"CÓDIGOS LINEALES ASOCIADOS A ESTRUCTURAS COMBINATORIAS"

JOSÉ NOÉ GUTIÉRREZ HERRERA

TESIS DOCTORAL

"CÓDIGOS LINEALES ASOCIADOS A ESTRUCTURAS COMBINATORIAS"

TESIS QUE PRESENTA

JOSÉ NOÉ GUTIÉRREZ HERRERA

PARA LA OBTENCIÓN DEL GRADO DE

DOCTOR EN CIENCIAS

ASESOR: DR. HORACIO TAPIA RECILLAS

NOVIEMBRE DE 2002

UNIVERSIDAD AUTÓNOMA METROPOLITANA-IZTAPALAPA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

Se agradece el apoyo a las siguientes instituciones y personas:

Al Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa.

Al CONACyT por otrogarme una beca para realizar mis estudios, y por el apoyo adicional a través del proyecto L0076E9607 "Teoría Algebraica de Códigos, Álgebra Conmutativa y Geometría Algebraica", bajo la responsabilidad del Dr. Horacio Tapia Recillas, del Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa.

A mis padres Nicolás Gutiérrez B. y Soledad Herrera C. así como a mi hermana Vicky por su apoyo estos años.

A mi amiga Diana Angélica por escribir para mi un programa de cómputo que resultó muy útil en la preparación del presente manuscrito.

A mi asesor, el Dr. Horacio Tapia Recillas, por su constante preocupación en el buen desarrollo de mi trabajo.

A mis sinodales por sus acertados comentarios y sugerencias para la mejor presentación de este escrito.

Índice

Introducción

En nuestra sociedad la transmisión de información y la recuperación de datos almacenados en medios digitales son cada vez más comunes. Sin embargo la inevitable presencia de ruido durante la transmisión introduce errores aleatorios en el mensaje provocando que lo que se recibe no siempre coincida con lo que fue enviado. La búsqueda de técnicas adecuadas para resolver este problema condujo al desarrollo de la Teoría de Códigos, entre cuyas aplicaciones encontramos hoy en día la comunicación vía satélite, la transmisión y almacenamiento de datos, la reproducción de discos compactos, la comunicación con naves en el espacio exterior, la transmisión de audio y video, etc., como se menciona en las referencias [10, 11, 29, 34, 55, 67, 69, 80].

La Teoría de Códigos ha sido estudiada ulilizando herramientas matemáticas tales como el Álgebra Conmutativa (cf. [61]), la Geometría Algebraica (cf. [77]) y la Matemática Discreta y Combinatoria (cf. [3, 75]). Es indudable que el uso de técnicas como Álgebra Conmutativa y Geometría Algebraica ha conducido a métodos de construcción de una amplia variedad de códigos. Desafortunadamente el conocimiento de tales temas es casi exclusivo del profesional de las Matemáticas, quedando fuera del curriculum de otras áreas del conocimiento, lo que dificulta la comunicación entre quien "diseña" el modelo matemático del código, quien lo implementa y quien finalmente hará uso de él. Por otro lado al emplear técnicas de la Matemática Discreta y Combinatoria no sólo se han obtenido tan buenos resultados como con otros métodos sino que aquellas son conocidas por un mayor número de personas. Esto permite que los resultados así obtenidos sean comprendidos, y por lo tanto utilizados, en un menor lapso de tiempo por un mayor número de personas. Actualmente podemos encontrar códigos asociados con varias estructuras: gráficas (grafos) [64, 75, 76], diseños de bloques [1], geometrías finitas [1], matroides [75], cuadrados latinos [67], conjuntos parcialmente ordenados [4, 8], esquemas asociativos [46], arreglos ortogonales [46], etc. Por los motivos antes expuestos el presente trabajo tiene un enfoque combinatorio. Todos los resultados originales que se mencionan aquí han sido reportados de manera más concisa en [19, 20, 21, 22, 23].

Otro de los problemas relacionados con la transmisión de mensajes es buscar que el este no sea alterado o leido por terceras personas no autorizadas, y que la persona que lo envia no pueda negar que lo hizo, es decir el problema es la integridad y no-repudio de la información. La ciencia que se encarga de estudiar este tipo de problemas se denomina *Critpografía,* que al igual de la Teoría de Códigos ha

sido analizada con y sin la ayuda de la Matemática Discreta y Combinatoria. El tema es tratado con herramientas de Teoría de los Números en [65], un libro más moderno que incluye el enfoque de curvas elípticas es [38]. El tema es tratado con herramientas de Matemática Combinatoria en [74]. Recientemente se ha descubierto un método para compartir un secreto entre varias personas denominado *Criptografía Visual.* Esta cumple la condición de si una persona no autorizada intercepta a lo más cierta cantidad de partes en que se dividió el secreto y tiene a su disposición un poder infinito de cómputo, será incapaz de obtener información alguna del mensaje original. Una referencia sobre este tema, que también puede estudiarse desde un punto de vista combinatorio, es [2]. La Criptografía es un tema que no será tratado en este trabajo.

Son dos los resultados principales que se enuncian en este escrito: el primero es una relación tipo MacWilliams con una generalización de la métrica de Hamming (teorema 35). En la teoría clásica de códigos la identidad de MacWilliams es una de las más importantes ecuaciones. Esta nueva relación permite obtener infomación adicional sobre la manera en la que se distribuye el soporte de los vectores que representan los mensajes codificados. Este trabajo ha sido generalizado de dos maneras distintas e independientes en [30, 36].

El segundo resultado (teorema 48) es un método de construcción de códigos lineales a partir de matrices muy simples de ceros y unos, algunos alcanzando los mejores parámetros posibles (ejemplos 70 y 77). La familia de códigos así construida contiene a los códigos binarios de Reed-Muller (proposición 51) y a los códigos asociados a sistemas de ciclos (corolario 74) como algunos de sus miembros.

Se ha puesto una especial atención en los códigos binarios de Reed-Muller, logrando determinar algunas de sus propiedades combinatorias como son:

Una construcción de tales códigos a partir de matrices identidad y de matrices circulantes cuyo primer renglón está constituido por un par de unos consecutivos y el resto de ceros (proposición 51 y corolario 52).

Un conjunto de generadores para los códigos de Reed-Muller de primer orden, que juntos forman un 1-diseño, además de una base para tales códigos en términos de esta estructura combinatoria (teorema 55).

Una base constituida por vectores de peso mínimo, construida por un simple algorítmo polinomial y relacionada con los códigos mencionados en el punto anterior (teorema 65).

Una base construida en base a esferas de Hamming, que permite escribir manualmente una base sin realizar operación alguna e identificar fácilmente si se ha cometido algún error (teorema 84).

Una base de vectores de peso mínimo junto con las ecuaciones de las variedades lineales, sobre el campo binario, de las cuales provienen (teorema 86).

El presente escrito se divide en dos partes para una mejor comprensión de las ideas originales que contiene. La primera comprende los capítulos 1 y 2 en la que los conceptos generales de la Teoría de Códigos (Correctores de Errores) es explicada, y

ninguna aportación original es incluida. La segunda parte abarca los capítulos 3,4,5 y 6 en los que las aportaciones originales son descritas.

El primer capítulo contiene una exposición de las nociones básicas sobre la Teoría de Códigos, haciendo especial énfasis en los llamados *códigos binarios de Reed-Muller,* pues éstos jugarán un papel muy importante en la segunda parte de este trabajo. En el segundo capítulo la atención se centra en el estudio una de las familias más importantes de códigos: la de los códigos cíclicos, que jugarán un papel principal en el desarrollo de los capítulos 4 y 5.

El tercer capítulo es una versión extendida de [20], en el que se presenta una identidad tipo MacWilliams, para códigos con un tipo especial de métrica definida por conjuntos parcialmente ordenados (teorema 35). La importancia de este nuevo resultado radica en la información que nos brinda sobre el número de elementos de un código (palabras codificadas) que tienen entrada igual a uno en una posición coordenada fija.

En el capítulo 4 se describen varios métodos para incrementar el valor de los parámetros de los códigos lineales binarios (relación 4.2, teorema 48, relación 4.5 y teorema 63). La combinación de tales técnicas conducen a construir una amplia familia de códigos, que contiene a los códigos de Reed-Muller así como a varios códigos que alcanzan valores óptimos de sus parámetros. Se muestra que a partir de códigos lineales sin capacidad para detectar o corregir los errores pueden obtenerse códigos de parámetros óptimos al aplicar la construcción propuesta. Se muestra además que los denominados códigos de Reed-Muller de primer orden, pueden ser fácilmente construidos a partir de una matriz identidad de orden 2×2 (teorema 55), y que este tipo de códigos tiene un conjunto de generadores que pueden ser vistos como una estructura combinatoria denominada 1-diseño, se muestra además una base para los códigos en términos del 1-diseño.

En el capítulo 5 se presentan los códigos binarios asociados a una estructura combinatoria denominada sistema de ciclos, la cual es una partición de las aristas de una gráfica en ciclos de la misma longitud. Restringiéndonos al caso de ciclos de longitud múltiplo de cuatro de una gráfica bipartita completa no dirigida se determinan los parámetros de los códigos asociados. Se concluye que estos códigos son un caso especial de aquellos definidos en el capítulo previo, que contienen varios códigos de Reed-Muller, además de que algunos códigos con los mejores parámetros que puede alcanzarce son obtenidos. Una versión más concisa de esta exposición y la del capítulo precedente puede consultarse en [22].

El capítulo 6 contiene una serie de resultados que se obtubieron paralelamente al trabajo principal de este escrito (capítulos 3, 4 y 5). En la primera sección se describe una manera de encontrar una base para los códigos binarios de Reed-Muller sin efectuar cálculos algebraicos, en base a las llamadas esferas de Hamming (teorema 84) y puede consultarse también en [19]. La segunda sección contiene uno de los resultados principales de [23] y describe una base para los códigos binarios de Reed-Muller, formada por vectores de peso mínimo, además se da su descripción en

términos de variedades afines (teorema 86). La tercera sección trata sobre una una relación tipo Parseval sobre el anillo $\mathbb{Z}_n$, de los enteros módulo n (corolario 96), da respuesta al problema de encontrar el número de soluciones de una ecuación lineal sobre este mismo anillo (teorema 93), y concluye con una caracterización de una clase de funciones tipo bent (proposición 97). Los resultados de ésta última sección aparecen publicados, omitiendo algunos detalles, en [21].

El capítulo 7 contiene algunas conclusiones respecto a este trabajo así como posibles líneas de investigación que pueden seguirse en un futuro.

Por último se anexa un apéndice que contiene una lista de los polinomios característico y generador de un tipo de códigos definidos en el cuarto capítulo.

CAPÍTULO 1

CONCEPTOS GENERALES

El desarrollo de la Teoría de Códigos comenzó con un escrito de Claude Shannon publicado en 1948 (cf. [70]). Shannon define una cantidad llamada la *capacidad del canal* atribuible a cualquier canal de comunicación. Prueba entonces que si la capacidad del canal es mayor que la razón de transmisión de éste (medidas ambas en bits por segundo), existe un sistema de comunicación con una probabilidad de detectar y corregir errores tan alta como se deseé. Lamentablemente Shannon no dice cosa alguna sobre la manera de elaborarlo, pues su prueba es probabilística y no constructiva. El trabajo subsiguiente de muchos investigadores, comenzando con el de R. Hamming en 1950 ([25]), ha estado dirigido a alcanzar tal meta.

En este capítulo se introduce el concepto de *código lineal corrector de errores*, y se estudian algunas de sus propiedades principales, así como otros conceptos básicos tales como matrices generadora y de chequeo de paridad, la distancia de Hamming y el polinomio enumerador de pesos de un código.

Existen varios textos en los cuales puede encontrarse un estudio más amplio de los temas expuestos en este y el siguiente capítulo, en la bibliografía se mencionan algunos de ellos. A continuación se ofrece un breve comentario sobre aquellos que mayor influencia tuvieron sobre el presente trabajo. Desde su publicación el libro de MacWilliams y Sloane [46] se convirtió en referencia obligada para todo aquel que deseé estudiar los fundamentos de la Teoría de Códigos. Un libro en el que se enfatiza la relación entre la Teoría de la Información y la de Códigos es [66]. En [3, 75] podemos encontrar una introducción a este tema desde el punto de vista combinatorio, y por último en [1] se estudian los códigos asociados a estructuras combinatorias denominadas diseños de bloques, haciendo uso de las propiedades de estas.

1.1 Códigos lineales y sus parámetros

En esta sección se presenta el concepto de código lineal detector-corrector de errores. Se muestra que un código lineal puede ser generado matricialmente y se indican diversas formas de contruir nuevos códigos a partir de otros ya conocidos.

A lo largo del presente escrito un *código* será simplemente un conjunto de cadenas de símbolos de la misma longitud, definidas sobre algún alfabeto prefijado.

Más formalmente tenemos la siguiente definición del objeto que nos ocupa (cf. [46])

Definición 1 *Sean n, k enteros positivos, $k \leq n$, $\mathcal{A}$ un alfabeto y B un subconjunto no vacío de $\mathcal{A}^k$. Una* ***función de codificación*** *es una función inyectiva ϕ: $B \longrightarrow \mathcal{A}^n$. Su imagen, $C = Im(\phi)$, se conoce como* ***código (corrector de errores) sobre*** *$\mathcal{A}$.*

El alfabeto $\mathcal{A}$ será tomado siempre como el campo finito con q elementos $\mathbb{F}_q$, donde q es una potencia de un número primo p. Esto nos conduce a la necesidad de realizar la aritmética en $\mathbb{F}_q$ de manera eficiente, tal problema es considerado por ejemplo en [51]. Ahora definiremos una clase especial de códigos, que serán a los que principalmente dedicaremos nuestra atención.

Definición 2 *Si la función ϕ arriba definida es lineal, el código correspondiente C será un $[n, k]$* ***código lineal*** *sobre $\mathbb{F}_q$.*

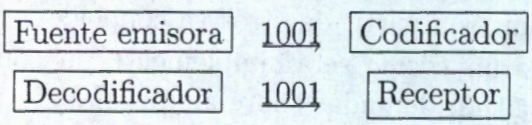
En otras palabras, un código es simplemente un subconjunto de $\mathbb{F}_q^n$ mientras que un $[n, k]$ código lineal es un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión k. Nos referiremos a los elementos de un código como *palabras codificadas* y al entero n como la *longitud* de las palabras codificadas. Por otro lado *un canal de comunicación* consiste del alfabeto finito $\mathbb{F}_q = \{a_1, \ldots, a_q\}$ sobre el que se define el código, y un conjunto de probabilidades de transmisión, $P(\text{se recibe } a_j \mid a_i \text{ es enviada})$, que satisface

$$\sum_{j=1}^{q} P\left(\text{se recibe } a_j \mid a_i \text{ es enviada}\right) = 1$$

para todo i. Aquí $P(\text{se recibe } a_j \mid a_i \text{ es enviada})$ denota la probabilidad de que se reciba el símbolo a_j dado que se envió a_i. Supondremos además que cada símbolo recibido depende probabilísticamente sólo del que fue enviado. Como ejemplo considérese el *canal simétrico binario,* en el cual el alfabeto consta de los dos únicos símbolos: 0 y 1. Si la probabilidad de que ocurra un error es p, entonces

$$P\left(\text{se recibe } 0 \mid 1 \text{ es enviado}\right) = P\left(\text{se recibe } 1 \mid 0 \text{ es enviado}\right) = p$$
$$P\left(\text{se recibe } 0 \mid 0 \text{ es enviado}\right) = P\left(\text{se recibe } 1 \mid 1 \text{ es enviado}\right) = 1 - p$$

El esquema general de codificación-decodificación consiste en una fuente emisora (que envia un mensaje), un codificador (la función de codificación), un canal (el medio por el cual viaja el mensaje), un decodificador (una función que detecta y corrige los errores ocurridos durante la transmisión y da por resultado el mensaje original) y por úlitmo un receptor. Este esquema puede visualizarse como en el diagrama mostrado abajo en el cual el mensaje enviado 1001 sufre un error en su primer símbolo durante su transmisión.



La idea general de la codificación es añadir a cada mensaje una cadena de símbolos de redundancia, que más tarde permitan la detección y corrección de los errores adquiridos durante la transmisión. Obviamente la transmisión del mensaje codificado resulta entonces más lenta que si el mensaje se trasmitiera sin codificar. A fin de comparar la cantidad de símbolos en un mensaje y su codificación se introduce la *razón* del código, definida como $R = k/n$, para un $[n, k]$ código lineal.

En 1972 el *Mariner 9* utilizó un $[32, 6]$ código binario, cuya razón es $R \approx \frac{1}{5}$, para transmitir fotografías en blanco y negro del planeta Marte (cf. [46]). Las fotografías eran divididas en pequeños rectángulos, siéndoles asignados a cada uno de éstos un tono de gris de entre $2^6 = 64$ opciones disponibles. Cada tono de color tenía asignado una cadena binaria de longitud 6, la cual era codificada como una cadena de longitud 32. Resulta claro entonces que un mensaje codificado estaba constituido por aproximadamente cinco veces más símbolos que el mensaje original (sin codificar). Sin embargo como cada una de las 64 posibles cadenas binarias de longitud 6 correspondía a un tono de gris, si ocurriera un error durante la transmisión y el mensaje no fuera codificado el receptor sería incapaz de detectarlo (y por lo tanto de corregirlo). Por otro lado el código empleado, que pertenece a la familia de códigos lineales conocida como códigos de Reed-Muller y que estudiaremos en la última sección de este capítulo, detecta y corrige hasta siete de éstos errores (cf. [67]).

En un canal binario simétrico, con probabilidad de error $p < \frac{1}{2}$, la probabilidad de recibir un símbolo codificado sin error es $1 - p$. De ahí que la probabilidad de recibir sin error una palabra codificada de longitud n es $(1-p)^n$, y la de que al transmitir $\mathbf{c}$ se reciba $\mathbf{x} = \mathbf{c} + \mathbf{e}$, donde $\mathbf{e}$ es un vector de longitud n con t unos, es $P(\text{se recibe } \mathbf{x} \mid \mathbf{c} \text{ es enviada}) = p^t (1-p)^{n-t}$. Como $1 - p > p$, esta última probabilidad es inversamente proporcional a t, es decir,

$$(1-p)^n > p(1-p)^{n-1} > p^2(1-p)^{n-2} > \cdots .$$

Por lo tanto la palabra codificada con mayor probabilidad de haber sido enviada es aquella con más símbolos en común con la recibida. También notemos que la probabilidad de que ocurran t errores durante la transmisión es

$$\binom{n}{t} p^t (1-p)^{n-t}.$$

El anterior argumento nos lleva a la necesidad de comparar los símbolos del mensaje recibido con cada una de las palabras codificadas. Para este fin se introduce una distancia en el espacio $\mathbb{F}_q^n$ como se describe a continuación.

Definición 3 *La **distancia de Hamming** entre las palabras $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ es el número de posiciones en las que ambas difieren. Tal número será denotado como $d(\mathbf{x}, \mathbf{y})$.*

Es fácil comprobar que la función d antes definida es en efecto una distancia en $\mathbb{F}_q^n$. Así que al recibir un mensaje $\mathbf{x}$ la palabra codificada con mayor probabilidad de haber sido enviada es aquella más cercana a $\mathbf{x}$ (en la distancia de Hamming).

Definimos ahora el *soporte* de una palabra $\mathbf{x} \in \mathbb{F}_q^n$, denotado $sop(\mathbf{x})$, como el conjunto de sus posiciones coordenadas en las que tiene entradas no cero. El *peso de Hamming* de $\mathbf{x}$, abreviado $ps(\mathbf{x})$, lo definiremos entonces como la cardinalidad de su soporte. Obviamente la relación $d(\mathbf{x}, \mathbf{y}) = ps(\mathbf{x} - \mathbf{y})$ es siempre válida. También definimos la *distancia mínima* de un código dado C como el mínimo de las distancias entre sus palabras codificadas distintas. Notemos entonces que para un código lineal su distancia mínima es el mínimo de los pesos de las palabras codificadas no cero.

La capacidad que tiene un código C para detectar y corregir errores depende del valor de su distancia mínima como lo muestra el siguiente resultado (cf. [46]), donde $\lfloor u \rfloor$ denota la parte entera de u.

Teorema 4 *Sea C un código lineal con distancia mínima d. Entoces C tiene la capacidad de detectar errores de transimisión de peso $\leq a$, $a \in \mathbb{N}$ si, y sólo si $d \geq a+1$. Además el código tiene capacidad de corregir errores de transmisión de peso $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$. En particular cuando d es par, el código puede detectar hasta $\frac{d}{2}$ errores, de los cuales es capaz de corregir hasta $\frac{d-2}{2}$.*

El espacio ortogonal a un $[n,k]$ código lineal C sobre $\mathbb{F}_q$ se conoce como *código dual a C* y es denotado como $C^{\perp}$, esto es

$$C^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^n : \mathbf{c} \cdot \mathbf{x} = 0, \text{ para toda } \mathbf{c} \in C \right\},$$

donde $\mathbf{c} \cdot \mathbf{x} = c_1x_1 + c_2x_2 + \cdots + c_nx_n$, es el producto interno usual en $\mathbb{F}_q^n$. Así $C^{\perp}$ resulta ser un $[n, n-k]$ código lineal sobre $\mathbb{F}_q$. No es difícil probar que el espacio dual de $C^{\perp}$ es C. (cf. [46]).

Ya que para un $[n,k]$ código lineal C su función de codificación puede ser expresada matricialmente, existen matrices G y H tales que

$$C = \left\{ \mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k \right\} = \left\{ \mathbf{x} \in \mathbb{F}_q^n : H\mathbf{x}^T = 0 \right\}.$$

La matriz G (resp. H) se conoce como *matriz generadora (resp. de chequeo de paridad)* del código. Los renglones de la matriz G forman una base para el código C, el cual a su vez es solución de un sistema homogéneo de ecuacionés lineales con matriz de coeficientes H. Utilizando operaciones elementales sobre los renglones de G y permutaciones de sus columnas podemos transformarla en una matriz de la forma $(I_k \mid A)$, conocida como la *forma estándard* de la matriz generadora, donde I_k es la matriz identidad de $k \times k$ y A es una matriz de $k \times (n-k)$. Es bien conocido (cf. [46]) que una matriz generadora de un código lineal C es una matriz de chequeo de paridad del código dual $C^{\perp}$ y viceversa. Además dadas matrices generadora G y de chequeo de paridad H de C se satisfacen las igualdades $HG^t = 0$ y $GH^t = 0$. Cuando la matriz G está dada en forma estándard, i.e. $G = (I_k \mid A)$, la matriz de chequeo de paridad se obtiene como $H = (-A^t \mid I_k)$, (cf. [46]).

El siguiente resultado nos muestra que existe una estrecha relación entre la distancia mínima de un código lineal y su matriz de chequeo de paridad (cf. [46]).

Aunque en general es difícil determinar la distancia mínima de un código, este teorema permite calcular fácilmente tal parámetro para algunas familias de códigos.

Teorema 5 *Sea C un código lineal con distancia mínima d y matriz de chequeo de paridad H. Entonces d es el menor entero positivo r para el cual existen r columnas linealmente dependientes en H.*

Hemos visto que un $[n, k, d]$ código lineal sobre $\mathbb{F}_q$ puede transmitir q^k mensajes y corregir $\left\lfloor \frac{d-1}{2} \right\rfloor$ errores que ocurran durante la transmisión. Por tales resultados lo ideal sería encontrar códigos con valores para k y d tan grandes como sea posible. Esto es, códigos cuya capacidad para transmitir información y corregir los errores ocurridos durante esta sea tan grande como sea posible. Desafortunadamente esta situación está limitada por los parámetros mismos del código, como lo indica la siguiente proposición (cf. [46]):

Proposición 6 ***(La cota Singleton)*** *Para todo $[n, k, d]$ código lineal C sobre $\mathbb{F}_q$ se cumple la desigualdad $d + k \leq n + 1$. Cuando la igualdad es válida se dice que C es* ***distancia máxima separable*** *o simplemente* ***MDS****.*

Se conocen varias desigualdades más que los parámetros de un código deben satisfacer. Una de las más útiles, enunciada en primer lugar por R. Hamming, por lo que también se conoce como *cota de Hamming*, es la siguiente (cf. [67]):

Proposición 7 ***(La cota por empaquetamiento con esferas)*** *Para todo $[n, k, d]$ código lineal sobre $\mathbb{F}_q$, si $\varrho = \lfloor (d-1)/2 \rfloor$, entonces*

$$q^k \left(1 + (q-1)\, n + (q-1)^2 \binom{n}{2} + \cdots + (q-1)^{\varrho} \binom{n}{\varrho} \right) \leq q^n.$$

1.1.1 Nuevos códigos a partir de los ya existentes

En Matemáticas es muy común obtener nuevas estructruas a partir de las ya conocidas. En Teoría de Códigos se conocen varias maneras de obtener nuevos códigos a partir de los ya conocidos, por ejemplo ya hemos mencionado al código dual. A continuación describiremos algunos de tales procedimientos (cf. [46]).

El **código extendido** $\widehat{C}$ del $[n, k]$ código C sobre $\mathbb{F}_q$ es el código de longitud $n + 1$ consistente de todos los vectores de la forma

$$\left(c_1, \ldots, c_n, -\sum_{i=1}^{n} c_i \right),$$

donde $(c_1, \ldots, c_n) \in C$. Esta forma de construir un nuevo código se denomina *añadir un chequeo de paridad total*, pues si $(c_1, \ldots, c_n, c_{n+1}) \in \widehat{C}$ entonces $\sum_{i=1}^{n+1} c_i = 0$. Si G y H son matrices generadora y de chequeo de paridad para C, respectivamente, entoces la matriz generadora $\widehat{G}$ para $\widehat{C}$ se obtiene añadiendo a G una columna de tal forma que la suma de las columnas de $\widehat{G}$ resulte el vector cero. Por otro lado una matriz de chequeo de paridad $\widehat{H}$ de $\widehat{C}$ se obtiene agregando a H una columna de ceros y un renglón de unos.

Ejemplo 8 El [7,4,3] código binario C con matrices generadora y de chequeo de paridad

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

respectivamente, se extiende al añadirle un chequeo de paridad total, a un [8,4,4] código lineal $\widehat{C}$ con matrices generadora y de chequeo de paridad como se describen a contiuación:

$$\widehat{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \qquad \widehat{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Sean C_1 un $[n_1, k_1, d_1]$ código y C_2 un $[n_2, k_2, d_2]$ código, ambos lineales sobre $\mathbb{F}_q$. Denotaremos al vector $\mathbf{v}$ concatenado al vector $\mathbf{u}$ como $|\mathbf{u}|\mathbf{v}|$. La **suma directa** de C_1 y C_2, denotada $C_1 \oplus C_2$, consiste de todos los vectores de la forma $|\mathbf{u}|\mathbf{v}|$ con $\mathbf{u} \in C_1$ y $\mathbf{v} \in C_2$. Entonces $C_1 \oplus C_2$ es un $[n_1 + n_2, k_1 + k_2, d = \min\{d_1, d_2\}]$ código lineal sobre $\mathbb{F}_q$ (note que esta no es la suma directa en el sentido del Álgebra Lineal) (cf. [46]).

La construcción $|\mathbf{u}|\mathbf{u} + \mathbf{v}|$. Sean C_1 y C_2 como en el párrafo anterior, y supóngase además que $n_1 = n_2 = n$. Podemos entonces formar un código C_3 consistente de las palabras codificadas $|\mathbf{u}|\mathbf{u} + \mathbf{v}|$, con $\mathbf{u} \in C_1$ y $\mathbf{v} \in C_2$. Entonces C_3 es un $[2n, k_1 + k_2, d = \min\{d_1 + d_2\}]$ código lineal sobre $\mathbb{F}_q$ (cf.[46]). A pesar de que se obtienen mejores resultados con esta construcción que con la suma directa, en los capítulos cuarto y quinto esta última jugará un papel importante en la construcción de códigos algunos de ellos alcanzando los mejores parámetros posibles.

Juxtaposición. Dados dos códigos sobre el mismo campo finito, con parámetros $[n_1, k, d_1]$ y $[n_2, k, d_2]$ respectivamente, se obtiene un $[n_1 + n_2, k, d_1 + d_2]$-código al escribir las matrices generadoras de los códigos una después de la otra (cf. [6]).

Producto directo. Si G_t es la matriz generadora de un $[n_t, k_t, d_t]$-códigos lineal, $t = 1, 2$, y $G_1 = (g_{i,j})$ entonces $G_1 \otimes G_2 := (g_{i,j}G_2)$ es una matriz generadora de un $[n_1 n_2, k_1 k_2, d_1 d_2]$-código lineal.

Métodos adicionales para combinar códigos pueden encontrarse en [46], capítulo 18, y en [6].

1.2 Decodificación con síndrome

Hasta este punto hemos explicado la forma de codificar un mensaje, ahora nos dedicaremos al problema de decodificar el mensaje recibido. Existen varias maneras de hacer esto, aunque algunas sólo se aplican a ciertas familias de códigos. Aquí explicaremos un proceso general de decodificación, el cual sólo es eficiente para valores pequeños de la longitud y la distancia mínima.

Definición 9 *Sea H la matriz de chequeo de paridad de un código lineal sobre $\mathbb{F}_q$. Para todo $\mathbf{x} \in \mathbb{F}_q$ se define el* ***síndrome*** *de $\mathbf{x}$ como $S = H\mathbf{x}^t$.*

Con esta definición podemos caracterizar al código lineal C como el conjunto de todos los elementos de $\mathbb{F}_q$ con síndrome cero.

El síndrome induce una partición en el espacio $\mathbb{F}_q^n$ como lo señala la siguiente proposición (cf. [67]):

Teorema 10 *Sean C un código lineal de longitud n sobre $\mathbb{F}_q$ y H una matriz de chequeo de paridad de C. Entonces los vectores $\mathbf{x}$ e $\mathbf{y}$ de $\mathbb{F}_q^n$ tienen el mismo síndrome si, y sólo si están en la misma clase del espacio cociente $\mathbb{F}_q^n/C$. Además para un código lineal binario el síndrome es igual a la suma de las columnas de la matriz de chequeo de paridad H donde ocurrieron los errores.*

Enseguida se resume el método de decodificación con síndrome (cf. [46]):

Teorema 11 *Sea C un código lineal. La palabra recibida $\mathbf{x}$ debe decodificarse como la palabra codificada $\mathbf{c} = \mathbf{x} - \mathbf{a}$, donde $\mathbf{a}$ es una palabra de peso mínimo $\leq \lfloor (d-1)/2 \rfloor$ en la clase $\mathbf{x} + C$ del espacio cociente $\mathbb{F}_q^n/C$. Dicho de otra manera $\mathbf{a}$ es la palabra con el menor peso entre las que tienen el mismo síndrome que $\mathbf{x}$.*

En el teorema precedente si no existe una palabra de peso a lo más $\lfloor (d-1)/2 \rfloor$ en la clase $\mathbf{x} + C$ entonces no es posible elegir en esta clase una palabra codificada como la más probable de haber sido enviada si se recibió el vector $\mathbf{x}$.

1.3 El polinomio enumerador de pesos

Dado un código cualquiera de longitud n, un problema interesante en Teoría de Códigos es determinar el número A_i de palabras codificadas de peso i, $0 \leq i \leq n$. A la sucesión $A_0, \ldots, A_n$ se le conoce como *distribución de peso* del código. El problema es difícil en general, pero F. J. MacWilliams (cf. [45]) obtuvo una fórmula que permite determinar la distribución de peso (y por lo tanto la distancia mínima) del código dual, conociendo la del código original. Por este resultado, entre un código y su dual

muchas veces se trabaja con el código con menor número de palabras codificadas. Enseguida enunciaremos tal resultado y mostraremos algunas de sus consecuencias.

MacWilliams definió un polinomio cuyos coeficientes son los números A_i, el cual nos da información sobre la estructrua del código. Tal polinomio, que definimos a continuación, ha resultado sumamente últil en el estudio de la teoría que nos ocupa, además varias generalizaciones y resultados análogos han sido obtenidos desde entonces, como se hace por ejemplo en [16, 20, 30, 36, 47]. La definición del polinomio es

Definición 12 *Dado un código lineal C definido sobre $\mathbb{F}_q$ su* ***polinomio enumerador de pesos,*** *$\mathcal{E}_C$, está definido como*

$$\mathcal{E}_C(x) = \sum_{\mathbf{c}\in C} x^{ps(\mathbf{c})}.$$

Si n denota la longitud de C, también es frecuente expresar este polinomio de la siguiente forma

$$\mathcal{E}_C(x,y) = \sum_{\mathbf{c}\in C} x^{ps(\mathbf{c})} y^{n-ps(\mathbf{c})} = \sum_{i=0}^{n} A_i x^i y^{n-i}.$$

El siguiente resultado es conocido como *la identidad de MacWilliams (cf. [46]):*

Teorema 13 ***(MacWilliams)*** *Los polinomios enumeradores de pesos de un código lineal C sobre $\mathbb{F}_q$ y su dual $C^\perp$ están relacionados por la siguiente ecuación*

$$\mathcal{E}_{C^\perp}(x,y) = \frac{1}{|C|}\mathcal{E}_C\left(y-x, y+(q-1)x\right). \tag{1.1}$$

1.3.1 Polinomios de Krawtchouk

Aunque la identidad de MacWilliams determina completamente al polinomio enumerador de pesos de un código lineal, en una situación práctica puede ser que no todos los elementos de la distribución de peso de un código sean conocidos. Para resolver este problema V. Pless definió en 1963 los *momentos* (cf. [56]), para los cuales los polinomios de Krawtchouk, un tipo especial de polinomios ortogonales, resultan sumamente importantes.

