i,j)} \in (I_{\overline{\mathbb{S}}})_3$, $g \in \sum_{i=0}^{N} Y_i (I_{\overline{\mathbb{S}}})_3$.

De manera inductiva podemos probar que $(I_{\overline{\mathbb{S}}})_d = \sum_{i=0}^{N} Y_i (I_{\overline{\mathbb{S}}})_{d-1}$.

a) $3 \leq d \leq r$. Es decir, $3n \leq nd \leq q - l < q + 1$.
Sea $W = \sum_{i=1}^{N} Y_i (I_{\mathbb{S}})_{d-1}$ y $\overline{W} = \sum_{i=1}^{N} Y_i (I_{\overline{\mathbb{S}}})_{d-1}$, si $\{f_i\}_i$ una base para el $K-$espacio vectorial W, entonces $\{f_i \otimes_K 1\}_i$ es una base para el $\overline{K}-$espacio vectorial $W \otimes_K \overline{K}$ por lo tanto $dim_K W = dim_{\overline{K}} W \otimes_K \overline{K}$, además $W \otimes_K \overline{K} \simeq_K \overline{W} = (I_{\overline{\mathbb{S}}})_d$, se sigue que $dim_K (I_{\mathbb{S}})_d = dim_{\overline{K}} (I_{\overline{\mathbb{S}}})_d = dim_K W$, por lo tanto $W = (I_{\mathbb{S}})_d$.

b) $d \geq r + 2$. Como $\frac{q-l}{n} + 1 \leq d - 1$, tenemos $q + (n - l) \leq n(d - 1)$, por lo tanto $q+1 \leq n(d-1) < nd$. Así si $f \in (I_{\mathbb{S}})_d$ entonces $\varphi_f \in (I_{\mathbb{P}^m})_{nd} =< X_i^q X_j - X_i X_j^q$, $0 \leq i < j \leq m >$ y así $\varphi_f = \sum_{0 \leq i < j \leq m} g_{ij}(X_i^q X_j - X_i X_j^q)$ donde g_{ij}'s son formas de grado $nd - (q + 1)$. Ya que $n(d - 1) \geq q + 1$, i.e, $nd - (q + 1) \geq n$ los g_{ij}'s pueden escribirse como: $g_{ij} = M_0 h_{ij}(1) + \cdots + M_N h_{ij}(N)$, donde los M_l son monomios de grado n y los $h_{ij}(l)$ son formas de grado $nd - (q + 1) - n$. Así

$$\varphi_f = \sum_{i,j} \sum_{l=0}^{N} M_l h_{ij}(l)(X_i^q X_j - X_i X_j^q)$$

Note que para todo i, j, l, la forma $h_{ij}(l)(X_i^q X_j - X_i X_j^q) \in (I_{\mathbb{P}^m})_{n(d-1)}$. Por lo tanto $\varphi_f = M_0 H_{i0} + \cdots + M_N H_{iN}$ con M_l monomios en las variables $X_0, \ldots, X_m$ de grado n y $H_{ij} \in (I_{\mathbb{P}^m})_{n(d-1)}$. Se sigue que $f = Y_0 \lambda_{i0}(H_{i0}) + \cdots + Y_N \lambda_{iN}(H_{iN})$ donde cada $\lambda_{ij}(H_{ij})$ está en $(I_{\mathbb{S}})_{d-1}$ y es tal que $\varphi_{\lambda_{ij}(H_{ij})} = H_{ij}$. Del argumento anterior se concluye que $f \in \sum_{i=0}^{N} Y_i (I_{\mathbb{S}})_{d-1}$.

Para probar 3, supongamos que $a_m + 1 \equiv j \mod n$ con $0 < j < n$ sea $d = \frac{a_m + 1 - j}{n}$, entonces $H_{\mathbb{S}}(d+1) = H_{\mathbb{P}^m}(n(d+1))$. Como $n(d+1) = a_m + 1 - j + n$ y $n - j > 0$, se sigue que $n(d+1) > a_m$ y por lo tanto $H_{\mathbb{S}}(d+1) = s$. Además, como $j > 0$, se tiene que $a_m + 1 - j < a_m + 1$ por lo que $H_{\mathbb{S}}(d) = H_{\mathbb{P}^m}(nd) = H_{\mathbb{P}^m}(a_m + 1 - j) < s$. De la definición del a-invariante se sigue que $d = a_{\mathbb{S}}$. El caso $j = 0$ es similar ya que si $d = \frac{a_m+1}{n} - 1$, entonces $H_{\mathbb{S}}(d) = H_{\mathbb{P}^m}(nd) = H_{\mathbb{P}_m}(a_m + 1 - n) < |\mathbb{P}^m| = s$, y $H_{\mathbb{S}}(d + 1) = H_{\mathbb{P}^m}(n(d + 1)) = H_{\mathbb{P}^m}(a_m + 1) = |\mathbb{P}^m| = s$, demostrando que $a_s = \frac{a_m+1}{n} - 1$.

Sea $f \in (R_N)_d$ un polinomio homogéneo de grado d, y sea $M_0, \ldots, M_N$ todos los monomios de grado n en las variables $X_0, \ldots, X_m$. Entonces $f(M_0, \ldots, M_N) \in (R_m)_{nd}$. Sea $\mathbb{P}^m = \{P_1, \ldots, P_s\}$ y $Q_i = v_n(P_i) = [M_0(P_i), \ldots, M_N(P_i)] \in \mathbb{S}$, $i = 1, \ldots, s$. Si $Z = (f(Q_1), \ldots, f(Q_s)) \in C_{\mathbb{S}}(d)$, entonces

$$Z = (f(M_0, \ldots, M_N)(P_1), \ldots, f(M_0, \ldots, M_N)(P_{m_1})) \tag{3.17}$$

pertenece a $C_{\mathbb{P}^m}(nd)$ así $\delta_m(nd) \leq w(Z)$. La otra desigualdad se sigue por el isomorfismo inducido por la función φ entre los K-espacios vectoriales $(R_N)_d/(I_{\mathbb{S}})_d$ y $(R_m)_{nd}/(I_{\mathbb{P}^m})_{nd}$.

■

Ejemplo 3.2.4 Sea $K = \mathbb{F}_8$ y $\rho_2 : \mathbb{P}^2 \to \mathbb{P}^5$ la inversión de Veronese de grado 2 con $S = \rho_2(\mathbb{P}^2)$.

Como $\mathrm{reg}(\mathrm{R}_2/\mathrm{I}_{\mathbb{P}^2}) = 15$ de la ecuación 3.13 se tiene que $\mathrm{reg}(\mathrm{R}_5/\mathrm{I}_{\mathrm{s}}) = 8$.

Los parámetros básicos de $\{C_S(d)\}_{0 \leq d \leq 8}$ por Teorema 3.2.3 y tabla del Ejemplo 3.1.2 son

d	1	2	3	4	5	6	7	8
$\lvert S\rvert = \lvert\mathbb{P}^2\rvert$	73	73	73	73	73	73	73	73
$H_S(d) = H_{\mathbb{P}^2}(2d)$	6	15	28	45	58	67	72	73
$\delta_{\mathbb{S}}(d) = \delta_{\mathbb{P}^2}(2d)$	56	40	24	8	6	4	2	1

Ya que $\mathrm{reg}(\mathrm{R}_5/\mathrm{I}_{\mathrm{S}}) \equiv 0 \bmod 2$ por el Teorema 3.2.3 $I_S =< (I_S)_2, (I_S)_5 >$.

3.3. Código asociado a la inmersión de Segre

Definición 3.3.1 Sea $\mathbb{P}^n$ y $\mathbb{P}^m$ el espacio proyectivo sobre un campo K, se define la inmersión de Segre como:

$$\psi : \mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^N$$

$$([a_0, \ldots, a_n], [b_0, \ldots, b_m]) \mapsto [a_0b_0, \ldots, a_0b_m, a_1b_0, \ldots, a_1b_m, \ldots, a_nb_0, \ldots, a_nb_m] \tag{3.18}$$

donde $N = n + m + nm$. La imagen de ψ es una variedad algebraica conocida como la variedad de Segre.

Proposición 3.3.2 *ψ está bien definida y es inyectiva. En particular, si K es un campo finito $|\psi(\mathbb{P}^n \times \mathbb{P}^m)| = |\mathbb{P}^n||\mathbb{P}^m|$.*

Demostración. Veamos que ψ está bien definida, es claro que ψ no se anula en todos los puntos de su imagen. Sean $\alpha, \beta \in K^*$, entonces

$$\psi([\alpha a_0, \ldots, \alpha a_n], [\beta b_0, \ldots, \beta b_m]) = [\ldots, \alpha\beta a_i b_j, \ldots] =$$

$$\alpha\beta[\ldots, a_i b_j \ldots] = \psi([a_0, \ldots, a_n], [b_0, \ldots, b_m]).$$

ψ es inyectiva, sean $A = [a_0, \ldots, a_n]$, $B = [b_0, \ldots, b_m]$, $C = [c_0, \ldots, c_n]$ y $D = [d_0, \ldots, d_m]$ tales que $\psi(A, B) = \psi(C, D)$, esto es $(\ldots, a_i b_j, \ldots) = \lambda(\ldots, c_i d_j, \ldots)$ para algún $\lambda \in K^*$, podemos hallar un $b_k \neq 0$ y un $d_j \neq 0$, entonces, en particular tenemos que $b_k a_i = \lambda d_j c_i \, \forall \, i = 0, \ldots, n$, i.e., $a_i = \frac{\lambda d_j}{b_k} c_i$ y esto nos dice que $A = C$, se procede de manera análoga para mostrar que $B = D$, por lo que ψ es inyectiva. ■

Proposición 3.3.3 *Si K es un campo algebraicamente cerrado, el ideal anulador de $\psi(\mathbb{P}^n \times \mathbb{P}^m)$ es $\langle z_{ij} z_{kl} - z_{il} z_{kj} \rangle$ en el anillo de polinomios $K[z_{00}, \ldots, z_{nm}]$.*

Demostración. Vea [19] ■

Teorema 3.3.4 *Sea $X = \psi(\mathbb{P}^n \times \mathbb{P}^m)$ un subconjunto de el espacio proyectivo $\mathbb{P}^N$ sobre un campo K con q elementos. Si $C_X(d)$ denota el código Reed-Muller generalizado de grado d asociado a X, entonces lo siguiente se satisface.*

1. *La longitud del código $C_X(d)$ es $(\frac{q^{n+1}-1}{q-1})(\frac{q^{m+1}-1}{q-1})$.*
2. *Para cada $d \geq 0$, la dimensión de $C_X(d)$ es*

$$H_X(d) = H_{\mathbb{P}^n}(d) H_{\mathbb{P}^m}(d) \tag{3.19}$$

Y el ideal anulador de la variedad de Segre es de la forma

$$I_X = \langle (I_X)_2, (I_X)_{q+1} \rangle \tag{3.20}$$

3. *El índice de regularidad asociado a $C_X(d)$ es:*

$$\mathrm{reg}(\mathrm{R_N}/\mathrm{I_X}) = \max\{\mathrm{reg}(\mathrm{R_n}/\mathrm{I_{\mathbb{P}^n}}), \mathrm{reg}(\mathrm{R_m}/\mathrm{I_{\mathbb{P}^m}})\} \tag{3.21}$$

4. *La distancia mínima es $\delta_X(d) = \delta_{\mathbb{P}^n}(d)\delta_{\mathbb{P}^m}(d) \; \forall d \geq 0$.*

Demostración. Para este teorema usaremos la siguiente notación: $\overline{K}$ denota la cerradura algebraica de K y $R_n = K[x_0, \ldots, x_n]$, $R_m = K[y_0, \ldots, y_m]$, $R_N = K[z_{00}, \ldots, z_{nm}]$ denotan los anillos de polinomios correspondientes a $\mathbb{P}^n$, $\mathbb{P}^m$, $\mathbb{P}^N$ y $\overline{R}_n = \overline{K}[x_0, \ldots, x_n]$, $\overline{R}_m = \overline{K}[y_0, \ldots, y_m]$, $\overline{R}_N = \overline{K}[z_{00}, \ldots, z_{nm}]$ son los anillos de polinomios correspondientes a $\mathbb{P}^n(\overline{K})$, $\mathbb{P}^m(\overline{K})$, $\mathbb{P}^N(\overline{K})$.

El inciso 1 se sigue de la proposición anterior.

Probemos 2: Sea $B = K[x_0y_0, \ldots, x_ny_m] \subset K[x_0, \ldots, x_n, y_0, \ldots, y_m]$ el álgebra graduada dada por:

$$B_d = \left\langle \sum_{I,J} a_{I,J} x^I y^J | a_{IJ} \in K,\ |I| = |J| = d \geq 0 \right\rangle_K$$

entonces el epimorfismo

$$\theta : (R_N)_d \to B_d$$
$$f \mapsto \theta_f := f(x_0y_0, \ldots, x_ny_m)$$

es tal que $\ker\theta = (I_X)_2(R_N)_{d-2}$. De la proposición 3.3.3 se tiene que $(I_X)_2 = \langle z_{ij}z_{kl} - z_{il}z_{kj}\rangle_K$ por lo que $(I_X)_2(R_N)_{d-2} \subseteq \ker\theta$.

Probemos que $\ker\theta \subseteq (I_X)_2(R_N)_{d-2}$. Sea $\{Q_{ij}\}$ una base de Gröbner de $\langle (I_X)_2\rangle$ entonces cada Q_{ij} es homogéneo de grado 2 y sea $f \in \ker\theta$, usando el algoritmo de la división $f = \sum_{i,j} f_{ij}Q_{ij} + r$ donde $f_{ij} \in (R_N)_{d-2}$ y ningún monomio de r es divisible por $in_\prec(Q_{ij})$, como $z_{ij}z_{kl} \in in_\prec(\langle (I_X)_2\rangle)$ entonces alguno de los Q_{ij} dividen a cada $z_{ij}z_{kl}$ pero como son del mismo grado $\{z_{ij}z_{kl}\} \subseteq \{in_\prec(Q_{ij})\}$ luego $r = \sum_{i,j} a_{ij}z_{ij}^d$ y se sigue que $\sum_{i,j} a_{ij}(x_iy_j)^d = \theta(r) = \theta(f) = 0$ por lo que $a_{ij} = 0\ \forall i, j$, es decir, $r = 0$.

