"CÓDIGOS LINEALES Y GEOMETRÍAS FINITAS"

POR

JOSÉ NOÉ GUTIÉRREZ HERRERA

TESIS DE MAESTRÍA

"CÓDIGOS LINEALES Y GEOMETRÍAS FINITAS"

TESIS QUE PRESENTA

JOSÉ NOÉ GUTIÉRREZ HERRERA

PARA LA OBTENCIÓN DEL GRADO DE
MAESTRO EN MATEMÁTICAS

ASESOR: DR. HORACIO TAPIA RECILLAS

FEBRERO 1997

UNIVERSIDAD AUTÓNOMA METROPOLITANA-IZTAPALAPA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

ÍNDICE

AGRADECIMIENTOS:

Agradezco a mis padres, Nicolás y Soledad, y a mi hermana, Vicky, porque siempre he podido contar con ellos: gracias por su incondicional apoyo.

Deseo expresar mi agradecimiento a los profesores del departamento de matemáticas de la Facultad de Ciencias de la U.A.S.L.P. por haberme dado los conocimientos necesarios para realizar mis estudios de posgrado, muy en especial al M. en C. Carlos E. Angulo Águila por la amistad y apoyo que me brindó durante mi estancia en dicha institución y al Profr. Jaime Velázquez Pantoja por enseñarme que el aprendizaje de las matemáticas puede ser una alegre experiencia.

Deseo expresar mi reconocimiento al CONACyT por su apoyo al otorgarme una beca para realizar mis estudios de maestría y para desarrollar el presente trabajo de tesis.

Va mi gratitud al departamento de matemáticas de la UAM-I, donde realicé mis estudios a nivel maestría, por haberme encaminado a la realización del presente escrito; especialmente al Dr. Horacio Tapia Recillas sin cuyo apoyo y asesoría no habría podido concluir este trabajo.

Por último agradezco a los profesores Dr. Carlos Rentería Márquez, Dr. Carlos Signoret Poillon y M. en C. Adolfo Torres Cházaro por su trabajo en la revisión de este trabajo en la cual me dieron importantes sugerencias y comentarios para una mejor presentación.

PREFACIO

La teoría de códigos comenzó su desarrollo hacia finales de la década de los 40's con los trabajos de R. Hamming (cf. [24]), M.J.E. Golay (ver [18]) y C. Shannon (cf. [47]). A partir de entonces la teoría se ha desarrollado cada vez más con el auxilio de técnicas matemáticas como la Teoría de los Números, Geometría Algebraica, Geometrías Finitas, Teoría de Gráficas, etc. El presente trabajo está dirigido al estudio de algunas de las relaciones existentes entre la teoría de códigos y las Geometrías Finitas.

Este trabajo se divide en 6 capítulos y un apéndice. En los primeros tres capítulos sólo se presentan resultados generales conocidos, mientras que en el resto se intercalan algunas aportaciones propias. En cada proposición extraida de algún texto se indica la referencia correspondiente, por ejemplo [45; 196] significa que el resultado que le sigue puede encontrarse en la página 196 de la referencia [45]. Se indica por □ el fin de una demostración.

En el primer capítulo se presenta una idea general de la problemática de la teoría de los códigos detectores-correctores de errores.

El segundo capítulo está dirigido al estudio de los conceptos generales de los códigos lineales. Se presenta la definición de código lineal detector-corrector de errores como un subespacio de un espacio vectorial de dimensión finita sobre un campo finito, y se definen sus tres principales parámetros (longitud, dimensión y distancia mínima). Se definen también las matrices generadora y de chequeo de paridad de un código lineal, las cuales determinan completamente al código. Al recibir una palabra codificada, esto es un elemento del código, es necesario saber cómo decodificarla por lo que se muestra un método general para decodificar un código lineal, conocido como decodificación con síndrome.

En el tercer capítulo se definen los códigos cíclicos, una clase especial de códigos lineales muy utilizados en la práctica, como se menciona al final del primer capítulo. Se muestra una relación entre este tipo de códigos y el álgebra conmutativa, y se hace uso de esta relación para calcular una matriz generadora para estos códigos. Enseguida se estudian ciertos tipos de códigos cíclicos: los llamados códigos de Hamming, con capacidad de detectar y corregir un error (que además tienen la máxima dimensión que puede tener un código lineal de longitud $(q^n - 1)/(q - 1)$, donde q es una potencia de la característica del campo finito); los códigos BCH, capaces de corregir una cantidad prefijada de errores; y los códigos de Reed-Solomon, un tipo de

códigos BCH los cuales tienen los parámetros ideales de un código.

En el capítulo cuatro se introduce el concepto de diseño. Se estudian dos tipos importantes de diseños: aquellos que surgen de las geometrías finitas proyectiva y afín. Se incluye una sección sobre el plano de Fano, la geometría proyectiva más simple. Esta consiste sólo de siete puntos, sin embargo tiene bastantes propiedades especiales. En este apartado se prueban algunas propiedades más de este diseño, aparte de las ya mostradas anteriormente. En [30] se describe un método para encontrar una base de un código binario de Hamming consistente en vectores de incidencia de las líneas de una geometría proyectiva; en el caso especial del código de Hamming $\mathcal{H}_3$ hemos podido caracterizar tales bases. También se calcula explícitamente el grupo de automorfismos del plano de Fano el cual resulta ser un grupo simple, de orden 168, no-conmutativo y doblemente transitivo, además se muestra una relación entre tal grupo de automorfismos y el código $\mathcal{H}_3$.

El capítulo cinco está dedicado al estudio de un tipo especial de códigos directamente relacionados con las geometrías finitas: los códigos de Reed-Muller y los códigos de Reed-Muller generalizados. Se muestra que los códigos binarios de Hamming pueden ser recuperados a partir de los códigos de Reed-Muller y que los códigos de Reed-Muller pueden, a su vez, ser obtenidos de ciertas geometrías finitas.

También se caracterizan los códigos asociados a los sistemas triples y cuádruples de Steiner, ya que algunos de estos surgen de ciertas geometrías finitas.

El sexto capítulo está dedicado al estudio los conjuntos diferencia y ciertos códigos asociados con gráficas, en esta sección se dan algunas aportaciones originales

Por último aparece un apéndice sobre posibles líneas de investigación para investigaciones futuras.

El propósito del presente trabajo es brindar a la comunidad una referencia más sobre la teoría de los códigos lineales detectores-correctores de errores, en especial aquellos relacionados con las geometrías finitas.

1 Introducción

Notación:
q : potencia de un primo p
$\mathbf{F}_q$: campo finito con q elementos
$\mathbf{F}_q^*$: grupo cíclico multiplicativo $\mathbf{F}_q - \{0\}$
$\mathbf{F}_q^n$: espacio vectorial de dimensión n sobre $\mathbf{F}_q$
$\mathbf{F}_q[x_1, \ldots, x_m]$: anillo de polinomios en $x_1, \ldots, x_m$ con coeficientes en $\mathbf{F}_q$
$P(A)$: conjunto potencia del conjunto A
$P_t(A)$: familia de los subconjuntos de A con cardinalidad t
χ_A : función característica del conjunto A

1.1 El problema principal

La idea de los códigos detectores-correctores de errores surgió originalmente como una respuesta a problemas prácticos de ingeniería eléctrica. Estos fueron inventados para corregir errores en los canales de comunicación producidos por ruido (se utiliza una codificación de los mensajes a enviar para dotarlos de alguna protección contra los posibles errores que introduzca el canal).

El problema que la teoría de códigos se encarga de estudiar podemos describirlo como sigue: Proveniente de una fuente emisora llega información a un cierto destino llamado el receptor a través de un medio al que llamaremos **canal,** el cual puede ser un cable telefónico, el espacio, fibras ópticas, etc., sin embargo en la práctica es probable que la información enviada no sea precisamente la que se reciba, debido a que puede haber ruido en el canal, entonces ocurre un error en la información. El problema consiste en detectar y corregir esos errores. Así pues se construye un codificador el cual no sólo permita enviar la información a través del canal sino que también, anexando información adicional llamada **redundancia,** permita detectar y corregir los errores que hayan ocurrido durante la transmisión.

Ejemplo 1.1 Supóngase que deseamos enviar un mensaje, digamos SI, al cual se le asigna la cadena 1001. El codificador lo expresa como 1001101 y lo envía, pero por haber ruido en el canal de transmisión se recibe el mensaje 0001101. Esto es, ha ocurrido un error en la primera posición del mensaje codificado, el decodificador debe de ser capaz de detectar y corregir este error.

Podemos resumir este ejemplo en el siguiente diagrama:

1001	→	1001101	→	0001101	→	1001101	→	1001
mensaje enviado		*mensaje codificado*	*canal*	*mensaje con error*		*mensaje corregido*		*mensaje recibido*

Comenzamos a construir un modelo del canal de transmisión. Se pretende que sea lo suficientemente complejo para garantizar su adecuado funcionamiento y lo suficientemente sencillo para modelarlo matemáticamente. El alfabeto que usaremos será el formado por los elementos de algún campo finito, el cual frecuentemente será el binario por ser más útil en la práctica y por sencillez.

Suponga que se tiene un canal con alfabeto de salida $a_1, a_2, \ldots, a_k$ y alfabeto de llegada $b_1, b_2, \ldots, b_n$. Supóngase que cada letra de llegada depende estadísticamente de la correspondiente letra de salida solamente. Escribimos $P(b_j \mid a_i)$ para denotar la probabilidad de que b_j se reciba dado que a_i fue enviada. Por ejemplo consideremos el así llamado *canal binario simétrico*. En este canal tenemos $P(1 \mid 0) = P(0 \mid 1) \doteq p$ y $P(1 \mid 1) = P(0 \mid 0) = 1 - p$ donde $0 < p < \frac{1}{2}$. Los valores 0 y $\frac{1}{2}$ de p son omitidos ya que en el primer caso el canal carece de errores y no es necesario codificar, mientras que en el segundo la palabra recibida no depende de la que fue enviada y el canal no es útil para transmitir.

Ejemplo 1.2 Supóngase que se desea transmitir la cadena $\bar{c} = 100110 \in \mathbf{F}_2^6$, y supóngase también que la probabilidad de transmisión incorrecta es $p = 0.07$, así la probabilidad de transmitir $\bar{c}$ sin errores es $(0.93)^6 \approx 0.65$.

La probabilidad de que la palabra enviada se reciba con un error en la primera posición es, por eventos independientes, $(0.07)(0.93)^5 \approx 0.049$. Con $\bar{e} = 100000$ se puede escribir $\bar{c} + \bar{e} = \bar{r}$, entonces $\bar{r}$ es la palabra recibida y $\bar{e}$, se denomina el **patrón de error.**

Para calcular la probabilidad de que la palabra recibida difiera de la enviada en exactamente dos posiciones se suman las probabilidades de cada patrón de errores formado por dos unos y cuatro ceros. Cada patrón tiene probabilidad de error $(0.07)^2(0.93)^4 \approx 0.004$, entonces la probabilidad de que ocurran dos errores durante la transmisión es

$$\binom{6}{2} (0.07)^2(0.93)^4 \approx 0.055$$

En general se tiene el siguiente

Teorema 1.1 [20;336] *Sea* $\bar{c} \in \mathbf{F}_2^n$. *Para transmitir* $\bar{c}$ *por un canal binario simétrico con probabilidad de error* p a) *la probabilidad de que la palabra recibida sea* $\bar{r} = \bar{c} + \bar{e}$, *donde* $\bar{e}$ *es un patrón de error con* k *unos y* $(n-k)$ *ceros, es* $p^k(1-p)^{n-k}$. b) *la probabilidad de que ocurran* k *errores durante la transmisión es*

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

Ejemplo 1.3 Entre los ejemplos más sencillos de código detector-corrector de errores está el así llamado **código de repetición.** Este código es útil para enviar dos mensajes, digamos SI y NO. Para esto los mensajes se codifican como los vectores $(0,\ldots,0)$ y $(1,\ldots,1)$ del espacio $\mathbf{F}_q^n$, respectivamente. En este caso la decodificación resulta sencilla, basta con contar la cantidad de 0's y de 1's en la palabra recibida, si la mayoría son 0 diremos que un 0 fue enviado mientras que si la mayoría son 1 entonces decimos que se envió un 1.

A lo largo del presente trabajo se tratarán diversos modelos matemáticos para codificar mensajes, para que un modelo resulte útil debe de tener una probabilidad de error pequeño.

Cabe mencionar que algunos de los códigos que se estudiarán a lo largo del presente trabajo han tenido y tienen aplicaciones concretas. Por ejemplo el código de Reed-Muller de primer orden $RM(1,5)$ fue utilizado en 1972 por el Mariner 9 para la transmisión de fotografías de Marte en blanco y negro (cf. [34;149],[45;133]). La NASA usa con bastante frecuencia los códigos de Reed-Solomon en sus programas espaciales, por ejemplo los utilizó en sus misiones *Galileo,Magellan* y *Ulysses* (cf. [45;134]).

2 Códigos lineales

La noción de código error-corrector fue descubierto por R.V. Hamming en 1950, y aparece descrito por primera vez en la referencia [24]. Además el concepto de código lineal fue enunciado primero, en 1956, por D. Slepian (ver [48]).

2.1 Conceptos generales

Sea $\mathbf{F}_q$ el campo de orden q, con q una potencia de un primo p.