A lo largo de esta sección supondremos que los polinomios enumeradores de pesos del $[n,k]$ código C y su dual son $\mathcal{E}_C(x,y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$ y $\mathcal{E}_{C^\perp}(x,y) = \sum_{i=0}^{n} D_i x^i y^{n-i}$ respectivamente.

Definición 14 *Sea q una potencia del primo p y n, k enteros con $0 \leq k \leq n$, el polinomio $Q_k(x;n) := Q_k(x) \in \mathbb{R}[x]$ con función generadora*

$$(1+(q-1)z)^{n-x}(1-z)^x = \sum_{k=0}^{\infty} Q_k(x)\ z^k \tag{1.2}$$

se denomina ***polinomio de Krawtchouk.***

Desarrollando el miembro derecho de (1.2) se observa que el polinomio de Krauthcouk tiene la siguiente expresión

$$Q_k(x) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j}\binom{n-x}{k-j}.$$

Se conocen expresiones equivalentes para $Q_k(x)$, como son las siguientes [3, 46]:

$$\begin{aligned} Q_k(x) &= \sum_{j=0}^{k} (-q)^j (q-1)^{k-j} \binom{n-j}{k-j}\binom{x}{j}. \\ Q_k(x) &= \sum_{j=0}^{k} (-1)^j q^{k-j} \binom{n-k+j}{j}\binom{n-x}{k-j}. \end{aligned}$$

La primera de estas igualdades se obtiene expresando el miembro izquierdo de (1.2) como $(1-(q-1)z)^n \left(1-\frac{qz}{1+(q-1)z}\right)^x$. Pero si lo reescribimos para que tome la forma $(1-z)^n\left(1+\frac{qz}{1-z}\right)^{n-x}$ conseguimos la última de las ecuaciones. Por lo tanto el polinomio de Krawtchouk es un polinomio de grado k en la indeterminada x.

La identidad de MacWilliams (1.1) es

$$\sum_{i=0}^{n} A_i x^i y^{n-i} = \frac{1}{|C^{\perp}|} \sum_{i=0}^{n} A'_i (y-x)^i (y+(q-1)x)^{n-i}.$$

Haciéndo $y = 1$ resulta

$$\sum_{i=0}^{n} A_i x^i = \frac{1}{q^{n-k}} \sum_{i=0}^{n} D_i (1-x)^i (1+(q-1)x)^{n-i}. \tag{1.3}$$

Para $x = 1$ la relación (1.3) se reduce a

$$\sum_{i=0}^{n} \frac{A_i}{q^k} = 1.$$

Además, como puede verse fácilmente, los enumeradores de pesos del código C y de su dual están relacionados por la igualdad

$$D_k = \frac{1}{|C|} \sum_{i=0}^{n} A_i Q_k(i).$$

Derivando (1.3) con respecto a x y tomando el límite cuando y tiende a 1 se obtiene el primer momento:

$$\sum_{i=1}^{n} \frac{iA_i}{q^k} = \frac{1}{q}\left(n(q-1) - D_1\right) = \frac{q-1}{q} n, \quad \text{si} \quad D_1 = 0.$$

Esto es, cuando $D_1 = 0$, el peso medio del código es $n\,(q-1)\,/q$. Similarmente obtenemos los llamados *momentos binomiales* de $A_0, A_1, \ldots, A_n$, que en el caso bianario son como se muestra a continuación (cf. [46])

$$\sum_{i=r}^{n} \binom{i}{r} \frac{A_i}{2^k} = \frac{1}{2^r} \sum_{i=0}^{r} (-1)^i \binom{n-i}{r-i} D_i$$

para $r = 0, 1, \ldots, n$

Si se conoce la distancia mínima $d^\perp$ del código dual y $r < d^\perp$, la ecuación anterior se reduce a

$$\sum_{i=r}^{n} \binom{i}{r} \frac{A_i}{2^k} = \frac{1}{2^r} \binom{n}{r}.$$

En otras palabras el r-ésimo momento binomial, para $r = 0, 1, \ldots, d^\perp - 1$ es independiente del código.

1.4 Estructuras de incidencia

En esta sección se recuerdan las definiciones de estructura de incidencia y diseño así como algunos resultados básicos sobre el tema (una mayor información puede encontrarse en [1, 66, 75]). Los diseños son estructuras combinatorias que presentan una regularidad tal en sus parámetros que permiten sean utilizados para producir códigos correctores de errores importantes desde el punto de vista práctico, por ejemplo los códigos generalizados de Reed-Muller (cf. [1]). Otra de sus aplicaciones prácticas es a la Criptografía (cf. [2, 9, 74]), por último [9] es una amplia referencia sobre varios de sus usos.

Definición 15 *Una* ***estructura de incidencia finita*** *es una tripleta de conjuntos* $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, *donde* $\mathcal{P}$ *y* $\mathcal{B}$ *son conjuntos finitos y ajenos e* $\mathcal{I}$ *es un subconjunto no vacío del producto cartesiano* $\mathcal{P} \times \mathcal{B}$. *Los elementos de* $\mathcal{P}$ *son llamados* ***puntos*** *o* ***variedades***, *mientras que a los de* $\mathcal{B}$ *se les conoce como* ***bloques***. *Si* $(p, B) \in \mathcal{I}$ *diremos que* p *es* ***incidente*** *con* B.

Algunas veces existe una correspondencia biunívoca entre los bloques y los conjuntos de puntos incidentes a estos. Por ejemplo cuando $\mathcal{B}$ es el conjunto potencia de $\mathcal{P}$, y el punto $p \in \mathcal{P}$ es incidente con el bloque B si y sólo si $p \in B$. Cuando existe tal correspondencia usualemente se escribe $p \in B$ en lugar de $(p, B) \in \mathcal{I}$. Por otro lado en una estructura de incidencia finita arbitraria es posible que bloques distintos sean incidentes con el mismo número de puntos, es decir existen los llamados *bloques repetidos.* Estructuras de incidencia sin esta última característica se denominan *simples.*

Una de las clases más estudiadas de estructuras de incidencia es la de los llamados *diseños de bloques,* que nosotros llamaremos simplemente *diseños.* Estas estructuras han sido utilizadas en la Estadística y más tarde en la Teoría de Códigos (cf. [1]), y la Criptografía (cf. [2, 9, 74]).

Definición 16 *Sean t, v, k y λ cuatro enteros no negativos. Una estructura de incidencia $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ es un t-(v, k, λ)* ***diseño,*** *o brevemente un* ***t-diseño,*** *si existen v puntos, cada bloque es incidente con exactamente k puntos y cualesquiera t puntos son incidentes con precisamente λ bloques.*

Supongamos ahora que $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ es un t-(v, k, λ) diseño. Si $t = \lambda = 1$ el diseño es simplemente una partición de $\mathcal{P}$ en subconjuntos de cardinalidad k. Cuando $k = 2$, $\mathcal{D}$ es una gráfica no dirigida y sin lazos, con conjunto de vértices $\mathcal{P}$ y cuyas aristas son los bloques. Por último si $t = 1$, el diseño es llamado *configuración táctica.*

Se sabe que el número de bloques de un t-(v, k, λ) diseño, denotado por b, satisface la igualdad (cf. [1]):

$$b\binom{k}{t} = \lambda\binom{v}{t}. \tag{1.4}$$

Es igualmente un hecho bien conocido que un t-diseño es también un s diseño, para todo entero positivo $s \leq t$. (cf. [1]).

Una estructura de incidencia finita puede ser descrita matricialmente a través de su *matriz de incidecia.*

Definición 17 *Sea $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ una estructura de incidencia finita con conjunto de puntos $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ y bloques $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$. Una* ***matriz de incidencia*** *para $\mathcal{S}$ es una matriz $A(\mathcal{S}) = (a_{i,j})$ de $b \times v$, donde $a_{i,j} = \chi_{\mathcal{I}}(p_j, B_i)$ y χ_Y es la función característica del conjunto Y. El renglón $(a_{i,1}, a_{i,2}, \ldots, a_{i,v})$ de A, denotado como $\mathbf{v}^{B_i}$, se conoce como el* ***vector de incidencia*** *del bloque B_i.*

En particular cuando $\mathcal{S}$ resulte ser un diseño, la matriz de incidecia de $\mathcal{S}$ tendrá k entradas igual a uno en cada renglón, y r entradas no cero en cada columna.

Por ejemplo un *sistema triple de Steiner* es un 2-$(v, 3, 1)$ diseño (descubiertos por T. P. Kirkman en 1847) y un *sistema cuádruple de Steiner* es un 3-$(v, 4, 1)$ diseño (c.f. [1], pág. 296).

En las referencias [1] y [46] se mencionan algunos diseños asociados a códigos lineales. Más interesante para nosotros será el ampliamete estudiado problema inverso, estos es, construir códigos a partir de diseños y en general a estructuras de incidencia.

Definición 18 *El $\mathbb{F}_q$-código lineal asociado a la estructura de incidencia $\mathcal{S}$, $C_q(\mathcal{S})$, es el $\mathbb{F}_q$-espacio vectorial generado por los vectores de incidencia de $\mathcal{S}$.*

Entonces los renglones de la matriz de incidencia de $A(\mathcal{S})$ constituyen un conjunto de generadores para el código $C_q(\mathcal{S})$. Por ejemplo entre las familias más estudiadas de códigos asociados a diseños se encuetra la de los códigos generalizados de Reed-Muller (cf. [1]), la cual estudiaremos en la siguiente sección.

1.5 Los códigos de Reed-Muller

Los códigos de Reed-Muller forman una de las familias de códigos que mejor han sido estudiadas, tanto por sus propiedades teóricas como prácticas. Fueron descubiertos, en el caso binario, por I. S. Reed (cf. [63]) y D. E. Muller (ver [50]) y generalizados más tarde de manera independiente, entre otros, por P. Delsarte en [12], por T. Kasami, S. Lin y W. W. Peterson en [33], por J. L. Massey, D. J. Costello y J. Justensen en [48], C. Rentería y H. Tapia-Recillas en [61], etc. Esta familia de códigos alcanza valores óptimos en sus parámetros para valores pequeños de éstos, además se conocen métodos eficientes para codificar y decodificar mensajes haciendo uso de sus propiedades. Por estas razones han sido empleados en la práctica. Por ejemplo en 1972 el *Mariner 9* utilizó un $[32, 6, 16]$ código binario para transmitir fotografías en blanco y negro del planeta Marte, donde cada elemento de $\mathbb{F}_2^6$ correspondía a un tono de gris (cf. [34, 67]). El código empleado es un miembro de la familia que estudiaremos en esta sección.

Una manera de definir los códigos de Reed-Muller es a través de funciones del espacio vectorial $\mathbb{F}_q^m$ en el campo $\mathbb{F}_q$. Tales funciones son todas de tipo polinomial, como lo afirma el siguiente lema [1]:

Lema 19 *Supongamos que $\mathbf{w} = (w_1, w_2, \ldots, w_m)$ es un elemento de $\mathbb{F}_q^m$. Entonces su función característica está dada por*

$$\chi_{\mathbf{w}}(x_1, \ldots, x_m) = \prod_{i=1}^{m} \left[1 - (x_i - w_i)^{q-1}\right].$$

Como todo elemento de $\mathbb{F}_q$ satisface la ecuación $x^q = x$ podemos reducir estos polinomios módulo $x_i^q - x_i$, para $i = 1, 2, \ldots, m$. Por lo tanto en el anillo $\mathbb{F}_q[x_1, \ldots x_m] / (x_1^q - x_1, \ldots, x_m^q - x_m) = \oplus_{r \geq 0} A_r$, donde A_r es la componente homogénea de grado r, están contenidas todas las funciones antes mencionadas. Con estas observaciones estamos ya en condiciones de dar la definición de los códigos generalizados de Reed-Muller [1]:

Definición 20 *Sea m un entero positivo y q una potencia de un primo. Para cualquier entero ρ tal que $0 \leq \rho \leq m(q-1)$, el* ***código generalizado de Reed-Muller de orden*** *ρ, sobre el campo $\mathbb{F}_q$, denotado como $RM_q(\rho, m)$, es el conjunto*

$$RM_q(\rho, m) = \{(f(p_1), \ldots, f(p_{q^m})) : f \in \oplus_{0 \leq r} A_r\},$$

donde $p_1, \ldots, p_{q^m}$ son los distintos puntos de $\mathbb{F}_q^m$.

Enunciamos sin demostaración algunas de las propiedades de esta familia de códigos (cf. [1, 61])

Teorema 21 *Para todo entero ρ, con $0 \leq \rho \leq m(q-1)$, se tiene*

$$a) \quad \dim(RM_q(\rho, m)) = \sum_{i=0}^{\rho} \sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{i-kq+m-1}{i-kq}.$$

$$b) \quad RM_q(\rho, m)^{\perp} = RM_q(m(q-1) - 1 - \rho, m)$$

Además si $\rho = r(q-1) + s < m(q-1)$ con $0 \leq s < q-1$ entonces el código $RM_q(\rho, m)$ tiene distancia mínima $(q-s)\, q^{m-r-1}$.

De mayor importancia en el desarrollo del presente trabajo serán los códigos binarios de Reed-Muller. En este caso el código $RM_q(\rho, m)$ será denotado simplemente como $RM(\rho, m)$. Los parámetros de esta familia están dados en el siguiente resultado [1]:

Corolario 22 *Para todo entero ρ, con $0 \leq \rho \leq m$, el código $RM(\rho, m)$ tiene longitud 2^m, su distancia mínima es $2^{m-\rho}$ y su dimensión es:*

$$\dim(RM(\rho, m)) = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{\rho}.$$

Cualquier código lineal con los parámetros de un código binario de Reed-Muller es equivalente a un código de este último tipo [46]. En [1] encontramos el siguiente resultado que relaciona los códigos binarios de Reed-Muller con la geometría finita afín sobre el campo binario, en particular los autores hacen notar que las variedades afines de dimensión ρ en $\mathbb{F}_2^m$ son los bloques de un 2-diseño, cuyos puntos son los elementos de este espacio.

Proposición 23 *Los vectores de peso mínimo del código $RM(m-\rho, m)$ son los vectores de incidencia de las variedades afines de dimensión ρ, en la geometría afín de dimensión m sobre el campo con dos elementos. Además tal código es generado por sus vectores de peso mínimo.*

Sin embargo no fue sino hasta 1998 cuando Gao y Key [15] determinan una base para este tipo de códigos consistente de vectores de incidencia de variedades afines.

Una manera alternativa de obtener los códigos binarios de Reed-Muller es a través de la construcción $|\mathbf{u}|\ \mathbf{u}+\mathbf{v}|$, como se describe en [46] (pág. 374) este es un método recursivo muy simple:

$$RM(\rho+1,m+1)=\{|\mathbf{u}|\ \mathbf{u}+\mathbf{v}|:\mathbf{u}\in RM(\rho+1,m),\ \mathbf{v}\in RM(\rho,m)\}.$$

Recientemente se han estudiado códigos análogos a los generalizados de Reed-Muller, como en [40] donde se generalizan estos códigos a través de una construcción de algunos de sus subcódigos. También se ha considerado el problema de restringir el conjunto sobre el cual se evalúan los polinomios en $\oplus_{0\leq r}A_r$ o bien en A_r, o incluso ya no evaluarlos en un subconjunto del espacio afín, sino en el proyectivo, por ejemplo: en [72] se evalúan los polinomios en A_r en los puntos del espacio proyectivo, los códigos obtenidos al evaluar los poliniomios en A_r en un conjunto que es una interseción completa en el espacio proyectivo son estudiados en [14], mientras que en la referencia [17] el conjunto elegido son los puntos de la variedad de Segre y en [62] son los puntos de una variedad de Veronese. Los códigos binarios de Reed-Muller son recuperados a partir de un conjunto parcialmente ordenado en [4], mientras que en [57] se muestra que los códigos binarios de primer orden están relacionados a ciertos estructuras combinatorias denominadas matroides.

1.5.1 Códigos binarios de Hamming

Los códigos binarios de Hamming forman la primer familia de códigos construida. Enseguida se mencionarán sus parámetros.

Si se suprime una posición coordenada arbitraria pero fija a cada una de las palabras del código $RM(\rho,m)$ se disminuye tanto su longitud como su distancia mínima en una unidad conservando su dimensión. Como veremos en el siguiente capítulo esta simple operación permite la implementación de este tipo de códigos sin que se requiera de una cantidad significativa de memoria en su almacenamiento.

Definición 24 *El* ***código agujerado de Reed-Muller*** $RM(\rho,m)^*$ *está definido para* $0\leq\rho\leq m$ *como el código que se obtiene de* $RM(\rho,m)$ *al suprimirle una posición coordenada fija a cada una de sus palabras codificadas.*

Dado un entero $m\geq 2$, los códigos $RM(m-2,m)^*$ se denotan $\mathcal{H}_m$ y son también conocidos como *códigos binarios de Hamming.* Usualmente este código se define como aquel cuyas columnas de su matriz de chequeo de paridad H son las representaciones en base dos de los enteros positivos menores a 2^m (obviamente H tiene m renglones). Por lo tanto $\mathcal{H}_m$ tiene parámetros $[2^m, 2^m-m-1, 3]$. Esta es la primer familia de códigos que se contruyó, precisamente por R. Hamming en 1950 (cf. [25]).

Cuando un mensaje es codificado no existe garantía de que el vector recibido pueda ser correctamente decodificado, incluso puede suceder que sea imposible decodificarlo. Si todo mensaje recibido puede ser decodificado (correcta o incorrectamente) el código se dice *perfecto,* o más formalmente enunciamos la siguiente

Definición 25 *Sea C un $[n, k, d]$ código lineal sobre $\mathbb{F}_q$. Si las esferas de radio $t = \lfloor \frac{d-1}{2} \rfloor$ con centro en las palabras codificadas de C forman una partición del espacio $\mathbb{F}_q^n$, entonces el código se dice* **perfecto.**

Los códigos binarios de Hamming son perfectos (cf. [46], pág. 25). Al igual que los códigos binarios de Reed-Muller los códigos de Hamming pueden generalizarse a cualquier campo finito. Como antes, podemos afirmar que los códigos generalizados de Hamming son así mismo códigos perfectos (cf. [1], pág. 58).

CAPÍTULO 2

CÓDIGOS CUASI-CÍCLICOS

Desde que los llamados códigos cíclicos fueron descubiertos han constituido una de las familias más utilizadas en la práctica. Han sido implementados, por ejemplo, para corregir los errores que ocurren en los "chips" de memoria de las computadoras (cf. [34]), en la transmisión de fotografías desde el espacio exterior (cf. [34]) y en la reproducción de discos compactos (cf. [34]). La razón principal de su amplio uso se encuentra en la facilidad para implementarlos, pues en el proceso de codificación solamente se utiliza la suma de vectores binarios y corrimientos cíclicos. Además los códigos lineales que son cíclicos gozan de la propiedad de contar con una base formada de un vector y algunos de sus corrimientos cíclicos, por lo que almacenar el código no requiere de un gasto significativo de memoria. Definiremos un código cíclico como aquel en el cual el corrimiento de una palabra codificada resulta en una palabra codificada. Al generalizar este concepto sustituyendo la palabra "corrimento cíclico" por "t corrimientos cíclicos", t un entero positivo, estaremos ante los códigos cuasi-cíclicos.

En la primera sección de este capítulo definimos un código cíclico y damos algunas de sus propiedades básicas. En la segunda sección estudiamos las relaciones de recurrencia lineal que nos permitirán determinar la dimensión de algunos códigos lineales. En la tercera sección definimos los conceptos de matriz circulante y código cuasi-cíclico. Una mayor información de tales códigos puede consultarse en [46], capítulo 16.

2.1 Códigos Cíclicos

El concepto de código cíclico es muy importante tanto desde el punto de vista práctico, pues tales códigos son fácilmente implementados sin un gasto significativo de memoria en su almacenamiento, y también desde el punto de vista teórico, pues pueden ser pensados como ideales de un anillo de polinomios.

Diremos que un código C es *cíclico* si es invariante bajo corrimientos cíclicos, esto es, si $(a_0, a_1, \ldots, a_{n-1}) \in C$ implica $(a_{n-1}, a_0, a_1 \ldots, a_{n-2}) \in C$.

Es fácil convencerse que la función

$$\begin{gathered} \psi : \mathbb{F}_q^n \longrightarrow R_n = \mathbb{F}_q[x]/(x^n - 1) \\ (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \end{gathered}$$

es un isomorfismo de $\mathbb{F}_q$-espacios vectoriales, donde un corrimiento cíclico en $\mathbb{F}_q^n$ corresponde a una multiplicación por x en R_n. Bajo esta función ψ un código lineal C de longitud n sobre $\mathbb{F}_q$ es cíclico si y sólo si $\psi(C)$ es un ideal de R_n (cf. [46]), razón por la cual de aquí en adelante llamaremos indistintamente código cíclico tanto al código lineal en sí como al ideal correpondiente.

Enseguida resumimos algunas de las propiedades básicas de un código cíclico lineal, la demostración puede consultarse por ejemplo en [46].

Teorema 26 *Sea C un código lineal de longitud n sobre $\mathbb{F}_q$. Entonces*

a) existe un único polinomio mónico $g(x)$ en C, de grado minimal, que divide a toda palabra codificada. Tal polinomio recibe el nombre de ***polinomio generador*** *para C.*

b) $g(x)$ divide a $x^n - 1$ en $\mathbb{F}_q[x]$.

c) si $g(x)$ es de grado r todo mensaje $f(x)$ es de grado menor que $n - r$. La codificación de $f(x)$ es $f(x)\,g(x)$, y la dimensión de C es $n - r$.

d) si $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, una matriz generadora del código C es

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{r-1} & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{r-2} & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{r-3} & g_{r-2} & g_{r-1} & g_r & \cdots & 0 \\ \vdots & & & \vdots & & \vdots & & & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{pmatrix}.$$

e) El polinomio $h(x) = \frac{x^n-1}{g(x)}$ se denomina ***polinomio de chequeo de paridad*** *del código C. El código dual $C^\perp$ es cíclico, y su polinomio generador es un múltiplo constante de $h^*(x) = x^{n-r}h(1/x)$ (el* ***polinomio recíproco*** *de $h(x)$).*

Entre las familias de códigos cíclicos más importantes se encuentran los códigos binarios agujerados de Reed-Muller $RM(\rho, m)^*$, y por lo tanto también los códigos binarios de Hamming, los códigos BCH y de Reed-Solomon (cf. [46], capítulos 9 y 10). En particular los códigos de Reed-Solomon se han implementado en los reproductores de discos compactos (cf. [34]).

2.2 Sucesiones generadas por recurrencias lineales

Las sucesiones generadas por relaciones de recurrencia son de gran importacia en varias ramas de la Matemática, y como tales sucesiones pueden ser fácilmente implementadas, utilizando los llamados registros de retroalimentación, resultan de gran importancia en la práctica. Cuando los términos dependen linealmente de cierto número de valores iniciales la sucesión se denomina *recurrencia lineal.* Estas sucesiones son aplicadas en la Teoría de Códigos, entre otras cosas para decodificar los llamados códigos *BCH* (cf. [46]), en la Criptografía, para generar sucesiones pseudoaleatorias (cf. [13, 42]), etc. A continuación describiremos las principales definiciones y resultados relativos al tema.

Sean L un entero positivo y $\{a_0, a_1, \ldots, a_{L-1}\}$, $\{s_0, s_1, \ldots, s_{L-1}\}$ dos sucesiones finitas de elementos en el campo $\mathbb{F}_q$. La sucesión de elementos de $\mathbb{F}_q$ generada por la relación

$$s_{n+L} = a_{L-1}s_{n+L-1} + a_{L-2}s_{n+L-2} + \cdots + a_0 s_n \tag{2.1}$$

para $n \geq 0$, es llamada *sucesión homogénea de recurencia lineal (de L-ésimo órden).*

Asociado a tal relación de recurrencia tenemos al polinomio

$$m(x) = x^L - a_{L-1}x^{L-1} - a_{L-2}x^{L-2} - \cdots - a_0 \in \mathbb{F}_q[x] \tag{2.2}$$

conocido como *polinomio característico* de la sucesión de recurrencia. El vector $\mathbf{s}_i$ definido como $\mathbf{s}_i = (s_i, s_{i+1}, \ldots, s_{i+L-1})$ se denomina *i-ésimo vector de estado* de la sucesión, y $\mathbf{s}_0$ es el *vector de estado inicial.* Los vectores de estado pueden también ser generados matricialmente por medio de la matriz compañera de $m(x)$,

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{L-1} \end{pmatrix}.$$

Si $L = 1$ entonces $A = (a_0)$. La manera de obtener los vectores de estado es como se describe enseguida (cf. [42]):

Proposición 27 *Sea $\{s_i\}_{i\in\mathbb{N}}$ una sucesión homogénea de recurrencia lineal generada por la relación (2.1) y sea A la matriz compañera de su polinomio característico. Entonces los vectores de estado de la sucesión satisfacen la relación*

$$\mathbf{s}_i = \mathbf{s}_0 A^i, \quad \text{para } i = 0, 1, 2, \ldots$$

El polinomio $m(x)$ recibe el nombre de *polinomio característico* de la sucesión porque es el polinomio característico de A, i.e., $m(x) = \det(xI - A)$, con I la matriz identidad de $L \times L$, sobre $\mathbb{F}_q$.

De mayor importancia en nuestro trabajo será el siguiente resultado (cf. [42]) en el cual utilizamos el concepto de *recíproco* de un polinomio $F(x)$ de grado m, que se define como $F^*(x) = x^m F\left(\frac{1}{x}\right)$.

Teorema 28 *Sean $\{s_i\}_{i\in\mathbb{N}}$ una sucesión homogénea de recurrencia lineal sobre $\mathbb{F}_q$ generada por (2.1) la cual es periódica con periodo r y supongamos además que $m^*(x) \in \mathbb{F}_q[x]$ es el recíproco de su polinomio característico. Entonces la ecuación*

$$f(x)\, m^*(x) = (x^r - 1)\, P(x) \tag{2.3}$$

es válida para

$$f(x) = \sum_{k=0}^{L-1} s_k\, x^k \qquad y \qquad P(x) = \sum_{j=0}^{L-1} \left(\sum_{i=0}^{j} a_{i+L-j} s_i \right) x^j,$$

donde $a_L = -1$.

Demostración La igualdad en (2.3) se verifica al comparar los coeficientes en ambos miembros. ■

Como debe ser claro, una sucesión de recurrencia lineal puede satisfacer muchas relaciones lineales de recurrencia aparte de la que la define. Por ejemplo, la sucesión constante $0, 0, 0, \ldots$ satisface cualquier relación lineal homogénea, y una sucesión periódica de recurrencia lineal con periodo r satisface las relaciones $s_{i+nr} = s_i$, para $i = 0, 1, \ldots$ y todo entero positivo n. El número de componentes de un dispositivo de retroalimentación que genera una sucesión de recurrencia lineal dada, depende del grado del polinomio característico con el cual se está generado la sucesión. Por esta razón resulta conveniente conocer un polinomio característico de grado mínimo. Se sabe que un polinomio con estas características es único, salvo múltiplos constantes y que goza de varias propiedades adicionales, por ejemplo, es fácil obtener de él el periodo mínimo de la sucesión (cf. [42]). El grado de tal polinomio es conocido como la *complejidad lineal* de la sucesión. Para fines de futura referencia damos la definción de este concepto.

Definición 29 *Sea $S = \{s_n\}_{n=0}^{\infty}$ una sucesión infinita de elementos del campo finito $\mathbb{F}_q$. El menor entero positivo L para el cual existen elementos $a_0, \ldots, a_{L-1}$ en $\mathbb{F}_q$ que satisfacen la ecuación (2.1) para $n \geq 0$, es llamada la* ***complejidad lineal*** *de S. Cuando no existe tal entero L se dice que la complejidad lineal es infinita.*

El *algorítmo de Berlekamp-Massey* (cf. [42]) nos proveé de un método recursivo para calcular el polinomio de grado mínimo de una sucesión homogénea de recurrencia lineal dada.

Sea $s_0, s_1, \ldots$ una sucesión de elementos de $\mathbb{F}_q$ generada por la relación (2.1), en la que tomamos $L = k$. Para $j = 0, 1, \ldots$ definamos polinomios $G(x) = \sum_{i=0}^{2k-1} s_i x^i$, $g_j(x)$, $h_j(x) \in \mathbb{F}_q[x]$, enteros m_j y elementos $b_j \in \mathbb{F}_q$ como se muestra enseguida. Las condiciones iniciales para el algorítmo son

$$g_0(x) = 1, \quad h_0(x) = x, \quad \text{y} \quad m_0 = 0.$$

El elemento b_j $(j = 0, 1, \ldots)$ será el coeficiente de x^j en el polinomio $g_j(x) G(x)$. Para $j \geq 0$ se procede recursivamente mediante las relaciones

$$g_{j+1}(x) = g_j(x) - b_j h_j(x),$$

$$h_{j+1}(x) = \begin{cases} b_j^{-1} x g_j(x) & \text{si } b_j \neq 0 \text{ y } m_j \neq 0, \\ x h_j(x) & \text{en otro caso} \end{cases}$$

$$m_{j+1} = \begin{cases} -m_j & \text{si } b_j \neq 0 \text{ y } m_j \neq 0, \\ m_j + 1 & \text{en otro caso} \end{cases}$$

Si se conoce el grado k del polinomio característico minimal de la sucesión $\{s_i\}$ entonces $g_{2k}(x)$ es su recíproco. Por lo tanto el polinomio minimal $m(x)$ es $m(x) = x^k g_{2k}(1/x)$. Pero si la única información con que se cuenta es que el grado del polinomio minimal no excede a k, entonces hacemos $r = \left\lfloor k + \frac{1}{2} - \frac{1}{2} m_{2k} \right\rfloor$. En este caso el polinomio $m(x)$ es calculado como $m(x) = x^r g_{2k}(1/x)$.

2.3 Matrices circulantes

Las familia de las así llamadas *matrices circulantes* (cf. [46], pág. 500) jugará un papel muy importante en el desarrollo posterior de este trabajo, por lo que enunciaremos algunos resultados sobre el tema y su relación con la Teoría de Códigos.

Definición 30 *Si r es un entero positivo y $s_0, s_1, \ldots, s_{r-1}$ es una sucesión de elementos de $\mathbb{F}_q$, entonces la matriz cuadrada*

$$A = \begin{pmatrix} s_0 & s_1 & \cdots & s_{r-1} \\ s_{r-1} & s_0 & \cdots & s_{r-2} \\ \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 & \cdots & s_0 \end{pmatrix} \tag{2.4}$$

se dice ***circulante.***

A continuación se recordarán algunas de las propiedades de esta clase de matrices. Para mayores detalles se pude consultar por ejemplo [46], página 500.

Teorema 31 *i) La álgebra de matrices circulantes de $r \times r$ es isomorfa a la álgebra de polinomios $\mathbb{F}_q[x]/(x^r - 1)$. Bajo este isomorfismo, φ digamos, a la matriz A en (2.4) le corresponde el polinomio $\varphi(A) = \sum_{i=0}^{r-1} s_i x^i$.*

ii) La matriz circulante A es invertible si y sólo si $\varphi(A)$ es primo relativo a $x^r - 1$. Su matriz inversa, si existe, es B, donde $\varphi(A)\varphi(B) \equiv 1 \pmod{x^r - 1}$.

iii) Si A es una matiriz circulante con $\varphi(A) = \sum_{i=0}^{r-1} s_i x^i$ entonces A^t es la matriz circulante correspondiente al polinomio $\varphi(A^t) = s_0 + s_{r-1}x + \cdots + s_1 x^{r-1}$.

iv) Si P es la matriz circulante correspondiente al polinomio x entonces una $\mathbb{F}_q$-base de las matrices circulantes es $\{P^i : 0 \leq i < r\}$. La matriz circulante A en (2.4) puede escribirse como $A = \sum_{i=0}^{r-1} s_i P^i$.

v) Sea C el $[2r, r]$ código lineal con matriz generadora $[I_r|A]$, donde I_r es la matriz identidad de $r \times r$. Entonces el código $C^\perp$ es equivalente a C. Además $C^\perp = C$ si, y sólo si $AA^t = I_r$.

vi) El rango de A en (2.4) es la complejidad lineal de la sucesión $S = \{s_i\}_{i=0}^{\infty}$, con $s_{i+r} = s_i$ (cf. [1]).

El código descrito en este teorema es un caso particular de la familia de códigos conocida como doblemente circulantes. Damos pues la definición general.

Se dice que un código lineal es *doblemente circulante* si tiene una matriz generadora de la forma siguiente:

$$\left(\begin{array}{c|ccccc} & a & a & \cdots & a & b \\ & & & & & c \\ & & & & & c \\ I_r & & & A & & \vdots \\ & & & & & c \end{array}\right),$$

donde A es una matriz circulante de $r \times r$ y los elementos a, b y c pueden ser 0 ó 1. Reciben este nombre también los códigos que se obtienen al suprimir el primer renglón y las primera y última columna de la matriz anterior. Obtenemos así un $[2r, r]$ código lineal con matriz generadora $[I_r|A]$.