Sea $\pi \circ \theta$ la transformación lineal suprayectiva

$$(R_N)_d \xrightarrow{\theta} B_d \xrightarrow{\pi} B_d/V_d$$
$$f \to \theta_f \to \theta_f + V_d$$

Entonces $(I_X)_d = \ker(\pi \circ \theta)$. Donde $V_d = (I_{\mathbb{P}^n})_d(R_m)_d + (I_{\mathbb{P}^m})_d(R_n)_d \subset B_d$ y

$$(I_{\mathbb{P}^n})_d(R_m)_d = \left\langle \sum_i f_i(x)f_i'(y) : f_i(x) \in (I_{\mathbb{P}^n})_d,\ f_i'(y) \in (R_m)_d \right\rangle_K \tag{3.22}$$

$$(I_{\mathbb{P}^m})_d(R_n)_d = \left\langle \sum_i g_i'(y)g_i(x) : g_i'(y) \in (I_{\mathbb{P}^m})_d,\ g_i(x) \in (R_n)_d \right\rangle_K \tag{3.23}$$

Si $f \in \ker(\pi \circ \theta)$ entonces $\theta_f \in V_d$. En este caso $\theta_f = \sum_i (f_i(x)f_i'(y) + g_i(x)g_i'(y))$ y $f(\psi(A, B)) = \theta_f(A, B) = 0\ \ \forall\ \ A \in \mathbb{P}^n\ , B \in \mathbb{P}^m$. Probando que $f \in I_X(d)$.

Si $f \in (I_X)_d$, $\theta_f(A, B) = 0\ \forall A \in \mathbb{P}^n, B \in \mathbb{P}^m$, entonces $\forall\lambda \in K^*\ \forall a = (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}$ con algún $a_i \neq 0$ y $\forall b = (b_0, \ldots, b_n) \in \mathbb{A}^{m+1}$ con algún $b_j \neq 0$ $\theta_f((\lambda a, \lambda b)) =$

$\theta_f(\lambda(a,b)) = 0$ y cuando $a = 0$ o $b = 0$ $\theta_f(\lambda a, \lambda b) = 0$ $\forall \lambda \in K$ por lo que $\theta_f(D) = 0$ $\forall D \in \mathbb{P}^s$ $(s = n + m + 1)$ luego $\theta_f \in I_{\mathbb{P}^s}$ y por el teorema 3.1.1 ecuación 3.2 se tiene lo siguiente

$$\theta_f(x,y) = \sum_{0\leq i<j\leq n} f_{ij}(x,y)({x_i}^q x_j - {x_j}^q x_i) + \sum_{0\leq i<j\leq m} g_{ij}(x,y)({y_i}^q y_j - {y_j}^q y_i) + \sum_{\substack{0\leq i\leq n \\ 0\leq j\leq m}} h_{ij}(x,y)({x_i}^q y_j - {y_j}^q x_i) \tag{3.24}$$

Donde $f_{ij}(x,y),\ g_{ij}(x,y),\ h_{ij}(x,y)$ son polinomios homogéneos de grado $2d-(q+1)$. Sea $a \in \mathbb{A}^{n+1}$ y $b \in \mathbb{A}^{m+1}$

$$\theta_f(x,b) = \sum_{0\leq i<j\leq m} f_{ij}(x,b)({x_i}^q x_j - {x_j}^q x_i) + \sum_{\substack{0\leq i\leq n \\ 0\leq j\leq m}} h_{ij}(x,b)({x_i}^q b_j - {b_j}^q x_i) \tag{3.25}$$

$$\theta_f(a,y) = \sum_{0\leq i<j\leq m} g_{ij}(a,y)({y_i}^q y_j - {y_j}^q y_i) + \sum_{\substack{0\leq i\leq n \\ 0\leq j\leq m}} h_{ij}(a,y)({a_i}^q y_j - {y_j}^q a_i) \tag{3.26}$$

Notando que los polinomios ${x_i}^q b_j - {b_j}^q x_i$, ${a_i}^q y_j - {y_j}^q a_i$ no son homogéneos, se sigue que $h_{ij}(x,y)$ es el polinomio cero, así:

$$\theta_f(x,y) = \sum_{0\leq i<j\leq n} f_{ij}(x,y)({x_i}^q x_j - {x_j}^q x_i) + \sum_{0\leq i<j\leq m} g_{ij}(x,y)({y_i}^q y_j - {y_j}^q y_i) \tag{3.27}$$

Consideraremos los siguientes casos:

- $2d < q+1$. Como θ_f tiene grado $2d$ en $K[x,y]$ y $\theta_f \in I_{\mathbb{P}^s}$ es combinación de polinomios de grado $q+1 > 2d$ entonces $\theta_f = 0$.

- $d < q+1$, $q+1 < 2d$.
  Los polinomios $g_{ij}(a,y)({y_i}^q y_j - {y_j}^q y_i)$, $f_{ij}(x,b)(x_i^q x_j - x_j^q x_i)$ son homogéneos de grado d y los polinomios $g_{ij}(a,y),\ h_{ij}(a,y)$ son polinomios homogéneos de grado $d-(q+1)$ o son el polinomio cero, de la hipótesis $d < q+1$ dichos polinomios son el polinomio 0 por lo que $\theta_f(x,y) \in V_d$.

- $d \geq q+1$.
  En este caso $\theta_f(x,y) = \sum f_{ij}(x,y)(x_i{}^q x_j - x_j{}^q x_i) + \sum g_{ij}(x,y)(y_i{}^q y_j - y_j{}^q y_i)$ donde $f_{ij}(a,y), g_{ij}(x,b)$, son polinomios homogéneos de grado d y $f_{ij}(x,b)$, $g_{ij}(a,y)$ son polinomios homogéneos de grado $d-(q+1)$ por lo que:

$$f_{ij}(x,y) = f'_{ij}(y)f''_j(x) \qquad f'_{ij}(y) \in (R_m)_d,\ f''_{ij}(x) \in (R_n)_{d-(q+1)}$$
$$g_{ij}(x,y) = g'_{ij}(x)g''_j(y) \qquad g'_{ij}(x) \in (R_n)_d,\ f''_{ij}(y) \in (R_m)_{d-(q+1)}$$

$$\theta_f(x,y) = \sum (f''_{ij}(x)(x_i{}^q x_j - x_j{}^q x_i))f'_{ij}(y) + \sum (g''_{ij}(y)(y_i{}^q y_j - y_j{}^q y_i))f'_{ij}(x)$$

  Ya que $f''_{ij}(x)(x_i{}^q x_j - x_j{}^q x_i) \in (I_{\mathbb{P}^n})_d$ y $g''_{ij}(y)(y_i{}^q y_j - y_j{}^q y_i) \in (I_{\mathbb{P}^m})_d$, $\theta_f \in V_d$.

Así $(R_N)_d/(I_X)_d \cong_K B_d/V_d$. Más aún: $B_d/V_d \cong_K (R_n/I_{\mathbb{P}^n})_d \otimes_K (R_m/I_{\mathbb{P}^m})_d$ (el isomorfismo natural). Tomando dimensiones se tiene que $H_X(d) = H_{\mathbb{P}^n}(d)H_{\mathbb{P}^m}(d)$.

Ahora probemos que $I_X = \langle (I_X)_2, (I_X)_{q+1} \rangle$. Sea $f \in (I_X)_d$

- Si $d < q+1$. $\theta_f = 0$, luego $f \in (I_X)_2(R_N)_{d-2}$, así $f \in \langle (I_X)_2, (I_X)_{q+1} \rangle$
- Si $d > q+1$.
  Basta demostrar que $(I_X)_d \subset W$, donde $W := \sum_{i,j} z_{ij}(I_X)_{d-1}$.
  Sabemos que $\theta_f(x,y) = \sum (f''_{ij}(x)(x_i{}^q x_j - x_j{}^q x_i))f'_{ij}(y) + \sum (g''_{ij}(y)(y_i{}^q y_j - y_j{}^q y_i))f'_{ij}(x) = \sum f''_{ij}(x)f'_{ij}(y)(x_i{}^q x_j - x_j{}^q x_i) + \sum g''_{ij}(y)f'_{ij}(x)(y_i{}^q y_j - y_j{}^q y_i)$ y como los polinomios $f''_{ij}(x)$, $f'_{ij}(y)$, $g''_{ij}(y)$, $f'_{ij}(x)$ son de grado positivo podemos reescribir a $\theta_f(x,y) = \sum_{i,j} x_i y_j m_{i,j}(x,y)$ con $m_{i,j}(x,y) \in (I_{\mathbb{P}^s})_{2d-2}$ por lo que $f(z) = \sum_{i,j} z_{ij} M_{i,j}(z)$ con $M_{i,j}(z) \in (I_X)_{d-1}$, es decir, $f \in W$.

El inciso 3 se sigue de 2.

Por último probemos el inciso 4: Sea $f \in (R_N)_d$ y sea $X = \{C_{11}, \ldots, C_{l_1 l_2}\}$ con $l_1 = \frac{q^{n+1}-1}{q-1}$, $l_2 = \frac{q^{m+1}-1}{q-1}$ y $C_{ij} = \psi(A_i, B_j)$ con $A_i \in \mathbb{P}^n$, $B_j \in \mathbb{P}^m$.
Sea $\Lambda = ev_d(f) = (f(C_{11}), \ldots, f(C_{l_1 l_2})) = (f(\psi(A_1, B_1)), \ldots, f(\psi(A_n, B_m))) = (\theta_f((x,y)(A_1, B_1), \ldots, \theta_f(x,y)(A_n, B_m))$.

Como $\theta_f(x,y) = \sum x^I y^J \in B_d$, para cada $A \in \mathbb{P}^n$ y $B \in \mathbb{P}^m$ en la representación estándar:
$\theta_{f_A}(y) = \theta_f(A,y) \in (R_m)_d$, $\theta_{f_B}(x) = \theta_f(x,B) \in (R_n)_d$

Para cada $i \in [1, l_1]$, $\Lambda_i = (\theta_{f_{A_i}}(B_1), \ldots, \theta_{f_{A_i}}(B_{l_2})) \in C_{\mathbb{P}^m}$ si $l = |\{i : \Lambda_i \neq 0\}| > 0$.

Desde que $w(\Lambda_i) \geq \delta_{\mathbb{P}^m}(d)$ con $\Lambda_i \neq 0$, entonces $w(\Lambda) \geq l\delta_{\mathbb{P}^m}(d)$.

De manera similar sea $\Gamma_j = (\theta_{f_{B_j}}(A_1), \ldots, \theta_{f_{B_j}}(A_{l_1})) \in C_{\mathbb{P}^n}$, para cada $j = 1, \ldots, l_2$.
Sea $\Gamma_j \neq 0$, si $l < \delta_{\mathbb{P}^n}(d)$ entonces $w(\Gamma_j) \leq l < \delta_{\mathbb{P}^n}(d)$ lo cual no puede ser.

Como $\delta_{\mathbb{P}^n}(d) < l$ entonces $\delta_{\mathbb{P}^n}(d)\delta_{\mathbb{P}^m}(d) \leq w(\Lambda)$, $\forall \Lambda \neq 0 \in C_X(d)$, es decir, $\delta_{\mathbb{P}^n}(d)\delta_{\mathbb{P}^m}(d) \leq \delta_X(d)$.

Sea $\Omega_1 = (g(A_1)), \ldots, g(A_{l_1}) \in C_{\mathbb{P}^n}(d)$ con $w(\Omega_1) = \delta_{\mathbb{P}^n}(d)$ y $g(x) \in (R_n)_d$ y $\Omega_2 = (h(B_1)), \ldots, h(B_{l_2}) \in C_{\mathbb{P}^m}(d)$ con $w(\Omega_2) = \delta_{\mathbb{P}^m}(d)$ y $h(y) \in (R_m)_d$. Ya que θ es una transformación lineal suprayectiva, existe $F \in (R_N)_d$ tal que

$$(gh(A_1, B_1), \ldots, gh(A_{l_1}), B_{l_2}) = (F(\psi(A_1, B_1)), \ldots, F(\psi(A_{l_1}, B_{l_2}))) := \Omega \in C_X(d)$$

y $w(\Omega) = \delta_{\mathbb{P}^n}(d)\delta_{\mathbb{P}^m}(d)$.
Probando que $\delta_X = \delta_{\mathbb{P}^n}(d)\delta_{\mathbb{P}^m}(d)$

■

Ejemplo 3.3.5 Sea $K = \mathbb{F}_4 = \{0, 1, a, a^2\}$, $\psi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ la inmersión de Segre. En este caso, los elementos de la variedad de Segre son:

$$X = \left\{ \begin{array}{c} (0,0,0,1), (0,0,1,0), (0,1,0,0), (1,0,0,0), (0,0,1,a), \\ (0,0,1,a^2), (0,0,1,1), (0,1,0,a), (1,a,a,a^2), (1,0,a,0), \\ (1,a^2,a,1), (1,1,a,a), (1,a,0,0), (1,a^2,0,0), (1,1,0,0), \\ (0,1,0,a^2), (1,a,a^2,1), (1,0,a^2,0), (1,a^2,a^2,a), (1,1,a^2,a^2), \\ (0,1,0,1), (1,a,1,a), (1,0,1,0), (1,a^2,1,a^2), (1,1,1,1) \end{array} \right\}$$

Del teorema (3.3.4) $\mathrm{reg}(\mathrm{R}_3/\mathrm{I}_X) = \mathrm{reg}(\mathrm{R}_1/\mathrm{I}_{\mathbb{P}^1}) = 4$, I_X esta generado por:

$$\left\{ \begin{array}{c} z_{10}z_{01} - z_{00}z_{11}, z_{01}^4 z_{11} - z_{01}z_{11}^4, z_{00}z_{01}^3 z_{11} - z_{00}z_{11}^4, z_{00}^2 z_{01}^2 z_{11} - \\ - z_{00}z_{10}z_{11}^3, z_{00}^3 z_{01}z_{11} - z_{00}z_{10}^2 z_{11}^2, z_{10}^4 z_{11} - z_{10}z_{11}^4, z_{00}z_{10}^3 z_{11} - \\ - z_{00}z_{11}^4, z_{00}^2 z_{10}^2 z_{11} - z_{00}z_{01}z_{11}^3, z_{00}^3 z_{10}z_{11} - z_{00}z_{01}^2 z_{11}^2, z_{00}^4 z_{11} - \\ - z_{00}z_{11}^4, z_{00}^4 z_{01} - z_{00}z_{01}^4, z_{00}^4 z_{10} - z_{00}z_{10}^4 \end{array} \right\}$$

y los parámetros básicos de $\{C_X(d)\}_{d \leq 4}$ son

d	1	2	3	4
$\lvert X\rvert = \lvert\mathbb{P}^1\rvert^2$	25	25	25	25
$H_X(d) = H_{\mathbb{P}^1}(d)^2$	4	9	16	25
$\delta_{\mathbb{X}}(d) = \delta_{\mathbb{P}^1}(d)^2$	16	9	4	1

3.4. Código asociado a una gráfica bipartita completa

Definición 3.4.1 Una gráfica G consiste en un conjunto no vacío V de p puntos junto con un conjunto prescrito E de q-parejas de distintos puntos de V. Cada par $x = \{u, v\}$ de puntos en E es una línea de G, y se dice que x une a u con v.