Definición 2.1 *Sean $n, k \in \mathbf{N}$, $k \leq n$. Un* **código** *de longitud n y dimensión k es una función inyectiva*

$$\phi : \mathbf{F}_q^k \longrightarrow \mathbf{F}_q^n.$$

Si ϕ es lineal entonces se dirá que el código es **lineal.**

En lo sucesivo, cuando hablemos de códigos lineales, no haremos distinción entre la función ϕ y su imagen y a ambas les llamaremos códigos lineales. Notemos que un código lineal $C = \phi(\mathbf{F}_q^k)$ es un subespacio lineal de $\mathbf{F}_q^n$ cuya dimensión es k. En este caso se dirá que C es un $[n, k]$-código lineal y a los elementos de C les llamaremos **palabras codificadas.**

Definición 2.2 *Dos códigos C_1 y C_2 se dirán* **equivalentes** *si C_1 puede obtenerse de C_2 intercambiando coordenadas y multiplicandolas por un elemento no cero de $\mathbf{F}_q$.*

Ejemplo 2.1 Los dos códigos siguientes son $[4, 2]$ códigos lineales binarios equivalentes.

$$C = \{(0,0,0,0), (0,1,0,1), (1,0,1,0), (1,1,1,1)\}$$
$$C' = \{(0,0,0,0), (1,0,0,1), (0,1,1,0), (1,1,1,1)\}$$

Al igual que en el caso real, podemos definir un producto interior en el espacio $\mathbf{F}_q^n$ de la manera usual, esto es si $\bar{u} = (u_1, \ldots, u_n)$ y $\bar{v} = (v_1, \ldots, v_n)$ son elementos de este espacio entonces

$$\bar{u} \cdot \bar{v} = u_1 v_1 + \cdots + u_n v_n.$$

Con esta noción podemos hablar del código ortogonal, como se hace en la siguiente

Definición 2.3 *Sea C un $[n,k]$ código lineal sobre $\mathbf{F}_q$. El espacio ortogonal a C, denotado por $C^{\perp}$, es llamado el* **código dual** *a C. Esto es $C^{\perp} = \{\bar{u} \in \mathbf{F}_q^n : \bar{u} \cdot \bar{v} = 0, \forall\ \bar{v} \in C\}$. Si $C \subseteq C^{\perp}$ se dice que C es* **auto-ortogonal** *y cuando la igualdad es válida C se denomina* **auto-dual.**

Ejemplo 2.2 Denotemos por $\mathbf{1}$ el vector de longitud n que tiene todas sus entradas igual a 1 y llamémosle el **vector todo-uno.** Es bien conocido, de álgebra lineal, que si W es un subespacio de un espacio vectorial de dimensión finita entonces la suma de las dimensiones de W y su ortogonal es precisamente la dimensión de V. Por lo tanto el código $(\mathbf{F}_q\mathbf{1})^{\perp}$ es un espacio vectorial de dimensión $n-1$ sobre $\mathbf{F}_q$, y puede comprobarse fácilmente que $\{\bar{e}_i - \bar{e}_n : 1 \leq i \leq n-1\}$ es una base del código, donde $\bar{e}_l$ es el vector en $\mathbf{F}_q$ que tiene un uno en la entrada l-ésima y cero en las demás. En particular este código es generado por $\{\bar{e}_i - \bar{e}_j : 1 \leq i, j \leq n\}$.

Ya que para todo código lineal C siempre se tiene la contención $C \subseteq C^{\perp\perp}$ y ambos códigos tienen la misma dimensión, el doble dual de C es C mismo.

Para cada código lineal $\phi : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ existe una matriz G, $k \times n$, con entradas en $\mathbf{F}_q$ tal que, si $C = \phi(\mathbf{F}_q^k)$ entonces

$$C = \{\bar{u}G : \bar{u} \in \mathbf{F}_q^k\}.$$

En efecto, elijamos la base canónica de $\mathbf{F}_q^k$, es decir la base formada por los k vectores linealmente independientes $\bar{e_1}, \bar{e_2}, ..., \bar{e_k}$ donde el vector $\bar{e_i}$ tiene un uno en la i-ésima entrada y cero en todas las demás, con $i = 1, 2, ... k$. Si $\phi(\bar{e_i}) = \bar{v_i}$, sea $\bar{v_i}$ el renglón i-ésimo de la matriz G, entonces cualquier elemento $\bar{u}$ en $\mathbf{F}_q^k$ es de la forma $\bar{u} = (u_1, u_2, ..., u_k) = \Sigma_{j=1}^k u_j \bar{e_j}$, con $u_t \in \mathbf{F}_q$, $t = 1, \ldots, k$ y al aplicar la función ϕ resulta:

$$\phi(\bar{u}) = \Sigma_{j=1}^k u_j \phi(\bar{e_j}) = (u_1, u_2, ..., u_k)G = \bar{u}G.$$

Esta matriz G recibe el nombre de **matriz generadora** del código y sus renglones forman una base para el código. Utilizando operaciones elementales sobre los renglones de G y permutaciones de sus columnas podemos tranformarla en una matriz conocida como la **forma estándard** de la matriz generadora; esta es una matriz de la forma (I_k, A), donde I_k es la matriz identidad de $k \times k$ y A es una matriz de $k \times (n-k)$:

Ya que los renglones de $G = (a_{ij})$ son linealmente independientes, el primero tiene una entrada no cero. Permutando la columna que contiene esta entrada con la primera obtenemos a_{11} distinto de cero. Añadiendo un múltiplo adecuado del primer renglón al segundo podemos hacer $a_{21} \neq 0$, y entonces sumar un múltiplo del segundo renglón al primero para hacer $a_{11} = 1$. Utilizando operaciones elementales entre renglones se hace $a_{i1} = 0$, para $i > 1$. El segundo renglón de G, al igual que el primero, tiene una entrada no cero, después de permutar la columna que contiene dicha entrada con la segunda columna obtenemos $a_{22} \neq 0$. Repitiendo un procedimento análogo al anterior hacemos $a_{22} = 1$, $a_{12} = 0$ y $a_{i2} = 0$, $i > 2$. Ya que el rango de la matriz G es k, al aplicar un razonamiento similar al anterior a cada renglón de la matriz obtenemos una matriz de la forma enunciada.

Cuando la matriz G está dada en forma estándard al codificar un mensaje aparece el mensaje original en las primeras k entradas de la palabra codificada; los elementos en las entradas restantes son los que nos permiten detectar errores ocurridos durante la transmisión del mensaje.

La función ϕ induce la sucesión exacta corta

$$0 \to \mathbf{F}_q^k \xrightarrow{\phi} \mathbf{F}_q^n \xrightarrow{\psi} \mathbf{F}_q^{n-k} \to 0,$$

donde $\psi(\bar{x}) = H\bar{x}^t$ ($\bar{x}^t$ es el vector transpuesto de $\bar{x}$) y los renglones de H forman una base para $\phi(\mathbf{F}_q^k)^\perp$. Ya que el núcleo de ψ es precisamente la imagen de ϕ,

$$\bar{x} \in C \quad \Longleftrightarrow \quad H\bar{x}^t = 0.$$

A esta matriz H (de $(n-k) \times n$) se le denomina **matriz de chequeo de paridad** del código C.

Ejemplo 2.3 La matriz de chequeo de paridad

$$H = \left(\begin{array}{cccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

define un código con $n = 7$ y $k = 4$.

El código del ejemplo anterior codifica el mensaje (u_1, u_2, u_3, u_4) como la palabra codificada $\bar{x} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, donde

$$x_1 = u_1, \; x_2 = u_2, \; x_3 = u_3, \; x_4 = u_4$$

y x_5, x_6 y x_7 son elegidos de tal forma que $H\bar{x}^t = 0$; en otras palabras deben de satisfacer el sistema de ecuaciones lineales

$$\begin{aligned} x_1 + x_3 + x_4 + x_5 &= 0, \\ x_2 + x_3 + x_4 + x_6 &= 0, \\ x_1 + x_2 + x_4 + x_7 &= 0. \end{aligned}$$

A los elementos x_5, x_6, x_7 se les llama "bits" de redundancia y se les conoce como **símbolos de chequeo de paridad** y a las ecuaciones anteriores como *ecuaciones de chequeo de paridad.* La razón de esto es que, por ejemplo, de la primera ecuación del sistema anterior, en un código sobre $\mathbf{F}_2$, sabemos que los símbolos x_1, x_3, x_4 y x_5 deben de sumar 0 módulo 2, esto es deben sumar un número entero par.

Proposición 2.1 [45; 199] *Si G es la matriz generadora del código C, entonces $C^{\perp} = \{\bar{u} \in \mathbf{F}_q^n : \bar{u}G^t = 0\}$, esto es, la matriz generadora de C es la de chequeo de paridad de $C^{\perp}$ y viceversa. Además $C^{\perp}$ es un $[n, n-k]$ código lineal.*

Demostración: Sea $\bar{u} \in C^{\perp}$. Ya que $\bar{u}$ es ortogonal a toda palabra codificada de C si, y sólo si, es ortogonal a toda palabra codificada en una base para C; se tiene la primera afirmación. De lo anterior obtenemos que G^t es la matriz de chequeo de paridad de $C^{\perp}$, de ahí que $C^{\perp}$ sea un $[n, n-k]$ código lineal. □

Proposición 2.2 [34; 6], [45; 200] *Las matrices generadora y de chequeo de paridad de un código lineal C sobre $\mathbf{F}_q$ están relacionadas por las ecuaciones: $HG^t = 0$ y $GH^t = 0$. Además $H = (A, I_{n-k})$ es una matriz de chequeo de paridad de C si y sólo si $G = (I_k, -A^t)$ es la forma estándard de la matriz generadora.*

Demostración: Que $HG^t = 0$ y $GH^t = 0$ es inmediato de la sucesión exacta anterior. Sea $\bar{x} = (x_1, \ldots, x_n)$ la palabra que resulta de codificar el mensaje $(u_1, u_2, \ldots, u_k)$. Si $H = (A, I_{n-k})$ en primer lugar debemos de tener $x_1 = u_1, \ldots, x_k = u_k$ esto es $(x_1, \ldots, x_k)^t = I_k(u_1, \ldots, u_k)^t$.

Por la definición de la matriz de chequeo de paridad, $0 = (A, I_{n-k})\bar{x}^t$, esto es, utilizando la igualdad matricial antes obtenida,

$$(x_{k+1}, \ldots, x_n)^t = -A(x_1, \ldots, x_k)^t = -A(u_1, \ldots, u_k)^t,$$

esto lo podemos expresar en una sola ecuación matricial como

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \left(\frac{I_k}{-A}\right) \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

y transponiendo

$$\bar{x} = \bar{u}G$$

donde

$$G = (I_k, -A^t). \square$$

Para fines de decodificación es conveniente poder hablar de la distancia entre las palabras en el espacio $\mathbf{F}_q^n$, esto lo hacemos introduciendo la llamada métrica de Hamming, pero antes definimos el así llamado peso de Hamming:

Definición 2.4 *El* **peso de Hamming**, *denotado como* $ps(\bar{a})$, *de un elemento* $\bar{a} \in \mathbf{F}_q^n$ *es el número de entradas distintas de cero de* $\bar{a}$.

Por ejemplo si $\bar{a} = (0, 1, 2, 0, 2,) \in \mathbf{F}_3^5$ se tiene $ps(\bar{a}) = 3$.

Ejemplo 2.4 Si $\bar{x}$ y $\bar{y}$ son vectores binarios de la misma longitud, digamos $\bar{x} = (x_1, \ldots, x_n)$ y $\bar{y} = (y_1, \ldots, y_n)$, defínase la **intersección** de $\bar{x}$ y $\bar{y}$ como

$$\bar{x} * \bar{y} = (x_1 y_1, \ldots, x_n y_n).$$

Entonces

$$ps(\bar{x} + \bar{y}) = ps(\bar{x}) + ps(\bar{y}) - 2ps(\bar{x} * \bar{y}),$$

como puede verificarse fácilmente examinando las contribuciones al peso en cada uno de los sumandos de cada pareja de entradas una de $\bar{x}$ y otra de $\bar{y}$.

El peso de Hamming induce una métrica en $\mathbf{F}_q^n$, de la forma siguiente:

Proposición 2.3 [34;9] *La función* $d : \mathbf{F}_q^n \times \mathbf{F}_q^n \longrightarrow \{0, 1, \ldots, n\} \subset \mathbf{R}$ *definida por* $d(\bar{x}, \bar{y}) = ps(\bar{x} - \bar{y})$ *es una métrica en este espacio, la* **métrica de Hamming**.

Demostración: Sean $\bar{x} = (x_1, \ldots, x_n)$, $\bar{y} = (y_1, \ldots, y_n)$ y $\bar{z} = (z_1, \ldots, z_n)$ elementos de $\mathbf{F}_q^n$. Es claro que esta función es no negativa y simétrica. Si $d(\bar{x}, \bar{y}) = 0$ entonces $x_i = y_i$ para todo $i = 1, \ldots, n$ y así $\bar{x} = \bar{y}$.