El concepto de código cíclico puede generalizarce más allá de los códigos doblemente circulantes. En efecto, en [46] nos encontramos con la siguiente definición:

Definición 32 *Sea s un entero positivo. Un código es llamado* ***cuasi-cíclico*** *si al aplicar s veces un corrimiento cíclico a una palabra codificada obtenemos nuevamente un elemento del código.*

En otras palabras, si $\sigma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ es la función $(x_0, x_1, \ldots, x_{n-1}) \longmapsto (x_{n-1}, x_0, x_1 \ldots, x_{n-2})$, entonces un código C inmerso en $\mathbb{F}_q^n$ se dice cuasi-cíclico si existe un entero positivo s tal que $\mathbf{c} \in C$ implica $\sigma^s(\mathbf{c}) \in C$. En el caso $s = 1$ obtenemos los códigos *cíclicos*.

Las columnas de la matriz generadora G, de orden $k \times mk$, de un código lineal pueden ser permutadas para llevar G a la forma $G = (G_0, G_1, \ldots, G_{m-1})$, donde cada G_i es una matriz circulante de $k \times k$. En [28] los autores mencionan que han realizado una investigación exhaustiva para determinar la distancia mínima de los códigos cuasi-cíclicos para valores pequeños de k. Gracias a esto han conjeturado que si ninguna matriz G_i tiene rango máximo entonces la distancia mínima del código cuasi-cíclico no es mejor que la de otro código cuasi-cíclico con los mismos parámetros m y k con al menos una de las matrices circulantes de rango máximo.

Una de las familias más importantes de códigos doblemente circulantes, y por lo tanto cuasi-ciclicos, es la de los llamados residuo cuadráticos (cf. [46], capítulo 16). Estos códigos son cíclicos y entre sus miembros se encuentran: el $[7, 4, 3]$ código binario de Hamming $\mathcal{H}_3$, el $[32, 16, 8]$ código binario de Reed-Muller $RM(2, 5)$, y el código binario de Golay de parámetros $[23, 12, 7]$ (un estudio de los códigos de Golay se encuentra en [46], capítulo 20).

CAPÍTULO 3

IDENTIDADES DE MACWILLIAMS PARA COPOS

Hasta este momento sólo se ha considerado el polinomio enumerador de pesos para un código lineal según se definió en la ecuación (1.1), sin embargo otros polinomios de la misma clase son conocidos (cf. [46]), por ejemplo *el enumerdor de pesos completo* que clasifica las palabras codificadas de acuerdo al número de veces que cada elemento del campo aparece en cada palabra, *el enumerador de pesos de Lee* toma una partición del campo y cuenta a los elementos en una clase como si se tratase del mismo. Recientemente este último peso ha cobrado importancia en el estudio de códigos que son lineales sobre el anillo $\mathbb{Z}_4$ (cf. [26, 79]). *El polinomio enumerador exacto* que determina completamente al código pero requiere del uso de muchas variables, *el enumerador de pesos conjuntos,* el cual determina los ceros en común entre dos palabras típicas de dos códigos distintos, etc.

En los últimos años se ha visto un enorme esfuerzo por calcular identidades tipo MacWilliams, para propósitos específicos. Por ejemplo en 1991 V.K. Wie (cf. [81]) introdujo el concepto de peso generalizado de Hamming que se ha estudiado en relación con la distribución de peso de códigos sobre extensiones de $\mathbb{F}_q$, así como en su relación con el llamado estado de complejidad de un código. El polinomio enumerdor de pesos generalizado se definió en [37] y una identidad de MacWilliams se obtuvo más tarde en [71]. En 1997 C. D. Godsil (cf. [16]) encontró una relación tipo MacWilliams para códigos inmersos en un producto de esquemas asociativos, y en el mismo año W. J. Martin y D. R. Stinson (ver [47]) probaron una identidad tipo MacWilliams utilizando esquemas asociativos para arreglos ortogonales ordenados y códigos lineales ordenados.

Como se estudió en la sección 1.3.1, los llamados polinomios de Krawtchouk están estrechamente relacionados con el polinomio enumerador de pesos de un código. En [41] tales polinomios son utilizados en el cálculo del máximo número de funciones booleanas en n variables entre las cuales cualesquiera T son independientes.

Utilizando el concepto de código lineal con métrica inducida por un conjunto parcialmente ordenado, introducido por R. Brualdi, J. S. Graves y K. L. Lawrence (cf. [8]), en este capítulo se deduce una relación para los polinomios enumeradores de pesos de un código y su dual con esta métrica. Se muestran varios ejemplos para ilustrar la fórmula y se dan algunas relaciones entre esta expresión y los análogos a los polinomios de Krawtchouk. En la sección final se muestra una segunda indentidad

del tipo MacWilliams. Estas fórmulas han sido generalizadas de manera distinta e independiente por D. S. Kim y J. G. Lee (cf. [36]), y por Y. Jang y J. Park (cf. [30]).

3.1 Introducción

Entre los problemas principales en la Teoría de Códigos se encuentra el siguiente (cf. [46]): dados dos enteros positivos m y n, determinar el mayor entero positivo d con la propiedad de que existen n elementos $h_1, h_2, \ldots, h_n$ en $\mathbb{F}_q^m$, tales que cualesquiera $d-1$ de ellos son linealmente independientes. La matriz H de orden $m \times n$ cuyas columnas son los vectores $h_1, h_2, \ldots, h_n$ es entonces la matriz de chequeo de paridad de un $[n, n-m, d]$-código lineal sobre $\mathbb{F}_q$. Una generalización al problema de determinar dicho entero es estudiado por H. Niederreiter en la serie de escritos [52, 53, 54]. R. Brualdi, J. S. Graves y K. L. Lawrence (cf. [8]) dan una generalización del problema a través del uso de conjuntos parcialmente ordenados (copos) e introducen el concepto de P-peso y P-código. En este capítulo probamos una identidad del tipo MacWilliams para el polinomio enumerador de pesos de un P-código. También presentamos algunos polinomios los cuales tienen propiedades similares a los clásicos polinomios de Krawtchouk. Los resultados que se presentan en esta sección aparecen publicados de manera más concisa en [20].

3.2 Conceptos Básicos

Sea $(P, <)$ un conjunto parcialmente ordenado, al cual llamaremos *copo*. Una *cadena* en P es un subconjunto de P tal que cualesquiera dos de sus elementos son comparables. Cuando en un subconjunto de P no existen elementos comparables el conjuntos se denomina *anticadena*. Un *ideal* I en P es un subconjunto con la siguiente propiedad: si $x \in I$ y $y < x$, entonces $y \in I$. Para un subconjunto A de P denotaremos al menor ideal de P conteniendo a A como $\langle A \rangle$, esto es, $\langle A \rangle$ es la intersección de todos los ideales de P que contienen a A.

Supongamos que $P = \{1, 2, \ldots, n\}$, el conjunto de las posiciones coordenadas del espacio vectorial $\mathbb{F}_q^n$, está ordenado de tal forma que $(P, <)$ es un copo. El *P-peso* de $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ se define como

$$ps_P(\mathbf{x}) = |\langle sop(\mathbf{x}) \rangle|,$$

donde $sop(\mathbf{x}) = \{i : x_i \neq 0\}$. La *P-distancia* de dos vectores $\mathbf{x}, \mathbf{y}$ en $\mathbb{F}_q^n$ está definida entonces como $d_P(\mathbf{x}, \mathbf{y}) = ps_P(\mathbf{x} - \mathbf{y})$. Además la P-distancia es una métrica en el espacio $\mathbb{F}_q^n$. Si P tiene el orden de una anticadena entonces los conceptos de P-peso y P-distancia resultan el peso y la distancia de Hamming respectivamente. El código $C \subset \mathbb{F}_q^n$ se dice *P-código* si $\mathbb{F}_q^n$ está provisto con la P-distancia inducida por el conjunto parcialmente ordenado P (cf. [8]).

3.3 La ecuación de MacWilliams

En esta sección damos un análogo para P-códigos a la clásica identidad de MacWilliams (1.1), la cual relaciona el polinomio enumerador de pesos de un código lineal con el correspondiente polinomio del código dual.

Recordemos que un código se dice *degenerado* si todas sus palabras codificadas tienen entrada cero en una posición coordenada fija, de otra forma el código se dice *no degenerado.*

Sea (C,P) un $[n,k]$ código lineal no degenerado sobre $\mathbb{F}_q$, provisto con la P-distancia inducida por el orden natural $1<2<\cdots<n$ en $P=\{1,2,\ldots,n\}$. Sea $\pi:\mathbb{F}_q^n\to\mathbb{F}_q^r$ la proyección sobre las posiciones coordenadas $i_1,i_2,\ldots,i_r$ con $1\leq i_1<i_2<\cdots<i_r\leq n$, $1\leq r\leq n$. Es fácil ver que cuando π es restringido al código (C,P) cada elemento de $\mathbb{F}_q^r$ es imagen de q^r palabras codificadas, esto es, π es una función regular (cf. [42]). De esta observación se sigue que el polinomio enumerador de pesos de (C,P) es:

$$\mathcal{E}_{(C,P)}(x,y)=$$
$$(q-1)\left[q^{k-1}x^n+q^{k-2}x^{n-1}y+\cdots+qx^{n-(k-2)}y^{k-2}+x^{n-(k-1)}y^{k-1}\right]+y^n.$$

El resultado principal de esta sección está basado en el siguiente lema, que más tarde resultará útil en el cálculo de una base para los llamados código binarios de Reed-Muller, constituida por vectores de peso mínimo.

Lema 33 *Sean $A=\{a_0,a_1,\ldots,a_t\}$ un conjunto finito, $\Lambda=\{a_0\}\times A^{n-1}$, $A^*=A-\{a_0\}$ y R un anillo. Entonces para cualesquera funciones $f_i:A\longrightarrow R$, $1\leq i\leq n$ las siguientes relaciones son válidas*

$$i)\qquad \sum_{(v_1,\ldots,v_n)\in A^n}\prod_{i=1}^{n}f_i(v_i)=\prod_{i=1}^{n}f_i(v_i)\sum_{v_i\in A}f_i(v_i).$$

$$ii)\qquad \sum_{(v_1,\ldots,v_n)\in A^n-\Lambda}\prod_{i=1}^{n}f_i(v_i)=\left[\sum_{a\in A^*}f_1(a)\right]\prod_{i=2}^{n}\sum_{v_i\in A}f_i(v_i).$$

Demostración Sea $\Lambda_i=\{\mathbf{x}\in A^n:x_1=a_i\}$, $0\leq i\leq t$, (por lo cual $\Lambda_0=\Lambda$).

i) La prueba se realiza por inducción sobre n. Para $n=1,2$ el resultado es obvio, así que supongámoslo válido para $n-1$. Entonces:

$$\begin{aligned}
&\sum_{(v_1,\ldots,v_n)\in A^n}\prod_{i=1}^{n}f_i(v_i)\\
&==\sum_{(v_1,\ldots,v_n)\in\Lambda_0}\prod_{i=1}^{n}f_i(v_i)+\cdots+\sum_{(v_1,\ldots,v_n)\in\Lambda_t}\prod_{i=1}^{n}f_i(v_i)\\
&=\left[\sum_{v_1\in A}f_1(v_1)\right]\sum_{(v_2,v_3,\ldots,v_n)\in A^{n-1}}\prod_{i=2}^{n}f_i(v_i)\\
&=\left[\sum_{v_1\in A}f_1(v_1)\right]\prod_{i=2}^{n}\sum_{v_i\in A}f_i(v_i),
\end{aligned}$$

donde la hipótesis de inducción es utilizada en la última igualdad.

ii) El resultado se sigue de (*i*) y de la igualdad

$$\begin{aligned}
&\sum_{(v_1,\ldots,v_n)\in A^n-\Lambda}\prod_{i=1}^{n} f_i(v_i)\\
&=\sum_{(v_1,\ldots,v_n)\in\Lambda_1}\prod_{i=1}^{n} f_i(v_i)+\cdots+\sum_{(v_1,\ldots,v_n)\in\Lambda_t}\prod_{i=1}^{n} f_i(v_i)\\
&=\left[\sum_{v_1\in A^*} f_1(v_1)\right]\sum_{(v_2,v_3,\ldots,v_n)\in A^{n-1}}\prod_{i=2}^{n} f_i(v_i).
\end{aligned}$$

Esto completa la prueba. ■

La prueba del teorema 13 está basada en el siguiente resultado, cuya prueba es dada en [46], pág. 127, y aquí se hará uso del mismo para obtener los resultados principales de este capítulo.

Lema 34 *Denotemos por p un número primo, fijo pero arbitrario. Sea R un anillo conmutativo con una raíz p-ésima primitiva de la unidad, digamos ω. Supongamos además que $C\subseteq\mathbb{F}_q^n=V$ es un código lineal, donde q es una potencia de p, y que T es una función $\mathbb{F}_p$-lineal de $\mathbb{F}_q$ sobre $\mathbb{F}_p$. Para cada función $f:V\longrightarrow R$ se define $\widehat{f}:V\longrightarrow R$ como*

$$\widehat{f}(\mathbf{u})=\sum_{\mathbf{v}\in V}\omega^{T(\mathbf{u}\cdot\mathbf{v})}f(\mathbf{v}).$$

Entonces

$$\sum_{\mathbf{u}\in C}\widehat{f}(\mathbf{u})=|C|\sum_{\mathbf{v}\in C^{\perp}}f(\mathbf{v}).$$

Demostración De la definición de $\widehat{f}$ se sigue que

$$\sum_{\mathbf{u}\in C}\widehat{f}(\mathbf{u})=\sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in V}\omega^{T(\mathbf{u}\cdot\mathbf{v})}f(\mathbf{v})=\sum_{\mathbf{v}\in V}f(\mathbf{v})\sum_{\mathbf{u}\in C}\omega^{T(\mathbf{u}\cdot\mathbf{v})}.$$

Si $\mathbf{v}\in C^{\perp}$ entonces $\mathbf{u}\cdot\mathbf{v}=\mathbf{0}$ y la suma interior es $|C|$. Pero cuando $\mathbf{v}$ no está en $C^{\perp}$ la función $\mathbf{u}\mapsto T(\mathbf{u}\cdot\mathbf{v})$ es un funcional $\mathbb{F}_p$-lineal que toma cada valor de $\mathbb{F}_p$ con la misma frecuencia, a saber $|C|/p$. En este último caso la suma interior resulta ser cero. ■

En el caso $p=2$ la función $f\mapsto\widehat{f}$ descrita arriba se conoce como la *trasformada de Hadamard.*

Por otro lado consideremos ahora la P-métrica inducida por el orden parcial

$$1 < i,\ i = 2, 3, \ldots, n \tag{3.1}$$

en el conjunto $P = \{1, 2, \ldots, n\}$.

Denotaremos por ps_H al peso de Hamming en $\mathbb{F}_q^n$. Si Γ es el hiperplano en $\mathbb{F}_q^n$ con ecuación $x_1 = 0$, definimos Γ^* como $\Gamma - \{\mathbf{0}\}$. Con esta notación es fácil ver que:

$$ps_P(\mathbf{u}) = \begin{cases} ps_H(\mathbf{u}), & \text{si } \mathbf{u} \in \mathbb{F}_q^n - \Gamma^* \\ ps_H(\mathbf{u}) + 1, & \text{si } \mathbf{u} \in \Gamma^* \end{cases}$$

Teorema 35 *Sea C un $[n,k]$ P-código lineal sobre el campo finito $\mathbb{F}_q$, con la P-métrica inducida por el orden parcial (3.1). Entonces los polinomios enumeradores de pesos de los códigos C y su dual $C^\perp$ satisfacen la siguiente relación:*

$$\mathcal{E}_{C^\perp}(x,y) = y^n - xy^n + \tfrac{qx}{|C|(y-x)} \left\{ \mathcal{E}_{C\cap\Gamma}(y-x, y+(q-1)x) - qx[y+(q-1)x]^{n-1} \right\}.$$

Demostración La idea básica de la demostración la da la prueba del teorema 13, sin embargo algunas consideraciones especiales serán necesarias en nuestro caso. Ya que q y n son enteros fijos, pero arbitrarios, utilizaremos las asignaciones $K := \mathbb{F}_q$ y $V := \mathbb{F}_q^n$.

Sea $\mathbb{C}[x,y]$ el anillo de polinomios sobre el campo de los números complejos en las indeterminadas x y y, y denotemos por Tr a la función traza de K sobre su campo primo $\mathbb{F}_p$ (i.e. q es potencia del primo p). Considere las siguientes funciones:

$$w : K \longrightarrow \mathbb{Z}, \quad w(0) = 0, \quad w(a) = 1 \text{ si } a \neq 0.$$
$$f : K \longrightarrow \mathbb{C}[x,y], \quad f(\mathbf{v}) = x^{ps_P(\mathbf{v})} y^{n - ps_P(\mathbf{v})}$$

y sea

$$\widehat{f}(u) = \sum_{\mathbf{v}\in V} f(\mathbf{v})\ \alpha^{Tr(\mathbf{u}\cdot\mathbf{v})}$$

donde α es una raíz p-ésima primitiva de la unidad en $\mathbb{C}$.

Entonces $\widehat{f}(u)$ puede ser escrita como

$$y^n + \sum_{\mathbf{v}\in V-\Gamma} x^{ps_P(\mathbf{v})} y^{n-ps_P(\mathbf{v})}\ \alpha^{Tr(\mathbf{u}\cdot\mathbf{v})} + \sum_{\mathbf{v}\in\Gamma^*} x^{ps_P(\mathbf{v})} y^{n-ps_P(\mathbf{v})}\ \alpha^{Tr(\mathbf{u}\cdot\mathbf{v})}.$$

A fin de evitar confusiones simplificaremos esta expresión en tres pasos. El polinomio en el primer símbolo de suma puede reescribirse como:

$$\begin{aligned} &\sum_{\mathbf{v}\in V-\Gamma} x^{ps_P(\mathbf{v})} y^{n-ps_P(\mathbf{v})}\ \alpha^{Tr(\mathbf{u}\cdot\mathbf{v})} \\ &= \sum_{(v_1,\ldots,v_n)\in V-\Gamma} x^{w(v_1)+\cdots+w(v_n)} y^{[1-w(v_1)]+\cdots+[1-w(v_n)]}\ \alpha^{Tr(u_1v_1+\cdots+u_nv_n)} \\ &= \sum_{(v_1,\ldots,v_n)\in V-\Gamma} x\alpha^{Tr(u_1v_1)} \prod_{i=2}^{n} x^{w(v_i)} y^{1-w(v_i)}\ \alpha^{Tr(u_iv_i)}. \end{aligned}$$

Del lema 33 (ii) se sigue que la última expresión es igual a:

$$x\left[\sum_{a\in K^*}\alpha^{Tr(au_1)}\right]\prod_{i=2}^{n}\sum_{v_i\in K}x^{w(v_i)}y^{1-w(v_i)}\,\alpha^{Tr(u_iv_i)}.$$

Por otro lado tenemos,

$$\begin{aligned}
&\sum_{\mathbf{v}\in\Gamma^*}x^{ps_P(\mathbf{v})}y^{n-ps_P(\mathbf{v})}\,\alpha^{Tr(\mathbf{u}\cdot\mathbf{v})}\\
&=\sum_{(v_1,\ldots,v_n)\in\Gamma^*}x^{w(v_1)+\cdots+w(v_n)}y^{[1-w(v_1)]+\cdots+[1-w(v_n)]}\,\alpha^{Tr(\mathbf{u}\cdot\mathbf{v})}\\
&=xy^{-1}\sum_{(v_1,\ldots,v_n)\in\Gamma}\prod_{i=1}^{n}x^{w(v_i)}y^{1-w(v_i)}\,\alpha^{Tr(u_iv_i)}-xy^{n-1}\\
&=xy^{-1}\sum_{(v_1,\ldots,v_n)\in\Gamma}y\prod_{i=2}^{n}x^{w(v_i)}y^{1-w(v_i)}\,\alpha^{Tr(u_iv_i)}-xy^{n-1}\\
&=x\prod_{i=2}^{n}\sum_{v_i\in K}x^{w(v_i)}y^{1-w(v_i)}\,\alpha^{Tr(u_iv_i)}-xy^{n-1}
\end{aligned}$$

donde la última igualdad se sigue del lema 33 (i). Por lo tanto:

$$\widehat{f}(\mathbf{u})=y^n-xy^{n-1}+x\left[\prod_{i=2}^{n}\sum_{v_i\in K}x^{w(v_i)}y^{1-w(v_i)}\alpha^{Tr(u_iv_i)}\right]\sum_{a\in K}\alpha^{Tr(au_1)}.$$

Si $u_1\neq 0$, entonces $\widehat{f}(\mathbf{u})=y^n-xy^n$. En otro caso:

$$\widehat{f}(\mathbf{u})=y^n-xy^n+qx\prod_{i=2}^{n}\sum_{v_i\in K}x^{w(v_i)}y^{1-w(v_i)}\alpha^{Tr(u_iv_i)}.$$

Cuando $u_i=0$, $(i\geq 2)$ la suma en esta expresión es igual a $y+(q-1)\,x$, en otro caso es:

$$y+\left[\frac{q}{p}\left(1+\alpha+\cdots+\alpha^{p-1}\right)-1\right]x=y-x.$$

Resumindo, escribimos la función $\widehat{f}(\mathbf{u})$ como

$$\widehat{f}(\mathbf{u})=\begin{cases}y^n-xy^n, & \text{si } \mathbf{u}\in V-\Gamma\\ y^n-xy^n+qx\,(y-x)^{ps_H(\mathbf{u})}\,[y+(q-1)\,x]^{n-1-ps_H(\mathbf{u})}, & \text{si } \mathbf{u}\in\Gamma.\end{cases}$$

Del lema 34 se tiene que

$$\begin{aligned}
\widehat{f}(\mathbf{u})&=y^n-xy^n+\tfrac{1}{|C|}\{qx+[y+(q-1)\,x]^{n-1}\\
&\quad+qx\textstyle\sum_{\mathbf{u}\in C\cap\Gamma^*}(y-x)^{ps_P(\mathbf{u})-1}\,[y+(q-1)\,x]^{n-1-ps_P(\mathbf{u})+1}\}.
\end{aligned}$$

El resultado se sigue ahora simplificando esta última relación. ■

Es interesante notar que la identidad obtenida puede ser fácilmente modificada para que sea válida en el caso en que tomemos la P-métrica inducida por el orden $j<i$, para todo entero positivo $i\leq n$, con $1\leq j\leq n$ y $j\neq i$.

3.3.1 Algunos ejemplos

En esta sección daremos varios ejemplos para ilustrar el resultado principal de la sección previa.

Ejemplo 36 El $[7,4,3]$ código binario de Hamming $H_3 = C$ es auto-ortogonal, es decir, $C^{\perp} \subset C$. En este caso

$$\begin{aligned}
\mathcal{E}_C(x,y) &= y^7 + 3x^3y^4 + 8x^4y^3 + 3x^5y^2 + x^7, \\
\mathcal{E}_{C^{\perp}}(x,y) &= y^7 + 4x^4y^3 + 3x^5y^2 + 3x^5y^2 + x^7, \\
\mathcal{E}_{C\cap\Gamma}(x,y) &= y^7 + 4x^4y^3 + 3x^5y^2.
\end{aligned}$$

Entonces el P-polinomio enumerador de pesos del código dual $C^{\perp}$ resulta

$$\begin{aligned}
\mathcal{E}_{C^{\perp}}(x,y) = \; & y^7 - xy^6 + \tfrac{2x(y-x)^{-1}}{16}\left[(y+x)^7 + 4(y-x)^4(y+x)^3\right. \\
& \left. +3(y-x)^5(y+x)^2 - 2x(y+x)^6\right].
\end{aligned}$$

Ejemplo 37 El código extendido de Hamming $\widehat{\mathcal{H}_3}$, el cual es también el código de Reed-Muller de primer orden $RM(1,3)$, es auto-dual, i.e. si $RM(1,3) = C$ entonces $C^{\perp} = C$. En este caso tenemos

$$\begin{aligned}
\mathcal{E}_C(x,y) &= \mathcal{E}_{C^{\perp}}(x,y) = y^8 + 7x^4y^4 + 7x^5y^4 + 3x^5y^3 + x^8, \\
\mathcal{E}_{C\cap\Gamma}(x,y) &= y^8 + 7x^5y^3.
\end{aligned}$$

Por lo tanto

$$\mathcal{E}_{C^{\perp}}(x,y) = y^8 - xy^7 + \frac{2x(y-x)^{-1}}{16}\left[(y+x)^8 + 7(y-x)^5(y+x)^3 - 2x(y+x)^7\right].$$

Ejemplo 38 Si $C = \{000, 011, 022\}$ es un código ternario, su dual es

$$C^{\perp} = \{000, 012, 021, 100, 112, 121, 200, 212, 221\}.$$

Tenemos entonces las siguientes relaciones

$$\mathcal{E}_C(x,y) = y^3 + 2x^3, \qquad \mathcal{E}_{C\cap\Gamma}(x,y) = y^3 + 2x^3.$$

De ahí que

$$\mathcal{E}_C(x,y) = y^3 - xy^2 + (y-x)^{-1}\left\{(y+2x)^3 + 2(y-x)^3 - 3x(y+2x)^2\right\}.$$

Ejemplo 39 El código símplex $\mathcal{H}_r^{\perp} := C$ de longitud $2^r - 1$ y dimensión r, tiene la propiedad de que todas sus palabras codificadas no cero tienen peso de Hamming $2^r - 1$. Si $n = 2^r - 1$, el P-polinomio enumerador de pesos del código y su dual son

$$\begin{aligned}\mathcal{E}_{C^{\perp}}(x,y) = &\quad y^n + \tfrac{n+1}{2}x^{(n+1)/2} + \tfrac{n-1}{2}x^{(n+3)/2}y^{(n-3)/2}, \quad y \\ \mathcal{E}_C(x,y) = &\quad y^n - xy^{n-1} \\ &+ \tfrac{2x(y-x)^{-1}}{n+1}\left[(y+x)^n + \tfrac{n-1}{2}(y-x)^{(n+3)/2}(y+x)^{(n-3)/2} - 2x(y+x)^{n-1}\right],\end{aligned}$$

respectivamente.

Ejemplo 40 Sea C el $[6,3]$ código lineal sobre el campo $\mathbb{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$, que se obtiene como el código asociado a los $\mathbb{F}_4$-puntos racionales de la curva elíptica dada por la ecuación $F(x,y,z) = x^3 + y^3 + z^3$. Una matriz generadora para este código es

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

Como puede verificarse fácilmente los P-polinomios enumeradores de pesos para C y su dual satisfacen

$$\begin{aligned}\mathcal{E}_C(x,y) &= \mathcal{E}_{C^{\perp}}(x,y) = y^6 + 30x^4y^2 + 15x^5y + 18x^6, \\ \mathcal{E}_{C \cap \Gamma}(x,y) &= y^6 + 15x^5y.\end{aligned}$$

Observe que los códigos C y su dual son distintos pues la palabra $(\omega\omega 1001)$ es un elemento de C pero no de $C^{\perp}$.

El polinomio enumerador de pesos para el último de los ejemplos mostrados arriba, con el peso de Hamming, es

$$\mathcal{E}_C(x,y) = \mathcal{E}_{C^{\perp}}(x,y) = y^6 + 45x^4y^2 + 18x^6.$$

Comparando los polinomios enumeradores de pesos, con diferentes P-pesos, es claro que de entre las 45 palabras de C con peso de Hamming 4, existen 15 que tienen su primera entrada distinta de cero. Por lo tanto el P-peso nos proveé de información adicional sobre la distribución de los soportes de las palabras codificadas.

3.3.2 P-polinomios de Krawtchouk

En la sección 1.3.1 se introdujeron los polinomios de Krawtchouk, los cuales surgen de forma natural al estudiar la manera en que se relacionan los coeficientes del polinomio enumerador de pesos de un código y su dual. En esta sección describiremos algunos polinomios asociados a un P-código lineal, los cuales son los análogos de aquellos antes mencionados.

Sea C un $[n,k]$-código lineal sobre el campo $\mathbb{F}_q$ con q elementos, y como antes denotemos por Γ a la variedad lineal en $\mathbb{F}_q^n$ con ecuación $x_1 = 0$. Supongamos que, en la P-métrica inducida por el orden (3.1) tenemos

$$\mathcal{E}_C(x,y) = \sum_{i=0}^{n} A_i x^i y^{n-i}, \qquad \mathcal{E}_{C\cap\Gamma}(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i},$$

$$\mathcal{E}_{C^\perp}(x,y) = \sum_{i=0}^{n} B_i x^i y^{n-i}, \qquad \mathcal{E}_{C^\perp\cap\Gamma}(x,y) = \sum_{i=0}^{n} b_i x^i y^{n-i},$$

con $a_0 = 1$ y $a_1 = 0$.

Un simple cálculo muestra que

$$(1-z)^{i-1}\left[1+(q-1)z\right]^{n-i} = \sum_{k=0}^{n-1} Q_k(i;n)\ z^k$$

es una función generadora para

$$Q_k(i;n) = \sum_{j=0}^{k-1} (-1)^j \binom{i-1}{j}\binom{n-i}{k-1-j}(q-1)^{k-1-j}.$$

Nos referiremos a la expresión $Q_k(i;n)$ como *P-polinomio de Krawtchouk.*

El polinomio $\mathcal{E}_{C^\perp}(x,y)$ puede reescribirse como se muestra a continuación.

$$\begin{aligned}
&\sum_{k=0}^{n} B_k x^k y^{n-k} \\
&= y^n - xy^{n-1} \\
&\quad + \tfrac{q}{|C|}\left\{\sum_{i=2}^{n} a_i x\,(y-x)^{i-1}\left[y+(q-1)x\right]^{n-i} + \tfrac{qx}{|C|}\left[y+(q-1)x\right]^{n-1}\right\} \\
&= y^n - xy^{n-1} + \tfrac{q}{|C|}\left[1+\sum_{i=2}^{n} a_i\right] xy^{n-1} \\
&\quad + \tfrac{q}{|C|}\sum_{k=2}^{n}\left[\sum_{i=2}^{n} a_i Q_k(i;n) + \tbinom{n-1}{k-1}(q-1)^{k-1}\right] x^k y^{n-k}.
\end{aligned}$$

Si en la primera de las anteriores relaciones hacemos $y = 1$, al evaluar la derivada respecto a x en $x = 1$ obtenemos:

$$\sum_{i=0}^{n} \frac{iA_i}{q^k} = \frac{1}{q}(1+n(q-1)-b_2) = \frac{1}{q}(1+n(q-1)), \quad \text{si } b_2 = 0.$$

Esta ecuación es análoga al llamado primer momento en la teoría clásica de códigos lineales, por lo que nos referiremos a ella como el *primer P-momento.*

Comparando coeficientes en las relaciones obtenidas arriba llegamos a:

$$\begin{aligned} B_0 &= 1, \\ B_1 &= -1 + \tfrac{q}{|C|}\left[1 + \sum_{i=2}^{n} a_i\right], \\ B_k &= \tfrac{q}{|C|}\left[\binom{n-1}{k-1}(q-1)^{k-1} + \sum_{i=2}^{n} a_i Q_k(i;n)\right], \quad k \geq 2. \end{aligned}$$

3.3.3 Una segunda identidad tipo MacWilliams

En la primera sección de este capítulo consideramos la P-métrica inducida por el orden parcial $1 < i$, para $i = 2, 3, \ldots, n$. A través de ejemplos mostramos que el polinomio enumerador de pesos asociado al P-peso correspondiente nos brinda información sobre la distribución de los soportes de las palabras codificadas.

Consideraremos el P-peso inducido por el orden

$$1, 2 < i, \quad \text{con } i = 3, 4, \ldots, n.$$

Dado un código lineal C definimos la función $\pi_i : C \to \mathbb{F}_q$ como la proyección sobre la i-ésima posición coordenada.

Teorema 41 *Sean Ω el subespacio vectorial en $\mathbb{F}_q^n$ determinado por las ecuaciones $x_1 = 0$ y $x_2 = 0$. Los polinomios enumeradores de un $[n,k]$-código lineal C sobre $\mathbb{F}_q$, y su dual $C^{\perp}$, están relacionados por la ecuación*

$$\begin{aligned} \mathcal{E}_{C^{\perp}}(x,y) = {} & y^n - x^2y^{n-2} + \tfrac{q^2x^2(y-x)^2}{|C|}\left\{\mathcal{E}_{C\cap\Omega}(y-x, y+(q-1)x)\right. \\ & \left. -qx[2(y-x)+qx][y+(q-1)x]^{n-2}\right\} \\ & + \begin{cases} 0, & \text{si } \pi_1 \neq 0 \text{ y } \pi_2 \neq 0, \\ 2(q-1)(xy^{n-1} - x^2y^{n-2}), & \text{si } \pi_1 = \pi_2 = 0, \\ (q-1)(xy^{n-1} - x^2y^{n-2}), & \text{en otro caso.} \end{cases} \end{aligned}$$

Demostración La demostración es análoga a la del teorema 35. Por este motivo sólo mencionaremos la relación entre el P-peso que estamos considerando y el peso de Hamming, así como la expresión simplificada para la correspondiente función $\widehat{f}(\mathbf{u})$.

