UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD IZTAPALAPA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA
POSGRADO EN MATEMÁTICAS

# CÓDIGOS PROYECTIVOS TIPO REED-MULLER SOBRE EL ROLLO NORMAL RACIONAL GENERALIZADO

## TESIS

QUE PARA OBTENER EL GRADO DE:

**Doctor en Ciencias (Matemáticas)**

PRESENTA:

**Xavier Ramírez Mondragón**

ASESOR:

Dr. Horacio Tapia Recillas

SINODALES:

Dr. Horacio Tapia Recillas
Dr. Felipe de Jesús Zaldívar Cruz
Dr. José Noé Guitiérrez Herrera
Dr.Guillermo Benito Morales Luna
Dr. Rafael Heraclio Villarreal Rodríguez

Ciudad de México, 16 de Octubre de 2019

# Resumen

En 1988 Lachaud introdujo la clase de los códigos proyectivos tipo Reed-Muller, los cuales se definen evaluando el espacio de polinomios homogéneos de un grado fijo $d$ en los puntos de $\mathbb{P}^n(\mathbb{F}_q)$, el espacio proyectivo $n$-dimensional sobre el campo finito con $q$ elementos $\mathbb{F}_q$.

La parte medular de este trabajo consiste en estudiar los códigos que se generan evaluando estos mismos polinomios en los puntos $\mathbb{F}_q$-racionales de un Rollo Normal Racional generalizado, el cual es una variedad proyectiva definida sobre la cerradura algebraica de $\mathbb{F}_q$. Dicha variedad puede construirse a partir de un conjunto de curvas normales racionales contenidas en espacios lineales complementarios de un espacio proyectivo.

Entre otras cosas se determina una fórmula para la dimensión de estos códigos en el caso general, así como las formas simplificadas que esta fórmula adopta bajo ciertas condiciones. También probamos que en ciertos casos nuestra construcción resulta ser equivalente a un producto directo de los códigos originalmente definidos por Lachaud. Damos el valor exacto para la distancia mínima para estos casos especiales. Utilizamos técnicas basadas en las bases de Gröbner.

# Introducción

Podríamos decir que la moderna teoría de códigos tiene sus orígenes a finales de la década de 1940. No haremos una lista exhaustiva, pero entre los trabajos más influyentes podemos citar el de Claude Shannon [38], el de Marcel Golay [18] y el de Richard Hamming [23]. El lector interesado en ahondar en la historia del génesis de la teoría de códigos puede consultar [6].

A grandes rasgos, podemos decir que la teoría de códigos surgió como respuesta a problemáticas relacionadas con la transmisión y almacenamiento de información digital. Como es bien sabido, un fragmento de información digital puede ser representado como una sucesión de ceros y unos, donde a cada elemento de la sucesión se le llama bit. A veces ocurren errores al almacenar o transmitir información que provocan que uno o varios bits cambien su valor de 0 a 1 o viceversa.

La idea básica de la teoría de códigos es agregar redundancia a la información para hacerla más robusta frente a los errores. A este proceso se le conoce como codificación y el resultado obtenido es un código. Para recupe-

rar la información se extrae la redundancia agregada, lo cual constituye la fase de decodificación.

Desde su surgimiento, la teoría de códigos ha tenido un gran crecimiento relacionando entre sí a varias áreas de las matemáticas, la computación y la ingeniería eléctrica. Esta teoría ha encontrado importantes aplicaciones en el área de las comunicaciones digitales, entre las que pueden contarse la transmisión de información desde naves espaciales, las transmisiones satelitales, la telefonía celular y el almacenamiento de información en dispositivos digitales -teléfonos celulares, tablets, computadoras, etc.

De entre todos los tipos de códigos, los códigos lineales ocupan un lugar preponderante. Estos códigos tienen una estructura algebraica de espacio vectorial sobre algún campo finito que facilita su descripción, su codificación y su decodificación. Entre los códigos lineales más conocidos y usados se encuentran los códigos de Hamming, Golay, BCH, Reed-Solomon, y Reed-Muller (ver por ejemplo [26]).

A veces puede transcurrir un lapso de tiempo considerable entre el estudio teórico de un código y su aplicación en el mundo real. Por ejemplo, los códigos de Reed-Solomon fueron creados en 1960 [34], pero su aplicación masiva tuvo que esperar a la década de 1980, con la aparición de los discos compactos.

Los códigos binarios de Reed-Muller son una familia de códigos lineales que fueron construidos y explorados por primera vez por Muller [32] en 1954. En ese mismo año, Reed describió un algoritmo de decodificación para estos códigos. Esta familia de códigos ha resultado ser de importancia práctica debido a que tanto su implementación como su decodificación son relativamente sencillas [26]. Desde el punto de vista puramente matemático, tienen relación con geometrías finitas afines y proyectivas [1].

A los códigos binarios de Reed-Muller suele llamárseles simplemente códigos de Reed-Muller y, como su nombre lo indica, están definidos sobre el campo con dos elementos $\mathbb{F}_2$. Esta construcción fue generalizada a un campo finito arbitrario $\mathbb{F}_q$ por Kasami, Lin y Peterson en 1968 [27, 28]. A la familia de códigos resultante se le conoce como códigos Reed-Muller generalizados.

Los códigos proyectivos tipo Reed-Muller fueron introducidos en 1988 por Lachaud [29]. Estos códigos se definen evaluando el espacio de polinomios homogéneos de un grado fijo $d$ en los puntos $\mathbb{F}_q$-racionales de $\mathbb{P}^n(\mathbb{F}_q)$, el espacio proyectivo $n$-dimensional sobre el campo finito con $q$ elementos $\mathbb{F}_q$. Pertenecen a la importante familia de los códigos de evaluación, a la que también pertenecen los códigos de Goppa (ver [19]).

Sörensen determinó fórmulas para la dimensión y la distancia mínima de los códigos proyectivos tipo Reed-Muller en [39], mientras que Rentería y Tapia-Recillas encontraron esas mismas fórmulas usando un enfoque distinto basado en la función de Hilbert [35]. Recientemente, el problema de determinar los pesos generalizados de Hamming para los códigos proyectivos tipo Reed-Muller ha despertado interés (ver [3, 4, 20]).

La definición original dada por Lachaud puede extenderse a subconjuntos arbitrarios $\mathcal{X}$ del espacio proyectivo $\mathbb{P}^n(\mathbb{F}_q)$. Ya se han estudiado varias instancias donde $\mathcal{X}$ es el conjunto de puntos $\mathbb{F}_q$-racionales de una variedad proyectiva definida sobre $\mathbb{F}_q$. Entre dichas instancias se cuentan el caso cuando $\mathcal{X}$ es una intersección completa en $\mathbb{P}^n(\mathbb{F}_q)$ [15], la variedad de Segre [21], una superficie cuadrática suave, una variedad torcida de Segre [13], y la variedad de Veronese [36] entre otras [8, 9, 22, 35].

En [8], Carvalho y Neumann estudiaron el caso cuando $\mathcal{X}$ es un Rollo Normal Racional (Rational Normal Scroll) generado por dos curvas normales racionales. En este trabajo estudiamos una generalización natural del problema abordado en [8] que surge cuando $\mathcal{X}$ es un Rollo Normal Racional generado por $n$ curvas normales racionales. En [24] se utiliza esta construcción generalizada del Rollo Normal Racional para construir una familia distinta de códigos lineales -usando las coordenadas de los puntos del Rollo como elementos de una matriz generadora.

En [8] se utilizan técnicas relacionadas con las bases de Gröbner y en este trabajo generalizamos dichas técnicas a nuestro caso. Las bases de Gröbner tienen su origen en la tesis doctoral de Bruno Buchberger [7]. En general, sirven para resolver problemas acerca de ideales polinomiales - es decir ideales en el anillo de polinomios de varias variables con coeficientes en un campo - de una forma algorítmica o computacional. Tienen aplicaciones en álgebra conmutativa, geometría algebraica, combinatoria, optimización, critptografía y por supuesto en teoría de códigos (ver entre otros [2, 14, 37]).

En este trabajo se entrelazan varias áreas de la matemática, a saber: teoría de códigos, álgebra conmutativa, geometría algebraica y combinatoria. El trabajo está organizado de la siguiente manera: En el Capítulo 1 se presentan los conceptos y resultados básicos de las bases de Gröbner, mismos que serán de utilidad más adelante.

En el Capítulo 2 se recuerdan conceptos básicos de teoría de códigos y se estudia cómo se pueden utilizar las bases de Gröbner para determinar los

parámetros de ciertos códigos lineales. En particular, se calculan los parámetros de los códigos Reed-Muller generalizados usando técnicas de bases de Gröbner. Cabe señalar que los parámtros de estos códigos son ya bien conocidos (ver por ejemplo [1, 27, 35]).

Una construcción del Rollo Normal Racional generalizado es presentada en el Capítulo 3. El contenido de este capítulo está basado principalmente en [25], si bien la presentación tanto de las definiciones y de los resultados es un poco distinta. Se establecen algunas propiedades básicas tanto de esta variedad algebraica como de su correspondiente ideal de anulación. Dichas propiedades resultarán ser de utilidad para estudiar los códigos construidos sobre los puntos racionales de esta variedad proyectiva.

El Capítulo 4 puede considerarse el núcleo de este trabajo. Primero recordamos cómo se definen los códigos proyectivos tipo Reed-Muller sobre los puntos racionales del Rollo Normal Racional generalizado. A continuación presentamos una construcción alternativa sugerida por la forma en la que se definió al Rollo. Usamos esta construcción adaptando algunas de las técnicas de bases de Gröbner presentadas en el Capítulo 2 para estudiar los códigos sobre el Rollo. Los resultados principales de este capítulo son los teoremas 4.4.4, 4.4.11, 4.4.12, 4.5.7, 4.5.8, 4.6.3 y el corolario 4.6.4. Todos estos resultados han sido publicados en [12].

En el apartado de conclusiones y perspectivas hacemos un recuento tanto de los avances obtenidos como de algunas metas a futuro.

El Apéndice A incluye un programa en Magma (ver [5]) con el que se pueden generar ejemplos numéricos para las construcciones de los capítulos 3 y 4.

Finalmente, el Apéndice B presenta el algoritmo de Buchberger, el cual nos dice cómo construir una base de Gröbner para cualquier ideal de un anillo de polinomios con coeficientes en un campo.

# Agradecimientos

Empezaré agradeciendo a dos instituciones que son fundamentales para el desarrollo científico de México. En primer lugar, estoy enormemente agradecido a la Universidad Autónoma Metropolitana, en particular al departamento de Matemáticas del campus Iztapalapa. Asismismo, estoy en deuda con el Consejo Nacional de Ciencia y Teconología, ya que gracias a la beca que me otorgaron - beca no. 209918- pude dedicar todas mis energías a efectuar la

investigación cuyos frutos están expuestos en este trabajo.

Agradezco enormemente a la Coordinación del Programa de posgrado del departamento de Matemáticas. El apoyo que me brindaron para hacer una estancia de investigación en Brasil resultó ser vital para la finalización de mi trabajo de investigación. Gracias también al centro de Cómputo de la UAM-I por la ayuda que me brindaron para usar una de sus supercomputadoras.

Gracias a mi director de tesis Horacio Tapia Recillas por su asesoramiento y apoyo, a Cícero Carvalho y Víctor Gonzalo López Neumann, con quienes tuve la fortuna de trabajar en la Universidade Federal de Uberlândia en Brasil. Agradezco también a Felipe Zaldívar que me dio a conocer la existencia del Rollo Normal Racional generalizado y me proporcionó bibliografía que me fue de utilidad.

Por supuesto que todo esto no hubiera sido posible sin el apoyo de mi familia: mi madre María Guadalupe, mi padre Javier, mi hermano Edgar, mi hijo Balam, mis tías Reynalda y Viola, mi abuela Lore. Les dedico esta tesis a todos ustedes.

Quiero también mencionar a toda la gente que alguna vez escucho tanto mis ideas como mis inquietudes y que me apoyó con algún consejo ya fuera a nivel técnico o humano: Elías Javier García Claro, Adolfo Torres Cházaro, Patricia Saavedra Barrera, Julio César García Corte, Rafael H. Villarreal, Manuel González Sarabia, Gabriel Villa Salvador, Martha Rzedowski, Rogelio Fernández-Alonso González, Pedro Damián Cruz Santiago.

Finalmente, gracias a la vida que me ha permitido cumplir una más de mis metas.

# Índice general

# Capítulo 1

# Fundamentos de Bases de Gröbner

La historia de la teoría de las bases de Gröbner comienza con el trabajo doctoral de Bruno Buchberger [7]. En dicho trabajo, Buchberger aborda el siguiente problema: dados un campo $k$ y un ideal $I$ en un anillo de polinomios $k[X_1, \ldots, X_n]$, encontrar una base para el anillo cociente $k[X_1, \ldots, X_n]/I$ como $k$-espacio vectorial. Para resolver dicho problema, Buchberger introduce el concepto de base de Gröbner de un ideal. El nombre lo eligió en honor a su director de tesis Wolfgang Gröbner.

Las bases de Gröbner han encontrado múltiples aplicaciones tanto en el Álgebra Conmutativa como en la Geometría Algebraica, permitiendo abordar diversos problemas desde un enfoque algorítmico o computacional (ver [2, 14]). También han encontrado aplicaciones en el área de la criptografía y en la teoría de códigos (ver por ejemplo [37]).

En este capítulo se presentan los conceptos y resultados básicos de la teoría de bases de Gröbner, mismos que serán de utilidad más adelante. El contenido está fundamentalmente basado en [10, 14]. Si el lector está interesado en profundizar más en este tema, le sugerimos revisar dichas referencias, así como [2, 37].

Uno de los objetivos de este capítulo es extender el algoritmo de la división de polinomios univariados al caso de varias variables. Una pieza clave para lograr este objetivo es el concepto de orden monomial, el cual nos permitirá ordenar los monomios de un polinomio en varias variables de una manera análoga a como ordenamos los monomios de un polinomio univariado con respecto al grado.

El siguiente paso es introducir el concepto de base de Gröbner de un ideal con respecto a un orden monomial dado. Se verá que es posible decidir si un polinomio $f$ está en un ideal $I$ dividiendo $f$ entre los elementos de una base de Gröbner para $I$ y observando el residuo: $f$ está en $I$ si y sólo si el residuo es cero.

Finalmente se introduce un concepto íntimamente relacionado con las bases de Gröbner: la huella de un ideal. Dicho concepto permite entre otras cosas determinar $k$-bases monomiales para cocientes de la forma $k[X_1, \ldots, X_n]/I$.

## 1.1. Órdenes monomiales

Sea $k$ un campo y denotemos por $k[\mathbf{X}]$ al anillo de polinomios $k[X_1, \ldots, X_n]$. Una expresión de la forma $aX_1^{\alpha_1} \cdots X_n^{\alpha_n}$, donde $a \in k^*$ y $\alpha_1, \ldots, \alpha_n \in \mathbb{N}_0$ se llama ***término***, mientras que a $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ se le denomina ***monomio***. En lo sucesivo usaremos la notación $\mathbf{X}^{\boldsymbol{\alpha}} := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, donde $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ es el ***vector de exponentes***. Denotamos por $\mathcal{M}$ al conjunto de monomios de $k[\mathbf{X}]$.

**Definición 1.1.1** Un ***orden monomial*** en $\mathcal{M}$ es una relación $\preceq$ que cumple los siguientes axiomas:

1. Es un orden total (relación reflexiva, antisimétrica y transitiva).

2. Es compatible con la multiplicación en el sentido que $\mathbf{X}^{\boldsymbol{\alpha}} \preceq \mathbf{X}^{\boldsymbol{\beta}} \implies \mathbf{X}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \preceq \mathbf{X}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$ para todo $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathbb{N}_0^n$.

3. Es un buen orden, lo cual quiere decir que cualquier subconjunto no vacío $\mathcal{A} \subset \mathcal{M}$ tiene un elemento mínimo.

Si para dos monomios $M, N$ tenemos $M \preceq N$ y $M \neq N$, entonces escribimos $M \prec N$.

**Lema 1.1.2** *Sea $\preceq$ un orden monomial y $M$ cualquier monomio. Se tiene entonces $1 = X_1^0 \cdots X_n^0 \preceq M$.*

**Prueba:** Como $\preceq$ es una relación reflexiva, se tiene $1 \preceq 1$. Ahora sea $M \neq 1$. Si se tuviera $M \prec 1$, entonces $M^{k+1} \prec M^k$ para toda $k \in \mathbb{N}$ y así el conjunto $\{M^k : k \in \mathbb{N}\}$ no tendría un elemento mínimo. $\square$

**Ejemplos 1.1.3**

1. El ***orden lexicográfico*** con $X_n \prec \cdots \prec X_1$ se define estableciendo que $\mathbf{X}^{\boldsymbol{\alpha}} \preceq_{lex} \mathbf{X}^{\boldsymbol{\beta}}$ sii $\boldsymbol{\alpha} = \boldsymbol{\beta}$ o si en la diferencia $\boldsymbol{\beta} - \boldsymbol{\alpha} \in \mathbb{Z}^n$, la primera entrada no cero de izquierda a derecha es positiva.

2. El ***orden lexicográfico graduado*** con $X_n \prec \cdots \prec X_1$ se define estableciendo que $\mathbf{X}^{\boldsymbol{\alpha}} \preceq_{grlex} \mathbf{X}^{\boldsymbol{\beta}}$ si $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ o si $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ y $\mathbf{X}^{\boldsymbol{\alpha}} \preceq_{lex} \mathbf{X}^{\boldsymbol{\beta}}$.

**Ejemplo 1.1.4** Comparemos los monomios $Y^{10}, XY^2, X^2Y \in k[X, Y]$ usando los órdenes monomiales del ejemplo anterior:

1. Usando $\preceq_{lex}$ con $Y \prec_{lex} X$, tenemos $Y^{10} \prec_{lex} XY^2 \prec_{lex} X^2Y$.

2. Usando $\preceq_{grlex}$ con $Y \prec_{grlex} X$, tenemos $XY^2 \prec_{grlex} X^2Y \prec_{grlex} Y^{10}$.

**Observación 1.1.5** Hay $n!$ órdenes lexicográficos (graduados) en $k[X_1, \ldots, X_n]$. Cada uno de ellos se corresponde con un ordenamiento $X_{i_1} \prec X_{i_2} \prec \cdots \prec X_{i_n}$ de las $n$ variables.

## 1.2. Un algoritmo de la división en $k[\mathbf{X}]$

El algoritmo de la división en el anillo de polinomios en una variable $k[X]$ nos dice que para cualesquiera polinomios $f, g \in k[X]$, $g \neq 0$, existen $q, r \in k[X]$ tales que podemos escribir:

$$f = q \cdot g + r,$$

donde el residuo $r$ o es cero o cumple $gr(r) < gr(g)$. El siguiente resultado es bastante conocido y se prueba haciendo uso del algoritmo de la división (ver por ejemplo [17]):

**Teorema 1.2.1** *El anillo $k[X]$ es un dominio de ideales principales. En otras palabras, todos los ideales de $k[X]$ son de la forma $I = (g)$ para algún $g \in k[X]$.*

Como consecuencia de este resultado, podemos saber si un polinomio $f$ pertenece a un ideal $0 \neq I = (g) \in k[X]$ usando el algoritmo de la división: $f \in (g)$ si y sólo si el residuo al dividir $f$ entre $g$ es cero.

Por otro lado, los ideales de $k[X_1, \ldots, X_n]$ no son necesariamente principales para $n > 1$, pero sí son finitamente generados, tal como lo establece el teorema de la base de Hilbert -ver por ejemplo [14]:

**Teorema 1.2.2** *Todo ideal $I \subset k[X_1, \ldots, X_n]$ tiene un conjunto finito de generadores. Dicho de otra forma, $I = (g_1, \ldots, g_s)$ para algunos $g_1, \ldots, g_s \in I$.*

Nuestra meta en este sección es presentar un algoritmo (teorema 1.2.5) que permita dividir un polinomio $f \in k[\mathbf{X}]$ entre una $s$-tupla ordenada $g_1, \ldots, g_s$ de polinomios en $k[\mathbf{X}]$. Esto quiere decir escribir $f$ en la forma

$$f = a_1 g_1 + \cdots a_s g_s + r,$$

donde los cocientes $a_1, \ldots, a_s$ y el residuo $r$ son polinomios en $k[\mathbf{X}]$.

Cuando dividimos polinomios de una variable, ordenamos los términos de los polinomios involucrados de acuerdo con el grado. De hecho, usando el lema 1.1.2 y la compatibilidad de los órdenes monomiales con el producto, vemos que el único orden monomial que existe en $k[X]$ es el dado por el grado: $1 \prec x \prec x^2 \prec \cdots$. Al dividir polinomios en varias variables también ordenamos los monomios con respecto a un orden monomial, pero en este caso se tienen muchos órdenes monomiales a elegir.