Por último probemos la desigualdad del triángulo. Sean $\bar{u} = (u_1, \ldots, u_n)$ y $\bar{v} = (v_1, \ldots, v_n)$ elementos de $\mathbf{F}_q^n$, entonces

$$ps(\bar{u}) \leq ps(\bar{u} - \bar{v}) + ps(\bar{v}).$$

En efecto, si para un cierto índice fijo i, u_i no es cero, se tienen dos casos a considerar: v_i es cero o no lo es, en cualquiera de los dos casos $\bar{u}$ y $\bar{v}$ contribuyen con un uno en el miembro derecho de la desigualdad para cada i como se describió. Ahora poniendo $\bar{u} = \bar{x} - \bar{y}$, $\bar{v} = \bar{z} - \bar{y}$ se obtiene

$$ps(\bar{x} - \bar{y}) \leq ps(\bar{x} - \bar{y}) + ps(\bar{z} - \bar{y}).$$

Esto es

$$d(\bar{x}, \bar{y}) \leq d(\bar{x}, \bar{z}) + d(\bar{z}, \bar{y}). \square$$

Una vez que se ha definido una métrica en el espacio estamos en posibilidad de hablar de conceptos asociados a una métrica, por ejemplo de esferas con un centro y radio dados. Se denotará a la **esfera** de centro $\bar{a} \in \mathbf{F}_q^n$ y radio $r \geq 0$ por $B(\bar{a}, r)$. Esto es $B(\bar{a}, r) = \{\bar{b} \in \mathbf{F}_q^n : d(\bar{a}, \bar{b}) \leq r\}$.

Recordemos que si la probabilidad de error es p, tenemos por ejemplo:

$$\text{Prob}\{\bar{e} = (0,0,0,0,0,0)\} = (1-p)^6, \ \text{Prob}\{\bar{e} = (0,0,0,1,0,0)\} = p(1-p)^5.$$

En general, cuando $\bar{v}$ es un vector de peso w se tiene

$$\text{Prob}\{\bar{e} = \bar{v}\} = p^w(1-p)^{n-w}.$$

Ya que $p < \frac{1}{2}$

$$(1-p)^6 > p(1-p)^5 > p^2(1-p)^4 > \cdots$$

Esto es, entre dos vectores de error el que es más probable de ocurrir es aquel de menor peso. Por lo tanto al decodificar una palabra se busca la palabra codificada más cercana (en el sentido de Hamming) a esta.

Ahora es posible introducir un tercer parámetro en la definición de códigos, el cual, como se verá, es de mucha utilidad para conocer la capacidad de un código para corregir errores ocurridos durante la transmisión.

Definición 2.5 La distancia mínima *del código*

$$\phi : \mathbf{F}_q^k \longrightarrow \mathbf{F}_q^n$$

se define como $d = min[\{d(\phi(\bar{a}), \phi(\bar{b})) : \bar{a}, \bar{b} \in \mathbf{F}_q^k\} - \{0\}]$. *Si* C *es un código lineal de dimensión* k, *longitud* n *y distancia mínima* d *diremos que* C *es un* $[n, k, d]$ *código lineal sobre* $\mathbf{F}_q$.

Para un código lineal C no es necesario verificar la distancia entre todo par de palabras codificadas, pues en este caso $d = \min\{ps(\bar{c}) : \bar{c} \in C - \{0\}\}$.

Teorema 2.1 [20; 340], [34; 10] *Sea* C *un* $[n, k, d]$ *código lineal. Entonces el código puede detectar errores de transmisión de peso* $\leq l$, $l \in \mathbf{Z}_0^+$ *si, y sólo si,* $d \geq l + 1$. *Además el código tiene capacidad de corregir errores de transmisión de peso* $\leq [[(d-1)/2]]$, *donde* $[[\cdot]]$ *denota a la función entero mayor. En particular cuando* d *es par, el código puede detectar* $\frac{d}{2}$ *errores y corregir* $\frac{d-2}{2}$ *simultáneamente.*

Demostración: Si la distancia mínima del código es al menos $l + 1$, aún cuando ocurran hasta l errores en la transmisión el mensaje recibido no estará en el código, por lo tanto es posible detectar todos los errores de peso $\leq l$; recíprocamente si $\bar{c}_1$, $\bar{c}_2$ son palabras codificadas tales que $d(\bar{c}_1, \bar{c}_2) < l + 1$, entonces $\bar{c}_1 = \bar{c}_2 + \bar{e}$ donde $ps(\bar{e}) \leq l$. Si al transmitir $\bar{c}_1$ se recibe $\bar{c}_2$ se esperaría que fue esta última palabra la que se envió, produciéndose así un error al detectar un error de peso $\leq l$. Esto prueba la primera parte del teorema.

Supóngase ahora que $d = 3$. Al construir esferas de radio 1 con centro en cada palabra codificada se obtienen esferas ajenas, pues si $\bar{c}_1$ y $\bar{c}_2$ son dos palabras codificadas distintas y $\bar{v} \in B_1(\bar{c}_1) \cap B_1(\bar{c}_2)$ entonces $d(\bar{c}_1, \bar{c}_2) \leq 3$, $d(\bar{c}_1, \bar{v}) \leq 1$ y $d(\bar{c}_2, \bar{v}) \leq 1$ lo cual contradice la desigualdad del triángulo. Si una palabra $\bar{u}$ es transmitida y ocurre un error de tal forma que se recibe un vector $\bar{a}$, entonces este vector está dentro de la esfera con centro en $\bar{u}$, y está más cercana a $\bar{u}$ que a cualquier otra palabra codificada $\bar{v}$. Por lo tanto decodificando como aquella palabra codificada más cercana a la palabra recibida el error será corregido.

Análogamente si $d = 2t + 1$, las esferas de radio t centradas en cada palabra codificada son disjuntas, y el código puede corregir t errores. Ahora supóngase que d es par. Las esferas de radio $\frac{d-2}{2}$ con centro en cada palabra

codificada son ajenas y así el código puede corregir $\frac{d-2}{2}$ errores. Pero si ocurren $\frac{d}{2}$ errores el vector recibido puede equidistar de dos palabras codificadas; en este caso el decodificador sólo podrá detectar que $\frac{d}{2}$ (o más) errores han ocurrido. Por otro lado, si ocurren más de $\frac{d}{2}$ errores el vector recibido puede ser más cercano a alguna otra palabra codificada que a la palabra correcta. Si esto sucede se decodificará incorrectamente. □

Definición 2.6 *Sea C un $[n,k,d]$ código lineal, y sea $t = [[(d-1)/2]]$. Si las esferas de radio t con centro en las palabras codificadas de C son ajenas y su unión contiene a todas las palabras de longitud n, el código se dice* **perfecto.**

Teorema 2.2 [5;37],[34;33] *Sea C un $[n,k,d]$ código lineal, con matriz de chequeo de paridad H. Entonces d es el menor entero r para el cual existen r columnas linealmente dependientes en H; o dicho de otro modo, H tiene d columnas linealmente dependientes y cualesquiera $d-1$ columnas de H son linealmente independientes.*

Demostración: Sea m un entero positivo fijo. Supóngase que $\bar{u}_1, ..., \bar{u}_n$ son las columnas de H, si al elegir m de estas columnas resultan ser linealmente dependientes, entonces existen $c_1, ..., c_n \in \mathbf{F}_q$ tales que

$$c_1\bar{u}_2 + \cdots + c_n\bar{u}_n = 0.$$

Matricialmente esto puede escribirse como $\bar{c}H^t = 0$, donde $\bar{c} = (c_1, \cdots, c_n) \in C$. Ya que $\bar{c}$ tiene peso $\leq m$ debe tenerse que la distancia mínima de C es $\leq m$. Esto lleva a la desigualdad $d \leq m$.

Supóngase ahora que $\bar{c}$ es una palabra codificada de peso m, entonces $\bar{c}H^t = 0$, así que existen m columnas de H las cuales son linealmente dependientes, en particular esto es válido cuando $m = d$. □

Proposición 2.4 [5;29] **(La cota Singleton)** *Para todo $[n,k,d]$ código lineal C sobre $\mathbf{F}_q$ 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.**

Demostración: $n-k$ es el rango de la matriz de chequeo de paridad H de C y es el máximo número de columnas linealmente independientes de H. □

Proposición 2.5 [5;30] **(La cota por empaquetamiento con esferas)** *Para todo* $[n,k,d]$ *código lineal* q*-ario, si* ρ *es el entero mayor de* $(d-1)/2$ *entonces*

$$q^k(1+(q-1)n+(q-1)^2\binom{n}{2}+\cdots+(q-1)^\rho\binom{n}{\rho})\leq q^n.$$

Demostración: El número de palabras en cada esfera con centro en una palabra codificada y radio ρ es

$$1+(q-1)n+(q-1)^2\binom{n}{2}+\cdots+(q-1)^\rho\binom{n}{\rho}.$$

Ya que las q^k esferas son ajenas entre sí y $\mid \mathbf{F}_q^n \mid = q^n$ se cumple la desigualdad.□

El **código extendido** $\hat{C}$ del $[n,k]$ código q-ario C es el código q-ario de longitud $n+1$ consistente de todos los vectores de la forma

$$(c_1,c_2,\ldots,c_n,-\sum_{i=1}^{n}c_i),$$

donde $(c_1,c_2,\ldots,c_n)\in C$. Esta forma de construir un nuevo código se denomina **añadir un chequeo de paridad total** pues si $(c_1,c_2,\ldots,c_{n+1})\in\hat{C}$ entonces $\sum_{i=1}^{n+1}c_i=0$. Si G y H son matrices generadora y de chequeo de paridad para C, respectivamente, entonces la matriz generadora $\hat{G}$ para $\hat{C}$ se obtiene añadiendo a G una columna de tal forma que la suma de las columnas de $\hat{G}$ resulte el vector cero, y la matriz de chequeo de paridad, $\hat{H}$ de $\hat{C}$, puede obtenerse de H agregándole una columna de ceros y un renglón de unos.

Ejemplo 2.5 El código binario $\hat{C}$ con matrices generadora $\hat{G}$ y de chequeo de paridad $\hat{H}$ dadas por

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

es el código extendido del $[5,3]$ código binario C con matriz generadora G y matriz de chequeo de paridad H, donde

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

Sean C_1 un $[n_1, k_1, d_1]$ código y C_2 un $[n_2, k_2, d_2]$ código, dos códigos lineales sobre $\mathbf{F}_q$. Denotaremos al vector $\bar{v}$ escrito enseguida del vector $\bar{u}$ como $\mid \bar{u} \mid \bar{v} \mid$. La suma directa de C_1 y C_2, $C_1 \oplus C_2$, consistirá de todos los vectores de la forma $\mid \bar{u} \mid \bar{v} \mid$ con $\bar{u} \in C_1$ y $\bar{v} \in C_2$. Este código es un $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ código lineal q-ario.

La construcción $\mid \bar{u} \mid \bar{u} + \bar{v} \mid$. Sean C_1 y C_2 como antes y supóngase además que $n_1 = n_2 = n$. Podemos entonces formar un código C_3 consistente de las palabras codificadas

$$\mid \bar{u} \mid \bar{u} + \bar{v} \mid, \ \bar{u} \in C_1 \text{ y } \bar{v} \in C_2.$$

Teorema 2.3 *C_3 es un $[2n, k_1 + k_2, d = \min\{d_1, d_2\}]$ código lineal sobre $\mathbf{F}_q$.*

Demostración: Sean $\bar{a} = \mid \bar{u} \mid \bar{u} + \bar{v} \mid$ y $\bar{b} = \mid \bar{u'} \mid \bar{u'} + \bar{v'} \mid$ dos palabras codificadas distintas de C_3, donde $\bar{u}, \bar{u'} \in C_1$ y $\bar{v}, \bar{v'} \in C_2$. Si $\bar{v} = \bar{v'}$ entonces $d(\bar{a}, \bar{b}) = 2d(\bar{u}, \bar{u'}) \geq 2d_1$. Supongamos pues que $\bar{v}$ es distinto de $\bar{v'}$, entonces

$$\begin{aligned} d(\bar{a}, \bar{b}) &= ps(\bar{u} - \bar{u'}) + ps(\bar{u} - \bar{u'} + \bar{v} - \bar{v'}) \\ &\geq ps(\bar{u} - \bar{u'}) + ps(\bar{v} - \bar{v'}) - ps(\bar{u} - \bar{u'}) \\ &\geq ps(\bar{v} - \bar{v'}) \geq d_2. \ \square \end{aligned}$$

2.2 Decodificación con síndrome

Definición 2.7 *Sea H la matriz de chequeo de paridad de un $[n, k]$ código lineal q-ario C. Para todo $\bar{x} \in \mathbf{F}_q^n$ se define el* **síndrome** *de $\bar{x}$ como $S = H\bar{x}^t$.*

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

Teorema 2.4 [45; 203], [51; 97] *Sean C un $[n, k]$ código lineal sobre $\mathbf{F}_q$ y H una matriz de chequeo de paridad de C. Entonces $\bar{x}$ y $\bar{y} \in \mathbf{F}_q^n$ tienen el mismo síndrome si, y sólo si, están en la misma clase en el espacio cociente $\mathbf{F}_q^n / C$.*

Demostración: Por definición $\bar{x}$ y $\bar{y}$ tienen el mismo síndrome si y sólo si $\bar{x} + C = \bar{y} + C$, esto lo podemos reescribir como $\bar{x} - \bar{y} \in C$, por la definición de código esto es equivalente a tener la igualdad matricial $H(\bar{x} - \bar{y})^t = 0$ o lo que es lo mismo $H\bar{x}^t = H\bar{y}^t$. $\square$

Teorema 2.5 [34; 17] *Para un código lineal binario C, el síndrome es igual a la suma de las columnas de la matriz de chequeo de paridad, H, donde ocurrieron los errores.*