Sean Γ y Λ las variedades lineales en $\mathbb{F}_q^n$ con ecuaciones $x_1 = 0$ y $x_2 = 0$ respectivamente, y denotemos por $\Gamma \triangle \Lambda$ su diferencia simétrica. Entonces

$$ps_P(\mathbf{u}) = \begin{cases} ps_H(\mathbf{u}), & \text{si } u_1 \neq 0 \text{ y } u_2 \neq 0, \\ ps_H(\mathbf{u}), & \text{si } u_i = 0 \text{ para todo } i \geq 3, \\ ps_H(\mathbf{u}) + 2, & \text{si } u_1 = u_2 = 0 \text{ y } \mathbf{u} \neq 0, \\ ps_H(\mathbf{u}) + 1, & \text{en otro caso.} \end{cases}$$

y la función $\widehat{f}(\mathbf{u})$ se reduce a:

$$\widehat{f}(\mathbf{u}) = \begin{cases} y^n - x^2y^{n-2} + 2(q-1)(xy^{n-1} - x^2y^{n-2}) \\ \quad + q^2x^2(y-x)^{ps_H(\mathbf{u})}[y + (q-1)x]^{n-2-ps_H(\mathbf{u})}, & \text{si } \mathbf{u} \in \Gamma \cap \Lambda, \\ y^n - x^2y^{n-2} + (q-2)(xy^{n-1} - x^2y^{n-2}), & \text{si } \mathbf{u} \in \Gamma \triangle \Lambda, \\ y^n - x^2y^{n-2} - 2xy^{n-1} + x^2y^{n-2}, & \text{en otro caso.} \end{cases}$$

Por un razonamiento similar al del teorema 35 se obtiene el resultado. ■

Como antes, podemos obtener fácilmente una identidad tipo MacWilliams para el P-peso inducido por el orden parcial $i, j < \ell$, para $1 \leq \ell \leq n$, y $\ell \neq i, j$.

Por último cabe mencionar que algunas identidades tipo MacWilliams para P-códigos pueden ser obtenidas haciendo uso del trabajo de Martin y Stinson [47] Además los resultados presentados en este capítulo han sido generalizados por D. S Kim y J. G. Lee (cf. [36]) y por Y. Jang y J. Park (cf. [30]), considerando cada grupo distintos órdenes parciales, en base a los resultados presentados en [20].

CAPÍTULO 4

EXTENSIONES DE CÓDIGOS

En este capítulo se presentan diversas formas de incrementar el valor de los parámetros de los códigos lineales. Mediante la combinación de tales técnicas se recuperarán los códigos binarios de Reed-Muller (sección 4.2), los códigos asociados a una familia de sistemas de ciclos (sección 5.2), y se mostrará que varios códigos con parámetros óptimos pueden ser construidos utilizando este método.

El capítulo está organizado de la siguiente manera: en la primera sección recordamos las definiciones de estructuras de incidencia y su relación con la Teoría de Códigos. En la segunda sección se presenta una clase de códigos cíclicos con distancia mínima 1 ó 2, los valores de sus parámetros son incrementados para obtener códigos con mejores parámetros y se prueba que los códigos binarios de Reed-Muller pueden construirse empleando este método. Se muestra además que los códigos binarios de Reed-Muller de primer orden pueden obtenerse fácilmente a partir de la matriz identidad de 2×2, y que tales códigos están generados por los vectores de incidencia de un 1-diseño (hasta ahora sólo se sabía que existe un 2-diseño cuyos vectores de incidencia generan tales códigos [1]), además una base para tales códigos es determinada. En la sección 4.3 se determinan los parámetros de una clase de códigos generados por la concatenación de algunas palabras codificadas de códigos definidos en la sección previa, y nuevamente los códigos de Reed-Muller son recuperados. La última sección contiene una descripción polinomial de una base para los códigos de Reed-Muller constituida por vectores de peso mínimo, resaltando el hecho que tal base corresponde a la construcción de las secciones anteriores en el presente capítulo, un resultado equivalente al de Gao y Key [15].

4.1 Antecedentes

Una *estructura de incidencia* $\mathcal{D}$ es una tripleta ordenada $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, donde $\mathcal{P}$ es un conjunto finito de *puntos*, $\mathcal{B}$ es una colección finita de conjuntos denominados *bloques*, donde $\mathcal{P} \cap \mathcal{B} = \emptyset$, e $\mathcal{I} \subset \mathcal{P} \times \mathcal{B}$ es la *relación de incidencia de* $\mathcal{D}$. Si el par (x, B) está en $\mathcal{I}$ diremos que el punto x es incidente con el bloque B. La función característica del bloque $B \in \mathcal{B}$ se denotará por χ_B, i.e., si $\mathcal{P} = \{x_1, \ldots, x_r\}$ entonces $\chi_B(x_j) = 1$ si el punto x_j is incidente con B y es cero en otro caso. El *vector de inicidencia* del bloque B es $\mathbf{v}^B = (\chi_B(x_1), \ldots, \chi_B(x_r))$. El arreglo rectangular cuyos renglones son los vectores de incidencia de $\mathcal{D}$ se denomina la *matriz de incidencia de* $\mathcal{D}$. El

código lineal binario asociado a $\mathcal{D}$, denotado como $C(\mathcal{D})$, es el $\mathbb{F}_2$-espacio vectorial generado por los vectores de incidencia de los bloques de $\mathcal{D}$ (en general este código lineal puede ser definido sobre cualquier campo finito, pero en el presente trabajo nos restringiremos al caso binario).

El código binario asociado a la estructura de incidencia $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, donde $\mathcal{P} = \mathbb{F}_2^m$, $\mathcal{B}$ es el conjunto de variedades afines de dimensión $(m-\rho)$ en $\mathbb{F}_2^m$ y (x, B) está en $\mathcal{I}$ si $x \in B$, i.e., $\mathcal{D}$ es un diseño de bloques, es el $\left[2^m, \sum_{i=0}^{\rho} \binom{m}{i}, 2^{m-\rho}\right]$-código binario de Reed-Muller de orden ρ, $RM(\rho, m)$, (cf. [1], teorema 5.3.3).

Sea $G = (V, A)$ una gráfica conexa finita y no dirigida, con m vértices V, n aristas A y supongamos que g es la mínima longitud que puede tomar un ciclo de G. Consideremos la estructura de incidencia $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ donde $\mathcal{P} = A$, $\mathcal{B}$ es el conjunto de ciclos de G y el par (x, B) está en $\mathcal{I}$ si x es una arista del ciclo B. Entonces el código $C(\mathcal{D})$ es el *espacio de ciclos*, que se estudia en la Teoría de Gráficas, el cual tiene parámetros $[n, n-m+1, g]$ (cf. [27]). Por ejemplo, el espacio de ciclos de la gráfica completa con $2n$ vértices es un $[n(2n-1), (n-1)(2n-1), 3]$-código lineal. En [24] se da un método para extender el código $C(\mathcal{D})$ a un $[n, k, g]$ código lineal binario, con $k > n - m + 1$. Este método es explicado en términos de subgráficas generadoras de G en [31]. El método es generalizado en 1999 considerando el código sobre un campo finito arbitrario y utilizando gráficas dirigidas (cf. [32]).

En este capítulo se analizará una familia de códigos cíclicos binarios generados por los corrimientos cíclicos de un vector de la forma $\mathbf{x} = 11\cdots100\cdots0$, cuyos parámetros $[n, k, d]$ son fácilmente calculados, en particular la distancia mínima será 1 ó 2. Estos códigos están asociados de manera natural a los sistemas de cilcos, como veremos en el siguiente capítulo. Se propone un método para incrementar el valor de la longitud y la distancia mínima de forma simultánea en estos códigos, sin alterar su dimensión, para enseguida aumentar el valor de la dimensión conservando las nuevas longitud y distancia mínima. También se considera el código lineal generado por la concatenación de algunas de las palabras codificadas de los códigos cíclicos antes descritos. Tales código son extendidos a códigos con mejores parámetros de manera semejante a como se describe antes. Por último se describe una base para los códigos binarios de Reed-Muller, constituida por vectores de peso mínimo, y la relación con el método propuesto para extender códigos es explicada.

A continuación resumimos los prinicpales resultados en [31] semajantes a los resultados que se obtendrán en secciones posteriores.

Recordemos que el número de aristas de una subgráfica $\Gamma = (V_1, A_1)$ de la gráfica $G = (V, A)$ incidentes con el vértice $x \in V_1$ es el *grado de* x respecto a Γ. El *patrón de grado impar* del Γ es entonces el conjunto de vértices de Γ con grado impar. Supongamos dada la estructura de incidencia $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', \mathcal{I}')$ donde $\mathcal{P}' = V$, $\mathcal{B}'$ es el conjunto de subgráficas de G con conjunto de vértices V (las subgráficas generadoras de G) y el par (x, B) está en $\mathcal{I}'$ si x es de grado impar en la subgráfica B. Entonces el código $C(\mathcal{D}')$ es un $[|V|, |V|-1, 2]$-código binario, consistente de todos los vectores

de longitud $|V|$ con peso par (cf. [31]). El siguiente par de resultados aparecen también en [31].

Teorema 42 *Sea C el $[n, n-m+1, g]$-código lineal que es el espacio de ciclos de la gráfica conexa, finita y no dirigida G. Entonces C puede ser extendido a un $[n, n-m+1+k, g]$ código lineal binario, si existe un $[m, k, 2g]$ código $\mathcal{O}$ con la propiedad de que cada una de sus palabras codificadas tiene peso par. La manera de obtener tal código extendido es añadiendo a C, como generadores adicionales, cualesquiera k subgráficas cuyos vectores de incidencia son linealmente independientes y sus patrones de grado impar respectivos formen una base para $\mathcal{O}$.*

Teorema 43 *Considere el espacio de ciclos C asociado a una gráfica conexa G. Supongamos que $V_1, \ldots, V_c$ es una partición del conjunto de vértices en conjuntos independientes con cardinalidades $v_1, \ldots, v_c$ respectivamente. Entonces C es un $[n, n-v+1, g]$-código y puede ser extendido a un código lineal binario con parámetros $[n, (n-v+1)+(k_1+\cdots+k_c), g]$ si existen $[v_i, k_i, g]$-códigos binarios $\mathcal{O}_i$, $1 \leq i \leq c$, con todas sus palabras codificadas de peso par. La manera de obtener tal código extendido es añadiendo a C, como generadores adicionales, cualesquiera k_i subgráficas de G, $i = 1, \ldots, c$, con patrón de grado impar contenido en V_i y formando una base para $\mathcal{O}_i$.*

Ejemplo 44 El espacio de ciclos de la gráfica bipartita $G = K_{v,v}$, con $v = 2^n$, es un código con parámetros $[2^{2n}, 2^{2n} - 2^{n+1} + 1, 4]$. Elijamos $\mathcal{O}_1$ y $\mathcal{O}_2$ ambos como el código extendido de Hamming con parámetros $[2^{2n}, 2^{2n} - 2n - 1, 4]$. Por el método arriba descrito obtenemos un $[2^{2n}, 2^{2n} - 2n - 1, 4]$-código lineal binario, el código $RM(2n-2, 2n)$, que a su vez es el código extendido de Hamming $\widehat{\mathcal{H}}_{2n}$. Tomando ahora la gráfica bipartita $G = K_{p,p'}$ donde $p = 2^{n+1}$ y $p' = 2^n$ por una construcción similar obtenemos los códigos $\widehat{\mathcal{H}}_{2n+1}$. Al suprimir una posición coordenada fija, pero arbitraria, en cada uno de los elementos de un código extendido de Hamming $\widehat{\mathcal{H}}_r$ se obtiene el código $\mathcal{H}_r$ (cf. [1]). Por lo que todo código binario de Hamming es recuperado en términos de subgráficas de una gráfica bipartita.

Otra familia de estructuras combinatorias asociada a ciclos de gráficas es la de los llamados *sistemas triples de Steiner*, STS, que son estructuras de incidencia $(\mathcal{P}, \mathcal{T}, \mathcal{I})$, donde $\mathcal{P}$ es un conjunto finito de puntos, $\mathcal{T}$ es una colección de subconjuntos de puntos llamados triángulos, tales que todo triángulo tiene cardinalidad 3, cualesquiera 2 puntos están contenidos en exactamente un triángulo y (p, B) está en $\mathcal{I}$ si $p \in B$ (cf. [1], pág. 296).*

En [35] los autores prueban que si la distancia mínima del código asociado a un STS es 3 entonces el STS proviene de una geometría finita, la cual es proyectiva en el caso binario y afín en el ternario. Como consecuencia se tiene que el código lineal

*En general un sistema de Steiner es un t-$(v, k, 1)$ diseño, $t \geq 2$ (cf. sección 1.4)

asociado al STS es un código binario de Hamming, en el primer caso mencionado, o un código generalizado de Reed-Muller en el segundo. Además se prueba que el código binario asociado a un sistema triple de Steiner contiene un subcódigo que, después de suprimirle las posiciones coordenadas donde todas sus palabras codificadas tienen entrada cero, es equivalente a un código binario de Hamming.

4.2 Los códigos $C_a^{(\eta)}(r)$

En esta sección se presenta una familia de códigos cíclicos de distancia mínima 2, que permitirán establecer fácilmente los parámetros de una serie de códigos cuasi-cíclicos. Se muestra también un método para incrementar la dimensión de estos códigos cuasi-cíclicos sin alterar su longitud ni su distancia mínima. Se prueba que la colección definida contiene varios códigos de parámetros óptimos además de la familia de códigos de Reed-Muller. La sección concluye con un resultado que muestra que los código binarios de Reed-Muller de primer orden $RM(1,m)$, $m \geq 2$, pueden obtenerse de la matriz identidad de 2×2, y que tales códigos son generados por los vectores de incidencia de un 1-diseño (a diferencia de los códigos $RM(\rho,m)$, $2 \leq \rho < m$, que son generados por los vectores de incidencia de un 2-diseño, como se muestra en [1]).

Dado un entero $\eta \geq 1$, denotaremos por $\mathbf{1}_\eta$ al vector de longitud η con todas sus entradas igual a 1 (este vector es conocido como el *vector todo-uno de longitud* η), similarmente dado un entero positivo θ el vector cero de $\mathbb{F}_2^\theta$ será $\mathbf{0}_\theta$. La concatenación de $\mathbf{1}_\eta$ y $\mathbf{0}_\theta$, es decir $|\mathbf{1}_\eta|\,\mathbf{0}_\theta|$, se representa simplemente como $\mathbf{1}_\eta\mathbf{0}_\theta$.

Para cualesquiera enteros a y r con $r > a \geq 1$, se define el código cíclico[†] $C_a(r)$ como aquel generado por los renglones de la matriz circulante con primer renglón $\mathbf{1}_a\mathbf{0}_{r-a}$. Es decir

$$\boxed{C_a(r) = \left\langle \textstyle\sum_{i=0}^{a-1} x^i \right\rangle, \qquad \textstyle\sum_{i=0}^{a-1} x^i \in \mathbb{F}_2[x]/(x^r - 1).} \tag{4.1}$$

Por ejemplo, $C_1(r) = \mathbb{F}_2^r$ y por el teorema 26, para $r \geq 2$ el código $C_2(r)$ consiste de todas las palabras de peso par de longitud r y es isomorfo al ideal de $\mathbb{F}_2[x]/(x^r - 1)$ generado por $1 + x$, por lo que tiene parámetros $[r, r-1, 2]$.

La dimensión L de este código puede calcularse a través del algorítmo de Berlekamp-Massey, como se explicó en la sección 2.2. Además la suma de $\mathbf{1}_a\mathbf{0}_{r-a}$ y su corrimiento cíclico tiene peso 2, así que la distancia mínima de $C_a(r)$ es 1 ó 2. Pero si una palabra de peso 1 está en este código, también lo estará su corrimiento cíclico, por lo que la distancia mínima de $C_a(r)$ es 1 si y sólo si su dimensión es igual a su longitud. Tenemos así que $C_a(r)$ es un código lineal con parámetros $[r, L, 2 - \delta_{r,L}]$, donde $\delta_{x,y}$ es la delta de Kronocker, es decir, $\delta_{x,y} = 1$ si $x = y$, y es cero en otro caso.

El polinomio característico de grado mínimo (cf. sección 2.2) de la sucesión $S = \{s_i\}_{i=0}^{\infty}$ donde $(s_0, \ldots, s_{r-1}) = \mathbf{1}_a\mathbf{0}_{r-a}$ y $s_{i+r} = s_i$ es llamado *el polinomio*

[†]Véase la definición general de código cíclico en la sección 2.1.

característico de $C_a(r)$. Recordemos que el recíproco del polinomio $F(x)$ de grado t es $F^*(x) = x^t F(x^{-1})$.

Proposición 45 *Sea* $m(x)$ *el polinomio característico del código* $C_a(r)$. *Entonces el polinomio generador de* $C_a(r)$ *es* $g(x) = (x^r - 1)/m^*(x)$.

Demostración Denotemos por L al grado de $m(x)$. El polinomio $f(x) = \sum_{i=0}^{a-1} x^i \in R_r = \mathbb{F}_2[x]/(x^r - 1)$ es un generador del código cíclico $C_a(r)$, no necesariamente el generador de grado mínimo. Por la relación (2.3) sabemos que existe un polinomio $P(x) \in \mathbb{F}_2[x]$ tal que $f(x)m^*(x) = P(x)(x^r - 1)$ en el anillo $\mathbb{F}_2[x]$. Por lo tanto $f(x)m^*(x) = 0$ en R_r. Como $f(x)$ es un generador de $C_a(r)$ se cumple la igualdad $c(x)m^*(x) = 0$ en R_r, para cualquier palabra codificada $c(x)$ de $C_a(r)$, en particular si $c(x) = g(x)$ es el polinomio generador de $C_a(r)$. Pero $g(x)m^*(x)$ tiene grado r en $\mathbb{F}_2[x]$, por lo que $g(x)m^*(x) = x^r - 1$. ■

La distancia mínima de los códigos $C_a(r)$ es a lo más dos, y por lo tanto son incapaces de detectar y corregir los errores que ocurran durante la transmisión. En el presente capítulo se describen dos métodos que permiten incrementar el valor de sus parámetros, en algunos casos alcanzando cotas superiores sobre la existencia de códigos. En lo que resta de este y el siguiente capítulo el trabajo se desarrollará en base a los códigos $C_a(r)$ y sus respectivos polinomios característicos $m(x)$ y generador $g(x)$. En el apéndice se da una lista de estos polinomios para $2 \leq r \leq 16$ y $1 \leq a < r$.

Recordemos que el producto de Kronecker de la matriz $M = (m_{ij})$ y el vector $\mathbf{v}$ es la matriz $M \otimes \mathbf{v} = (m_{ij}\mathbf{v})$ y que si C es un $[n, k, d]$-código lineal se define $C \otimes \mathbf{v} = \{\mathbf{c} \otimes \mathbf{v} : \mathbf{c} \in C\}$, que resulta ser un $[nn', k, dd']$-código lineal, donde n' es la longitud de $\mathbf{v}$ y d' es su peso (cf. [46], pág. 568). Si $\mathbf{v} = \mathbf{1}_\eta$ este proceso se denominará η-*construcción* y lo llamaremos (η, θ)-*construcción* si $\mathbf{v} = \mathbf{1}_\eta \mathbf{0}_\theta$, para cualesquiera enteros positivos η y θ.

Si $g(x)$ es el polinomio generador de $C_a(r)$ y η es un entero positivo, entonces se verifica fácilmente que el conjunto de polinomios $x^{2\eta t}\left(\sum_{i=0}^{2\eta-1} x^i\right) g(x^{2\eta})$, $0 \leq t < \dim(C_a(r))$, es una base de $C_a(r) \otimes \mathbf{1}_{2\eta}$.

Obsérvese que el código $C_a(r)$ puede ser extendido a un $[r, k_0, 2 - \delta_{r,L}]$-código lineal $C_a(r)^\circ$ como se muestra enseguida: sea $g(x)$ el polinomio generador de $C_a(r)$, si $(1 + x) \mid g(x)$, entonces $k_0 = r - 1$ (i.e. $C_a(r)^\circ = C_2(r)$), en otro caso tomamos $C_a(r)^\circ = C_a(r)$.

Dados enteros positivos η, a, r, con $a < r$, se define el código

$$\boxed{C_a^{(\eta)}(r) = C_a(r) \otimes \mathbf{1}_{2\eta}} \tag{4.2}$$

cuyos parámetros son $[2\eta r, L, (2 - \delta_{r,L})\, 2\eta]$, donde L es la dimensión de $C_a(r)$. Además esté código puede extenderse a $C_a^{(\eta)}(r)^\circ := C_a(r)^\circ \otimes \mathbf{1}_{2\eta}$ que tiene dimensión k_0, la dimensión de $C_a(r)^\circ$. El número k_0 es pequeño en general comparado con los valores

Mediante una 1-extensión obtenemos el código $C_1^{(1)}(2)$, generado por los renglones de

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

Por otro lado al aplicar una (1,1)-extensión al $[2,1,2]$-código $\{00,11\}$ obtenemos el $[4,1,2]$-código $\{0000,1010\}$. Por el teorema 48 este último código puede ser utilizado para extender $C_1^{(1)}(2)$ al código $C_1^{(1)}(2)^*$ de parámetros $[4,3,2]$, que resulta ser el código $C_2(4) = RM(1,2)$.

Este proceso de incrementar la dimensión de un código como se describe en el teorema 48 lo denominaremos *construcción tipo-K*. Una aplicación especial pero importante de esta construcción será recuperar los códigos binarios de Reed-Muller, $RM(\rho,m)$, a partir de los códigos $C_2(r)$ o $C_1(r)$. Para este fin requeriremos del siguiente lema.

Sean $\mathbb{N}$ el conjunto de enteros positivos y $\{T_n\}_{n=0}^{\infty}$ la sucesión de funciones $T_n : \mathbb{N} \to \mathbb{N}$, definidas como

$$T_n(\alpha) = \sum_{i=0}^{\alpha-1} \binom{\alpha+n}{i}. \tag{4.4}$$

Notemos que $T_n(\alpha) = \dim(RM(\alpha-1, \alpha+n))$. Enseguida deduciremos algunas propiedades de las funciones T_n, en particular mostraremos que estas funciones pueden ser definidas recursivamente.

Lema 50 *Para cualesquiera enteros $n \geq 0$ y $\alpha \geq 1$ las siguientes relaciones son válidas:*

i) $T_n(1) = 1$,

ii) $T_0(\alpha) = 2^\alpha - 1$,

iii) $T_{n+1}(\alpha+1) = T_n(\alpha+1) + T_{n+1}(\alpha)$,

iv) $\sum_{i=1}^{\alpha} T_n(i) = T_{n+1}(\alpha)$.

Demostración Las relaciones en *i)* y *ii)* son claras de la definición de T_n. *iii)* La suma $T_n(\alpha+1) + T_{n+1}(\alpha)$ puede ser expresada como

$$\begin{aligned} \sum_{i=0}^{\alpha} \binom{\alpha+n+1}{i} + \sum_{i=0}^{\alpha-1} \binom{\alpha+n+1}{i} &= \sum_{i=0}^{\alpha-1} \left[\binom{\alpha+n+1}{i+1} + \binom{\alpha+n+1}{i} \right] + \binom{\alpha+n+1}{0} \\ &= \sum_{i=0}^{\alpha-1} \binom{\alpha+n+2}{i} = T_{n+1}(\alpha+1). \end{aligned}$$

Enseguida se muestra un método general para incrementar la dimensión del código $C_a^{(\eta)}(r)^\circ$, para lo que requeriremos de algunas definiciones: Dado un entero $e \geq 1$ denotamos como $P(e)$ al mayor entero positivo t tal que $2^{t-1} \mid e$, y para todo entero $1 \leq i \leq P(e)$ se define $\mathbf{w}_i^{(e)} = \mathbf{1}_{e/2^{i-1}} \mathbf{0}_{e/2^{i-1}}$.

Note que los conjuntos $S_i^{(\eta)}(t)$'s son ajenos para un índice fijo i, además para cualquier vector binario $\mathbf{v}$ con soporte J, las siguientes relaciones son válidas:

S1) $S_i^{(\eta)}(t) = S_{i+1}^{(\eta)}(2t) \bigcup S_{i+1}^{(\eta)}(2t+1)$. si $2^i \mid \eta$,

S2) $\operatorname{sop}(\mathbf{v} \otimes \mathbf{1}_{2\eta}) = \bigcup_{j \in J} S_0^{(\eta)}(j-1)$.

S3) $\operatorname{sop}\left(\mathbf{v} \otimes \mathbf{w}_i^{(\eta)}\right) = \bigcup_{j \in J} S_i^{(\eta)}(2j-2)$.

Si $\{U_i\}_{i=1}^t$, $t \geq 1$, es una familia de subconjuntos de $\mathbb{F}_2^n$, entonces el código lineal generado por sus vectores se denotará como $\langle U_1, \ldots, U_t \rangle$. Para cualesquiera enteros positivos $L = \dim(C_a(r))$, η, a y r, con $a < r$, el siguiente resultado muestra cómo aumentar la dimensión del $[2\eta r, k_0, (2 - \delta_{r,L})\, 2\eta]$-código lineal $C_a^{(\eta)}(r)^\circ$, conservando su longitud y distancia mínima. Más en general dado un $[n, k_0, d]$ código lineal C se define $C^{(\eta)} = C \otimes \mathbf{1}_{2\eta}$, cuyos parámetros resultan entonces $[2\eta n, k_0, 2\eta d]$

Teorema 48 *Si* $P(\eta) = t$, *el código* $C^{(\eta)}$ *puede extenderse a un código* $C^{(\eta)*}$ *con parámetros* $\left[2\eta r, \sum_{j=0}^t k_j, 2\eta d\right]$ *si para* $1 \leq i \leq t$ *existe un* $[n2^{i-1}, k_i, d2^i]$*-código binario* $\mathbf{O}_i$. *La manera de obtener tal código* $C^{(\eta)*}$ *es añadiendo como generadores adicionales a* $C^{(\eta)}$ *los vectores que constituyen una base del código* $\mathbf{O}_i \otimes \mathbf{w}_i^{(\eta)}$, *para* $1 \leq i \leq t$.

Demostración Sean $\mathbf{O}_0^{(\eta)} = C^{(\eta)}$ y $\mathbf{O}_i^{(\eta)} = \mathbf{O}_i \otimes \mathbf{w}_i^{(\eta)}$, para $1 \leq i \leq t$. Entonces, por las relaciones **S2)** y **S3)** mencionadas arriba, el soporte de toda palabra codificada en $\mathbf{O}_i^{(\eta)}$, $0 \leq i \leq t$, es la unión de al menos $d2^i$ elementos de $HS_i^{(\eta)}$.

Supongamos que para un entero γ, $1 \leq \gamma < t$, el código $\mathbf{C} = \left\langle \mathbf{O}_0^{(\eta)}, \ldots, \mathbf{O}_\gamma^{(\eta)} \right\rangle$ tiene parámetros $[2\eta r, k_0 + k_1 + \cdots + k_\gamma, 2\eta d]$. Obviamente toda palabra codificada en $\mathbf{C}$ es la unión de al menos $d2^\gamma$ elementos de $HS_\gamma^{(\eta)}$.

Sea $\mathbf{v}_{\gamma+1}$ una palabra codificada de $\mathbf{O}_{\gamma+1}^{(\eta)}$ con soporte J. De la igualdad **S3)** tenemos que el soporte del vector $\mathbf{v} = \mathbf{v}_{\gamma+1} \otimes \mathbf{w}_{\gamma+1}^{(\eta)}$ es $\cup_{j \in J} S_{\gamma+1}^{(\eta)}(2j-2)$. Por **S1)** y para toda $\mathbf{c} \in \mathbf{C}$ el soporte de $\mathbf{c} + \mathbf{v}$ contiene exactamente uno de los conjuntos $S_{\gamma+1}^{(\eta)}(2j-2)$ o $S_{\gamma+1}^{(\eta)}(2j-1)$, para cualquier entero $j \in J$. Tenemos así las desigualdades $d(\mathbf{c}, \mathbf{v}) \geq ps(\mathbf{v}) \geq 2\eta d$. Por otro lado es fácil verificar que la dimensión de $\left\langle \mathbf{C}, \mathbf{O}_{\gamma+1}^{(\eta)} \right\rangle$ es precisamente $k_0 + k_1 + \cdots + k_{\gamma+1}$. ■

Ejemplo 49 El $[2,2,1]$-código binario $C_1(2) = RM(1,1)$ tiene matriz generadora

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

de los otros parámetros de $C_a(r)^\circ$, en el sentido que existen códigos de la misma longitud y distancia mínima pero de dimensión considerablemente mayor. Por ejemplo los parámetros del código $C_2^{(8)}(6)$ son $[96,5,32]$, pero el mejor código conocido de la misma longitud y distancia mínima +8i7uyyyytiene parámetros $[96,23,32]$ (cf. [6]). En el resto de esta sección mostraremos cómo extender el código $C_a^{(\eta)}(r)$ a un código de dimensión $k > k_0$, pero conservando su distancia mínima, por lo que ambos códigos tendrán la misma capacidad para detectar y corregir errores.

Para todo conjunto Y de enteros y cualesquiera enteros $t \geq 0$, y $u \geq 1$ se definen los conjuntos $t+Y = \{t+y : y \in Y\}$, $[u] = \{1,\ldots,u\}$.

Definición 46 *Dado el código $C_a^{(\eta)}(r)$ para cualesquiera enteros no negativos i y t tales que $2^i \mid 2\eta$, y $t < r2^i$, se define*

$$S_i^{(\eta)}(t) = \frac{\eta t}{2^{i-1}} + \left[\frac{\eta}{2^{i-1}}\right]. \tag{4.3}$$

Además se define $HS_i^{(\eta)} = \left\{S_i^{(\eta)}(2t) : 0 \leq t < r2^i\right\}$.

Sean $\eta \geq 1$ un entero, L la dimensión de $C_a(r)$ y $\mathbf{v} \in \mathbb{F}_2^{2\eta r}$, un vector de peso $(2-\delta_{r,L})2\eta$. Notemos que el soporte de toda palabra codificada en $C_a^{(\eta)}(r)^\circ$ es la unión de al menos $(2-\delta_{r,L})$ conjuntos en $HS_0^{(\eta)}$. Para extender este código añadiéndole el vector $\mathbf{v}$ sin disminuir su distancia mínima es necesario que para cualquier palabra codificada $\mathbf{c} \in C_a^{(\eta)}(r)^\circ$

$$d(\mathbf{c},\mathbf{v}) = ps(\mathbf{c}) + ps(\mathbf{v}) - 2ps(\mathbf{c}*\mathbf{v}) \geq (2-\delta_{r,L})2\eta,$$

esto es $ps(\mathbf{c}) \geq 2ps(\mathbf{c}*\mathbf{v})$, o equivalentemente si S es el soporte de $\mathbf{v}$ entonces $|S \cap G| \leq \eta$ para todo $G \in HS_0^{(\eta)}$. Pero si pedimos la condición $|S \cap G| < \eta$ para todo $G \in HS_0^{(\eta)}$ y $\mathbf{v}' = \mathbf{v}+\mathbf{c}$ entonces $\mathrm{sop}(\mathbf{v}')$ tiene cero o más de a puntos en común con cualquier $G \in HS_0^{(\eta)}$, así que $ps(\mathbf{v}) < 2ps(\mathbf{c}*\mathbf{v}')$ y por lo tanto $d(\mathbf{c},\mathbf{v}') < (2-\delta_{r,L})2\eta$. Esto siginifica que debemos pedir la condición $|S \cap G| = \eta$ para todo $G \in HS_0^{(\eta)}$.

Entonces elijamos un vector $\mathbf{v} = \mathbf{w} \otimes \mathbf{1}_\eta$, donde $\mathbf{w}$ es un vector binario de longitud $2r$ y peso $(2-\delta_{r,L})2$, es decir el soporte de $\mathbf{v}$ es la unión de exactamente $(2-\delta_{r,L})2$ de los conjuntos $S_1^{(\eta)}(t)$. Así la dimensión del $[2\eta r, k_0, (2-\delta_{r,L})2\eta]$-código $C_a^{(\eta)}(r)^\circ$ se incrementa en una unidad al agragarle el vector $\mathbf{v}$. Resumimos el razonamiento anterior en la siguiente

Proposición 47 *El código $C_a^{(\eta)}(r)$ puede ser extendido a un código $C_a^{(\eta)}(r)'$ con parámetros $[2\eta r, k_0+1, (2-\delta_{r,L})2\eta]$. Tal código $C_a^{(\eta)}(r)'$ se obtiene añadiendo un vector a $C_a^{(\eta)}(r)^\circ$ cuyo con soporte sea exactamente la unión de $(2-\delta_{r,L})2$ de los conjuntos $S_1^{(a)}(t)$, donde L es la dimensión de $C_a(r)$.*

iv) Si $\alpha = 1$ la relación es válida, así que podemos suponer $\alpha \geq 2$. De *iii*) se sigue fácilmente que $\sum_{i=\alpha-m}^{\alpha} T_n(i) + T_{n+1}(\alpha - m - 1) = T_{n+1}(\alpha)$, para todo entero $0 \leq m \leq \alpha - 2$. En particular cuando $m = \alpha - 2$ la relación *iv*) es obtenida. ■

Para cualquier entero positivo m el código binario de Reed-Muller $RM(\rho, m)$, es el código $C_2(2^m)$ si $\rho = m - 1$, el código $C_1(2^m) = \mathbb{F}_2^{2^m}$ si $\rho = m$, y $RM(0, m) = \{\mathbf{1}_{2^m}, \mathbf{0}_{2^m}\}$. Para $\rho \leq m - 2$ el código de Reed-Muller es recuperado en términos de los códigos cíclicos $C_a(r)$ definidos por la relación (4.1).