Al conjunto E se le conoce como el conjunto de aristas de la gráfica G y a V su conjunto de vértices y algunas veces se refiere a una gráfica como $G(V, E)$.

Escribiremos $x = uv$ y diremos que u y v son puntos adyacentes (algunas veces denotado por u *adj* v). También si v se encuentra en la línea x, decimos que v y x son incidentes.

Definición 3.4.2 Una gráfica G es **etiquetada** cuando los p puntos se distinguen uno del otro por nombres, tales como $v_1, \ldots, v_p$ y sus q-aristas también se distinguen: $x_1, \ldots, x_q$.

Definición 3.4.3 Sea G una gráfica etiquetada, con p puntos y q aristas. Entonces se define la **matriz de incidencia** $B = [b_{ij}]$ de tamaño $p \times q$ como la matriz cuyas entradas $b_{ij} = 1$ si v_i y x_j son incidentes y $b_{ij} = 0$ en otro caso.

Definición 3.4.4 Sea $r \geq 2$ un entero. Una gráfica $G = (V, E)$ es r-partita si existe una partición de V en r conjuntos independientes que llamamos clases, tales que para cualquier par de vértices en alguna clase se tiene que no son adyacentes. Para r=2 en vez de decir 2-partita, decimos bipartita.

Una gráfica r-partita donde cada par de vértices de distintas clases es adyacente se llama una gráfica r-partita completa, para $r = 2$ será gráfica bipartita completa.

Definición 3.4.5 Sea K un campo y $K_{n,m}$ una gráfica bipartita completa, definimos la variedad algebraica parametrizada por la matriz de incidencia de la gráfica $K_{n,m}$ como:

$$X = \{[t_1t_{n+1}, t_1t_{n+2}, \ldots, t_1t_{n+m}, t_2t_{n+1}, t_2t_{n+2}, \ldots, t_2t_{n+m}, \ldots t_nt_{n+1}, t_nt_{n+2}, \ldots, t_nt_{n+m}] \\ : t_i \in K^* \text{ for all } i = 1, \ldots, m+n\} \subseteq \mathbb{P}^{mn-1}$$

Y de hecho se puede escribir como

$$X = \{[1, \alpha_1, \alpha_2, \ldots, \alpha_{m-1}, \beta_1, \beta_1\alpha_1, \beta_1\alpha_2, \ldots, \beta_1\alpha_{m-1}, \beta_2, \beta_2\alpha_1, \beta_2\alpha_2, \ldots, \beta_2\alpha_{m-1}, \ldots, \\ \beta_{n-1}, \beta_{n-1}\alpha_1, \beta_{n-1}\alpha_2, \ldots, \beta_{n-1}\alpha_{m-1}] : \beta_1, \ldots, \beta_{n-1}\alpha_1, \ldots, \alpha_{m-1} \in K^*\}$$

Observación 3.4.6 *Sean*

$$X_1 = \{[1, \beta_1, \ldots, \beta_{n-1}] : \beta_1, \ldots, \beta_{n-1} \in K^*\} \tag{3.28}$$

$$X_2 = \{[1, \alpha_1, \ldots, \alpha_{m-1}] : \alpha_1, \ldots, \alpha_{m-1} \in K^*\} \tag{3.29}$$

y X como en la definición anterior. Si ψ es la inmersión de Segre restringida al conjunto $X_1 \times X_2 \subset \mathbb{P}^{n-1} \times \mathbb{P}^{m-1} \to \mathbb{P}^{mn-1}$. Entonces $\psi(X_1 \times X_2) = X$.

Teorema 3.4.7 *Sea $\mathbb{P}^{mn-1}$ el espacio proyectivo sobre un campo K con q elementos y $X \subseteq \mathbb{P}^{mn-1}$, $X_1 \subset \mathbb{P}^{n-1}$ y $X_2 \subset \mathbb{P}^{m-1}$ como en la observación anterior. El código Reed-Muller generalizado de orden d asociado a X: $C_X(d)$ satisface lo siguiente*

1 *La longitud del código $C_X(d)$ es $(q-1)^{n-1}(q-1)^{m-1}$*

2 *Para cada $d \geq 0$, la dimensión de $C_X(d)$ es*

$$H_X(d) = H_{X_1}(d)H_{X_2}(d) \tag{3.30}$$

Más aún la fórmula general de la función de Hilbert asociada a X_1 y X_2 esta dada por:

$$H_{X_1}(d) = \binom{n-1+d}{d} + \sum_{j=0}^{n-1}(-1)^j \binom{n-1}{i}\binom{n-1+d-i(q-1)}{d-i(q-1)} \tag{3.31}$$

y

$$H_{X_2}(d) = \binom{m-1+d}{d} + \sum_{j=0}^{m-1}(-1)^j \binom{m-1}{i}\binom{m-1+d-i(q-1)}{d-i(q-1)} \tag{3.32}$$

respectivamente.

3 *El índice de regularidad asociado a la famila $\{C_X(d)\}_{d\in\mathbb{N}_0}$ es*

$$\mathrm{reg}(\mathrm{R}_{(\mathrm{m}-1)(\mathrm{n}-1)}/\mathrm{I}_{\mathrm{X}}) = \max\{\mathrm{reg}(\mathrm{R}_{(\mathrm{n}-1)}/\mathrm{I}_{\mathrm{X}_1}), \mathrm{reg}(\mathrm{R}_{(\mathrm{m}-1)}/\mathrm{I}_{\mathrm{X}_2})\} \tag{3.33}$$

donde

$$\mathrm{reg}(\mathrm{R}_{(\mathrm{n}-1)}/\mathrm{I}_{\mathrm{X}_1}) = (\mathrm{n}-1)(\mathrm{q}-1) - \mathrm{n} + 1 \tag{3.34}$$

y

$$\mathrm{reg}(\mathrm{R}_{(\mathrm{m}-1)}/\mathrm{I}_{\mathrm{X}_2}) = (\mathrm{m}-1)(\mathrm{q}-1) - \mathrm{m} + 1 \tag{3.35}$$

4 *La distancia mínima es $\delta_X = \delta_{X_1}(d)\delta_{X_2}(d)$*

***Demostración*.**

El inciso 1 se sigue de que la inmersión de Segre en inyectiva y que $|X_1| = (q-1)^{n-1}$ y $|X_2| = (q-1)^{m-1}$.

Probemos 2. Sean $C_{X_1}(d)$ y $C_{X_2}(d)$ los códigos Reed Muller de orden d asociados a X_1 y X_2 respectivamente, como ya sabemos $C_{X_1}(d) \simeq (K[x_0, \ldots, x_{n-1}])_d/(I_{X_1})_d$ y $C_{X_2}(d) \simeq (K[y_0, \ldots, y_{m-1}])_d/(I_{X_2})_d$. La fórmula se sigue del isomorfismo

$$K[z_{00}, \ldots, z_{(m-1)(n-1)}]_d/(I_X)_d \simeq K[x_0, \ldots, x_{n-1}]_d/(I_{X_1})_d \otimes_K K[y_0, \ldots, y_{m-1}]_d/(I_{X_2})_d \tag{3.36}$$

El cual se probará en el siguiente capítulo (vea el Teorema 4.1.6). La demostración de las fórmulas 3.31 y 3.32 se encuentran en [24].

El inciso 3 es una consecuencia del isomorfismo en 3.36 y la prueba de las fórmulas 3.34 y 3.35 se encuentran en [24].

El inciso 4 se sigue de que $X = \psi(X1 \times X2)$ junto con el teorema 3.3.4 inciso 4.

■

Ejemplo 3.4.8 Sea $K_{2,3}$ la gráfica bipartita completa.

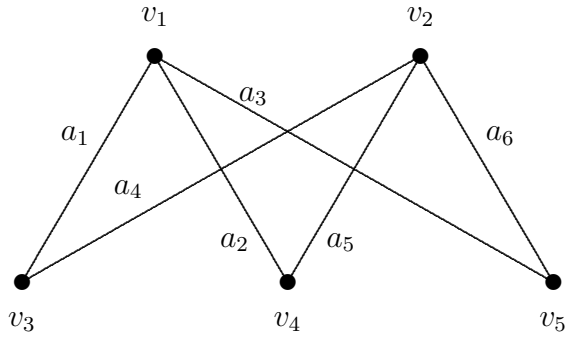

Figura 3.1: $K_{2,3}$

La matriz de incidencia asociada a $K_{2,3}$ está dada por.

$$B = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Si $K = \mathbb{F}_5$ la longitud del código $C_X(d)$ es $|X| = (5-1)^{2+3-2} = 64$, como la regularidad de X_1 y X_2 para este ejemplo es 3 y 6 respectivamente del teorema anterior $\mathrm{reg}(\mathrm{R_2/I_X}) = 5$. La siguiente tabla muestra los parámetros básicos de la familia $\{C_X(d)\}_{d \leq 5}$

d	1	2	3	4	5	6
$\lvert X\rvert$	64	64	64	64	64	64
$H_X(d)$	6	18	40	52	60	64
$\delta_{\mathbb{X}}(d) = \delta_{\mathbb{P}^1}(d)^2$	?	?	4	3	2	1

Capítulo 4

Algunas Generalizaciones de los Códigos de Segre

Dado $X_i \subset \mathbb{P}^{n_i}$, $i = 1, 2$ la imagen de $X_1 \times X_2$ bajo la inmersión de Segre ψ (vea ec. 3.18) denotada por X, se le llama *Producto de Segre* de X_1 y X_2. La inmersión de Segre es usada en geometría algebraica entre varias aplicaciones para mostrar que el producto de variedades es también una variedad proyectiva, vea [19, Lecture 2]. En Teoría de Códigos es usada para estudiar los pesos generalizados de Hamming de algunos productos de códigos (definición 1.1.9 y [33]) y lo que veremos en esta sección.

Los productos de Segre han sido estudiados por muchos autores; vea [10, 25, 21]. Nosotros daremos pruebas de dos resultados para los cuales no encontramos referencias (vea el Lemma 4.1.3 y el Teorema 4.1.6). Todos los demás resultados de esta sección se encuentran en la bibliografía.

Cuando K es un campo finito, un elemento de la familia de códigos Reed-Muller generalizados $\{C_X(d)\}_{d\in\mathbb{N}}$ lo llamaremos Código proyectivo de Segre. Nosotros estudiaremos los parámetros básicos y el segundo peso generalizado de Hamming de dichos códigos. El resultado principal expresa los parámetros básicos de $C_X(d)$ en términos de los parámetros de $C_{X_1}(d)$ y $C_{X_2}(d)$, además mostramos que $C_X(d)$ es el producto directo de $C_{X_1}(d)$ y $C_{X_2}(d)$ (vea el Teorema 4.2.1); esto quiere decir que el producto directo de dos códigos Reed-Muller proyectivos de grado d es de nuevo un código Reed-Muller proyectivo de grado d.

Fórmulas para los parámetros básicos de códigos Reed-Muller afines y proyectivos son conocidas para varias familias [4, 32, 8, 20, 13, 22, 14, 26, 25, 17, 9, 34]. Ya que los códigos Reed- Muller afines pueden considerarse como códigos Reed- Muller proyectivos [18], nuestros resultados pueden ser aplicados para obtener fórmulas explícitas de los parámeteros básicos de $C_X(d)$ si $C_{X_1}(d)$ está en una de esas familias y $C_{X_2}(d)$ está en otra de éstas familias o ambos están en la misma familia.

Como una aplicación recobramos algunos resultados de códigos Reed-Muller sobre la variedad de Segre y sobre el toro proyectivo [14, 15, 24, 25]. En efecto, si $X_1 = \mathbb{P}^{n_1}$ y $X_2 = \mathbb{P}^{n_2}$, usando el Teorema 4.2.1 recobramos la fórmula de la distancia mínima de $C_X(d)$ dada en la sección 3.3. Si $K^* = K \setminus \{0\}$ y X_i es la imagen de $(K^*)^{n_i}$, bajo la función $(K^*)^{n_i} \to \mathbb{P}^{n_i-1}$, $x \to [x]$, llamamos a X_i a *toro proyectivo* en $\mathbb{P}^{n_i-1}$. Si X_i es un toro proyectivo para $i = 1, 2$, usando el Teorema 4.2.1 recobramos la fórmula de la distancia mínima de $C_X(d)$. En ambos casos las fórmulas de los parámetros básicos de $C_{X_i}(d)$, $i = 1, 2$, están dadas en [34, Theorem 1] y [9, Theorem 3.5], respectivamente. También recobramos fórmulas para el segundo peso generalizado de Hamming dadas en [15, Theorem 5.1] y [24, Theorem 3] (vea el Corolario 4.2.5).

4.1. Producto directo de códigos

Sea $C_1 \subset K^{s_1}$ y $C_2 \subset K^{s_2}$ dos códigos lineales sobre un campo finito K y sea $M_{s_1 \times s_2}(K)$ el K-espacio vectorial de todas las matrices de tamaño $s_1 \times s_2$ con entradas en K.

El *producto directo* (también llamado *producto Kronecker*) de C_1 y C_2 denotado por $C_1 \underline{\otimes} C_2$, está definido como el código lineal que consiste de todas las matrices de tamaño $s_1 \times s_2$ en las cuáles las filas pertenecen a C_2 y las columnas a C_1; vea [27, p. 44]. El producto directo de códigos usualmente tiene distancia mínima pequeña pero son fáciles de decodificar y pueden ser útiles en ciertas aplicaciones; vea [28, Chapter 18].

