UNIVERSIDAD AUTONOMA METROPOLITANA Iztapalapa

CÓDIGOS REED-MULLER SOBRE CIERTOS SUBCONJUNTOS DEL ESPACIO PROYECTIVO.

TESIS

QUE PARA OBTENER EL GRADO DE

DOCTOR EN CIENCIAS
ESPECIALIDAD EN MATEMÁTICAS

PRESENTA

M. en C. Manuel González Sarabia

ASESORES

Dr. Carlos Rentería Márquez
Dr. Horacio Tapia Recillas

México, D.F., 21 de Noviembre de 2002.

Contents

Introducción

Podemos decir que la teoría de códigos surgió en 1948 cuando Claude E. Shannon publicó el artículo *The Mathematical Theory of Communication*, [33]. Los códigos detectores-correctores de error son muy útiles en el envío de información a través de canales ruidosos donde pueden ocurrir errores en el mensaje. Un ejemplo claro de lo anterior es el hecho siguiente: En 1965 el Mariner 4, de la NASA, envió a la tierra, haciendo uso de códigos detectores-correctores de error, las primeras imágenes del planeta Marte, imágenes valiosísimas en su momento, aunque de calidad mediana si las comparamos con las imágenes logradas en la actualidad (para más detalles puede consultarse la página web de la NASA: http://www.nasa.gov/).

La transmisión de información desde naves espaciales o a través de satélites de comunicaciones es uno de los paradigmas de la teoría de códigos. Los impresionantes avances tecnológicos, en tecnología digital, que en la actualidad son normales y que consideramos parte de nuestra vida cotidiana, como el teléfono celular, la televisión digital, los sistemas de navegación aérea y marítima, los CD-R, los DVD, en buena medida (pero no totalmente) no serían posibles sin el desarrollo de los códigos detectores-correctores de error, [41]. Estos códigos aparecen, además, en medicina (tomografía), en los códigos de barras y en consecuencia la importancia de su estudio y de la obtención de resultados originales en este contexto está fuera de discusión.

En este trabajo se presentan varios resultados correspondientes a lo que se llaman Códigos Reed-Muller definidos sobre ciertos subconjuntos del espacio proyectivo. De hecho, los códigos Reed-Muller fueron definidos por primera vez, y en el caso binario, en [24] y [26]. Quizás la primera prueba de fuego de estos códigos fue realizada en 1972, cuando el Mariner 9 repetía el experimento del Mariner 4, aunque con resultados cualitativos notoriamente mejores. La razón de esta mejoría se debió al uso de un potente código

detector-corrector de errores (del tipo Reed-Muller) capaz de corregir hasta 5 bits erróneos de cada secuencia de 32 bits, [3].

Este tipo de códigos fueron generalizados para el caso de cualquier campo finito en [5], [19] y [40].

En esta tesis se trabaja en la solución de problemas en teoría de códigos usando herramientas y conceptos de Algebra Conmutativa y Geometría Algebraica como la función de Hilbert, bases de Gröbner, sucesiones exactas, variedades proyectivas, etc.. Se encuentran algunos resultados relacionados con ciertos códigos lineales (se calcula por ejemplo la dimensión y distancia mínima para el caso de los códigos asociados a la variedad de Segre). Este enfoque es reciente y tiene como precursores a [1], [5], [14], [17], [19], [21], [23], [34].

El trabajo aquí presentado es una continuación natural (aparte del contexto mencionado anteriormente) de las investigaciones realizadas por mis asesores, los doctores Carlos Rentería Márquez y Horacio Tapia Recillas. Los resultados que ellos encontraron, [6], [10], [27], [28], [29], [30], [31], son la base fundamental para el desarrollo de los temas de esta tesis.

Otro de los tópicos importantes que se desarrollan es el concepto de los pesos generalizados de Hamming, introducidos por V.K. Wei en [38]. Es importante mencionar que aquí sólo se calcula el segundo peso generalizado y en un caso particular. Este tema se empezó a estudiar como una generalización natural al concepto de distancia mínima y en respuesta a un problema específico de criptografía ([25]). Los pesos generalizados de Hamming son usados en procesos de decodificación y para el estudio del comportamiento del código cuando es usado en un canal criptográfico de un tipo especial (wire-tap channel of type II). Más aún, se usan para clasificar códigos, para construir curvas sobre campos finitos con muchos puntos racionales y para otros problemas (ver [1]).

Este tipo de temas no ha perdido vigencia. Baste decir que, recientemente, H.G. Schaathun usó en [32] algunas cuestiones de la variedad de Segre para probar una conjetura de Wei y Yang relativa a los pesos generalizados de Hamming sobre códigos producto.

El tomar la decisión de estudiar estos tópicos no fue difícil. Son actuales, útiles en tecnología digital, criptografía, etc. Hay grupos importantes de

investigación en el mundo estudiando estos conceptos o algunos similares e íntimamente relacionados. En nuestro país se sigue impulsando el fortalecimiento de estos grupos y temas y hay gran variedad en los problemas que pueden ser abordados.

Cuando se empezaron a desarrollar algunos conceptos de Algebra Conmutativa y Geometría Algebraica nadie pensó que podrían aplicarse en cuestiones tan concretas y actuales como las que se desarrollan en este trabajo. Los conceptos de matemáticas básicas que aparecen son valiosos en sí mismos, pero adquieren doble valor al ser usados en otras ramas del conocimiento, sobre todo de caracter aplicado.

Las principales aportaciones a la teoría de códigos descritas en este trabajo para los códigos Reed-Muller asociados a la variedad de Segre son las siguientes:

- Dimensión
- $a-$invariante
- Ideal Anulador
- Distancia Mínima
- Segundo Peso Generalizado de Hamming

Además se encontró el código dual de los códigos Reed-Muller asociados a la variedad de Veronese y el correspondiente a Intersecciones Completas.

Es importante mencionar que aún hay muchos problemas abiertos en esta dirección, entre ellos:

- Describir el código dual de los códigos Reed-Muller asociados a la variedad de Segre.
- Encontrar la jerarquía de pesos de estos códigos (aquí solo se encuentran los primeros dos pesos generalizados).
- Encontrar la distancia mínima de los códigos Reed-Muller asociados a intersecciones completas.

La distribución de esta tesis es como sigue: En el **Capítulo 1** se describen algunos conceptos y resultados que son fundamentales para entender los tópicos aquí trabajados. En 1.1 se dan las definiciones elementales asociadas a los códigos lineales, sus parámetros, el código dual y la cota de Singleton. En 1.2 se dan las definiciones de la función de Hilbert y el $a-$invariante. En 1.3 se definen los objetos principales de estudio: Los códigos Reed-Muller definidos sobre ciertos subconjuntos del espacio proyectivo poniendo especial énfasis en el hecho de que la función de Hilbert da la dimensión de estos códigos. En 1.4 se recuerda el concepto de la variedad de Segre y se explica el significado de los códigos Reed-Muller definidos sobre esta variedad. En 1.5 se hace lo mismo que en 1.4 pero en el caso de la variedad de Veronese. Para este caso particular ya se conocen los parámetros básicos (ver [31]) y sólo se estudiará el dual de estos códigos. En 1.6 el proceso es nuevamente parecido pero para el caso de una intersección completa.

En el **Capítulo 2** se describen los primeros resultados de esta tesis, todos correspondientes a los códigos Reed-Muller definidos sobre la variedad de Segre. En 2.1 se encuentran la dimensión y el $a-$invariante de estos códigos; ambos conceptos quedan expresados en términos de los correspondientes a los códigos proyectivos Reed-Muller y que ya son conocidos, [29]. En 2.2 se demuestra que el ideal anulador está generado por sus componentes homogéneas de grados 2 y $q+1$. En 2.3 se encuentra el parámetro básico más importante de un código: su distancia mínima. Nuevamente el resultado obtenido queda en términos de las distancias mínimas de los códigos proyectivos correspondientes. Finalmente en 2.4 se da un ejemplo donde se describen, en ese caso particular, los principales parámetros de estos códigos. Como consequencia importante se obtiene que los códigos de este tipo no son MDS.

En el **Capítulo 3** se calcula el segundo peso generalizado de Hamming para los códigos estudiados en el capítulo anterior. En 3.1 se precisan las definiciones más importantes y los datos generales de este tópico incluyendo la distancia mínima y el segundo peso generalizado de los códigos proyectivos Reed-Muller. También se especifica la notación usada para estos códigos, en particular la forma matricial en que son representadas las palabras del código. En 3.2 se da el Teorema que calcula el segundo peso generalizado de Hamming para los códigos Reed-Muller estudiados en el capítulo 2.

En el **Capítulo 4** se calculan los duales de los códigos Reed-Muller aso-

ciados a la variedad de Veronese y los correspondientes a intersecciones completas. En 4.1 se analiza el caso de la variedad de Veronese y se encuentra su código dual. En 4.2 se analiza el caso de los códigos definidos sobre intersecciones completas y se encuentra su código dual. El espacio afín es un caso particular de esta situación y cuyo resultado ya es conocido (ver [29]). En 4.3 se da un ejemplo en un campo con 4 elementos y con una intersección completa específica en el plano proyectivo.

Finalmente, se dan las conclusiones del trabajo.

Los principales resultados correspondientes a los códigos Reed-Muller definidos sobre la variedad de Segre están por aparecer en el journal *Finite Fields and their Applications* de Elsevier Science (USA).

Chapter 1

Conceptos Generales

En este capítulo se describen algunos conceptos y resultados cuyo conocimiento será fundamental para entender los capítulos subsiguientes.

Es muy importante mencionar que los puntos del espacio proyectivo se supone que están en la siguiente forma estándard $(0, \ldots, 0, 1, a_1, a_2, \ldots, a_l)$, es decir, la primer entrada no cero del punto en cuestión es 1. Esto es para garantizar que los mapeos de evaluación dados más adelante estén bien definidos (ver (1.1), en la sección 1.3).

También vale la pena mencionar que en la literatura especializada es frecuente hablar de los puntos K-racionales de las variedades de Segre, Veronese o los de una intersección completa en vez de las variedades en sí. Sin embargo, por comodidad, hablaremos en este trabajo de las variedades indicadas y no de sus puntos K-racionales.

Notación

$\mathbb{N}$ denotará el conjunto de numeros naturales. Si L es campo, pondremos $L^* := L - \{0\}$. Si X es conjunto denotaremos por $|X|$ la cardinalidad de X. Si $x \in \mathbb{R}$ pondremos $[x]$ para denotar la parte entera de x. En este trabajo, a menos que se diga lo contrario, denotaremos por K el campo finito con $q = p^r$ elementos, donde p es primo arbitrario, esto es, $K := \mathbb{F}_q$. Por $\mathbb{P}^n(K)$ denotaremos el n-ésimo espacio proyectivo definido sobre $K = \mathbb{F}_q$.

1.1 Códigos lineales

En esta sección inicial se introducirán algunas de las nociones básicas de la teoría de códigos lineales. Para más detalles puede consultarse [22].