Proposición 51 *Para cualesquiera enteros* ρ, m, $3 \leq \rho + 2 \leq m$, *el código* $C_2(2^{\rho+1})$ *puede extenderse al código binario de Reed-Muller* $RM(\rho, m)$.

Demostración Sean $\mathbf{C} = C_2(2^{\rho+1})$, $\eta = 2^{m-\rho-2}$ y $\mathbf{O}_0 = \mathbf{C} \otimes \mathbf{1}_{2\eta}$. Entonces $\mathbf{C}$ tiene parámetros $[2^{\rho+1}, 2^{\rho+1} - 1, 2]$ y consiste de todas las palabras de peso par y longitud $2^{\rho+1}$, y $\mathbf{O}_0$ es un $[2^m, 2^{\rho+1} - 1, 2^{m-\rho}]$-código lineal. Para $1 \leq i \leq m - \rho - 1$, sean $\mathbf{O}_i$ el código de Reed-Muller $RM(\rho - 1, \rho + i)$ y $\mathbf{w}_i^{(\eta)} = \mathbf{1}_{2^{1-i}\eta}\mathbf{0}_{2^{1-i}\eta}$. La dimensión del código $\mathbf{O}_0$ es $T_0(\rho + 1)$ y la de $\mathbf{O}_i$ es $T_i(\rho)$, para $i \geq 1$. Del teorema 48 se sigue que el código $\mathbf{O}_0$ pude extenderse a un $\left[2^m, T_0(\rho + 1) + \sum_{i=1}^{m-\rho-1} T_i(\rho), 2^{m-\rho}\right]$-código lineal $\mathbf{O}_0^*$. Y por *iii*) lema 50 la dimensión de $\mathbf{O}_0^*$ es $T_{m-\rho-1}(\rho + 1)$, la dimensión del código binario de Reed-Muller $RM(\rho, m)$.

Supóngase que $p_i^{(m)} \in \mathbb{F}_2^m$ es la expansión binaria del entero i, entonces $\mathbb{F}_2^m = \left\{p_i^{(m)} : 0 \leq i < 2^m\right\}$. O equivalentemente el producto cartesiano $\mathbb{F}_2^m$ puede definirse recursivamente como sigue: 1) $p_0^{(1)} = 0$, $p_1^{(1)} = 1$ y 2) $p_{2i}^{(m+1)} = p_i^{(m)}|0$, $p_{2i+1}^{(m+1)} = p_1^{(m)}|1$, para $m \geq 1$, donde "|" denota la concatenación. Ahora nótese que $p_i^{(\beta)}$ es una solución del sistema lineal $\sum_{i=1}^{m} a_{ij}x_j = b_j$, $1 \leq j \leq b$ (donde $b \leq m \leq \beta$), si y sólo si $p_{2i}^{(\beta+1)}$ y $p_{2i+1}^{(\beta+1)}$ son soluciones también. Como el código $\mathbf{O}_0^*$ tiene generadores cuyo soporte es la unión de conjuntos del tipo $S_i^{(\eta)}(t)$, definidos por las relaciones (4.3), se sigue que estos generadores son los vectores de incidencia de algúna variedad afín de dimensión $(m - \rho)$ sobre el campo $\mathbb{F}_2$. Además el código de Reed-Muller $RM(\rho, m)$ es generado por los vectores de incidencia de las variedades afines de dimensión $(m - \rho)$ sobre el campo binario (proposición 23), por lo tanto $\mathbf{O}_0^* = RM(\rho, m)$ como se afimaba. ■

Los códigos de Reed-Muller pueden incluso ser recuperados en base a matrices identidad, como se muestra a continuación.

Corolario 52 *Para cualesquiera enteros* ρ, m, $2 \leq \rho + 1 \leq m$, *el código* $C_1(2^\rho)$ *puede extenderse al código de Reed-Muller* $RM(\rho, m)$.

Demostración Es suficiente con mostrar que el código $\mathbf{O}_0$ en la prueba de la proposición 51 puede obtenerse del código $C_1(2^\rho)$. Sean $\mathbf{C}_2 = C_1(2^\rho)$, $\eta = 2^{m-\rho-1}$ y

$\mathbf{O}_0' = \mathbf{C}_2 \otimes \mathbf{1}_{2\eta}$. Entonces $\mathbf{C}_2 = \mathbb{F}_2^{\rho}$ y $\mathbf{O}_0'$ es un $[2^m, 2^{\rho}, 2^{m-\rho}]$-código lineal. Elijamos $\mathbf{O}_1$ como el código de Reed-Muller $RM(\rho-1, \rho)$, y $\mathbf{w}_1^{(\eta)} = \mathbf{1}_{\eta}0_{\eta}$. Del teorema 48 se sigue que el código $\mathbf{O}_0'$ puede extenderse a un $[2^m, 2^{\rho+1}-1, 2^{m-\rho}]$-código lineal. Pero este es el código $\mathbf{O}_0$ en la prueba de la proposición 51, por lo que el mismo argumento que en dicha proposición nos conduce al resultado. ■

Ejemplo 53 El $[4,3,2]$ código $C_2(4) = RM(1,2)$ tiene matriz generadora

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

De acuerdo a la demostración de la proposición 51 el código $RM(0,2) = \{\mathbf{1}_4, \mathbf{0}_4\}$ de parámetros $[4,1,4]$ puede ser utilizado para extender $C_2(4)$ al $[8,4,4]$-código $RM(1,3) = \left\langle C_2^{(1)}(4), \mathbf{1}_4 \otimes 10 \right\rangle$ con matriz generadora

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Ejemplo 54 El $[8,7,2]$ código $C_2(8) = RM(2,3)$ tiene matriz generadora

$$G_3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

De acuerdo a la demostración de la proposición 51 puede utilizarce el código $RM(1,3)$, construido en el ejemplo previo, para extender $C_2(8)$ al $[16, 11, 4]$ código $RM(2,4) =$

$\left\langle C_2^{(1)}(8), RM(1,3) \otimes 10 \right\rangle$ con matriz generadora

$$G_4 = \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&1&0&1&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0 \\ 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \end{pmatrix}.$$

Notemos que en cada uno de los ejemplos previos se da una base para los códigos ahí construidos consistente de vectores de peso mínimo. Más adelante, en la última sección del presente capítulo y en la segunda sección del sexto se muestra una base para los códigos binarios de Reed-Muller consistente de vectores de peso mínimo.

Las palabras codificadas de peso mínimo en el código $RM(\rho, m)$ son los renglones de la matriz de incidencia de un 2-diseño[‡] (cf. [1]). Por otro lado los códigos $C_a(r)$ pueden ser utilizados para dar una descripción del código $RM(1,m)$ en términos de 1-diseños. Esta particular familia de códigos ha sido estudiada como un conjunto de polinomios (cf. [46]), como variedades afines sobre el campo binario (cf. [1]), como códigos asociados a matroides (cf. [57]), como códigos generados por los renglones de matrices de Hadamard (cf. [78], capítulo 18), etc.

El arreglo

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

es la matriz de incidenia de un 1-$(4,2,2)$ diseño. Mostraremos que el código lineal binario generado por los renglones de N, que es $C_2(4) = RM(1,2)$, puede extenderse a cualquier código binario de Reed-Muller de primer orden. La extensión se hará de tal forma que los generadores del código serán los vectores de incidencia de un 1-diseño y se mostrará una base para este código.

Definamos la matriz $N(i) = \mathbf{1}_{2^i} \otimes N \otimes \mathbf{1}_{2^{m-i-2}}$, $0 \leq i \leq m-2$, donde "$\otimes$" como antes denota el producto de Kronecker.

[‡]Un t-(v,k,λ) diseño es una estructura de incidencia con v puntos, donde cada bloque consta de k puntos, cualesquiera t puntos son incidentes con exactamente λ bloques y un punto x es incidente con un bloque B si $x \in B$. Véase la sección 1.4

Teorema 55 *Dado un entero $m \geq 2$, y para todo entero positivo $b \leq m-1$, la matriz con renglones $N(i)$, $0 \leq i \leq b-1$, es la matriz de incidencia para un 1-$(2^m, 2^{m-1}, 2^b)$ diseño $\mathcal{D}_b$. El código binario $C(\mathcal{D}_b)$ asociado a tal estructura es un $[2^m, 2+b, 2^{m-1}]$ código lineal, con polinomio enumerador de pesos $\mathcal{E}_C(x) = 1+\left(2^{b+2}-2\right) x^{2^{m-1}}+x^{2^m}$. Si $b = m-1$ el código $C(\mathcal{D}_b)$ es precisamente el código de Reed-Muller de primer orden $RM(1,m)$.*

Demostración Es fácil verificar que la matriz de renglones $N(i)$, $0 \leq i \leq b-1$, es la matriz de incidencia de un 1-diseño con los parámetros indicados. Por otro lado el espacio vectorial generado por los renglones de la matriz N es el $[4,3,2]$ código $C_2(4)$ antes descrito, por lo que $C(\mathcal{D}_1) = C_2(4) \otimes \mathbf{1}_{2^{m-2}}$ tiene parámetros $[4(2^{m-2}), 3, 2(2^{m-2})]$. Además el vector $\mathbf{1}_{2^m}$ es la suma de los primeros dos renglones de $N(0)$.

Denotemos como $\mathbf{v}_j$ al j-ésimo renglón de N, $j = 1,2,3,4$. Entonces $\mathbf{v}_1+\mathbf{v}_2 = \mathbf{v}_3+\mathbf{v}_4 = \mathbf{1}_4$ y $\mathbf{v}_1 \otimes \mathbf{1}_2 + \mathbf{1}_2 \otimes \mathbf{v}_1 = \mathbf{1}_2 \otimes \mathbf{v}_4$. Fácilmente podemos verificar que

i) $\mathbf{1}_{2^m} + \mathbf{1}_{2^i} \otimes \mathbf{v}_1 \otimes \mathbf{1}_{2^{m-i-2}} = \mathbf{1}_{2^i} \otimes \mathbf{v}_2 \otimes \mathbf{1}_{2^{m-i-2}}$,
ii) $\mathbf{1}_{2^i} \otimes \mathbf{v}_1 \otimes \mathbf{1}_{2^{m-i-2}} + \mathbf{1}_{2^{i-1}} \otimes \mathbf{v}_1 \otimes \mathbf{1}_{2^{m-i-2}} = \mathbf{1}_{2^i} \otimes \mathbf{v}_4 \otimes \mathbf{1}_{2^{m-i-2}}$,
iii) $\mathbf{1}_{2^m} + \mathbf{1}_{2^i} \otimes \mathbf{v}_4 \otimes \mathbf{1}_{2^{m-i-2}} = \mathbf{1}_{2^i} \otimes \mathbf{v}_3 \otimes \mathbf{1}_{2^{m-i-2}}$.

Es decir, para un índice fijo i_0, $1 \leq i_0 \leq a-1$, los renglones de la matriz $N(i_0)$, pueden ser expresados como combinación lineal de los renglones de las matrices $N(i)$, $i < i_0$, y el primer renglón de $N(i_0)$. Esto prueba que la dimensión de $C(\mathcal{D}_b)$ es como se afirma.

Al notar que $\mathbf{1}_{2^i} \otimes \mathbf{u}_1 \otimes \mathbf{1}_{2^{m-i-2}}$, $1 \leq i \leq m-2$, es el generador del código $RM(0, i+1) \otimes \mathbf{1}_{2^{m-i-2}}\mathbf{0}_{2^{m-i-2}}$ el resultado se sigue de la proposición 51. ■

De la demostración anterior concluimos que una base para el código $RM(1,m)$ está formada por los vectores $\mathbf{v}_i \otimes \mathbf{1}_{2^{m-2}}$, $i = 1,2,3$ además de $\mathbf{1}_{2^j} \otimes \mathbf{v}_1 \otimes \mathbf{1}_{2^{m-j-2}}$, $1 \leq j \leq m-2$. Del ejemplo 49 se tiene que de hecho los códigos binarios de Reed-Muller de primer orden pueden ser recuperados a partir de la matriz identidad de 2×2.

4.3 Los códigos $C_{a,b}^{(\eta,\theta)}(r,s)$

En la presente sección una nueva clase de códigos es definida utilizando los códigos $C_{a,b}(r,s)$ definidos en la sección previa. Los parámetros de los códigos en esta nueva familia serán incrementados de forma semajante a como se hizo con los códigos $C_a^{(\eta)}(r)$. Resultados similares fueron obtenidos en [24, 31], donde la dimensión del espacio de ciclos de una gráfica finita, conexa y no dirigida es incrementada. Los códigos aquí definidos serán utilizados en el siguiente capítulo para determinar los códigos lineales asociados a una estructura de incidencia conocida como sistema de ciclos.

Para cualesquiera enteros $r > a \geq 1$, $s > b \geq 1$ sean $\mathbf{u}^{(i)}$ y $\mathbf{v}^{(i)}$ el i-ésimo corrimiento cíclico de $\mathbf{1}_a\mathbf{0}_{r-a}$ y $\mathbf{1}_b\mathbf{0}_{s-b}$ respectivamente. Denotemos como $C_{a,b}(r,s)$ al

código generado por los vectores de la forma $\left|\mathbf{u}^{(i)}\right|\mathbf{v}^{(j)}|$, $i,j \geq 1$, es decir

$$\boxed{C_{a,b}(r,s) = \left\langle \left|\mathbf{u}^{(i)}\right|\mathbf{v}^{(j)}|\right\rangle_{i,j\geq 1}} \tag{4.5}$$

Los parámetros de este código serán dados en términos de aquellos de los códigos binarios $C_a(r)$ y $C_b(s)$ definidos en la sección anterior. De la definición es claro que $C_{a,b}(r,s) \subset C_a(r) \oplus C_b(s)$, la suma directa de los códigos $C_a(r)$ y $C_b(s)$.

Sean $L_1 = \dim(C_a(r))$, $L_2 = \dim(C_b(s))$ y además sean $m_1(x) = \sum_{j=0}^{L_1} a_j x^j$ y $m_2(x)$ los polinomios característicos de $C_a(r)$ y $C_b(s)$, definidos por la ecuación (2.2), respectivamente, y calculados por medio del algorítmo de Berlekamp-Massey. Recordemos que el peso de $m_1(x)$ es el peso de $\mathbf{a} = (a_{L_1}, a_{L_1-1}, \ldots, a_0) \in \mathbb{F}_2^{L_1+1}$. Es fácil ver que $\sum_{i=n}^{n+L_1} a_{i-n}\mathbf{u}^{(i)} = \mathbf{0}$, donde los subíndices son reducidos módulo r.

Los códigos $C_{a,b}(r,s)$ se dividen en dos clases:

Tipo d1: Si uno de los códigos $C_a(r)$ o $C_b(s)$ es el espacio total, es decir tiene la máxima dimensión, y el peso del polinomio característico del otro es imapr (los códigos de esta clase tienen distancia mínima 1).

Tipo d2: El resto de casos.

En general los códigos del tipo d1 no tienen buenos parámetros pero pueden ser estudiados de forma similar a como se hace con los del tipo d2. Por lo tanto sólo los código de este último tipo serán considerados y la mención del tipo será omitida en el resto del presente trabajo.

Los parámetros del código $C_{a,b}(r.s)$ son determinados en la siguiente

Proposición 56 *El código* $C_{a,b}(r,s)$ *tiene parámetros* $[r+s,k,2]$, *donde* $k = L_1 + L_2 - 1$, *si* $ps(m_1(x))$ *y* $ps(m_2(x))$ *son pares y* $k = L_1 + L_2$, *en otro caso.*

Demostración Sea $\mathcal{C} = C_{a,b}(r,s)$ y como antes supongamos que $\mathbf{u}^{(i)}$ y $\mathbf{v}^{(i)}$ son el i-ésimo corrimiento cíclico de $\mathbf{1}_a\mathbf{0}_{r-a}$ y $\mathbf{1}_b\mathbf{0}_{s-b}$ respectivamente. Probaremos que la dimensión de $\mathcal{C}$ depende del peso de los polinomios característicos de $C_a(r)$ y de $C_b(s)$.

En efecto, para todo $j \geq 0$ si $ps(m_1(x))$ es par entonces

$$\sum_{i=n}^{n+L_1-1} a_{i-n}|\mathbf{u}^{(i)}|\mathbf{v}^{(j)}| = |\mathbf{u}^{(n+L_1)}|\mathbf{v}^{(j)}|,$$

pero si es impar

$$\sum_{i=n}^{n+L_1-1} a_{i-n}|\mathbf{u}^{(i)}|\mathbf{v}^{(j)}| = |\mathbf{u}^{(n+L_1)}|\mathbf{0}_s|,$$

de ahí que $|\mathbf{u}^{(i)}|\mathbf{0}_s| \in \mathcal{C}$ para todo $i \geq 0$. Notemos además que $|\mathbf{u}^{(i)}|\mathbf{v}^{(j)}|$, $|\mathbf{u}^{(i)} \mid \mathbf{0}_s| \in \mathcal{C}$ implica $|\mathbf{0}_r|\mathbf{v}^{(j)}| \in \mathcal{C}$, por lo tanto si $ps(m_1(x))$ o $ps(m_2(x))$ es impar tendremos

$\mathcal{C} = C_a(r) \oplus C_b(s)$, en otro caso $\dim(\mathcal{C}) = L_1 + L_2 - 1$. En este último caso cualquier generador $|\mathbf{u}^{(i)}|\ \mathbf{v}^{(j)}|$ de $\mathcal{C}$ puede ser escrito como

$$|\mathbf{u}^{(i)}|\ \mathbf{v}^{(j_0)}| + |\mathbf{u}^{(i_0)}|\ \mathbf{v}^{(j_0)}| + |\mathbf{u}^{(i_0)}|\ \mathbf{v}^{(j)}|$$

y una base para el código es

$$\left\{|\mathbf{u}^{(i)}|\mathbf{v}^{(j_0)}|\right\}_{i=0}^{L_1-1} \cup \left\{|\mathbf{u}^{(i_0)}|\mathbf{v}^{(j)}|\right\}_{j=0}^{L_2-1},$$

para índices fijos $0 \leq i_0 < L_1$, $0 \leq j_0 < L_2$.

Nótese que aun cuando alguno de los códigos $C_a(r)$ o $C_b(s)$ tenga distancia mínima 1, $\mathcal{C}$ no tiene palabras codificadas de este peso, por lo tanto para toda $\mathbf{c} \in \mathcal{C}$ se cumple $ps(\mathbf{c}) \geq 2$. ■

Sean $g_1(x)$ y $g_2(x)$ los polinomios generadores de $C_a(r)$ y $C_b(s)$ respectivamente. El código $C_{a,b}(r,s)$ puede extenderse a un $[r+s, k_0, 2]$-código lineal $C_{a,b}(r,s)^\circ$ como se muestra enseguida:

- Si $(1+x)$ divide a $g_1(x)$ y a $g_2(x)$ entonces $k_0 = r+s-1$, i.e., $C_{a,b}(r,s)^\circ = C_2(r+s)$.
- Si $(1+x)$ no divide a $g_1(x)$ pero sí a $g_2(x)$ entonces $C_{a,b}(r,s)$ puede extenderse al código $C_{a,2}(r,s)$ de dimensión $L_1 + s - 1$. Cuando $L_1 = r$ tomamos $k_0 = L_1 + s - 1$, en otro caso podemos tomar $k_0 = L_1 + s$ añadiendo a este último código el vector $\mathbf{1}_1\mathbf{0}_{r-1}\mathbf{1}_1\mathbf{0}_{s-1}$ como generador adicional.
- Se tiene un resultado similar si $1+x$ únicamente divide al polinomio generador de $C_a(r)$.
- Si $L_1 < r$, $L_2 < s$ y $(1+x)$ no divide a $g_1(x)$ ni a $g_2(x)$ entonces k_0 es $\dim(C_{a,b}(r,s)) + 1$, que se obtiene como antes añadiendo a $C_{a,b}(r,s)$ el vector $\mathbf{1}_1\mathbf{0}_{r-1}\mathbf{1}_1\mathbf{0}_{s-1}$ como generador adicional.
- En otro caso $k_0 = \dim(C_{a,b}(r,s))$.

Tenemos así que $C_{a,b}(r,s)^\circ$ es un $[r+s, k_0, 2]$ código lineal binario.

Ejemplo 57 Los polinomios característico y generador del $[4,3,2]$-código cíclico $C_2(4)$ son $m(x) = 1+x+x^2+x^3$ y $g(x) = 1+x$ respectivamente (véase el apéndice). Por lo tanto $C_{2,2}(4,4)$ tiene parámetros $[8,5,2]$, y $C_{2,2}(4,4)^\circ$ resulta ser un $[8,7,2]$-código lineal con matriz generadora

$$G_5 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Si $\mathbf{v}_i$ y $\mathbf{w}_i$, $i=1,2$, son vectores binarios, $\mathbf{v}_i \in \mathbb{F}_2^{n_i}$ y $\mathbf{v} = |\mathbf{v}_1|\,\mathbf{v}_2|$ entonces el vector $|\mathbf{v}_1 \otimes \mathbf{w}_1|\,\mathbf{v}_2 \otimes \mathbf{w}_2|$ se denotará como $\mathbf{v} \otimes |\mathbf{w}_1|_{n_1}\,|\mathbf{w}_2|_{n_2}$. Para cualesquiera enteros positivos a, b, r, s, η, θ tales que $a < r$ y $b < s$ definimos el código $C_{a,b}^{(\eta,\theta)}(r,s) = C_{a,b}(r,s) \otimes |\mathbf{1}_{2\eta}|_r\,|\mathbf{1}_{2\theta}|_s$, es decir

$$\boxed{C_{a,b}^{(\eta,\theta)}(r,s) = \{|\mathbf{c}_1 \otimes \mathbf{1}_{2\eta}|\,\mathbf{c}_2 \otimes \mathbf{1}_{2\theta}| : |\mathbf{c}_1|\,\mathbf{c}_2| \in C_{a,b}(r,s),\ \mathbf{c}_1 \in C_a(r),\ \mathbf{c}_2 \in C_b(s)\}.} \tag{4.6}$$

Los parámetros del código $C_{a,b}^{(\eta,\theta)}(r,s)$ son fácilmente deducidos.

Proposición 58 *$C_{a,b}^{(\eta,\theta)}(r,s)$ es un $[2(\eta r+\theta s), k, 4\min\{\eta,\theta\}]$-código, donde k es la dimensión de $C_{a,b}(r,s)$.*

El código $C_{a,b}^{(\eta,\theta)}(r,s)$ puede extenderse a $C_{a,b}^{(\eta,\theta)}(r,s)^\circ = C_{a,b}(r,s)^\circ \otimes |\mathbf{1}_{2\eta}|_r\,|\mathbf{1}_{2\theta}|_s$ cuyos parámetros resultan $[2(\eta r+\theta s), k_0, 4\min\{\eta,\theta\}]$, donde $k_0 = \dim(C_{a,b}(r,s)^\circ)$. En el siguiente teorema se muestra una manera en que la dimensión de este último código puede ser incrementada sin alterar su longitud ni su distancia mínima, la cual es análoga a la construcción tipo-K definida en la sección anterior.

Definición 59 *Supóngase que $i, j, t, e \geq 0$ denotan enteros. Asociado a cada código $C_{a,b}^{(\eta,\theta)}(r,s)$ se definen los conjuntos*

$$\begin{aligned} S_i^{(\eta)}(t) &= \tfrac{t\eta}{2^{i-1}} + \left[\tfrac{\eta}{2^{i-1}}\right],\ \textit{si } 2^i \mid 2\eta \textit{ y } t < r2^i, \\ S_j^{(\eta,\theta)}(e) &= 2\eta r + \tfrac{e\theta}{2^{j-1}} + \left[\tfrac{b}{2^{j-1}}\right].\ \textit{si } 2^j \mid 2\theta \textit{ y } e < s2^j. \end{aligned} \tag{4.7}$$

Además $HS_i^{(\eta)} = \left\{S_i^{(\eta)}(2t) : 0 \leq t < r2^i\right\}$ *y* $HS_j^{(\eta,\theta)} = \left\{S_j^{(\eta,\theta)}(2e) : 0 \leq e < s2^j\right\}$.

Los conjuntos en (4.7) jugarán un papel similar al de los conjuntos definidos por la ecuación (4.3) en la sección 4.2. Agregaremos a $C_{a,b}^{(\eta,\theta)}(r,s)^\circ$, como generadores adicionales, vectores con soporte en los conjuntos $HS_i^{(\eta)}$ y $HS_j^{(\eta,\theta)}$.

Como en la sección 4.2, si $e \geq 1$ es un entero se denotará como $P(e)$ al mayor entero positivo t tal que $2^{t-1} \mid e$, y para todo entero $1 \leq i \leq P(e)$ el vector $\mathbf{w}_i^{(e)} = \mathbf{1}_{e/2^{i-1}}\mathbf{0}_{e/2^{i-1}}$ es definido.

Sin pérdida de generalidad podemos suponer que $P(\eta) \geq P(\theta)$. El código $C_{a,b}^{(\eta,\theta)}(r,s)^\circ$ puede extenderse utilizando la construcción tipo-K del teorema 48, es decir se incrementará su dimensión sin alterar su longitud ni su distancia mínima, como muesta el siguiente par de teoremas.

Teorema 60 *Si $P(\theta) = t$ el código $C_{a,b}^{(\eta,\theta)}(r,s)^\circ$ puede extenderse a un*

$$\left[2(\eta r+\theta s), \sum_{i=0}^{t} k_i, 4\min\{\eta,\theta\}\right]$$

código lineal $\mathbf{C}^*$, *si para cada* $1 \leq i \leq t$ *existe un* $[2^{i-1}(r+s), k_i, 2^{i+1}]$*-código lineal* $\mathbf{O}_i$. *Tal código* $\mathbf{C}^*$ *puede obtenerse añadiéndo a* $C_{a,b}^{(\eta,\theta)}(r,s)^\circ$ *cualesquiera* k_i *vectores que constituyan una base de* $\mathbf{O}_i \otimes \left|\mathbf{w}_i^{(\eta)}\right|_{r2^{i-1}} \left|\mathbf{w}_i^{(\theta)}\right|_{s2^{i-1}}$, $1 \leq i \leq t$, *como generadores adicionales, donde* $k_0 = \dim\left(C_{a,b}(r;s)^\circ\right)$.

Demostración La prueba es similar a la del teorema 48 por lo que se omiten algunos detalles. Sea $\mathbf{O}_i^* = \mathbf{O}_i \otimes \left|\mathbf{w}_i^{(\eta)}\right|_{r2^{i-1}} \left|\mathbf{w}_i^{(\theta)}\right|_{s2^{i-1}}$ para $1 \leq i \leq t$ y supongamos que el código $\mathbf{C} = \left\langle C_{a,b}^{(\eta,\theta)}, \mathbf{O}_1^*, \ldots, \mathbf{O}_\gamma^* \right\rangle$, donde $1 \leq \gamma < t$, tiene parámetros $\left[2(\eta r + \theta s), \sum_{i=0}^{\gamma} k_i, 4\min\{\eta,\theta\}\right]$. Entonces el soporte de cualquiera de las palabras codificadas de $\mathbf{C}$ es la unión de al menos $2^{\gamma+1}$ elementos de $HS_\gamma^{(\eta)} \cup HS_\gamma^{(\eta,\theta)}$.

Sea $\mathbf{v}_{\gamma+1}$ una palabra codificada de $\mathbf{O}_{\gamma+1}$ con soporte $J = J_1 \cup J_2$, donde $J_1 \subset \{1, \ldots, 2^\gamma r\}$ y $J_2 \subset 2^\gamma r + \{1, \ldots, 2^\gamma s\}$. Definamos $\mathbf{v} = \mathbf{v}_{\gamma+1} \otimes \left|\mathbf{w}_{\gamma+1}^{(\eta)}\right|_{r2^\gamma} \left|\mathbf{w}_{\gamma+1}^{(\theta)}\right|_{s2^\gamma}$, cuyo soporte es $\left(\cup_{j\in J_1} S_{\gamma+1}^{(\eta)}(2j-2)\right) \cup \left(\cup_{j\in J_2} S_{\gamma+1}^{(\eta,\theta)}(2j-2)\right)$. Por lo tanto para toda $\mathbf{c} \in \mathbf{C}$ tendremos $d(\mathbf{c},\mathbf{v}) \geq wt(\mathbf{v}) \geq 4\min\{\eta,\theta\}$. Se verifica fácilmente que la dimensión de $\left\langle \mathbf{C}, \mathbf{O}_1^*, \ldots, \mathbf{O}_{\gamma+1}^* \right\rangle$ es $\sum_{i=0}^{\gamma+1} k_i$. ■

Ejemplo 61 De la tabla contenida en el apéndice obtenemos que los polinomios característico y generador de $C_3(4)$ son $m_1(x) = 1 + x^4$ y $g_1(x) = 1$ respectivamente, mientras que los respectivos polinomios de $C_2(6)$ son $m_2(x) = (1+x^6)/(1+x)$ y $g_2(x) = 1 + x$. Por lo tanto $C_{3,2}(6,4)^\circ$ tiene parámetros $[10, 8, 2]$ de lo cual se deduce que $C_{3,2}^{(2,2)}(6,4)$ es un $[40, 8, 8]$-código. De acuerdo al teorema 60 se requiere de un $[10, 5, 4]$-código lineal binario $\mathbf{O}_1$ así como un $[20, 8, 8]$-código $\mathbf{O}_2$ con las mismas características.

Una matriz generadora para el código $\mathbf{O}_1$ se obtiene al elegir los primeros cuatro renglones así como el octavo y las primeras diez columnas de la matriz G_4 dada en el ejemplo 54 (es decir acortando el código $RM(2,4)$). Por otro lado considere el código cíclico (binario) generado por $g(x) = 1+x+x^5+x^6+x^7+x^9+x^{11} \in R_{23}$, donde como antes $R_{23} = \mathbb{F}_2[x]/(x^{23}-1)$ (este código se denomina de Golay). Entonces una base para el código $\mathbf{O}_2$ corresponde a los vectores $|x^j g(x)|\, 1|$ para $0 \leq j \leq 7$, después de suprimir aquellas posiciones coordendas donde todas las palabras codificadas tienen entrada cero.

Entonces es posible extender $C_{3,2}^{(2,2)}(6,4)$ a un $[40, 21, 8]$ código lineal. El código con mejores parámetros de la misma longitud y distancia mínima tiene dimensión 23 (cf. [6]), sin embargo el mejor código binario doblemente circulante con las mismas características tiene parámetros $[40, 20, 8]$ (cf. [46], pág. 509).

Para cualquier entero m el código de Reed-Muller $RM(m,m)$ es el espacio lineal $\mathbb{F}_2^m$, y $RM(m-1,m)$ es el código $C_{1,1}(2^{m-1}, 2^{m-1})$ definido en la sección 4.3. El siguiente resultado muestra que el código binario de Reed-Muller $RM(\rho,m)$, $2 \leq \rho + 2 < 2\rho + 2$, puede ser recuperado con los métodos descritos en esta sección.

Corolario 62 *Sean* m *y* ρ *enteros tales que* $2 \leq \rho \leq m-2$. *Sean* $a = b = 2$, $r = s = 2^{\rho}$ *y* $\eta = \theta = 2^{m-\rho-2}$. *Entonces el código* $C_{a,a}^{(\eta,\eta)}(r,r)^{\circ}$ *tiene parámetros* $[2^m, 2^{\rho+1}-1, 2^{m-\rho}]$ *y, como en la proposición 51, puede extenderse al código* $RM(\rho,m)$.

Demostración Del teorema 60 se deduce que los parámetros de $C_{a,a}^{(\eta,\eta)}(r,r)^{\circ}$ son como se afirma. Que tal código es efectivamente de Reed-Muller se sigue de la proposición 51 y del hecho que $C_{a,a}(r,r)^{\circ} = C_2(2r)$. ■

Para todo $x \in \mathbb{R}$ denotamos como $\lceil x \rceil$ al entero n tal que $n-1 < x \leq n$. Si $P(\eta) > P(\theta)$ la dimensión del código $\mathbf{C}^*$ del teorema 60 puede incrementarse aún más como es mostrado en el siguiente resultado.

Teorema 63 *El código* $\mathbf{C}^*$ *del teorema 60 puede extenderse a un*

$$\left[2(\eta r + \theta s), \sum_{i=0}^{P(\eta)} k_i, 4\min\{\eta,\theta\}\right]$$

código lineal $\mathbf{C}_2^*$, *si para* $P(\theta) < i \leq P(\eta)$ *existe un* $[2^{i-1}r, k_i, \lceil \theta 2^{i+1}/\eta \rceil]$ *código lineal* $\mathbf{O}_i$. *Tal código* $\mathbf{C}_2^*$ *puede obtenerse añadiendo a* $\mathbf{C}^*$ *cualesquiera* k_i *vectores que constituyan una base de* $\mathbf{O}_i \otimes \mathbf{w}_i^{(\eta)} \oplus \{\mathbf{0}_{2\theta s}\}$, $P(\theta) < i \leq P(\eta)$, *como generadores adicionales.*

Demostración La prueba es similar a aquella del teorema 48, es decir se realiza un análogo a una extensión tipo-K en las primeras $2\eta r$ posiciones coordenadas del código sin alterar la dimensión ni la distancia mínima del código que se extiende. Por lo tanto la prueba es omitida. ■

Ejemplo 64 El código $C_{2,2}(4,4)^{\circ}$ construido en el ejemplo 57 puede extenderse a $C_{2,2}^{(2,1)}(4,4)^{\circ}$, el cual tiene parámetro $[24,7,4]$, y una de sus matrices generadoras es la que se muestra a continuación

$$G_6 = \begin{pmatrix}
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0
\end{pmatrix}$$

Por otro lado elijamos los códigos $\mathbf{O}_1$ y $\mathbf{O}_2$ ambos iguales al código de Reed-Muller $RM(1,3)$, construido en el ejemplo 53, el cual tiene matriz generadora G_2 dada en

aquel ejemplo. Si agregamos a G_6 los renglones de las matrices $G_2 \otimes |\mathbf{1}_2\mathbf{0}_2|_4\,|\mathbf{1}_1\mathbf{0}_1|_4$ y $(G_2 \otimes \mathbf{1}_1\mathbf{0}_1|\,\mathbf{0}_8)$, es decir los renglones de

$$G_7 = \begin{pmatrix}
1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0&1&1&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

obtendremos un $[24, 15, 4]$-código lineal binario, el cual tiene los mejores parámetros que puede alcanzar un $[24, 15, d]$-código del mismo tipo (cf. [6]).