Denotamos el producto tensorial (en el sentido multilineal) de C_1 y C_2 [10, p. 573] por $C_1 \otimes_K C_2$. Como se probará en el Lemma 4.1.3, otra manera de ver el producto directo de C_1 y C_2 es como el producto tensorial.

Teorema 4.1.1 *[35, Theorems 2.5.2 and 2.5.3] Sea $C_i \subset K^{s_i}$ un código lineal de longitud s_i, dimensión l_i, y distancia mínima $\delta(C_i)$ para $i = 1, 2$. Entonces $C_1 \underline{\otimes} C_2$ tiene longitud $s_1 s_2$, dimensión $l_1 l_2$, y distancia mínima $\delta(C_1)\delta(C_2)$.*

Teorema 4.1.2 *[37, Theorem 3(d)] Sea $C_1 \subset K^{s_1}$ y $C_2 \subset K^{s_2}$ dos códigos lineales y sea $C = C_1 \underline{\otimes} C_2$ su producto directo. Entonces*

$$\delta_2(C) = \min\{\delta_1(C_1)\delta_2(C_2), \delta_2(C_1)\delta_1(C_2)\}.$$

Recordemos que para cualquier campo K hay un isomorfismo vec: $M_{s_1 \times s_2}(K) \to K^{s_1 s_2}$ de K-espacios vectoriales dado por $\text{vec}(A) = (F_1, \ldots, F_{s_1})$, donde $F_1, \ldots, F_{s_1}$ son las filas

de A. Considere la función bilineal ψ_0 dada por

$$\begin{array}{rcl} \psi_0 \colon K^{s_1} \times K^{s_2} & \longrightarrow & M_{s_1 \times s_2}(K) \\ ((a_1, \ldots, a_{s_1}), (b_1, \ldots, b_{s_2})) & \longmapsto & \begin{bmatrix} a_1b_1 & a_1b_2 & \ldots & a_1b_{s_2} \\ a_2b_1 & a_2b_2 & \ldots & a_2b_{s_2} \\ \vdots & \vdots & & \vdots \\ a_{s_1}b_1 & a_{s_1}b_2 & \ldots & a_{s_1}b_{s_2} \end{bmatrix}. \end{array}$$

La inmersión de Segre esta dada por

$$\psi([a], [b]) = [(\mathrm{vec} \circ \psi_0)(a, b)]$$

donde $a = (a_1, \ldots, a_{s_1})$ y $b = (b_1, \ldots, b_{s_2})$.

El siguiente lema no es difícil de probar y seguramente se conoce una equivalencia de su formulación; pero no pudimos encontrar una referencia con la correspondiente prueba.

Lema 4.1.3 *Hay un isomorfismo $T \colon C_1 \otimes_K C_2 \to C_1 \underline{\otimes} C_2$ de K-espacios vectoriales tal que $T(a \otimes b) = \psi_0(a, b)$ para $a \in C_1$ y $b \in C_2$.*

Demostración. Fijamos $l_i = \dim_K(C_i)$ para $i = 1, 2$. Usando la propiedad universal del producto tensorial [10, p. 573], ψ_0 induce una función lineal

$$\begin{array}{rcl} T \colon C_1 \otimes_K C_2 & \longrightarrow & C_1 \underline{\otimes} C_2, \text{ tal que,} \\ a \otimes b & \longmapsto & \psi_0(a, b) \end{array}$$

para $a \in C_1$ y $b \in C_2$. Por [29, Fórmula 5, p. 267] y el Teorema 4.1.1 se tiene que $C_1 \otimes_K C_2$ y $C_1 \underline{\otimes} C_2$ tienen dimensión $l_1 l_2$ por lo que es suficiente probar que T es inyectiva. Sean $\{\alpha_1, \ldots, \alpha_{l_1}\}$ y $\{\beta_1, \ldots, \beta_{l_2}\}$ bases de C_1 y C_2, respectivamente y sea γ en el kernel de T. Entonces

$$\gamma = \sum \lambda_{i,j} \alpha_i \otimes \beta_j$$

con $\lambda_{i,j}$ en K $\forall i, j$. Entonces

$$\begin{array}{rcl} T(\gamma) & = & \lambda_{1,1} T(\alpha_1 \otimes \beta_1) + \cdots + \lambda_{1,l_2} T(\alpha_1 \otimes \beta_{l_2}) + \\ & & \lambda_{2,1} T(\alpha_2 \otimes \beta_1) + \cdots + \lambda_{2,l_2} T(\alpha_2 \otimes \beta_{l_2}) + \\ & & \vdots \\ & & \lambda_{l_1,1} T(\alpha_{l_1} \otimes \beta_1) + \cdots + \lambda_{l_1,l_2} T(\alpha_{l_1} \otimes \beta_{l_2}). \end{array}$$

Si $\alpha_i = (\alpha_{i,1}, \ldots, \alpha_{i,s_1})$, $\beta_j = (\beta_{j,1}, \ldots, \beta_{j,s_2})$ para $i = 1, \ldots, l_1$, $j = 1, \ldots, l_2$, tenemos

$$T(\gamma) = \begin{bmatrix} (\lambda_{1,1}\alpha_{1,1}\beta_1 + \cdots + \lambda_{1,l_2}\alpha_{1,1}\beta_{l_2}) + \cdots + (\lambda_{l_1,1}\alpha_{l_1,1}\beta_1 + \cdots + \lambda_{l_1,l_2}\alpha_{l_1,1}\beta_{l_2}) \\ (\lambda_{1,1}\alpha_{1,2}\beta_1 + \cdots + \lambda_{1,l_2}\alpha_{1,2}\beta_{l_2}) + \cdots + (\lambda_{l_1,1}\alpha_{l_1,2}\beta_1 + \cdots + \lambda_{l_1,l_2}\alpha_{l_1,2}\beta_{l_2}) \\ \vdots \\ (\lambda_{1,1}\alpha_{1,s_1}\beta_1 + \cdots + \lambda_{1,l_2}\alpha_{1,s_1}\beta_{l_2}) + \cdots + (\lambda_{l_1,1}\alpha_{l_1,s_1}\beta_1 + \cdots + \lambda_{l_1,l_2}\alpha_{l_1,s_1}\beta_{l_2}) \end{bmatrix}.$$

Ya que $T(\gamma) = (0)$, usando que los β_i's son l.i tenemos

$$\lambda_{1,j}\alpha_1^\top + \cdots + \lambda_{l_1,j}\alpha_{l_1}^\top = 0 \text{ for } j = 1, \ldots, l_2.$$

Luego $\lambda_{i,j} = 0\ \forall i, j$ y $\gamma = 0$. ■

Definición 4.1.4 *[10, p. 304]* Sean $A = \oplus_{d\geq 0} A_d$, $B = \oplus_{d\geq 0} B_d$ dos álgebras estándar sobre un campo K. El *Producto de Segre* de A y B se define como el álgebra graduada:

$$A \otimes_{\mathcal{S}} B := (A_0 \otimes_K B_0) \oplus (A_1 \otimes_K B_1) \oplus \cdots \subset A \otimes_K B,$$

El álgebra del producto tensorial de A y B esta graduada por

$$(A \otimes_K B)_p := \sum_{i+j=p} A_i \otimes_K B_j.$$

Ejemplo 4.1.5 *[3, p. 161]* El producto de Segre (resp. producto tensorial) de R_{n_1} y R_{n_2} es

$$R_{n_1} \otimes_{\mathcal{S}} R_{n_2} \simeq K[\{x_i y_j |\, 0 \leq i \leq n_1,\, 0 \leq j \leq n_2\}]$$

(resp. $R_{n_1} \otimes_K R_{n_2} \simeq K[x_0, \ldots, x_{n_1}, x_0, \ldots, x_{n_2}]$). Notemos que los elementos $x_i y_j$ tienen grado normalizado 1 como elementos de $R_{n_1} \otimes_{\mathcal{S}} R_{n_2}$ y grado total 2 como elementos de $R_{n_1} \otimes_K R_{n_1}$.

El siguiente resultado es muy conocido si X_1 y X_2 son conjuntos algebraicos proyectivos; vea [10, Exercise 13.14(d)]. Sin embargo David Eisenbud señaló que el resultado es válido en general. Nosotros damos una prueba del caso general.

Teorema 4.1.6 *Sea K un campo. Si X_1, X_2 son subconjuntos de los espacios proyectivos $\mathbb{P}^{n_1}$, $\mathbb{P}^{n_2}$, respectivamente, y $X \subseteq \mathbb{P}^N$ ($N = n_1 + n_2 + n_1 n_2$) es el producto de Segre de X_1 y X_2, entonces lo siguiente se satisface:*

(a) $(R_{n_1}/I_{X_1})_d \otimes_K (R_{n_2}/I_{X_2})_d \simeq (R_N/I_X)_d$ *como K-espacios vectoriales para $d \geq 0$.*

(b) $(R_{n_1}/I_{X_1})_d \otimes_{\mathcal{S}} (R_{n_2}/I_{X_2})_d \simeq (R_N/I_X)_d$ *como ágebras estándar graduadas.*

(c) $H_{X_1}(d)H_{X_2}(d) = H_X(d)$ *para $d \geq 0$.*

(d) $\operatorname{reg}(R_N/I_X) = \operatorname{máx}\{\operatorname{reg}(R_{n_1}/I_{X_1}), \operatorname{reg}(R_{n_2}/I_{X_2})\}$.

(e) Si $\rho_1 = \dim(R_{n_1}/I_{X_1})$ *y* $\rho_2 = \dim(R_{n_2}/I_{X_2})$, *entonces*

$$\deg(R_N/I_X) = \deg(R_{n_1}/I_{X_1}) \deg(R_{n_2}/I_{X_2}) \binom{\rho_1 + \rho_2}{\rho_1}.$$

Demostración.

(a) Sea $x^\alpha \in (R_{n_1})_d$ y $y^\beta \in (R_{n_2})_d$ entonces existen $l_{ij} \in \mathbb{N}_0$ tales que $x^\alpha y^\beta = (x_0y_0)^{l_{00}} \cdots (x_{n_1}y_{n_2})^{l_{n_1n_2}}$. Definimos la función $K-$bilineal

$$\sigma : (R_{n_1})_d \times (R_{n_2})_d \to (R_N)_d$$
$$(x^\alpha, y^\beta) \mapsto (z_{00})^{l_{00}} \cdots (z_{n_1n_2})^{l_{n_1n_2}}$$

note que para cada monomio $z^\gamma = (z_{00})^{\gamma_{00}} \cdots (z_{n_1n_2})^{\gamma_{n_1n_2}} \in (R_N)_d$ los monomios $x^{\gamma_1} = x_0^{\gamma_{00}+\cdots+\gamma_{0n_2}} \cdots x_{n_1}^{\gamma_{n_10}+\cdots+\gamma_{n_1n_2}} \in (R_{n_1})_d$ y $y^{\gamma_2} = y_0^{\gamma_{00}+\cdots+\gamma_{n_10}} \cdots y_{n_2}^{\gamma_{0n_2}+\cdots+\gamma_{n_1n_2}} \in (R_{n_2})_d$ son tales que $\sigma(x^{\gamma_1}, y^{\gamma_2}) = z^\gamma$. entonces σ induce una función $K-$bilineal

$$\overline{\sigma} : (R_{n_1}/I_{X_1})_d \times (R_{n_2}/I_{X_2})_d \to (R_N/I_X)_d$$

Si $f \in (I_{X_1})_d$, $g \in (I_{X_2})_d$ y $c \in X$ entonces hay $a \in X_1$ y $b \in X_2$ tales que $\sigma(f,g)(c) = \sigma(f,g)(\psi(a,b)) = f(a)g(b) = 0$ luego $\overline{\sigma}$ esta bien definida.

Para mostrar (a) vamos a probar que $((R_N)_d, \overline{\sigma})$ satisface la propiedad universal del producto tensorial $(R_{n_1}/I_{X_1})_d \otimes_K (R_{n_2}/I_{X_2})_d$.

Sea $\phi : (R_{n_1}/I_{X_1})_d \times (R_{n_2}/I_{X_2})_d \to M$ una función $K-$bilineal con M un K-espacio vectorial, entonces el $K-$morfismo

$$\overline{\phi} : (R_N)_d/(I_X)_d \to M$$
$$\overline{z^\gamma} \mapsto \phi(\overline{x^{\gamma_1}}, \overline{y^{\gamma_2}})$$

Está bien definido y hace conmutar el siguiente diagrama

$$\begin{array}{ccc} (R_{n_1}/I_{X_1})_d \times (R_{n_2}/I_{X_2})_d & \xrightarrow{\overline{\sigma}} & (R_N)_d/(I_X)_d \\ & \searrow^{\phi} & \downarrow \overline{\phi} \\ & & M \end{array}$$

Obviamente $\overline{\phi}$ es única para ϕ. Para probar que $\overline{\phi}$ está bien definida, sea $h \in (I_X)_d$ y $(f,g) \in (R_{n_1})_d \times (R_{n_2})_d$ tales que $\sigma(f,g) = h$. Si $\exists a \in X_1$ tal que $f(a) \neq 0$ entonces el polinomio $f(a)g(y) = \sigma(f,g)(\psi(a,y)) = h(\psi(a,y)) \in (R_{n_2})_d$ es tal que $f(a)g(b) = \sigma(f,g)(\psi(a,b)) = h(\psi(a,b)) = 0$ para todo $b \in X_2$ luego $g \in (I_{X_2})_d$, análogamente $f \in (I_{X_1})_d$ si $\exists b \in X_2$ tal que $g(b) \neq 0$, así que $(\overline{f}, \overline{g}) = (0, \overline{g})$ o $(\overline{f}, \overline{g}) = (\overline{g}, 0)$ luego $\overline{\psi}(\overline{h}) = \overline{\psi}(0) = \psi(\overline{f}, \overline{g}) = 0$. Si $h_1, h_2 \in R_N$ satisfacen que $h_1 - h_2 \in I_X$ entonces $\overline{\psi}(\overline{h_1 - h_2}) = \overline{\psi}(0) = 0$ por lo que $\overline{\psi}(\overline{h_1}) = \overline{\psi}(h_2)$.