Consideremos el K-espacio vectorial $K^n = (\mathbb{F}_q)^n$.

***Definición* 1.1** La distancia de Hamming sobre K^n es la función

$$\delta : K^n \times K^n \to \mathbb{N} \cup \{0\}$$

$$\delta\left((a_1, \ldots, a_n), (b_1, \ldots, b_n)\right) := |\{i : a_i \neq b_i\}|.$$

La distancia de Hamming es una métrica en K^n como puede verificarse fácilmente.

***Definición* 1.2** El peso de Hamming de un elemento $a = (a_1, \ldots, a_n) \in K^n$ se define como

$$w(a) := \delta(a, 0) = |\{i : a_i \neq 0\}|.$$

***Definición* 1.3** Un código lineal C (sobre el alfabeto K) es un subespacio lineal de K^n. Los elementos de C serán las palabras del código. Llamaremos a n la longitud del código y a su dimensión $k := \dim_K C$, como $K-$espacio vectorial, la dimensión de C. En este caso, un $[n, k]-$código es un código de longitud n y dimensión k.

***Definición* 1.4** La distancia mínima, $\delta(C)$, de un código no trivial C se define como

$$\delta(C) := \min\{\delta(a, b) : a, b \in C \text{ y } a \neq b\}.$$

Por las definiciones anteriores se tiene que $\delta(a, b) = \delta(a - b, 0) = w(a - b)$, por lo que

$$\delta(C) = \min\{w(a) : 0 \neq a \in C\}$$

***Definición* 1.5** Un $[n, k]-$código C, con distancia mínima δ se denota como un $[n, k, \delta]-$código. A los enteros n, k, δ les llamaremos parámetros básicos del código correspondiente.

Para un código C con distancia mínima δ sea $t := \left[\frac{\delta-1}{2}\right]$. Si $a \in K^n$ y $\delta(a,c) \leq t$ para algún $c \in C$, entonces c es la única palabra con $\delta(a,c) \leq t$.

Lo anterior significa que si al transmitir información, se recibe el vector a, y este difiere de c en a lo más t componentes, entonces se acepta a c como la palabra transmitida. Por este hecho se dice que C es un código corrector de t errores.

***Definición* 1.6** El producto interno canónico sobre K^n está definido por

$$\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle := \sum_{i=1}^{n} a_i b_i.$$

***Definición* 1.7** Si $C \subseteq K^n$ es un código lineal, entonces el código dual de C es

$$C^{\perp} := \{u \in K^n : \langle u, a \rangle = 0 \text{ para todo } a \in C\}.$$

Uno de los más importantes problemas de la teoría de códigos es construir códigos con dimensión y distancia mínima grandes, en comparación con su longitud, debido a que la capacidad de corrección de errores depende de la distancia mínima. Sin embargo hay ciertas limitaciones en este sentido, una de ellas, la más sencilla, es la cota de Singleton:

***Proposición* 1.1 (Singleton)** *Para un $[n,k,\delta]-$código lineal C se cumple que*

$$k + \delta \leq n + 1$$

Demostración. [35], página 41. ■

***Definición* 1.8** Los códigos con $k + \delta = n + 1$ son llamados códigos MDS (códigos de máxima distancia separable).

En este trabajo se calcularán los parámetros básicos de los llamados códigos Reed-Muller definidos sobre la variedad de Segre (capítulo 2) y los duales de otras dos clases de códigos (capítulo 4).

1.2 Función de Hilbert y $a-$invariante

En esta sección se recuerda el concepto de función de Hilbert y algunos resultados que serán importantes más adelante ([4]).

Sean $K = \mathbb{F}_q$ y $A := K[X_0, \ldots, X_n] = \bigoplus_{i\geq 0} A_i$ el anillo de polinomios en las indeterminadas $X_0, \ldots, X_n$ con coeficientes en K, con la graduación natural, es decir, A_i consta de todos los polinomios homegéneos de grado i y el cero.

Sea X un subconjunto no vacío de $\mathbb{P}^n(K)$. Más adelante X jugará el papel de la variedad de Segre, la de Veronese o el de una Intersección Completa. Sea $I_X :=< f \in A : f \text{ es homogéneo y } f(P) = 0 \text{ para todo } P \in X >= \bigoplus_{i\geq 0} I_X(i)$, donde $I_X(i)$ significa la parte homogénea de grado i de I_X, el ideal anulador graduado de X en A. De igual manera, consideremos $R := A/I_X$ como el anillo coordenado del conjunto X.

***Definición* 1.9** La función de Hilbert del anillo coordenado $R = A/I_X$ se define como

$$H_X : \mathbb{N} \cup 0 \to \mathbb{N} \cup 0$$
$$H_X(d) := \dim_K A_d/I_X(d) = \dim_K A_d - \dim_K I_X(d).$$

***Proposición* 1.2** Usemos la notación anterior y sea $\gamma_X := \min\{i \geq 0 : I_X(i) \neq 0\}$, entonces existe un entero a_X de tal forma que

(I) $H_X(d) = \dim_K A_d = \binom{n+d}{n}$ si y sólo si $d < \gamma_X$.

(II) $H_X(d) < H_X(d+1) < |X|$ si $0 \leq d < a_X$.

(III) $H_X(d) = |X|$ para $d \geq a_X + 1$.

Demostración. [9], página 166. ■

***Definición* 1.10** El entero a_X de la Proposición anterior se llama el $a-$invariante de R, o el $a-$invariante de I, o incluso el $a-$invariante de X.

***Definición* 1.11** Puesto que el valor de la función de Hilbert a partir de $a_X + 1$ es constante (igual a la cardinalidad de X), este número, $a_X + 1$, se llama índice de regularidad de R.

1.3 Códigos Reed-Muller

Aquí se introducen los códigos cuyas características aparecerán en el desarrollo del presente trabajo y se analiza cuál es la importancia de la función de Hilbert cuya definición aparece en la sección anterior. Estos códigos son una generalización de los originales códigos Reed-Muller introducidos en 1954 (cf. [24], [26]).

Sea $K = \mathbb{F}_q$ y $A_d \subseteq K[X_0, \ldots, X_n]$ la colección de todos los polinomios homogéneos de grado d, y el cero.

***Definición* 1.12** Sean $d \in \mathbb{N} \cup \{0\}$ y $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$. Definimos el mapeo evaluación siguiente

$$ev_d : A_d \rightarrow K^m$$

$$ev_d(f) = (f(P_1), \ldots, f(P_m)). \tag{1.1}$$

Es claro que este mapeo es $K-$lineal. Además el núcleo de esta aplicación es $I_X(d)$.

***Definición* 1.13** El código Reed-Muller, de orden d, sobre el conjunto X, el cual se denota por $C_X(d)$, se define como la imagen del mapeo evaluación ev_d.

Esta clase de códigos será el objeto de estudio de este trabajo.

Notemos que el código $C_X(d)$ es isomorfo a $A_d/I_X(d)$ y por lo tanto

$$\dim_K C_X(d) = H_X(d).$$

Para el caso en que X es la variedad de Segre (ver sección 1.4) se determinan algunos de los parámetros de los códigos correspondientes, entre ellos

la distancia mínima y el segundo peso generalizado de Hamming, que son, en general, difíciles de determinar (capítulos 2 y 3).

Para otras dos situaciones adicionales (variedad de Veronese e Intersecciones Completas) se encontrará sólo el código dual de esta clase de códigos (capítulo 4), debido a que ya se conocen sus parámetros básicos ([6], Teorema 3.1 y [31]).

1.4 Variedad de Segre

La definición general de códigos Reed-Muller asociados al subconjunto $X \subseteq \mathbb{P}^n(K)$ es válida no importando qué características particulares tenga éste; sin embargo, buscamos qué subconjuntos del espacio proyectivo se deben ocupar para que podamos calcular los parámetros básicos de estos códigos (longitud, dimensión, distancia mínima).

Algunos investigadores han descrito varios aspectos de los códigos $C_X(d)$ para ciertos subconjuntos $X \subseteq \mathbb{P}^n(K)$. Por ejemplo, Lachaud ([21]) y después Sørensen ([34]) calcularon estos parámetros para el caso $X = \mathbb{P}^n(K)$. De hecho, C. Rentería y H. Tapia-Recillas hicieron lo propio para este caso, el caso del espacio afín y otros más ([6], [29], [31]).

Es natural, pues, elegir subconjuntos de $\mathbb{P}^n(K)$ que sean interesantes. Entre estos se encuentran las variedades de Segre, Veronese y las intersecciones completas, de las cuales se recordará su definición.

***Definición* 1.14** Sea $K = \mathbb{F}_q$. El mapeo de Segre está definido como ([15], página 25)

$$\varphi : \mathbb{P}^n(K) \times \mathbb{P}^m(K) \to \mathbb{P}^N(K),$$

$$\varphi\left(\underline{x}, \underline{y}\right) = (x_0 y_0, \ldots, x_i y_j, \ldots, x_n y_m),$$

donde

$$\underline{x} = (x_0, \ldots, x_n) \in \mathbb{P}^n(K), \qquad \underline{y} = (y_0, \ldots, y_m) \in \mathbb{P}^m(K),$$
$$N = (m+1)(n+1) - 1.$$

Obsérvese que el mapeo φ está bien definido y es inyectivo.

***Definición* 1.15** La imagen S de la aplicación φ es conocida como la variedad (proyectiva) de Segre, ([16]), i.e.,

$$S = \varphi\left(\mathbb{P}^n(K) \times \mathbb{P}^m(K)\right) = \left\{P_{ij} \in \mathbb{P}^N(K) : P_{ij} = \varphi\left(P_i, Q_j\right)\right\}$$

donde $P_i \in \mathbb{P}^n(K)$, $Q_j \in \mathbb{P}^m(K)$, $i \in \{1, \ldots, k_1\}$, $j \in \{1, \ldots, k_2\}$ con $k_1 = |\mathbb{P}^n(K)| = \frac{q^{n+1}-1}{q-1}$, $k_2 = |\mathbb{P}^m(K)| = \frac{q^{m+1}-1}{q-1}$.

En este caso $C_S(d)$ es la imagen del mapeo de evaluación

$$K[Z_{00}, \ldots, Z_{ij}, \ldots, Z_{nm}]_d \to K^{k_1 k_2},$$

$$f \to \left(f\left(P_{11}\right), \ldots, f\left(P_{k_1 k_2}\right)\right).$$

***Definición* 1.16** El código $C_S(d)$ le llamaremos el código Reed-Muller de orden d asociado a la variedad de Segre.

En el capítulo 2 se determinan los parámetros de estos códigos.