Demostración: El síndrome de $\bar{u} \in \mathbf{F}_q^n$, $S = H\bar{u}^t$, es cero si y sólo si $\bar{u} \in C$, por lo tanto si no ocurren errores, $S = 0$. Ahora si $\bar{u} = \bar{c} + \bar{e}$, donde $\bar{c} \in C$, se tiene

$$S = H\bar{u}^t = H\bar{c}^t + H\bar{e}^t = H\bar{e}^t.$$

Por último, si ocurren errores en las posiciones $i, j, k, \ldots$ digamos, el vector de error es $\bar{e}_i + \bar{e}_j + \bar{e}_k + \cdots$ donde $\bar{e}_t$ es el vector que tiene un 1 en la posición t y cero en las demás, entonces $S = \sum H\bar{e}_\alpha$. □

Ya que es imposible evitar los ruidos en los canales de transmisión siempre habrá la posibilidad de que al enviar un mensaje se produzca algún error. Sin embargo al utilizar teoría de códigos lineales para enviar la información puede suponerse que si no han ocurrido demasiados errores y la palabra recibida no pertenece al código entonces basta con compararla con cada una de las palabras de este y la que más se asemeje debe ser el mensaje enviado. Formalizando esta idea se enuncia la siguiente

Definición 2.8 *Si $\bar{u}$ es una palabra recibida y $\bar{c}$ es una palabra codificada tal que $d = d(\bar{c}, \bar{u})$ es mínima entonces d es llamada* **mínima distancia de decodificación.**

Teorema 2.6 [45; 203] *Sea C un código lineal con matriz de chequeo de paridad H. La distancia mínima de decodificación equivale a decodificar una palabra recibida $\bar{x}$ como una palabra $\bar{c} = \bar{x} - \bar{a}$, donde $\bar{a}$ es una palabra de peso mínimo en la clase $\bar{x} + C$ del espacio cociente $\mathbf{F}_q^n/C$, o dicho de otra manera, $\bar{a}$ es una palabra de menor peso con el mismo síndrome que $\bar{x}$.*

Demostración: Supongamos que la palabra $\bar{x}$ es recibida. Debemos de decodificar $\bar{x}$ como una palabra $\bar{c} \in C$ tal que $\bar{a} = \bar{x} - \bar{c}$ tiene el menor peso; esto es, debemos de decodificar $\bar{x}$ como la palabra $\bar{c} = \bar{x} - \bar{a} \in C$, donde $\bar{a}$ es de peso mínimo en $\bar{x} + C$. □

A continuación se describe el proceso de decodificación, utilizando el concepto de síndrome, descrito en el teorema anterior; se construye el así llamado **arreglo estándard** de C (cf. [34; 16], [45; 203])

$$\begin{array}{rccccc} C: & \mathbf{0} & \bar{c}_1 & \bar{c}_2 & \cdots & \bar{c}_m \\ \bar{a}_1+C: & \bar{a}_1 & \bar{c}_1+\bar{a}_1 & \bar{c}_2+\bar{a}_1 & \cdots & \bar{c}_m+\bar{a}_1 \\ \bar{a}_2+C: & \bar{a}_2 & \bar{c}_1+\bar{a}_2 & \bar{c}_2+\bar{a}_2 & \cdots & \bar{c}_m+\bar{a}_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \bar{a}_s+C: & \bar{a}_s & \bar{c}_1+\bar{a}_s & \bar{c}_2+\bar{a}_s & \cdots & \bar{c}_m+\bar{a}_s \end{array}$$

En el primer renglón aparecen los elementos de C. El i-ésimo renglón es la clase $\bar{a}_i + C$, donde $\bar{a}_i$ es una palabra de peso mínimo que no se encuentra en ninguno de los renglones superiores del arreglo. El proceso es continuado hasta que no hay más palabras $\bar{a}_i \in \mathbf{F}_q^n$ que elegir.

Por lo anteriormente mostrado, si dos palabras se encuentran en el mismo renglón del arreglo entonces tienen el mismo síndrome y viceversa.

A las palabras $\bar{0}, \bar{a}_1, ..., \bar{a}_s$ se les conoce como **dirigentes** o **líderes de clase**.

He aquí la importancia de haber construido así el arreglo:
Supóngase que una palabra $\bar{x}$ es recibida y se encuentra en la j-ésima columna del arreglo estándard, entonces $\bar{x} = \bar{c}_j + \bar{a}_i$ para algún i donde $\bar{a}_i$ tiene peso mínimo en $\bar{x} + C$. La palabra recibida $\bar{x}$ es decodificada como $\bar{c}_j$, esto es, como la palabra codificada en la parte superior de la columna que contiene a $\bar{x}$.

Ya que cada renglón es una clase, todos los miembros de un mismo renglón comparten el mismo síndrome. Así, basta con tener la tabla de los líderes de clase y sus respectivos síndromes para el proceso de decodificación. En efecto si, por ejemplo, la palabra $\bar{x}$ es recibida calculamos su síndrome y es decodificada como $\bar{c} = \bar{x} - \bar{a}_i$, donde a_i es el líder de clase con el mismo síndrome que $\bar{x}$.

Un error en la transmisión será corregido si y sólo si el error corresponde a un dirigente de clase. En efecto supóngase que la palabra codificada $\bar{c}$ es enviada pero se recibe la palabra $\bar{x} = \bar{c} + \bar{e}$, donde $\bar{e}$ es el vector de error. Cuando $\bar{e}$ es un dirigente de clase decodificaremos $\bar{x}$ correctamente como $\bar{x} - \bar{e} = \bar{c}$. Pero si $\bar{e}$ no es un dirigente de clase, entonces debe de estar en, digamos, el j-ésimo renglón del arreglo estándard, y la palabra recibida será decodificada como $\bar{x} - \bar{a}_j$ que es distinta de $\bar{x} - \bar{e} = \bar{c}$, lo cual

es incorrecto, así pues si d es la distancia mínima del código entonces todas las palabras codificadas de peso menor o igual a $[[(d-1)/2]]$ deben aparecer como dirigentes de clase en nuestro arreglo.

Ejemplo 2.6 A continuación se listan las clases del código C con matriz generadora

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

$$\begin{aligned}
(0,0,0,0) + C &= \{(0,0,0,0),(0,1,0,0),(1,1,0,1),(1,0,0,1)\},\\
(1,0,0,0) + C &= \{(1,0,0,0),(1,1,0,0),(0,1,0,1),(0,0,0,1)\},\\
(0,0,1,0) + C &= \{(0,0,1,0),(1,1,1,1),(0,1,1,0),(1,0,1,1)\},\\
(1,0,1,0) + C &= \{(1,0,1,0),(1,1,1,0),(0,1,1,1),(0,0,1,1)\}.
\end{aligned}$$

El arreglo estándard resulta entonces:

$$\begin{array}{cccc}
(0,0,0,0) & (0,1,0,0) & (1,1,0,1) & (1,0,0,1) \\
(1,0,0,0) & (1,1,0,0) & (0,1,0,1) & (0,0,0,1) \\
(0,0,1,0) & (0,1,1,0) & (1,1,1,1) & (1,0,1,1) \\
(1,0,1,0) & (1,1,1,0) & (0,1,1,1) & (0,0,1,1)
\end{array}$$

Una matriz de chequeo de paridad es

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

Con esta podemos crear una tabla de líderes de clase y sus síndromes, por ejemplo $(1,0,1,0)H^t = (1,1)$, así

Líderes de clase	Síndrome
$(0,0,0,0)$	$(0,0)$
$(1,0,0,0)$	$(0,1)$
$(0,0,1,0)$	$(1,0)$
$(1,0,1,0)$	$(1,1)$

Para decodificar una palabra recibida, digamos $\bar{x} = (1,1,1,0)$, calculamos su síndrome $(1,1,1,0) \cdot H^t = (1,1)$; y de acuerdo a la tabla de síndrome el líder de clase es $\bar{a}_i = (1,0,1,0)$, así que decodificamos $\bar{x}$ como

$$\bar{x} - \bar{a}_i = (1,1,1,0) + (1,0,1,0) = (0,1,0,0).$$

2.3 Coeficientes binomiales gaussianos

Definición 2.9 *Sea b un número real distinto de la unidad. Para cada entero no negativo k se define el* **coeficiente binomial gaussiano** b**-ario** $\begin{bmatrix} x \\ k \end{bmatrix}_b$ *como*

$$\begin{bmatrix} x \\ 0 \end{bmatrix}_b = 1,$$

$$\begin{bmatrix} x \\ k \end{bmatrix}_b = \frac{(b^x-1)(b^x-b)\cdots(b^x-b^{k-1})}{(b^k-1)(b^k-b)\cdots(b^k-b^{k-1})}$$

$$= \frac{(1+b+\cdots+b^{x-1})(b+\cdots+b^{x-1})\cdots(b^{k-1}+\cdots+b^{x-1})}{(1+b+\cdots+b^{k-1})(b+\cdots+b^{k-1})\cdots(b^{k-2}+b^{k-1})b^{k-1}}$$

$$= \frac{(b^x-1)(b^{x-1}-1)\cdots(b^{x-k+1}-1)}{(b^k-1)(b^{k-1}-1)\cdots(b-1)} = \prod_{t=0}^{k-1} \frac{b^{x-t}-1}{b^{k-t}-1}$$

El principal interés de estudiar estas cantidades es la información que nos dan sobre ciertas geometrías finitas, como veremos más tarde. Los coeficientes binomiales gaussianos tienen varias propiedades similares a las de los coeficientes binomiales comunes (cf. [34; 444]) pero en el desarrollo del presente trabajo bastará con la que se enuncia en el teorema siguiente.

Teorema 2.7 [34; 444] *El número de $[n, k]$ códigos lineales q-arios distintos es el coeficiente binomial gaussiano q-ario* $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Demostración: Ya que un código lineal es un espacio vectorial el número de códigos de longitud n y dimensión k es el número de formas de elegir k vectores linealmente independientes dividido por el número de bases que generan un mismo espacio de dimensión k.

El número de formas de elegir k vectores linealmente independientes es

$$(q^n - 1)(q^n - q)\cdots(q^n - q^{k-1}).$$

Esto es claro notando que el primer factor cuenta las formas de elegir un vector no cero, $\bar{u}$, en un espacio vectorial de dimensión n, digamos U. El segundo factor cuenta las formas de elegir un vector en $U - \langle \bar{u} \rangle$, y así sucesivamente.

El número de bases en un subespacio de dimensión k es, por un razonamiento análogo al anterior

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1}),$$

por lo tanto el número de $[n, k]$ códigos lineales distintos es

$$\frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})} = \begin{bmatrix} n \\ k \end{bmatrix}_q . \square$$

2.4 El polinomio enumerador de peso

Si α es un elemento de $K = \mathbf{F}_{q^n}$ su **traza**, relativa al subcampo $F = \mathbf{F}_q$, se define como

$$Tr_{K/F}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}.$$

Teorema 2.8 [35;97] *La traza es una función F-lineal de K sobre F tal que, para todo $\alpha \in K$, $Tr_{K/F}(\alpha^q) = Tr_{K/F}(\alpha)$.*

Sea $V = \mathbf{F}_2^n$ junto con el producto interior estándard $\bar{x} \cdot \bar{y} = \sum_1^n x_i y_i$, donde $\bar{x} = (x_1, \ldots, x_n)$ y $\bar{y} = (y_1, \ldots, y_n)$. Para toda función f de V en un anillo conmutativo R, la **transformada de Hadamard** $\hat{f} : V \to R$, de f se define como

$$\hat{f}(\bar{u}) = \sum_{\bar{v} \in V} (-1)^{\bar{u} \cdot \bar{v}} f(\bar{v}).$$

Lema 2.1 [5;66] *Sea C un código binario, con la notación anterior,*

$$\sum_{\bar{u} \in C} \hat{f}(\bar{u}) = \mid C \mid \sum_{\bar{v} \in C^\perp} f(\bar{v}),$$

donde $C^\perp$ es el código dual a C.

Demostración: De la definición de la transformación de Hadamard se sigue que

$$\sum_{\bar{u} \in C} \hat{f}(\bar{u}) = \sum_{\bar{u} \in C} \sum_{\bar{v} \in V} (-1)^{\bar{u} \cdot \bar{v}} f(\bar{v}) = \sum_{v \in V} f(\bar{v}) \sum_{\bar{u} \in C} (-1)^{\bar{u} \cdot \bar{v}}.$$

Si $\bar{v} \in C^{\perp}$ entonces $\bar{u} \cdot \bar{v} = 0$ y la suma interior es $\mid C \mid$. Pero si $\bar{v}$ un vector no en $C^{\perp}$ entonces $\bar{u} \cdot \bar{v}$ toma los valores 0 y 1 el mismo número de veces a medida que $\bar{u}$ varía sobre C (ya que el conjunto de vectores $\bar{u}$ de C para los cuales $\bar{u} \cdot \bar{v} = 0$ es un subgrupo de C de índice 2) y por lo tanto la suma interior es cero. □

Ahora se pretende generalizar este resultado a un campo finito arbitrario. El (-1) en la definición de la transformación de Hadamard, que es una raíz cuadrada de 1, debe de ser reemplazado por una raíz p-ésima de la unidad, para un primo adecuado p. Supóngase que el anillo conmutativo R contiene tal raíz p-ésima de la unidad y sustitúyase el producto interior por la función traza. La prueba de la siguiente proposición es esencialmente la misma que la del lema anterior, tan sólo debe de notarse que la función $u \mapsto Tr(\bar{u} \cdot \bar{v})$, $\bar{v}$ no en $C^{\perp}$, es un funcional $\mathbf{F}_p$-lineal que toma cada valor de $\mathbf{F}_p$ con la misma frecuencia, a saber, q^n/p, donde $\bar{u} \in \mathbf{F}_q^n$.