Los ítems (b) a (e) se siguen directamente de (a) y su prueba.

■

4.2. Parámetros básicos de los códigos proyectivos de Segre

En esta sección estudiaremos los códigos proyectivos de Segre y sus parámetros básicos; incluyendo el segundo peso generalizado de Hamming. Se demuestra que el producto directo de códigos Reed-Muller generalizados son códigos proyectivos de Segre. Después daremos algunas aplicaciones.

Teorema 4.2.1 *Sea K un campo finito, sea $X_i \subset \mathbb{P}^{n_i}$ para $i = 1, 2$, y sea X el producto de Segre de X_1 y X_2. Lo siguiente se cumple.*

(a) $|X| = |X_1||X_2|$.

(b) $\dim_K(C_X(d)) = \dim_K(C_{X_1}(d)) \dim_K(C_{X_2}(d))$ *para* $d \geq 1$.

(c) $C_X(d)$ *es el producto directo* $C_{X_1}(d) \otimes C_{X_2}(d)$ *de* $C_{X_1}(d)$ *y* $C_{X_2}(d)$ *para* $d \geq 1$.

(d) $\delta(C_X(d)) = \delta(C_{X_1}(d))\delta(C_{X_2}(d))$ *para* $d \geq 1$.

(e) $\delta_2(C_X(d)) = \min\{\delta_1(C_{X_1}(d))\delta_2(C_{X_2}(d)), \delta_2(C_{X_1}(d))\delta_1(C_{X_2}(d))\}$ *para* $d \geq 1$.

(f) $\delta(C_X(d)) = 1$ *para* $d \geq \max\{\mathrm{reg}(R_{n_1}/I_{X_1}), \mathrm{reg}(R_{n_2}/I_{X_2})\}$.

Demostración.

(a): Es claro por que la inmersión de Segre es inyectiva (vea la proposición 3.3.2).

(b): Ya que $(R_{n_1})_d/(I_{X_1})_d \simeq C_{X_1}(d)$, $(R_{n_2})_d/(I_{X_2})_d \simeq C_{X_2}(d)$, y $(R_N)_d/(I_X)_d \simeq C_X(d)$, los resultados se siguen de Theorem 4.1.6.

(c): Dado $f \in (R_N)_d$, las entradas de $\mathrm{ev}_d(f)$ pueden reescribirse como:

$$\begin{array}{rcccccc} \mathrm{ev}_d(f) & = & (f(P_{1,1}), & f(P_{1,2}), \ldots, & f(P_{1,n_2}), & \to \Gamma_1 \\ & & f(P_{2,1}), & f(P_{2,2}), \ldots, & f(P_{2,n_2}), & \to \Gamma_2 \\ & & \vdots & \vdots & \vdots & \vdots \\ & & f(P_{n_1,1}), & f(P_{n_1,2}), \ldots, & f(P_{n_1,n_2})) & \to \Gamma_{n_1} \\ & & \downarrow & \downarrow & \downarrow & \\ & & \Lambda_1 & \Lambda_2 \quad \cdots & \Lambda_{n_2} & \end{array} \tag{4.1}$$

donde $\Gamma_1, \ldots, \Gamma_{n_1}$ y $\Lambda_1, \ldots, \Lambda_{n_2}$ son vectores fila y vectores columna, respectivamente. Así $\mathrm{ev}_d(f)$ puede verse como la matriz de tamaño $n_1 \times n_2$. Ahora mostraremos que

$\Gamma_i \in C_{X_2}(d)$ y $\Lambda_j^\top \in C_{X_1}(d)$ $\forall i, j$. Definimos los siguientes polinomios $h_{Q_i} \in (R_{n_2})_d$ y $g_{R_j} \in (R_{n_1})_d$ como

$$\begin{aligned} h_{Q_i} &= f(\alpha_{i,1} \cdot y_1, \alpha_{i,1} \cdot y_2, \ldots, \alpha_{i,1} \cdot y_{n_2}, \\ &\quad \alpha_{i,2} \cdot y_1, \alpha_{i,2} \cdot y_2, \ldots, \alpha_{i,2} \cdot y_{n_2}, \\ &\quad \vdots \\ &\quad \alpha_{i,n_1} \cdot y_1, \alpha_{i,n_1} \cdot y_2, \ldots, \alpha_{i,n_1} \cdot y_{n_2}), \end{aligned}$$

$$\begin{aligned} g_{R_j} &= f(x_1 \cdot \beta_{j,1}, x_1 \cdot \beta_{j,2}, \ldots, x_1 \cdot \beta_{j,n_2}, \\ &\quad x_2 \cdot \beta_{j,1}, x_2 \cdot \beta_{j,2}, \ldots, x_2 \cdot \beta_{j,n_2}, \\ &\quad \vdots \\ &\quad x_{n_1} \cdot \beta_{j,1}, x_{n_1} \cdot \beta_{j,2}, \ldots, x_{n_1} \cdot \beta_{j,n_2}). \end{aligned}$$

Observe que $f(P_{ij}) = h_{Q_i}(R_j) = g_{R_j}(Q_i)$. Notando las igualdades

$$\begin{aligned} \Gamma_i &= (f(P_{i1}), f(P_{i2}), \ldots, f(P_{is_2})) = \\ &\quad (h_{Q_i}(R_1), h_{Q_i}(R_2), \ldots, h_{Q_i}(R_{s_2})) = \mathrm{ev}_d^2(h_{Q_i}), \\ \Lambda_j^\top &= \frac{1}{(\beta_{j,\ell_j})^d} \cdot \mathrm{ev}_d^1(g_{R_j}), \end{aligned}$$

para $i = 1, \ldots, s_1$ y $j = 1, \ldots, s_2$, tenemos que $\Gamma_i \in C_{X_2}(d)$ y $\Lambda_j^\top \in C_{X_1}(d)$ para todo i, j. Esto prueba que $C_X(d)$ puede verse como un subespacio lineal de $C_{X_1}(d) \underline{\otimes} C_{X_2}(d)$. Por la parte (b) y el Teorema 4.1.1 loa códigos lineales $C_X(d)$ y $C_{X_1}(d) \underline{\otimes} C_{X_2}(d)$ tienen la misma dimensión. Por lo tanto estos espacios son iguales.

(d): Del Teorema 4.1.1 y la parte (c), se tiene $\delta(C_X(d)) = \delta(C_{X_1}(d))\delta(C_{X_2}(d))$ para $d \geq 1$.

(e): Se sigue una vez más por el Teorema 4.1.2 y la parte (c).

(f): Se sigue del Teorema 4.1.6(d).

■

Observación 4.2.2 *Este resultado nos dice que el producto directo de códigos Reed-Muller proyectivos es de nuevo un código Reed-Muller proyectivo.*

Definición 4.2.3 Si $K^* = K \setminus \{0\}$ y X_i es la imagen de $(K^*)^{n_i+1}$ bajo la función $(K^*)^{n_i+1} \to \mathbb{P}^{n_i}$, $x \to [x]$, llamamos a X_i un *toro proyectivo* en $\mathbb{P}^{n_i}$.

Nuestro teorema principal da una amplia generalización de la mayoría de los resultados en [14, 15, 24, 25].

Observación 4.2.4 *Si $X_1 = \mathbb{P}^{n_1}$ y $X_2 = \mathbb{P}^{n_2}$, usando el Teorema 4.2.1 recobramos la fórmula de la distancia mínima de $C_X(d)$ dada en [25, Theorem 5.1], y si X_i es un toro proyectivo para $i = 1, 2$, usando el Teorema 4.2.1 recobramos la fórmula de la distancia mínima de $C_X(d)$ dada en [14, Theorem 5.5]. En ambos casos las fórmulas de los parámetros básicos de $C_{X_i}(d)$, $i = 1, 2$, están dados en [34, Theorem 1] y [9, Theorem 3.5], respectivamente. También recobramos las fórmulas para el segundo peso generalizado de Hamming de algunos códigos Reed-Muller proyectivos que surgen de gráficas bipartitas completas dadas en [15, Theorem 5.1] y [24, Theorem 3] (vea Corolario 4.2.5).*

Resulta que la fórmula dada en el Teorema 4.2.1(e) es una generalización de gran alcance del siguiente resultado.

Corolario 4.2.5 *[15, Theorem 5.1] Sea X el producto de Segre de dos toros proyectivos X_1 y X_2. Entonces el segundo peso generalizado de Hamming de $C_X(d)$ esta dado por*

$$\delta_2(C_X(d)) = \min\{\delta_1(C_{X_1}(d))\delta_2(C_{X_2}(d)), \delta_2(C_{X_1}(d))\delta_1(C_{X_2}(d))\}.$$

Definición 4.2.6 Si X es parametrizado por monomios $t^{v_1}, \ldots, t^{v_s}$, decimos que $C_X(d)$ es un *código proyectivo parametrizado* de grado d.

Corolario 4.2.7 *Si $C_{X_i}(d)$ es un código proyectivo parametrizado de orden d para $i = 1, 2$, entonces también lo es su correspondiente código proyectivo de Segre $C_X(d)$.*

Demostración. Es suficiente ver que si X_1 y X_2 son parametrizados por $t^{v_1}, \ldots t^{v_s}$ y $w^{u_1}, \ldots w^{u_r}$, respectivamente, entonces X es parametrizado por $t^{v_i}w^{u_j}$, $i = 1, \ldots, s$, $j = 1, \ldots, r$. ■

Capítulo 5

Distancia Mínima

Sea $R = K[x_0, \ldots, x_n]$ el anillo de polinomios sobre un campo K con la graduación estándar e $I \neq 0$ un ideal homogéneo con dimensión de Krull k.

Definición 5.0.8 El grado o multiplicidad de R/I es el entero positivo

$$deg(R/I) := \begin{cases} (k-1)! \lim_{d\to\infty} H_I(d)/d^{k-1} & \text{si } k \geq 0 \\ dim_K R/I & \text{si } k = 0 \end{cases}$$

Sea $\mathcal{F}_d$ el conjunto de todos los divisores de R/I que no pertenecen a I de grado $d \geq 0$:

$$\mathcal{F}_d := \{f \in R_d : f \notin I,\ (I : f) \neq I\}, \tag{5.1}$$

donde $(I : f) = \{h \in R : hf \in I\}$. Notemos que $\mathcal{F}_0 = \emptyset$.

El objetivo principal de este capítulo es estudiar la función $\delta_I : \mathbb{N} \to \mathbb{Z}$ la cual llamamos función distancia mínima de I. Si I es un ideal primo, entonces $\mathcal{F}_d = \emptyset\ \forall d \geq 0$ y $\delta_I(d) = deg(R/I)$. Demostraremos que δ_I generaliza la función distancia mínima de códigos Reed-Muller sobre campos finitos. Ésta formulación algebraica da una nueva herramienta para estudiarlos.

Definición 5.0.9 Sea R un anillo y M un $R-$módulo y sea $r \in R - \{0\}$, si existe $x \in M - \{0\}$ tal que $rx = 0$ entonces decimos que r es un divisor de cero de M, si $\forall x \in M - \{0\}$ se tiene que $rx \neq 0$ entonces decimos que r es un elemento regular de M.

Definición 5.0.10 Sea R un anillo y M un $R-$módulo. Sea $x \in M$, definimos el ideal anulador de x como:

$$ann(x) := \{r \in R : rx = 0\}$$

Definición 5.0.11 Sea R un anillo e I un ideal de R. Para cada $f \in R$ definimos el ideal cociente de I respecto a f como $(I : f) = \{h \in R : hf \in I\}$. Notemos que f es un divisor de cero de S/I si y solo si $(I : f) \neq I$.

Definición 5.0.12 Sea R un anillo conmutativo con identidad y M un R-módulo, definimos el conjunto de primos asociados de M como:

$$Assoc(M) := \{P \in Spec(R) : P = ann(x) \text{ para algún } x \in M \ \}$$

Proposición 5.0.13 *[11] Sea R un anillo conmutativo Noetheriano con identidad y M un R-módulo finitamente generado, si $\mathcal{C}$ es la familia de todos los ideales anuladores de elementos de M entonces los elementos de $Assoc(M)$ son elementos maximales de $\mathcal{C}$ y $Assoc(M)$ es un conjunto finito.*

Corolario 5.0.14 *Si R es un anillo Noetheriano conmutativo con identidad, I un ideal de R y $\mathcal{Z}(R/I)$ denota el conjunto de divisores de cero de R/I entonces*

$$\mathcal{Z}(R/I) = \bigcup_{i=1}^{m} \mathfrak{p}_i$$

Donde $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ son los primos asociados de R/I

Definición 5.0.15 Sea R un anillo y $P \in Spec(R)$, definimos la altura de P, denotada por $ht(P)$, como el supremo de longitudes de todas las cadenas primas descendentes de P. Para un ideal propio de R, definimos la altura de I, como $ht(I) := \text{ínf}\{ht(P) : P \in Spec(R) \ \& \ I \subseteq P\}$.

Proposición 5.0.16 *Sea R un anillo Noetheriano e I un ideal propio de R. El conjunto de ideales primos minimales sobre I coincide con el conjunto de ideales primos minimales de $Assoc(R/I)$. Por lo que $ht(I) = \text{mín}\{ht(P) : \ P \in Assoc(R/I)\}$*

Teorema 5.0.17 *[2] Sea R un anillo conmutativo Noetheriano con identidad e I un ideal de R. Entonces existen $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ ideales primarios de R tales que*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

Y

$$I \neq \mathfrak{q}_1 \cap \cdots \cap \widehat{\mathfrak{q}_i} \cdots \cap \mathfrak{q}_m$$

$\forall \ 0 \leq i \leq m$

Al conjunto $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$ se le llama descomposición primaria irredundante de I y satisface que $Assoc(R/I) = \{\mathfrak{p}_1 = rad(\mathfrak{q}_1), \ldots, \mathfrak{p}_m = rad(\mathfrak{q}_m)\}$.

Proposición 5.0.18 *([16], Lemma 5.3.11, [31])Si I es un ideal de R y $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ es una descomposición primaria irredundante, entonces:*

$$deg(R/I) = \sum_{ht(\mathfrak{q}_i)=ht(I)} deg(R/\mathfrak{q}_i).$$

Definición 5.0.19 La regularidad de R/I, denotada por reg(R/I), es el mínimo entero $r \geq 0$ tal que $H_I(d) = h_I(d)\ \forall d \geq r$.