4.4 Una base del código $RM(\rho, m)$ de vectores de peso mínimo

En esta sección se describe una base para el código de Reed-Muller formada por vectores de peso mínimo y su relación con la familia de códigos del tipo $C_a(r)$ es explicada. La importancia de este resultado, que es equivalente al obtenido por Gao y Key en [15], radica en que al utilizar vectores de peso mínimo se facilitan las operaciones para codificar y decodificar mensajes.

En la presente sección denotaremos como R_n al anillo cociente $\mathbb{F}_2[x]/(1+x^n)$ de los polinomios en la indeterminada x con coeficientes binarios reducidos módulo $1+x^n$. En el enunciado de nuestro resultado se utilizará la siguiente notación: El vector $\mathbf{v} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_2^n$ puede ser representado en forma polinomial como $\varphi_n(\mathbf{v}) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R_n$.

Sea $\mu = m - \rho \in \mathbb{N}$. Para todo vector $\mathbf{a} = (a_1, \ldots, a_\mu) \in \mathbb{N}^\mu$ el polinomio $F_{\mathbf{a}}(x) \in R_{2^m}$ es definido como

$$F_{\mathbf{a}}(x) = \prod_{i=1}^{\mu} \left(1 + x^{2^{a_i}}\right).$$

Como $F_{\mathbf{a}}(x)$ es el producto de μ binomios de la forma $1 + x^{2^{a_i}}$, este polinomio es la suma de 2^μ monomios, i.e., su peso es 2^μ. En el siguiente resultado se determina una base para el código binario de Reed-Muller $RM(\rho, m)$ consistente de vectores de peso mínimo. En la demostración se utilizarán las funciones $T_n(\alpha) = \sum_{i=0}^{\alpha-1} \binom{\alpha+n}{i}$ definidas por la ecuación (4.4).

Teorema 65 *Sean m y ρ dos enteros con $0 \le \rho < m$ y $\mu = m - \rho$. Definamos $\Omega = \{0\}$ si $\mu = 1$ y $\Omega = \{\mathbf{a} \in \mathbb{N}^\mu : 0 \le a_1 < \cdots < a_\mu < m,\ a_i = a_{\mu-1} + 1\}$ si $\mu > 1$.*

Entonces el conjunto de vectores

$$\mathcal{F} = \left\{ x^{t\ 2^{a_\mu}}\ F_{\mathbf{a}}(x) : \mathbf{a} \in \Omega,\ t = 0, 1, \ldots, 2^{m-a_\mu} - 2 \right\}$$

es una base para el código binario de Reed-Muller RM (ρ, m).

Demostración Sean $f(x) \in \mathbb{F}_2[x]$, y φ_n la función descrita en el segundo párrafo de esta sección. Se verifica fácilmente que para cualquier entero $b \geq 0$, si $\varphi_n(\mathbf{v}) = f(x)$, entonces

(1) $\prod_{k=0}^{b-1}\left(1 + x^{2^k}\right) f\left(x^{2^b}\right)$ es la imagen de $\mathbf{v} \otimes \mathbf{1}_{2^b}$ bajo $\varphi_{n2^b(2^b-1)}$ y

(2) $\prod_{k=0}^{b-1}\left(1 + x^{2^k}\right) f\left(x^{2^{b+1}}\right)$ corresponde a $\mathbf{v} \otimes \mathbf{1}_{2^b}\mathbf{0}_{2^b}$ bajo $\varphi_{n2^{b+1}(2^b-1)}$.

Si $\mu = 1$ entonces el código $RM(\rho, m)$ es el código peso par de parámetros $[2^m, 2^m - 1, 2]$ consistente de todas las palabras de peso par de longitud 2^m. Este código es cíclico y visto como esta clase de código es generado por el polinomio $1 + x \in R_{2^m}$ (véase la sección 2.1 para la definicón de este concepto). Por lo tanto los vectores $x^t(1 + x) = x^t F_0(x)$, con $0 \leq t \leq 2^m - 2$, constituyen una base del código, tal como se afirma.

Si $\rho = 0$ el código $RM(\rho, m)$ tiene parámetros $[2^m, 1, 2^m]$ y es el código de repetición $\{\mathbf{0}_{2^m}, \mathbf{1}_{2^m}\}$. En este caso Ω consiste de un único vector $\mathbf{a}$ de longitud m con $a_i = i - 1$ para $1 \leq i \leq m$, y el conjunto $\mathcal{F}$ resulta como se espera.

Los casos restantes son analizados a través de la proposición 51. Como $C_2(2^{\rho+1})$ es el código cíclico peso par de longitud $2^{\rho+1}$, por el inciso (1) mencionado arriba $C_2(2^{\rho+1}) \otimes \mathbf{1}_{2^{\mu-1-i}}$ tiene como una de sus bases a los vectores $x^{t2^{\mu-1}} \prod_{i=0}^{\mu-1}\left(1 + x^{2^i}\right) \in R_{2^\mu}$. Por otro lado supongamos que para $0 \leq i < \mu$ el código $RM(\rho - 1, \rho + i)$ tiene una base consistente de los vectores $x^{t2^{a_{\mu_i}}} F_{\mathbf{a}}(x) \in R_{2^{\rho+i}}$, con $\mu_i = i + 1$ y $0 \leq a_1 < \cdots < a_{\mu_i}$. Entonces $RM(\rho - 1, \rho + i) \otimes \mathbf{1}_{2^{\mu-1-i}}\mathbf{0}_{2^{\mu-1-i}}$ tendrá una base formada por los vectores

$$x^{t2^{a_{\mu_i}+\mu-i}} \prod_{j=0}^{\mu-2-i}\left(1 + x^{2^j}\right) \prod_{j=0}^{\mu_i}\left(1 + x^{2^{a_j+\mu-i}}\right),$$

donde a los productos se les asigna el valor de 1 si el límite superior es negativo. El resultado se sigue ahora de la proposición 51. ■

Ejemplo 66 El $[32, 16, 8]$ código $RM(2, 5)$ tiene una base constituida por vectores

de peso mínimo dada por los siguientes polinomios

$$x^{4t}\prod_{k\in K}\left(1+x^{2^k}\right). \qquad K=\{0,1,2\}, \quad 0\leq t\leq 6.$$

$$x^{8t}\prod_{k\in K}\left(1+x^{2^k}\right). \qquad K=\{0,2,3\}, \quad 0\leq t\leq 2.$$

$$x^{16t}\prod_{k\in K}\left(1+x^{2^k}\right). \qquad K=\{0,3,4\}, \quad 0\leq t\leq 0.$$

$$x^{8t}\prod_{k\in K}\left(1+x^{2^k}\right). \qquad K=\{1,2,3\}, \quad 0\leq t\leq 2.$$

$$x^{16t}\prod_{k\in K}\left(1+x^{2^k}\right), \qquad K=\{1,3,4\}, \quad 0\leq t\leq 0.$$

$$x^{16t}\prod_{k\in K}\left(1+x^{2^k}\right), \qquad K=\{2,3,4\}, \quad 0\leq t\leq 0.$$

CAPÍTULO 5

CÓDIGOS ASOCIADOS A SISTEMAS DE CICLOS

El trabajo en este capítulo es similar al de Key y Sullivan [35], quienes estudian los códigos asociados a sistemas triples y cuádruples de Steiner (cf. sección 1.4), concluyendo que sólo al considerar como conjunto de escalares a campos de característica 2 ó 3 pueden obtenerse códigos no triviales. Concluyen que en este caso el código binario contiene un subcódigo que puede ser acortado a un código binario de Hamming suprimiendo las posiciones coordenadas donde todas las palabras codificadas tienen entradas cero. En el presente escrito también se desarrolla un trabajo similar al que aparece en [24, 31], donde un $[n, k, d]$-código lineal (el espacio de ciclos de una gráfica) es extendido a un $[n, k', d]$-código lineal, con $k' > k$. En el espacio de ciclos de una gráfica G se considera la estructura de incidencia cuyo conjunto de puntos está constituido por las aristas de la gráfica, y donde los bloques son los ciclos de G. Mediante un ejemplo muestran que su construcción los conduce a recuperar los códigos binarios de Hamming al elegir G como una gráfica bipartita completa no dirigida con el número adecuado de vértices.

Una manera de definir un sistema triple de Steiner es la siguiente (cf. [43], pág. 325): sea K_n la gráfica completa no dirigida con n vértices. Un sistema triple de Steiner es un par ordenado $(\mathcal{P}, \mathcal{T})$, donde $\mathcal{P}$ es el conjunto de vértices de K_n y $\mathcal{T}$ es una partición de sus aristas en copias de K_3. En la literatura existen varios trabajos que generalizan estas ideas para responder a la siguiente pregunta: ¿es posible descomponer una gráfica G en copias de una gráfica dada Γ de tal forma que sus copias, vistas como subgráficas de G, no tengan aristas en común? (cf. [5]). Frecuentemente Γ es elegida como una gráfica completa o un ciclo. En el segundo caso se tiene el concepto de sistema de ciclos (cf. [43], pág. 325):

Definición 67 *Sean $m \geq 3$ un entero y $G = (V, A)$ una gráfica finita conexa no dirigida con conjunto de vértices V y aristas A. Un m-sistema de ciclos de la gráfica G, m-$SC(G)$, es una pareja ordenada (V, Υ), donde Υ es una partición de las aristas de G en ciclos de longitud m.*

En particular los sistemas triples de Steiner forman un sistema de ciclos, con ciclos de longitud 3, de la gráfica completa no dirigida. En este capítulo consideraremos la estructura de incidencia (cf. sección 1.4) con conjunto de bloques formado por los ciclos de un sistema de ciclos de una gráfica bipartita, y cuyo conjunto de

puntos consistirá de los vértices de la gráfica, por lo que en cierto sentido nuestro trabajo complementa y establece una relación entre los antes mencionados.

Sean $G = (V, A)$ una gráfica finita, conexa y no dirigida y (V, Υ) un m-sistema de ciclos de G. En este capítulo consideraremos la estructura de incidencia $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, que también denotaremos como $m\text{-}SC(G)$, donde $\mathcal{P} = V$, $\mathcal{B} = \Upsilon$, y el par (x, B) está en $\mathcal{I}$ si el vértice x es incidente al ciclo B.

En general consideraremos la estructura de incidencia $\mathcal{D}^* = (\mathcal{P}^*, \mathcal{B}^*, \mathcal{I}^*)$, donde $\mathcal{P}^* = V$, $\mathcal{B}^*$ es la colección de todas las subgráficas de G, y el par (x, Γ) está en $\mathcal{I}^*$ si el vértice x es incidente a la subgráfica Γ de G. Por lo que el concepto de *vector de incidencia de la subgráfica* Γ de G está bien definido.

El capítulo se divide en tres secciones. La primera trata sobre los 4-sistemas de ciclos de una gráfica bipartita completa no dirigida y los códigos asociados a tales estructruras. Se muestra mediante ejemplos que tal construcción conduce a códigos con parámetros óptimos, en particular a los código binarios de Hamming. Por último se prueba que el código asociado a un 4-sistema de ciclos de una gráfica completa contiene un código asociado a una gráfica completa bipartita y que este último no puede ser extendido, añadiéndole vectores del primero, sin disminuir su distancia mínima. En la segunda sección se generalizan los resultados obtenidos en la primera considerando sistemas de ciclos del mismo tipo de gráficas, pero tomando los ciclos de longitud múltiplo de 4. En este caso se hace notar que los códigos obtenidos pertenecen a la familia de códigos definidos en el capítulo previo por lo que sus parámetros son fácilmente calculados. Se muestra además que algunos códigos binarios de Reed-Muller son recuperados como códigos asociados a Sistemas de Ciclos. La última sección contiene una descripción de códigos binarios asociados a una descomposición de una gráfica bipartita completa dirigida en circuitos de longitud par sin aristas en común. En este último caso los códigos que se obtienen son también un caso particular de los estudiados en el capítulo anterior.

5.1 Los 4-SC de $K_{m,n}$

En esta sección se presentan los códigos binarios asociados a un 4-sistema de ciclos de una gráfica bipartita completa no dirigida.

La descomposición de la gráfica bipartita completa no dirigida $K_{m,n}$, con conjunto de vértices $X = \{x_i\}_{i=0}^{m-1}$ y $Y = \{y_j\}_{j=0}^{n-1}$, en ciclos de una longitud par fija y sin aristas en común es descrita en [73]. En particular para descomponer esta gráfica en ciclos de longitud 4 es necesario y suficiente que m y n sean ambos pares, digamos $m = 2r$ y $n = 2s$. Para $0 \leq \mu \leq r-1$ y $0 \leq \lambda \leq s-1$ sean $g_\mu = \{x_{2\mu}, x_{2\mu+1}\}$ y $h_\lambda = \{y_{2\lambda}, y_{2\lambda+1}\}$. Definamos además los conjuntos

$$\begin{aligned} F &= \{g_\mu\}_{\mu=0}^{r-1} \cup \{h_{\lambda+1}\}_{\lambda=0}^{s-1} \\ F_0 &= \{x_{2\mu}\}_{\mu=0}^{r-1} \cup \{y_{2\lambda}\}_{\lambda=0}^{s-1} \end{aligned} \tag{5.1}$$

Entonces la descomposición de $K_{2r,2s}$ en 4-ciclos está dada por los rs ciclos:

$$\Gamma_{\mu,\lambda} = \{(a,c,b,d) \mid \{a,b\} = g_\mu, \{c,d\} = h_\lambda\}.$$

El código lineal binario asociado al 4-SC $(K_{2r,2s})$, como se describió en la sección 1.4, será denotado como $C_4(r,s)$. Los parámetros de este código serán calculados y una base formada por vectores de peso mínimo será mostrada en el siguiente resultado.

Proposición 68 *El código $C_4(r,s)$ es un $[2(r+s), r+s-1, 4]$ código lineal sobre $\mathbb{F}_2$. Además todas sus palabras codificadas tienen peso divisible por 4. Si $1 \leq \lambda_0 < r$ y $1 \leq \mu_0 < s$ son índices fijos entonces una base para este código es el conjunto $\mathcal{A}$ formado por los vectores de incidencia de los 4-ciclos $\Gamma_{\mu_0,\lambda}$ y Γ_{μ,λ_0}, donde $0 \leq \mu < r$ y $0 \leq \lambda < s$.*

Demostración Como los elementos del conjunto F definido en (5.1) son todos distintos, los vectores de incidencia en $\mathcal{A}$ son linealmente independientes. Además la relación

$$\mathbf{v}^{\Gamma_{\mu,\lambda}} = \mathbf{v}^{\Gamma_{\mu_0,\lambda}} + \mathbf{v}^{\Gamma_{\mu_0,\lambda_0}} + \mathbf{v}^{\Gamma_{\mu,\lambda_0}}$$

muestra que $\mathcal{A}$ is un conjunto de generadores para $\mathcal{C} = C_4(r,s)$. El código $\mathcal{C}$ es autoortogonal (i.e., $\mathcal{C} \subset \mathcal{C}^\perp$), y todos sus generadores tiene peso 4, así que el peso de cada una de las palabras codificadas es divisible por 4 (cf. [46], pág. 27). ■

Dados un entero positivo n y un subconjunto $U \subset \mathbb{F}_2^n$, como en el capítulo anterior $U \otimes 10$ denota la colección de vectores $(u_1, 0, u_2, 0, \cdots, u_n, 0)$, donde $(u_1, u_2, \cdots, u_n) \in U$. Recordemos además que todo vector binario $\mathbf{v}$ de longitud $2(r+s)$ puede ser visto como el vector de incidencia de una subgráfica de $K_{2r,2s}$ cuyo conjunto de vértices es el soporte de $\mathbf{v}$.

Enseguida se muestra la manera de extender el código $C_4(r,s)$ de la proposición 68 a un código con mayor dimensión y con idéntica longitud y distancia mínima, por lo que el código extendido conservará misma la capacidad de detectar y corregir errores que tiene $C_4(r,s)$.

Proposición 69 *El código $C_4(r,s)$ puede ser extendido a un código lineal sobre $\mathbb{F}_2$, $C_4(r,s)^*$, con parámetros $[2(r+s), r+s-1+k, 4]$, si existe un $[r+s, k, 4]$-código lineal binario $\mathcal{C}$. La manera de obtener tal código $C_4(r,s)^*$ es añadiéndo a $C_4(r,s)$ los vectores de una base de $\mathcal{C} \otimes 10$ como generadores adicionales.*

Demostración Sean $K_{r,s}$ una subgráfica bipartita completa de $K_{2r,2s}$ cuyo conjunto de vértices es F_0, definido por (5.1) y Γ a su vez una subgráfica $K_{r,s}$ tal que el vector de incidencia de Γ, $\mathbf{v}^\Gamma \in \mathbb{F}_2^{r+s}$, está en $\mathcal{C}$. Por lo tanto el vector $\mathbf{u}^\Gamma = \mathbf{v}^\Gamma \otimes 10$ será una palabra codificada en $C_4(r,s)^*$ y es el vector de incidencia de Γ vista ahora

como subgráfica de $K_{2r,2s}$. Supongamos que F es definido como en (5.1), y que F_0 es el conjunto de índices para las posiciones coordenadas de $\mathbb{F}_2^{r+s}$, el subespacio de $\mathbb{F}_2^{2(r+s)}$ en el que $\mathcal{C}$ se encuentra inmerso. Si $\{z_1, z_2\} \in F$ y z_1 está en el soporte de $\mathbf{v}^\Gamma$ entonces, para cualquier palabra codificada $\mathbf{c} \in C_4(r,s)$, exactamente uno de los vértices z_1 o z_2 se encuentra en el soporte de $\mathbf{c}+\mathbf{u}^\Gamma$. De ahí que $d\left(\mathbf{c}, \mathbf{u}^\Gamma\right) \geq ps\left(\mathbf{u}^\Gamma\right) \geq 4$.

Sean $\mathbf{v}_1, \ldots, \mathbf{v}_{r+s-1}$ una base de $C(r,s)$, $\mathbf{v}^{\Gamma_i}$, $1 \leq i \leq k$, una base de $\mathcal{C}$, para una subgráfica Γ_i de $K_{r,s}$ y $\mathbf{u}_i = \mathbf{v}^{\Gamma_i} \otimes 10$. Se verifica fácilmente que el conjunto $\left\{\mathbf{v}_1, \ldots, \mathbf{v}_{r+s-1}, \mathbf{v}^{\Gamma_1}, \ldots, \mathbf{v}^{\Gamma_k},\right\}$ es linealmente independiente, lo que prueba que la dimensión de $C_4(r,s)^*$ es como se menciona. ■

Sea n un entero positivo y sean $U_1, \ldots, U_t$ subconjuntos de $\mathbb{F}_2^n$. El $\mathbb{F}_2$-espacio vectorial generado por los conjuntos $U_i \subset \mathbb{F}_2^n$, $1 \leq i \leq t$, se denotará como $\langle U_1, \ldots, U_t \rangle$. Si cualquiera de los subconjuntos U_i tiene un único elemento, digamos $U_i = \{\mathbf{v}\}$, las llaves serán omitidas. A continuación se darán un par de ejemplos para ilustrar el resultado anterior.

Ejemplo 70 Se da la construcción explícita de un $[40, 33, 4]$ código lineal binario, la cual es dividida en tres pasos para simplificar su presentación. En cada uno de estos pasos un código con la mayor dimensión posible, dadas la longitud y distancia mínima, es obtenido de acuerdo a los resultados en [6].

Paso 1 $C_4(2,3)$ es un $[10,4,4]$-código lineal con una base formada por, digamos, los vectores $\mathbf{v}^{\{x_2,y_0,x_3,y_1\}}$ y $\mathbf{v}^{\{x_0,y_{2j},x_1,y_{2j+1}\}}$, $j = 1,2,3$. Sea $\mathbf{O}_1 = \{\mathbf{1}_4\mathbf{0}_1, \mathbf{0}_5\}$, entonces $\mathbf{C}_1 = \langle C_4(2,3), \mathbf{O}_1 \otimes 10\rangle$, el código lineal asociado al 4-$SC(K_{4,6})$, tiene parámetros $[10, 4+1, 4]$.

Paso 2 El $[20,9,4]$-código lineal $C_4(4,6)$ puede extenderse al $[20, 9+5, 4]$-código $\mathbf{C}_2$ al añadirle cinco vectores linealmente independientes de la forma $\mathbf{v} \otimes 10$, con $\mathbf{v} \in \mathbf{C}_1$. Este es el código asociado al 4-$SC(K_{8,12})$.

Paso 3 El código $C_4(8,12)$ tiene parámetros $[40, 19, 4]$. Entonces los parámetros de $\langle C_4(8,12), \mathbf{C}_2 \otimes 10\rangle$ resultan $[40, 19+14, 4]$, como se deseaba. Este último es el código asociado al 4-$SC(K_{16,24})$.

Insistimos nuevamente en que esta construcción puede ser explicada en términos de subgráficas de $K_{16,24}$, como ya se ha mencionado.

Ejemplo 71 Sea $RM(\rho, m)$ el código binario de Reed-Muller de orden ρ $(m \geq 2)$ y obsérvese que, por la proposición 68, $C_4(2^{m-1}, 2^{m-1})$ tiene parámetros $[2^m, 2^{m-1}-1, 4]$. De acuerdo a la proposición 69 este código puede extenderse a un $[2^m, 2^m - m - 1, 4]$-código lineal binario, el código $RM(m-2, m)$, añadiéndole los vectores del código $\mathcal{C} = RM(m-3, m-1) \otimes 10$. Al suprimir una posición coordenada fija a todas las palabras codificadas del código $RM(m-2, m)$ se obtiene un $[2^m - 1, 2^m - m - 1, 3]$ código, el cual es el código binario de Hamming $\mathcal{H}_m$.

Sea K_n la gráfica completa no dirigida en n vértices. El número de aristas de K_n es $\binom{n}{2} = \frac{n(n-1)}{2}$, por lo que para descomponer K_n en ciclos de longitud $m \geq 3$ sin

aristas en común es necesario que $\frac{n(n-1)}{2m}$ sea un entero. Tenemos así la siguiente lista de condiciones necesarias para la existencia de un m-$SC(K_n)$ (cf. [43]):

1. $n \geq m$, si $n > 1$,
2. n es impar, y
3. $2m \mid n(n-1)$.

De la condición 2 se sigue que un 4-$SC(K_n)$ existe sólo si $8|(n-1)$.

Ejemplo 72 Sean $\mathbb{Z}_9$ el anillo de enteros mólulo 9 y $\Upsilon = \{(i, 4+i, 5+i, 3+i) : i \in \mathbb{Z}_9\}$ un conjunto de ciclos de K_9 (suponemos que Z_9 es el conjunto de vértices de la gráfica). Note que todo par $\{a, b\} \subset \mathbb{Z}_9$, $a \neq b$, es la arista de exactamente un ciclo en Υ. Por lo tanto se tiene una partición de las aristas de la gráfica K_9 en 4-ciclos, es decir (V, Υ) es un 4-$SC(K_9)$ de orden 9.

La construcción $n+8$. Enseguida se recuerda el método recursivo de construcción de un 4-$SC(K_{n+8})$ como se describe en [43], pag. 331. Supóngase que $(\{\infty\} \cup X, \Upsilon_1)$ es un 4-$SC(K_n)$ y que $(\{\infty\} \cup Y, \Upsilon_2)$ es un 4-$SC(K_9)$. Al elegir particiones de los conjuntos X y Y en subconjuntos de cardinalidad 2, se obtienen los conjuntos $H = \{h_1, h_2, \ldots, h_{(n-1)/2}\}$ y $G = \{g_1, g_2, g_3, g_4\}$ respectivamente. Sea $F = H \cup G$ (notemos que F es el conjunto definido por la relación (5.1)). Y sea $\Upsilon_3 = \{(a, c, b, d) : \{a, b\} \in H, \{c, d\} \in G\}$. Como el número de ciclos en el 4-$SC(K_{n+8})$ es $\binom{n+8}{2}/4$, la cardinalidad de $\Upsilon_1 \cup \Upsilon_2 \cup \Upsilon_3$, se sigue que $(\{\infty\} \cup X \cup Y, \Upsilon_1 \cup \Upsilon_2 \cup \Upsilon_3)$ es un 4-SC de orden $n+8$ de la gráfica K_{n+8}. La estructura de incidencia $\mathcal{G} = (X \cup Y, \Upsilon_3, \mathcal{I})$. $n > 9$, donde $(z, \Gamma) \in \mathcal{I}$ si z es un vértice del ciclo Γ, está asociada a una descomposición de la gráfica bipartita completa no dirigida, $K_{n-1,8}$ digamos, con conjuntos de vértices X y Y, en ciclos de longitud 4 sin aristas en común (cf. [43]).

Note que los 4-SC son construidos con copias de 4-SC of order 9 de K_9. Por ejemplo si tomamos dos copias de un 4-$SC(K_9)$ entonces obtendremos un 4-$SC(K_{17})$. Ahora podemos construir un 4-SC de orden $\equiv 1 \pmod 8$ y tenemos el siguiente resultado (cf. [43]):

Teorema 73 *Un 4-$SC(K_n)$ de orden n existe si y sólo si $n \equiv 1 \pmod 8$.*

Ahora nos preguntamos ¿qué podemos decir acerca del código binario asociado al 4-$SC(K_{n+8})$, $n \equiv 1 \pmod 8$? Sea Γ un ciclo en $\Upsilon_2 \cup \Upsilon_1$, los conjuntos de ciclos del 4-$SC(K_n)$ descritos en la construcción $n+8$, y sea $C(4a, 4)^*$ el código descrito en la proposicón 69, donde $8a = n-1$. Si el punto ∞ es un vértice de Γ es fácil verificar que el soporte de toda palabra codificada de $C_4(4a, 4)^*$ no debe tener más de 2 puntos en común con el vector de incidencia de Γ. De ahí que no podamos añadir ninguna palabra codificada a $C_4(4a, 4)^*$ sin disminuir su distancia mínima. Sin embargo podemos decir que el código binario asociado al 4-$SC(K_{n+8})$ contiene un subcódigo que puede ser acortado al código $C_4(4a, 4)$ suprimiendo la posición coordenada correspondiente a ∞.

Como se mostró en el ejemplo 70 si $8a = 2^m - 8$, $m > 3$, el código $C_4(4a, 4)$, que está asociado a la gráfica bipartita $K_{2^m-8,8}$, se extiende al código $C_4(4a, 4)^*$, el cual resulta ser el código binario de Hamming $\mathcal{H}_m$ al suprimirle cualquier posición coordenada. Por el párrafo anterior sabemos que los códigos binarios de Hamming forman un subconjunto de los códigos asociado a gráficas completas K_{2^m+1}. En la literatura existen dos resultados similares a esta observación. El primero es el resultado principal en [35] (teorema 1), el cual afirma que el código binario asociado a un 3-sistema de ciclos de la gráfica completa no dirigida, es decir, un sistema triple de Steiner, siempre contiene un subcódigo que puede ser acortado al código binario de Hamming suprimiéndole las posiciones coordenadas donde todas las palabras codificadas tienen entrada cero. El segundo es el ejemplo 5.2 en [31], que muestra que los códigos binarios de Hamming pueden obtenerse suprimiendo una posición coordenada fija pero arbitraria a todas las palabras codificadas del código gráfico asociado a la gráfica $K_{m,n}$, donde $m = n = 2^a$ o $m = 2^{a+1}$ y $n = 2^a$ (a es un entero positivo).

Ya que la matriz de incidencia del 4-$SC(K_9)$ en una matriz circulante B, podemos considerar al código binario doblemente circulante (ver sección 2.3) con matriz generadora $G = (I \mid B)$, donde I es es la matriz identidad. En este caso obtenemos un $[18, 9, 5]$ código lineal binario el cual, como todos los códigos doblemente circulantes, es equivalente a su propio código dual.

5.2 Códigos asociados a un $4e$-$SC(K_{m,n})$

Sean a, b, r, s enteros positivos, $r \geq a$, $s \geq b$ y sea $K_{2br,2as}$ la gráfica bipartita completa no dirigida con conjunto de vértices $X = \{x_0, \ldots, x_{2br-1}\}$ y $Y = \{y_0, \ldots, y_{2as-1}\}$. Dominique Sotteau [73] da la descomposición de esta gráfica en un $4ab$-Sistema de Ciclos, probando que consta de rs ciclos $C_{\lambda,\mu}$, con $0 \leq \lambda \leq s-1$ y $0 \leq \mu \leq r-1$, los cuales están dados como se muestra a continuación:

$$C_{\lambda,\mu} = \left(\cdots \left(\cdots x_{b(2\mu+i)+j} \; y_{2a(\lambda+j)+i} \cdots \right)_{0 \leq i \leq 2a-1} \cdots \right)_{0 \leq j \leq b-1}$$

donde los subíndices de x son reducidos módulo $2br$ mientras que los de y lo son módulo $2as$.

El vector de incidencia del ciclo $C_{\lambda,\mu}$ es $\mathbf{v}^{C_{\lambda,\mu}} = \left| \mathbf{v}_X^{C_{\lambda,\mu}} \middle| \mathbf{v}_Y^{C_{\lambda,\mu}} \right|$, donde $\mathbf{v}_X^{C_{\lambda,\mu}} = \left(\chi_{C_{\lambda,\mu}}(x_i) \right)_{i=0}^{2br-1}$ y $\mathbf{v}_Y^{C_{\lambda,\mu}} = \left(\chi_{C_{\lambda,\mu}}(y_j) \right)_{j=0}^{2as-1}$.

Las siguientes relaciones, para $0 \leq i \leq 2a-1$ y $0 \leq j \leq b-1$ se verifican fácilmente:

(a1) $2b\mu \leq b(2\mu + i) + j \leq 2b\mu + (2ab - 1)$

(a2) $2a\lambda \leq 2a(\lambda + j)\lambda + i \leq 2a\lambda + (2ab - 1)$.

Como en un ciclo dado $C_{\lambda,\mu}$ los índices λ y μ están fijos, por las desigualdades **(a1)** y **(a2)** concluimos que $\operatorname{sop}\left(\mathbf{v}_X^{C_{\lambda,\mu}}\right) = \cup_{i=\mu}^{\mu+a} S_0^{(b)}(t)$ y $\operatorname{sop}\left(\mathbf{v}_Y^{C_{\lambda,\mu}}\right) = \cup_{j=\lambda}^{\lambda+b} S_0^{(b,a)}(e)$,

donde los conjuntos $S_0^{(b)}(t)$ y $S_0^{(b,a)}(e)$ están definidos por la ecuación (4.7). Por lo tanto los vectores $\mathbf{v}_X^{C_{\lambda,\mu}}$ y $\mathbf{v}_Y^{C_{\lambda,\mu}}$ son los generadores de los códigos $C_a^{(b)}(r)$ y $C_b^{(a)}(s)$, respectivamente. La matriz binaria con renglones $\mathbf{v}_X^{C_{\lambda,\mu}}$ tiene renglones repetidos, los cuales corresponden a parejas (μ,λ) para un valor fijo de μ. Después de suprimir los renglones repetidos obtenemos la matriz $A\otimes\mathbf{1}_{2b}$, donde A es una matriz circulante con primer renglón $\mathbf{1}_a\mathbf{0}_{r-a}$, por lo que el código generado por sus renglones es el código $C_a(r)$.

Por otro lado toda palabra codificada $\mathbf{c}$ del código asociado a $4ab$-SC $(K_{2br,2as})$ puede ser escrita como $\mathbf{v}\otimes|\mathbf{1}_{2b}|_r\,\mathbf{1}_{2a}|_s$, donde $\mathbf{v}=|\mathbf{v}_1|\,\mathbf{v}_2|$ con $\mathbf{v}_1\in C_a(r)$ y $\mathbf{v}_2\in C_b(s)$. Es decir, tal código es $C_{a,b}^{(b,a)}(r,s)$,el código definido en la sección 4.3. Se encontró que si los polinomios característicos de $C_a(r)$ y $C_b(s)$ son $m_1(x)$ (de grado L_a) y $m_2(x)$ (de grado L_b) respectivamente, entonces los parámetros de tal códigos son $[2(br+as),k,4\min\{a,b\}]$, donde $k=L_a+L_b-1$ si $ps(m_1(x))$ y $ps(m_1(x))$ son pares, y $k=L_a+L_b$ en otro caso. En particular se sigue que el código $C_4(r,s)$ definido en la sección 5.1 es $C_{1,1}^{(1,1)}(r,s)$.