**Definiciones 1.2.3** Sea $f = \sum_{i=1}^{m} a_i M_i \in k[\mathbf{X}]$ un polinomio no cero, donde $a_i \in k$, $a_i \neq 0$, $M_i \in \mathcal{M}$ para todo $1 \leq i \leq m$ y $M_i \neq M_j$ para $i \neq j$. Sea $\preceq$ un orden monomial y $1 \leq l \leq m$ tal que $M_l$ es el monomio más grande que aparece en la expresión de $f$ con respecto a este orden monomial. A $M_l$ le llamamos el ***monomio líder*** (en inglés "leading monomial") de $f$ y lo denotamos como $lm(f)$. El ***término líder*** ("leading term") de $f$ es $lt(f) := a_l M_l$, mientras que el ***coeficiente líder*** ("leading coefficient") de $f$ es $lc(f) = a_l$.

Antes de enunciar el resultado principal de esta sección, daremos un ejemplo que nos permitirá comprenderlo mejor.

**Ejemplo 1.2.4** Dividamos $f = X^2Y + XY^2 + Y^2$ entre $g_1 = XY - 1$ y $g_2 = Y^2 - 1$. Elegimos el orden lexicográfico con $Y \prec X$. Primero observamos que los términos de todos los polinomios involucrados ya están dispuestos en orden descendente de acuerdo a $\prec$. Ahora disponemos los polinomios según el siguiente esquema gráfico:

$$\begin{array}{rll} a_1: & & r: \\ a_2: & & \\ g_1: XY-1 & |\overline{X^2Y + XY^2 + Y^2} & \to p = X^2Y + XY^2 + Y^2 \\ g_2: Y^2-1 & & \end{array}$$

Tenemos un dividendo $f = X^2Y + XY^2 + Y^2$ y dos divisores $g_1 = XY - 1$, $g_2 = Y^2 - 1$. Asociamos respectivamente un cociente a cada uno de estos divisores: $a_1$, $a_2$. Tenemos también un residuo $r$ y un dividendo parcial $p$. Inicialmente el dividendo parcial es igual a $f$.

Observamos que $lt(p) = X^2Y$ es divisible entre $lt(g_1) = XY$. Entonces, actualizamos el valor del primer cociente: $a_1 := lt(p)/lt(g_1) = X$. También actualizamos el valor del dividendo parcial: $p := p - (lt(p)/lt(g_1))g_1 = X^2Y + XY^2 + Y^2 - X \cdot (XY - 1) = XY^2 + X + Y^2$.

$$\begin{array}{rll} a_1: & X & r: \\ a_2: & & \\ g_1: XY-1 & |\overline{X^2Y + XY^2 + Y^2} & \\ g_2: Y^2-1 & & \\ & \underline{\quad X^2Y - X\quad} & \\ & XY^2 + X + Y^2 & \to p = XY^2 + Y^2 - X \end{array}$$

Ahora, $lt(p) = XY^2$ es divisible tanto por $lt(g_1) = XY$ como por $lt(g_2) = Y^2$. Sin embargo, por la manera en la que ordenamos los dividendos, $g_1$ tiene prioridad y actualizamos su cociente asociado: $a_1 := a_1 + lt(p)/lt(g_1) = X + Y$. Actualizamos el valor de $p$ de manera análoga a lo hecho en el caso anterior: $p := p - (lt(p)/lt(g_1))g_1 = X + Y^2 + Y$.

$$
\begin{array}{rcl}
a_1: & X+Y & r: \\
a_2: & & \\
g_1: XY-1 & |\overline{X^2Y+XY^2+Y^2} & \\
g_2: Y^2-1 & & \\
 & \underline{\qquad X^2Y-X} & \\
 & \overline{XY^2+X+Y^2} & \\
 & \underline{\qquad XY^2-Y} & \\
 & \overline{X+Y^2+Y} & \rightarrow p = X+Y^2+Y
\end{array}
$$

A diferencia de los pasos anteriores, vemos que $lt(p) = X$ no es divisible ni por $lt(g_1) = XY$ ni por $lt(g_2) = Y^2$. Entonces, restamos $lt(p)$ de $p$, $p := p - lt(p) = Y^2 + Y$, y lo sumamos al residuo, $r := lt(p) = X$.

$$
\begin{array}{rcl}
a_1: & X+Y & r: X \\
a_2: & & \\
g_1: XY-1 & |\overline{X^2Y+XY^2+Y^2} & \\
g_2: Y^2-1 & & \\
 & \underline{\qquad X^2Y-X} & \\
 & \overline{XY^2+X+Y^2} & \\
 & \underline{\qquad XY^2-Y} & \\
 & \overline{X+Y^2+Y} & \\
 & Y^2+Y & \rightarrow p = Y^2+Y
\end{array}
$$

En el paso siguiente, observamos que $lt(p) = Y^2$ no es divisible por $lt(g_1) = XY$ pero sí lo es por $lt(g_2) = Y^2$. Entonces actualizamos los valores de $a_2$ y $p$: $a_2 = lt(p)/lt(g_2) = 1$, $p := p - (lt(p)/lt(g_2))g_2 = Y + 1$.

$$
\begin{array}{rcl}
a_1: & X+Y & r: X \\
a_2: & 1 & \\
g_1: XY-1 & |\overline{X^2Y+XY^2+Y^2} & \\
g_2: Y^2-1 & & \\
 & \underline{\qquad X^2Y-X} & \\
 & \overline{XY^2+X+Y^2} & \\
 & \underline{\qquad XY^2-Y} & \\
 & \overline{X+Y^2+Y} & \\
 & Y^2+Y & \\
 & \underline{\qquad Y^2-1} & \\
 & \overline{Y+1} & \rightarrow p = Y+1
\end{array}
$$

Ahora $lt(p) = Y$ no es divisible ni por $lt(g_1)$ ni por $lt(g_2)$. Lo restamos de $p$ y lo sumamos al residuo para obtener $p := 1$, $r = X + Y$.

$$\begin{array}{rrll} a_1\colon & X+Y & & r\colon X+Y \\ a_2\colon & 1 & & \\ g_1\colon XY-1 & |\overline{X^2Y+XY^2+Y^2} & & \\ g_2\colon Y^2-1 & & & \\ & \underline{X^2Y-X} & & \\ & XY^2+X+Y^2 & & \\ & \underline{XY^2-Y} & & \\ & X+Y^2+Y & & \\ & Y^2+Y & & \\ & \underline{Y^2-1} & & \\ & Y+1 & & \\ & 1 & \to p=1 & \end{array}$$

Nuevamente, $lt(p) = 1$ no es divisible ni por $lt(g_1)$ ni por $lt(g_2)$. Como en el paso anterior, lo restamos de $p$ y lo sumamos al residuo obteniendo $p := 0$, $r = X + Y + 1$.

$$\begin{array}{rrll} a_1\colon & X+Y & & r\colon X+Y+1 \\ a_2\colon & 1 & & \\ g_1\colon XY-1 & |\overline{X^2Y+XY^2+Y^2} & & \\ g_2\colon Y^2-1 & & & \\ & \underline{X^2Y-X} & & \\ & XY^2+X+Y^2 & & \\ & \underline{XY^2-Y} & & \\ & X+Y^2+Y & & \\ & Y^2+Y & & \\ & \underline{Y^2-1} & & \\ & Y+1 & & \\ & 1 & & \\ & 0 & \to p=0 & \end{array}$$

Como $p = 0$, el procedimiento ha finalizado. Obtuvimos los cocientes $a_1 = X + Y$, $a_2 = 1$ y el residuo $r = X + Y + 1$, con lo que expresamos a $f$ en la forma:

$$f = a_1 g_1 + a_2 g_2 + r,$$

o bien,

$$X^2Y + XY^2 + Y^2 = (X + Y)(XY - 1) + (1)(Y^2 - 1) + X + Y + 1.$$

Este ejemplo ilustra el siguiente resultado general, cuya demostración puede ser consultada en [14]:

**Teorema 1.2.5** *Sea $\preceq$ un orden monomial en $k[\mathbf{X}]$ y sea $G = (g_1, \ldots, g_s)$ una s-tupla ordenada de polinomios. Entonces, todo polinomio $f \in k[\mathbf{X}]$ puede escribirse en la forma $f = a_1g_1 + \cdots + a_sg_s + r$, donde $a_i, r \in k[\mathbf{X}]$ y $r = 0$ o $r$ es una k-combinación lineal de monomios, ninguno de los cuales es divisible por ninguno de los $lt(g_1), \ldots, lt(g_s)$. Llamamos a los $a_1, \ldots, a_s$* **cocientes** *y a $r$ un* **residuo** *en la división de $f$ por $G$. Más aún, si $a_ig_i \neq 0$, entonces $lm(a_ig_i) \preceq lm(f)$.*

## 1.3. Definición de base de Gröbner y propiedades básicas

Ahora que ha sido presentado un algoritmo de la división en $k[X_1, \ldots, X_n]$, surge la pregunta si éste permitirá decidir si un polinomio $f$ pertenece a un ideal $I = (g_1, \ldots, g_s)$ tal como en el caso de una sola variable. Por un lado, si al dividir $f$ entre $G = (g_1, \ldots, g_s)$ se obtiene un residuo cero, es decir, si

$$f = a_1g_1 + \cdots a_sg_s,$$

con $a_i$ en $k[X_1, \ldots, X_n]$ para $i = 1, \ldots, s$, entonces es obvio que $f \in I$. Sin embargo, si obtenemos un residuo distinto de cero,

$$f = a_1g_1 + \cdots a_sg_s + r,\ r \neq 0,$$

¿podemos concluir que $f \notin I$? El siguiente ejemplo nos muestra que en general no es así.

**Ejemplo 1.3.1** Sea $k = \mathbb{R}$ y $\prec$ el orden lexicográfico con $Z \prec Y \prec X$. Si dividimos $f := X^2 + \frac{1}{2}Y^2Z - Z - 1$ entre $G := (g_1, g_2)$, donde $g_1 := X^2 + Z^2 - 1$, $g_2 := X^2 + Y^2 + (Z-1)^2 - 4$, obtenemos:

$$X^2 + \tfrac{1}{2}Y^2Z - Z - 1 = 1 \cdot (X^2 + Z^2 - 1) + 0 \cdot (X^2 + Y^2 + (Z-1)^2 - 4) + \tfrac{1}{2}Y^2Z - Z^2 - Z;$$

es decir, obtenemos como residuo $\frac{1}{2}Y^2Z - Z^2 - Z \neq 0$. Sin embargo, si dividimos $f$ entre $G' := (g_2, g_1)$, el resultado es:

$$X^2+\tfrac{1}{2}Y^2Z-Z-1=(-\tfrac{1}{2}Z+1)\cdot(X^2+Z^2-1)+\tfrac{1}{2}Z\cdot(X^2+Y^2+(Z-1)^2-4);$$

es decir, tenemos un residuo cero y concluimos que de hecho $f \in I := (g_1, g_2)$.

Este ejemplo nos muestra que en el algoritmo de la división, tanto los cocientes como el residuo dependen del orden en que se tomen los dividendos. En particular, un orden de los dividendos puede arrojar un residuo cero, mientras que un orden distinto dé como resultado un residuo distinto de cero. Esto nos motiva a introducir el siguiente concepto.

**Definición 1.3.2** Sea $I \subset k[\mathbf{X}]$ un ideal no cero y $\preceq$ un orden monomial. Un conjunto $\{g_1, \ldots, g_s\} \subset I$ es una ***base de Gröbner*** para $I$ (con respecto a $\preceq$) si para todo $0 \neq f \in I$ se tiene que $lm(g_i) \mid lm(f)$ para algún $1 \leq i \leq s$.

**Lema 1.3.3** *Sea $\{g_1, \ldots, g_s\} \subset I$ una base de Gröbner para $I$. Entonces, $f \in I$ si y sólo si el residuo en la división de $f$ por $\{g_1, \ldots, g_s\}$ es cero. Así, una base de Gröbner de $I$ es en particular una base para $I$ como ideal.*

**Prueba:** Escribamos $f = a_1g_1 + \cdots + a_sg_s + r$ usando el algoritmo de la división. Si $r = 0$, entonces $f = a_1g_1 + \cdots + a_sg_s$, donde $a_i \in k[\mathbf{X}]$ y así, $f \in I$. Ahora, sea $f \in I$. Se tiene $r = f - (a_1g_1 + \cdots + a_sg_s) \in I$. Si fuera cierto que $r \neq 0$, entonces $r$ sería un polinomio no cero en $I$ cuyo monomio líder no es divisible por $lm(g_i)$ para $i \in \{1, \ldots, s\}$, contradiciendo el hecho que $\{g_1, \ldots, g_s\} \subset I$ es una base de Gröbner para $I$. □

**Proposición 1.3.4** *Sea $\{g_1, \ldots, g_s\} \subset I$ una base de Gröbner para $I$. En la división de $f$ por $\{g_1, \ldots, g_s\}$, el residuo es el mismo, independientemente del orden que elegimos para $g_1, \ldots, g_s$ en el algoritmo de la división.*

**Prueba:** Supongamos que $f = a_1g_1 + \cdots + a_sg_s + r = a'_1g_1 + \cdots + a'_sg_s + r'$, donde $r, r'a_i, a'_i \in k[\mathbf{X}]$ para $i \in \{1, \ldots, s\}$ y ninguno de los monomios que aparecen en $r, r'$ es divisible por $lm(g_i)$ para $i \in \{1, \ldots, s\}$. Se tiene $r - r' = (a_1 - a'_1)g_1 + \cdots + (a_s - a'_s)g_s \in I$ y se debe tener $r - r' = 0$, pues de otro modo, $r - r'$ sería un polinomio no cero en $I$ cuyo monomio líder no es divisible por $lm(g_i)$ para $i \in \{1, \ldots, s\}$, contradiciendo el hecho que $\{g_1, \ldots, g_s\} \subset I$ es una base de Gröbner para $I$. □

Así pues, las bases de Gröbner se comportan muy bien cuando se usan en el algoritmo de la división. Ahora es natural plantearse la siguiente pregunta:

¿Tiene todo ideal de $k[\mathbf{X}]$ una base de Gröbner? La respuesta es afirmativa y este hecho puede demostrarse de forma constructiva usano un procedimiento conocido como algoritmo de Buchberger.

La idea básica del algoritmo de Buchberger es partir de una base cualquiera $\{g_1, ..., g_s\}$ de un ideal $I \subset k[\mathbf{X}]$. Si ésta no es una base de Gröbner, entonces es posible determinar un número finito de polinomios $g_{s+1}, ..., g_t$ tales que el conjunto $\{g_1, ..., g_s, g_{s+1}, ..., g_t\}$ es una base de Gröbner para $I$. El lector interesado puede encontrar más detalles en [2, 14] o consultar el Apéndice B de este trabajo.

## 1.4. La huella de un ideal

El siguiente concepto está íntimamente relacionado con las bases de Gröbner y será frecuentemente usado más adelante.

**Definición 1.4.1** Sea $I \subset k[\mathbf{X}]$ un ideal. La ***huella*** de $I$ (con respecto a $\preceq$) es el conjunto

$$\Delta(I) := \{M \in \mathcal{M} : M \text{ no es monomio líder de ningún polinomio en } I\}.$$

El siguiente resultado nos muestra la relación entre las bases de Gröbner y la huella de un ideal.

**Proposición 1.4.2** *Sea $I \subset k[\mathbf{X}]$ un ideal y sea $\{g_1, \ldots, g_s\}$ una base de Gröbner para $I$. Entonces, un monomio $M$ está en $\Delta(I)$ si y sólo si $M$ no es múltiplo de $lm(g_i)$ para ningún $i \in \{1, \ldots, s\}$.*

**Prueba:** Por definición de $\Delta(I)$, se tiene $M \notin \Delta(I)$ si y sólo si $M$ aparece como monomio líder de algún polinomio en $I$. Por definición de base de Gröbner, esto ocurre si y sólo si $M$ es múltiplo de algún $lm(g_i)$, $i \in \{1, \ldots, s\}$. □

El siguiente resultado es de importancia capital para las aplicaciones a la teoría de códigos.

**Teorema 1.4.3 ([10], teorema 2.14)** *Sea $I \subset k[\mathbf{X}]$ un ideal. Entonces, $\mathcal{B} := \{M + I : M \in \Delta(I)\}$ es una base para $k[\mathbf{X}]/I$ como $k$-espacio vectorial.*

**Prueba:** Sea $\mathcal{G}$ una base de Gröbner con respecto al mismo orden monomial usado para definir $\Delta(I)$ y sea $f \in k[\mathbf{X}]$. Al dividir $f$ por $\mathcal{G}$, se obtiene un residuo de la forma $r = \sum_{i=1}^{t} b_i M_i$, donde $b_i \in k$ y $M_i \in \Delta(I)$ para $i \in \{1, \ldots, t\}$. Como $f + I = r + I$, $\mathcal{B}$ genera a $k[\mathbf{X}]/I$ como $k$-espacio vectorial. Veamos que $\mathcal{B}$ es linealmente independiente. En efecto, supongamos que $\sum_{i=1}^{l} c_i M_i \in I$ con $c_i \in k$ y $M_i \in \Delta(I)$ para $i \in \{1, \ldots, l\}$. Entonces, debe tenerse $c_i = 0$ para $i \in \{1, \ldots, l\}$, pues de lo contrario $\sum_{i=1}^{l} c_i M_i$ sería un polinomio en $I$ cuyo monomio líder no es monomio líder de ningún polinomio en $I$. $\square$

# Capítulo 2

# Bases de Gröbner en Teoría de Códigos

## 2.1. Códigos lineales

En esta sección se recordarán conceptos básicos de códigos correctores de errores definidos sobre un campo finito. Para mayores detalles puede consultarse la abundante literatura sobre el tema, por ejemplo: [31, 42].

Un ***código lineal*** $q$-ario de ***longitud*** $n$ es un $\mathbb{F}_q$-subespacio vectorial $C$ de $\mathbb{F}_q^n$, donde $\mathbb{F}_q$ es el campo finito con $q$ elementos. A $\mathbb{F}_q$ se le conoce como el ***alfabeto*** del código y a los elementos de $C$ se les llama ***palabras*** del código. Si $C$ tiene dimensión $k$ sobre $\mathbb{F}_q$, entonces se dice que es un $[n, k]$-código.

Para dos vectores $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en $\mathbb{F}_q^n$, la ***distancia de Hamming*** entre $x$ e $y$ se define como

$$d(x, y) := \sharp\{i : x_i \neq y_i, 1 \leq i \leq n\}.$$

Es un hecho bien conocido que la distancia de Hamming es una métrica.

La ***distancia mínima*** de un código $C$ se define como:

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

Un código lineal $q$-ario $C$ de longitud $n$, dimensión $k$ y distancia mínima $d$ se dice que es un $[n, k, d]$-código.

## 2.2. Códigos de variedad afín

Las bases de Gröbner han sido aplicadas al estudio de ciertas familias de códigos lineales. Un ejemplo notable de esto es el caso de los códigos de variedad afín, los cuales fueron introducidos en 1998 por Fitzgerald y Lax [16]. En esta sección se recuerda la construcción de los códigos de variedad afín y se muestra cómo se utilizan las bases de Gröbner para determinar o estimar sus parámetros básicos.

### 2.2.1. Definiciones y cálculo de la dimensión

Consideremos un subconjunto $\mathcal{X} := \{P_1, \ldots, P_m\} \subset \mathbb{A}^n := \mathbb{A}^n(\mathbb{F}_q)$, el espacio afín de dimension $n$ sobre el campo finito con $q$ elementos $\mathbb{F}_q$. Sea $I_{\mathcal{X}} := \{f \in \mathbb{F}_q[\mathbf{X}] : f(P) = 0 \text{ para todo } P \in \mathcal{X}\}$ el ***ideal de anulación*** de $\mathcal{X}$.

Consideremos la ***función evaluación*** sobre $\mathcal{X}$:

$$\phi : \mathbb{F}_q[\mathbf{X}]/I_{\mathcal{X}} \to \mathbb{F}_q^m,\ f + I_{\mathcal{X}} \mapsto (f(P_1), \ldots, f(P_m)).$$

**Proposición 2.2.1 ([10], teorema 3.7)** *El mapeo $\phi$ es un isomorfismo de espacios vectoriales.*

**Prueba:** Es claro que $\phi$ es un mapeo lineal inyectivo. Dado el punto $P_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{A}^n$, sea $f_i := \prod_{j=1}^{n}(1 - (X_j - a_{ij})^{q-1})$. Resulta claro que $f_i(P_j) = \delta_{ij}$ y por consiguiente $\phi$ es suprayectiva. □

**Definición 2.2.2** Si $L \subset \mathbb{F}_q[\mathbf{X}]/I_{\mathcal{X}}$ es un $\mathbb{F}_q$-subespacio, se define $C_L := \phi(L) \subset \mathbb{F}_q^m$ como el ***código de variedad afín*** sobre $\mathcal{X}$.