Si R es un anillo Cohen-Macaulay y $dim(R/I) = 1$, entonces reg(R/I) es la regularidad de Castelnuovo-Mumford de R/I en el sentido de poner[7]. Si $dim(R/I) = 0$, entonces reg(R/I) es el mínimo entero tal que $\mathfrak{m}^d \subset I$

Definición 5.0.20 (la huella de un ideal). Sea $\prec$ un orden monomial en R y sea I un ideal no cero de R.

Un monomio $x^a \in R$ se dice monomio estándar de R/I con respecto a $\prec$ si $x^a \notin in_\prec(I)$. El conjunto de monomios estándar, denotado por $\Delta_\prec(I)$ lo llamaremos la huella de R/I.

Definición 5.0.21 Sea $\prec$ un orden monomial de R y $f \in R$ un polinomio homogéneo de grado d tal que $in_\prec(f) \in \Delta_\prec(I)$, entonces decimos que f es un polinomio estándar de R/I.

Observación 5.0.22 *La imagen de los polinomios estándar de grado d bajo la función canónica $R \to R/I$ es igual a R_d/I_d y la imagen de $\Delta_\prec(I)$ es una base de R/I como $K-$espacio vectorial. En particular si I es graduado, entonces $H_I(d)$ es el número de monomios estándar de grado d.*

Lema 5.0.23 *Sea I un ideal de R y $\mathcal{G} = \{g_1, \ldots, g_r\}$ un conjunto generador de I, entonces*

$$\Delta_\prec(I) \subseteq \Delta_\prec(in_\prec(g_1), \ldots, in_\prec(g_r))$$

Si $\mathcal{G} = \{g_1, \ldots, g_r\}$ es una base de Gröbner de I (vea el capítulo 2 y sección 2.3 de ésta tesis) la igualdad se cumple.

Demostración. Sea $x^a \in \Delta_\prec(I)$. Si $x^a \notin \Delta_\prec(in_\prec(g_1), \ldots, in_\prec(g_r))$, entonces $x^a = x^c in_\prec(g_i)$ para algún i entonces $x^a = in_\prec(x^c g_i)$, con $x^c g_i \in I$, una contradicción. Si $\mathcal{G}$ es una base de Gröbner de I, se sigue de su definición. ■

Lema 5.0.24 *Sea $\mathcal{G} = \{g_1, \ldots, g_r\}$ una base de Gröbner de I. Si para algún i, la variable x_i no divide a $in_\prec(g_j)$ para todo j, entonces x_i es valor regular de R/I.*

Demostración. Asuma que $x_i f \in I$. Por el algoritmo de la división $f = g + r$ con $g \in I$ y $r = 0$ o $r \neq 0$ y $in_\prec(r) \in \Delta_\prec(I)$. Si $r \neq 0$ entonces $x_i in_\prec(r) \in in_\prec(I)$ pero x_i es regular, así que $in_\prec(r) \in in_\prec(I)$ lo cual es una contradicción. ■

Corolario 5.0.25 *Si x_i es un divisor de cero de R/I para todo i entonces x_i pertenece a alguno de los monomios iniciales de g_j para algún j.*

Teorema 5.0.26 *Si I es un ideal graduado de R entonces R/I y $R/in \prec (I)$ tienen la misma función de Hilbert por lo tanto el mismo grado y regularidad.*

Lema 5.0.27 *Sea $\mathbb{P}^n$ el espacio proyectivo de dimensión n sobre un campo K y X un subconjunto finito de $\mathbb{P}^n$ y sea $[P] \in X$ con $P = (p_0, \ldots, p_n)$. Entonces el ideal anulador de $[P]$ es un ideal primo de la forma*

$$I_{[P]} = \langle p_j x_i - p_i x_j : i \neq j \in \{0, \ldots, n\} \rangle \tag{5.2}$$

Y $\operatorname{reg}(\mathrm{R}/\mathrm{I}_{[\mathrm{P}]}) = 1$, más aún $ht(I_{[P]}) = n$ y $I_X = \bigcap_{[P]\in X} I_{[P]}$ es la descomposición primaria de I_X. En particular I_X es un ideal radical.

Demostración.

- Primero probaremos la igualdad en (5.2). Es claro que

  $$\langle p_j x_i - p_i x_j : i \neq j \in \{0, \ldots, n\} \rangle \subseteq I_{[P]}$$

  para la otra contención probaremos que existe un subconjunto de $\{p_j x_i - p_i x_j : i \neq j \in \{0, \ldots, n\}\}$ que es base de Gröbner de $I_{[P]}$ bajo el siguiente orden.

  Dados $\alpha, \beta \in \mathbb{Z}_0^{n+1}$ $\alpha \prec \beta$ si $|\alpha| < |\beta|$ o $|\alpha| = |\beta|$ y la primera entrada no cero más a la izquierda de $\beta - \alpha$ es negativa. Notemos que bajo este orden $x_0 \prec x_1 \prec \ldots \prec x_n$.

  Sin pérdida de generalidad supongamos que $p_0 = 1$ así que para todo $i \in \{1, ..., n\}$ $x_i - p_i x_0$ pertenece a $I_{[P]}$ y es distinto de cero por lo que $x_i = in_\prec(x_i - p_i x_0) \in in_\prec(I_{[P]})$. Vamos a probar que $\{x_1, \ldots, x_n\}$ es un conjunto generador de $in_\prec(I_{[P]})$, en efecto, dado que $in_\prec(I_{[P]})$ es el ideal generado por los monomios líderes de polinomios en $I_{[P]}$ y que $I_{[P]}$ es homogéneo, es suficiente probar que para cada polinomio no cero $f \in (I_{[P]})_d$ con $d \in \mathbb{N}$, $in_\prec(f) \in \langle x_1, \ldots, x_n \rangle$, así supongamos lo contrario, que existe $f \in (I_{[P]})_d$ tal que $in_\prec(f) = x_0^d$ para algún d, pero para cualquier conjunto de índices $\{j_0, ..., j_n\}$ tales que $j_0 + \cdots + j_n = d$ se tiene que $x_0^{j_i} \prec x_i^{j_i}$ $\forall i \in \{1, \ldots, n\}$ luego $x_0^d \prec x_0^{j_0} x_1^{j_1} \cdots x_n^{j_n}$ lo que implica que $f = a x_0^d$ lo cual contradice al hecho de que $f \in I_{[P]}$. Luego $in_\prec(I_{[P]}) = \langle x_1, \ldots, x_n \rangle$ y se sigue que $\{x_i - p_i x_0\}_{i \neq 0}$ es base de Gröbner de $I_{[P]}$.

- Por el Teorema 5.0.26
$$\mathrm{reg(R/I_{[P]}) = reg(R/in_{\prec}(I_{[P]}))}$$
y como $(in_{\prec}(I_{[P]}))_1 = \langle x_1, \ldots, x_n \rangle_K$ entonces
$$H_{R/in_{\prec}(I_{[P]})}(1) = \binom{n+1}{1} - n = (n+1) - n = |X|$$
luego $reg(R/I_{[P]}) = 1$.

- Ahora probemos que $ht(I_{[P]}) = n$. Ya que $I_{[P]}$ es un ideal primo, comencemos con probar que cada elemento de la siguiente cadena es un ideal primo de R:
$$P_0 \subset P_1 \subset P_2 \subset \ldots \subset P_n$$
donde
$$P_0 = 0$$
$$P_1 = \langle x_n - p_n x_0 \rangle$$
$$P_2 = \langle x_n - p_n x_0, x_{n-1} - p_{n-1} x_0 \rangle$$
$$\vdots$$
$$P_n = \langle x_n - p_n x_0, x_{n-1} - p_{n-1} x_0, \ldots, x_1 - p_1 x_0 \rangle = I_{[P]}$$
Notemos que para cada $i \in [1, n]$ el conjunto ordenado:
$$\mathcal{G}_i = \{x_n - p_n x_0, x_{n-1} - p_{n-1} x_0, \ldots, x_{n-(i-1)} - p_{n-(i-1)} x_0\}$$
es base de Gröbner de P_i, es decir, $in_{\prec}(P_i) = \langle x_n, \ldots, x_{n-(i-1)} \rangle$. En efecto, sea $i \neq 0$, por el Critero de Buchberger's (Teorema 2.3.13) es suficiente probar que para cualesquiera $s \neq t$ en el intervalo $[n-(i-1), n]$ el residuo de dividir al $S-$polinomio $S(x_s - a_s x_0, x_t - a_t x_0) = a_t x_0 x_s - a_s x_0 x_t$ por $\mathcal{G}_i$ es cero. Si $a_s = 0$ o $a_t = 0$ es claro, así supongamos $a_s \neq 0$, $a_t \neq 0$ y $s > t$, por el algoritmo de la división $a_t x_0 x_s - a_s x_0 x_t = a_t x_0 (x_s - a_s x_0) - a_s x_0 (x_t - a_t x_0)$. Se sigue que para todo $i > 0$ $\mathcal{G}_i$ es base de Gröbner de I luego $in_{\prec}(P_i) = \langle x_n, \ldots, x_{n-(i-1)} \rangle \in Spec(R)$ y por el Lema 2.3.11, $P_i \in Spec(R)$ $\forall i \in \{1, ..., n\}$ por lo tanto $n \leq ht(I_{[P]})$ y como $R/I_{[P]} \simeq K[x_0]$ bajo el homomorfismo $f \mapsto res(f)^{\mathcal{G}_1}$ donde $res(f)^{\mathcal{G}_1}$ es el residuo de dividir a f por $\mathcal{G}_1$ $dim(R/I_{[P]}) = 1$, además se tiene que para cualquier ideal I y anillo R $ht(I) + dim(R/I) \leq dim(R)$, en nuestro caso tenemos lo siguiente $ht(I_{[P]}) + 1 \leq n + 1$ luego $ht(I_{[P]}) = n$.

■

Lema 5.0.28 *Sea $Y = \{[P], [Q]\} \subseteq \mathbb{P}^n$. Lo siguiente se cumple:*

1. $\mathrm{regR/I_Y} = 1$
2. *Existe $h \in R$ homogéneo de grado 1 tal que $h(P) \neq 0$ y $h(Q) = 0$.*
3. *Para cada $d \geq 1$ existe $f \in R_d$ tal que $f(P) \neq 0$ y $f(P) = 0$.*
4. *Si $X \subseteq \mathbb{P}^n$ con al menos dos elementos y $d \geq 1$ entonces existe $f \in R_d$ tal que $f \notin I_X$ y $(I_X : f) \neq I_X$.*

Demostración.

1. Por la proposición 2.2.8 $H_Y(0) = 1 < H_Y(1)$ y como $|Y| = 2$ entonces $\mathrm{reg(R/I_Y)} = 1$
2. Consideremos la función

$$ev_1 : R_1 \to K^2, \quad f \mapsto (f(P), f(Q)).$$

   Por la parte 1, ev_1 es sobre así que $\exists h \in R_1$ tal que $(h([P]), h([Q])) = (1, 0)$

3. Se sigue 2 tomando $f = h^d$
4. Si $|X| \geq 2$ sean $[P] \neq [Q] \in X$entonces para cada $d \geq 1$ sea f como en 3, notemos $f \notin I_X$ y $f \in I_{[Q]}$, como $I_{[Q]} \in Assoc(R/I_X)$ por el corolario 5.0.14 f es un divisor de cero de R/I_X luego $(I_X : f) \neq I_X$.

■

Proposición 5.0.29 *Existe un entero $r \geq 0$ tal que*

$$|X| = \delta_X(0) > \delta_X(1) > \ldots > \delta_X(d) = \delta_X(r) = 1 \ \forall d \geq r$$

Demostración. Supongamos que $\delta_X(d) > 1$, es suficiente probar que $\delta_X(d) > \delta_X(d+1)$. Sea $g \notin I_X$, si $V_X(g) := \{[P] \in X : g(P) = 0\}$ entonces el peso de hamming de $(g(P_1), \ldots, g(P_{|X|})$ es $|X| - |V_X(g)|$, si además g es tal que

$$|V_X(g)| = \text{máx}\{|V_X(f)| : ev_d(f) \neq 0;\ f \in R_d\}$$

Entonces $\delta_X(d) = |X| - |V_X(g)| \geq 2$ así que existen $[P], [Q] \in X$ distintos tales que $g(P), g(Q) \neq 0$. Por el lema anterior existe $h \in R_1$ tal que $h(P) \neq 0$ y $h(Q) = 0$ luego $hg \in R_{d+1}$ es tal que $hg \notin I_X$ con al menos $|V_X(g)|+1$ ceros, se sigue que $\delta_X(d) > \delta_X(d+1)$

■

5.1. Calculando el número de ceros usando el grado

En esta sección daremos una fórmula del grado para calcular el número de ceros que un polinomio homogéneo tiene en cualquier subconjunto finito de un espacio proyectivo sobre cualquier campo.

Definición 5.1.1 Sea R un anillo e $I \subseteq R$ un ideal, decimos que I es no-mixto si todos sus primos asociados tienen la misma altura.

Definición 5.1.2 Sea R un anillo y I un ideal de R. Decimos que I es un ideal radical si coincide con su radical, es decir, $rad(I) = I$.

Ejemplo 5.1.3 Sea $X \subset \mathbb{P}^n$ un subconjunto finito del $n-$espacio proyectivo sobre un campo. Del lema 5.0.27 I_X es un ideal radical no mixto de R.