De la prueba de la proposición 56, para cualesquiera índices fijos λ_0 and μ_0, una base para el código $C_{a,b}^{(b,a)}(r,s)$ es el conjunto

$$\left\{\mathbf{v}^{C_{\lambda,\mu_0}}\right\}_{\lambda=0}^{L_a-1}\cup\left\{\mathbf{v}^{C_{\lambda_0,\mu}}\right\}_{\mu=0}^{L_b-1},$$

si $ps(m_1(x))$ y $ps(m_2(x))$ son ambos pares, y

$$\left\{|\mathbf{v}_X^{C_{\lambda,\mu_0}}|\mathbf{0}_{2as}|\right\}_{\lambda=0}^{L_a-1}\cup\left\{|\mathbf{0}_{2br}|\mathbf{v}_Y^{C_{\lambda_0,\mu}}|\right\}_{\mu=0}^{L_b-1}$$

en otro caso.

Se ha mostrado que el código asociado a $4ab$-SC $(K_{2br,2as})$ es $C_{a,b}^{(b,a)}(r,s)$, el código definido por la relación 4.6. Podemos extender este código como se hizo en la sección 4.3, primero al código $C_{a,b}^{(b,a)}(r,s)^*$, definido inmediatamente despúes de la demostración a la proposición 56, para enseguida extenderlo tal y como se hizo en el teorema 60.

Como en la sección 4.3 para todo entero $e>0$ sea $P(e)$ el mayor entero positivo t tal que $2^{t-1}\mid e$, y para cada entero $1\le i\le P(e)$ definimos $\mathbf{w}_i^{(e)}=\mathbf{1}_{e/2^{i-1}}\mathbf{0}_{e/2^{i-1}}$. Por último la dimensión de $C_{a,b}^{(b,a)}(r,s)^*$ es denotada como k_0. Sin pérdida de generalidad podemos suponer que $P(b)\ge P(a)$:

Corolario 74 *Sea* $t=P(b)$. *El código* $C_{b,a}^{(b,a)}(r,s)$ *puede extenderse a un*

$$\left[2(br+as),\sum_{i=0}^{t}k_i,4\min\{a,b\}\right]$$

código lineal $\mathbf{C}^*$, *siempre que exista un* $[2^{i-1}(r+s),k_i,2^{i+1}]$ *código lineal* $\mathbf{O}_i$, *para todo entero positivo* $i\le\min P(a)$, *y un* $[2^{j-1}r,k_j,\lceil a2^{j+1}/b\rceil]$ *código lineal* $\mathbf{O}_j$ *para* $P(a)<j\le t$.

Tal código $\mathbf{C}^*$ *puede obtenerse agregando a* $C_{b,a}^{(b,a)}(r,s)^\circ$ *los vectores de incidencia de cualesquiera* k_i *subgráficas de* $K_{2ar,2bs}$ *con vértices en el soporte de los elementos de una base para* $\mathbf{O}_i \otimes \left|\mathbf{w}_i^{(b)}\right|_{r2^{i-1}} \left|\mathbf{w}_i^{(a)}\right|_{s2^{i-1}}$, $1 \leq i \leq P(a)$, *y una base para* $\left(\mathbf{O}_j \otimes \mathbf{w}_j^{(b)}\right) \oplus \{\mathbf{0}_{2as}\}$, $P(a) < j \leq t$. *como generadores adicionales.*

Ejemplo 75 Elegiendo los valores $a = b = \eta = \theta = 2$ and $r = s = 4$, un código binario asociado al 16-$SC(K_{16,16})$ será construido como se indica en el corolario 74. Como $C_{2,2}(4,4)$ es un $[8,5,2]$-código binario, $C_{2,2}^{(2,2)}(4,4)^\circ$ tiene parámetros $[32,7,8]$. Si $\mathbf{O}_1 = RM(1,3)$ y $\mathbf{O}_2 = RM(1,4)$, entonces $C_{2,2}^{(2,2)}(4,4)$ puede extenderse a un código de parámetros $[32,16,8]$, el código de Reed-Muller $RM(2,5)$.

Ejemplo 76 El código $C_{4,4}(8,8)$ tiene parámetros $[16,9,2]$, y puede extenderse al $[16,15,2]$-código $C_{4,4}(8,8)^\circ$, por lo que $C_{4,4}^{(4,4)}(8,8)^\circ$ tendrá parámetros $[128,15,16]$. Eligiendo $\mathbf{O}_1 = RM(2,4)$, $\mathbf{O}_2 = RM(2,5)$ y $\mathbf{O}_3 = RM(2,6)$, por el corolario 74, concluimos que un código binario asociado al 64-$SC(K_{64,64})$ es el código $RM(3,7)$.

5.3 Códigos asociados a un $2e$-$SC\left(K_{m,n}^*\right)$

Supóngase que a, b, r, s son enteros positivos, $r > b$ y $s > a$, y supóngase además que $K_{ar,bs}^*$ es la gráfica completa dirigida con conjunto de véritices $X = \{x_0, \ldots, x_{2ar-1}\}$ y $Y = \{y_0, \ldots, y_{2bs-1}\}$. Una descomposición de esta gráfica en circuitos de longitud $2ab$ sin aristas en común existe y tiene rs ciclos $C_{\lambda,\mu}$, con $0 \leq \lambda \leq s-1$ y $0 \leq \mu \leq r-1$, dados por:

$$C_{\lambda,\mu} = \left(\cdots\left(\cdots x_{a(\mu+i)+j}\ y_{b(\lambda+j)+i}\cdots\right)_{0\leq i\leq b-1}\cdots\right)_{0\leq j\leq a-1}$$

donde como antes los subíndices de x son reducidos módulo ar y los de y lo son módulo bs (cf. [73]).

No es dificil verificar que si a o b es un número impar ningún código con buenos parámetros puede obtenerse. Así supongamos que a y b son ambos números pares (que por abuso de notación son representados como $2a$ y $2b$ respectivamente).

Un argumento similar al descrito en el caso de la gráfica completa no dirigida muestra que el códigos asociado a la gráfica $K_{2ar,2bs}^*$ es $C_{2b,2a}^{(a,b)}(r,s)$ y sus parámetros están dados por el teorema 60.

Ejemplo 77 Una amplia familia de códigos es obtenida asociada a gráficas completas dirigidas. Por ejemplo el código asociado a la gráfica $K_{8,8}^*$ cuando es descompuesta en circuitos de longitud 8 sin aristas en común es el código binario de Reed-Muller $RM(2,4)$. Si considereamos la gráfica $K_{8,6}^*$ se obtiene un $[14,9,4]$ código binario. Ambos códigos tienen parámetros óptimos (cf. [6]).

Otro tipo de trabajos sobre códigos asociados a gráficas pueden ser encontrados en: [18, 32, 58, 64, 76]. El problema inverso, es decir gráficas asociadas a códigos, es analizado en [7].

CAPÍTULO 6

RESULTADOS VARIOS

En este capítulo se describen resultados adicionales que se han obtenido paralelamente al desarrollo principal de esta tesis. El primero de ellos indica una manera recursiva de construir una matriz generadora para los códigos binarios de Reed-Muller (cf. [19]). En la segunda parte se determina una base de vectores de peso mínimo para la familia de códigos ya mencionada, los cuales son los vectores de incidencia de variedades afines, todas con la misma dimesión (cf. [23]). En la tercera parte se determina el número de soluciones de una ecuación lineal en m indeterminadas sobre $\mathbb{Z}_n$, el anillo de los enteros módulo n. Se prueba además una relación tipo Parseval para una familia de funciones definidas sobre $\mathbb{Z}_n$, que enseguida es utilizada para caracterizar una clase de funciones muy especial, una familia de las llamadas funciones bent generalizadas. Éste último resultado aparece publicado en [21].

6.1 Códigos binarios de Reed-Muller y esferas de Hamming

En 1980 K. P. Bogart (cf. [4]) describió un método para construir códigos a partir de conjuntos parcialmente ordenados $(P, \leq)$, (copos). Además probó que cuando se toma a la familia de subconjuntos de un conjunto finito, ordenado por inclusión, los códigos que se obtienen son los códigos binarios de Reed-Muller. En la siguiente sección se hace uso de tal resultado para dar una construcción recursiva de una matriz generadora para los códigos binarios de Reed-Muller.

6.1.1 Códigos asociados a copos

Para cada elemento x de un copo $(P, \leq)$, el *ideal principal* de P generado por x, es el conjunto $\langle x \rangle = \{y \in P : y \leq x\}$.

De aquí en adelante supondremos que $P = \{x_1, \ldots, x_n\}$ es un copo finito. Si $A \subseteq P$, χ_A denotará a la función característica de A. Con esta notación, a cada $x \in P$ le asociamos su vector característico $\mathbf{v}_x = \left(\chi_{\langle x_1 \rangle}(x), \ldots, \chi_{\langle x_n \rangle}(x)\right)$. Estos vectores forman una base de K^n, donde K es un campo finito.

Para cada subconjunto S de P se define el *código de incidencia* de P, denotado $RM(P, S)$, como el espacio vectorial de K^n generado por los vectores de incidencia $\mathbf{v}_s$, para todo $s \in S$. Obviamente $RM(P, S)$ es un código lineal de longitud $|P|$ y dimensión $|S|$ sobre el campo K.

Supongamos que M es un conjunto con m elementos y que ρ es un entero positivo, $\rho \leq m$. Tomemos a P como el conjunto potencia de M, ordenado por inclusión, y a S como la colección de subconjuntos con a lo más ρ elementos. El espacio vectorial K^n es una álgebra bajo la multiplicación componente a componente, donde se verifica $\mathbf{v}_x * \mathbf{v}_y = \mathbf{v}_{\{x,y\}}$, para $x, y \in M$. Entonces, el código de Reed-Muller $RM(\rho, m)$ es el código formado por los polinomios de grado a lo más ρ en los vectores $\mathbf{v}_x$, con $x \in M$ (se define $\mathbf{v}_x^0 = \mathbf{1}$).

6.1.2 La construcción

Para cualesquiera dos arreglos (disposiciones) binarias rectangulares A, B, con el mismo número de renglones, denotaremos por $|A|\ B|$ al arreglo cuyo t-ésimo renglón es el t-ésimo renglón de B escrito enseguida del correspondiente renglón de A; esto es la concatenación de A y B.

Si n y r, $0 \leq r \leq n$, son dos enteros, también denotaremos al coeficiente binomial $\binom{n}{r}$ como $C(n,r)$.

El conjunto de vectores binarios $E_r^n = \{\mathbf{x} \in \mathbb{F}_2^n : ps(\mathbf{x}) = r\}$ se conoce como la *esfera de Hamming de radio* r, sobre $\mathbb{F}_2^n$. Denotaremos por S_r^n, al arreglo de $C(n,r) \times n$ cuyos renglones son los vectores en E_r^n, los cuales aparecen ordenados por el orden lexicográfico de sus soportes. $(S_r^n)^t$ representará al arreglo transpuesto de S_r^n.

Ejemplo 78 A continuación se muestran los arreglos S_2^4 y $(S_2^4)^t$.

$$\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array} \qquad \begin{array}{cccccc} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Sean $\alpha = C(n,r)$ y $A = \{1, \ldots, n\}$. Supóngase que $\mathbf{u}_1, \ldots, \mathbf{u}_n$ son los renglones de $(S_r^n)^t$ y que $\mathbb{P}_i(A)$ es la familia de los subconjuntos de A con cardinalidad i, ordenados lexicográficamente. Ordenamos el conjunto

$$Q = \left\{ \mathbf{y} \in \mathbb{F}_2^\alpha : \mathbf{x} = \prod_{j \in B} \mathbf{u}_j,\ B \in \mathbb{P}_i(A) \right\}$$

definiendo

$$\left(\prod_{j \in B_1} \mathbf{u}_j \right) \leq \left(\prod_{j \in B_2} \mathbf{u}_j \right) \qquad \text{si } B_1 \leq B_2, \tag{6.1}$$

donde $\prod$ denota el producto componente a componente $(*)$ antes definido.

Definición 79 *El* ***cero producto*** *de* S_r^n *se define como*

$$T_0(S_r^n) = T_0(n,r) = S_\alpha^\alpha,\ \alpha = C(n,r).$$

Para cada entero positivo $i \leq n$, *el* i-***ésimo producto*** *de* S_r^n, *denotado como* $T_i(S_r^n) = T_i(n,r)$, *es el arreglo de* $C(n,i) \times C(n,r)$ *cuyos renglones son los vectores en* Q *los cuales aparecen en el orden (6.1).*

Ejemplo 80 Calculemos el segundo producto de S_2^4, $T_2(4,2)$.

$$\begin{aligned}
\mathbf{u}_1 * \mathbf{u}_2 &= 100000\\
\mathbf{u}_1 * \mathbf{u}_3 &= 010000\\
\mathbf{u}_1 * \mathbf{u}_4 &= 001000\\
\mathbf{u}_2 * \mathbf{u}_3 &= 000100\\
\mathbf{u}_2 * \mathbf{u}_4 &= 000010\\
\mathbf{u}_3 * \mathbf{u}_4 &= 000001
\end{aligned}$$

Este arreglo es S_1^6, esto es, $T_2(4,2) = S_1^6$.

Sea $O(l,m)$ el arreglo de $l \times m$ cuyas entradas son todas cero. Definimos también el i-ésimo producto de $\{a\} \times S_r^n$, $a \in \mathbb{F}_2$, $1 \leq i \leq n+1$, tomando $\mathbf{u}_0 = a\mathbf{1} \in \mathbb{F}_2^\alpha$, $\alpha = C(n,r)$, y definiendo el i-ésimo producto T_i de manera análoga a la anterior, donde $\mathbf{1}$ es el vector de logitud α con todas sus entradas igual a la unidad.

Ahora se tiene la siguiente

Proposición 81 *Para cualesquiera enteros* n, r *con* $0 \leq r \leq n$ *y* $n > 0$ *se cumple*

R0) $T_1(n,r) = (S_r^n)^t$

R1)

$$\begin{aligned}
T_i(n,1) &= O(C(n,i), n), && 2 \leq i \leq n.\\
T_i(n,n) &= T_1(C(n,i), C(n,i)), && 1 \leq i \leq n.\\
T_n(n,r) &= O(1, C(n,r)), && 1 \leq r < n.
\end{aligned}$$

R2) *si* $r > 1$, *entonces*

$$T_i(n,r) = \begin{pmatrix} T_{i-1}(n-1,r-1) & O\left(\binom{n-1}{i-1}, \binom{n-1}{r}\right)\\ T_i(n-1,r-1) & T_i(n-1,r)\end{pmatrix}$$

Demostración Las relaciones en (R0) y (R1) son inmediatas de las definiciones. (R2) se sigue de las igualdades $T_i(\{1\} \times S_r^n) = \begin{pmatrix} T_{i-1}(n,r)\\ T_i(n,r)\end{pmatrix}$,

$$\begin{aligned}
T_i(\{0\} \times S_r^n) &= \begin{pmatrix} O(C(n,i-1), C(n,r))\\ T_i(n,r)\end{pmatrix},\\
T_i(n,r) &= \begin{pmatrix} T_i(\{1\} \times S_{r-1}^{n-1}) & T_i(\{0\} \times S_r^{n-1})\end{pmatrix},
\end{aligned}$$

como puede fácilmente observarse. ■

Ejemplo 82 Si aplicamos la proposición 81 para calcular el segundo producto $T_2(3,2)$, obtenemos: $T_2(3,2) = \begin{pmatrix} S_1^2 & O(2,1) \\ O(1,3) & S_1^1 \end{pmatrix}$. Por lo tanto, $T_2(3,2) = S_1^3$.

Proposición 83 *Para cualesquiera enteros n, i, r con $r < i \leq n$, se tiene*

$$T_i(n,r) = O(C(n,i), C(n,r)), \quad y \quad T_i(n,i) = S_1^{C(n,i)}$$

Demostración Basta aplicar inducción matemática. ■

Teorema 84 *Una matriz generadora para el código binario de Reed-Muller $RM(\rho, m)$, está dada por el arreglo $(T_i(m,j))$ donde $0 \leq i \leq \rho$, $0 \leq j \leq m$.*

Demostración Sea $M = \{z_1, \ldots, z_m\}$. Supóngase que el código de Reed-Muller, $RM(\rho, m)$, es construido como se describe al final de la sección 6.1.1. La función biyectiva

$$\chi : P \longrightarrow \mathbb{F}_2^m, \quad A \mapsto (\chi_A(z_1), \ldots, \chi_A(z_m)), \quad z_j \in M, \ 1 \leq j \leq m,$$

nos permite tomar a P como $\mathbb{F}_2^m$ con el orden por contensión de sus soportes (i.e. $x, y \in \mathbb{F}_2^m$, $x \leq y \iff x * y = x$). Supóngase también que los vectores en $\mathbb{F}_2^m$ han sido agrupados por su peso de Hamming, y que son numerados de acuerdo al orden lexicográfico de sus soportes. De aquí la conclusión es clara. ■

Ejemplo 85 Si ρ es un entero, $0 \leq \rho \leq 4$, una matriz generadora para el código de Reed-Muller $RM(\rho, 4)$, puede obtenerse del arreglo

$$G = \begin{pmatrix} S_1^1 & S_4^4 & S_6^6 & S_4^4 & S_1^1 \\ & S_1^{4t} & S_2^{4t} & S_3^{4t} & S_4^{4t} \\ & & S_1^6 & B_{2,3} & S_6^6 \\ & & & S_1^4 & S_4^{4t} \\ & & & & S_1^1 \end{pmatrix}$$

donde las entradas vacías son arreglos con todas sus entradas cero y donde

$$B_{2,3} = \begin{pmatrix} S_2^{3t} & O(3,1) \\ S_1^3 & S_3^{3t} \end{pmatrix}.$$

Este último arreglo es la esfera de Hamming de radio 2 sobre $\mathbb{F}_2^4$, con los vectores ordenados por el orden dual al lexicográfico inverso. Para obtener una matriz generadora de, digamos, el código $RM(2,4)$ basta con desarrollar los arreglos en los primeros tres renglones de G.

Por ejemplo una matriz generadora para el código $RM\,(2,4)$ es

$$G_{24} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ & & & & & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ & & & & & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ & & & & & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ & & & & & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ & & & & & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ & & & & & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

donde los espacios vacíos denotan entradas cero.

Esta manera de construir una matriz generadora G para un código binario de Reed-Muller nos evita el evaluar funciones booleanas en todos los puntos de un espacio afín. Además de esta forma es posible verificar de manera inmediata si se ha cometido algún error al escribir la matriz G.

6.2 Una base para los códigos binarios de Reed-Muller

Un hecho conocido en la Teoría de Códigos es que los vectores de incidencia de las variedades afines de dimensión $(m-\rho)$, en el espacio $\mathbb{F}_2^m$, generan al código de Reed-Muller $RM\,(\rho,m)$ (cf. [1]). Sin embargo no fue sino hasta 1998 que J.D. Key y S. Gao [15], lograron determinar una base para tales códigos en los términos geométricos que indica el enunciado anterior. En otras palabras, estos autores determinan una manera de elegir un conjunto de variedades afines de la misma dimensión, $m-\rho$, de tal forma que sus vectores de incidencia forman una base para el código $RM\,(\rho,m)$. Utilizando uno de los resultados anteriores (lema 33) se describe otra base para estos códigos con las mismas características que aquella de Key y Gao. La importancia de este resultado es que nos permite estudiar de manera más sencilla las distintas formas conocidas que existen para describir los códigos binarios de Reed-Muller, además de que la base encontrada está constituida por vectores de peso mínimo lo cual simplifica el proceso de codificación y decodificación.

Denotaremos como $\left\{M_{k,j} : 1 \leq j \leq \binom{m}{k}\right\}$ a la familia de subconjuntos de $[m] := \{1,2,\ldots,m\}$ de cardinalidad k, para cada entero no negativo $k \leq m$.

Teorema 86 *Sean m y ρ dos enteros con $0 \leq \rho \leq m$. Para cada par de enteros k y j, $1 \leq k \leq \rho$, $1 \leq j \leq \binom{m}{k}$, elíjanse $\rho - k$ enteros distintos $a\,(k,j,t)$ en $[m] - M_{k,j}$, donde $k+1 \leq t \leq \rho$. Entonces los vectores de incidencia de las variedades afines con*

función característica

$$\left(\prod_{i\in M_{k,j}} x_i\right)\prod_{t=k+1}^{\rho}\left(1+x_{a_{(k,j,t)}}\right)$$

forman una base para el código binario $RM(\rho,m)$, *(donde* $\prod_{i\in M_{0,j}} x_i$ *y* $\prod_{t=\rho+1}^{\rho}\left(1+x_{a_{(k,j,t)}}\right)$ *se definen ambos como 1 para cualquier* j*).*

Demostración Es suficiente con probar que cada uno de los monomios $\prod_{i\in M_{k,j}} x_i$ puede expresarse como una $\mathbb{F}_2$-combinación lineal de los polinomios descritos en el enunciado del teorema. Supongamos que esto es válido para todos los enteros positivos $k > k_0$, para algún $k_0 < r$ y cualquier j. Sean $A = \mathbb{F}_2$ y $R = \mathbb{F}_2[x_1,\ldots,x_m]/(x_i^2+x_i)$, el anillo de polinomios en las indeterminadas $x_1, x_2, \ldots, x_m$ con coeficientes en $\mathbb{F}_2$, reducidos módulo $x_i^2+x_i$, $1 \le i \le m$. Definamos además las funciones $f_t : A \longrightarrow R$ como $f_t(0) = 1 + x_{a_{(k,j,t)}}$ y $f_t(1) = x_{a_{(k,j,t)}}$, donde $k+1 \le t \le \rho$. Haciendo $\mathbf{v} = (v_{k+1},\ldots,v_\rho) \in A^{\rho-k}$, por el lema 33 podemos escribir

$$\begin{aligned}\prod_{i\in M_{k_0,j}} x_i &= \prod_{i\in M_{k_0,j}} x_i \prod_{t=k_0+1}^{\rho}\left(1+x_{a_{(k_0,j,t)}}+x_{a_{(k_0,j,t)}}\right)\\ &= \prod_{i\in M_{k_0,j}} x_i \sum_{\mathbf{v}\in A^{\rho-k}}\prod_{i=k_0+1}^{\rho} f_i(v_i).\end{aligned}$$

El último de los miembros en la igualdad anterior se descompone como

$$\left(\prod_{i\in M_{k_0,j}} x_i\right)h(\mathbf{X}) + \left(\prod_{i\in M_{k_0,j}} x_i\right)\prod_{t=k_0+1}^{\rho}\left(1+x_{a_{(k_0,j,t)}}\right),$$

donde $h(\mathbf{X})$ es un polinomio en $x_{a_{j,k,t}}$ que satisface $F(\mathbf{0}) = 0$. El segundo de los sumandos forma parte de la base propuesta y se ha supuesto que el primero es expresable como combinación lineal de esta. Esto pueba el resultado. ■

Ejemplo 87 Una base para el $[16,15,2]$ código $RM(3,4)$ está constituida, además de los monomios $x_ix_jx_k$ con $1 \le i < j < k \le 4$, por los siguiente polinomios.

$$\begin{array}{ll} x_1x_2(1+x_3) & x_1(1+x_2)(1+x_4)\\ x_1x_3(1+x_4) & x_2(1+x_3)(1+x_4)\\ x_1x_4(1+x_2) & x_3(1+x_1)(1+x_2)\\ x_2x_3(1+x_4) & x_4(1+x_2)(1+x_3)\\ x_2x_4(1+x_1) & (1+x_1)(1+x_2)(1+x_3)\\ x_3x_4(1+x_1) & \end{array}$$

Así por ejemplo

$$\begin{aligned} x_i x_3 &= x_i x_3 (1 + x_4 + x_4) = x_i x_3 (1 + x_4) + x_i x_3 x_4, \ i = 1, 2 \\ x_3 &= x_3 (1 + x_1 + x_1)(1 + x_2 + x_2) \\ &= x_3 (1 + x_1)(1 + x_2) + x_1 x_3 + x_2 x_3 + x_1 x_2 x_3 \end{aligned}$$

Donde por ejemplo $x_2 x_3 (1 + x_4)$ corresponde a la variedad afín consistente de los vectores $\mathbf{x} \in \mathbb{F}_2^4$ tales que $x_2 x_3 (1 + x_4) = 1$, es decir el conjunto de puntos en $\mathbb{F}_2^4$ que satisface las ecuaciones lineales $x_2 = 1$, $x_3 = 1$ y $x_4 = 0$.

6.3 Una relación tipo Parseval sobre $\mathbb{Z}_n$

Las funciones "*bent*" se han definido (cf. [68]) como aquellas funciones booleanas binarias ($f : \mathbb{Z}_2^m \to \mathbb{Z}_2$, m entero par) cuya distancia de Hamming al código binario de Reed-Muller de primer orden es máxima. Equivalentemente podemos decir que f es bent si la transformada discreta de Fourier de la función real $F_f(\mathbf{x}) = (-1)^{f(\mathbf{x})}$, esto es, $\widehat{F_f}(\mathbf{s}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{f(\mathbf{u}) + \mathbf{s}^t \mathbf{u}}$, satisface $\left| \widehat{F}_f \right| = 2^{m/2}$. El concepto de funciones tipo bent ha tenido importandes aplicaciones en la teoría algebraica de códigos, en la criptografía y en el estudio de sucesiones, entre otras. Esto ha conducido a la generalización del concepto a funciones definidas no ya sólo sobre el campo binario sino sobre un anillo $\mathbb{Z}_n$ de los enteros módulo n, trabajo que aparece reportado en [39].

En esta sección se dan condiciones necesarias y suficientes para que una ecuación lineal sobre el anillo $\mathbb{Z}_n$ tenga solución, y se determina este número para todo valor del entero n. Se prueba además una relación tipo Parseval sobre $\mathbb{Z}_n$ que más tarde es utilizada para caracterizar una familia de funciones bent sobre el mismo anillo. El trabajo aqui expuesto aparece publicado de manera más concisa en [21].

6.3.1 Funciones bent generalizadas

Recordemos la definición de función bent generalizada dada en [39]. Tomemos la raíz r-ésima primitiva de la unidad $\omega = e^{2\pi i / r}$ en los números complejos, $r \geq 2$, donde $i = \sqrt{-1}$.

Para cada función f de $\mathbb{Z}_r^m$ en $\mathbb{Z}_r$ se define la función con valores complejos $\omega^f : \mathbb{Z}_r^m \to \mathbb{C}$ como $\omega^f(\mathbf{u}) = \omega^{f(\mathbf{u})}$.

Definición 88 *La **transformada discreta de Fourier** de una función $g : \mathbb{Z}_r^m \to \mathbb{C}$ está definida como*

$$G(\mathbf{s}) = \frac{1}{\sqrt{r^m}} \sum_{\mathbf{u} \in \mathbb{Z}_r^m} g(\mathbf{u}) \omega^{-\mathbf{s}^t \mathbf{u}}, \quad \mathbf{s} \in \mathbb{Z}_r^m.$$

Definición 89 *Una función* $f : \mathbb{Z}_r^m \to \mathbb{Z}_r$ *es* ***bent generalizada*** *si los coeficientes de la transformada discreta de Fourier de la función* ω^f *satisfacen*

$$\left| \frac{1}{\sqrt{r^m}} \sum_{\mathbf{u} \in \mathbb{Z}_r^m} \omega^{f(\mathbf{u}) - \boldsymbol{\xi}^t \mathbf{u}} \right| = 1, \quad \textit{para todo } \boldsymbol{\xi} \in \mathbb{Z}_r^m.$$

En [39] podemos encontrar varias propiedades de las funciones bent generalizadas.

6.3.2 El número de soluciones de una ecuación lineal sobre $\mathbb{Z}_n$

El problema de determinar el número de soluciones de una ecuación lineal definida sobre un campo finito ha sido estudiado debido a su importancia en varias ramas de la Matemática (cf. [42]). Es fácil ver que la ecuación lineal $\sum_{i=1}^{m} a_i\, x_i = b$ tiene exactamente q^{m-1} soluciones sobre el campo finito $\mathbb{F}_q$ con q elementos. Ahora estamos interesados en resolver el mismo problema cuando reemplazamos el campo finito por el anillo $\mathbb{Z}_n$.

A fin de evitar confusiones, los elementos de $\mathbb{Z}_n$ se denotan como $\overline{a}, \overline{b}, \overline{r}, \overline{s}, \overline{z}, \ldots$ y los representantes de cada clase como a, b, r, s, z, respectivamente, donde tomaremos cada representante como el entero no negativo menor que n.

Antes de comenzar el desarrollo de la solución recordemos algunos conceptos que se usarán más adelante.

La *suma* de cualesquiera dos subconjuntos no vacíos de $\mathbb{Z}_n$, digamos $A = \{\overline{a}_i\}_{i=1}^{\alpha}$ y $B = \{\overline{b}_i\}_{j=1}^{\theta}$, está definida como el conjunto

$$A + B = \left\{ \overline{a}_i + \overline{b}_i : 1 \leq i \leq \alpha,\ 1 \leq j \leq \theta \right\}.$$

Nótese que para cualquier elemento $\overline{c} \in \mathbb{Z}_n$ el conjunto $\overline{c}\mathbb{Z}_n = \{\overline{cz} : \overline{z} \in \mathbb{Z}_n\}$ es un ideal de $\mathbb{Z}_n$. La suma de dos ideales de este tipo es nuevamente un ideal de la misma clase, como lo indica el siguiente

Lema 90 *Sean* $\overline{a}$ *y* $\overline{b}$ *dos elementos no cero de* $\mathbb{Z}_n$, *y sea* $d = \mathrm{mcd}(a, b)$. *Entonces*

$$\overline{a}\mathbb{Z}_n + \overline{b}\mathbb{Z}_n = \overline{d}\mathbb{Z}_n.$$

Demostración Como $d = \mathrm{mcd}\,(a, b)$ entonces existen enteros x, y, a_1, b_1 tales que $a = da_1$, $b = db_1$ y $d = ax + by$.

Sea $\overline{z}$ un elemento de $\overline{a}\mathbb{Z}_n + \overline{b}\mathbb{Z}_n$, entonces existen $\overline{u} \in \mathbb{Z}_n$, $\overline{v} \in \mathbb{Z}_n$ con la propiedad de que $\overline{z} = \overline{au} + \overline{v}\overline{b}$. Ahora $\overline{z}$ puede ser escrito como $\overline{z} = \overline{d}\left(\overline{ua}_1 + \overline{v}\overline{b}_1\right)$, por lo que $\overline{z} \in \overline{d}\mathbb{Z}_n$.

Por otro lado si $\overline{g} \in \overline{d}\mathbb{Z}_n$ entonces $\overline{g} = \overline{de}$ para algún $\overline{e} \in \mathbb{Z}_n$. De ahí que $\overline{g} = \overline{axe} + \overline{byc}$ y $\overline{g} \in \overline{a}\mathbb{Z}_n + \overline{b}\mathbb{Z}_n$. ■

El número de elementos de un ideal de la forma $\overline{a}\mathbb{Z}_n$ juega un papel principal en la solución de nuestro problema. Hemos encontrado la siguiente respuesta:

Lema 91 *Sea* $\overline{a}$ *un elemento no cero de* $\mathbb{Z}_n$, *y sea* $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ *la función definida como* $\varphi(\overline{x}) = \overline{ax}$. *Entonces*

$$|\ker(\varphi)| = \frac{n\ a}{\mathrm{mcd}(n,a)} \qquad y \qquad |\overline{a}\mathbb{Z}_n| = \frac{\mathrm{mcd}(n,a)}{a}$$

Demostración Sea s un entero positivo tal que $\mathrm{mcm}(a,n) = as$. Como $\overline{a}(\overline{sv}) = \overline{0}$ en $\mathbb{Z}_n$ para todo $\overline{v} \in \mathbb{Z}_n$, la cardinalidad de $\ker(\varphi)$ resulta ser

$$|\ker(\varphi)| = |\{v \in \mathbb{Z} : 0 \leq sv < n\}| = \frac{n\ a}{\mathrm{mcd}(n,a)}.$$

Por otro lado la cardinalidad de $\overline{a}\mathbb{Z}_n$ es la de $im(\varphi)$, la cual es $\frac{n}{|\ker(\varphi)|} = \frac{\mathrm{mcm}(n,a)}{a}$. ■

La solución

Dividimos el problema de encontrar el número de soluciones para la ecuación

$$\sum_{k=1}^{m} \overline{a}_k\ x_k = \overline{b} \tag{6.2}$$

sobre el anillo $\mathbb{Z}_n$ en dos casos. El segundo es general y resuelve este problema completamente, sin embargo se da la prueba del primero, que es el caso en que n es potencia de primo, debido a su sencillez.

Note que si algún coeficiente $\overline{a}_k$ en la ecuación (6.2) es una unidad en $\mathbb{Z}_n$ entonces la ecuación tiene n^{m-1} soluciones, así que nos restringiremos al caso en el que todos los coeficientes sean no unidades.