Del Teorema 1.4.3 se tiene el siguiente resultado:

**Proposición 2.2.3** *El conjunto $\{M \in \Delta(I_{\mathcal{X}}) : M + I_{\mathcal{X}} \in L\}$ es una base para $L$, donde $\Delta(I_{\mathcal{X}})$ es la huella del ideal $I_{\mathcal{X}}$. En particular, $dim_{\mathbb{F}_q}(C_L) = dim(L) = |\{M \in \Delta(I_{\mathcal{X}}) : M + I_{\mathcal{X}} \in L\}|$.*

### 2.2.2. Estimación de la distancia mínima

La distancia mínima de $C_L$ es

$$d(C_L) := min\{|sop(f(P_1), \ldots, f(P_m))| : f + I_{\mathcal{X}} \in L\backslash\{0\}\},$$

donde $sop(f(P_1), \ldots, f(P_m))$ denota el soporte del vector $(f(P_1), \ldots, f(P_m))$, es decir, el conjunto de entradas no cero.

Para $f \in \mathbb{F}_q[\mathbf{X}]$ sea $I_{\mathcal{X},f} := I_{\mathcal{X}} + (f) = \{g + hf : g \in I_{\mathcal{X}}, h \in \mathbb{F}_q[\mathbf{X}]\}$, y $V(I_{\mathcal{X},f}) := \{P \in \mathcal{X} : g(P) + h(P)f(P) = 0 \text{ para todo } g + hf \in I_{\mathcal{X},f}\}$. Esto es equivalente a definir $V(I_{\mathcal{X},f}) := \{P \in \mathcal{X} : f(P) = 0\}$. El siguiente resultado se sigue directamente de las definiciones.

**Lema 2.2.4** *Para $f + I_{\mathcal{X}} \in L\backslash\{0\}$ se tiene que $d(C_L) \leq |\mathcal{X}| - |V(I_{\mathcal{X},f})|$. Más aún, $d(C_L) = min\{|\mathcal{X}| - |V(I_{\mathcal{X},f})| : f + I_{\mathcal{X}} \in L\backslash\{0\}\}$.*

**Lema 2.2.5** *Para todo $f + I_{\mathcal{X}} \in L$ se tiene $|V(I_{\mathcal{X},f})| \leq |\Delta(I_{\mathcal{X},f})|$.*

**Prueba:** Dado $f + I_{\mathcal{X}} \in L$, sea $V(I_{\mathcal{X},f}) = \{Q_1, \ldots, Q_t\}$. Usando el mismo razonamiento que en la proposición 2.2.1, existen polinomios $f_1, \ldots, f_t$ tales que $f_i(Q_j) = \delta_{ij}$, $i, j \in \{1, \ldots, t\}$. Asimismo, no es difícil checar que $\{f_i + I_{\mathcal{X},f} : 1 \leq i \leq t\}$ es un conjunto linealmente independiente en $\mathbb{F}_q[\mathbf{X}]/I_{\mathcal{X},f}$ lo cual muestra que $|V(I_{\mathcal{X},f})| \leq dim(\mathbb{F}_q[\mathbf{X}]/I_{\mathcal{X},f}) = |\Delta(I_{\mathcal{X},f})|$. □

**Definición 2.2.6** Sea $\{g_1, \ldots, g_s\}$ una base de Gröbner para $I_{\mathcal{X}}$ y $f + I_{\mathcal{X}} \in L$. La ***pseudohuella*** de $I_{\mathcal{X}}$, denotada $\Delta(\mathcal{X}, f)$, es el conjunto de monomios en $\mathbb{F}_q[\mathbf{X}]$ que no son múltiplos ni de $lm(f)$ ni de $lm(g_i)$ para $i \in \{1, \ldots, s\}$.

**Lema 2.2.7** *Para todo $f + I_{\mathcal{X}} \in L$ se tiene $\Delta(I_{\mathcal{X},f}) \subset \Delta(\mathcal{X}, f)$.*

**Prueba:** Mostraremos que dado un monomio $M$, $M \notin \Delta(\mathcal{X}, f)$ implica $M \notin \Delta(I_{\mathcal{X},f})$. La condición $M \notin \Delta(\mathcal{X}, f)$ quiere decir que $M$ es múltiplo ya sea de $lm(f)$ o de algún $lm(g_i)$, $i \in \{1, \ldots, s\}$. Si $lm(g_i)|M$, entonces $M \in I_{\mathcal{X}} \subset I_{\mathcal{X},f}$ con lo que $M \notin \Delta(I_{\mathcal{X},f})$. Si $M = h \cdot lm(f)$, se tiene $M = lm(h \cdot f) \in (f) \subset I_{\mathcal{X},f}$, con lo cual $M \notin \Delta(I_{\mathcal{X},f})$. □

**Lema 2.2.8** *Para todo $f + I_{\mathcal{X}} \in L$ se tiene $|\mathcal{X}| - |\Delta(\mathcal{X}, f)| = |\{M \in \Delta(I_{\mathcal{X}}) : lm(f)|M\}|$.*

**Prueba:** Tenemos $\Delta(\mathcal{X}, f) \subset \Delta(I_{\mathcal{X}})$ y por la proposición 2.2.1, $|\mathcal{X}| = |\Delta(I_{\mathcal{X}})|$, así que $|\mathcal{X}| - |\Delta(\mathcal{X}, f)| = |\Delta(I_{\mathcal{X}})| - |\Delta(\mathcal{X}, f)| = |\Delta(I_{\mathcal{X}}) \backslash \Delta(\mathcal{X}, f)| = |\{M \in \Delta(I_{\mathcal{X}}) : lm(f)|M\}|$. □

**Proposición 2.2.9** *Para $M \in \Delta(I_{\mathcal{X}})$, definimos*

$$\delta(M) := |\{N \in \Delta(I_{\mathcal{X}}) : M|N\}|.$$

*Se tiene entonces la siguiente cota inferior para la distancia mínima:*

$$d(C_L) \geq min(\{\delta(M) : M \in \Delta(I_{\mathcal{X}})\}).$$

**Prueba:** Del lema 2.2.4 sabemos que para algún $f + I_{\mathcal{X}} \in L \backslash \{0\}$ se cumple $d(C_L) = |\mathcal{X}| - |V(I_{\mathcal{X},f})|$. Usando los tres lemas anteriores se tiene

$$\begin{aligned} |\mathcal{X}| - |V(I_{\mathcal{X},f})| &\geq |\mathcal{X}| - |\Delta(I_{\mathcal{X},f})| \geq \\ |\mathcal{X}| - |\Delta(\mathcal{X}, f)| &= |\{M \in \Delta(I_{\mathcal{X}}) : lm(f)|M\}|, \end{aligned}$$

para todo $f + I_{\mathcal{X}} \in L \backslash 0$. Si $lm(f) \in I_{\mathcal{X}}$, entonces $(f - lm(f)) + I_{\mathcal{X}} = f + I_{\mathcal{X}}$. Por la proposición 2.2.3, el conjunto $\{M \in \Delta(I_{\mathcal{X}}) : M + I_{\mathcal{X}} \in L\}$ es una base para $L$ como $\mathbb{F}_q$-espacio vectorial. Por lo tanto, podemos suponer sin pérdida de generalidad que $f$ es una combinación lineal de monomios en $\Delta(I_{\mathcal{X}})$, así que en particular $lm(f) \in \Delta(I_{\mathcal{X}})$. □

**Corolario 2.2.10** *Sea $M^* \in \Delta(I_{\mathcal{X}})$ tal que*

$$\delta(M^*) = min(\{\delta(M) : M \in \Delta(I_{\mathcal{X}})\}).$$

*Si existe un $f + I_{\mathcal{X}} \neq 0 + I_{\mathcal{X}}$ tal que $lm(f) = M^*$ y $\{f, g_1, \ldots, g_s\}$ es una base de Gröbner para $I_{\mathcal{X},f}$, entonces $d(C_L) = \delta(M^*)$.*

## 2.3. Códigos Reed-Muller generalizados

Los códigos Reed-Muller generalizados fueron introducidos por Kasami, Lin y Peterson en 1968 (ver [27]) y forman parte de la familia de códigos de evaluación. En 1997, Rentería y Tapia-Recillas usaron técnicas de álgebra conmutativa para obtener de una manera alternativa sus parámetros [35].

Estos códigos pertenecen a la familia de los códigos de variedad afín. En la presente sección aplicaremos las técnicas de bases de Gröbner descritas en la sección anterior al estudio de los códigos Reed-Muller generalizados obteniendo resultados ya conocidos (ver[1, 27, 35]). Esto nos permitirá familiarizarnos con la forma en la que se usan las bases de Gröbner en la teoría de códigos.

En el caso que nos ocupa tenemos $\mathcal{X} = \mathbb{A}^n$ y

$$L = \{f + I_{\mathbb{A}^n} : f \in \mathbb{F}_q[\mathbf{X}], f = 0 \text{ o } deg(f) \leq d\}.$$

Llamamos a $C_{\mathbb{A}^n}(d) := C_L$ el ***código de Reed-Muller*** de orden $d$. Con $\prec$ denotaremos al orden monomial lexicográfico dado por $X_1 \prec \cdots \prec X_n$. Necesitamos el siguiente resultado:

**Lema 2.3.1 ([35], proposición 1 y observación 1)** *El conjunto*

$$\{X_i^q - X_i : 1 \leq i \leq n\}$$

*es una base de Gröbner para $I_{\mathbb{A}^n}$ con respecto a $\prec$.*

Observemos que de acuerdo con la proposición 1.4.2,

$$\Delta_{\succ}(I_{\mathbb{A}^n}) := \Delta(I_{\mathbb{A}^n}) = \{X_1^{\alpha_1} \cdots X_n^{\alpha_n} : 0 \leq \alpha_i < q \text{ para } 1 \leq i \leq n\}.$$

**Teorema 2.3.2 ([1], teorema 5.5; [35], proposición 5)**
*La dimensión de $C_{\mathbb{A}^n}(d)$ es* $\displaystyle\sum_{i=0}^{n}(-1)^i\binom{n}{i}\binom{n+d-iq}{d-iq}$.

**Prueba:** El conjunto $\{M + I_{\mathbb{A}^n} : M \in \Delta(I_{\mathbb{A}^n}) \text{ y } deg(M) \leq d\}$ es una base para $C_{\mathbb{A}^n}(d)$ como $\mathbb{F}_q$-espacio vectorial.

Ahora bien, los monomios $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \Delta(I_{\mathbb{A}^n})$ con $\displaystyle\sum_{i=0}^{n}\alpha_i = j$ se corresponden con las soluciones enteras a la ecuación

$$\alpha_1 + \cdots + \alpha_n = j$$

con las restricciones $0 \leq \alpha_i < q$ para $1 \leq i \leq n$. A su vez, el número de soluciones a esta ecuación con las restricciones dadas es el coeficiente de grado $j$ de

$$(1+X+\cdots+X^{q-1})^n = \left(\frac{1-X^q}{1-X}\right)^n =$$

$$(1-X^q)^n \cdot \frac{1}{(1-X)^n} = \left[\sum_{i=0}^{n}(-1)^i\binom{n}{i}X^{iq}\right]\left[\sum_{k=0}^{\infty}\binom{k+n-1}{k}X^k\right],$$

el cual es $\sum_{i=0}^{n}(-1)^i\binom{n}{i}\binom{n+j-iq-1}{j-iq}$. Sumando esta expresión desde $j=0$ hasta $j=d$ obtenemos:

$$\sum_{j=0}^{d}\sum_{i=0}^{n}(-1)^i\binom{n}{i}\binom{n+j-iq-1}{j-iq} = \sum_{i=0}^{n}\sum_{j=0}^{d}(-1)^i\binom{n}{i}\binom{n+j-iq-1}{j-iq} =$$

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i}\sum_{j=iq}^{d}\binom{n+j-iq-1}{j-iq}.$$

Efectuando los cambios de variables $l := j-iq$, $r = d-iq$, la expresión $\sum_{j=iq}^{d}\binom{n+j-iq-1}{j-iq}$ se transforma en $\sum_{l=0}^{r}\binom{n+l-1}{l}$. Haciendo uso de la identidad binomial $\binom{n+r}{r} = \sum_{l=0}^{r}\binom{n+l-1}{l}$ y regresando a las variables originales obtenemos:

$$\sum_{j=iq}^{d}\binom{n+j-iq-1}{j-iq} = \binom{n+d-iq}{d-iq}.$$

□

El siguiente resultado -que es un caso espeial del lema 3.5 en [10]- será útil para determinar la distancia mínima:

**Lema 2.3.3** *Sea* $d = k(q-1)+l < n(q-1)$ *con* $0 \leq k < n$, $0 \leq l < q-1$. *Entonces*

$$min\left\{\prod_{i=1}^{n}(q-\alpha_i) : 0 \leq \alpha_i < q \text{ para } 1 \leq i \leq n, \sum_{i=0}^{n}\alpha_i \leq d\right\} = (q-l)q^{n-k-1}.$$

**Prueba:** Para empezar, sea $\alpha = (\alpha_1, \ldots, \alpha_n)$ y supongamos que $\sum_{i=0}^{n}\alpha_i < d$. Debe tenerse $0 \leq \alpha_{i_1} < q-1$ para algún $1 \leq i_1 \leq n$. Se define $\alpha' = (\alpha'_1, \ldots, \alpha'_n)$, donde $\alpha'_{i_1} = \alpha_{i_1}+1 < q$ y $\alpha'_i = \alpha_i$ para $1 \leq i \leq n$, $i \neq i_1$. Se tiene $\sum_{i=0}^{n}\alpha'_i \leq d$ y $\prod_{i=1}^{n}(q-\alpha_i) - \prod_{i=1}^{n}(q-\alpha'_i) = \prod_{i=1, i\neq i_1}^{n}(q-\alpha_i)(q-\alpha_{i_1}-q+\alpha_{i_1}+1) > 0$. De esta manera, el mínimo debe obtenerse cuando $\sum_{i=0}^{n}\alpha_i = d$.

Sea $\alpha = (\alpha_1, \ldots, \alpha_n)$ tal que $\sum_{i=0}^{n}\alpha_i = d$ y supongamos que $\alpha_{i_1} < q-1$ para algún $i_1 \in \{1, \ldots, k\}$. Entonces, existe un $i_2 \in \{k+1, \ldots, n\}$ tal que $\alpha_{i_2} > 0$. Hay dos casos:

1. $\alpha_{i_1} + \alpha_{i_2} \leq q-1$. En este caso, se define $\alpha' = (\alpha'_1, \ldots, \alpha'_n)$ con $\alpha'_{i_1} = \alpha_{i_1} + \alpha_{i_2}$, $\alpha'_{i_2} = 0$ y $\alpha'_i = \alpha_i$ para $1 \leq i \leq n$, $i \neq i_1, i_2$. Así $\sum_{i=0}^{n}\alpha'_i = d$ y $\prod_{i=1}^{n}(q-\alpha_i) - \prod_{i=1}^{n}(q-\alpha'_i) = (\alpha_{i_1}\alpha_{i_2})\prod_{i=1, i\neq i_1, i_2}^{n}(q-\alpha_i) \geq 0$.

2. $\alpha_{i_1} + \alpha_{i_2} > q-1$. En este caso, definimos $\alpha' = (\alpha'_1, \ldots, \alpha'_n)$ con $\alpha'_{i_1} = q-1$, $\alpha'_{i_2} = \alpha_{i_2} - (q-1-\alpha_{i_1})$ y $\alpha'_i = \alpha_i$ para $1 \leq i \leq n$, $i \neq i_1, i_2$. Así, $\sum_{i=0}^{n}\alpha'_i = d$ y

$$\prod_{i=1}^{n}(q-\alpha_i) - \prod_{i=1}^{n}(q-\alpha'_i) = (q-1-\alpha_{i_1})(q-1-\alpha_{i_2})\prod_{i=1, i\neq i_1, i_2}^{n}(q-\alpha_i) \geq 0.$$

De esta manera, puede suponerse también que $\alpha_i = q-1$ para todo $i \in \{1, \ldots, k\}$. Supongamos ahora que $0 < \alpha_{k+1} < l$. Existe $i_1 \in \{k+2, \ldots, l\}$ tal que $\alpha_{i_1} > 0$. Se define $\alpha' = (\alpha'_1, \ldots, \alpha'_n)$, donde ,$\alpha'_{k+1} = \alpha_{k+1}+\alpha_{i_1}$, $\alpha'_{i_1} = 0$

y $\alpha'_i = \alpha_i$ para $1 \leq i \leq n$, $i \neq k+1, i_1$. Así, $\prod_{i=1}^{n}(q-\alpha_i) - \prod_{i=1}^{n}(q-\alpha'_i) = (\alpha_{k+1}\alpha_{i_1}) \prod_{i=1, i\neq i_1, i_2}^{n}(q-\alpha_i) > 0$.

Ha quedado probado que el mínimo se obtiene con el vector

$$\alpha = (\alpha_1, \ldots, \alpha_n) = (q-1, \ldots, q-1, l, 0, \ldots, 0).$$

Para este vector se tiene

$$\prod_{i=1}^{n}(q-\alpha_i) = (q-l)q^{n-k-1}.$$

□

**Teorema 2.3.4 ([1], corolario 5.26; [27], teorema 5)** *La distancia mínima de $C_{\mathbb{A}^n}(d)$ es*

$$d(C_{\mathbb{A}^n}(d)) := (q-l)q^{n-k-1},$$

*donde $d = k(q-1)+l < n(q-1)$ con $0 \leq k < n$, $0 \leq l < q-1$.*

**Prueba:** Si $M = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \Delta(I_{\mathbb{A}^n})$, entonces $N \in \Delta(I_{\mathbb{A}^n})$ y $M|N$ si y sólo si $N = X_1^{\beta_1} \cdots X_n^{\beta_n}$ con $\alpha_i \leq \beta_i < q$ para $1 \leq i \leq n$. Así, $\delta(M) = \prod_{i=1}^{n}(q-\alpha_i)$. De acuerdo con la proposición 2.2.9, se tiene

$$d(C_{\mathbb{A}^n}(d)) \geq min\{\delta(M) : M \in \Delta(I_{\mathbb{A}^n})\} =$$
$$min\left\{\prod_{i=1}^{n}(q-\alpha_i) : 0 \leq \alpha_i < q \text{ para } 1 \leq i \leq n, \sum_{i=0}^{n}\alpha_i \leq d\right\} = (q-l)q^{n-k-1}.$$

Sea $\mathbb{F}_q^* = \{a_1, \ldots, a_{q-1}\}$ y consideremos el polinomio

$$G := \left(\prod_{i=1}^{k}(X_i^{q-1}-1)\right)\prod_{j=1}^{l}(X_{k+1}-a_j).$$

El grado de $G$ es $k(q-1)+l = d$ y $G$ tiene $q^n - (q-l)q^{n-k-1}$ raíces en $\mathbb{A}^n$. Usando el lema 2.2.4 se tiene $d(C_{\mathbb{A}^n}(d)) \leq |\mathbb{A}^n| - V(I_{\mathbb{A}^n,G}) = (q-l)q^{n-k-1}$. □

Lo expuesto en esta sección ilustra el uso de las bases de Gröbner -en particular la relación entre las bases de Gröbner y la huella de un ideal- para determinar los parámetros de los códigos Reed-Muller generalizados.

Como vimos, los códigos generalizados de Reed-Muller pertenecen a la familia de códigos de variedad afín. La construcción que hemos estudiado puede ser generalizada para variedades proyectivas para obtener los códigos proyectivos tipo Reed-Muller. Ya han sido estudiadas varias instancias de estos códigos -ver por ejemplo [8, 9, 13, 15, 21, 22, 29, 35]. En el capítulo 4 recordamos la definición general de los códigos proyectivos tipo Reed-Muller y la aplicamos al caso particular del Rollo normal racional generalizado -la variedad algebraica proyectiva que juega un papel medular en este trabajo.

# Capítulo 3

# El Rollo Normal Racional

## 3.1. Caracterización geométrica

En este capítulo presentamos una construcción geométrica del Rollo Normal Racional -Rational Normal Scroll en inglés- definido sobre un campo finito $\mathbb{F}_q$ como unión ajena de subespacios de un espacio proyectivo. Para mayores referencias sobre las construcciones y resultados de este capítulo remitimos al lector a [25, 24].