Vale la pena mencionar que en el caso en que K es un campo algebraicamente cerrado, $I_S = \langle I_S(2)\rangle$. Más aún, si $Z_{ij} = X_i Y_j$, entonces ([15], [8])

$$I_S = \langle Z_{ij}Z_{kl} - Z_{il}Z_{kj} : i, k = 0, \ldots, n \ , \ j, l = 0, \ldots, m\rangle \tag{1.2}$$

1.5 Variedad de Veronese

Otro subconjunto del espacio proyectivo sobre el cual se han estudiado algunos códigos lineales ([27], [31]) es la variedad de Veronese de la cual a continuación se recuerda su definición.

***Definición* 1.17** El mapeo de Veronese ν_n de grado n, está dado por ([8], [15], [16])

$$\nu_n : \mathbb{P}^m(K) \to \mathbb{P}^N(K),$$

$$\nu_n(\underline{z}) = (\ldots, M(\underline{z}), \ldots)$$

donde $\underline{z} = (z_0, \ldots, z_m) \in \mathbb{P}^m(K)$ y $M(\underline{z})$ corre sobre todos los monomios de grado n en las variables $Z_0, \ldots, Z_m$ y $N = \binom{n+m}{n} - 1$.

***Definición* 1.18** La imagen del mapeo ν_n es conocida como la variedad de Veronese (se acostumbra decir de grado n, pero por comodidad usaremos de manera implícita el valor de n y nos referiremos a ella simplemente como la variedad de Veronese), la cual denotaremos por V.

En este caso, $C_V(d)$ es la imagen del mapeo siguiente

$$K[Y_0, \ldots, Y_N]_d \to K^{|V|},$$

$$f \to (f(\ldots, M, \ldots)(Q_1), \ldots, f(\ldots, M, \ldots)(Q_{k_2}))$$

donde $k_2 = |\mathbb{P}^m(K)|$ y $\mathbb{P}^m(K) = \{Q_1, \ldots, Q_{k_2}\}$.

***Definición* 1.19** Al código $C_V(d)$ le llamaremos el código Reed-Muller de orden d sobre la variedad de Veronese.

Para los códigos Reed-Muller asociados a la variedad de Veronese sobre el campo K ya se han calculado los parámetros principales ([31], Lema 2 y Teorema 1, página 4).

Resta calcular, y se hará en el capítulo 4, el dual de este tipo de códigos. Esta es la razón por la que introducimos los conceptos de esta sección.

1.6 Intersecciones Completas

***Definición* 1.20** Un subconjunto $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$, se llama una intersección completa ([15], [16]) si su ideal anulador está generado por una sucesión regular de n elementos, es decir, $I_X = \langle F_1, \ldots, F_n \rangle$ y la clase de F_i en el anillo $A/\langle F_1, \ldots, F_{i-1} \rangle$ no es un divisor de cero para $i = 1, \ldots, n$.

***Definición* 1.21** El código lineal $C_X(d)$, que llamaremos el código Reed-Muller de orden d asociado a la intersección completa X, es en este caso la imagen del mapeo de evaluación siguiente

$$ev_X(d) : K\left[X_0, \ldots, X_n\right]_d \to K^m,$$

$$f \to \left(f\left(P_1\right), \ldots, f\left(P_m\right)\right).$$

Ya se han descrito varias de las propiedades de estos códigos Reed-Muller asociados a Intersecciones Completas, (cf. [6]). Sin embargo todavía es un problema abierto el determinar su distancia mínima.

En [6] pueden encontrarse algunos ejemplos de intersecciones completas: el espacio afín, los K-puntos racionales de la cuártica de Klein cuando K es un campo con ocho elementos, los K-puntos racionales de la curva Hermitiana y el conjunto, la línea proyectiva, que determina al código Reed-Solomon doblemente extendido.

En el capítulo 4 se describirá el dual de esta clase de códigos.

Chapter 2

Códigos Reed-Muller sobre la variedad de Segre

La definición de los códigos Reed-Muller asociados a la variedad de Segre fue hecha en la sección 1.4 del capítulo 1. Aquí se usará la notación que ahí fue introducida, recordando que S es la variedad de Segre.

Vale la pena comentar que recientemente, cf. [32], la variedad de Segre se usó para probar una conjetura de Wei y Yang (cf. [39]) relativa a los pesos generalizados de Hamming sobre códigos producto, lo que pone de manifiesto la importancia de su estudio.

En este capítulo se calculan la dimensión (sección 2.1) y la distancia mínima (sección 2.3) de esta clase de códigos. Además se describe el ideal anulador del anillo coordenado correspondiente. Finalmente se da un ejemplo que permite ilustrar los conceptos anteriores.

Es importante mencionar que los resultados de este capítulo serán publicados en el journal *Finite Fields and their Applications* de Elsevier Science, USA ([10]).

2.1 Dimensión y $a-$invariante

Sea $K = \mathbb{F}_q$. Utilizaremos la notación: $A_N := K[Z_{00}, \ldots, Z_{nm}]$ con $N = (m+1)(n+1)-1$ y para escribir los monomios, digamos $X_0^{i_0} \cdots X_n^{i_n}$ se usará

$\underline{X}^I$, para $Y_0^{j_0} \cdots Y_m^{j_m}$ se usará $\underline{Y}^J$; además, $|I| := \sum_{s=0}^{n} i_s$, $|J| := \sum_{s=0}^{m} j_s$.

Notemos que $|S| = |\mathbb{P}^n(K)| \cdot |\mathbb{P}^m(K)| = k_1 k_2$ (pues el mapeo de Segre es inyectivo) con $k_1 = |\mathbb{P}^n(K)|$ y $k_2 = |\mathbb{P}^m(K)|$.

Además, puesto que será fundamental en las siguientes demostraciones, es necesario introducir algunas definiciones para el caso de la cerradura algebraica: Sea $\overline{K}$ la cerradura algebraica de K y $\overline{S}$ la imagen del mapeo

$$\overline{\varphi} : \mathbb{P}^n(\overline{K}) \times \mathbb{P}^m(\overline{K}) \to \mathbb{P}^N(\overline{K}),$$

$$\overline{\varphi}\left(\underline{x}, \underline{y}\right) = (x_0 y_0, \ldots, x_i y_j, \ldots, x_n y_m).$$

Además $\overline{A}_N := \overline{K}[Z_{00}, \ldots, Z_{nm}]$ y sea $I_{\overline{S}}$ el ideal anulador de $\overline{S}$.

***Observación* 1** Puesto que $\overline{K}$ es algebraicamente cerrado, es conocido que ([15], página 51):

$$I_{\overline{S}} = \langle I_{\overline{S}}(2) \rangle .$$

***Observación* 2** En [29], Proposición 8, página 406, se demuestra que

$$I_{\mathbb{P}^n(K)} = \left\langle X_i^q X_j - X_i X_j^q : \ 0 \leq i < j \leq n \right\rangle .$$

Sea $B := K[X_0 Y_0, \ldots, X_n Y_m]$ la subálgebra de $K[X_0, \ldots, X_n, Y_0, \ldots, Y_m]$ con la graduación dada por

$$B_d = \left\{ \sum_{I,J} a_{I,J} \underline{X}^I \underline{Y}^J : a_{I,J} \in K \ , \ |I| = |J| = d \right\}, d \geq 0 \qquad (2.1)$$

Esto quiere decir que $B = \bigoplus_{d \geq 0} B_d$.

El siguiente resultado es el primer escalón que permitirá llegar al objetivo de esta sección: determinar la dimensión del código Reed-Muller de orden d definido sobre la variedad de Segre, $C_S(d)$.

Lema 1 *Si $N=(m+1)(n+1)-1$, S la variedad de Segre y $d\geq 2$ entonces el núcleo de la transformación lineal suprayectiva*

$$\theta : A_N(d) \to B_d \quad , \quad f \to \theta_f \tag{2.2}$$

donde $\theta_f\left(\underline{X},\underline{Y}\right)=f\left(X_0Y_0,\ldots,X_nY_m\right)$ es $I_S(2)A_N(d-2)$

Demostración. (i) Verifiquemos que $I_S(2)A_N(d-2)\subseteq \ker\theta$.

En efecto, sea $f=\sum_{i=1}^{s} g_ih_i$ con $g_i\in I_S(2)$, $h_i\in A_N(d-2)$. En este caso

$$\theta_f\left(\underline{x},\underline{y}\right)=\sum_{i=1}^{s} g_i\left(x_0y_0,\ldots,x_ny_m\right)h_i\left(x_0y_0,\ldots,x_ny_m\right)$$

y como $g_i\in I_S(2)$ concluimos que $g_i\left(x_0y_0,\ldots,x_ny_m\right)=0$ para todo $i=1,\ldots,s$. Por tanto $\theta_f\equiv 0$ y en consecuencia $f\in\ker\theta$.

(ii) Probemos que $\ker\theta\subseteq I_S(2)A_N(d-2)$.

Sea $f\in\ker\theta$. Se sigue de la observación 1 que $\ker\theta\subseteq I_{\overline{S}}=\langle Q_{ij}\rangle$ con $Q_{ij}\in I_S(2)$, de hecho los Q_{ij} son los polinomios homogéneos de grado dos que aparecen en (1.2) de la sección 1.4. Tomando algún orden monomial, por ejemplo el orden LEX(icográfico)

$$Z_{00}>Z_{01}>\cdots>Z_{0m}>Z_{10}>Z_{11}>\cdots>Z_{1m}>\cdots>Z_{nm}$$

por el algoritmo de la división generalizado, podemos escribir $f=\sum_{i,j}\lambda_{ij}Q_{ij}+$ r, donde $\lambda_{ij}\in A_N(d-2)$, $\mathrm{r}\in A_N$ y r no es divisible por los términos líderes de los Q_{ij}. Puesto que, por definición, $\{Q_{ij}\}$ forma una base de Gröbner para $I_{\overline{S}}$, entonces $\mathrm{r}=0$ (pues $f\in I_{\overline{S}}$). Por tanto, $f=\sum_{i,j}\lambda_{ij}Q_{ij}\in I_S(2)A_N(d-2)$.

(i) y (ii) prueban la igualdad requerida. ■

El siguiente resultado será útil para determinar la función de Hilbert del anillo A_N/I_S.

Sea

$$V_d:=A_m(d)I_{\mathbb{P}^n(K)}(d)+A_n(d)I_{\mathbb{P}^m(K)}(d)\subseteq B_d,$$

donde $A_m=K\left[Y_0,\ldots,Y_m\right]$ y $A_n=K\left[X_0,\ldots,X_n\right]$.

***Proposición* 1** *$I_S(d)$ es el núcleo de la transformación lineal suprayectiva $\pi \circ \theta$, donde*

$$A_N(d) \xrightarrow{\theta} B_d \xrightarrow{\pi} B_d/V_d \tag{2.3}$$

con $f \to \theta_f \to \theta_f + V_d$.

Demostración. (i) Verifiquemos que $\ker(\pi \circ \theta) \subseteq I_S(d)$.