Proposición 2.6 [5; 167] *Sea R como antes. con $\omega \in R$ una raíz p-ésima primitiva de la unidad, y supóngase que C es cualquier código lineal sobre $\mathbf{F}_q$, donde q es una potencia de p. Sean Tr la traza de $\mathbf{F}_q$ sobre $\mathbf{F}_p$ y $V = \mathbf{F}_q^n$. Para cada función f de V en R se define $\hat{f}$ por*

$$\hat{f}(\bar{u}) = \sum_{\bar{v} \in V} \omega^{Tr(\bar{u} \cdot \bar{v})} f(\bar{v}).$$

Entonces

$$\sum_{\bar{u} \in C} \hat{f}(\bar{u}) = \mid C \mid \sum_{\bar{v} \in C^{\perp}} f(\bar{v}).$$

Definición 2.10 *Sea C un código lineal sobre $\mathbf{F}_q$. Entonces el* **polinomio enumerador de peso** *de C es*

$$W_C(x) = \sum_{\bar{c} \in C} x^{ps(\bar{c})}.$$

Es claro que el coeficiente de x^i es el número de palabras codificadas de peso i, y si C tiene longitud n y existen A_i palabras codifiadas de peso i en C entonces

$$W_C(x) = \sum_{0}^{n} A_i x^i.$$

También son frecuentes las siguientes formas del polinomio enumerador de peso

$$W_C(x,y) = \sum_{\bar{c}\in C} x^{ps(\bar{c})}y^{n-ps(\bar{c})} = \sum_{0}^{n} A_i x^i y^{n-i}.$$

Al conjunto de los A_i no cero se le denomina **distribución de peso** del código.

En general es difícil calcular los enumeradores de peso para un código arbitrario, por ejemplo los enumeradores de peso de los códigos asociados a planos proyectivos de órdenes $2, 3$ y 4 pueden determinarse directamente, pero para los planos de órdenes 5 y 7 aún no han sido determinados, el del plano de orden 8 ya ha sido calculado (cf. [5;82]). Por fortuna existe una manera de calcular el polinomio enumerador de peso del código dual de un código lineal si se conoce la distribución de peso de dicho código

Teorema 2.9 [5;83] (**MacWilliams**) *Los polinomios enumeradores de peso de un código lineal q-ario C y su dual, $C^{\perp}$ están relacionados por la siguiente ecuación*

$$W_{C^{\perp}}(x,y) = \frac{1}{\mid C \mid} W_C(y-x, y+(q-1)x).$$

Demostración: Sea R el anillo de polinomios en x y y sobre los números complejos (o cualquier campo con una raíz p-ésima primitiva de la unidad), y sea q una potencia de p. Para cualquier vector $\bar{v}$ del espacio V, en el cual C está inmerso, sea

$$f(\bar{v}) = x^{ps(\bar{v})}y^{n-ps(\bar{v})}.$$

Defínase la función w de $F = \mathbf{F}_q$ en $\mathbf{Z}$ de la siguiente manera:

$$w(0) = 0, \quad w(a) = 1, \text{ para } a \text{ distinto de cero,}$$

entonces, para $\bar{v} = (v_1, \ldots, v_n)$ se cumple $ps(\bar{v}) = \sum_1^n w(v_i)$. Con la notación de la proposición anterior se tiene

$$\hat{f}(\bar{u}) = \sum_{\bar{v}\in V} x^{ps(\bar{v})}y^{n-ps(\bar{v})}\omega^{Tr(\bar{u}\cdot\bar{v})}$$

y, en términos de la función w, esto puede escribirse como

$$\sum_{v_1,\ldots,v_n\in F} x^{w(v_1)+\cdots+w(v_n)}y^{(1-w(v_1))+\cdots+(1-w(v_n))}\omega^{Tr(u_1v_1+\cdots+u_nv_n)}$$

o bien como

$$\prod_{i=1}^{n} \sum_{v_i \in F} x^{w(v_i)} y^{1-w(v_i)} \omega^{Tr(u_i v_i)}.$$

Cuando $u_i = 0$, la suma interior es $y + (q-1)x$ y cuando no lo es la suma es

$$y - x(\frac{q}{p} \sum_{i=0}^{p-1} \omega^i - 1) = y - x + \frac{q}{p}(1 + \omega + \cdots + \omega^{p-1}) = y - x.$$

De ahí que

$$\hat{f}(\bar{u}) = (y-x)^{ps(\bar{u})}(y + (q-1)x)^{n-ps(\bar{u})},$$

y por la proposición anterior se tiene el resultado deseado. □

3 Códigos cíclicos

Los códigos cíclicos fueron descubiertos por E. Prange en 1957, y aparecen descritos por primera vez en la referencia [39].

3.1 Generalidades

Definición 3.1 *Se dice que un* $[n, k, d]$ *código lineal sobre* $\mathbf{F}_q$ *es* **cíclico** *si cualquier corrimiento cíclico de una palabra codificada sigue estando en el código; esto es, si* $(c_0, c_1, ..., c_{n-1}) \in C$ *implica que* $(c_{n-1}, c_0, ..., c_{n-2}) \in C$.

En lo que resta de este trabajo un vector se denotará como una n-ada o bien como una cadena, por ejemplo el vector $(1, 3, 0, 1)$, sobre el campo adecuado y en la base elegida, también se dentotará como 1301.

De aquí en adelante denotaremos al elemento $a_m x^m + a_{m-1}x^{m-1} + \cdots a_1 x + a_0 + \langle x^n - 1\rangle$ del anillo cociente $\mathbf{F}_q[x]/\langle x^n - 1\rangle$ como $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$. (Se supone que este último polinomio ya ha sido reducido módulo $x^n - 1$).

La función

$$\psi : \mathbf{F}_q^n \longrightarrow R_n = \mathbf{F}_q[x]/\langle x^n - 1\rangle$$

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots a_{n-1}x^{n-1}$$

es un isomorfismo de $\mathbf{F}_q$-espacios vectoriales con la siguiente propiedad:

Proposición 3.1 [34; 189] *Un* $[n, k, d]$ *código lineal* q*-ario* C *es cíclico si y sólo si* $\psi(C)$ *es un ideal de* R_n.

Demostración: Supóngase que el código C es cíclico. Obviamente $\psi(C)$ es un grupo aditivo abeliano. Sea $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \psi(C)$ entonces su imagen inversa bajo ψ es $(a_0, a_1, \ldots, a_{n-1}) \in C$, de ahí que $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ también está en C y la imágen de este último es $a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} = x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1})$. Esto prueba la primera parte de la proposición ya que pedir la cerradura de $\psi(C)$ bajo la multiplicación por los polinomios en R_n es equivalente a pedir su cerradura bajo la multiplicación por escalares y la indeterminada.

Inversamente supóngase ahora que $\psi(C)$ es un ideal de R_n. Si la n-ada $(a_0, a_1, \ldots, a_{n-1})$ está en C entonces

$$\psi(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \psi(C)$$

y $x(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-2} \in \psi(C)$ por lo que la imagen inversa de este último, que es $(a_{n-1}, a_0, \ldots, a_{n-2})$, está en C. □

Para cada polinomio $f(x) \in \mathbf{F}_q[x]$ el ideal generado por $f(x)$ se denotará como $\langle f(x) \rangle$.

Antes de seguir adelante detengámonos un momento para recordar algunos resultados de Álgebra: (para su prueba pueden consultarse [8], [17], [32], [34], [35] y [45])

1.-Denotemos por K un campo arbitrario. Si I es un ideal de $\mathbf{K}[x]$, entonces el anillo cociente $\mathbf{K}[x]/I$ es un dominio de ideales principales.

2.-Existe una correspondencia biyectiva entre los ideales de $\mathbf{K}[x]/I$ y los ideales de $\mathbf{K}[x]$ que contienen a I, dada por $J \mapsto J/I$, donde J es un ideal de $\mathbf{K}[x]$ que contiene a I. Además esta correspondencia preserva la contención de ideales.

3.-En particular si $I = \langle f(x) \rangle$ entonces los ideales de $\mathbf{K}[x]/I$ son $\langle f_i(x) \rangle$, donde los polinomios $f_i(x)$ son los divisores de $f(x)$ en el anillo $\mathbf{K}[x]$.

4.-El polinomio minimal de $\alpha \in \mathbf{F}_{q^n}$ sobre $\mathbf{F}_q$ es

$$irr(\alpha, \mathbf{F}_q) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{d-1}}),$$

donde d es el menor entero positivo para el cual $\alpha^{q^d} = \alpha$.

Enseguida se describe un método para factorizar el polinomo $x^n - 1$ sobre $\mathbf{F}_q$ (cf. [13; 59], [45; 310]). Como veremos, conocer esto nos permite determinar todos los códigos cíclicos. En primer lugar puede suponerse que n y q son primos relativos, pues si $n = kq$ entonces $x^n - 1 = (x^k - 1)^q$. Derivando $x^n - 1$ obtenemos nx^{n-1} el cual es primo relativo a $x^n - 1$ pues $(n, q) = 1$, por lo tanto todos los ceros de $x^n - 1$ son distintos.

Si $\mathbf{F}_{q^d}$ es el campo de descomposición para $x^n - 1$ sobre $\mathbf{F}_q$, entonces d es el menor entero positivo para el cual $q^d \equiv 1 \ (mod\ n)$. A tal entero d se le llama el **orden de q módulo n** y se denota por $o_n(q)$.

Sean $d = o_n(q)$ y β un elemento primitivo de $\mathbf{F}_{q^d}$ (es decir β es un elemento generador del grupo multiplicativo $\mathbf{F}_{q^d} - \{0\}$), entonces $\omega = \beta^{(q^d-1)/n}$ es una raíz n-ésima primitiva de la unidad en el mismo campo. Por lo tanto las raices de $x^n - 1$ son

$$1, \omega, \omega^2, \ldots, \omega^{n-1}.$$

La factorización de $x^n - 1$ resulta entonces el mínimo común múltiplo de los polinomios minimales de estos elementos. Si para $i = 0, \ldots, n-1$ denotamos por $m_i(x)$ el polinomio minimal para ω^i entonces

$$m_i(x) = (x - \omega^i)(x - \omega^{iq})(x - \omega^{iq^2}) \cdots (x - \omega^{iq^{d-1}}),$$

donde d es el menor entero positivo para el cual $iq^d \equiv i \ (mod\ n)$. Defínase la **i-ésima clase ciclotómica** para q módulo n como

$$C_i = \{i, iq, iq^2, \ldots, iq^{d-1}\},$$

por lo tanto si $i \in C_k$ entonces $m_i(x) = \prod_{j \in C_k}(x - \omega^j)$

Ya que todo ideal en R_n es principal, todo código cíclico es generado por un único polinomio.

Podemos ahora enunciar el primer resultado de esta sección.

Teorema 3.1 [34; 190] *Sea C un código cíclico de longitud n sobre $\mathbf{F}_q$ (o sea un ideal de R_n).*

a) *Existe un único polinomio mónico de grado minimal $g(x)$, tal que $\langle g(x) \rangle = C$, el cual es llamado el* **polinomio generador** *para C.*

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

c) *Si $g(x)$ es de grado r, todo $c(x) \in C$ puede ser escrito de manera única como $c(x) = f(x)g(x)$ en $\mathbf{F}_q[x]$, donde $f(x) \in \mathbf{F}_q[x]$ es de grado menor que $n - r$. En otras palabras el mensaje $f(x)$ se codifica como $f(x)g(x)$. Además* $\dim(C) = n - r$.

d) *Si $g(x) = g_0 + g_1 x + \cdots + g_r x^r$, la matriz generadora del código es*

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

o bien usando la notación obvia

$$G = \begin{pmatrix} g(x) & & & \\ & xg(x) & & \\ & & \cdots & \\ & & & x^{n-r-1}g(x) \end{pmatrix},$$

donde las entradas en blanco de la matriz son ceros.

Demostración: El primer inciso es claro pues el código C es un ideal del dominio de ideales principales R_n. Para el segundo inciso, ya que $\mathbf{F}_q[x]$ es un dominio euclideano, escribamos, en este anillo, $x^n-1 = q(x)g(x)+r(x)$, donde el grado de $r(x) < r$. Pero en R_n esto significa que $r(x) = -q(x)h(x) \in C$, lo cual no es posible a menos que $r(x) = 0$.