Sea $e \geq 1$ un entero. Una *curva normal racional de grado e* es la imagen de la función

$$\begin{array}{rccl} v_e\colon & \mathbb{P}^1(\mathbb{F}_q) & \to & \mathbb{P}^e(\mathbb{F}_q) \\ & (x_0 : x_1) & \mapsto & (x_0^e : x_0^{e-1}x_1 : \cdots : x_0x_1^{e-1} : x_1^e)\ . \end{array}$$

Sean $e_0 \geq e_1 \geq e_2 \geq \ldots \geq e_n \geq 1$ enteros, y sea

$$\ell = (e_0 + 1) + (e_1 + 1) + \ldots + (e_n + 1) - 1 = \sum_{i=0}^{n} e_i + n.$$

Denotaremos los puntos de $\mathbb{P}^\ell(\mathbb{F}_q)$ en la forma

$$(x_{0,0} : \cdots : x_{0,e_0} : x_{1,0} : \cdots : x_{1,e_1} : \cdots : x_{n,0} : \cdots : x_{n,e_n}).$$

Para $i \in \{0, \ldots, n\}$, el conjunto de puntos tales que $x_{s,t} = 0$ para todo $s \in \{0, \ldots, n\} \setminus \{i\}$ y todo $t \in \{0, \ldots, e_s\}$ es un subespacio lineal de $\mathbb{P}^\ell(\mathbb{F}_q)$ de dimensión $e_i$ al que denotaremos por $\mathbb{P}^{e_i}$. La imagen de la función

$$\begin{array}{rccl} u_i\colon & \mathbb{P}^1(\mathbb{F}_q) & \to & \mathbb{P}^{e_i} \subset \mathbb{P}^\ell(\mathbb{F}_q) \\ & (b_0 : b_1) & \mapsto & (0 : \cdots : 0 : b_0^{e_i} : b_0^{e_i-1}b_1 : \cdots : b_1^{e_i} : 0 \cdots : 0) \end{array}$$

es una curva normal racional de grado $e_i$. Para cada $(b_0 : b_1) \in \mathbb{P}^1(\mathbb{F}_q)$, sea $L_{(b_0:b_1)}$ el subespacio lineal de $\mathbb{P}^\ell(\mathbb{F}_q)$ generado por los puntos $u_0(b_0 : b_1), \ldots, u_n(b_0 : b_1)$. En otras palabras, $L_{(b_0:b_1)}$ es el conjunto de puntos de la forma

$$(a_0 b_0^{e_0} : a_0 b_0^{e_0-1} b_1 : \cdots : a_0 b_1^{e_0} : \cdots : a_n b_0^{e_n} : a_n b_0^{e_n-1} b_1 : \cdots : a_n b_1^{e_n}),$$

donde $(a_0 : \cdots : a_n) \in \mathbb{P}^n(\mathbb{F}_q)$.

**Definición 3.1.1** El ***Rollo Normal Racional*** de tipo $e_0, \ldots, e_n$ es el conjunto [25, 24]

$$S_{e_0,\ldots,e_n} := \bigcup_{(b_0:b_1)\in\mathbb{P}^1} L_{(b_0:b_1)} \subset \mathbb{P}^\ell(\mathbb{F}_q).$$

La construcción para el Rollo Normal Racional mostrada en [8] es un caso particular de esta construcción tomando $n = 1$. De ahora en adelante fijaremos a los enteros $e_0, \ldots, e_n$ y denotaremos a $S_{e_0,\ldots,e_n}$ como $S$. El siguiente resultado nos permitirá contar los puntos $\mathbb{F}_q$-racionales de $S$.

**Proposición 3.1.2** *Si $(b_0 : b_1)$ y $(\tilde{b}_0 : \tilde{b}_1)$ son puntos distintos de $\mathbb{P}^1(\mathbb{F}_q)$, entonces $L_{(b_0:b_1)}$ y $L_{(\tilde{b}_0:\tilde{b}_1)}$ son subespacios ajenos.*

**Prueba:** Supongamos que existen $(a_0 : \cdots : a_n), (\tilde{a}_0 : \cdots : \tilde{a}_n) \in \mathbb{P}^n(\mathbb{F}_q)$ tales que

$$\begin{aligned}(a_0 b_0^{e_0} :& a_0 b_0^{e_0-1} b_1 : \cdots : a_0 b_1^{e_0} : \cdots : a_n b_0^{e_n} : a_n b_0^{e_n-1} b_1 : \cdots : a_n b_1^{e_n}) = \\ & (\tilde{a}_0 \tilde{b}_0^{e_0} : \tilde{a}_0 \tilde{b}_0^{e_0-1} \tilde{b}_1 : \cdots : \tilde{a}_0 \tilde{b}_1^{e_0} : \cdots : \tilde{a}_n \tilde{b}_0^{e_n} : \tilde{a}_n \tilde{b}_0^{e_n-1} \tilde{b}_1 : \cdots : \tilde{a}_n \tilde{b}_1^{e_n}).\end{aligned}$$

Sea $j$ el menor subíndice tal que $a_j \neq 0$. Supongamos primero que $b_0 \neq 0$. Así, la primera entrada no cero de izquierda a derecha en la primera expresión es $a_j b_0^{e_j}$ en la posición $(j, 0)$. Entonces, la primera entrada no cero de izquierda a derecha en la segunda expresión es $\tilde{a}_j \tilde{b}_0^{e_j}$. Por lo tanto $\tilde{a}_j \neq 0$ y podemos tomar el cociente entre las entradas $(j, 1)$ y $(j, 0)$ para obtener

$$\frac{a_j b_0^{e_j-1} b_1}{a_j b_0^{e_j}} = \frac{\tilde{a}_j \tilde{b}_0^{e_j-1} \tilde{b}_1}{\tilde{a}_j \tilde{b}_0^{e_j}}.$$

Por lo tanto, concluimos que $b_1/b_0 = \tilde{b}_1/\tilde{b}_0$.

Ahora supongamos que $b_0 = 0$. Entonces, la primera entrada no cero de izquierda a derecha en la primera expresión es $a_j b_1^{e_j}$ en la posición $(j, e_j)$. La primera entrada no cero de izquierda a derecha en la segunda expresión ocurre en la misma posición y es $\tilde{a}_j \tilde{b}_1^{e_j}$. Por otro lado, debemos tener $\tilde{a}_j \tilde{b}_0^{e_j} = 0$, lo que implica que $\tilde{b}_0 = 0$. □

**Corolario 3.1.3** *$S$ es la unión disjunta de $(q+1)$ subespacios lineales de dimensión $n$ y $|S| = (q^n + \cdots + q + 1)(q+1)$.*

**Prueba:** Para todo $(b_0 : b_1) \in \mathbb{P}^1(\mathbb{F}_q)$, los puntos en el conjunto $\{u_0(b_0 : b_1), \ldots, u_n(b_0 : b_1)\}$ están en subespacios lineales de $\mathbb{P}^\ell(\mathbb{F}_q)$ mutuamente ajenos. Entonces este conjunto es linealmente independiente y genera un subespacio $L_{(b_0:b_1)}$ de dimensión $n$ que contiene $q^n + \cdots + q + 1 = |\mathbb{P}^n(\mathbb{F}_q)|$ puntos. Tenemos $q + 1 = |\mathbb{P}^1(\mathbb{F}_q)|$ de estos espacios que de acuerdo a la proposición anterior son mutuamente ajenos. □

## 3.2. El Rollo como variedad algebraica

En esta sección presentamos a $S$ como el conjunto de puntos racionales de una variedad proyectiva.

**Teorema 3.2.1** *Sea $G \subset \mathbb{F}_q[X_{0,0}, \ldots, X_{0,e_0}, \ldots, X_{n,0}, \ldots, X_{n,e_n}]$ el conjunto de menores $2 \times 2$ de la matriz*

$$\mathcal{M} := \begin{pmatrix} X_{0,0} & \ldots & X_{0,e_0-1} & X_{1,0} & \ldots & X_{1,e_1-1} & \ldots & X_{n,0} & \ldots & X_{n,e_n-1} \\ X_{0,1} & \ldots & X_{0,e_0} & X_{1,1} & \ldots & X_{1,e_1} & \ldots & X_{n,1} & \ldots & X_{n,e_n} \end{pmatrix},$$

*y sea $I$ el ideal generado por $G$. $S$ está formado por los ceros en $\mathbb{P}^l(\mathbb{F}_q)$ de $I$.*

**Prueba:** Los menores de $\mathcal{M}$ son los binomios de la forma

$$X_{i,j}X_{k,l} - X_{i,j+1}X_{k,l-1}$$

con $0 \leq i \leq k \leq n$, $0 \leq j \leq e_i - 1$, $0 \leq l \leq e_k$, $j < l - 1$ si $i = k$.

Por otro lado, los puntos de $S$ son de la forma

$$(a_0 b_0^{e_0} : a_0 b_0^{e_0-1} b_1 : \cdots : a_0 b_1^{e_0} : \cdots : a_n b_0^{e_n} : a_n b_0^{e_n-1} b_1 : \cdots : a_n b_1^{e_n})$$

con $(a_0, \ldots, a_n) \in \mathbb{F}_q^{n+1} \backslash \{0\}$, $(b_0, b_1) \in \mathbb{F}_q^2 \backslash \{0\}$. Sustituyendo las coordenadas de un punto de S en cualquiera de los polinomios de $G$ obtenemos

$$(a_i b_0^{e_i - j} b_1^j)(a_k b_0^{e_k - l} b_1^l) - (a_i b_0^{e_i - j - 1} b_1^{j+1})(a_k b_0^{e_k - l + 1} b_1^{l-1}) =$$

$$a_i a_k b_0^{e_i + e_k - j - l} b_1^{j+l} - a_i a_k b_0^{e_i + e_k - j - l} b_1^{j+l} = 0,$$

así que todos los puntos de $S$ son ceros de $I$.

Ahora consideremos un punto

$$P = (x_{0,0}, \ldots, x_{0,e_0}, \ldots, x_{n,0}, \ldots, x_{n,e_n}) \in \mathbb{P}^l(\mathbb{F}_q)$$

que anule a todos los polinomios de $G$. Sea $x_{i,s}$ la primera entrada no cero de izquierda a derecha en $P$. Consideramos dos casos.

1. $s = 0$. Entonces $x_{i,0} \neq 0$ y la igualdad:

   $$x_{i,0} x_{i,j} = x_{i,1} x_{i,j-1}, \text{ o bien}$$

   $$x_{i,j} = b_1 x_{i,j-1}$$

   se cumple para $1 < j \leq e_i$, donde sin pérdida de generalidad suponemos que $x_{i,0} = 1$ y hacemos la definición $b_1 := x_{i,1}$. Resulta así que $x_{i,1} = b_1$, $x_{i,2} = b_1^2$ y en general $x_{i,j} = b_1^j$ para $1 \leq j \leq e_i$. Por otro lado, para $i < k \leq n$, $1 \leq l \leq e_k$ se cumple

   $$x_{i,0} x_{k,l} = x_{k,l-1} x_{i,1}.$$

   Si definimos $a_k := x_{k,0}$, se tiene $x_{k,1} = a_k b_1$, $x_{k,2} = a_k b_1^2$ y en general $x_{k,l} = a_k b_1^l$ para $1 \leq l \leq e_k$. Así, en este caso $P$ tiene la forma

   $$(0 : \cdots : 0 : 1 : b_1 : \cdots : b_1^{e_i} : \cdots : a_n : a_n b_1 : \cdots : a_n b_1^{e_n}).$$

2. $s > 0$. Entonces $x_{i,0} = 0$ y como las relaciones

   $$x_{i,j} x_{i,j+2} = x_{i,j+1}^2$$

se cumplen para $0 \leq j < e_i - 1$, se tiene $x_{i,j} = 0$ para $0 \leq j \leq e_i - 1$. De esta forma, concluimos que $s = e_i$, $x_{i,e_i} \neq 0$ y sin pérdida de generalidad, asumimos que $x_{i,e_i} = 1$.

Ahora, como $P$ cumple las relaciones

$$x_{i,e_{i-1}} x_{k,l} = x_{i,e_i} x_{k,l-1}$$

para $i < k \leq n$, $0 < l \leq e_k$, concluimos que $x_{k,0} = x_{k,1} = \cdots = x_{k,e_k-1} = 0$ para $i < k \leq n$. Si definimos $a_k := x_{k,e_k}$ para $i < k \leq n$, se concluye que $P$ tiene la forma:

$$(0 : \cdots : 0 : 1 : 0 \cdots : 0 : a_{i+1} : \cdots : 0 : \cdots : 0 : a_n).$$

□

**Proposición 3.2.2** *Sea $\succ$ el orden lexicográfico en los monomios de $\mathbb{F}_q[\mathbf{X}]$, donde*

$$X_{0,0} \succ X_{0,1} \succ \cdots \succ X_{0,e_0} \succ X_{1,0} \succ \cdots \succ X_{1,e_1} \succ \cdots \succ X_{n,0} \succ \cdots X_{n,e_n}.$$

*El conjunto $G$ del teorema 3.2.1 es una base de Gröbner para $I$ con respecto a $\succ$.*

**Prueba:** Definimos

$$g_{(s,t),(u,v)} := X_{s,t} X_{u,v} - X_{s,t+1} X_{u,v-1}$$

para $s, u \in \{0, \ldots, n\}$, $t \in \{0, \ldots, e_s - 1\}$, $v \in \{1, \ldots, e_u\}$ con $s < u$ o $s = u$ y $t+1 < v$. Sean $g_{(s,t),(u,v)}, g_{(i,j),(k,l)} \in G$. Observemos que sus monomios líderes son respectivamente $X_{s,t}X_{u,v}$ y $X_{i,j}X_{k,l}$. De acuerdo con el teorema B.0.8 y la proposición B.0.11, para probar que $G$ es una base de Gröbner para $I$, es suficiente probar que si los monomios líderes de $g_{(s,t),(u,v)}$ y $g_{(i,j),(k,l)}$ no son coprimos, entonces su $S$-polinomio puede escribirse en la forma $a_1 g_1 + \cdots + a_m g_m$, donde $a_i \in \mathbb{F}_q[\mathbf{X}]$, $g_i \in G$ y el monomio líder de $a_i g_i$ es menor o igual que el polinomio líder del $S$-polinomio para todo $i = 1, \ldots, m$.

Supongamos que $X_{s,t} < X_{i,j}$. Entonces, para que $X_{s,t}X_{u,v}$ y $X_{i,j}X_{k,l}$ sean no coprimos debe tenerse ya sea $X_{u,v} = X_{i,j}$ o $X_{u,v} = X_{k,l}$ . Si $X_{u,v} = X_{i,j}$,

entonces

$$\begin{aligned} S(g_{(s,t),(u,v)}, g_{(u,v),(k,l)}) =& X_{k,l}\ g_{(s,t),(u,v)} - X_{s,t}\ g_{(u,v),(k,l)} \\ =& - X_{k,l}X_{s,t+1}X_{u,v-1} + X_{s,t}X_{u,v+1}X_{k,l-1} \\ = -X_{s,t+1}(X_{u,v-1}X_{k,l} - & X_{u,v}X_{k,l-1}) + X_{k,l-1}(X_{s,t}X_{u,v+1} - X_{s,t+1}X_{u,v}) \\ =& - X_{s,t+1}g_{(u,v-1),(k,l)} + X_{k,l-1}g_{(s,t),(u,v+1)}. \end{aligned}$$

Si $X_{u,v} = X_{k,l}$, entonces

$$\begin{aligned} S(g_{(s,t),(u,v)}, g_{(i,j),(u,v)}) =& X_{i,j}\ g_{(s,t),(u,v)} - X_{s,t}\ g_{(i,j),(u,v)} \\ =& X_{s,t}X_{i,j+1}X_{u,v-1} - X_{i,j}X_{s,t+1}X_{u,v-1} \\ =& X_{u,v-1}g_{(s,t),(i,j+1)}. \end{aligned}$$

Supongamos ahora que $X_{s,t} = X_{i,j}$ y también, sin pérdida de generalidad, supongamos que $X_{u,v} > X_{k,l}$. Entonces

$$S(g_{(s,t),(u,v)}, g_{(s,t),(k,l)}) = -X_{s,t+1}(X_{u,v-1}X_{k,l} - X_{u,v}X_{k,l-1}).$$

De $X_{u,v} > X_{k,l}$ se sigue que $u < k$ o $u = k$ y $v < l$, así que en cualquier caso $S(g_{(s,t),(u,v)}, g_{(s,t),(k,l)}) = -X_{s,t+1}g_{(u,v-1),(k,l)}$. Queda probada la proposición. □

# Capítulo 4

# Códigos proyectivos tipo Reed-Muller sobre el Rollo Normal Racional

Este es el capítulo más importante del presente trabajo, ya que aquí se presentan nuestras aportaciones originales. Recordamos la construcción general de los códigos proyectivos tipo Reed-Muller y la aplicamos al Rollo Normal Racional introducido en el capítulo anterior. Obtenemos un conjunto de expresiones que nos permiten determinar la dimensión de estos códigos, así como fórmulas para la distancia mínima en un caso particular. Se recuperan los resultados de [8] al sustituir $n = 1$ en las ecuaciones que deduciremos a continuación. Cabe mencionar que los resultados principales de este capítulo han sido publicados en [12].

## 4.1. Construcción general

Sea $\mathbb{F}_q[\mathbf{X}] := \mathbb{F}_q[X_0, \ldots, X_n]$ el anillo de polinomios en $n+1$ variables sobre $\mathbb{F}_q$. Consideramos a $\mathbb{F}_q[\mathbf{X}]$ con la graduación natural y denotamos por $\mathbb{F}_q[\mathbf{X}]_d$ su componente de grado $d$, la cual es un $\mathbb{F}_q$-espacio vectorial. Sea $\mathbb{P}^n := \mathbb{P}^n(\mathbb{F}_q)$ el espacio proyectivo $n$-dimensional sobre $\mathbb{F}_q$ y $\mathcal{X} = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n$. Escribimos las coordenadas de estos puntos en la ***forma estándar***, es decir, la primera coordenada distinta de cero es igual a 1.

Para $d \geq 0$, definimos la ***función evaluación*** siguiente:

$$\begin{array}{rccc} ev_d: & \mathbb{F}_q[X]_d & \to & \mathbb{F}_q^m \\ & f & \mapsto & (f(P_1), \ldots, f(P_m)) \end{array}.$$

Resulta claro que $ev_d$ es una función $\mathbb{F}_q$-lineal. Con esta notación, el ***código proyectivo tipo Reed-Muller*** de orden $d$ sobre el conjunto $\mathcal{X}$, denotado como $C_{\mathcal{X}}(d)$, se define como la imagen del mapeo $ev_d$.

Consideramos el ***Ideal de Anulación*** de $\mathcal{X}$, definido como

$$I_{\mathcal{X}} := (\{f \in \mathbb{F}_q[\mathbf{X}] : f \text{ es homogéneo y } f(P) = 0 \text{ para todo } P \in \mathcal{X}\}).$$

$I_{\mathcal{X}}$ es un ideal homogéneo y su componente de grado $d$ es $I_{\mathcal{X}}(d) := I_{\mathcal{X}} \cap \mathbb{F}_q[\mathbf{X}]_d$. Entonces $ker(ev_d) = I_{\mathcal{X}}(d)$ y así $C_{\mathcal{X}}(d) \simeq \mathbb{F}_q[\mathbf{X}]_d / I_{\mathcal{X}}(d)$.

Esta construcción funciona para un subconjunto $\mathcal{X} \subseteq \mathbb{P}^n$ arbitrario, sin embargo es preferible que $\mathcal{X}$ esté formado por los puntos racionales de alguna variedad algebraica, ya que esta estructura permite estudiar con mayor facilidad los códigos construidos. Algunos ejemplos de instancias particulares de esta construcción los encontramos en [15, 21, 22, 29, 36, 35, 39].

## 4.2. Construcción sobre $\mathbb{P}^m(\mathbb{F}_q)$

En [29, 35, 39] se estudió el caso cuando $\mathcal{X} := \mathbb{P}^m(\mathbb{F}_q)$, el espacio proyectivo total, que como es bien sabido, tiene $N_m := q^m + q^{m-1} + \cdots + 1$ puntos $\mathbb{F}_q$-racionales, digamos $P_1, \ldots, P_{N_m}$. Aquí repasamos de manera breve algunos resultados referentes a estos códigos que usaremos más adelante.

Para dos enteros positivos $d, m$, se define el código proyectivo Reed-Muller de orden $d$ sobre $\mathbb{P}^m(\mathbb{F}_q)$ como la imagen del mapeo evaluación

$$\begin{array}{rccc} ev_{d,m}: & \mathbb{F}_q[Y_0, \ldots, Y_m]_d & \to & \mathbb{F}_q^{N_m} \\ & f & \mapsto & (f(P_1), \ldots, f(P_{N_m})), \end{array}$$

a la que denotamos como $\mathrm{PRM}(d, m)$. El siguiente resultado nos da información básica con respecto a este código:

**Teorema 4.2.1** *[35, 39] Si $d \geq m(q-1)$, el mapeo $ev_{d,m}$ es suprayectivo y $\mathrm{PRM}(d, m) = \mathbb{F}_q^{N_m}$. Si $1 \leq d \leq m(q-1)$, la dimensión y la distancia mínima*

$\delta_{\mathrm{PRM}}(d,m)$ *de* $\mathrm{PRM}(d,m)$ *están dadas respectivamente por las expresiones:*

$$\dim(\mathrm{PRM}(d,m)) = \sum_{j=0}^{m}\sum_{i=0}^{j}(-1)^i\binom{j}{i}\binom{j+d-1-iq}{d-1-iq}$$

$$\delta_{\mathrm{PRM}}(d,m) = (q-r)q^{m-k-1}$$

*donde* $d-1 = k(q-1)+r$ *y* $0 \leq r < q-1$.