Si $f \in \ker(\pi \circ \theta)$ entonces $\theta_f \in V_d$, digamos que $\theta_f = \sum_{i=1}^{s} h_i m_i + \sum_{j=1}^{l} M_j T_j$ con $h_i \in I_{\mathbb{P}^n}(d)$, $m_i \in A_m(d)$, $M_j \in A_n(d)$, $T_j \in I_{\mathbb{P}^m}(d)$ para todo $i = 1, \ldots, s$, $j = 1, \ldots, l$. En este caso $f(\varphi(P,Q)) = \theta_f(P,Q) = 0$ para todo $P \in \mathbb{P}^n(K)$, $Q \in \mathbb{P}^m(K)$ por lo que $f(P_{ij}) = 0$ para cada $P_{ij} \in S$. Esto prueba que $f \in I_S(d)$.

(ii) Probemos que $I_S(d) \subseteq \ker(\pi \circ \theta)$.

Sea $f \in I_S(d)$, i.e., $\theta_f(P,Q) = 0$ para todo $P \in \mathbb{P}^n(K)$, $Q \in \mathbb{P}^m(K)$, es decir, $\theta_f \in I_{\mathbb{P}^s(K)}$ con $s = m+n+1$. Para demostrar lo que se quiere, consideremos los siguientes tres casos:

(I) $2d < q+1$.

Por la observación 2 se tiene que $I_{\mathbb{P}^s(K)} = \langle X_i^q X_j - X_i X_j^q : \ 0 \le i < j \le s \rangle$. Luego $\theta_f \equiv 0$ ó $\deg(\theta_f) \ge q+1$, pero como $\theta_f \in B_d$, $\deg(\theta_f) = 2d < q+1$, se concluye que $\theta_f \equiv 0$ y en tal caso $f \in \ker(\pi \circ \theta)$.

(II) $2d \ge q+1$, $d < q+1$.

Puesto que $\theta_f \in I_{\mathbb{P}^s(K)} = \langle W_i^q W_j - W_i W_j^q : 0 \le i < j \le s \rangle$ con $\{W_i\}_{i=1}^{s} = \{X_0, \ldots, X_n, Y_0, \ldots, Y_m\}$ (observación 2) y dado que $\theta_f \in B_d$ (donde los polinomios son bi-homogéneos con bi-grado d), necesariamente tenemos que $\theta_f \in \langle X_i^q X_j - X_i X_j^q \ , \ Y_k^q Y_l - Y_k Y_l^q : 0 \le i < j \le n \ , \ 0 \le k < l \le m \rangle$, es decir, $\theta_f = \sum_{i,j} m_{ij} \left(X_i^q X_j - X_i X_j^q\right) + \sum_{k,l} M_{kl} \left(Y_k^q Y_l - Y_k Y_l^q\right)$ con m_{ij}, M_{kl} polinomios homogéneos de grado $2d-(q+1)$. Pero en este caso obtendríamos que $d \ge q+1$ lo que implica que $\theta_f \equiv 0$ y en consecuencia $\theta_f \in V_d$, es decir, $f \in \ker(\pi \circ \theta)$.

(III) $d \ge q+1$.

De manera equivalente al caso (II), sea

$$\theta_f = \sum_{i,j} m_{ij} \left(X_i^q X_j - X_i X_j^q \right) + \sum_{k,l} M_{kl} \left(Y_k^q Y_l - Y_k Y_l^q \right)$$

pero en este caso podemos escribir

$$\theta_f = \sum_{i,j} m_{ij}^{'} \left(X_i^q X_j - X_i X_j^q \right) m_{ij}^{''} + \sum_{k,l} M_{kl}^{'} \left(Y_k^q Y_l - Y_k Y_l^q \right) M_{kl}^{''}$$

(agrupando las X's entre ellas y lo mismo para las Y's) con $m_{ij}^{''} \in A_m(d)$ y $M_{kl}^{''} \in A_n(d)$. Además es obvio que $m_{ij}^{'} \left(X_i^q X_j - X_i X_j^q \right) \in I_{\mathbb{P}^n(K)}(d)$ y $M_{kl}^{'} \left(Y_k^q Y_l - Y_k Y_l^q \right) \in I_{\mathbb{P}^m(K)}(d)$. Esto prueba que $\theta_f \in V_d$ y por tanto $f \in \ker(\pi \circ \theta)$.

De (i) y (ii) se sigue la afirmación. ■

***Observación* 3** De la demostración anterior obtenemos (ver partes (I) y (II)) que si $f \in I_S(d)$ con $d < q+1$ entonces $\theta_f \equiv 0$ y usando el Lema 1 concluimos que $f \in I_S(2) A_N(d-2)$. Resumiendo: $I_S(d) \subseteq \langle I_S(2) \rangle$ si $d < q+1$.

Esta observación será parte importante para la descripción del ideal anulador de S que en la siguiente sección se explica.

Como resultado de la proposición anterior obtenemos la dimensión de los códigos Reed-Muller asociados a la variedad de Segre y el $a-$invariante del correspondiente anillo A_N/I_S. Los siguientes dos Corolarios son los resultados más importantes de esta sección.

***Corolario* 1** *La función de Hilbert del anillo A_N/I_S está dada por*

$$H_S(d) = H_{\mathbb{P}^n(K)}(d) \cdot H_{\mathbb{P}^m(K)}(d) \tag{2.4}$$

Demostración. Se sigue de la proposición anterior que $A_N(d)/I_S(d) \cong B_d/V_d$. Además, usando la propiedad universal del producto tensorial y los mapeos naturales, se verifica que

$$B_d/V_d \cong A_n(d)/I_{\mathbb{P}^n(K)}(d) \otimes_K A_m(d)/I_{\mathbb{P}^m(K)}(d).$$

Luego, $A_N(d)/I_S(d) \cong A_n(d)/I_{\mathbb{P}^n(K)}(d) \otimes_K A_m(d)/I_{\mathbb{P}^m(K)}(d)$ de donde se sigue la afirmación. ■

***Observación* 4** En [29], Proposición 12, página 409, se obtiene el valor de la función de Hilbert para el caso del espacio proyectivo $\mathbb{P}^n(K)$, $K = \mathbb{F}_q$:

$$H_{\mathbb{P}^n(K)}(d) = \sum_{j=0}^{n} \sum_{i=0}^{j} (-1)^i \binom{j}{i} \binom{j+d-1-iq}{d-1-iq},\ d > 0$$

donde $\binom{a}{b}$ es un coeficiente binomial generalizado, es decir, $\binom{\nu}{\nu} = 1$ para todo ν en $\mathbb{Z}$ y $\binom{k}{t} = 0$ si $k < t$. Por tanto, con el Teorema anterior, sabemos cual es la dimensión de los códigos Reed-Muller asociados a la variedad de Segre.

***Corolario* 2** *Denotemos por a_S el $a-$invariante del anillo A_N/I_S donde S es la variedad de Segre. Entonces a_S viene dado por:*

$$a_S = \max\{n(q-1), m(q-1)\} \tag{2.5}$$

donde n y m son los mismos que en la definición de la variedad de Segre.

Demostración. En [29], proposición 10, se prueba que $a_{\mathbb{P}^n(K)} = n(q-1)$, $a_{\mathbb{P}^m(K)} = m(q-1)$. El resultado es inmediato del Corolario anterior y del hecho de que $H_S(d) < k_1 k_2$ si $d \leq \max\left\{a_{\mathbb{P}^n(K)}, a_{\mathbb{P}^m(K)}\right\}$ y $H_S(d) = k_1 k_2$ en el caso en que $d > \max\left\{a_{\mathbb{P}^n(K)}, a_{\mathbb{P}^m(K)}\right\}$ donde $k_1 = |\mathbb{P}^n(K)|$ y $k_2 = |\mathbb{P}^m(K)|$. ■

2.2 Ideal anulador

La siguiente proposición describe el ideal anulador de S detallando sus generadores.

***Proposición* 2** *Sean $K = \mathbb{F}_q$ y S la variedad de Segre. El ideal anulador I_S está dado por*

$$I_S = \langle I_S(2), I_S(q+1) \rangle . \tag{2.6}$$

Demostración. (i) $d < q + 1$.

Por la observación 3 sabemos que en este caso $I_S(d) \subseteq \langle I_S(2) \rangle$. Basta entonces probar esta inclusión para el caso $d > q + 1$.

(ii) $d > q + 1$.

Es suficiente verificar que $I_S(d) \subseteq \sum_{i,j} Z_{ij} I_S(d-1)$. Usando la notación de la proposición 1, sea

$$\theta_f = \sum_{i,j} m_{ij} \left(X_i^q X_j - X_i X_j^q \right) + \sum_{k,l} M_{kl} \left(Y_k^q Y_l - Y_k Y_l^q \right).$$

Puesto que $d > q + 1$ y que $\theta_f \in B_d$, podemos escribir

$$\theta_f = \sum_{i,j} (X_i Y_j) F_{ij} \left(X_i^q X_j - X_i X_j^q \right) + \sum_{k,l} \left(X_k Y_l \right) F'_{kl} \left(Y_k^q Y_l - Y_k Y_l^q \right).$$

Luego, $\theta_f = \sum_{i,j} X_i Y_j \tau_{ij}$ con $\tau_{ij} \in I_{\mathbb{P}^s(K)}$ $(2d-2)$. Entonces $f = \sum_{i,j} Z_{ij} \tau'_{ij}$ con $\tau'_{ij} \in I_S(d-1)$. ■

Tenemos hasta ahora la dimensión del código $C_S(d)$, el $a-$invariante e ideal anulador para el caso de la variedad de Segre. En la siguiente sección se calcula otro de los parámetros: la distancia mínima.

2.3 Distancia Mínima

Uno de los parámetros básicos de un código lineal es su distancia mínima. Este parámetro es muy importante pues es el que permite detectar el número de errores que puede corregir este código ([22]).

Sea $K = \mathbb{F}_q$. Para calcular la distancia mínima $\delta_S(d)$ de $C_S(d)$, con S la variedad de Segre, se usará $\delta_{\mathbb{P}^n(K)}(d)$ y $\delta_{\mathbb{P}^m(K)}(d)$ para las distancias mínimas de los códigos proyectivos Reed-Muller $C_{\mathbb{P}^n(K)}(d)$ y $C_{\mathbb{P}^m(K)}(d)$ respectivamente.

***Teorema* 1** *Sean $K = \mathbb{F}_q$, S la variedad de Segre y $C_S(d)$ el código Reed-Muller de orden d definido sobre S. La distancia mínima del código $C_S(d)$ está dada por*

$$\delta_S(d) = \delta_{\mathbb{P}^n(K)}(d) \cdot \delta_{\mathbb{P}^m(K)}(d) \tag{2.7}$$

Más aún, si $d \leq min\{n(q-1), m(q-1)\}$,

$$\delta_S(d) = [(q-s)\, q^{n-r-1}] \cdot [(q-s)\, q^{m-r-1}] \tag{2.8}$$

donde $d-1 = r\,(q-1)+s$, $0 \leq s < q-1$.