Ahora sólo resta probar c) y d): De (a) vemos que si $c(x) \in C$ tiene grado $< n$, entonces es de la forma $q(x)g(x)$ en R_n, así que $c(x) = q(x)g(x)+e(x)(x^n-1) = [q(x)+e(x)h(x)]g(x) = f(x)g(x)$ en $\mathbf{F}_q[x]$, donde $f(x)$ es un polinomio de grado $\leq n-r-1$. De ahí que el código consiste de múltiplos de $g(x)$ por polinomios de grado $\leq n-r-1$, en $\mathbf{F}_q[x]$. Los polinomios $g(x), xg(x), ..., x^{n-r-1}g(x)$ son linealmente independientes, por lo tanto el código tiene dimensión $n-r$. □

Ejemplo 3.1 El código cíclico con polinomio generador x^2+1 sobre el anillo $R_4 = \mathbf{F_2}[x]/\langle x^4-1\rangle$, como puede comprobarse por simple cálculo es

$$C = \{0, x^2+1, x^3+x, x^3+x^2+x+1\} = \{0000, 0101, 1010, 1111\}.$$

Ejemplo 3.2 Analicemos el código cíclico C con polinomio generador $\langle 1+x\rangle$ en $R_3 = F_2[x]/\langle x^3-1\rangle$. C es de dimensión 2, y consta de las palabras

$$C = \{0, 1+x, x+x^2, 1+x^2\} = \{000, 110, 101, 011\}.$$

Ya que $1+x^2 = (1+x)^2$ se da la contención $\langle 1+x^2\rangle \subseteq \langle 1+x\rangle$. Sin embargo debemos notar que $x(1+x^2) = x+1$, $(1+x)(1+x^2) = x+x^2$, $x^2(1+x^2) = x^2+x$, $(1+x^2)^2 = 1+x$ y por último $(1+x+x^2)(1+x^2) = 0$. Esto lo que significa es que C es generado por otro polinomio aparte del polinomio generador, a saber $1+x^2$.

El ejemplo anterior nos lleva naturalmente a la pregunta de cuándo un polinomio es generador para un código cíclico (esto es un polinomo mónico de grado mínimo en R_n que genere al código), la respuesta la da el

Teorema 3.2 [45;323] *Un polinomio mónico $p(x) \in R_n$ es un polinomio generador para un código cíclico C si y sólo si $p(x)$ divide a $x^n - 1$.*

Demostración: Sea $x^n - 1 = q(x)p(x) + r(x)$ con $\text{grad}(r(x)) < r$. Entonces $q(x)p(x) \equiv -r(x) \bmod(x^n - 1)$, esto es $r(x) \in C$ lo cual sólo es posible si $r(x) = 0$.

Recíprocamente, supóngase que $p(x)$ divide a $x^n - 1$, y que $g(x)$ es un polinomio generador para el código $\langle p(x) \rangle$. Supóngase además que $p(x)$ y $g(x)$ son distintos, en particular esto significa que el grado de $p(x)$ es mayor que el de $g(x)$. Por hipótesis existe un polinomio $f(x)$ tal que $x^n - 1 = p(x)f(x)$, además también existe un polinomio $h(x)$ tal que $g(x) \equiv h(x)p(x) \bmod(x^n - 1)$. Así que

$$f(x)g(x) \equiv h(x)p(x)f(x) \equiv h(x)(x^n - 1) \equiv 0, \bmod(x^n - 1)$$

pero $\text{grad}(g(x)f(x)) < \text{grad}(p(x)f(x)) = n$, por lo que $g(x)f(x) = 0$; ya que esto no es posible, se concluye que $p(x) = g(x)$. □

Supóngase que $x^n - 1 = \prod_i m_i(x)$, donde los $m_i(x)$ son polinomios mónicos irreducibles sobre $\mathbf{F}_q$. Para cada cero, digamos α, de un $m_i(x)$ en un campo de extensión de $\mathbf{F}_q$, $m_i(x)$ es el polinomio minimal de dicho cero sobre $\mathbf{F}_q$, y para $f(x) \in \mathbf{F}_q[x]$, se tiene que $f(\alpha) = 0$ si y sólo si $f(x) = q(x)m_i(x)$, para algún polinomio $q(x) \in \mathbf{F}_q[x]$.

En particular cuando $f(x) \in R_n$, entonces $f(\alpha) = 0$ si y sólo si $f(x) \in \langle m_i(x) \rangle$ (aquí pensamos al polinomio $f(x)$ reducido módulo $x^n - 1$ no como una clase lateral). Se ha probado el siguiente

Teorema 3.3 [45;327] *Sea $g(x) = q_1(x) \cdots q_t(x)$ el producto de t factores irreducibles de $x^n - 1$, y sea $\alpha_1, \cdots, \alpha_u$ el conjunto de las raices de $g(x)$ en el campo de descomposición de $x^n - 1$ sobre $\mathbf{F}_q$. Entonces*

$$\langle g(x) \rangle = \{f(x) \in R_n : f(\alpha_1) = 0, ..., f(\alpha_u) = 0\}$$

Además si β_i es una raíz de $q_i(x)$ para $i = 1, ..., t$ entonces

$$\langle g(x) \rangle = \{f(x) \in R_n : f(\beta_1) = 0, ..., f(\beta_t) = 0\}.$$

Definición 3.2 *Las raices del polinomio generador de un código cíclico de longitud n son llamadas* **ceros del código**, *todas las otras raices de $x^n - 1$ son llamadas* **no ceros del código**.

Supóngase que $\alpha_1, ..., \alpha_u$ son raices n-ésimas de la unidad, en el campo de extensión $\mathbf{F}_{q^d}$. Si $f(x) = \sum f_i x^j$ es un elemento en R_n entonces α_i es un cero de f si y sólo si $\sum_j f_j \cdot \alpha_i^j = 0$.

Por otra parte $\mathbf{F}_{q^d}$ es un espacio vectorial de dimensión d sobre $\mathbf{F}_q$, así que cada una de las potencias α_i^j pueden escribirse como un vector columna $[\alpha_i^j]$ de longitud d sobre $\mathbf{F}_q$. Además como $f_j \in \mathbf{F}_q$, se tiene $[f_j \cdot \alpha_i^j] = f_j \cdot [\alpha_i^j]$ de ahí que

$$\sum_j f_j \cdot \alpha_i^j = 0 \Longleftrightarrow \sum_j f_j \cdot [\alpha_i^j] = [\sum_j f_j \cdot \alpha_i^j] = 0,$$

si se definen

$$H = \begin{pmatrix} [1] & [\alpha_1^1] & \cdots & [\alpha_1^{n-1}] \\ [1] & [\alpha_2^1] & \cdots & [\alpha_2^{n-1}] \\ \vdots & \vdots & \vdots & \vdots \\ [1] & [\alpha_u^1] & \cdots & [\alpha_u^{n-1}] \end{pmatrix}$$

y $\bar{f} = (f_0, f_1, ..., f_{n-1})$ entonces $\bar{f}(\alpha_i) = 0$, para $i = 1, ..., u$ si y sólo si $H\bar{f}^t = 0$. Por lo tanto el conjunto de n-adas $\bar{f} = (f_0, f_1, \ldots, f_{n-1})$, tales que $\sum f_i x^i \in R_n$ tiene a $\alpha_1, \ldots, \alpha_u$ como ceros es un espacio vectorial (el núcleo de H), de ahí que H es una matriz de chequeo de paridad para tal espacio vectorial, el cual por definición es un código lineal. Esta es la manera de recuperar una matriz de chequeo de paridad de un código cíclico conociendo los ceros de código.

3.2 Polinomio de chequeo de paridad

Ya sabemos que si $g(x)$ es el polinomio generador de un código cíclico C entonces este polinomio divide a $x^n - 1$, por lo tanto $\frac{x^n-1}{g(x)}$ es un polinomio, digamos $h(x) = h_0 + h_1 x + \cdots h_k x^k$. Este es el llamado **polinomio de chequeo de paridad** de C.

Supóngase que $c(x) = \sum_{i=0}^{n-1} c_i x^i \in C$, esto es $c(x) = f(x)g(x)$ para algún elemento $f(x) \in R_n$; entonces

$$c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) = 0. \qquad \text{en } R_n.$$

Por otra parte el coeficiente de x^i en este producto es

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0, \qquad j = 0, 1, \ldots, n-1,$$

cada una de estas relaciones es conocida como ecuación de chequeo de paridad del código. Si

$$H = \begin{pmatrix} & & h_k & \cdots & h_2 & h_1 & h_0 \\ & h_k & \cdots & h_2 & h_1 & h_0 & \\ \cdots & \cdots & \cdots & \cdots & \cdots & & \\ h_k & \cdots & h_2 & h_1 & h_0 & & \end{pmatrix}$$

de las ecuaciones anteriores, para que $\bar{c} = (c_0, \ldots, c_{n-1}) \in C$ es suficiente que $H\bar{c}^t = 0$. Es más, esta condición es también necesaria ya que los renglones de H son linealmente independientes, (en efecto pues así lo son los polinomios $h(x)$, $xh(x), \ldots, x^{n-r-1}h(x)$), y $k = \text{grad}(h(x)) = n - \text{grad}(g(x))$, la dimensión de C. Por lo tanto H es una matriz de chequeo de paridad para C.

Ejemplo 3.3 Considérese el código cíclico sobre $\mathbf{F}_2$ con polinomio generador $x^3 + x^2 + 1 \in R_7 = \mathbf{F}_2[x]/\langle x^7 - 1\rangle$, (como se verá más tarde este es un código binario de Hamming). El polinomio de chequeo de paridad de este código es $(x-1)(x^3+x+1) = x^4 + x^3 + x^2 + 1$, por lo tanto

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

es una matriz de chequeo de paridad para el código.

A partir del razonamiento precedente podemos deducir inmediatamente que para un código la propiedad de ser cíclico es invariante bajo ortogonalidad, en efecto

Teorema 3.4 [45; 196] *Sea C un código cíclico con polinomio de chequeo de paridad $h(x)$, y sea h_k el coeficente líder de $h(x)$. Entonces el código dual $C^\perp$ es equivalente al código cíclico con polinomio generador $g^\perp(x) = h_k^{-1} x^{\text{grad}(h(x))} h(x^{-1})$.*

Demostración: Supóngase que $h(x) = h_0 + h_1 x + \cdots h_k x^k$. La matriz

$$G = \begin{pmatrix} g^{\perp}(x) & & & \\ & xg^{\perp}(x) & & \\ & & \cdots & \\ & & & x^{n-r-1}g^{\perp}(x) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & h_k^{-1}h_{k-1} & h_k^{-1}h_{k-2} & \cdots & h_k^{-1}h_0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & h_k^{-1}h_{k-1} & \cdots & h_k^{-1}h_1 & h_k^{-1}h_0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & & & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & h_k^{-1}h_{k-1} & \cdots & h_k^{-1}h_1 & h_k^{-1}h_0 \end{pmatrix}$$

se obtiene de la matriz H definida al principio de la sección por una permutación de sus columnas. (Recuérdese que la matriz H es una matriz generadora para $C^{\perp}$). □

Ejemplo 3.4 El polinomio generador para el código del ejemplo anterior es

$$g^{\perp}(x) = x^4(x^{-4} + x^{-3} + x^{-2} + 1) = 1 + x + x^2 + x^4.$$

3.3 Polinomios de Mattson-Solomon

Esta sección está basada en [45; 342] por lo que se omiten las referencias de cada resultado. Sea ω una raíz n-ésima primitiva de la unidad sobre F_q. Un **polinomio de Mattson-Solomon** $p_{ms}(x)$ es un polinomio asociado a otro polinomio $p(x) \in R_n$ de la siguiente manera:

$$p_{ms}(x) = \sum_{i=0}^{n-1} p(\omega^{-i})x^i = p(1) + p(\omega^{-1})x + p(\omega^{-2})x^2 + \cdots + p(\omega^{-(n-1)})x^{n-1}.$$

Los polinomios de Matson-Solomon también pueden ser escritos como

$$p_{ms}(x) = \sum_{i=0}^{n-1} p(\omega^{n-i})x^i = \sum_{i=1}^{n} p(\omega^i)x^{n-i}.$$

Si $p(x) = \sum p_j x^j$ y $p_{ms}(x) = \sum \tilde{p}_i x^i$ entonces

$$\sum_{i=0}^{n-1} \tilde{p}_i x^i = p_{ms}(x) = \sum_{i=0}^{n-1} p(\omega^{-i})x^i = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p_j(\omega^{-ij})x_i$$

lo que puede escribirse matricialmente como

$$\begin{pmatrix} \tilde{p}_{n-1} \\ \tilde{p}_{n-2} \\ \vdots \\ \tilde{p}_1 \\ \tilde{p}_0 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^{n-2} & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{n-4} & \omega^{n-2} \\ \vdots & & & \vdots & & \vdots \\ 1 & \omega^{n-1} & \omega^{n-2} & \cdots & \omega^2 & \omega \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-2} \\ p_{n-1} \end{pmatrix}.$$

El siguiente resultado muestra la forma de recuperar un polinomio a partir de su polinomio de Mattson-Solomon.

Teorema 3.5 *Si $p(x)$ es un polinomio en R_n entonces*

$$p(x) = \frac{1}{n} \sum_{i=0}^{n-1} p_{ms}(\omega^i) x^i.$$

Demostración: En primer lugar se probará que $\sum_{j=0}^{n-1} \omega^{-j(k-i)} = n\delta_{k-i,0}$, para $k = i, i+1, \ldots, i+n-1$, donde $\delta_{i,j}$ es la función delta de Kronecker. En efecto, si $k - i = 0$ entonces $\sum_{j=0}^{n-1} 1^{-j} = n = n\delta_{0,0}$, por otra parte si $\mid k-i \mid > 0$ entonces $k-i < n$ esto es ω^{k-i} no es 1 por lo tanto $\sum_{j=0}^{n-1} \omega^{-(k-i)j} = \frac{1-[\omega^{-(k-i)}]^n}{1-\omega^{-(k-i)}} = 0$.