*En la fórmula para la dimensión asumimos que* $\binom{a}{b} = 0$ *si* $b < 0$, *por lo que si* $d \leq q$, *entonces*

$$\dim(\mathrm{PRM}(d,m)) = \sum_{j=0}^{m}\binom{j+d-1}{d-1} = \binom{d+m}{d}.$$

En [35] se muestra que el conjunto $\{Y_i^q Y_j - Y_i Y_j^q \,:\, 0 \leq i < j \leq m\}$ es una base de Gröbner para el ideal de anulación de $\mathbb{P}^m(\mathbb{F}_q)$ -al que denotaremos como $I_m$- con respecto al orden lexicográfico donde $Y_m \prec \cdots \prec Y_0$ .

Sabemos por el teorema 1.4.3 que las clases laterales de los elementos de $\Delta(I_m)$ en $\mathbb{F}_q[Y_0,\ldots,Y_m]/I_m$ forman una base para este $\mathbb{F}_q$-espacio. Por la proposición 1.4.2, sabemos que el conjunto $\Delta(I_m)$ está formado por todos los monomios que no son múltiplos de ninguno de los monomios líderes de los generadores de $I_m$. El siguiente resultado se sigue inmediatamente de esta discusión.

**Lema 4.2.2** *Los monomios de* $\Delta(I_m)$ *son de la forma* $Y_0^{\beta_0}\cdots Y_j^{\beta_j}$, *donde* $j \in \{0,\ldots,m\}$, $\beta_j \neq 0$, $\beta_i = 0$ *si* $i > j$ *y* $0 \leq \beta_i \leq q-1$ *si* $0 \leq i < j$. *Además, las clases laterales de los elementos del conjunto*

$$\Delta(I_m)_d := \{Y_0^{\beta_0}\cdots Y_m^{\beta_m} \in \Delta(I_m) \,:\, \deg(Y_0^{\beta_0}\cdots Y_n^{\beta_m}) = d\}$$

*forman una base para el cociente* $\mathbb{F}_q[Y_0,\ldots,Y_m]_d/I_m(d)$ *como* $\mathbb{F}_q$*-espacio, donde* $I_m(d)$ *es la componente homogénea de grado* $d$ *del ideal graduado* $I_m$.

De este resultado se desprende que la dimensión del código proyectivo tipo Reed-Muller $\mathrm{PRM}(d,m)$ puede obtenerse contando los elementos de $\Delta(I_m)_d$. Los autores de [35] calcularon la dimensión de $\mathrm{PRM}(d,m)$ usando funciones de Hilbert. Por supuesto que ambos métodos arrojan el mismo resultado.

## 4.3. Construcción sobre el Rollo Normal Racional generalizado

Ahora construimos códigos proyectivos tipo Reed-Muller sobre los puntos $\mathbb{F}_q$-racionales del Rollo Normal Racional generalizado $S$ que fue introducido en el capítulo 3. Sea $N := (q^n + \cdots + q + 1)(q + 1)$ y sean $P_1, \ldots, P_N$ los puntos $\mathbb{F}_q$-racionales de $S$. Escribimos

$$\mathbb{F}_q[\mathbf{X}] := \mathbb{F}_q[X_{0,0}, \ldots, X_{0,e_0}, X_{1,0}, \ldots, X_{1,e_1}, \ldots, X_{n,0}, \ldots, X_{n,e_n}].$$

**Definición 4.3.1** Consideramos el mapeo evaluación

$$\begin{array}{rccc} ev_d: & \mathbb{F}_q[\mathbf{X}]_d & \to & \mathbb{F}_q^N \\ & f & \mapsto & (f(P_1), \ldots, f(P_N)) \end{array},$$

donde hemos escrito los puntos del Rollo en notación estándar. El código correspondiente, denotado por $C_S(d)$, es el *código proyectivo tipo Reed-Muller sobre* $S$.

Sea $I_S$ el ideal de anulación de $S$; es decir, el ideal de $\mathbb{F}_q[\mathbf{X}]$ generado por todos los polinomios homogéneos que se anulan en $S$. Denotamos la componente de grado $d$ de $I_S$ como $I_S(d)$. Claramente $C_S(d)$ es isomorfo a $\mathbb{F}_q[\mathbf{X}]_d/I_S(d)$ como $\mathbb{F}_q$-espacio vectorial.

**Observación 4.3.2** Se tiene $I \subsetneq I_S$, donde $I$ es el ideal generado por los menores de la matriz $\mathcal{M}$ definida en el teorema 3.2.1.

**Prueba:** En primer lugar, resulta claro que $I \subset I_S$. Por otro lado, si consideramos el binomio $X_{0,0}^q X_{1,0} - X_{0,0} X_{1,0}^q$, es claro que este se anula en todos los puntos de $\mathbb{P}^\ell(\mathbb{F}_q)$. Su monomio líder con respecto al orden monomial usado en la proposición 3.2.2 es $X_{0,0}^q X_{1,0}$. Ahora, como $X_{0,0}$ y $X_{1,0}$ aparecen únicamente en el primer renglón de $\mathcal{M}$, puede verse que este monomio no es múltiplo del monomio líder de ningún polinomio de $G$ -la base de Gröbner de la proposición 3.2.2. De esta manera, $X_{0,0}^q X_{1,0} - X_{0,0} X_{1,0}^q$ no pertenece a $I$. □

## 4.4. Una Construcción alternativa del código $C_S(d)$

Tal como acabamos de observar, el ideal $I$ está contenido propiamente en el ideal $I_S$. En lugar de determinar $I_S$ o $I_S(d)$, generalizaremos las ideas presentadas en [8] para determinar un cociente que es isomorfo a $\mathbb{F}_q[\mathbf{X}]_d/I_S(d)$, y de esta manera se calculará la dimensión de $C_S(d)$.

De acuerdo con el capítulo 3, los puntos $\mathbb{F}_q$-racionales del Rollo Normal Racional tienen la forma

$$(a_0b_0^{e_0} : a_0b_0^{e_0-1}b_1 : \cdots : a_0b_1^{e_0} : \cdots : a_nb_0^{e_n} : a_nb_0^{e_n-1}b_1 : \cdots : a_nb_1^{e_n})$$

con $(a_0, \ldots, a_n) \in \mathbb{F}_q^{n+1}\backslash\{0\}$, $(b_0, b_1) \in \mathbb{F}_q^2\backslash\{0\}$.

Esto nos motiva a definir un morfismo de álgebras

$$\psi\colon \mathbb{F}_q[\mathbf{X}] \to \mathbb{F}_q[Y_0, \ldots, Y_n, Z_0, Z_1],$$

el cual lleva $X_{i,j}$ hacia $Y_iZ_0^{e_i-j}Z_1^j$ para todo $i \in \{0, \ldots, n\}$ y $j \in \{0, \ldots, e_i\}$, donde los $e_i$'s son los enteros no negativos que se usaron en la construcción del Rollo.

Escribiremos $\mathbb{F}_q[\mathbf{Y}, \mathbf{Z}]$ para referirnos a $\mathbb{F}_q[Y_0, \ldots, Y_n, Z_0, Z_1]$. El siguiente lema muestra el efecto de $\psi$ al actuar sobre un monomio arbitrario de $\mathbb{F}_q[\mathbf{X}]$.

**Lema 4.4.1** *Sea $X_{0,0}^{\alpha_{0,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}} \in \mathbb{F}_q[\mathbf{X}]_d$ un monomio de grado $d$ y sea $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ su imagen bajo $\psi$. Entonces:*

1. $\beta_i = \sum_{j=0}^{e_i} \alpha_{i,j}$ *para todo* $0 \leq i \leq n$.
2. $\sum_{i=0}^{n} \beta_i = d$.
3. $\gamma_0 = \sum_{i=0}^{n} \sum_{j=0}^{e_i} (e_i - j)\alpha_{i,j}$.
4. $\gamma_1 = \sum_{i=0}^{n} \sum_{j=0}^{e_i} j\alpha_{i,j}$.
5. $\gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i\beta_i$.

**Prueba:** Por la definición de $\psi$, tenemos

$$\psi(\mathbf{X}^\alpha) = (Y_0Z_0^{e_0})^{\alpha_{0,0}} \cdots (Y_0Z_1^{e_0})^{\alpha_{0,e_0}} \cdots (Y_nZ_0^{e_n})^{\alpha_{0,e_n}} \cdots (Y_nZ_1^{e_n})^{\alpha_{n,e_n}}.$$

Es posible escribir esta expresión en la forma

$$Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1},$$

donde

$$\begin{aligned} \beta_i &:= \alpha_{i,0} + \ldots + \alpha_{i,e_i}, \\ \gamma_0 &:= \sum_{j=0}^{e_0} (e_0 - j)\alpha_{0,j} + \ldots + \sum_{j=0}^{e_n} (e_n - j)\alpha_{n,j}, \\ \gamma_1 &:= \sum_{j=0}^{e_0} j\alpha_{0,j} + \ldots + \sum_{j=0}^{e_n} j\alpha_{n,j}. \end{aligned}$$

Así que se tiene

$$\textstyle\sum_{i=0}^{n} \beta_i = \sum_{i=0}^{n} \sum_{j=0}^{e_i} \alpha_{i,j} = deg(\mathbf{X}^{\alpha}) = d$$

y también

$$\gamma_0 + \gamma_1 = \textstyle\sum_{i=0}^{n} \sum_{j=0}^{e_i} (e_i - j)\alpha_{i,j} + \sum_{i=0}^{n} \sum_{j=0}^{e_i} j\alpha_{i,j} = \sum_{i=0}^{n} (e_i \sum_{j=0}^{e_i} \alpha_{i,j}).$$

Por la parte 1, la última expresión es equivalente a $\sum_{i=0}^{n} e_i\beta_i$.

□

Definimos el álgebra $\mathcal{B} := \psi(\mathbb{F}_q[\mathbf{X}]) \subset \mathbb{F}_q[\mathbf{Y}, \mathbf{Z}]$ y el grado de un monomio $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \mathcal{B}$ como $\sum_{i=0}^{n} \beta_i$. De esta manera $\mathcal{B}$ se convierte en un álgebra graduada cuya componente de grado $d$ es $\mathcal{B}_d = \psi(\mathbb{F}_q[\mathbf{X}]_d)$ y $\psi$ es un morfismo graduado de álgebras.

**Proposición 4.4.2** *$\mathcal{B}_d$ is es un $\mathbb{F}_q$-espacio vectorial de dimensión finita y el conjunto*

$$M_d := \{Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \mathbb{F}_q[\mathbf{Y}, \mathbf{Z}] : \sum_{i=0}^{n} \beta_i = d, \gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i\beta_i\}$$

*es una base.*

**Prueba:** Del lema anterior se sigue que $\mathcal{B}_d$ está en el espacio generado por $M_d$. Para probar la otra inclusión, sean $\beta_0, \ldots, \beta_n$ enteros no negativos tales que $\sum_{i=0}^{n} \beta_i = d$. Es suficiente probar que cualquier monomio de la forma $Y_0^{\beta_0} \ldots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ con $\gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i\beta_i$ es un elemento de $\mathcal{B}_d$. Usaremos un argumento inductivo sobre $\gamma_0$ para probar esto.

Si $\gamma_0 = 0$, entonces

$$\psi(X_{0,e_0}^{\beta_0} X_{1,e_1}^{\beta_1} \cdots X_{n,e_n}^{\beta_n}) = Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^0 Z_1^{\sum_{i=0}^{n} e_i\beta_i} \in \mathcal{B}_d.$$

Supongamos ahora que dados $0 \leq \gamma_0 < \sum_{i=0}^{n} e_i\beta_i$ y enteros no negativos $\beta_0, \ldots, \beta_n$ tales que $\sum_{i=0}^{n} \beta_i = d$, existe un monomio

$$X_{0,0}^{\alpha_{0,0}} \cdots X_{0,e_0}^{\alpha_{0,e_0}} \cdots X_{n,0}^{\alpha_{n,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}},$$

tal que

$$\psi(X_{0,0}^{\alpha_{0,0}} \cdots X_{0,e_0}^{\alpha_{0,e_0}} \cdots X_{n,0}^{\alpha_{n,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}}) = Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1},$$

donde $\gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i\beta_i$. Se tiene $\gamma_1 > 0$, así que $\alpha_{k,l} > 0$ para algún $1 \leq l \leq e_k$ y algún $0 \leq k \leq n$. Ahora se define $\widetilde{\alpha}_{k,l-1} = \alpha_{k,l-1} + 1$, $\widetilde{\alpha}_{k,l} = \alpha_{k,l} - 1$ y $\widetilde{\alpha}_{i,j} = \alpha_{i,j}$ si

$(i,j) \neq (k,l-1), (k,l)$. De las relaciones del lema 4.4.1 se sigue que

$$\psi(X_{0,0}^{\widetilde{\alpha}_{0,0}} \cdots X_{0,e_0}^{\widetilde{\alpha}_{0,e_0}} \cdots X_{n,0}^{\widetilde{\alpha}_{n,0}} \cdots X_{n,e_n}^{\widetilde{\alpha}_{n,e_n}}) = Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0+1} Z_1^{\gamma_1-1},$$

lo cual completa la prueba. □

**Corolario 4.4.3** *El conjunto*

$$M := \{Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \mathbb{F}_q[\mathbf{Y}, \mathbf{Z}] : \gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i\beta_i\}$$

*es una base para $\mathcal{B}$ como $\mathbb{F}_q$-espacio vectorial.*

Por el corolario 3.1.3, sabemos que el producto cartesiano $\mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ y $S$ tienen el mismo número de puntos racionales. La construcción de $S$ y

la proposición 3.1.2, nos sugieren una biyección $\varphi\colon \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q) \to S$ definida por

$$\varphi((a_0 : \cdots : a_n), (b_0 : b_1)) = \\ (a_0 b_0^{e_0} : a_0 b_0^{e_0-1} b_1 : \cdots : a_0 b_1^{e_0} : \cdots : a_n b_0^{e_n} : a_n b_0^{e_n-1} b_1 : \cdots : a_n b_1^{e_n}),$$

donde escribimos los puntos de $\mathbb{P}^n(\mathbb{F}_q)$ y $\mathbb{P}^1(\mathbb{F}_q)$ en notación estándar.

Para $1 \leq i \leq N$, definamos $Q_i := \varphi^{-1}(P_i)$, donde $\{P_1, \ldots, P_N\}$ es el conjunto de puntos $\mathbb{F}_q$-racionales de $S$ que usamos para definir $C_S(d)$. Consideremos ahora la siguiente evaluación $\mathbb{F}_q$-lineal sobre $\mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$:

$$\begin{array}{rccc} \widetilde{ev}_d : & \mathcal{B}_d & \to & \mathbb{F}_q^N \\ & f & \mapsto & (f(Q_1), \ldots, f(Q_N)), \end{array}$$

donde la evaluación del monomio $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ se define como

$$Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}((a_0 : \cdots : a_n), (b_0 : b_1)) = a_0^{\beta_0} \cdots a_n^{\beta_n} b_0^{\gamma_0} b_1^{\gamma_1}.$$

**Teorema 4.4.4** *El diagrama*

$$\begin{array}{ccc} \mathbb{F}_q[\mathbf{X}]_d & \xrightarrow{\psi} & \mathcal{B}_d \\ & \searrow^{ev_d} & \swarrow_{\widetilde{ev}_d} \\ & \mathbb{F}_q^N & \end{array}$$

*conmuta y la imagen de $\widetilde{ev}_d$ es $C_S(d)$.*

**Prueba:** Sea $Q = ((a_0 : \cdots : a_n), (b_0 : b_1)) \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$ (donde los puntos están escritos en notación estándar) y sea $P = \varphi(Q)$ (escrito también en notación estándar). Sea $\mathbf{X}^{\boldsymbol{\alpha}} = X_{0,0}^{\alpha_{0,0}} \cdots X_{0,e_0}^{\alpha_{0,e_0}} \cdots X_{n,0}^{\alpha_{n,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}} \in \mathbb{F}_q[\mathbf{X}]_d$ un monomio de grado $d$. Entonces

$$\begin{aligned} \mathbf{X}^{\boldsymbol{\alpha}}(P) =& (a_0 b_0^{e_0})^{\alpha_{0,0}} \cdots (a_0 b_1^{e_0})^{\alpha_{0,e_0}} \cdots (a_n b_0^{e_n})^{\alpha_{n,0}} \cdots (a_n b_1^{e_n})^{\alpha_{n,e_n}} \\ =& a_0^{\beta_0} \cdots a_n^{\beta_n} b_0^{\gamma_0} b_1^{\gamma_1}, \end{aligned}$$

donde $\beta_i = \sum_{j=0}^{e_i} \alpha_{i,j}$ para todo $0 \leq i \leq n$, $\sum_{i=0}^{n} \beta_i = d$, $\gamma_0 = \sum_{i=0}^{n} \sum_{j=0}^{e_i} (e_i - j)\alpha_{i,j}$, y $\gamma_1 = \sum_{i=0}^{n} \sum_{j=0}^{e_i} j\alpha_{i,j}$. De esta forma el monomio $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ está en $\mathcal{B}_d$ y

$$a_0^{\beta_0} \cdots a_n^{\beta_n} b_0^{\gamma_0} b_1^{\gamma_1} = Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}(Q) = \psi(\mathbf{X}^{\boldsymbol{\alpha}})(Q).$$

Esto prueba que el diagrama conmuta. Como $\psi$ es suprayectiva, las imágenes de $ev_d$ y $\widetilde{ev}_d$ son iguales. □

Definamos $J_d := ker(\widetilde{ev}_d)$. Una consecuencia del resultado anterior es

$$\mathbb{F}_q[\mathbb{X}]_d/I_S(d) \simeq C_S(d) \simeq \mathcal{B}_d/J_d,$$

y $\psi^{-1}(J_d) = I_S(d)$. De este manera, estudiar el código $\widetilde{ev}_d(\mathcal{B}_d)$ es equivalente a estudiar $C_S(d)$. En particular, es posible determinar la dimensión de $C_S(d)$ contando los elementos en una base para $\mathcal{B}_d/J_d$. Es claro que las clases de los monomios de $M_d$ en $\mathcal{B}_d/J_d$ son un conjunto generador para $\mathcal{B}_d/J_d$.

**Definición 4.4.5** Sea $\widetilde{J}_d$ el $\mathbb{F}_q$-subespacio vectorial de $\mathcal{B}_d$ generado por los binomios del tipo

$$Y_0^{\beta_0}\cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} - Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1},$$

donde $Y_0^{\beta_0}\cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}, Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1} \in M_d$, y para todo $i \in \{0,\ldots,n\}$,

$$\begin{array}{l} \beta_i \equiv \tilde{\beta}_i \pmod{q-1},\ \ \gamma_i \equiv \tilde{\gamma}_i \pmod{q-1}, \\ \beta_i = 0 \iff \tilde{\beta}_i = 0,\ \ \gamma_i = 0 \iff \tilde{\gamma}_i = 0. \end{array}$$

La motivación para esta definición es que los monomios que aparecen restándose tienen la misma evaluación en todos los puntos del producto cartesiano $\mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$.

Claramente $\widetilde{J}_d \subset J_d$, y más adelante se mostrará que de hecho se cumple la igualdad. Definimos un orden monomial en los elementos del conjunto $M_d$ estableciendo que

$$Y_0^{\beta_0}\cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \prec Y_0^{\overline{\beta}_0}\cdots Y_n^{\overline{\beta}_n} Z_0^{\overline{\gamma}_0} Z_1^{\overline{\gamma}_1},$$

si la primera entrada no cero de izquierda a derecha en $(\beta_0 - \overline{\beta}_0, \ldots, \beta_n - \overline{\beta}_n, \gamma_0 - \overline{\gamma}_0)$ es negativa.

En lo sucesivo, denotaremos la clase de un monomio $Y_0^{\beta_0}\cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ en el espacio cociente $\mathcal{B}_d/\widetilde{J}_d$ como $[Y_0^{\beta_0}\cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}]$.