Demostración. Sean $f \in A_N(d)$ y $S = \{P_{11}, \ldots, P_{k_1k_2}\}$ donde $k_1 = |\mathbb{P}^n(K)|$ y $k_2 = |\mathbb{P}^m(K)|$. Sea $\Lambda = (f(P_{11}), \ldots, f(P_{k_1k_2})) \in C_S(d) - \{0\}$. Si φ es el mapeo de Segre, entonces para todo i, j existen $P_i \in \mathbb{P}^n(K)$, $Q_j \in \mathbb{P}^m(K)$ de tal forma que $\varphi(P_i, Q_j) = P_{ij}$. Por tanto:

$$\Lambda = (f(X_0Y_0, \ldots, X_nY_m)(P_1, Q_1), \ldots, f(X_0Y_0, \ldots, X_nY_m)(P_{k_1}, Q_{k_2})).$$

donde $f(X_0Y_0, \ldots, X_nY_m) = \sum_{i,j} a_{I,J}\underline{X}^I\underline{Y}^J$. Para cada $P \in \mathbb{P}^n(K)$ (respectivamente $Q \in \mathbb{P}^m(K)$) definamos $f_P(\underline{Y}) := \sum_{i,j} a_{I,J}P^I\underline{Y}^J \in A_m(d)$ (respectivamente $f_Q(\underline{X}) = \sum_{i,j} a_{I,J}\underline{X}^IQ^J \in A_n(d)$).

Para cada $i = 1, \ldots, k_1$, sea $\Lambda_i := (f_{P_i}(Q_1), \ldots, f_{P_i}(Q_{k_2})) \in C_{\mathbb{P}^m(K)}(d)$ y $k_3 :=| \{i : \Lambda_i \neq 0\} |> 0$.

Dado que $\omega(\Lambda_i) \geq \delta_{\mathbb{P}^m(K)}(d)$ para todo i tal que $\Lambda_i \neq 0$, entonces $\omega(\Lambda) \geq k_3\delta_{\mathbb{P}^m(K)}(d)$, (donde $\omega(\Lambda_i)$ denota el peso de Hamming de Λ_i).

De manera similar, tomemos $\Gamma_j := \left(f_{Q_j}(P_1), \ldots, f_{Q_j}(P_{k_1})\right) \in C_{\mathbb{P}^n(K)}(d)$ para cada $j \in \{1, \ldots, k_2\}$. Sea j tal que $\Gamma_j \neq 0$. Si $k_3 < \delta_{\mathbb{P}^n(K)}(d)$ entonces $\omega(\Gamma_j) \leq k_3 < \delta_{\mathbb{P}^n(K)}(d)$ lo cual no es posible ya que $\Gamma_j \in C_{\mathbb{P}^n(K)}(d)$. Por tanto $k_3 \geq \delta_{\mathbb{P}^n(K)}(d)$ y en consecuencia $\omega(\Lambda) \geq \delta_{\mathbb{P}^n(K)}(d) \cdot \delta_{\mathbb{P}^m(K)}(d)$.

Para finalizar la demostración es suficiente encontrar una palabra del código $C_S(d)$ cuyo peso sea exactamente $\delta_{\mathbb{P}^n(K)}(d) \cdot \delta_{\mathbb{P}^m(K)}(d)$.

Consideremos $\Omega_1 := (g(P_1), \ldots, g(P_{k_1})) \in C_{\mathbb{P}^n(K)}(d)$ con $\omega(\Omega_1) = \delta_{\mathbb{P}^n(K)}(d)$ y $g \in A_n(d)$, (respectivamente $\Omega_2 := (h(Q_1), \ldots, h(Q_{k_2})) \in C_{\mathbb{P}^m(K)}(d)$ con $\omega(\Omega_2) = \delta_{\mathbb{P}^m(K)}(d)$ y $h \in A_m(d)$). Puesto que el mapeo θ (definido en la sección 2.1 de este capítulo) es suprayectivo, sea $F \in A_N(d)$ tal que:

$$(gh(P_1,Q_1),\ldots,gh(P_{k_1},Q_{k_2})) = (F(\varphi(P_1,Q_1)),\ldots,F(\varphi(P_{k_1},Q_{k_2}))) =: \Omega \in C_S(d).$$

En este caso $\omega(\Omega) = \delta_{\mathbb{P}^n(K)}(d) \cdot \delta_{\mathbb{P}^m(K)}(d)$. ■

***Observación* 5** De [29], Proposición 18, página 412, sabemos que la distancia mínima del Código proyectivo Reed-Muller $C_{\mathbb{P}^n(K)}(d)$, cuando $d \leq n(q-1)$, es $\delta_{\mathbb{P}^n(K)}(d) = (q-s)\,q^{n-r-1}$ donde, por algoritmo de la división existen $r, s \in \mathbb{Z}$ tales que $d-1 = r(q-1)+s$, $0 \leq s < q-1$. Se sigue que

$$\delta_S(d) = [(q-s)\,q^{n-r-1}] \cdot [(q-s)\,q^{m-r-1}].$$

En la sección siguiente se ejemplificará el Teorema 2 junto con los resultados descritos en este Capítulo.

2.4 Ejemplo

Ilustramos los principales resultados obtenidos, correspondientes a los códigos Reed-Muller asociados a la variedad de Segre, con el siguiente ejemplo.

***Ejemplo* 2.1** Sea $K = \mathbb{F}_4 = \{0, 1, a, a^2\}$ con a un elemento primitivo de K y $\varphi : \mathbb{P}^1(K) \times \mathbb{P}^1(K) \to \mathbb{P}^3(K)$ el mapeo de Segre. Nótese que en este caso $k_1 = k_2 = |\mathbb{P}^1(K)| = 5$ y por tanto $|S| = 25$, de hecho:

$$\begin{gathered} S = \{(0,0,0,1),(0,0,1,0),(0,1,0,0),(1,0,0,0),(0,0,1,a),\\ (0,0,1,a^2),(0,0,1,1),(0,1,0,a),(1,a,a,a^2),(1,0,a,0),\\ (1,a^2,a,1),(1,1,a,a),(1,a,0,0),(1,a^2,0,0),(1,1,0,0),\\ (0,1,0,a^2),(1,a,a^2,1),(1,0,a^2,0),(1,a^2,a^2,a),(1,1,a^2,a^2),\\ (0,1,0,1),(1,a,1,a),(1,0,1,0),(1,a^2,1,a^2),(1,1,1,1)\} \end{gathered}$$

Del Corolario 2 se sigue que $a_S = 3$. Para este ejemplo concreto se tomará $d = 2$. Por la observación 4 se tiene que $H_{\mathbb{P}^1}(2) = 3$ y por tanto, por el Corolario 1, $H_S(2) = 9$. Por consiguiente $\dim_K C_S(2) = 9$.

De la proposición 1 se sigue que $I_S = \langle I_S(2), I_S(5)\rangle$. Si $Z_{00}, Z_{10}, Z_{01}, Z_{11}$ representan las coordenadas de $\mathbb{P}^3(K)$, un conjunto de generadores para I_S es:

$$\{Z_{10}Z_{01} - Z_{00}Z_{11}, Z_{01}^4Z_{11} - Z_{01}Z_{11}^4, Z_{00}Z_{01}^3Z_{11} - Z_{00}Z_{11}^4, Z_{00}^2Z_{01}^2Z_{11} - \\ -Z_{00}Z_{10}Z_{11}^3, Z_{00}^3Z_{01}Z_{11} - Z_{00}Z_{10}^2Z_{11}^2, Z_{10}^4Z_{11} - Z_{10}Z_{11}^4, Z_{00}Z_{10}^3Z_{11} - \\ -Z_{00}Z_{11}^4, Z_{00}^2Z_{10}^2Z_{11} - Z_{00}Z_{01}Z_{11}^3, Z_{00}^3Z_{10}Z_{11} - Z_{00}Z_{01}^2Z_{11}^2, Z_{00}^4Z_{11} - \\ -Z_{00}Z_{11}^4, Z_{00}^4Z_{01} - Z_{00}Z_{01}^4, Z_{00}^4Z_{10} - Z_{00}Z_{10}^4\}$$

Ahora bien, si tomamos $Z_{ij} = X_iY_j$ para todo $i = 0, 1$, $j = 0, 1$ es fácil verificar que los generadores del ideal I_S pueden obtenerse de los elementos del $K-$espacio vectorial

$$W := \left[I_{\mathbb{P}^1(K)}(2) \otimes_K A_1(2)\right] \oplus \left[A_1(2) \otimes_K I_{\mathbb{P}^1(K)}(2)\right] \tag{2.9}$$

Por ejemplo si $Y_0Y_1^4\left(X_0^4X_1 - X_0X_1^4\right) \in W$ entonces

$$Y_0Y_1^4\left(X_0^4X_1 - X_0X_1^4\right) = \left(X_0Y_0\right)\left(X_0^3Y_1^3\right)\left(X_1Y_1\right) - X_0Y_0\left(X_1Y_1\right)^4 = Z_{00}Z_{01}^3 \\ Z_{11} - Z_{00}Z_{11}^4 \in I_S.$$

Por supuesto que podemos escoger de múltiples formas los elementos de W. Esta es una forma sencilla para obtener a un conjunto de generadores de I_S.

Además, según el Teorema 2, $\delta_S(2) = 9$, pues por la observación 5 de la misma sección, $\delta_{\mathbb{P}^1(K)}(2) = 3$. Se sigue que esta clase de códigos no es, en general, MDS.

Por otra parte, una base para $A_3(2)/I_S(2)$ es

$$\{Z_{00}^2, Z_{00}Z_{01}, Z_{00}Z_{10}, Z_{00}Z_{11}, Z_{01}^2, Z_{01}Z_{11}, Z_{10}^2, Z_{10}Z_{11}, Z_{11}^2\}.$$

De la base anterior puede ser obtenida una matriz generadora del código $C_S(d)$.

Los cálculos de este ejemplo fueron realizados con la ayuda del paquete de computación *Macaulay2* ([13]).

En el siguiente capítulo se describirá el segundo peso generalizado de los códigos Reed-Muller asociados a la variedad de Segre.

Chapter 3

Segundo peso generalizado de Hamming

En este capítulo se determina el segundo peso generalizado de Hamming en el caso de los códigos tratados en el capítulo anterior (Códigos Reed-Muller sobre la variedad de Segre). Los pesos generalizados de Hamming fueron introducidos por V.K. Wei en [38]. La razón original de su estudio fue un problema de Criptografía (codes for wire-tap channels of type II, [25]) y además constituyen una generalización natural del concepto de distancia mínima (el primero de estos pesos es precisamente la distancia mínima del código). Este tópico es de gran importancia en los estudios recientes de teoría de códigos debido a que tiene múltiples aplicaciones, entre las que se cuentan: funciones $t-$elásticas, complejidad de ramificación en códigos lineales y clasificación de códigos ([2], [7], [20]).

3.1 Notación y definiciones básicas

Para mayor información sobre este tema pueden consultarse [17], [37] y [38].