Lema 5.1.4 *Sea $I \subset R$ un ideal graduado radical no mixto de R. Si $f \in R$ es homogéneo, $(I : f) \neq I$ y $\mathcal{A}$ es el conjunto de todos los primos asociados de R/I que contienen a f, entonces $ht(I) = ht(I, f)$ y*

$$degR/(I, f) = \sum_{\mathfrak{p} \in \mathcal{A}} degR/\mathfrak{p}.$$

***Demostración*.** Si f es un divisor de cero de I entonces $f \in \bigcup_{\mathfrak{p} \in Assoc(R/I)} \mathfrak{p}$ por lo que el conjunto $\mathcal{A} \neq \emptyset$ y $f \in \bigcup_{\mathfrak{p} \in \mathcal{A}} \mathfrak{p}$, por la proposición 5.0.13 para todo $\mathfrak{p} \in \mathcal{A}$: $I \subseteq (I, f) \subseteq \mathfrak{p}$, por la proposición 5.0.18 y el hecho de que I es no-mixto: $ht(I) = ht(I, f) = ht(P)$ para todo $\mathfrak{p} \in \mathcal{A}$, más aún, como para cualquier $\mathfrak{p} \in \mathcal{A}$, $\mathfrak{p}$ es minimal para I (vea la proposición 5.0.18), también lo es para (I, f) así $\mathcal{A} \subseteq Assoc(R/(I, f))$, más aún, el conjunto de primos asociados de $R/(I, f)$ que tienen altura igual a $ht(I)$ es $\mathcal{A}$. Sea

$$(I, f) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}_{r+1}^{'} \cap \cdots \cap \mathfrak{q}_t^{'} \tag{5.3}$$

una descomposición irredundante de (I, f). Donde $rad(q_i) = p_i$, $\mathcal{A} = \{\mathfrak{p}_1, \ldots \mathfrak{p}_r\}$, y $ht(\mathfrak{q}_i^{'}) > ht(I)$ para $i > r$. Asumamos que $Assoc(R/I) = \{\mathfrak{p}_1, \ldots \mathfrak{p}_m\}$ con $m \geq r$, como I es un ideal radical, entonces $I = \bigcap_{i=1}^{m} \mathfrak{p}_i$. Probaremos la siguiente igualdad

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}_{r+1}^{'} \cap \cdots \cap \mathfrak{q}_t^{'} \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m \tag{5.4}$$

La inclusión " $\supseteq$ " es clara por que $\mathfrak{p}_i \supseteq \mathfrak{q}_i$ $\forall i \in \{1, \ldots, m\}$. La desigualdad " $\subseteq$ " se sigue, notando el lado derecho de la ecuación (5.4) es igual a $(I, f) \cap \mathfrak{p}_{r+1} \cap \cdots \cap \mathfrak{p}_m$ y consecuentemente contiene a $I = \bigcap_{i=1}^{m} \mathfrak{p}_i$. Notemos además que $rad(\mathfrak{q}_j^{'}) = \mathfrak{p}_j^{'} \not\subset \mathfrak{p}_i$ $\forall i, j$ y $\mathfrak{q}_j, \mathfrak{p}_j \not\subset \mathfrak{p}_i \forall i \neq j$ luego $(R - \mathfrak{p}_i) \cap \mathfrak{p}_j$, $(R - \mathfrak{p}_i) \cap \mathfrak{p}_j^{'} \neq \emptyset$ $\forall i \neq j$ por lo que $(\mathfrak{p}_j)_{\mathfrak{p}_i} = (\mathfrak{p}_j^{'})_{\mathfrak{p}_i} = R_{\mathfrak{p}_i}$ así que $I_{\mathfrak{p}_i} = \bigcap (\mathfrak{p}_j)_{\mathfrak{p}_i} = (\mathfrak{p}_i)_{\mathfrak{p}_i} = (\mathfrak{q}_i)_{\mathfrak{p}_i}$ y por lo tanto $\mathfrak{p}_i = I_{\mathfrak{p}_i} \cap R = I_{\mathfrak{q}_i} \cap R = \mathfrak{q}_i$, de la ecuación (5.3) y la proposición 5.0.18 se sigue el Lemma. ■

Lema 5.1.5 *Sea X un subconjunto finito de $\mathbb{P}^n$. Si $f \neq 0 \in R^h$ entonces*

$$|V_X(f)| = \begin{cases} degR/(I_X, f) & si\ (I_X : f) \neq I_X \\ 0 & si\ (I_X : f) = I_X \end{cases}$$

Demostración. Por el lema 5.0.27 los primos correspondientes a su descomposición primaria son $\{I_{[Q]}\}_{[Q]\in X}$ y son tales que $regR/I_{[Q]} = 1\ \forall [Q] \in X$, sea $\mathcal{A}$ el conjunto de ideales $I_{[P]}$ tales que $f \in I_{[P]}$ entonces $f(P) = 0$ si y solo si $I_{[P]} \in \mathcal{A}$ por lo que

$$|V_X(f)| = \sum_{[P]\in V_X(f)} 1 = \sum_{I_{[P]}\in\mathcal{A}} 1 = \sum_{I_{[P]}\in\mathcal{A}} degR/I_{[P]}$$

Si $(I_X : f) \neq I_X$ por el lema 5.1.4 $|V_X(f)| = degR/(I, f)$. Si $(I_X : f) = I_X$ entonces f es regular luego $f \notin \bigcup_{[P]\in X} I_{[P]}$ por lo que $V_X(f) = \emptyset$ y $|V_X(f)| = 0$. ■

5.2. La función distancia mínima de un ideal graduado

En esta sección estudiaremos la función distancia mínima δ_I de un ideal graduado I y mostraremos que generaliza la función distancia mínima de un código Reed-Muller. El siguiente resultado se usa para acotar el número de ceros de polinomios sobre campos finitos y estudiar sus propiedades generales

Lema 5.2.1 *Sea I un ideal no mezclado de R y $\prec$ un orden monomial sobre R. Si $f \in R^h$ y $(I : f) \neq I$ entonces*

$$degR/(I, f) \leq R/(in_\prec(I), in_\prec(f)) \leq degR/I$$

y $degR/(I, f) < degR/I$ si I es un ideal radical no mezclado tal que $f \notin I$

Demostración. Sea $J = (I, f)$ y $L = (in_\prec(I), in_\prec(f))$.

Primero mostraremos que $dim(R/L) = dim(R/I)$. Como $f \in \mathcal{Z}(R/I)$ e I es no mezclado para todo $\mathfrak{p} \in Assoc(R/I)$ $dim(R/I) = dim(R/\mathfrak{p})$, así escogemos $\mathfrak{p}$ tal que $f \in \mathfrak{p}$ luego $I \subset J \subset \mathfrak{p}$ y obtenemos $dim(R/J) = dim(R/I)$ pero por el teorema 5.0.26 R/J y R/L tienen misma función de Hilbert por lo que $dimR/J = dimR/L$ luego

$$dim(R/J) = dim(R/L) = dim(R/I)$$

Sea $\mathcal{G} = \{g_1, \ldots, g_r\}$ una base de Gröbner de I entonces $\mathcal{G} \cup \{f\}$ genera a $J = (I, f)$ y por el lema 5.0.23 tenemos que

$$\Delta_\prec(J) \subseteq \Delta_\prec(in_\prec(g_1), \ldots, in_\prec(g_r), in_\prec(f)) = \Delta_\prec(L)$$

Probemos que $\Delta_\prec(L) \subseteq \Delta_\prec(I)$. Sea $m \in \Delta_\prec(L)$ entonces ningún monomio del conjunto $\{in_\prec(g_1), \ldots, in_\prec(g_r)\}$ lo divide, luego $m \in \Delta_\prec(I)$. Así

$$\Delta_\prec(J) \subseteq \Delta_\prec(L) \subseteq \Delta_\prec(I)$$

Por lo que

$$0 \leq H_J(d) \leq H_L(d) \leq H_I(d) \ \ \forall d \geq 0 \tag{5.5}$$

Se sigue de que $dim(R/J) = dim(R/L) = dim(R/I)$, la definición del grado y de la ecuación (5.5) que

$$degR/J \leq degR/L \leq degR/I$$

Si I es un ideal radical no mixto y $f \notin I$ entonces existe un ideal primo minimal de I tal que $f \notin \mathfrak{p}$, del lema 5.1.4 $deg(R/(I,f)) < deg(R/I)$. ■

Observación 5.2.2 *Si I es un ideal no mezclado de R de dimensión 1 entonces $(I:f) = I$ si y sólo si $dim(R/(I,f))$. Recordemos que $(I:f) = I$ si y solo si f es elemento regular de R/I: Como $(I,f) \supset I$ entonces $dimR/(I,f) \leq dimR/I$. Sean $\mathfrak{q}_0 \supseteq \mathfrak{q}_1$ ideales primos sobre (I,f), entonces $I \subset (I,f) \subseteq \mathfrak{q}_1 \subseteq \mathfrak{q}_0$. Si $\mathfrak{q}_1 \neq \mathfrak{q}_0$ entonces q_1 es minimal sobre I pues $dimR/I = 1$ luego f no es regular $\#_c$, se sigue que $dimR/(I,f) = 0$. En este caso puede que $deg(R/(I,f)) < deg(R/I)$.*

Corolario 5.2.3 *Sea $X \subset \mathbb{P}^n$ un conjunto finito, $\prec$ un orden monomial de R y I_X el ideal anulador de X. Si $f \in R^h$ es divisor de cero de I_X entonces*

$$|V_X(f)| = deg(R/(I_X,f)) \leq deg(R/I_X) \leq deg(R/(in_\prec(I_X), in_\prec(f))) \leq deg(R/I_X)$$

y $deg(R/(I_X,f)) < deg(R/I_X)$ si $f \notin I_X$.

Definición 5.2.4 Definimos la función distancia mínima de I como $\delta_I : \mathbb{N} \to \mathbb{Z}$ dada por:

$$\delta_I(d) = \begin{cases} deg(R/I) - \text{máx}\{deg(R/(I,f)) : f \in \mathcal{F}_d\} \\ deg(R/I) \qquad\qquad\qquad\qquad si\ \mathcal{F}_d = \emptyset \end{cases}$$

Donde $\mathcal{F}_d = \{f \in R_d : f \notin I \ y \ (I:f) \neq I\}$.

Sea I como en la definición anterior, $\prec$ un orden monomial de R, $\mathcal{G}$ una base de Groebner de I y $\Delta_\prec(I)$ la huella de I. Si $\Delta_\prec(I) \cap R_d = \{x^{a_1}, \ldots, x^{a_n}\}$ y $\mathcal{F}_{\prec,d} = \{f = \sum \lambda_i x^{a_i} : f \neq 0, \ \lambda_i \in K, \ (I:f) \neq I\}$, usando el algoritmo de la división podemos escribir:

$$\begin{aligned} \delta_I(d) &= deg(R/I) - \text{máx}\{deg(R/(I,f)) : f \in \mathcal{F}_d\} \\ &= deg(R/I) - \text{máx}\{deg(R/(I,f)) : f \in \mathcal{F}_{\prec,d}\} \end{aligned} \tag{5.6}$$

Teorema 5.2.5 *Sea I es un ideal graduado no mezclado de R, $\prec$ es un orden monomial de R y $\mathcal{G}$ una base de Gröbner de I. Si $\Delta_\prec(I)_d^p$ es el conjunto de polinomios estándar de grado d, entonces*

$$\begin{aligned}\delta_I(d) &= \text{mín}\{deg(R/(I:f)) : f \in R_d - I\} \\ &= \text{mín}\{deg(R/(I:f)) : f \in \Delta_\prec(I)_d^p\}\end{aligned}$$

Demostración. La segunda igualdad se cumple por el algoritmo de la división $f \in R_d - I$ si y sólo si el residuo de dividir a f por $\mathcal{G}$ es $h \in \Delta_\prec(I)_d^p$ así que $(I:f) = (I:h)$.

Probaremos la primera igualdad.

Si $\mathcal{F}_d = \emptyset$. $\delta_I(d) = deg(R/I)$, como cada $f \in R_d - I$ satisface que $(I:f) = I$ entonces $\text{mín}\{deg(R/(I:f)) : f \in R_d - I\} = deg(R/I) = \delta_I(d)$.

Si $\mathcal{F}_d \neq \emptyset$. Sea $f \in \mathcal{F}_d$, usando que I es no mixto no es difícil ver que $dim(R/I) = dim(R/(I:f)) = dim(R/(I,f))$; además hay sucesiones exactas:

$$0 \to (I:f)/I \to R/I \to R/(I,f) \to 0$$

$$0 \to (I:f)/I \to R/I(-d) \xrightarrow{f} R/I \to R/(I,f) \to 0$$

Recordemos que $R/I(-d)$ es la graduación de R/I inducida por el corrimiento $-d$ (vea 1.2.4).Notemos que el morfismo $R/I(d) \to R/I$ inducido por la multiplicación por f es graduado. Por la aditividad de la función de Hilbert tenemos:

$$dim_K(I:f)/I(i) = H_I(i) - H_{(I:f)}(i) = H_I(i-d) - H_I(i) + H_{(I,f)}(i)\ \forall i \geq 0 \quad (5.7)$$

Por definición de $\delta_I(d)$ es suficiente mostrar la siguiente igualdad

$$deg(R/(I:f)) = deg(R/I) - deg(R/(I,f)) \quad (5.8)$$

Suponiendo que la igualdad en la ecuación (5.8) tendríamos que $\delta_I(d) = deg(R/I) - \text{máx}\{deg(R/(I,f)) : f \in \mathcal{F}_d\} = deg(R/I) - \text{máx}\{deg(R/I) - deg(R/(I:f)) : f \in \mathcal{F}_d\} = \text{mín}\{deg(R/(I:f)) : f \in R_d - I\}$.

Regresando a la prueba de la ecuación (5.8).

Si $dimR/I = 0$ usando la ecuación (5.5) tenemos

$$\sum_{i\geq 0} H_I(i) - \sum_{i\geq 0} H_{(I:f)}(i) = \sum_{i\geq 0} H_I(i-d) - \sum_{i\geq 0}(i) + \sum_{\geq 0} H_{(I,f)}(d)$$

como $\sum_{i\geq 0} H_I(i-d) = \sum_{i\geq 0} H_I(i)$ se tiene que

$$\begin{aligned}deg(R/(I:f)) = dim_K R/(I:f) &= \sum_{i\geq 0} H_{(I:f)}(i) = \sum_{i\geq 0} H_I(i) - \sum_{i\geq 0} H_(I,f)(i) \\ &= dim_K R/I - dim_K R/(I,f) = deg(R/I) - deg(R/(I,f))\end{aligned}$$

Si $k = dimR/I - 1$ por el teorema de Hilbert-Serre: $H_I, H_{(I:f)}, H_{(I,f)}$ son polinomios de grado k para $i \gg 0$. Entonces, dividiendo por i^k y tomando límites cuando $i \to \infty$ la igualdad de la ecuación (5.8) se cumple.