**Lema 4.4.6** *Sea* $Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1} \in \mathcal{B}_d$ *y* $j := max\{0 \leq i \leq n : \beta_i \neq 0\}$. *El monomio mínimo con respecto a* $\prec$ *en* $[Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}]$ *es* $Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n}Z_0^{\tilde{\gamma}_0}Z_1^{\tilde{\gamma}_1}$, *donde*

$$\tilde{\beta}_i = \begin{cases} 0 & si\ \beta_i = 0, i \in \{0,\ldots,n\}, \\ a\ con\ \ 1 \leq a \leq q-1,\ a \equiv \beta_i\ (\text{mód } q-1) & si\ \ 0 \leq i < j\ y\ \beta_i \neq 0, \\ d - \sum_{s=0}^{j-1} \tilde{\beta}_s & si\ i = j, \end{cases}$$

$$\tilde{\gamma}_0 = \begin{cases} 0 & si\ \gamma_0 = 0, \\ b\ con\ \ 1 \leq b \leq q-1, b \equiv \gamma_0\ (\text{mód } q-1) & si\ 0 < \gamma_0 < \sum_{i=0}^{j} \beta_i e_i, \\ \sum_{i=0}^{j} \tilde{\beta}_i e_i & si\ \gamma_0 = \sum_{i=0}^{j} \beta_i e_i, \end{cases}$$

$$\tilde{\gamma}_1 := \sum_{i=0}^{j} \tilde{\beta}_i e_i - \tilde{\gamma}_0.$$

**Prueba:** De las definiciones de $\tilde{\beta}_0,\ldots,\tilde{\beta}_n$, $\tilde{\gamma}_0$ y $\tilde{\gamma}_1$, se sigue que el monomio $Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n}Z_0^{\tilde{\gamma}_0}Z_1^{\tilde{\gamma}_1}$ está en $\mathcal{B}_d$ y

$$Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1} - Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n}Z_0^{\tilde{\gamma}_0}Z_1^{\tilde{\gamma}_1} \in \widetilde{J}_d.$$

Resulta claro también que $\tilde{\beta}_i = 0$ para $j+1 \leq i \leq n$, ya que $\beta_i = 0$ para $i \geq j+1$. Más aún, el valor de $\tilde{\beta}_i$ es el menor posible para $0 \leq i \leq j-1$. Así, si $Y_0^{\delta_0}\cdots Y_n^{\delta_n}Z_0^{\theta_0}Z_1^{\theta_1} \in [Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}]$ y $\delta_i > \tilde{\beta}_i$ para algún $i \in \{0,\ldots,j-1\}$, entonces

$$Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n}Z_0^{\tilde{\gamma}_0}Z_1^{\tilde{\gamma}_1} \prec Y_0^{\delta_0}\cdots Y_n^{\delta_n}Z_0^{\theta_0}Z_1^{\theta_1}.$$

Si $\delta_i = \tilde{\beta}_i$ para $i \in \{0,\ldots,j-1\}$, notemos que $\delta_i = 0$ para $i \in \{j+1,\ldots,n\}$ y $\delta_j = d - \sum_{s=0}^{j-1}\tilde{\beta}_s = \tilde{\beta}_j$. Como $\tilde{\gamma}_0$ tiene también el mínimo valor posible, se tiene

$$Y_0^{\tilde{\beta}_0}\cdots Y_n^{\tilde{\beta}_n}Z_0^{\tilde{\gamma}_0}Z_1^{\tilde{\gamma}_1} \preceq Y_0^{\delta_0}\cdots Y_n^{\delta_n}Z_0^{\theta_0}Z_1^{\theta_1},$$

lo cual termina la prueba. □

De acuerdo con el teorema 1.4.3, una $\mathbb{F}_q$-base para un anillo cociente de la forma $\mathbb{F}_q[\mathbf{X}]/I$ está dada por las clases laterales de los monomios en la huella $\Delta(I)$ con respecto a algún orden monomial. Por otro lado, los monomios en $\Delta(I)$ son precisamente aquellos que no aparecen como monomios líderes de ningún polinomio en el ideal $I$. Esta idea permite traducir el problema de determinar la dimensión de los códigos de variedad afín a un problema de conteo de monomios.

Adaptaremos la técnica que se usó con los códigos de variedad afín al caso en consideración. Por la forma en la que fue definido $\widetilde{J}_d$, los monomios de $M_d$ que no aparecen como monomios líderes de ningún polinomio en $\widetilde{J}_d$ son precisamente aquellos que son mínimos dentro de su clase lateral. Esto nos motiva a dar la siguiente definición.

**Definición 4.4.7** Sea $\Delta(\mathcal{B})_d$ el conjunto de monomios $Y_0^{\beta_0}\cdots Y_j^{\beta_j}Z_0^{\gamma_0}Z_1^{\gamma_1} \in \mathcal{B}_d$ tales que $Y_0^{\beta_0}\cdots Y_j^{\beta_j}Z_0^{\gamma_0}Z_1^{\gamma_1}$ es el elemento mínimo de $[Y_0^{\beta_0}\cdots Y_j^{\beta_j}Z_0^{\gamma_0}Z_1^{\gamma_1}]$.

**Definición 4.4.8** Definimos el ***peso*** de un vector $\boldsymbol{\beta} = (\beta_0, \ldots, \beta_n) \in \mathbb{N}_0^{n+1}$ como

$$\rho(\beta_0, \ldots, \beta_n) := \textstyle\sum_{i=0}^{n} e_i\beta_i,$$

donde los $e_i$'s son los enteros no negativos que se usaron en la construcción del Rollo.

**Lema 4.4.9** *Los elementos de $\Delta(\mathcal{B})_d$ son exactamente los monomios de la forma $Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}$ con $Y_0^{\beta_0}\cdots Y_n^{\beta_n} \in \Delta(I_n)_d$ y $Z_0^{\gamma_0}Z_1^{\gamma_1} \in \Delta(I_1)_{\rho(\beta_0,\ldots,\beta_n)}$.*

**Prueba:** Es una consecuencia directa de los lemas 4.2.2 y 4.4.6. □

**Proposición 4.4.10** *Sea $h$ una $\mathbb{F}_q$-combinación lineal de elementos de $\Delta(\mathcal{B})_d$ tal que $h(Q) = 0$ para todo $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. Entonces $h = 0$.*

**Prueba:** Escribamos $\boldsymbol{\beta} = (\beta_0, \ldots, \beta_n)$, $\boldsymbol{\gamma} = (\gamma_0, \gamma_1)$ y $\mathbf{Y}^{\boldsymbol{\beta}} = Y_0^{\beta_0}\cdots Y_n^{\beta_n}$, $\mathbf{Z}^{\boldsymbol{\gamma}} = Z_0^{\gamma_0}Z_1^{\gamma_1}$. Sea

$$h = \sum_{\mathbf{Y}^{\boldsymbol{\beta}}\mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(\mathcal{B})_d} c_{(\boldsymbol{\beta};\boldsymbol{\gamma})}\mathbf{Y}^{\boldsymbol{\beta}}\mathbf{Z}^{\boldsymbol{\gamma}}$$

una $\mathbb{F}_q$-combinación lineal de elementos de $\Delta(\mathcal{B})_d$ tal que $h(Q) = 0$ para todo $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$, y sea $(b_0 : b_1) \in \mathbb{P}^1(\mathbb{F}_q)$. Entonces el polinomio

$$h_{(b_0:b_1)} := \sum_{\mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d} \left( \sum_{\substack{\boldsymbol{\gamma} \text{ tal que} \\ \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{\rho(\boldsymbol{\beta})}}} c_{(\boldsymbol{\beta};\boldsymbol{\gamma})} b_0^{\gamma_0} b_1^{\gamma_1} \right) \mathbf{Y}^{\boldsymbol{\beta}}$$

se anula en todos los puntos de $\mathbb{P}^n(\mathbb{F}_q)$. Esto quiere decir que $h_{(b_0:b_1)}$ es un elemento de $I_n(d)$. Como es una $\mathbb{F}_q$-combinación lineal de elementos de $\Delta(I_n)_d$ y $\Delta(I_n)_d$ es una base para el cociente $\mathbb{F}_q[Y_0, \ldots, Y_n]/I_n(d)$, se sigue que para todo $\boldsymbol{\beta}$ tal que $\mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d$, el polinomio

$$\sum_{\substack{\boldsymbol{\gamma} \text{ tal que} \\ \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{\rho(\boldsymbol{\beta})}}} c_{(\boldsymbol{\beta};\boldsymbol{\gamma})} Z_0^{\gamma_0} Z_1^{\gamma_1}$$

se anula en todos los puntos de $\mathbb{P}^1(\mathbb{F}_q)$. Este polinomio es entonces un elemento de $I_1(d)$ y es una $\mathbb{F}_q$-combinación lineal de elementos de $\Delta(I_1)_{\rho(\boldsymbol{\beta})}$. Concluimos que $c_{(\boldsymbol{\beta};\boldsymbol{\gamma})} = 0$ siempre que $\mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{\rho(\boldsymbol{\beta})}$ y $\mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d$, o equivalentemente, siempre que $\mathbf{Y}^{\boldsymbol{\beta}}\mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(\mathcal{B})_d$. Hemos así probado que $h = 0$. □

Las dos proposiciones siguientes son consecuencias importantes de este resultado.

**Teorema 4.4.11** $J_d = \widetilde{J}_d$.

**Prueba:** Se tiene claramente la inclusión $\widetilde{J}_d \subset J_d$. Observemos que dado un polinomio $g \in J_d$, existe un polinomio $\widetilde{g}$ en el $\mathbb{F}_q$-espacio $\langle \Delta(\mathcal{B})_d \rangle$ generado por $\Delta(\mathcal{B})_d$ tal que $g - \widetilde{g} \in \widetilde{J}_d$. Entonces $g(Q) = \widetilde{g}(Q)$ para todo $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$, así que $\widetilde{g}(Q) = 0$ para todo $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. Por el resultado anterior tenemos entonces $\widetilde{g} = 0$, por lo cual $g \in \widetilde{J}_d$. □

**Teorema 4.4.12** *Las clases laterales de los monomios de $\Delta(\mathcal{B})_d$ en $B_d/J_d$ forman una base para $B_d/J_d$ como $\mathbb{F}_q$-espacio vectorial.*

**Prueba:** Obviamente, las clases de los monomios de $\Delta(\mathcal{B})_d$ generan a $B_d/J_d$ como $\mathbb{F}_q$-espacio vectorial. Por la proposición 4.4.10, el conjunto formado por estas clases es linealmente independiente. □

## 4.5. La Dimensión de $C_S(d)$

Sabemos por la última proposición de la sección anterior que $\dim C_S(d) = |\Delta(\mathcal{B})_d|$. En esta sección se presentan algunas fórmulas que permiten calcular $|\Delta(\mathcal{B})_d|$. Por el lema 4.4.9, los elementos de $\Delta(\mathcal{B})_d$ son exactamente los monomios de la forma $Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}$ con $Y_0^{\beta_0}\cdots Y_n^{\beta_n} \in \Delta(I_n)_d$ y $Z_0^{\gamma_0}Z_1^{\gamma_1} \in \Delta(I_1)_{\rho(\beta_0,\ldots,\beta_n)}$. Para $j \in \{0,\ldots,n\}$, definimos

$$\Delta(\mathcal{B})_{d,j} := \{Y_0^{\beta_0}\cdots Y_j^{\beta_j}Z_0^{\gamma_0}Z_1^{\gamma_1} \in \Delta(\mathcal{B})_d \mid \beta_j > 0\}.$$

El siguiente resultado es inmediato y es nuestro primer paso para calcular la dimensión:

**Lema 4.5.1** $|\Delta(\mathcal{B})_d| = \sum_{j=0}^{n} |\Delta(\mathcal{B})_{d,j}|$.

A continuación derivaremos una expresión que nos permita calcular $|\Delta(\mathcal{B})_{d,j}|$ para $0 \leq j \leq n$. Si $\sum_{i=0}^{j}\beta_i = d$, entonces

$$\sum_{i=0}^{j} e_i\beta_i = \sum_{i=0}^{j-1} e_i\beta_i + e_j\left(d - \sum_{i=0}^{j-1}\beta_i\right) = \sum_{i=0}^{j-1} m_{i,j}\beta_i + e_j d, \qquad (4.1)$$

donde hemos definido $m_{i,j} := e_i - e_j$ para $0 \leq i \leq j \leq n$, y $\sum_{i=0}^{-1} m_{i,0}\beta_i := 0$.

**Lema 4.5.2** *Para $j \in \{0,\ldots,n\}$ se tiene*

$$max\{\sum_{i=0}^{j} e_i\beta_i : Y_0^{\beta_0}\cdots Y_j^{\beta_j} \in \Delta(I_n)_d \text{ y } \beta_j > 0\} = m_{0,j}(d-1) + e_j d$$

**Prueba:** Primero notemos que

$$m_{0,j}(d-1) + e_j d = (e_0 - e_j)(d-1) + e_j d = e_0(d-1) + e_j,$$

que es el valor de $\sum_{i=0}^{j} e_i\beta_i$ cuando $\beta_0 = d-1$, $\beta_j = 1$ y $\beta_i = 0$ para $i \neq 0, j$. Si $\tilde{\beta}_0,\ldots,\tilde{\beta}_j$ son tales que $\sum_{i=0}^{j}\tilde{\beta}_i = d$, entonces

$$\sum_{i=0}^{j} e_i\tilde{\beta}_i = \sum_{i=0}^{j-1} e_i\tilde{\beta}_i + e_j(\tilde{\beta}_j - 1) + e_j.$$

Como $e_0 \geq e_i$ para $0 \leq i \leq j$, se tiene

$$\sum_{i=0}^{j} e_i\tilde{\beta}_i \leq \sum_{i=0}^{j-1} e_0\tilde{\beta}_i + e_0(\tilde{\beta}_j - 1) + e_j = e_0\left(\sum_{i=0}^{j}\tilde{\beta}_i - 1\right) + e_j = e_0(d-1) + e_j.$$

□

**Definición 4.5.3** Para $j \in \{0, \ldots, n\}$ y $0 \leq s \leq m_{0,j}(d-1)$ sea

$$\mathcal{A}_d(j,s) := |\{Y_0^{\beta_0}\cdots Y_j^{\beta_j} \in \Delta(I_n)_d : \beta_j > 0 \text{ y } \textstyle\sum_{i=0}^{j} e_i\beta_i = s + e_jd\}|.$$

**Proposición 4.5.4** *Para $j \in \{0, \ldots, n\}$,*

$$|\Delta(\mathcal{B})_{d,j}| = \sum_{s=0}^{q-e_jd}(e_jd + s + 1)\mathcal{A}_d(j,s) + (q+1)\sum_{s=q-e_jd+1}^{m_{0,j}(d-1)}\mathcal{A}_d(j,s).$$

**Prueba:** Los monomios en $\Delta(\mathcal{B})_{d,j}$ tienen la forma $Y_0^{\beta_0}\cdots Y_j^{\beta_j}Z_0^{\gamma_0}Z_1^{\gamma_1}$ con $Y_0^{\beta_0}\cdots Y_j^{\beta_j} \in \Delta(I_n)_d$, $\beta_j > 0$ y $Z_0^{\gamma_0}Z_1^{\gamma_1} \in \Delta(I_1)_{\rho(\beta_0,\ldots,\beta_j,0,\ldots,0)}$. Supongamos que ya hemos seleccionado un monomio $Y_0^{\beta_0}\cdots Y_j^{\beta_j} \in \Delta(I_n)_d$ con $\beta_j > 0$. Por el lema 4.2.2, $\sum_{i=0}^{j}\beta_j = d$ y $0 \leq \beta_i < q$ para $0 \leq i < j$. Tal como hicimos en la ecuación 4.1, escribamos $\rho(\beta_0, \ldots, \beta_j, 0, \ldots, 0) = \sum_{i=0}^{j} e_i\beta_i = s + e_jd$, donde $s = \sum_{i=0}^{j-1} m_{i,j}\beta_i$.

Ahora debemos seleccionar $\gamma_0$ dentro del conjunto $\{0, \ldots, \text{mín}(q-1, s + e_jd - 1\} \cup \{s + e_jd\}$ y $\gamma_1$ queda fijado por la relación $\gamma_1 = s + e_jd - \gamma_0$. Si $s + e_jd > q$, entonces hay exactamente $q+1$ posibilidades de elección para $\gamma_0$, a saber, $\{0, \ldots, q-1, s + e_jd\}$. Si $s + e_jd \leq q$, entonces hay $s + e_jd + 1$ diferentes opciones para $\gamma_0$, a saber, $\{0, \ldots, s + e_jd\}$. El resultado se sigue usando la definición de $\mathcal{A}_d(j,s)$.

□

La siguiente observación es consecuencia directa del lema 4.2.2 y de la ecuación 4.1.

**Observación 4.5.5** $\mathcal{A}_d(j,s)$ es el número de soluciones enteras no negativas del sistema

$$\begin{cases} \beta_0 + \cdots + \beta_{j-1} + \beta_j &= d \\ m_{0,j}\beta_0 + \cdots + m_{j-1,j}\beta_{j-1} &= s \end{cases} \tag{4.2}$$

con las restricciones $\beta_j > 0$ y $0 \leq \beta_i < q$ para $0 \leq i < j$, donde convenimos en que la segunda ecuación de este sistema se vuelve $0 = 0$ cuando $j = 0$.

El próximo resultado nos da un método para calcular $\mathcal{A}_d(j, s)$.

**Lema 4.5.6** *Para $j \in \{0, \ldots, n\}$ y $s \in \{0, \ldots, m_{0,j}(d-1)\}$,*

$$\mathcal{A}_d(j, s) = \frac{1}{d!s!} \frac{\partial^{d+s} g}{\partial^d x \, \partial^s y}(0, 0),$$

*donde*

$$g(x, y) = \frac{x}{1-x} \cdot \prod_{i=0}^{j-1} \frac{1 - x^q y^{qm_{i,j}}}{1 - xy^{m_{i,j}}}.$$

**Prueba:** Una función generadora para el número de soluciones enteras no negativas del sistema de ecuaciones (4.2) está dada por

$$\begin{aligned} g(x, y) &= (x + x^2 + \cdots) \prod_{i=0}^{j-1} \left(1 + xy^{m_{i,j}} + \cdots + (xy^{m_{i,j}})^{q-1}\right) \\ &= \frac{x}{1-x} \cdot \prod_{i=0}^{j-1} \frac{1 - x^q y^{qm_{i,j}}}{1 - xy^{m_{i,j}}}, \end{aligned}$$

donde para $0 \leq i \leq j$, los exponentes de $x$ e $y$ en $1 + xy^{m_{i,j}} + \cdots + (xy^{m_{i,j}})^{q-1}$ representan respectivamente las elecciones posibles para $\beta_i$ y $m_{i,j}\beta_i$ y convenimos que el producto $\prod_{i=0}^{j-1} (1 + xy^{m_{i,j}} + \cdots + (xy^{m_{i,j}})^{q-1})$ es igual a 1 si $j = 0$. Por otro lado, los exponentes de $x$ in $(x + x^2 + \cdots)$ representan las elecciones posibles para $\beta_j$. Para una introducción a las funciones generadoras, el lector puede consultar por ejemplo [41]. Así, el coeficiente de $x^d y^s$ en esta expresión nos da el número de soluciones enteras no negativas de (4.2) y podemos determinarlo mediante la expresión

$$\frac{1}{d!s!} \frac{\partial^{d+s} g}{\partial^d x \, \partial^s y}(0, 0).$$

□

A continuación calcularemos la dimensión de $C_S(d)$ en algunos casos particulares.

**Teorema 4.5.7** *Si* $d > \dfrac{q-1}{e_n}$, *entonces*

$$\dim(C_S(d)) = (q+1)\sum_{j=0}^{n}\sum_{i=0}^{j}(-1)^i\binom{j}{i}\binom{j+d-1-iq}{d-1-iq}.$$

**Prueba:** Tenemos $\dim(C_S(d)) = |\Delta(\mathcal{B})_d| = \sum_{j=0}^{n}|\Delta(\mathcal{B})_{d,j}|$. Como $e_j \geq e_n$ para $0 \leq j \leq n$, se sigue que $q - e_j d \leq q - e_n d < 1$ . Así, por la proposición 4.5.4 tenemos

$$|\Delta(\mathcal{B})_{d,j}| = (q+1)\sum_{s=0}^{m_{0,j}(d-1)}\mathcal{A}_d(j,s)$$

para $0 \leq j \leq n$. Obsérvese además que en este caso la expresión $\sum_{s=0}^{m_{0,j}(d-1)}\mathcal{A}_d(j,s)$ cuenta el número de soluciones en enteros no negativos de la ecuación

$$\beta_0 + \cdots + \beta_j = d$$

con las restricciones $\beta_j > 0$ y $0 \leq \beta_i < q$ para $0 \leq i < j$. Esto equivale a determinar el coeficiente de $x^d$ en la expresión

$$\begin{aligned}(1+x+x^2+\cdots+x^{q-1})^j(x+x^2+\cdots) &= x\left(\frac{1-x^q}{1-x}\right)^j\left(\frac{1}{1-x}\right)\\ &= x(1-x^q)^j\left(\frac{1}{1-x}\right)^{j+1} =\end{aligned}$$

$$x\left[\sum_{i=0}^{j}(-1)^i\binom{j}{i}x^{iq}\right]\left[\sum_{k=0}^{\infty}\binom{k+j}{k}x^k\right],$$

el cual está dado por

$$\sum_{i=0}^{j}(-1)^i\binom{j}{i}\binom{j+d-1-iq}{d-1-iq}.$$

El resultado se obtiene sumando estas expresiones desde $j = 0$ hasta $j = n$ y multiplicando por $q+1$. □

**Teorema 4.5.8** *Si $d > n(q-1)$, entonces*

$$\dim(C_S(d)) = (q+1)(q^n + q^{n-1} + \cdots + 1).$$

**Prueba:** Si $d > n(q-1)$, entonces $d \geq n(q-1)+1 \geq (q-1)+1 = q$. Como $d \leq e_n d$, entonces $e_n d > q-1$, lo que implica $q - e_j d < 1$ para $0 \leq j \leq n$. Por la proposición 4.5.4 se tiene

$$\dim(C_S(d)) = \sum_{j=0}^{n} (q+1) \sum_{s=0}^{m_{0,j}(d-1)} \mathcal{A}_d(j,s).$$

Al igual que en la proposición anterior, $\sum_{s=0}^{m_{0,j}(d-1)} \mathcal{A}_d(j,s)$ cuenta el número de soluciones enteras no negativas de la ecuación $\beta_0 + \cdots + \beta_j = d$ con las restricciones $\beta_j > 0$ y $0 \leq \beta_i < q$ para $0 \leq i < j$. Como $d > q$, tenemos $q^j$ de estas soluciones. De esta manera se obtiene

$$\sum_{s=0}^{m_{0,j}(d-1)} \mathcal{A}_d(j,s) = q^j.$$

□

A continuación presentamos algunos ejemplos numéricos de los parámetros de los códigos proyectivos tipo Reed-Muller sobre el Rollo. Estos ejemplos fueron generados usando un programa escrito en Magma ([5]). El código fuente de este programa está incluido en el apéndice A.