***Definición* 3.1** Sean $K = \mathbb{F}_q$ y $C \subseteq K^n$ un $[n, k] -$ código lineal. Se define el soporte de C como

$$\operatorname{sop}(C) := \{j : \text{ existe un elemento } x = (x_1, \ldots, x_n) \in C \text{ con } x_j \neq 0\}.$$

***Definición* 3.2** Si C es un $[n,k]-$código lineal y $1 \leq r \leq k$, el $r-$ésimo peso generalizado de Hamming de C está definido como

$$d_r(C) := \min\{|\mathrm{sop}(D)| : D \text{ es un subcódigo de dimensión } r \text{ de } C\}.$$

Obviamente $d_1(C) = \delta(C) =$ distancia mínima de C.

Los pesos generalizados de Hamming han sido determinados en varias situaciones particulares ([37]), entre ellas: códigos asociados a variedades hermitianas, Grassmanianas, superficies del Pezzo, códigos de Goppa y códigos BCH.

También es importante mencionar que estos conceptos tienen una interpretación geométrica. En este caso el valor de $n - d_r(C)$ es igual con

$$\max\left\{|X \cap \Pi| : \Pi \text{ es un subespacio proyectivo de codimensión } r \text{ en } \mathbb{P}^{k-1}(K)\right\}$$

donde X es un sistema proyectivo ([37], página 1564).

Además estos pesos generalizados de Hamming tienen varias propiedades que son importantes, entre ellas se cuentan las siguientes

***Proposición* 3.1** *Si C es un $[n,k]-$código lineal con $d_1 \geq 1$ entonces*

$$0 < d_1 < d_2 < \cdots < d_k = n$$

Demostración. [37], Proposición 3.1, página 1565. ■

***Proposición* 3.2** *Sean C un $[n,k]-$código lineal y d_r su $r-$ésimo peso generalizado de Hamming. Entonces*

$$r \leq d_r \leq n - k + r \qquad \textit{(cota tipo Singleton)}$$

Demostración. [37], Corolario 3.1, página 1566. ■

***Definición* 3.3** Un $[n,k]-$código lineal es llamado $r-$MDS, si para algún r, con $1 \leq r \leq k$, se cumple que $d_r = n - k + r$.

Notemos que este concepto es la generalización natural de los códigos MDS (caso $r = 1$).

Las propiedades anteriores son válidas en general para cualquier tipo de códigos lineales definidos sobre campos finitos. Sin embargo estamos interesados sólo en el caso de los códigos del capítulo 2. Para obtener el resultado importante en este sentido (segundo peso generalizado de Hamming) se requiere conocer la distancia mínima (primer peso generalizado de Hamming) y el segundo peso generalizado de Hamming en el caso de los códigos proyectivos Reed-Muller. Estas dos cantidades ya son conocidas y su valor es:

***Proposición* 3.3** *La distancia mínima del código proyectivo Reed-Muller de orden $\nu \leq q$, $C_{\mathbb{P}^m}(K)$, con $K = \mathbb{F}_q$ está dada por*

$$d_1\left(C_{\mathbb{P}^m(K)}(\nu)\right) = q^m + (1-\nu)\, q^{m-1}.$$

Demostración. [37], Corolario 7.4 a), página 1577.■

***Proposición* 3.4** *El segundo peso generalizado de Hamming del código proyectivo Reed-Muller de orden $\nu < q$, $C_{\mathbb{P}^m}(K)$, con $K = \mathbb{F}_q$ está dado por*

$$d_2\left(C_{\mathbb{P}^m(K)}(\nu)\right) = q^m + (2-\nu)\, q^{m-1} - q^{m-2}.$$

Demostración. [37], Corolario 7.4 b), página 1577. ■

***Observación* 6** Las Proposiciones 3.3 y 3.4, además de un cálculo directo, muestran que si $\nu < q$ entonces

$$d_1\left(C_{\mathbb{P}^m(K)}(\nu)\right) \cdot d_2\left(C_{\mathbb{P}^n(K)}(\nu)\right) = d_2\left(C_{\mathbb{P}^m(K)}(\nu)\right) \cdot d_1\left(C_{\mathbb{P}^n(K)}(\nu)\right).$$

Se usará la notación que se introdujo en el capítulo anterior, en particular la usada en el Teorema 1 de la sección 2.3. Por supuesto $K = \mathbb{F}_q$, S es la variedad de Segre, $\mathbb{P}^m(K) = \{Q_1, \ldots, Q_{k_2}\}$, $\mathbb{P}^n(K) = \{P_1, \ldots, P_{k_1}\}$.

Notemos que si $\Lambda \in C_S(\nu)$, esta palabra del código puede ser representada como una matriz de la forma

$$\begin{pmatrix} f_{P_1}(Q_1) & \cdots & f_{P_1}(Q_{k_2}) \\ f_{P_2}(Q_1) & \cdots & f_{P_2}(Q_{k_2}) \\ \cdots & \cdots & \cdots \\ f_{P_{k_1}}(Q_1) & \cdots & f_{P_{k_1}}(Q_{k_2}) \end{pmatrix} \tag{3.1}$$

Donde las filas son elementos de $C_{\mathbb{P}^m(K)}(\nu)$ y las columnas son elementos de $C_{\mathbb{P}^n(K)}(\nu)$.

3.2 Segundo peso generalizado

El resultado principal de este capítulo es el siguiente Teorema el cual describe el segundo peso generalizado de Hamming en el caso de los códigos del capítulo anterior.

Teorema 2 *Sean $K = \mathbb{F}_q$, $S \subseteq \mathbb{P}^N(K)$ la variedad proyectiva de Segre, donde $N = (n+1)(m+1) - 1$ y $C_S(\nu)$ el codigo proyectivo Reed-Muller de orden ν definido sobre S donde $\nu < q$. Entonces el segundo peso generalizado $d_2(C_S(\nu))$ viene dado por*

$$d_2(C_S(\nu)) = d_1\left(C_{\mathbb{P}^n(K)}(\nu)\right) \cdot d_2\left(C_{\mathbb{P}^m(K)}(\nu)\right)$$

Más aún

$$d_2(C_S(\nu)) = (q^n + (1-\nu)q^{n-1})(q^m + (2-\nu)q^{m-1} - q^{m-2}).$$

Demostración. (I) Sean C_1 un subcódigo de dimensión 1 de $C_{\mathbb{P}^n(K)}(\nu)$ y C_2 un subcódigo de dimensión 2 de $C_{\mathbb{P}^m(K)}(\nu)$. Entonces $C_1 \otimes_K C_2$ (producto tensorial de espacios vectoriales) es un subcódigo de dimensión 2 de $C_S(\nu)$. En consecuencia

$$d_2\left(C_S\left(\nu\right)\right) \leq \left|\mathrm{sop}\left(C_1 \otimes_K C_2\right)\right| = \left|\mathrm{sop}\left(C_1\right)\right| \cdot \left|\mathrm{sop}\left(C_2\right)\right|$$

y por tanto

$$d_2\left(C_S\left(\nu\right)\right) \leq d_1\left(C_{\mathbb{P}^n(K)}\left(\nu\right)\right) \cdot d_2\left(C_{\mathbb{P}^m(K)}\left(\nu\right)\right) \tag{3.2}$$

(II) Sea D un subcódigo de dimensión 2 de $C_S\left(\nu\right)$. Toda palabra del código puede ser vista como una matriz de la forma (3.1). Sea D_R el subcódigo de $C_{\mathbb{P}^m(K)}\left(\nu\right) \subseteq K^{k_2}$ generado por las filas de esta matriz cuando consideramos todas las matrices correspondientes a todos los elementos de D. De la misma forma, sea D_C el subcódigo de $C_{\mathbb{P}^n(K)}\left(\nu\right) \subseteq K^{k_1}$ generado por las columnas de las mismas matrices.

Notemos que si $\dim_K D_R = \dim_K D_C = 1$ entonces $\dim_K D \neq 2$. Por tanto $\dim_K D_R \geq 2$ ó $\dim_K D_C \geq 2$. Si $\dim_K D_R \geq 2$ se cumple que $\left|\mathrm{sop}D_R\right| \geq d_2\left(C_{\mathbb{P}^m(K)}\left(\nu\right)\right)$. Si algún elemento de la matriz es no cero, existen por lo menos $d_1\left(C_{\mathbb{P}^n(K)}\left(\nu\right)\right)$ componentes no cero en la columna correspondiente. Luego

$$\left|\mathrm{sop}\left(D\right)\right| \geq d_2\left(C_{\mathbb{P}^m(K)}\left(\nu\right)\right) \cdot d_1\left(C_{\mathbb{P}^n(K)}\left(\nu\right)\right)$$

y por tanto

$$d_2\left(C_S\left(\nu\right)\right) \geq d_2\left(C_{\mathbb{P}^m(K)}\left(\nu\right)\right) \cdot d_1\left(C_{\mathbb{P}^n(K)}\left(\nu\right)\right) \tag{3.3}$$

De forma análoga, si $\dim_K D_C \geq 2$ obtenemos

$$d_2\left(C_S\left(\nu\right)\right) \geq d_1\left(C_{\mathbb{P}^m(K)}\left(\nu\right)\right) \cdot d_2\left(C_{\mathbb{P}^n(K)}\left(\nu\right)\right) \tag{3.4}$$

y el Teorema se sigue de (3.2), (3.3) y (3.4). ■

Para terminar este capítulo se dará un ejemplo:

***Ejemplo* 3.1** Sea K un campo finito con 4 elementos, $K = \{0, 1, a, a^2\}$, donde a es un elemento primitivo de K. Consideremos el caso particular $n = 2, m = 3$, en la definición del mapeo de Segre dado en la sección 1.3 del capítulo 1.

Dado que $\mid \mathbb{P}^2(K) \mid = 21$ y $\mid \mathbb{P}^3(K) \mid = 85$ tenemos que $\mid S \mid = 1785$. Más aún

- $d_1\left(C_{\mathbb{P}^2(K)}(2)\right) = 12$,
- $d_1\left(C_{\mathbb{P}^3(K)}(2)\right) = 48$,
- $d_2\left(C_{\mathbb{P}^2(K)}(2)\right) = 15$,
- $d_2\left(C_{\mathbb{P}^3(K)}(2)\right) = 60$

y entonces

$$d_2\left(C_S(2)\right) = 720.$$

Chapter 4

Códigos Duales

En los dos capítulos anteriores se describieron algunas propiedades de los códigos Reed-Muller asociados a la variedad de Segre.

En este capítulo se caracterizarán los duales de los códigos Reed-Muller asociados a la variedad de Veronese y los correspondientes a Intersecciones Completas.

Ya se había mencionado que para los casos anteriores (variedad de Veronese e Intersecciones Completas) ya se conocen los principales parámetros de esta clase de códigos (cf. [6], [31]), pero faltaba por encontrar el código dual.