■

Definición 5.2.6

$$fp_I(d) = \begin{cases} deg(R/I) - \text{máx}\{deg(R/(in_\prec(I), x^a) : x^a \in \Delta_\prec(I)_d & si\ \Delta_\prec(I)_d \neq \emptyset\} \\ deg(R/I) & si\ \Delta_\prec(I)_d \end{cases}$$

Ahora veremos el resultado principal de este capítulo

Teorema 5.2.7 *Sea $\prec$ un orden monomial de R e I un ideal homogéneo no mezclado con $dimR/I \geq 1$ tal que t_i es un divisor de cero de R/I para todo $i = 0, \ldots, n$. Lo siguiente se cumple*

(i) $\mathcal{F}_d \neq \emptyset$ *para* $d \geq 0$.

(ii) $\delta_I(d) \geq fp_I(d)$ *para* $d \geq 1$

(iii) $deg(R/(I, x^a)) \leq deg(R/(in_\prec(I), x^a)) \leq deg(R/I)$ *para cualquier* $x^a \in \Delta_\prec(I)_d$.

(iv) $fp_I(d) \geq 0$

(v) $\delta_I(d) \geq \delta_I(d+1) \geq 0$ *para todo* $d \geq 1$

(vi) Si I es un ideal radical y sus primos asociados están generados por formas lineales, entonces hay un entero $r \geq 0$ tal que

$$\delta_I(1) > \delta_I(2) > \ldots > \delta_I(r) = \delta_I(d) = 1 \text{ para } d \geq r \tag{5.9}$$

***Demostración*.**

(i) Ya que $dimR/I \geq 0$ sabemos que existe $l \in \{0, \ldots, n\}$ tal que $x_l^d \notin I$ y como x_l es divisor de cero lo es también x_l^d por lo que $(I : x_l^d) \neq I$, luego $x_l^d \in \mathcal{F}_d$

(ii,iv) Como $\mathcal{F}_d \neq \emptyset$, sea $F \in \mathcal{F}_d$ tal que

$$\delta_I(d) = deg(R/I) - deg(R/(I, f))$$

Asumamos que F es combinación lineal de monomios estándar de R/I respecto a $\prec$. El lema 5.2.1 nos dice que

$$degR/(I, F) \leq R/(in_\prec(I), in_\prec(F)) \leq degS/I$$

Donde $in_{\prec}(F)$ es un monomio estándar de R/I De la definición de $fp_I(d)$ tenemos las siguientes desigualdades

$$deg(R/(I,F)) \leq deg(R/I) - fp_I(d) \leq deg(R/I)$$

$$-deg(R/I) \leq -deg(R/I) + fp_I(d) \leq -deg(R/(I,F))$$

$$0 \leq fp_I(d) \leq deg(R/I) - deg(R/(I,F)) = \delta_I(d)$$

(iii) Por el lema 5.0.24 cualquier monomio estándar de grado d es divisor de cero de R/I, por el lema 5.2.1 tenemos las desigualdades en (iii).

(v) Como $\mathcal{F}_d \neq \emptyset$ y $\delta_I(d) \geq 0$ tomemos $F \in \mathcal{F}_d$ tal que

$$deg(R/(I,F)) = deg(R/I) - \delta_I(d)$$

Hay $h \in S_1$ tal que $hF \notin I$ porque de otro modo el ideal maximal $\mathfrak{m} = \langle x_0, \ldots, x_n \rangle$ sería un primo asociado de R/I, una contradicción al hecho de que I es un ideal radical no mezclado de $dimR/I \geq 1$. Si $hF \in I \ \forall h \in R_1$ entonces $x_l \in ann(\overline{F})$ para todo $l \in \{0, \ldots, n\}$ luego $\mathfrak{m} \subseteq ann(\overline{F})$, por lo que $\mathfrak{m} = ann(\overline{F})$ y se sigue que $\mathfrak{m} \in Assoc(R/I)$ con $dimR/\mathfrak{m} = 0$. Lo cual contradice una vez más que I es no mezclado de dimensión mayor o igual que uno. Como F es divisor de cero de R/I también los es $hf \in \mathcal{F}_{d+1}$ y además

$$ht(I) = ht(I,F) = ht(I,hF)$$

tomando funciones de Hilbert en la sucesión exacta

$$0 \to (I,F)/(I,hf) \to R/(I,hF) \to R/(I,f) \to 0$$

obtenemos

$$dim_K(I,F)/(I,hf)(d) - H_{(I,hF)}(d) + H_{I,f}(d+1) = 0$$

luego

$$H_{(I,hF)}(d) \geq H_{(I,F)}(d+1)$$

y

$$deg(R/(I,hF)) \geq deg(R/(I,F)) = deg(R/I) - \delta_I(d)$$

Por lo que

$$\text{máx}\{deg(R/(I,g)) : g \in \mathcal{F}_{d+1}\} \geq deg(R/(I:hF)) \geq deg(R/I) - \delta_I(d)$$

y así

$$\delta_I(d) \geq deg(R/I) - \text{máx}\{deg(R/(I,g)) : g \in \mathcal{F}_{d+1}\} = \delta_I(d+1)$$

(vi) Por el lema 5.2.1 $\delta_I(d) \geq 1$ para $d \geq 1$. Asumamos que $\delta_I(d) > 1$. Por (v) es suficiente mostrar que $\delta_I(d) > \delta_I(d+1)$. Sea $F \in \mathcal{F}_d$ tal que $deg(R/(I,F)) = deg(R/I) - \delta_I(d)$ y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados de I entonces por el lema 5.1.4 tenemos

$$\delta_I(d) = deg(R/I) - deg(R/(I,F)) = \sum_{i=1}^{m} deg(R/\mathfrak{p}_i) - \sum_{j:F\in\mathfrak{p}_j} deg(R/\mathfrak{p}_j) \geq 2$$

Así que hay $\mathfrak{p}_k, \mathfrak{p}_l$ tales que $F \notin \mathfrak{p}_k \cup \mathfrak{p}_l$. Como I es no mezclado existe $h \in \mathfrak{p}_k - \mathfrak{p}_l$ tal que h es homogéneo de grado 1. Entonces $hF \notin I$ por que $h \notin \mathfrak{p}_j$ y como hF es divisor de cero de I entonces $(I : hF) \neq I$. Notando que $F \notin \mathfrak{p}_k$ y $hF \in \mathfrak{p}_k$ por el lema 3.1

$deg(R/I) - \delta_I(d) = deg(R/(I,F)) = \sum_{j:F\in\mathfrak{p}_j} deg(R/\mathfrak{p}_j) < \sum_{k:hF\in\mathfrak{p}_k} deg(R/\mathfrak{p}_k) = deg(R/(I,hF)) \leq deg(R/I) - \delta_I(d+1)$.

■

Corolario 5.2.8 *Si I es un ideal Cohen-Macaulay libre de cuadrados y monomial, entonces hay un entero $r \geq 0$ tal que*

$$\delta_I(1) > \delta_I(2) > \ldots > \delta_I(r) = \delta_I(d) = 1 \text{ para } d \geq r$$

Resultados, discusión, conclusiones y perspectivas

El gran logro de este trabajo es la maduréz y exploración de resultados referentes a teoría de códigos a través del álgebra conmutativa y geometría algebraica clásica. Ya que lo expuesto no es más que el seguimiento de mi tesis de licenciatura "Introducción a la Teoría de Códigos Evaluación".

Siendo más concreta, ésta tesis contiene el material necesario para introducirse a la teoría de códigos algebraicos de manera natural y progresiva. Más aún, contiene ejemplos y demostraciones que ayudan al lector a reforzar las definiciones y teoremas clave para su estudio.

Para lectores más experimentados en el tema podrán encontrar ideas y demostraciones de resultados de gran interés como lo es la generalización de los códigos de Segre, la cual da una perspectiva diferente de estudiar un código, es decir, para cada código algebraico podríamos definir una descomposición de Segre y obtener de manera independiente cada uno de sus parámetros con la idea de disminuir la complejidad de su cálculo, a lo cual se siguen las siguientes preguntas: ¿es posible definir para cada código una descomposición de Segre?, ¿de existir dicha descomposición, que tan difícil sería obtenerla? y por último ¿estaríamos reemplazando un problema con otro problema más difícil de calcular?.

Sin dejar de lado el último capítulo, la construcción de la distancia mínima de un ideal y la correspondencia con la distancia mínima de su código asociado, es un gran resultado ya que como hemos mencionado antes, su naturaleza algebraica da nuevas herramientas para su cálculo. Recordemos que es el parámetro más difícil de calcular en el sentido que a diferencia de la dimensión y longitud, no teníamos la gran variedad de resultados que ayudan a su cálculo.

Bibliografía

[1] A. V. Geramita, M. K., and Robbiano, L. Cayley-bacharach schemes and their canonical modules. *Trans. Amer.Math. Soc. 339 No 1* (1993), 163–189.

[2] Atiyah, M. *Introduction to commutative algebra*. Westview Press, 1994.

[3] Bruns, W., and Gubeladze, J. *Polytopes, rings, and K-theory*. Springer Science & Business Media, 2009.

[4] C. Carvalho, V. G. L. N., and López, H. H. Projective nested cartesian codes. *Preprint arXiv:1411.6819v1* (2014).

[5] C. Renter´ıa, A. S., and Villarreal, R. H. Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields. *Finite Fields Appl. 17 no. 1* (2011), 81–104.

[6] Carvalho, C. On the second hamming weight of some reed-muller type codes. *Finite Fields Appl. 24* (2013), 88–94.

[7] D. Cox, J. L., and O'Shea, D. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.

[8] Dias, E., and Neves, J. Codes over a weighted torus. *Finite Fields Appl. 33* (2015), 66–79.

[9] E. Sarmiento, M. V. P., and Villarreal, R. H. The minimum distance of parameterized codes on projective tori. *Appl. Algebra Engrg. Comm. Comput.* **22** *no. 4* (2011), 249–264.

[10] Eisenbud, D. *Commutative Algebra with a view toward Algebraic Geometry*. 150. Graduate Texts in Mathematics Springer-Verlag, 1995.

[11] Ford, T. J. *Separable Algebras over Commutative Rings*.

[12] Geil, O. On the second weight of generalized reed-muller codes. *Des. Codes Cryptogr 48* (2008), 323–330.

[13] Geil, O., and Thomsen, C. Weighted reed-muller codes revisited. *Des. Codes Cryptogr. 66* (2013), 195–220.

[14] González-Sarabia, M., and Rentería, C. Evaluation codes associated to complete bipartite graphs. *Int. J. Algebra 2* (2008), no. 1–4, 163–170.

[15] González-Sarabia, M., and Rentería, C. The second generalized hamming weight of some evaluation codes arising from complete bipartite graphs. *Int. J. Contemp. Math. Sci. 4* (2009), no. 25–28 and 1345–1352.

[16] Greuel, G.-M., and Pfister, G. *A Singular introduction to commutative algebra.* Springer Science & Business Media, 2012.

[17] H. H. López, C. R., and Villarreal, R. H. Affine cartesian codes. *Des. Codes Cryptogr.* **71** *no. 1* (2014), 5–19.

[18] H. H. López, E. Sarmiento, M. V. P., and Villarreal, R. H. Parameterized affine codes. *Studia Sci. Math. Hungar.* **49** *no. 3* (2012), 406–418.

[19] Harris, J. *Algebraic Geometry. A first course*, vol. 133. Graduate Texts in Mathematics , Springer-Verlag, New York, 1992.

[20] I. M. Duursma, C. R., and Tapia-Recillas, H. Reed–muller codes on complete intersections. *Appl. Algebra Engrg. Comm. Comput. 11 no. 6* (2001), 455–462.

[21] Kahle, T., and Rauh, J. Toric fiber products versus segre products. *Abh. Math. Semin. Univ. Hambg. 84 no. 2* (2014), 187–201.

[22] L. Gold, J. L., and Schenck, H. Cayley-bacharach and evaluation codes on complete intersections. *J. Pure Appl. Algebra 196 no. 1* (2005), 91–99.

[23] López, H. H., and Villarreal, R. H. Computing the degree of a lattice ideal of dimension one. *Symbolic Comput. 65* (2014), 15–28.

[24] M. González-Sarabia, C. R., and de la Torre, M. H. Minimum distance and second generalizaed hamming weight of two particular linear codes. *Congressus Numerantium 8* (2002), 511–518.

[25] M. González-Sarabia, C. R., and H., T.-R. Reed–muller-type codes over the segre variety. *Finite Fields Appl.* **8** *no. 4* (2002), 511–518.

[26] M. González-Sarabia, C. R., and Sánchez, A. J. Minimum distance of some evaluation codes. *Appl. Algebra Engrg. Comm. Comput. 24 2* (2013), 95–106.

[27] M. Tsfasman, S. V., and Nogin, D. *Algebraic geometric codes*: *basic notions, Mathematical Surveys and Monographs 139*. American Mathematical Society, Providence, RI, 2007.

[28] MacWilliams, F. J., and Sloane, N. *The Theory of Error-correcting Codes*. North-Holland, 1977.

[29] Matsumura, H. *Commutative Ring Theory*. Cambridge, Studies in Advanced Mathematics **8**, Cambridge University Press, 1986.

[30] Neves, J., Pinto, M. V., and Villarreal, R. H. Vanishing ideals over graphs and even cycles. *Communications in Algebra 43*, 3 (2015), 1050–1075.

[31] O'Carroll, L., Planas-Vilanova, F., and Villarreal, R. H. Degree and algebraic properties of lattice and matrix ideals. *SIAM Journal on Discrete Mathematics 28*, 1 (2014), 394–427.

[32] P. Delsarte, J. M. G., and MacWilliams, F. J. On generalized reed–muller codes and their relatives. *Information and Control 16* (1970), 403–442.

[33] Schaathun, H. G., and Willems, W. A lower bound on the weight hierarchies of product codes. *Discrete Appl. Math 128* (2003), 251–261.

[34] Sørensen, A. B. Projective reed-muller codes. *IEEE Trans. Inf. Theory IT-37, No.6* (1991), 1567–1576.

[35] van Lint, J. H. *coding theory.* Lecture Notes in Mathematics Vol. 201 *(1973).*

[36] Wei, V. K. *Generalized hamming weights for linear codes.* IEEE Trans. Inform. Theory 37 no. 5 *(1991), 1412–1418.*

[37] Wei, V. K., and Yang, K. *On the generalized hamming weights of product codes.* IEEE Trans. Inform. Theory 39 no. 5 *(1993), 1709–1713.*