**Ejemplos 4.5.9** *Consideremos el Rollo $S := S_{3,2,1}$ definido sobre $\mathbb{F}_4$. La siguiente tabla muestra los parámetros básicos del código $C_S(d)$ cuando $d$ oscila entre 1 y 7.*

| $d$ | *longitud* | *dimensión* | *distancia mínima* |
|---|---|---|---|
| 1 | 105 | 9 | 32 |
| 2 | 105 | 27 | 12 |
| 3 | 105 | 49 | 8 |
| 4 | 105 | 75 | 4 |
| 5 | 105 | 90 | 3 |
| 6 | 105 | 100 | 2 |
| 7 | 105 | 105 | 1 |

## 4.6. Los parámetros de $C_S(d)$ en un caso especial

Sea $\theta$ el isomorfismo entre el $\mathbb{F}_q$-espacio vectorial $M_{N_1\times N_2}(\mathbb{F}_q)$ de las matrices de $N_1 \times N_2$ y $\mathbb{F}_q^{N_1N2}$ dado por

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N_2} \\ a_{21} & a_{22} & \cdots & a_{2N_2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{N_11} & a_{22} & \cdots & a_{N_1N_2} \end{pmatrix} \mapsto (a_{11}, a_{12}, \ldots, a_{1N_2}, \ldots, a_{N_11}, a_{N_12}, \ldots, a_{N_1N_2}).$$

**Definición 4.6.1** Para $i = 1, 2$, sea $C_i \subseteq \mathbb{F}_q^{n_i}$ un código lineal, donde $n_i$ es un entero positivo y sea $M_{n_1\times n_2}(\mathbb{F}_q)$ el espacio vectorial de matrices de $n_1 \times n_2$ con entradas en $\mathbb{F}_q$. El ***producto directo*** de $C_1$ y $C_2$, el cual denotamos por $C_1 \underline{\otimes} C_2$, se define como la imagen bajo $\theta$ de todas las matrices en $M_{n_1\times n_2}(\mathbb{F}_q)$ cuyos renglones pertenecen a $C_2$ y cuyas columnas pertenecen a $C_1$.

**Proposición 4.6.2** *Sea $C_i \subseteq \mathbb{F}_q^{n_i}$ un código lineal de dimensión $k_i$ con distancia mínima $\delta_i$ para $i = 1, 2$. Entonces:*

1. *$C_1 \underline{\otimes} C_2$ tiene longitud $n_1n_2$, dimensión $k_1k_2$ y distancia mínima $\delta_1\delta_2$.*
2. *Si $\{u_i : 1 \leq i \leq k_1\}$ es una base para $C_1$ y $\{v_j : 1 \leq j \leq k_2\}$ es una base para $C_2$, entonces $\{\theta(u_i^{\mathsf{T}} v_j) : 1 \leq i \leq k_1, 1 \leq j \leq k_2\}$ es una base para $C_1 \underline{\otimes} C_2$, donde $u_i^{\mathsf{T}}$ es una matriz de $n_1 \times 1$ y $v_j$ es una matriz de $1 \times n_2$.*

**Prueba:** La primera parte se prueba en [42], teoremas 2.5.2 y 2.5.3. La segunda parte es una consecuencia del lema 2.3 en [40]. □

Usaremos estos resultados para calcular la distancia mínima de $C_S(d)$ en un caso especial.

**Teorema 4.6.3** *Supongamos que $e_0 = e_1 = \cdots = e_n = e$. Entonces*

$$C_S(d) \cong \mathrm{PRM}(d, n) \underline{\otimes} \mathrm{PRM}(de, 1).$$

**Prueba:** Como $e_0 = e_1 = \cdots = e_n = e$, sabemos por el lema 4.4.9 y la proposición 1.4.3 que el conjunto

$$\{\widetilde{ev}_d(\mathbf{Y}^{\boldsymbol{\beta}}\mathbf{Z}^{\boldsymbol{\gamma}}) : \mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d \text{ y } \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{de}\}$$

es una base para $C_S(d) \subset \mathbb{F}_q^N(\mathbb{F}_q)$, donde $I_n$ e $I_1$ son respectivamente los ideales de anulación de $\mathbb{P}^n(\mathbb{F}_q)$ y $\mathbb{P}^1(\mathbb{F}_q)$, $\Delta(I_n)_d$ y $\Delta(I_1)_{de}$ sus huellas con respecto a los órdenes lexicográficos $Y_n \prec_n \cdots \prec_n Y_0$, $Z_1 \prec_1 Z_0$ y $N = (q+1)(q^n + \cdots + q + 1)$.

Sea $d_1 = \dim(\mathrm{PRM}(d,n))$ la dimensión del código proyectivo tipo Reed-Muller de orden $d$ sobre $\mathbb{P}^n(\mathbb{F}_q)$. Similarmente, sea $d_2 = \dim(\mathrm{PRM}(de,1))$ la dimensión del código proyectivo tipo Reed-Muller de orden $de$ sobre $\mathbb{P}^1(\mathbb{F}_q)$ y sean $\Delta(I_n)_d := \{\mathbf{Y}^{\boldsymbol{\beta}_1}, \ldots, \mathbf{Y}^{\boldsymbol{\beta}_{d_1}}\}$, $\Delta(I_1)_{de} := \{\mathbf{Z}^{\boldsymbol{\gamma}_1}, \ldots, \mathbf{Z}^{\boldsymbol{\gamma}_{d_2}}\}$.

Usando la notación introducida en la sección 4.2, sabemos que $\{\varphi_{d,n}(\mathbf{Y}^{\boldsymbol{\beta}_1}), \ldots, \varphi_{d,n}(\mathbf{Y}^{\boldsymbol{\beta}_{d_1}})\}$ y $\{\varphi_{de,1}(\mathbf{Z}^{\boldsymbol{\gamma}_1}), \ldots, \varphi_{de,1}(\mathbf{Z}^{\boldsymbol{\gamma}_{d_2}})\}$ son bases respectivamente para $\mathrm{PRM}(d,n)$ y $\mathrm{PRM}(de,1)$ como $\mathbb{F}_q$-espacios.

Por la proposición 4.6.2, $\mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1) \subset \mathbb{F}_q^{N_n N_1}(\mathbb{F}_q) = \mathbb{F}_q^N(\mathbb{F}_q)$, donde $N_n = q^n + \cdots + q + 1$ y $N_1 = q + 1$. Además, el conjunto

$$\{\theta(\varphi_{d,n}(\mathbf{Y}^{\boldsymbol{\beta}_i})^{\mathsf{T}} \varphi_{de,1}(\mathbf{Z}^{\boldsymbol{\gamma}_j})) \, : \, i = 1, \ldots, d_1; \; j = 1, \ldots, d_2\},$$

es una base para $\mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1)$.

Podemos observar que para $i \in \{1, \ldots, d_1\}$ y $j \in \{1, \ldots, d_2\}$, las entradas de los vectores $\widetilde{ev}_d(\mathbf{Y}^{\boldsymbol{\beta}_i}\mathbf{Z}^{\boldsymbol{\gamma}_j})$ y $\theta(\varphi_{d,n}(\mathbf{Y}^{\boldsymbol{\beta}_i})^{\mathsf{T}} \varphi_{de,1}(\mathbf{Z}^{\boldsymbol{\gamma}_j}))$ tienen la misma forma, a saber:

$$a_0^{\beta_0} \cdots a_n^{\beta_n} b_0^{\gamma_0} b_1^{\gamma_1},$$

donde $((a_0 : \cdots : a_n), (b_0 : b_1)) \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. La única posible diferencia sería el orden en que aparecen las entradas. Esto prueba que $C_S(d) \cong \mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1)$.

□

**Corolario 4.6.4** *Sea $\delta(C_S(d))$ la distancia mínima de $C_S(d)$. Si $e_0 = e_1 = \cdots = e_n = e$, entonces la dimensión y distacia mínima de $C_S(d)$ están dadas de la manera siguiente.*

1. *Si $d \geq n(q-1)$ entonces,*

$$\dim(C_S(d)) = (q^n + \cdots + q + 1)(q+1) \quad \text{y} \quad \delta(C_S(d)) = 1.$$

2. *Si* $(q-1)/e < d \leq n(q-1)$ *entonces,*

$$\dim(C_S(d)) = (q+1)\sum_{j=0}^{n}\sum_{i=0}^{j}(-1)^i\binom{j}{i}\binom{j+d-1-iq}{d-1-iq} \quad y$$

$$\delta(C_S(d)) = (q-r)q^{n-k-1}, \ \textit{donde}\ d-1 = k(q-1)+r \ y\ 0 \leq r < q-1.$$

3. *Si* $1 \leq d \leq (q-1)/e$, *entonces*

$$\dim(C_S(d)) = (de+1)\binom{n+d}{d} \text{ y}$$

$$\delta(C_S(d)) = (q-d+1)(q-de+1)q^{n-1}.$$

**Prueba:** Esta es una consecuencia de las dos proposiciones anteriores y del teorema 4.2.1. Notemos que si $d \geq n(q-1)$, entonces $de \geq (q-1)$, así que $\mathrm{PRM}(d,n) = \mathbb{F}_q^{q^n+\cdots+q+1}$ y $\mathrm{PRM}(de,1) = \mathbb{F}_q^{q+1}$.

Por otro lado, $(q-1)/e < d \leq n(q-1)$ implica $de > q-1$ y $\mathrm{PRM}(de,1) = \mathbb{F}_q^{q+1}$.

Finalmente, si $1 \leq d \leq (q-1)/e$, entonces $de < q-1$ y $d < q-1$ y aplicando nuevamente las fórmulas del teorema 4.2.1 obtenemos el resultado. □

# Conclusiones y Perspectivas

El problema que hemos abordado en este trabajo es una generalización del caso estudiado en [8]. Mi asesor Horacio Tapia me dio a conocer dicho trabajo y el profesor Felipe Zaldívar me sugirió que había una manera bastante natural de generalizarlo.

El primer paso consistió en estudiar y entender a fondo las ideas y métodos presentados en [8]. Después tuvimos que entender la construcción del Rollo Normal Racional generalizado y la presentamos en una forma elemental útil a nuestros propósitos. A continuación, observamos que los códigos proyectivos tipo Reed-Muller sobre el Rollo Normal Racional son equivalentes a ciertos códigos de evaluación sobre un producto cartesiano de espacios proyectivos. Dicha observación nos permitió encontrar fórmulas para la dimensión de estos códigos usando técnicas inspiradas en las bases de Gröbner.

También descubrimos que los códigos estudiados en este trabajo son equivalentes a un producto directo de los códigos proyectivos Reed-Muller sobre el espacio proyectivo total en algunos casos especiales.

Con respecto al cálculo de la distancia mínima en el caso general, no fuimos capaces de obtener al menos una buena cota usando las técnicas de bases de Gröbner. Este es un problema que queda abierto para futuras investigaciones.

En general, creemos que el trabajo expuesto en esta tesis es una buena aportación a la teoría de códigos. Como trabajo a futuro, nos gustaría explorar posibles aplicaciones de los códigos estudiados en esta tesis a la construcción de códigos cuánticos. También nos gustaría abordar otros problemas en teoría de códigos que puedan resolverse usando bases de Gröbner.

# Apéndice A

# Programa en Magma para generar ejemplos

En esta sección incluimos varios fragmentos de código en Magma ([5]) que permiten generar en primer lugar un rollo normal racional generalizado y a continuación los códigos proyectivos tipo Reed-Muller definidos sobre él. Las instrucciones están basadas en las construcciones de los capítulos 3 y 4.

La siguiente función genera las coordenadas de los puntos de un espacio proyectivo de una dimensión dada sobre un campo finito.

```
function projective_space(field, dimension)
    space:= [];
    for i:= 0 to dimension do
        for affine_coords in
        SetToSequence(Set(CartesianPower(field, dimension -i))) do
            point:= [0: j in [0..i-1]];
            point cat:= [1];
            for coordinate in affine_coords do
                point cat:= [coordinate];
            end for;
            space cat:= [point];
        end for;
    end for;
    return space;
end function;
```

A continuación tenemos el mapeo de Veronese. Toma como parámetros de entrada una recta proyectiva y un grado $d$ para producir como resultado una curva normal racional de grado $d$.

```
function veronese_map(line, degree)
    curve:= [];
    for x in line do
        y:= [];
        for i:= 0 to degree do
            y cat:= [(x[1]^(degree - i))*(x[2]^i)];
        end for;
        curve cat:= [y];
```

```
    end for;
    return curve;
end function;
```

Definimos una función que dados un campo finito y un conjunto de grados para las curvas normales racionales construye un rollo normal racional.

```
function higher_scroll(field, curves)
    n:= #curves - 1;
    P_n:= projective_space(field, n);
    number_spaces:= #curves[1];
    scroll:= [];
    for i:=1 to number_spaces do
        for coefficients in P_n do;
            point:= [];
            for j:=1 to n+1 do
                for coord in curves[j][i] do
                    point cat:= [coefficients[j]*coord];
                end for;
            end for;
            scroll cat:= [point];
        end for;
    end for;
    return(scroll);
end function;
```

Esta función produce todos los monomios de un grado dado en el anillo de polinomios $\mathbb{F}_q[Y_0, \ldots, Y_n, Z_0, Z_1]$. Los monomios son representadas como vectores de exponentes.

```
function generate_monomials(degrees_curves, d)
    l:= &+degrees_curves + #degrees_curves - 1;
    coordinates:= [i: i in [1..l+1]];
    monomials:= [];
    combinations:= Multisets(SequenceToSet(coordinates), d);
    for combination in combinations do
        monomial:= [0: i in coordinates];
        for exponent in combination do
            monomial[exponent]:= monomial[exponent] + 1;
        end for;
        monomials cat:= [monomial];
    end for;
    return(monomials);
end function;
```

Ahora definimos una función que evalúa un monomio en un punto.

```
function evaluate_monomial(monomial, point)
    evaluation:= 1;
    for i:= 1 to #monomial do
        if monomial[i] ne 0 then
            evaluation:= evaluation*point[i]^monomial[i];
        end if;
    end for;
    return(evaluation);
end function;
```

A partir de la función anterior definimos otra que evalúa un conjunto de monomios en un conjunto de puntos.

```
function evaluation_morphism(set, monomials)
    evaluations:= [];
```

```
    for monomial in monomials do
        evaluation:= [];
        for point in set do
            evaluation cat:= [evaluate_monomial(monomial, point)];
        end for;
        evaluations cat:= [evaluation];
    end for;
    return(evaluations);
end function;
```

Ahora ya estamos en condiciones de construir códigos proyectivos tipo Reed-Muller definidos sobre un Rollo Normal Racional. Primero necesitamos definir un campo base, un vector de grados para las curvas y un grado para el mapeo evaluación.

```
k := FiniteField(2);
e := [3,2,1];
d := 1;
```

Producimos el rollo normal racional así como el correspondiente código proyectivo tipo Reed-Muller.

```
P_1:= projective_space(k,1);
curves:= [veronese_map(P_1, degree): degree in e];
scroll:= higher_scroll(k, curves);
monomials:= generate_monomials(e, d);
evaluations:= evaluation_morphism(scroll, monomials);

M:= Matrix(k, #evaluations, #scroll, evaluations);
C:= LinearCode(M);
print(Length(C));
print(Dimension(C));
print(MinimumWeight(C));
```

# Apéndice B

# El algoritmo de Buchberger

En este apéndice se prueba el algoritmo de Buchberger, el cual nos dice cómo construir una base de Gröbner para un ideal. Para mayores referencias, el lector puede consultar [14].

**Definición B.0.5** Fijemos un orden monomial $\prec$ en $K[\mathbf{X}] := K[X_1, \ldots, X_n]$, donde $K$ es un campo. Sean $f, g \in K[\mathbf{X}]\backslash\{0\}$ tales que $lm(f) = \mathbf{X}^{\boldsymbol{\alpha}}$ y $lm(g) = \mathbf{X}^{\boldsymbol{\beta}}$, donde $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}_0^n$. Sea $\boldsymbol{\gamma} := (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}_0^n$, donde $\gamma_i := max\{\alpha_i, \beta_i\}$ para $1 \leq i \leq n$. Definimos el ***S-polinomio*** de $f$ y $g$ como

$$S(f, g) := \frac{\mathbf{X}^{\boldsymbol{\gamma}}}{lt(f)} \cdot f - \frac{\mathbf{X}^{\boldsymbol{\gamma}}}{lt(g)} \cdot g.$$

**Lema B.0.6** *Sea $\prec$ un orden monomial y supongamos que tenemos $\sum_i^s c_i g_i$ con $c_i \in k$, $g_i \in K[\mathbf{X}]$ tal que $lt(g_i) = d_i \mathbf{X}^{\boldsymbol{\alpha}}$ con $d_i \in K\backslash\{0\}$ para $1 \leq i \leq s$. Si $lm\left(\sum_i^s c_i g_i\right) \prec \mathbf{X}^{\boldsymbol{\alpha}}$, entonces $\sum_i^s c_i g_i$ es una $K$-combinación lineal de S-polinomios $S(g_j, g_k)$ para $j, k \in \{1, \ldots, s\}$. Además se tiene que $lm(S(g_j, g_k)) \prec \mathbf{X}^{\boldsymbol{\alpha}}$ para todo $j, k \in \{1, \ldots, s\}$.*

**Prueba:** Para $1 \leq i \leq s$ definimos $p_i := f_i/d_i$. El S-polinomio de $g_j$ y $g_k$ es:

$$S(g_j, g_k) = \frac{\mathbf{X}^{\boldsymbol{\alpha}}}{d_j \mathbf{X}^{\boldsymbol{\alpha}}} \cdot g_j - \frac{\mathbf{X}^{\boldsymbol{\alpha}}}{d_k \mathbf{X}^{\boldsymbol{\alpha}}} \cdot g_k = p_j - p_k$$

para $j, k \in \{1, \ldots, s\}$. Como $lm(g_i) = \mathbf{X}^{\boldsymbol{\alpha}}$ para $1 \leq i \leq s$ y $lm\left(\sum_i^s c_i g_i\right) \prec \mathbf{X}^{\boldsymbol{\alpha}}$, se debe tener $\sum_i^s c_i d_i = 0$. Escribamos

$$\sum_i^s c_i g_i = \sum_i^s c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s =$$
$$c_1 d_1 S(g_1, g_2) + (c_1 d_1 + c_2 d_2) S(g_2, g_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(g_{s-1}, g_s).$$

Finalmente, como $lt(p_j) = \mathbf{X}^{\boldsymbol{\alpha}} = lt(p_k)$, se sigue que $lm(S(g_j, g_k)) \prec \mathbf{X}^{\boldsymbol{\alpha}}$. □

**Definición B.0.7** Fijemos un orden monomial $\prec$ en $K[\mathbf{X}]$ y sea $G = \{g_1, \ldots, g_s\} \subset K[\mathbf{X}]$. Supongamos que podemos escribir $f \in K[\mathbf{X}]$ en la forma

$$f = a_1 g_1 + \cdots a_s g_s,$$

donde $a_i \in K[\mathbf{X}]$, $lm(a_i g_i) \preceq lm(f)$ siempre que $a_i g_i \neq 0$. Entonces, decimos que $f$ se ***reduce a cero módulo*** $G$ y escribimos $f \to_G 0$.

**Teorema B.0.8** *Sea $G = \{g_1, \ldots, g_s\}$ base de un ideal $I \subset K[\mathbf{X}]$. $G$ es una base de Gröbner para $I$ -con respecto a un orden monomial $\prec$- si y sólo si $S(g_i, g_j) \to_G 0$ para todo $i \neq j$.*

**Prueba:** $\Longrightarrow$ : Si $G$ es una base de Gröbner, entonces, como $S(g_i, g_j) \in I$, usando el algoritmo de la división, podemos expresar a $S(g_i, g_j)$ en la forma:

$$S(g_i, g_j) = a_{1ij} g_1 + \cdots a_{sij} g_s,$$

donde $lm(S(g_i, g_j)) \succeq lm(a_k ij g_k)$ siempre que $a_k ij g_k \neq 0$. Esto es precisamente lo que quiere decir $S(g_i, g_j) \to_G 0$.