Dos resultados que serán fundamentales en el desarrollo de este trabajo son:

Lema 2 *Sean* $K = \mathbb{F}_q$, $a_n = n(q-1)$ *el* $a-$*invariante de* $\mathbb{P}^n(K)$, *y* ν, μ *tales que* $\nu + \mu = a_n$. *Entonces*

$$H_{\mathbb{P}^n(K)}(\nu) + H_{\mathbb{P}^n(K)}(\mu) = \begin{cases} H_{\mathbb{P}^n(K)}(a_n+1) & si\ \nu \not\equiv 0\ mod(q-1) \\ H_{\mathbb{P}^n(K)}(a_n) & si\ \nu \equiv 0\ mod(q-1) \end{cases} \tag{4.1}$$

Demostración. [29], Proposición 13, página 409. ■

Lema 3 *Sea* $\overline{f} \in K[X_0, \ldots, X_n]/I_{\mathbb{P}^n(K)}$ *de grado* d *tal que* $d \leq a_n$, *y* $d \equiv 0\ mod(q-1)$. *Entonces*

$$\sum\nolimits_{P \in \mathbb{P}^n(K)} \overline{f}(P) = 0.$$

Demostración. [34], Lema 8, página 1578. ■

4.1 Duales de los códigos Reed-Muller asociados a la variedad de Veronese.

En esta sección se usará la notación introducida en el capítulo 1, sección 1.5, respecto a la variedad de Veronese, en particular V denotará dicha variedad. De igual manera que en secciones anteriores, $K = \mathbb{F}_q$.

Además, $a_m = m(q-1)$ es el $a-$invariante del anillo coordenado asociado al m-espacio proyectivo $\mathbb{P}^m(K) = \{Q_1, \ldots, Q_{k_2}\}$ ([29], página 407).

Para el caso de los códigos Reed-Muller asociados a la variedad de Veronese, su código dual está dado por:

Teorema 3 *Sea $C_V(d)$ el código Reed-Muller de orden d sobre la variedad de Veronese con $K = \mathbb{F}_q$ y $k_2 = |\mathbb{P}^m(K)|$. Si n es un número natural tal que $nd \leq a_m$, entonces el código dual de $C_V(d)$, que se denota por $C_V^{\perp}(d)$, está dado por*

$$C_V^{\perp}(d) = \begin{cases} C_{\mathbb{P}^m(K)}(a_m - nd) & si \quad nd \not\equiv 0 \bmod (q-1) \\ \left\langle \overline{1}, C_{\mathbb{P}^m(K)}(a_m - nd) \right\rangle & si \quad nd \equiv 0 \bmod (q-1) \end{cases} \tag{4.2}$$

donde $\overline{1}$ es el vector de K^{k_2} cuyas coordenadas son únicamente unos.

Demostración. (i) $nd \not\equiv 0 \bmod (q-1)$.

Sea $\underline{x} = (f(\ldots, M, \ldots)(Q_1), \ldots, f(\ldots, M, \ldots)(Q_{k_2}))$ una palabra del código $C_V(d)$ con $\deg(f) = d$. Notemos que $\underline{x} = (F(Q_1), \ldots, F(Q_{k_2}))$ con $\deg(F) = nd$. Si tomamos $\underline{y} = (h(Q_1), \ldots, h(Q_{k_2}))$ en $C_{\mathbb{P}^m(K)}(a_m - nd)$ donde $\deg(h) = a_m - nd$, dado que $\deg(Fh) = a_m$ del Lema 3 se sigue que

$$\underline{x} \cdot \underline{y} = \sum_{i=1}^{k_2} (Fh)(Q_i) = 0$$

Por consiguiente, $C_{\mathbb{P}^m(K)}(a_m - nd) \subseteq C_V^{\perp}(d)$.

La igualdad de estos códigos se sigue del hecho siguiente (y el Lema 2)

$$\dim_K C_V(d) + \dim_K C_{\mathbb{P}^m(K)}(a_m - nd) = H_{\mathbb{P}^m(K)}(nd) + H_{\mathbb{P}^m(K)}(a_m - nd) = H_{\mathbb{P}^m(K)}(a_m + 1) = k_2 = \#(\mathbb{P}^m(K)).$$

(ii) $nd \equiv 0 \bmod (q-1)$.

Sea $\underline{x}$ como en el caso (i) y $\underline{z} := (\lambda + h(Q_1), \ldots, \lambda + h(Q_{k_2}))$ en el subespacio $\left\langle \overline{1}, C_{\mathbb{P}^m(K)}(a_m - nd) \right\rangle$, con λ en K. Entonces

$$\underline{x} \cdot \underline{z} = \sum_{i=1}^{k_2} (Fh)(Q_i) + \lambda \sum_{i=1}^{k_2} F(Q_i).$$

Como $\deg(Fh) = a_m$ se sigue que $\sum_{i=1}^{k_2} (Fh)(Q_i) = 0$. De hecho, $\sum_{i=1}^{k_2} F(Q_i) = 0$ debido a que $\deg(F) \leq nd \leq a_m$, y $nd \equiv 0 \bmod (\mathrm{q}-1)$ (Lema 3). Por tanto, $\left\langle \overline{1}, C_{\mathbb{P}^m(K)}(a_m - nd) \right\rangle \subseteq C_S^{\perp}(d)$.

Nuevamente, tomando dimensiones:

$$\dim_K C_V(d) + \dim_K \left\langle \overline{1}, C_{\mathbb{P}^m(K)}(a_m - nd) \right\rangle = H_{\mathbb{P}^m(K)}(nd) + H_{\mathbb{P}^m(K)}(a_m - nd) + 1 = H_{\mathbb{P}^m(K)}(a_m) + 1 = k_2.$$

(i) y (ii) prueban el Teorema. ■

Resta analizar el caso de intersecciones completas, que se hará en la siguiente sección.

4.2 Duales de los códigos Reed-Muller asociados a intersecciones completas

En esta sección usaremos la notación introducida en la sección 1.6 del capítulo 1, donde $K = \mathbb{F}_q$. En particular, $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$ es una intersección completa. Para la demostración del Lema siguiente se recordará a continuación la definición de un esquema Cayley-Bacharach (para más detalles se puede consultar [9]).

***Definición* 4.1** Sea $U \subseteq \mathbb{P}^t(K)$, con $|U| = s$. U es llamado un *esquema Cayley-Bacharach* si cualquiera dos subconjuntos de $s-1$ puntos de U tienen la misma función de Hilbert.

Equivalentemente, [9], página 171, si toda hipersuperficie de grado menor que $a_U + 1$ que contiene $s - 1$ puntos de U, contiene todos los puntos de U (donde a_U es el a-invariante del anillo coordenado asociado a U).

En particular, todo subconjunto de $\mathbb{P}^t(K)$ que es una intersección completa de t hipersuperficies es un esquema Cayley-Bacharach.

En [6], Corolario 3.2, página 9, se prueba que $C_X^{\perp}(a_X)$ es unidimensional.

En esta sección se hace una generalización de este resultado y se encuentra el dual de los códigos $C_X(d)$ para $d \leq a_X$.

Para llegar a este resultado es necesario el siguiente Lema:

***Lema* 4** *Sea $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$ una intersección completa. La distancia mínima $\delta_X(a_X)$ de $C_X(a_X)$ es 2.*

Demostración. Como $\dim_K C_X(a_X) = m - 1$, de la cota de Singleton se sigue que $\delta_X(a_X) + m - 1 \leq m + 1$ y por lo tanto $\delta_X(a_X) \leq 2$.
Si $\Lambda = (f(P_1), \ldots, f(P_m)) \in C_X(a_X)$ con $\omega(\Lambda) = 1$ ($\omega(\Lambda)$ significa el peso de Hamming de Λ), tendríamos que $f(P_j) = 0$ para todo $j \neq i$, $f(P_i) \neq 0$ para algún $i \in \{1, \ldots, m\}$. Pero esto contradice el hecho que X es un esquema Cayley-Bacharach.

De lo anterior se concluye que $\delta_X(a_X) = 2$. ■

El siguiente resultado es uno de los más importantes de este trabajo. Generaliza varios casos particulares previos que habían sido estudiados y que se engloban en el concepto de Intersección Completa, como el caso del espacio afín y otros que pueden ser consultados en [6], [29], [30].

Para este resultado es necesario recordar la definición de códigos equivalentes, debido a que este concepto tiene varias connotaciones (para más detalles puede consultarse [35]).

***Definición* 4.2** Dos códigos $C_1, C_2 \subseteq \mathbb{F}_q^m$ son *equivalentes* si podemos encontrar un vector $a = (a_1, \ldots, a_m) \in \left(\mathbb{F}_q{}^*\right)^m$ tal que $C_2 = a \cdot C_1$, i.e.,

$$C_2 = \{(a_1 c_1, \ldots, a_m c_m) : (c_1, \ldots, c_m) \in C_1\}.$$

Evidentemente, códigos equivalentes tienen la misma dimensión, la misma distancia mínima y la misma distribución de pesos.

***Teorema* 4** *Sea $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$ una intersección completa y $d \leq a_X$, con a_X el $a-$invariante de X. Entonces*

$$C_X^{\perp}(d) \text{ y } C_X(a_X - d) \text{ son códigos equivalentes} \tag{4.3}$$

Demostración. Como $\dim_K C_X(a_X) = m-1$ su matriz de chequeo de paridad tiene la forma $\mathbb{H} = (b_1, \ldots, b_m)$ donde $b_i \in K$ para $i \in \{1, \ldots, m\}$. Por consiguiente $C_X^{\perp}(a_X) = \langle (b_1, \ldots, b_m) \rangle$.

Si $b_i = 0$ para algún $i \in \{1, \ldots, m\}$, tendríamos que $\mathbb{H} \cdot \underline{e}_i = 0$ donde $\underline{e}_i$ es el $i-$ésimo vector canónico de K^m. Es decir, $\underline{e}_i \in C_X(a_X)$, pero esto no es posible por el Lema anterior.

En consecuencia, $C_X^{\perp}(a_X) = \langle (b_1, \ldots, b_m) \rangle$ y $b_i \neq 0$ para toda $i \in \{1, \ldots, m\}$.

Sea $\Lambda_1 = (b_1 g(P_1), \ldots, b_m g(P_m)) \in (b_1, \ldots, b_m) C_X(a_X - d)$, donde $\deg(g) = a_X - d$ y sea $\Lambda_2 = (f(P_1), \ldots, f(P_m)) \in C_X(d)$. Entonces $\Lambda_1 \cdot \Lambda_2 = \sum_{i=1}^{m} b_i (fg)(P_i)$. Puesto que $\deg(fg) = a_X$ y $C_X^{\perp}(a_X) = \langle (b_1, \ldots, b_m) \rangle$, se concluye que $\Lambda_1 \cdot \Lambda_2 = 0$, i.e., $C_X^{\perp}(d)$ contiene a $(b_1, \ldots, b_m) C_X(a_X - d)$.