Ahora si $p(x) = \sum p_i x^i$ entonces

$$\frac{1}{n} \sum_{j=0}^{n-1} p(\omega^{-j}) \omega^{ij} = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} p_k \omega^{-jk} \omega^{ij} = \frac{1}{n} \sum_{k=0}^{n-1} p_k \sum_{j=0}^{n-1} \omega^{-j(k-i)},$$

aplicando el resultado antes obtenido

$$\frac{1}{n} \sum_{j=0}^{n-1} p(\omega^{-j}) \omega^{ij} = \frac{1}{n} \sum_{k=0}^{n-1} p_k n \delta_{k-i,0} = p_i.$$

Así pues

$$\frac{1}{n} p_{ms}(\omega^i) = \frac{1}{n} \sum_{j=0}^{n-1} p(\omega^{-j})(\omega^{ij}) = p_i.$$

Y el polinomio $p(x)$ viene dado como

$$p(x) = \frac{1}{n} \sum_{i=0}^{n-1} p_{ms}(\omega^i) x^i. \; \square$$

Sea $\psi : \mathbf{F}_q^n \to R_n$ la función definida en la página 26, se define el peso de $p(x) \in R_n$ como el peso de $\psi^{-1}(p(x))$. Los siguientes corolarios muestran algunas aplicaciones de los polinomios de Mattson-Solomon. Ya que los primeros dos son inmediatos del teorema anterior no se da su prueba.

Corolario 3.1 *El peso de $p(x) \in R_n$ es igual a $n - s$, donde s es el número de ceros de p_{ms} entre las raices n-ésimas de la unidad.*

Corolario 3.2 *El peso de $p(x) \in R_n$ es $\geq n - grad(p_{ms}(x))$.*

Corolario 3.3 (La cota BCH) *Sea ω una raíz n-ésima primitiva de la unidad sobre $\mathbf{F}_q$. Sea C un código cíclico en R_n, cuyo polinomio generador $g(x)$ es el polinomio mónico de menor grado sobre $\mathbf{F}_q$ que tiene a los elementos*

$$\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$$

entre sus ceros, donde $b \geq 1$ y $b + \delta - 1 < n$. Entonces C tiene distancia mínima al menos δ.

Demostración: Sean $d = \delta - 1$ y $c(x) \in C$. Ya que $g(x)$ divide a $c(x)$, se tiene $c(\omega^i) = 0$ para $i = b, \ldots, b + d - 1$. De ahí que $c_{ms}(x) = \sum_{i=1}^{n} c(\omega^i) x^{n-i}$ es igual a

$$c_{ms}(x) = c(\omega)x^{n-1} + \ldots + c(\omega^{b-1})x^{n-b+1} + c(\omega^{b+d})x^{n-b-d} + \ldots + c(\omega^n).$$

Ahora, multiplicando por x^{b-1} se obtiene que $x^{b-1}c_{ms}(x)$ es igual a

$$\begin{aligned} &c(\omega)x^{n+b-2} + \ldots + c(\omega^{b-1})x^n + c(\omega^{b+d})x^{n-d-1} + \ldots + c(\omega^n)x^{b-1} \\ &= x^n[c(\omega)x^{b-2} + \ldots + c(\omega^{b-1})] + \{c(\omega^{b+d})x^{n-d-1} + \ldots + c(\omega^n)x^{b-1}\}. \end{aligned}$$

Denotando por $p(x)$ al polinomio entre corchetes y por $q(x)$ al polinomio entre llaves, entonces la igualdad anterior puede ser escrita como

$$x^{b-1}c_{ms}(x) = x^n p(x) + q(x) = (x^n - 1)p(x) + p(x) + q(x).$$

Esta ecuación muestra que ω^i es una raíz de c_{ms} si y sólo si es una raíz del polinomio $p(x) + q(x)$, el cual tiene grado $n - d - 1$ pues $b + d - 1 < n$ implica que $b - 2 < n - d - 1$. Luego $c_{ms}(x)$ no tiene más de $n - d - 1$ raices entre las raices n-ésimas de la unidad, y por el corolario anterior el peso de $c(x)$ es al menos $n - (n - d - 1) = d + 1$. □

Este corolario muestra como puede obtenerse un código con distancia mínima al menos una cantidad predeterminada δ, dando su polinomio generador con $\delta - 1$ ceros consecutivos, o sea potencias consecutivas de una raíz n-ésima de la unidad. El corolario puede ser generalizado como sigue.

Teorema 3.6 *Sea ω una raíz n-ésima de la unidad. Sea C un código cíclico en R_n, cuyo polinomio generador $g(x)$ es el polinomio mónico de menor grado que contiene a los $\delta - 1$ elementos*

$$\omega^b, \omega^{b+r}, \ldots, \omega^{b+(\delta-2)r}$$

entre sus ceros, donde $(r, n) = 1, b \geq 1$ y $b + (\delta - 2)r < n$. Entonces C tiene distancia mínima al menos δ.

Demostración: Sea $\beta = \omega^r$, $(r, n) = 1$. Entonces β es una raíz n-ésima de la unidad, por lo tanto $\omega^b = \beta^t$ para algún entero t, y el código tiene ceros $\beta^t, \beta^{t+1}, \ldots, \beta^{t+\delta-2}$, esto reduce el problema al corolario anterior. □

3.4 Códigos de Hamming

Estos códigos fueron descubiertos por Marcel Golay en 1949 (cf. [18]), y generalizan a los códigos binarios descubiertos por Richard Hamming (cf. [24]), por lo que llevan el nombre de este último. Se desea construir un código perfecto (ver definición 2.6) sobre el espacio $\mathbf{F}_q^r$ capaz de corregir un error, lo cual nos lleva, por el teorema 2.2, a pedir distancia mínima tres. Para esto basta con que la matriz de chequeo de paridad del código no tenga dos columnas linealmente dependientes.

Definición 3.3 *Dado un entero $r \geq 2$, el* **código de Hamming** $\mathcal{H}_r(q)$ *sobre el campo $\mathbf{F}_q$, es el código q-ario que tiene una matriz de chequeo de paridad de r por $(q^r - 1)/(q - 1)$ cuyas columnas son representantes no cero de cada uno de los subespacios de dimensión 1 de $\mathbf{F}_{q^r}$, cada uno apareciendo una sola vez.*

En particular un código binario de Hamming $\mathcal{H}_r(2) = \mathcal{H}_r$ de longitud $n = 2^r - 1$, $(r \geq 2)$ tiene como matriz de chequeo de paridad H aquella cuyas columnas son todos los vectores binarios no cero de longitud r, cada uno apareciendo exactamente una vez, es decir las columnas de H son precisamente los elementos de $\mathbf{F}_2^r - \{\mathbf{0}\}$. Claramente $\mathcal{H}_r$ es un $[n = 2^r - 1, k = 2^r - 1 - r, d = 3]$ código. En general se tiene el siguiente

Teorema 3.7 [5; 58] *El código q-ario $\mathcal{H}_r(q)$ es un*

$$[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$$

código perfecto, capaz de corregir un error.

Demostración: Ya que el número de subespacios de $\mathbf{F}_q^r$ con dimensión 1 es $n = (q^r-1)/(q-1)$, esta es precisamente la longitud del código. Por otro lado $\mathbf{F}_{q^r}$ es de grado r sobre $\mathbf{F}_q$, de ahí que esta es la dimensión del espacio columna de H, esto es el rango de H es r, por lo que la dimensión del código es $n-r$. Además como ningún par de columnas de H son linealmente dependientes la distancia mínima ciertamente no es 2, es más si elegimos las columnas, correspondientes a $\bar{u}$ y $\bar{v}$, digamos, entonces también aparecerá en H la columna correspondiente a $\bar{u}+\bar{v}$, por lo cual la distancia mínima de $\mathcal{H}_q(r)$ es 3, de ahí que corrija un error.

El número de vectores de $\mathbf{F}_q^r$ contenidos las esferas de radio 1 con centro en cada una de las palabras codificadas es, por ser ajenas las esferas,

$$q^{n-r}(1+(q-1)n) = q^{n-r}(1+(q^r-1)) = q^n.$$

esto muestra que el código es perfecto. □

Ejemplo 3.5 El $[7,4,3]$ código binario de Hamming $\mathcal{H}_3$ tiene matriz de chequeo de paridad

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

Nótese que si vemos a las columnas de H como las expresiones binarias de números naturales las tenemos ordenadas naturalmente, o escribiéndola en forma estándard

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

A continuación se listan los mensajes w y su codificación respectiva utilizando esta última matriz

1001	1001001		1010	1010101	000	0000000
1000	1000110		0110	0110110	111	1111111
0100	0100101		1011	1011010		
0010	0010011		0111	0111001		
0101	0101010		0001	0001111		
0011	0011100		1101	1101100		
1110	1110000		1100	1100011		

Figura 1. El código $\mathcal{H}_3$.

Arreglando las columnas de una matriz de chequeo de paridad de un código binario de Hamming de tal forma que la i-ésima columna sea la expansión binaria de i, decodificar un mensaje es bastante sencillo. Por ejemplo si $\bar{x}$ es la palabra recibida, primero se calcula su síndrome, si éste es 0 se decodifica como $\bar{x}$, pero si no es así entonces se supone que ha ocurrido precisamente un error en la i-ésima posición, donde i es la representación binaria del síndrome de $\bar{x}$, y se decodifica esta palabra como $\bar{x} + \bar{e}_i$, donde $\bar{e}_i$ es el vector con un 1 en la posición i-ésima y cero en las demás.

Ejemplo 3.6 *Sea* $\mathbf{F}_4 = \{0, 1, \omega, \omega^2 = \omega + 1\}$, *entonces el* $[5, 3, 3]$ *código de Hamming sobre* $\mathbf{F}_4$ *tiene matriz de chequeo de paridad*

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

Teorema 3.8 [11;52],[51;46] *Todo código binario de Hamming,* $\mathcal{H}_r$, *es cíclico, y su polinomio generador es el polinomio minimal sobre* $\mathbf{F}_2$ *de un elemento primitivo de* $\mathbf{F}_{2^r}$.

Demostración: Sea α un elemento primitivo de $\mathbf{F}_{2^r}$. Entonces los elementos no cero de este campo son $1, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}$, y utilizando el isomorfismo canónico entre el $\mathbf{F}_2$-espacio $\mathbf{F}_2^r$ y el campo $\mathbf{F}_{2^r}$, cada uno de estos elementos pueden ser representados como r-tuplas binarias no nulas. Con esta notación el código binario de Hamming $\mathcal{H}_r$ tiene como matriz de chequeo de paridad a:

$$H = (1, \alpha, \ldots, \alpha^{2^r-2}).$$

donde cada entrada es reemplazada por el vector columna binario de longitud r correspondiente. Por otro lado un vector $\bar{c} = (c_0, c_1, ..., c_{n-1}) \in \mathcal{H}_r$ si y sólo si $H\bar{c}^t = 0$, esto es si y sólo si $\sum_{i=0}^{n-1} c_i\alpha^i = 0$, o lo que es lo mismo $p(\alpha) = 0$, donde $p(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. Resumiendo, $\bar{c} \in \mathcal{H}_r$ si y sólo si el polinomio minimal, $m(x)$, de α divide a $p(x)$; así que $\mathcal{H}_r$ consiste de todos los múltiplos de $m(x)$. Esto prueba que el código de Hamming $\mathcal{H}_r$ es un código cíclico con polinomio generador $g(x) = m(x)$; el polinomio minimal de un elemento generador del campo $\mathbf{F}_{2^r}$. □

Una consecuencia inmediata del teorema anterior es el

Corolario 3.4 *La matriz generadora para el código binario de Hamming $\mathcal{H}_r$ es*

$$G = \begin{pmatrix} m_1(x) & & & & \\ & xm_1(x) & & & \\ & & x^2m_1(x) & & \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ & & & & x^{n-r-1}m_1(x) \end{pmatrix}$$

Ejemplo 3.7 La factorización de $x^7 - 1$, sobre $\mathbf{F}_2$, como producto de polinomios irreducibles es $(x-1)(x^3+x+1)(x^3+x^2+1)$, y ambos polinomios de grado tres son un polinomio minimal para un elemento primitivo del grupo multiplicativo $\mathbf{F}_{2^3}^*$, como puede comprobarse directamente. Tomemos por ejemplo a $x^3 + x^2 + 1$. La matriz $H = (1, \alpha, \alpha^2, \ldots, \alpha^6)$, con α satisfaciendo la relación $\alpha^3 + \alpha^2 + 1 = 0$, es la matriz para un $[7, 4, 3]$ código binario de Hamming, H_3 y puede representarse como:

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

Además, de acuerdo al corolario anterior, una matriz generadora para este código es

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

Para el caso q-ario el código de Hamming también es cíclico, bajo algunas condiciones. Más precisamente se enuncia el siguiente

Teorema 3.9 [45;329] *Si r y $q-1$ son primos relativos y $n = \frac{q^r-1}{q-1}$ entonces el código q-ario de Hamming $\mathcal{H}_r(q)$ es equivalente a un código cíclico.*

Demostración Sea s el orden de q módulo n. Entonces $\mathbf{F}_{q^s}$ es el campo de descomposición para $x^n - 1$, y es el menor entero para el cual $\frac{q^r-1}{q-1} \mid q^s - 1$. Pero $\frac{q^r-1}{q-1} \mid q^s - 1$ es válido si $s = r$, además como

$$\frac{q^r - 1}{q - 1} > q^{r-1} - 1$$

r es precisamente el menor entero con la propiedad deseada, esto es $s = r$. Sea β un generador del grupo $\mathbf{F}_{q^r}^*$, además $\omega = \beta^{(q^s-1)/n} = \beta^{q-1}$ es una raíz primitiva de la unidad sobre $\mathbf{F}_q$. Construyamos la matriz $H = (\omega^0\ \omega^1 \ldots \omega^{n-1})$, cuyas columnas son las representaciones vectoriales de potencias de ω. Mostraremos que cualesquiera dos columnas de H son linealmente independientes, con lo cual se obtiene que el código cíclico con matriz de chequeo de paridad H, digamos C, tiene longitud n y dimensión $k \geq n - r$. Utililzando la cota de empaquetamiento con esferas (proposición 2.5), obtenemos inmediatamente que $k = n - r$ y $d = 3$, por lo cual el código C será equivalente a $\mathcal{H}_r(q)$.