$\Longleftarrow$ : Sea $f \in I$; entonces, como $G$ es una base para $I$, podemos escribir

$$f = \sum_{i=1}^{s} h_i g_i \tag{B.1}$$

con $h_i \in k[\mathbf{X}]$. En general, pueden existir varias expresiones de la forma B.1 para $f$ y cada una nos dará un cierto $\mathbf{X}^{\boldsymbol{\gamma}} := max_{\succeq}\{lm(h_1 g_1), \ldots, lm(h_s g_s)\}$. Como un orden monomial es un buen orden, elegimos la expresión que nos dé al mínimo $\mathbf{X}^{\boldsymbol{\gamma}}$. Si $lm(f) = \mathbf{X}^{\boldsymbol{\gamma}}$, entonces $lm(f) = lm(h_i g_i)$ para algún $i \in \{1, \ldots, s\}$, lo cual implica que $lt(g_i) | lt(f)$ y $G$ es una base de Gröbner.

Supongamos que $lm(f) \prec \mathbf{X}^{\boldsymbol{\gamma}}$ para llegar a una contradicción. Entonces podemos escribir

$$f = \sum_{lm(h_i g_i) = \mathbf{X}^{\boldsymbol{\gamma}}} h_i g_i + \sum_{lm(h_i g_i) \prec \mathbf{X}^{\boldsymbol{\gamma}}} h_i g_i =$$

$$\sum_{lm(h_ig_i)=\mathbf{X}^{\boldsymbol{\gamma}}} lt(h_i)g_i + \sum_{lm(h_ig_i)=\mathbf{X}^{\boldsymbol{\gamma}}} (h_i - lt(h_i))g_i + \sum_{lm(h_ig_i)\prec\mathbf{X}^{\boldsymbol{\gamma}}} h_ig_i.$$

Como tanto $lm(f)$ como los monomios que aparecen en la segunda y tercera sumas son menores que $\mathbf{X}^{\boldsymbol{\gamma}}$, debe ser también que el monomio líder de la primera suma sea menor a $\mathbf{X}^{\boldsymbol{\gamma}}$. Sea $lt(h_i) = c_i\mathbf{X}^{\boldsymbol{\alpha}(i)}$ con $c_i \in k$ para $1 \leq i \leq s$. Usando el lema B.0.6 podemos expresar la suma

$$\sum_{lm(h_ig_i)=\mathbf{X}^{\boldsymbol{\gamma}}} lt(h_i)g_i = \sum_{lm(h_ig_i)=\mathbf{X}^{\boldsymbol{\gamma}}} c_i\mathbf{X}^{\boldsymbol{\alpha}(i)}g_i$$

como una combinación lineal de S-polinomios $S(\mathbf{X}^{\boldsymbol{\alpha}(j)}g_j, \mathbf{X}^{\boldsymbol{\alpha}(k)}g_k)$, $j,k \in \{1,\ldots,s\}$. Pero

$$S(\mathbf{X}^{\boldsymbol{\alpha}(j)}g_j, \mathbf{X}^{\boldsymbol{\alpha}(k)}g_k) = \frac{\mathbf{X}^{\boldsymbol{\gamma}}}{\mathbf{X}^{\boldsymbol{\alpha}(j)}lt(g_j)} \cdot \mathbf{X}^{\boldsymbol{\alpha}(j)}g_j - \frac{\mathbf{X}^{\boldsymbol{\gamma}}}{\mathbf{X}^{\boldsymbol{\alpha}(k)}lt(g_k)} \cdot \mathbf{X}^{\boldsymbol{\alpha}(k)}g_k = \mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}_{jk}}S(g_j,g_k),$$

donde $\mathbf{X}^{\boldsymbol{\beta}_{jk}}$ es el mínimo común múltiplo de $lm(g_j)$ y $lm(g_k)$. De esta forma existen constantes $c_{jk} \in k$ tales que

$$\sum_{lm(h_ig_i)=\mathbf{X}^{\boldsymbol{\gamma}}} lt(h_i)g_i = \sum_{j,k} c_{jk}\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}_{jk}}S(g_j,g_k).$$

Usano ahora la hipótesis $S(g_j,g_k) \to_G 0$, podemos escribir

$$S(g_j,g_k) = \sum_{i=1}^{s} a_{ijk}g_i,$$

donde $a_{ijk} \in k[\mathbf{X}]$ y $lm(a_{ijk}g_i) \preceq lm(S(g_j,g_k))$ siempre que $a_{ijk}g_i \neq 0$. Tenemos así

$$\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}_{jk}}S(g_j,g_k) = \sum_{i=1}^{s} b_{ijk}g_i.$$

donde $b_{ijk} := \mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}_{jk}}a_{ijk}$. Se cumple entonces que

$$lm(b_{ijk}g_i) \preceq lm(\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}_{jk}}S(g_j,g_k)) \prec \mathbf{X}^{\boldsymbol{\gamma}},$$

donde la segunda desigualdad es por el lema B.0.6. Llegamos así a la expresión

$$\sum_{lm(h_i g_i)=\mathbf{X}^{\boldsymbol{\gamma}}} lt(h_i)g_i = \sum_{j,k} c_{jk}\mathbf{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk}\left(\sum_i b_{ijk} g_i\right) = \sum_i \tilde{h}_i g_i.$$

Esta expresión tiene la propiedad $lm(\tilde{h}_i g_i) \prec \mathbf{X}^{\boldsymbol{\gamma}}$ para toda $i$. Así, podemos escribir

$$f = \sum_{lm(h_i g_i)=\mathbf{X}^{\boldsymbol{\gamma}}} lt(h_i)g_i + \sum_{lm(h_i g_i)=\mathbf{X}^{\boldsymbol{\gamma}}} (h_i - lt(h_i))g_i + \sum_{lm(h_i g_i)\prec\mathbf{X}^{\boldsymbol{\gamma}}} h_i g_i =$$

$$\sum_i \tilde{h}_i g_i + \sum_{lm(h_i g_i)=\mathbf{X}^{\boldsymbol{\gamma}}} (h_i - lt(h_i))g_i + \sum_{lm(h_i g_i)\prec\mathbf{X}^{\boldsymbol{\gamma}}} h_i g_i,$$

la cual es una combinación polinomial de los $g_i$'s en la que todos los monomios que aparecen son menores a $\mathbf{X}^{\boldsymbol{\alpha}}$, lo cual contradice la minimalidad de $\mathbf{X}^{\boldsymbol{\alpha}}$. □

**Definición B.0.9** Escribiremos $\overline{f}^F$ para denotar al residuo que resulta al dividir un polinomio $f$ entre una $s$-tupla ordenada $F := (f_1, \ldots, f_s)$.

Ahora estamos ya en condiciones de enunciar y probar el algoritmo de Buchberger:

**Teorema B.0.10** *Sea $0 \neq I = (f_1, \ldots, f_s) \subset K[\mathbf{X}]$ un ideal y $\prec$ un orden monomial en $K[\mathbf{X}]$. Entonces podemos construir una base de Gröbner para $I$ en un número finito de pasos mediante el siguiente algoritmo:*

*Entrada:* $F = \{f_1, \ldots, f_s\}$
*Salida: Una base de Gröbner* $G = \{g_1, \ldots, g_t\}$ *para* $I$ *tal que* $F \subset G$
$G := F$
$G' := \{0\}$
***while*** $G' \neq G$ ***do***
  $G' := G$
  ***for all*** $\{p, q\} \in G'$, $p \neq q$ ***do***
    $r := \overline{S(p,q)}^{G'}$
    ***if*** $r \neq 0$ ***then***
      $G := G \cup \{r\}$

***end if***
***end for***
***end while***

**Prueba:** En cada paso del algoritmo, dado $G = (g_1, \ldots, g_s)$, $< lt(G) >$ y $< lt(G) >$ denotarán respectivamente a los ideales

$$< G >:= (g_1, \ldots, g_t)$$
$$< lt(g) >:= (lt(g_1), \ldots, lt(g_t)).$$

Primero mostraremos que se cumple la contención $G \subset I$ en todo momento. Esto es cierto al comienzo, cuando se define $G := F$. Ahora, si se cumple $G \subset I$, entonces, para todos los $p, q$ en $G$, el $S$-polinomio $S(p, q)$ también está en $I$. Así, al dividir $S(p, q)$ entre $G' := G \subset I$, se obtiene un residuo $r := \overline{S(p,q)}^{G'}$ que también está en $I$, de tal forma que $G' \cup \{r\} \subset I$.

El algoritmo termina si en algún punto del mismo se cumple que $\overline{S(p,q)}^{G'} = 0$ para todo $p, q$ en $G$. Por el teorema B.0.8, se tendría que $G$ es una base de Gröbner para $I$ con respecto a $\prec$.

De esta forma, sólo resta probar que el algoritmo realmente termina. Para ver esto, notemos que cuando estamos dentro del ciclo while, si se cumple $r := \overline{S(p,q)}^{G'} \neq 0$ para algunos $p, q \in G$, entonces se redefine $G$ como $G := G' \cup \{r\}$. Afirmamos que en este caso

$$< lt(G') > \subsetneq < lt(G) >= lt < (G' \cup \{r\}) >.$$

En efecto, Si se tuviera $lt(r) \in < lt(G') >$, entonces sería posible escribir

$$lt(r) = \sum_{i=1}^{t} h_i lt(g_i),$$

donde $G' = \{g_1, \ldots, g_s\}$ y los $h_i$ son polinomios en $k[\mathbf{X}]$. Al expandir el lado derecho de esta igualdad, se obtiene una suma de monomios, todos los cuales son divisibles por algún $lt(g_i)$, por lo cual $lt(r)$ debería también debería ser divisible por algún $lt(g_i)$. Sin embargo, como $r$ es el residuo que se obtiene al dividir $S(p, q)$ entre $G'$, el algoritmo de la división nos dice que $lt(r)$ no es divisible por ninguno de los términos líderes de los elementos de $G'$. Por lo tanto, conlcuimos que $lt(r) \notin < lt(G') >$.

Así, los ideales $< lt(G_i) >$ que se obtienen en cada paso del ciclo while forman una cadena estrictamente ascendente. Como $k[\mathbf{X}]$ es un anillo noetheriano, esta cadena debe estabilizarse en algún momento. En otras palabras, el algoritmo debe terminar.

□

El siguiente resultado, usado junto con el teorema B.0.8, nos da un criterio práctico para saber si una base de un ideal es de hecho una base de Gröbner.

**Proposición B.0.11** *Sea $G$ un subconjunto finito de $k[\mathbf{X}]$, $\prec$ un orden monomial en $k[\mathbf{X}]$ y supongamos que tenemos $f, g \in G$ tales que $lm(f)$ y $lm(g)$ son coprimos. Entonces $S(f, g) \to_G 0$.*

**Prueba:** Por simplicidad supondremos que $f$ y $g$ han sido multiplicados por constantes adecuadas de tal forma que $lc(f) = lc(g) = 1$. Escribimos $f = lm(f) + p$, $g = lm(g) + q$. Como $lm(f)$ y $lm(g)$ son coprimos se tiene

$$S(f,g) = \frac{lm(f)lm(g)}{lm(f)} \cdot f + \frac{lm(f)lm(g)}{lm(g)} \cdot g = lm(g) \cdot f - lm(f) \cdot g =$$
$$(g-q) \cdot f - (f-p) \cdot g = g \cdot f - q \cdot f - f \cdot g + p \cdot g = p \cdot g - q \cdot f.$$

Si se tuviera $lm(p) \cdot lm(g) = lm(q) \cdot lm(f)$, entonces se tendría $lm(g)|lm(q) \cdot lm(f)$. Como $lm(f)$y $lm(g)$ son coprimos, esto implicaría $lm(g)|lm(q)$, lo cual es absurdo porque $lm(g) \succ lm(q)$.

Entonces $lm(S(f,g)) = max\{lm(p \cdot g), lm(q \cdot f)\}$, y como $f, g \in G$, concluimos $S(f, g) \to_G 0$. □

# Bibliografía


[1] E. F. Assmus Jr., and J. D. Key, *Polynomial Codes and Finite Geometries*, in Handbook of Coding Theory, V. Pless and W. Huffman, Eds., vol. II, Elsevier, 1998, pp. 1269-1343.

[2] T. Becker and W. Weispfenning, *Gröbner bases*, Springer Graduate Texts in Mathematics, 1993.

[3] P. Beelen, M. Datta and S. R. Ghorpade, *A Combinatorial Approach to the Number of Solutions of Systems of Homogeneous Polynomial Equations over Finite Fields*, arXiv:1807.01683v2, 2018.

[4] P. Beelen, M. Datta and S. R. Ghorpade, *Maximum Number of common Zeros of Homogeneous Polynomials over Finite Fields*, Proceedings of the American Mathematical Society, vol. 146, number 4, pp. 1451-1468, April 2018.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system.* I. The user language, J. Symbolic Comput., 24 (1997), 235-265.

[6] E. R. Berlekamp, *Key papers in the development of coding theory*, IEEE Press, New York, 1974.

[7] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Mathematical Institute, University of Innsbruck, Austria. PhD Thesis, 1965.

[8] C. Carvalho and V.G.L. Neumann, *Projective Reed-Muller type codes on rational normal scrolls*, Finite Fields and Their Applications., vol. 37, pp. 85-107, 2016.

[9] C. Carvalho, V.G.L. Neumann and H. Lopez, *Projective Nested Cartesian Codes*, Bull. Braz. Math. Soc. 48, pp. 283-302, 2017.

[10] C. Carvalho. *Gröbner bases methods in coding theory*, in Algebra for Secure and Reliable Commnication Modeling, Eds. M. Lahyane and E. Martínez-Moro, American Mathematical Society, 2015, pp. 73-86.

[11] C. Carvalho, *On the second Hamming weight of some Reed-Muller type codes*, Finite Fields and their Applications., vol.24, pp. 88-94, 2013.

[12] C. Carvalho, X. Ramírez-Mondragón, V. G. L. Neumann, H. Tapia-Recillas. *Projective Reed-Muller type codes on higher dimensional scrolls*, Designs, Codes and Cryptography, vol. 87, issue 9, pp. 2027-2042, 2019.

[13] A. Couvreur and I. Duursma, *Evaluation codes from smooth quadric surfaces and twisted Segre varieties*, Des. Codes Cryptogr., 66, pp. 291-303, 2013.

[14] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, 3rd. ed., New York, Springer Undergraduate Texts in Mathematics, 2007.

[15] I. Duursma, C. Rentería and H. Tapia-Recillas, *Reed-Muller codes on complete intersections*, Applicable Algebra in Engineering, Communication and Computing, AAECC 11, pp. 455-462, 2001.

[16] J. Fitzgerald, R.F. Lax, *Decoding affine variety codes using Gröbner bases*, Designs, Codes and Cryptography, vol. 13, pp. 147-158, 1998.

[17] J. B. Fraleigh, *A First Course In Abstract Algebra*, Addison Wesley, 7th. ed., 2003.

[18] M. J. E. Golay, *Notes on digital coding*, Proceedings of the IRE, v. 37, page 657, June 1949.

[19] V. D. Goppa, *Geometry and Codes*, Springer-Science+Business Media, B.V., Mathematics and Its Applications (Soviet Series), 1988.

[20] M. González-Sarabia, J. Martínez-Bernal, R. H. Villarreal and C. E. Vívares, *Generalized Minimum Distance Functions*, Journal of Algebraic Combinatorics, doi:10.1007/s10801-018-0855-x, Oct. 2018.

[21] M. González-Sarabia, C. Rentería and H. Tapia Recillas, *Reed-Muller type Codes Over the Segre Variety*, Finite Fields and their Applications, vol. 8, issue 4, pp. 511-518, 2002.

[22] M. González-Sarabia, C. Rentería, *The dual code of some Reed-Muller type codes*, Applicable Algebra in Enginnering, Communication and Computing, vol. 14, issue 5, pp. 329-333, 2004.

[23] R.W. Hamming, *Error Detecting and Error Correcting Codes*, Bell System Technical Journal, 29: 147-160, April 1950.

[24] G. M. Hana and T. Johnsen, *Scroll Codes*, Des. Codes Cryptogr., vol. 45, pp. 365-377, 2007.

[25] J. Harris, *Algebraic Geometry: A First Course*, Springer-Verlag, GTM, no. 133, 1992.

[26] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[27] T. Kasami, S. Lin and W. W. Peterson, *New generalizations of the Reed-Muller codes–I: Primitive codes*, IEEE Trans. Inform. Theory, vol. 14, no. 2, pp. 189-199, 1968.

[28] T. Kasami, S. Lin and W. W. Peterson, *New generalizations of the Reed-Muller codes–II: Nonprimitive codes*, IEEE Trans. Inform. Theory, vol. 14, no. 2, pp. 199-205, 1968.

[29] G. Lachaud, *Projective Reed-Muller codes*. In: Cohen G., Godlewski P. (eds) Coding Theory and Applications. Lecture Notes in Computer Science, v. 311. Springer, Berlin, Heidelberg, 1988.

[30] H. H. López, C. Rentería-Márquez, R. H. Villarreal, *Affine cartesian codes*, Des. Codes Cryptogr., vol. 71, pp. 5-19, 2014.

[31] F. J. MacWilliams and J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Co., 1977.

[32] D. E. Muller, *Applications of Boolean algebra to switching circuit design and to error correction*, IRE. Trans. Elec. Comp., vol. 3, pp. 6-12, 1954.

[33] I. Reed, *A class of multiple-error-correcting codes and a decoding scheme*, IEEE Trans. Inform. Theory, vol. 4, pp. 38-49, 1954.

[34] I. S. Reed, G. Solomon, *Polynomial Codes over certain Finite Fields*, Journal of the Society for Industrial and Applied Mathematics, Vol. 8 No.2 (1960), pp. 300-304.

[35] C. Rentería and H. Tapia-Recillas, *Reed-Muller Codes: An Ideal Theory Approach*, Communications in Algebra, vol. 25, issue 2, pp. 401-413, 1997.

[36] C. Rentería and H. Tapia-Recillas, *Reed-Muller type codes on the Veronese Variety over finite fields*, Coding Theory, Cryptography and Related Areas, J. Buchmann, T. Hoholdt, H. Stichtenoth, H. Tapia-Recillas, eds., ISBN 3-540-66248-0, Springer-Verlag, pp. 237-243, 2000.

[37] M. Sala, T. Mora, L. Perret, S. Sakata and C. Traverso, eds., *Gröbner Bases, Coding, and Criptography*, Springer, 2009.

[38] C. Shannon, *A mathematical theory of communication*, Bell System Technical Journal, vol. 27, pp. 379-423, 623-656, 1948.

[39] A. B. Sörensen, *Projective Reed-Muller Codes*, IEEE Trans. on Inform. Theory, vol. 37, no. 6, pp. 1567-1576, 1991.

[40] A. Tochimani, M. V. Pinto and R. H. Villarreal, *Direct products in projective Segre codes*, Finite Fields and Their Applications, vol. 39, pp. 96-110, 2016.

[41] A. Tucker, *Applied Combinatorics*, 6th. edition, John Wiley and Sons, 2012.

[42] J.H. van Lint, *Coding Theory*, second printing, Lect. Notes Math., vol. 201, Springer-Verlag, Berlin, New York, 1973.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

# ACTA DE DISERTACIÓN PÚBLICA

No. 00066
**Matrícula: 2142800120**

Códigos proyectivos tipo Reed-Muller sobre el rollo normal racional generalizado.

En la Ciudad de México, se presentaron a las 12:00 horas del día 16 del mes de octubre del año 2019 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. HORACIO TAPIA RECILLAS
DR. RAFAEL HERACLIO VILLAREAL RODRIGUEZ
DR. JOSE NOE GUTIERREZ HERRERA
DR. GUILLERMO BENITO MORALES LUNA
DR. FELIPE DE JESUS ZALDIVAR CRUZ

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron a la presentación de la Disertación Pública cuya denominación aparece al margen, para la obtención del grado de:

DOCTOR EN CIENCIAS (MATEMATICAS)

DE: XAVIER RAMIREZ MONDRAGON

y de acuerdo con el artículo 78 fracción IV del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

XAVIER RAMIREZ MONDRAGON
ALUMNO

REVISÓ

MTRA. ROSALIA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JESUS ALBERTO OCHOA TAPIA

PRESIDENTE

DR. HORACIO TAPIA RECILLAS

VOCAL

DR. RAFAEL HERACLIO VILLAREAL RODRIGUEZ

VOCAL

DR. JOSE NOE GUTIERREZ HERRERA

VOCAL

DR. GUILLERMO BENITO MORALES LUNA

SECRETARIO

DR. FELIPE DE JESUS ZALDIVAR CRUZ