Como ([6], Proposición 2.7, página 6)

$$\dim_K C_X(d) + \dim_K (b_1, \ldots, b_m) C_X(a_X - d) = H_X(d) + H_X(a_X - d) = m$$

se sigue el resultado. ■

***Observación* 7** El Teorema anterior puede resumirse en la siguiente afirmación: $C_X^{\perp}(d) = (b_1, \ldots, b_m) C_X(a_X - d)$ donde $(b_1, \ldots, b_m)$ es un generador del espacio unidimensional $C_X^{\perp}(a_X)$.

***Observación* 8** Consideremos el caso $X = \mathbb{A}^n(K)$, es decir X es el $n-$ espacio afín. Como X es una Intersección Completa ([6]) y $C_X^{\perp}(a_X) = \langle \overline{1} \rangle$, donde $\overline{1}$ es el vector cuyas coordenadas son únicamente unos, del Teorema 4 se obtiene el resultado, ya conocido, $C_X^{\perp}(d) = C_X(a_X - d)$.

4.3 Ejemplo

Para analizar el resultado fundamental de la sección anterior es conveniente proporcionar un caso específico como el siguiente.

En este ejemplo se trabajará con una intersección completa sobre el plano proyectivo en un campo con 4 elementos, para definir un código mediante un mapeo de evaluación sobre los puntos de esta intersección completa y poder así determinar su código dual (cf. [18]).

***Ejemplo* 4.1** Sea K un campo finito con 4 elementos, $K = \{0, 1, \alpha, \alpha^2\}$, con α un elemento primitivo de K. Tomaremos $X := \{(1, t_1, t_2) : t_1, t_2 \in K^*\}$ como un subconjunto de $\mathbb{P}^2(K)$. De hecho:

$$\begin{aligned} X = \{&(1,1,1),(1,\alpha,1),(1,\alpha^2,1),(1,1,\alpha),(1,\alpha,\alpha),\\ &(1,\alpha^2,\alpha),(1,1,\alpha^2),(1,\alpha,\alpha^2),(1,\alpha^2,\alpha^2)\} \end{aligned} \tag{4.4}$$

y además:

$$I_X = \left\langle X_1^3 - X_0^3, X_2^3 - X_0^3 \right\rangle \tag{4.5}$$

En este caso, $a_X = 3$. También se tiene que $\dim_K C_X(3) = 8$. Más aún, $\delta_X(3) = 2$ (véase el Lema 4 de la sección 4.2) y

$$C_X^{\perp}(3) = \left\langle (\alpha, \alpha^2, 1, \alpha^2, 1, \alpha, 1, \alpha, \alpha^2) \right\rangle.$$

Por lo tanto, se sigue del Teorema 4, que

$$C_X^{\perp}(d) = (\alpha, \alpha^2, 1, \alpha^2, 1, \alpha, 1, \alpha, \alpha^2) \cdot C_X(a_X - d)$$

para cualquier $d \leq a_X$.

***Observación* 9** Nuevamente, como en el ejemplo del capítulo anterior, el uso del paquete de computación Macaulay2 ([13]) fue fundamental para los cálculos del ejemplo anterior.

Conclusiones

El objetivo fundamental del presente trabajo (hacer contribuciones, modestas pero importantes, en la Teoría de códigos) ha sido cumplido.

En los capítulos anteriores se han descrito algunos resultados que vienen a formar parte de esta rama del conocimiento (Teoría de códigos) que no podemos llamar emergente pero sí de más o menos reciente creación (cincuenta años aproximadamente).

En este proceso se han usado como herramientas básicas algunas ramas de las matemáticas (Algebra conmutativa y Geometría algebraica), tradicionalmente ligadas al ámbito puramente académico, para resolver algunas cuestiones que, como se explica en la introducción, han tenido aplicaciones concretas indudables.

Por supuesto que el contenido matemático es la esencia de este trabajo, independientemente de sus implicaciones colaterales.

Esta tesis tiene, en conclusión, la pretensión de poner un granito de arena en el desarrollo científico de nuestro país.

Bibliography

[1] M. Boguslavsky, *On the Number of Solutions of Polynomial Systems*. Finite Fields and their Aplicattions, Vol. **3**, No. 4, pp. 287-299, Oct. (1997).

[2] B. Chor *et al. The bit extraction problem of t-resilient functions*. IEEE, 26th Annual Symp. on Foundations of Computer Science, pp. 396-407, (1985).

[3] B. Cooke. *Reed-Muller Error Correcting Codes*. MIT Undergraduate Journal of Mathematics, pp. 21-26, (1995).

[4] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties and Algorithms*. UTM, Springer-Verlag, (1992).

[5] P. Delsarte, J.M. Goethals, F.J. MacWilliams. *On generalized Reed-Muller codes and their relatives*. Inform. and Control, Vol. **16**, pp. 403-422, (1970).

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

[7] G.D. Forney, Jr. *Dimension lenght profiles and trellis complexity of linear block codes*. IEEE Trans. Inform. Theory, Vol. **40**, pp. 1741-1752, (1994).

[8] W. Fulton. *Algebraic curves: An introduction to algebraic geometry*. W.A. Benjamin, Inc. New York, Amsterdam, (1969).

[9] A.V. Geramita, M. Kreuzer and L. Robbiano. *Cayley-Bacharach schemes and their canonical modules*. Transactions of the AMS, Vol. **339**, number 1, pp. 163-189, sept. (1993).

[10] M. González-Sarabia, C. Rentería and H. Tapia-Recillas. *Reed-Muller-Type Codes Over the Segre Variety*. To appear in Finite Fields and their Applications, (2002).

[11] M. González-Sarabia, C. Rentería. *The dual code of some Reed-Muller-type codes*. Submitted for publication, (2002).

[12] M. González-Sarabia, C. Rentería and M.A. Hernández de la Torre. *Minimum distance and second generalized Hamming weight of two particular linear codes*. Preprint (2002).

[13] D.R. Grayson, M. Stillman. *Macaulay 2*,(1999).

[14] J.P. Hansen. *Points in Uniform Position and Maximum Distance Separable Codes, Zero Dimensional schemes*. Proc. Int. Conf., Ravello, 1992, Walter de Gruyter, Berlin, pp. 205-211, (1994).

[15] J. Harris. *Algebraic Geometry: A First Course*. Springer-Verlag, GTM, No. 133, (1992).

[16] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, (1977).

[17] P. Heijnen and R. Pellikan. *Generalized Hamming Weights of $q-ary$ Reed-Muller Codes*. IEEE Trans. Inf. Theory, Vol. **44**, pp. 181-196, Jan. (1998).

[18] M.A. Hernández de la Torre. *Aplicaciones del Algebra Conmutativa y la Geometría Algebraica a la Teoría de Códigos Algebraicos*. ESFM del IPN, Tesis de Maestría, (2000).

[19] T. Kasami, S. Lin, and W.W. Peterson. *New generalizations of the Reed-Muller codes. Part I: Primitive codes*. IEEE Trans. Inform. Theory, Vol. **IT-14, no. 2**, pp. 189-199, (1968).

[20] T. Kasami, T. Tanaka, T. Fujiwara and S. Lin. *On complexity of trellis structure of linear block codes*. IEEE Trans. Inform. Theory, Vol. **39**, pp. 1057-1064, (1993).

[21] G. Lachaud. *The parameters of the projective Reed-Muller codes*. Discrete Mathematics **81**, pp. 217-221, (1990).

[22] F.J. MacWilliams and J.A. Sloane. *The theory of Error-Correcting Codes*. North-Holland Publ. Co., Amsterdam, New York, Oxford, (1977).

[23] D.J. Mercier, R. Rolland. *Polynômes homogènes qui s'annulent sur l'espace projectif* $\mathbb{P}^m(\mathbb{F}_q)$. Journal of Pure and Applied Algebra. Elsevier Science, Vol. **124 (1-3)**, pp. 227-240, (1998).

[24] R.E. Muller. *Applications of Boolean algebra to switching circuit design and to error detection*. IRE Trans Electron. Comput., Vol. **EC-3**, pp. 6-12, (1954).

[25] L.H. Ozarow and A.D. Wyner. *Wire-tap channel II*. AT&T Bell Labs Tech. J., Vol. **63**, pp. 665-680, (1984).

[26] I.S. Reed. *A class of multiple-error-correcting codes and the decoding scheme*. IRE Trans. Inform. Theory, Vol. **PGIT-4**, pp. 38-49, (1954).

[27] C. Rentería, H. Tapia-Recillas. *A connection between the Veronese Map and Reed-Muller codes*. C. Numerantium Vol. **102**, pp. 175-181, (1994).

[28] C. Rentería, H. Tapia-Recillas. *Linear codes associated to the ideal of points in* $\mathbb{P}^d$ *and its canonical module*. Communications in Algebra **24 (3)**, pp. 1083-1090, (1996).

[29] C. Rentería, H. Tapia-Recillas. *Reed-Muller codes: An ideal theory approach*. Communications in Algebra **25 (2)**, pp. 401-413, (1997).

[30] C. Rentería, H. Tapia-Recillas. *The a-invariant of some Reed-Muller Codes*. Applicable Algebra in Engineering, Communications and Computing, (AAECC), Springer-Verlag, Vol. **10**, No. 1 (1999).

[31] C. Rentería, 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).

[32] H.G. Schaathun. *The Weight Hierarchy of Product Codes*. IEEE Trans. Inf. Theory, Vol. **46**, pp. 2648-2651, Nov. (2000).

[33] C.E. Shannon. *The Mathematical Theory of Communications*. Bell System Technical Journal 27, pp. 379-423, 623-656, (1948).

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

[35] H. Stichtenoth. *Algebraic Function Fields and codes*. University Text, Springer-Verlag, (1993).

[36] M. Tsfasman and S. Vladut. *Algebraic-geometric codes*. Kluwer Academic Pub., Math. and its Appl. **58**, (1991).

[37] M. A. Tsfasman and S. G. Vladut. *Geometric approach to higher weights*. IEEE Trans. Inf. Theory, pt. I (Special Issue on Algebraic-Geometry Codes), Vol. **41**, pp. 1564-1588, Nov. (1995).

[38] V.K. Wei. *Generalized Hamming Weights for Linear Codes*. IEEE Trans. Inf. Theory, Vol. **37**, pp. 1412-1418, (1991).

[39] V.K. Wei and K. Yang. *On the Generalized Hamming Weights of Product Codes*. IEEE Trans. Inf. Theory, Vol. **39**, pp. 1709-1713, Sept. (1993).

[40] E.J. Weldon. *New Generalizations of the Reed-Muller codes. Part II: Nonprimitive codes*. Trans. Inform. Theory, Vol. **IT-14**, pp. 199-205, (1968).

[41] X. Youxin, C. Jin, F. Changgeng. *Implementation of coding and encryption in satellite channel*. Communication Technology Procedings, ICCT'96, Vol. **1**, pp. 31-34, (1996).