Elijamos un entero n, potencia de un número primo p, digamos $n = p^r$. Las no-unidades de $\mathbb{Z}_{p^r}$ son $\overline{0}$ y $\overline{p}^i\overline{a}$, donde $1 \leq a < p$ (es decir $\overline{a}$ es una unidad de $\mathbb{Z}_{p^r}$) y $1 \leq i < r$. Entonces la ecuación (6.2) puede ser expresada como

$$\sum_{k=1}^{m} \overline{a}_k\overline{p}^{i_k}\ x_k = \overline{b}. \tag{6.3}$$

Supongamos que i es el mínimo de los exponentes i_k, $1 \leq k \leq m$. De la factorización $\overline{p}^i \sum_{k=1}^{m} \overline{a}_k\overline{p}^{i_k - i}\ x_k = \overline{b}$ observamos que la ecuación puede ser resuelta si y sólo si $\overline{b} \in \overline{p}^i\mathbb{Z}_{p^r}$. En este caso, ya que los elementos $\overline{a}_k$ son unidades en $\mathbb{Z}_{p^r}$, resulta sencillo determinar el número de soluciones. Tenemos, por los lemas de la sección anterior, que el número de soluciones es

$$(p^r)^{m-1}\left|\{\overline{y} \in \mathbb{Z}_{p^r} : \overline{p}^i\overline{y} = \overline{b}\}\right| = p^{r(m-1)+i}.$$

Por lo tanto se ha probado la siguiente

Proposición 92 *Sea i el mínimo de los exponentes i_k en la ecuación (6.3) definida sobre el anillo $\mathbb{Z}_{p^r}$, con p un primo y $r \geq 1$. Entonces esta ecuación tiene $p^{(m-1)r+i}$ soluciones si $\overline{b} \in \overline{p}^i\mathbb{Z}_{p^r}$ y cero en otro caso.*

Ahora probaremos el caso general

Teorema 93 *La ecuación (6.2) tiene solución si, y sólo si, $\overline{b} \in \overline{d}\mathbb{Z}_n$, donde d es el máximo común divisor de $a_1, \ldots, a_m$. En este caso el número de soluciones es $\frac{n^m d}{\text{mcm}(n,d)}$.*

Demostración La primera afirmación es obvia después de notar que, por el lema 90, $\overline{d}\mathbb{Z}_n = \sum_{k=1}^{m} \overline{a}_k\mathbb{Z}_n$, así que sólo probaremos la segunda parte del teorema. Como la función lineal $\varphi : \mathbb{Z}_n^m \to \mathbb{Z}_n$. $\varphi(x_1, \ldots, x_m) = \sum_{k=1}^{m} \overline{a}_k\, x_k$ es balanceada, es decir todo valor en su imágen es tomado el mismo número de veces, se tiene que $|\ker(\varphi)| = \frac{n^m}{|\text{im}(\varphi)|}$. Por lo tanto la ecuación (6.2) tiene cero o $\frac{n^m}{|\overline{d}\mathbb{Z}_n|}$ soluciones. ■

Es sencillo probar que el resultado de la proposición anterior es un caso particular de este último.

6.3.3 Una clase de funciones bent

En lo que resta de esta sección se establecerá una relación tipo Parseval, válida para una familia de funciones definidas sobre el anillo $\mathbb{Z}_n$. Este resultado se utiliza enseguida para dar una caracterización de una clase de funciones bent generalizadas.

A fin de caracterizar cierta familia de funciones bent generalizadas $\mathbb{Z}_n$ será necesario conocer el valor de la siguiente suma exponencial.

Lema 94 *Sea n un entero positivo y sea ω una raíz n-ésima primitiva de la unidad. Entonces*

$$\sum_{\mathbf{u} \in \mathbb{Z}_n^m} \omega^{\mathbf{u}^t\mathbf{v}} = n^m \delta_{v,0}$$

donde $\delta_{\mathbf{x},\mathbf{y}}$ es la delta de Kronecker.

Demostración La prueba es similar a la del lema 34. ■

Utilizando el teorema 93 deduciremos una relación tipo Parseval para una familia de funciones definidas sobre $\mathbb{Z}_n$. Elijamos una raíz n-ésima de la unidad en los números complejos y llamémosle ω. Para cualquier función $f : \mathbb{Z}_n^m \to \mathbb{Z}_n$ y todo elemento $\gamma \in \mathbb{Z}_n$ definamos la función $F_{\gamma f}(\mathbf{v}) = \omega^{\gamma f(\mathbf{v})}$. Denotemos también como $\widehat{F}_{\gamma f}$ a la transformada discreta de Fourier de la función γf, esto es $\widehat{F}_{\gamma f}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_n^m} \omega^{\gamma f(\mathbf{u}) - \mathbf{v}^t\mathbf{u}}$.

Proposición 95 *Si* $n = 2t$ *entonces*

$$\sum_{\mathbf{u}\in\mathbb{Z}_n^m} \widehat{F}_{tf}(\mathbf{u})\,\widehat{F}_{tf}(\mathbf{u}+\mathbf{v}) = n^{2m}\delta_{\mathbf{v},\mathbf{0}},$$

para toda función $f : \mathbb{Z}_n^m \to \mathbb{Z}_n$ *tal que* $f(-\mathbf{z}) = f(\mathbf{z})$ *para todo* $\mathbf{z} \in \mathbb{Z}_n^m$.

Demostración Es fácil verificar las siguentes igualdades: $F_{tf}(\mathbf{z})\,F_{tf}(\mathbf{z}) = \omega^{2tf(\mathbf{z})} = 1$ y $\sum_{\mathbf{u}\in\mathbb{Z}_n^m} i^{\mathbf{u}^t(\mathbf{z}+\mathbf{x})} = 4^m\delta_{\mathbf{z},-\mathbf{x}}$. El resto de la prueba es análogo a la dada en [46] (lema 2, pág. 416) para funciones boolenas binarias, haciendo uso del teorema 93. ■

Corolario 96 *(Relación tipo Parseval) Sea* $f : \mathbb{Z}_n^m \to \mathbb{Z}_n$ *una función tal que* $f(-\boldsymbol{\omega}) = f(\boldsymbol{\omega})$ *para todo* $\boldsymbol{\omega} \in \mathbb{Z}_n^m$, *y supongamos que* $n = 2t$. *Entonces, con la notación anterior,*

$$\sum_{\mathbf{u}\in\mathbb{Z}_n^m} \widehat{F}_{tf}(\mathbf{u})^2 = n^{2m}.$$

Este último corolario nos conduce caracterizar una familia de funciones bent generalizadas definidas sobre el anillo $\mathbb{Z}_n$.

Proposición 97 *Sea* $f : \mathbb{Z}_n^m \to \mathbb{Z}_n$ *una función tal que* $f(-\boldsymbol{\omega}) = f(\boldsymbol{\omega})$ *para todo* $\boldsymbol{\omega} \in \mathbb{Z}_n^m$, *supongamos además que* $n = 2t$ *y que* $m = 2k$. *Entonces* tf *es una función bent generalizada si y sólo si* $0 \le \left|\widehat{F}_{tf}(\mathbf{u})\right| \le n^k$.

Demostración Si la función tf es bent claramente se cumplen las desigualdades $0 \le \left|\widehat{F}_{tf}(\mathbf{u})\right| \le n^k$. Por otro lado si $\left|\widehat{F}_{tf}(\mathbf{u})\right| = n^k - j$, para $0 \le j \le n^k$, entonces $\left|\widehat{F}_{tf}(\mathbf{u})\right|^2 \le n^m$. Pero por el corolario 96 tenemos que $n^{2m}\left|\sum_{\mathbf{u}\in\mathbb{Z}_n^m} \widehat{F}_{tf}(\mathbf{u})^2\right| \le \sum_{\mathbf{u}\in\mathbb{Z}_n^m}\left|\widehat{F}_{tf}(\mathbf{u})\right|^2 \le n^{2m}$, de donde $\left|\widehat{F}_{tf}(\mathbf{u})\right|^2 = n^m$, como se quería probar. ■

CAPÍTULO 7

CONCLUSIONES Y LÍNEAS FUTURAS DE INVESTIGACIÓN

En esta última parte de la tesis se resumen las principales conclusiones obtenidas a lo largo del escrito y se plantean algunos problemas que han quedado abiertos a lo largo de la exposición.

7.1 Conclusiones

Podemos considerar que son tres las metas principales que motivaron el desarrollo de este trabajo. Enseguida se resumen las conclusiones:

- Se ha propuesto introducir una métrica en el espacio en que se encuentre inmerso un código lineal, distinta a la métrica de Hamming que usualmente se considera, logrando con ello obtener información adicional sobre la manera en que se distribuyen los pesos del código (capítulo 3). Este trabajo ha tenido una gran aceptación y al momento de redactar este escrito se conocen ya dos generalizaciones distintas a los resultados obtenidos en el tema (cf. [30] y [36]).

- Se describe un método de construcción de códigos lineales con el que se han recuperado como casos particulares a los códigos binarios de Reed-Muller, los códigos asociados a sistemas de ciclos y varios códigos con parámetros que alcanzan cotas generales (capítulo 4).

- Una preocupación constante en el desarrollo de este trabajo fue determinar diferentes bases para los códigos binarios de Reed-Muller consistentes de vectores de peso mínimo, para facilitar su implementación, que sean más fácilmente calculadas que si se evaluaran polinomios (que es la forma en que usualmente se encuentran) y además dar una descripción de esas bases en términos de las variedades afines asociadas. Se logró tal objetivo y aparece resuelto en los capítulos 4 y 6.

7.2 Problemas abiertos

1. Determinar relaciones tipo MacWilliams al considerar P-métricas, con P un copo. ¿Qué información adicional puede obtenerse del código? ¿Bajo qué condiciones un código es perfecto, MDS, etc. con esta nueva métrica?

2. Existe un m-sistema de ciclos, m un entero par, de la gáfica completa no dirigida K_n con n vértices, n satisfaciendo algunas condiciones muy simples, el cual puede ser contruido con el previo conocimiento de un m-sitema de ciclos de una gráfica bipartita completa no dirigida (cf. [43], teorema 2.8). Si $m \equiv 0 \pmod 4$, pueden utilizarce los códigos definidos en este trabajo para encontrar los parámetros de un código asociado a un m-$SC(K_n)$?

3. ¿Bajo qué condiciones del parámetro a son iguales dos códigos del tipo $C_a(r)$? Por ejemplo $C_2(5)$ es el mismo código que $C_4(5)$.

4. El polinomio generador del código cíclico $C_a(r)$ parece tener la propiedad de ser su propio recíproco, es decir $g^*(x) = g(x)$ ¿es esto válido en general?

5. En el método de extensión de códigos se ha comenzado con un código cíclico $C_a(r)$. ¿Cómo debe elegirse un código inicial en general (no necesariamente del tipo $C_a(r)$) para garantizar resultados óptimos, tanto en los parámetros de los códigos como en sus propiedades matemáticas y prácticas? ¿Qué nuevas familias de códigos pueden obtenerse con este método? ¿Qué puede decirse de sus códigos duales?

6. ¿Existe una manera eficiente de decodificar los códigos introducidos en los capítulos 4 y 5 seleccionando adecuadamente los códigos auxiliares $\mathbf{O}_i$?

7. ¿Puede generalizarce el método de extensión de códigos dada en el capítulo 4 a códigos no lineales? ¿y a códigos no binarios?

8. ¿Qué pude decirse sobre el código asociado a un sistema de ciclos en general? Por ejemplo un sistema pentagonal de Steiner es un 5-sisterna de ciclos de la gráfica completa no dirigida K_n con n vértices, en particular el 5-$SC(K_{11})$ es un 2-$(11,5,2)$ diseño (cf. [44]). Los ciclos del 5-$SC(K_{11})$ pueden ser elegidos como $\{(i, i+3, i+4, i+8, i+2) : i \in \mathbb{Z}_{11}\}$, donde $\mathbb{Z}_{11}$ es el anillo de los enteros módulo 11, entonces es fácil verificar que el código ternario asociado a este sistema de ciclos es el código de Golay de parámetros $[11, 6, 5]$.

Apéndice

La siguiente lista muestra los polinomios característico $m(x)$ y generador $g(x)$ para los códigos $C_a(r)$ definidos por la relación (4.1), cuyos parámetros son $[r, L, 2-\delta_{r,L}]$, donde $\delta_{x,y}$ es la delta de Kronecker y L es el grado de $m(x)$. Los resultados se obtuvieron utilizando el algorítmo de Berlekamp-Massey programado en Mathematica. Por cuestiones de espacio algunos polinomios se escriben en forma de cociente.

r	a	$\{m(x), \quad g(x)\}$
2	1	$\{1+x^2, \quad 1\}$
2	2	$\{1+x, \quad 1+x\}$
3	1	$\{1+x^3, \quad 1\}$
3	2	$\{1+x+x^2, \quad 1+x\}$
4	1	$\{1+x^4, \quad 1\}$
4	2	$\{1+x+x^2+x^3, \quad 1+x\}$
4	3	$\{1+x^4, \quad 1\}$
5	1	$\{1+x^5, \quad 1\}$
5	2	$\{1+x+x^2+x^3+x^4, \quad 1+x\}$
5	3	$\{1+x^5, \quad 1\}$
5	4	$\{1+x+x^2+x^3+x^4, \quad 1+x\}$
6	1	$\{1+x^6, \quad 1\}$
6	2	$\{1+x+x^2+x^3+x^4+x^5, \quad 1+x\}$
6	3	$\{1+x+x^3+x^4, \quad 1+x+x^2\}$
6	4	$\{1+x^2+x^4, \quad 1+x^2\}$
6	5	$\{1+x^6, \quad 1\}$
7	1	$\{1+x^7, \quad 1\}$
7	2	$\{1+x+x^2+x^3+x^4+x^5+x^6, \quad 1+x\}$
7	3	$\{1+x^7, \quad 1\}$
7	4	$\{1+x+x^2+x^3+x^4+x^5+x^6, \quad 1+x\}$
7	5	$\{1+x^7, \quad 1\}$
7	6	$\{1+x+x^2+x^3+x^4+x^5+x^6, \quad 1+x\}$
8	1	$\{1+x^8, \quad 1\}$
8	2	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7, \quad 1+x\}$
8	3	$\{1+x^8, \quad 1\}$
8	4	$\{1+x+x^4+x^5, \quad 1+x+x^2+x^3\}$
8	5	$\{1+x^8, \quad 1\}$
8	6	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7, \quad 1+x\}$
8	7	$\{1+x^8, \quad 1\}$
9	1	$\{1+x^9, \quad 1\}$

r	a	$\{m(x),\quad g(x)\}$
9	2	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8,\quad 1+x\}$
9	3	$\{1+x+x^3+x^4+x^6+x^7,\quad 1+x+x^2\}$
9	4	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8,\quad 1+x\}$
9	5	$\{1+x^9,\quad 1\}$
9	6	$\{1+x^3+x^6,\quad 1+x^3\}$
9	7	$\{1+x^9,\quad 1\}$
9	8	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8,\quad 1+x\}$
10	1	$\{1+x^{10},\quad 1\}$
10	2	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9,\quad 1+x\}$
10	3	$\{1+x^{10},\quad 1\}$
10	4	$\{1+x^2+x^4+x^6+x^8,\quad 1+x^2\}$
10	5	$\{1+x+x^5+x^6,\quad 1+x+x^2+x^3+x^4\}$
10	6	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9,\quad 1+x\}$
10	7	$\{1+x^{10},\quad 1\}$
10	8	$\{1+x^2+x^4+x^6+x^8,\quad 1+x^2\}$
10	9	$\{1+x^{10},\quad 1\}$
11	1	$\{1+x^{11},\quad 1\}$
11	2	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10},\quad 1+x\}$
11	3	$\{1+x^{11},\quad 1\}$
11	4	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10},\quad 1+x\}$
11	5	$\{1+x^{11},\quad 1\}$
11	6	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10},\quad 1+x\}$
11	7	$\{1+x^{11},\quad 1\}$
11	8	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10},\quad 1+x\}$
11	9	$\{1+x^{11},\quad 1\}$
11	10	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10},\quad 1+x\}$
12	1	$\{1+x^{12},\quad 1\}$
12	2	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11},\quad 1+x\}$
12	3	$\{1+x+x^3+x^4+x^6+x^7+x^9+x^{10},\quad 1+x+x^2\}$
12	4	$\{1+x+x^4+x^5+x^8+x^9,\quad 1+x+x^2+x^3\}$
12	5	$\{1+x^{12},\quad 1\}$
12	6	$\{1+x+x^6+x^7,\quad 1+x+x^2+x^3+x^4+x^5\}$
12	7	$\{1+x^{12},\quad 1\}$
12	8	$\{1+x^4+x^8,\quad 1+x^4\}$
12	9	$\{1+x+x^3+x^4+x^6+x^7+x^9+x^{10},\quad 1+x+x^2\}$
12	10	$\{1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11},\quad 1+x\}$
12	11	$\{1+x^{12},\quad 1\}$
13	1	$\{1+x^{13},\quad 1\}$
13	2	$\{(1+x^{13})/(1+x),\quad 1+x\}$
13	3	$\{1+x^{13},\quad 1\}$
13	4	$\{(1+x^{13})/(1+x),\quad 1+x\}$

r	a	$\{m(x), \quad g(x)\}$
13	5	$\{1+x^{13}, \quad 1\}$
13	6	$\{(1+x^{13})/(1+x), \quad 1+x\}$
13	7	$\{1+x^{13}, \quad 1\}$
13	8	$\{(1+x^{13})/(1+x), \quad 1+x\}$
13	9	$\{1+x^{13}, \quad 1\}$
13	10	$\{(1+x^{13})/(1+x), \quad 1+x\}$
13	11	$\{1+x^{13}, \quad 1\}$
13	12	$\{(1+x^{13})/(1+x), \quad 1+x\}$
14	1	$\{1+x^{14}, \quad 1\}$
14	2	$\{(1+x^{14})/(1+x), \quad 1+x\}$
14	3	$\{1+x^{14}, \quad 1\}$
14	4	$\{(1+x^{14})/(1+x^2), \quad 1+x^2\}$
14	5	$\{1+x^{14}, \quad 1\}$
14	6	$\{(1+x^{14})/(1+x), \quad 1+x\}$
14	7	$\{1+x+x^7+x^8, \quad (1+x^7)/(1+x)\}$
14	8	$\{(1+x^{14})/(1+x^2), \quad 1+x^2\}$
14	9	$\{1+x^{14}, \quad 1\}$
14	10	$\{(1+x^{14})/(1+x), \quad 1+x\}$
14	11	$\{1+x^{14}, \quad 1\}$
14	12	$\{(1+x^{14})/(1+x^2), \quad 1+x^2\}$
14	13	$\{1+x^{14}, \quad 1\}$
15	1	$\{1+x^{15}, \quad 1\}$
15	2	$\{(1+x^{15})/(1+x), \quad 1+x\}$
15	3	$\{(1+x^{15})/(1+x+x^2), \quad 1+x+x^2\}$
15	4	$\{(1+x^{15})/(1+x), \quad 1+x\}$
15	5	$\{1+x+x^5+x^6+x^{10}+x^{11}, \quad 1+x+x^2+x^3+x^4\}$
15	6	$\{(1+x^{15})/(1+x^3), \quad 1+x^3\}$
15	7	$\{1+x^{15}, \quad 1\}$
15	8	$\{(1+x^{15})/(1+x), \quad 1+x\}$
15	9	$\{(1+x^{15})/(1+x+x^2), \quad 1+x+x^2\}$
15	10	$\{1+x^5+x^{10}, \quad 1+x^5\}$
15	11	$\{1+x^{15}, \quad 1\}$
15	12	$\{1+x^3+x^6+x^9+x^{12}, \quad 1+x^3\}$
15	13	$\{1+x^{15}, \quad 1\}$
15	14	$\{(1+x^{15})/(1+x), \quad 1+x\}$
16	1	$\{1+x^{16}, \quad 1\}$
16	2	$\{(1+x)^{15}, \quad 1+x\}$
16	3	$\{1+x^{16}, \quad 1\}$
16	4	$\{(1+x^{16})/(1+x)^3, \quad (1+x)^3\}$
16	5	$\{1+x^{16}, \quad 1\}$
16	6	$\{(1+x)^{15}, \quad 1+x\}$

r	a	$\{m(x), \quad g(x)\}$
16	7	$\{1+x^{16}, \quad 1\}$
16	8	$\{(1+x)^9, \quad (1+x)^7\}$
16	9	$\{1+x^{16}, \quad 1\}$
16	10	$\{(1+x)^{15}, \quad 1+x\}$
16	11	$\{1+x^{16}, \quad 1\}$
16	12	$\{(1+x^{16})/(1+x)^3, \quad (1+x)^3\}$
16	13	$\{1+x^{16}, \quad 1\}$
16	14	$\{(1+x)^{15}, \quad 1+x\}$
16	15	$\{1+x^{16}, \quad 1\}$

Referencias

1. Assmus, E.F. Jr. and Key, J.D. *Designs and Their Codes.* Cambridge University Press, 1992.
2. Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. *Visual Cryptography for General Accsess Structrures.* Information and Computation **129** (1996) 86-106. También disponible gratuitamente en: http://www.carc.math.uwaterloo.ca/~dstinson/
3. Blake, I.F. and Mullin, R.C. *An Introduction to Algebraic and Combinatorial Coding Theory.* Academic Press, 1976.
4. Bogart, K.P. *Incidence codes of posets: Eulerian posets and Reed-Muller codes.* Discrete Math. **31** (1980) 1-7.
5. Bosák, J. *Decompositions of Graphs.* Kluwer Academic Publ., 1990.
6. Brouwer, A.E. *Bounds on the Size of Linear Codes.* Chapter 4 of "Handbook of Coding Theory". Edited by V.S. Pless y W.C. Huffman. 1998. Existe también una versión en línea en: http://www.win.tue.nl/~aeb/voorlincod.html
7. Brouwer, A.E., Cohen, A.M. and Neumaier, A. *Distance regular graphs.* Springer-Verlag, 1989.
8. Brualdi, R.A. and Graves, J.S. and Lawrence, K.M. *Codes with Poset Metric.* Discrete Math. **147** (1995) 57-72.
9. Colburn, C.J., Dinitz, J.H. and Stinson, D.R. *Applications of Combinatorial Designs to Communications, Cryptography, and Networking.* Surveys in Combinatorics, Cambridge University Press, 1999, pages 37-100. Disponible gratuitamente en: http://www.carc.math.uwaterloo.ca/~dstinson/
10. Costello, D.J. Jr., Hagenaver, J., Imai, H. and Wicker, S.B. *Applications of Error-Control Coding.* IEEE Trans. Infrom. Theory **44** (1998) 2531-2560.
11. Davida, G.I., Frankel, Y., Matt, B.J. and Peralta, R. *On the Relation of Error Correlation and Cryptography to an off line biometric based identification scheme.* (1998) Preprint.
12. Delsarte, P., Goethals, J.-M., and MacWilliams, F.J. *On generalized Reed-Muller codes and their relatives.* Info. and Control, **16** (1974) 403-442.
13. Díaz S., S. *Generación de sucesiones pseudoaleatorias criptográficamente fuertes.* Tesis de Maestría. UAM-I. En preparación.
14. Duursma, I.M., Rentería, C, and Tapia-Recillas, H. *Reed-Muller Codes on Complete Intersections.* Applicable Algebra in Engineering, Communication and Computing (AAECC) **11** (2001) 455-462.
15. Gao, S. and Key, J.D. *Bases of Minimum-Weight Vectors for Codes from Designs.* Finite Fields and their Applications **4** (1998) 1-15.
16. Godsil, C.D. *MacWilliams theorem for product schemes.* (1998) Preprint.
17. González S., M., Rentería, C. and Tapia-Recillas, H. *Reed-Muller type codes over the Segre variety.* Submited to Finite Fields and Their Applications.

18. Gutiérrez, J.N. *Códigos Lineales y Geometrías Finitas.* Tesis de maestría. UAM-I, 1997.
19. Gutiérrez, J.N. y Tapia-Recillas, H. *Códigos binarios de Reed-Muller y esferas de Hamming.* Aportaciones Matemáticas. Serie Comunicaciones **22** (1998) 71-75.
20. Gutiérrez, J.N. and Tapia-Recillas, H. *A MacWilliams Identity for Poset-Codes.* Congressus Numerantium **133** (1998) 63-73.
21. Gutiérrez, J.N., Tapia-Recillas, H. and Vega, G. *A Parseval type of relation on $\mathbb{Z}_n$.* Proc. of the World Multiconference on Systematics, Cybernetics and Informatics, Orlando, Florida, USA, **7** (2000) 672-674
22. Gutiérrez, J.N. and Tapia-Recillas, H. *Extensions of linear codes.* (2002) Preprint.
23. Gutiérrez, J.N. y Tapia-Recillas, H. *A minimum weight basis for the binary Reed-Muller code.* To appear in Cogressus Numerantium.
24. Hakimi, S.L. and Bredson, J.G. *Graph theoretic error-correcting codes.* IEEE Trans. on Inform. Theory, vol. **IT-14** (1968) 584-591.
25. Hamming, R.W. *Error detecting and error correcting codes.* Bell Syst. Tech. J., **29** (1950) 147-160.
26. Hammons, A. R. Jr., Kumar, P. Vijay, Calderbank, A.R., Sloane, N.J.A. and Solé, P. *The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes.* IEEE Trans. on Inform. Theory **40** (1994) 301-319.
27. Harary, F. *Graph Theory.* Addison-Wesley Publ. Co., 1969.
28. Heijnen, P., van Tilborg, H., Verhoeff, T. and Weijs, S. *Some New Binary, Quasi-Cyclic Codes.* IEEE Trans. on Inform. Theory **44** (1998) 1994-1996.
29. Imai, H. and Matsumoto, T. *Coding Theory and Its Applications in Japan.* LNCS **356** (1987) 301-305.
30. Jang, Y. and Park, J. *On a MacWilliams type identity and perfecteness for a binary linear $(n, n-1, j)$-poset code.* Preprint (2001).
31. Jungnickel, D. and Vanstone, S.A. *Graphical Codes Revisited.* IEEE Trans. on Inform. Theory **43** (1997) 136-146.
32. Jungnickel, D. and Vanstone, S.A. *q-ary graphical codes.* Discrete Math. **208/209** (1999) 375-386.
33. Kasami, T., Lin, S. and Peterson, W.W. *Generalized Reed-Muller codes.* Electron. Commun. Japan **51-C** (3) (1968) 94-104.
34. Key, J.D. *Some error-correcting codes and their applications.* Chapter 14 of "*Applied Mathematical Modeling: a Multidisciplinary Approach*" D. R. Shier and K. T. Wallenius (Eds.), Chapman & Hall/CRC press, Boca Raton, FL., 1999. También disponible gratuitamente en: http://www.math.clemson.edu/faculty/Key/
35. Key, J.D. and Sullivan, F.E. *Codes of Steiner Triple and Quadruple Systems.* Des. Codes and Cryptography, **3** (1993) 117-125.
36. Kim, D.S. and Lee, J.G. *A Macwilliams-type identity for linear codes on weak order.* Preprint (2001).
37. Kløve, T. *Support weight distribution of linear codes.* Discrete Math. vol. **106/107**

(1992) 311-316.

38. Koblitz, N. *Algebraic Aspects of Cryptography.* Spinger-Verlag. 1998.
39. Kumar, P.V., Scholtz, R. A. and Welch, L.R. *Generalized Bent Functions and Their Properties.* J. of Combinatorial Theory, Series A, **40** (1995) 90-107
40. Lachaud, G., Lucien, I., Mercier, D. and Rolland, R. *Cyclic codes related to Reed-Muller codes.* Preprint (1997).
41. Levenshtein, V.I. *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces.* IEEE Trans. on Inform. Theory, vol. **41** (1995) 1303-1321.
42. Lidl, R. and Niederreiter, H. *Finite Fields.* Encyclopedia of Mathematics and its Applications. Addison-Wesley Publ., 1983.
43. Lindner, C.C. and Rodger, C.A. *Descompositions into Cycles II: Cycle Systems.* Chapter 8 of *Contemporary Design Theory. A collection of Surveys.* Edited by J.H. Dinitz and D.R. Stinson. Wiley-Interscience Publication, John Wiley & Sons., 1992
44. Lindner, C.C. and Stinson, D.R. *Steiner Pentagon Systems.* Discrete Math. **52** (1984) 75-89.
45. MacWilliams, F.J. *A theorem on the distribution of weights in a systematic code.* Bell System Tech. J. **42** (1962) 79-64.
46. MacWilliams, F.J. and Sloane, N.J.A. *The Theory of Error-Correcting Codes.* North-Holland, 1988.
47. Martin, W.J. and Stinson, D.R. *Association schemes for ordered orthogonal arrays and* (T, M, S)*-nets.* Canadian Journal of Mathematics **51** (1999) 326-346.
48. Massey, J.L., Costello, D.J. and Justensen. J. *Polynomial weights and coset constructions.* IEEE Trans. Info. Theory **19** (1973) 101-110.
49. Morales, L.B. and Velarde C. *A Complete Classfication of* $(12, 4, 3)$*-RBIBDs.* Journal of Combin. Designs **9** (2001) 385-400.
50. Muller, D.E. *Applications of Boolean algebra to switching circuit design and error detection.* IEEE Trans. Computers **3** (1954) 6-12.
51. Muñoz G., J.I. *Aritmética rápida sobre campos finitos.* Tesis de Maestría. UAM-I, 2001.
52. Niederreiter, H. *Point sets and sequences with small discrepancy.* Monatsh. Math. **104** (1987) 273-337.
53. Niederreiter, H. *A combinatorial problem for vector spaces over finite fields.* Discrete Math. **96** (1991) 221-228.
54. Niederreiter, H. *Orthogonal arrays and other combinatorial aspects in the theory of uniform point distributions in unit cubes.* Discrete Math. **106/107** (1992) 361-367.
55. Nikityuk, N.M. *The method of syndrome coding and its applications for data compression and prossesing in high energy physics experiments.* LNCS **357** (1988) 324-335.
56. Pless, V. *Power moment identities on weight distribution in error correcting codes.* Information and Control **6** (1963) 147-152.

57. Rajpal, S. *On binary k-paving matroids and Reed-Muller codes.* Discrete Math. **190** (1998) 191-200.

58. Rentería, C. *Códigos Geométricos y Códigos Asociados a Gráficas.* Tesis Doctoral. UAM-I, 1994.

59. Rentería, C. and Tapia-Recillas. H. *A Connection between the Veronese Map and Reed-Muller Codes.* C. Numerantium **102** (1994) 175-181.

60. Rentería, C. and Tapia-Recillas. H. *A connection between Commutative Algebra and Coding Theory.* Applications Algèbre et Aritmetique **1** (1996) 1-8.

61. Rentería, C. and Tapia-Recillas, H. *Reed-Muller Codes: An Ideal Theory Approach.* Communications in Algebra **25** (1997) 401-413.

62. Rentería, C. and Tapia-Recillas, H. *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.) Springer Verlag ISBN 3-540-6624-0 (2000) 237-243.

63. Reed, I.S. *A class of multiple-error-correcting codes and the decoding shceme.* IEEE Trans. Info. Theory **4** (1954) 38-49.

64. Rifá, J. *On the construction of completely regular linear code from distance-regular graphs.* LNCS **356** (1987) 376-394.

65. Robling, D.E. *Cryptography and Data Security.* Addison-Wesley. 1983.

66. Roman, S. *Coding and information theory.* Springer Verlang (GTM) 1992.

67. Roman, S. *Introduction to Coding and Information Theory.* Springer Verlang (UTM) 1997.

68. Rothauss, O.S. *On bent functions.* J. of Combinatorial Theory, Series A, **20** (1976) 300-305.

69. Schouhamer, K.A., Siegel, P.H. and Wolf, J.K. *Codes for Digital Recorders.* IEEE Trans. Inform. Theory, **44,** (1998) 2260-2299.

70. Shannon, C.E. *A mathematical theory of communication.* Bell Syst. Tech. J. **27** (1948) 379-423 and 623-656.

71. Simonis, J. *The effective lenght of subcodes.* AAECC vol. **5** (1994) 371-377.

72. Sorensen, A.B. *Projective Reed-Muller Codes.* IEEE Trans. Inform. Theory **37** (1991) 1567-1576.

73. Sotteau, D. *Decomposition of $K_{m,n}$ $(K^*_{m,n})$ into Cycles (Circuits) of Length 2k.* J. of Combin. Theory, Series B **30** (1981) 75-81.

74. Stinson, D.R. *Combinatorial Designs and Cryptography.* Surveys in Combinatorics 1993. Edited by K. Walker. London Math. Society Lecture Notes Series **187**. Cambridge University Press, 1993 257-287.

75. Tonchev, V.D. *Combinatorial Configurations: Designs, Codes, Graphs.* Pitman Monographs and Surveys in Pure and Applied Mathematics **40**. Longman Scientific & Technical, 1988.

76. Tonchev, V.D. *Error-correcting codes from graphs.* To appear in Discrete Math.

77. van Lint, J.H. and van der Geer, G. *Introduction to Coding Theory and Algebraic Geometry.* Birkhäuser, DMV Seminar Band **12,** 1988.

78. van Lint, J.H. and Wilson, R. M. *A course in Combinatorics.* Cambridge Univesity Press, 1992.

79. Vega H., G. *Algunos resultados sobre funciones booleanas, cajas de sustitución y $\mathbb{Z}_2^k$-códigos lineales*. Tesis doctoral. UAM-I, 2000.

80. Wicker, S.B. *Deep Space Applications.* Chapter 25 of: *Handbook of Coding Theory.* Edited by V. S. Pless and W. C. Huffman. Elsevier Science, 1998.

81. Wie, V.K. *Generalized Hamming weights for linear codes.* IEEE Trans. Infrom. Theory **37** (1991) 1412-1418.