Ya que $q - 1 \mid q^j - 1$ tenemos $q^j = (q-1)a_j + 1$ para algún entero a_j. Por otra parte $n = \frac{q^r-1}{q-1} = 1 + q + \cdots q^{r-1}$ así que

$$n = \sum_{i=0}^{r-1} q_j = (q-1)\sum a_j + r;$$

esto es, $(r, q-1) = 1$ si y sólo si $(n, q-1) = 1$.

Dos columnas de H son linealmente dependientes si y sólo si una es un múltiplo escalar de la otra, por lo tanto las columnas de H correspondientes a ω^i y ω^j son linealmente dependientes si y sólo si $\omega^{i-j} \in \mathbf{F}_q^*$. Pero un elemento no cero está en $\mathbf{F}_q$ si y sólo si es raíz del polinomio $x^{q-1} - 1$ (cf. [17]), por lo que las columnas correspondientes a ω^i y ω^j son linealmente dependientes si y sólo si $\omega^{(i-j)(q-1)} = 1$. Siendo ω una raíz n-ésima primitiva de la unidad esto es equivalente a que $(i-j)(q-1) \equiv 0 \bmod n$. Por lo mostrado en el párrafo anterior, $(n, q-1) = 1$, de ahí que $i = j$. □

3.4.1 El código símplex

Los códigos duales a los códigos binarios de Hamming $\mathcal{H}_r$ son llamados **códigos símplex** y se denotan como Σ_r. Ya que $\mathcal{H}_r$ es un $[2^r-1, 2^r-1-r]$ código, el código símplex Σ_r es un código lineal de longitud 2^r-1 y dimensión $2^r-1-(2^r-1-r)=r$, además una matriz de chequeo de paridad para $\mathcal{H}_r$ es una matriz generadora para Σ_r.

Ejemplo 3.8 Una matriz de chequeo de paridad de $\mathcal{H}_2$, y por lo tanto una matriz generadora para el código símplex Σ_2 es

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

y los elementos del código símplex Σ_2 son

$$\Sigma_2 = \begin{matrix} 000 \\ 011 \\ 101 \\ 110 \end{matrix}.$$

Para Σ_3 se tiene

$$G_3 = \left(\begin{array}{ccc|c|ccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc|c|ccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline \multicolumn{3}{c|}{G_2} & 0 & \multicolumn{3}{c}{G_2} \end{array}\right).$$

Por lo tanto

$$\Sigma_3 = \begin{array}{c|c|c} \Sigma_2 & \mathbf{0} & \Sigma_2 \\ \Sigma_2 & \mathbf{1} & \Sigma_2^c \end{array}$$

donde Σ_2^c significa cambiar cada 1 de Σ_2 por 0 y viceversa.

Generalizando estos ejemplos se obtiene el

Teorema 3.10 [34, 30], [45; 257] *Sea Σ_r el $[2^r-1, r]$ código símplex. Entonces*

1.- *toda palabra en Σ_r, excepto la cero, tiene peso 2^{r-1}; por lo tanto Σ_r es un $[2^r-1, r, 2^{r-1}]$ código.*

2.- *la distancia entre dos palabras distintas en Σ_r es 2^{r-1}.*

3.- *Σ_r es un código cíclico.*

Demostración: (1) La prueba es por inducción sobre r. Si G_r es la matriz generadora para Σ_r entonces

$$G_{r+1} = \begin{pmatrix} 00\cdots0 & 1 & 11\cdots1 \\ G_r & \mathbf{0} & G_r \end{pmatrix}.$$

Así el código símplex resulta ser

$$\Sigma_{r+1} = \begin{array}{c|c|c} \Sigma_r & \mathbf{0} & \Sigma_r \\ \Sigma_r & \mathbf{1} & \Sigma_r^c \end{array}$$

(2) Se sigue inmediatamente de la igualdad $d(\bar{x},\bar{y}) = ps(\bar{x}-\bar{y}) = 2^{r-1}$.

(3) Ya se ha visto que, para un código, la propiedad de ser cíclico es invariante bajo dualidad. □

La parte (2) del teorema anterior explica el porqué se les da el nombre de códigos símplex a los códigos Σ_r; la razón de esto es porque las palabras codificadas de este código forman los vétrices de un simplejo regular.

Al extender el código binario de Hamming $\mathcal{H}_r$ se obtiene un $[2^r, 2^r-1-r, 4]$ código, el cual ahora puede detectar dos errores aunque solo puede corregir uno. Cuando el número de errores que es posible detectar excede al número de errores que pueden corregirse se dice que la decodificación es **incompleta**.

3.5 Códigos BCH

Hemos visto que los códigos de Hamming son códigos que corrigen un sólo error. Existen códigos que en cierto sentido son generalizaciones de estos y que son capaces de corregir t errores que ocurran durante la transmisión, para un entero dado t. Estos son los llamados códigos BCH, llamados así porque, en el caso binario, A. Hocquenghem los descubrió en 1959 (ver [28]), y R.C. Bose y D.K. Ray-Chaudhuri los descubrieron, independientemente del primero, en 1960 (cf. [10]). La generalización al caso q-ario fue realizada por D.C. Gorenstein y N. Zierler (cf. [19]). Los códigos de Reed-Solomon, que son un caso particular de aquellos, fueron descubiertos por I.S. Reed y G. Solomon (cf. [42]).

Ya hemos visto que un código cíclico puede ser definido a través de sus ceros. Los códigos BCH son códigos cíclicos con un conjunto especial de ceros, más precisamente

Definición 3.4 *Sean ω un raíz n-ésima primitiva de la unidad en $\mathbf{F}_q$, y $g(x)$ el polinomio mónico de menor grado sobre $\mathbf{F}_q$ que tiene los $\delta - 1$ elementos*

$$\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$$

entre sus ceros, donde $b \geq 1$ y $\delta \geq 1$. El código cíclico q-ario $B_q(n, \delta, \omega, b)$ de longitud n, con polinomio generador $g(x)$, es llamado **código BCH** *con* **distancia designada** δ.

Cuando $b = 1$ el código $B_q(n, \delta, \omega) = B_q(n, \delta, \omega, 1)$ es llamado un código BCH en **sentido limitado**. *Cuando ω es un elemento primitivo del campo $\mathbf{F}_q$, o sea, cuando $n = q^s - 1$ para algún entero s, el código BCH correspondiente se dice* **primitivo**.

De la definición anterior se tiene que el polinomio generador del código BCH es

$$g(x) = \text{mcm}\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\},$$

donde $m_i(x)$ es el polinomio minimal de ω^i, $i = b, \ldots, b + \delta - 2$, y mcm significa tomar el mínimo común múltiplo de los polinomios del conjunto. Además los códigos binarios BCH en sentido limitado son generalizaciones de los códigos de Hamming. Hemos visto que los códigos de Hamming pueden definirse como códigos cíclicos cuyo polinomio generador es el polinomio mónico de menor grado sobre $\mathbf{F}_2$ que tiene una raíz n-ésima de la unidad como cero. Por lo tanto, los códigos binarios de Hamming son códigos BCH primitivos en sentido limitado de distancia designada 2.

Teorema 3.11 [34;202] *El código BCH q-ario $B_q(n, \delta, \omega, b)$ de longitud n y distancia designada δ tiene parámetros*

$$\dim(B_q(n, \delta, \omega, b)) \geq n - (\delta - 1)o_n(q)$$

(donde $o_n(q)$, es el menor entero positivo d para el cual $q^d \equiv 1 \ (mod\ n)$) y distancia mínima al menos δ.

Demostración: La segunda afirmación no es más que el teorema de la cota BCH. Para el primer enunciado recuérdese que el campo de descomposición de $x^n - 1$ sobre $\mathbf{F}_q$ es de grado s sobre este campo, donde $s = o_n(q)$, y además $\text{grad}(m_i(x)) \leq s$ para cada polinomio minimal $m_i(x)$, de ahí que $\text{grad}(x) = n-$dimensión del código$\leq s(\delta - 1)$. Por lo tanto

$$\dim(B_q(n, \delta, \omega, b)) = n - (\delta - 1)o_n(q). \ \square$$

Una matriz de chequeo de paridad para estos códigos es

$$H = \begin{pmatrix} 1 & \omega^b & \cdots & \omega^{(n-1)b} \\ 1 & \omega^{b+1} & \cdots & \omega^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{b+\delta-2} & \cdots & \omega^{(n-1)(b+\delta-2)} \end{pmatrix}$$

donde cada entrada ω^i es sustituida por el vector columna $[\omega^i]$ en $\mathbf{F}_q^s$ correspondiente, bajo el isomorfismo canónico entre este espacio y el campo $\mathbf{F}_{q^s}$.

Los códigos cíclicos pueden considerarse como códigos BCH, como se hace en la siguiente definición. Esto permite tener una cota inferior para la distancia mínima de un código cíclico:

Definición 3.5 *Un código* **cíclico** *de longitud n sobre $\mathbf{F}_q$ es un código BCH de distancia designada δ tal que para algún entero $b \geq 1$.*

$$g(x) = \text{mcm}\{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\},$$

en otras palabras, $g(x)$ es el polinomio mónico de menor grado sobre el campo $\mathbf{F}_q$ que tiene a $\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$ como ceros. Así $\bar{c} = (c_0, \ldots, c_{n-1})$ está en el código si y sólo si $c(\omega^b) = c(\omega^{b+1}) = \cdots = c(\omega^{b+\delta-2}) = 0$, donde $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in R_n$.

Esto es, el código tiene como ceros a $\delta - 1$ potencias consecutivas de ω; por lo tanto su distancia mínima es mayor o igual que δ.

3.5.1 Códigos BCH binarios

Ya que β y β^p tienen el mismo polinomio minimal cuando $q = 2$, el cual es $m_{2i}(x) = m_i(x)$, el grado de $g(x)$ es reducido. Supóngase que $b = 1$, entonces para todo $\varepsilon \geq 1$ los siguientes polinomios son iguales:

$$\begin{aligned} g_1(x) &= \text{mcm}\{m_1(x), m_2(x), \ldots, m_{2\varepsilon}(x)\}, \\ g_2(x) &= \text{mcm}\{m_1(x), m_2(x), \ldots, m_{2\varepsilon-1}(x)\}, \\ g_3(x) &= \text{mcm}\{m_1(x), m_3(x), \ldots, m_{2\varepsilon-1}(x)\}. \end{aligned}$$

(en el último conjunto de polinomios m_i todos tienen índice impar). Del primer polinomio se tiene $b + \delta - 2 = 1 + \delta - 2 = \varepsilon$, esto es, $\delta = 2\varepsilon + 1$:

mientras que del segundo polinomio se tiene $b+\delta-2=1+\delta-2=2\varepsilon-1$, o sea $\delta=2\varepsilon$. De la igualdad de los polinomios se concluye que

$$B_2(n,2\varepsilon+1,\omega)=B_2(n,2\varepsilon,\omega).$$

Esto lo que significa es que podemos restringir nuestra atención a códigos BCH binarios en sentido limitado de distancia designada impar.

El polinomio $g_3(x)$ es el polinomio generador de los código BCH con distancia designada $2t$ o $2t+1$. Por otra parte $\text{grad}(m_{b+i}(x)) \leq o_n(2)$, por lo tanto $\text{grad}(g(x)) \leq to_n(2)$, y la dimensión del código es entonces $\geq m-to_n(2)$. La matriz de chequeo de paridad correspondiente es:

$$H=\begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{2t-1} & \omega^{(2t-1)(2)} & \cdots & \omega^{(2t-1)(n-1)} \end{pmatrix}$$

donde cada entrada es reemplazada por la correspondiente m-tupla. Es más, la segunda columna de H sólo requiere contener $\omega, \omega^{i_1}, \omega^{i_2}, \ldots$ donde $1, i_1, i_2, \ldots$ están en diferentes clases ciclotómicas (consultar página 27).

Ejemplo 3.9 Considérese el código BCH binario de longitud 7 y distancia designada 3. Este código tiene como polinomio generador a:

$$g(x)=\text{mcm}\{m_1(x),m_2(x)\}=m_1(x).$$

Supóngase que el campo $\mathbf{F}_8$ es generado por ω, con $\omega^3+\omega^2+1=0$. Entonces la matriz generadora del código es

$$H=\begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^6 \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^5 \end{pmatrix}.$$

Haciendo las sustituciones respectivas se tiene:

$$H=\left(\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{array}\right)$$

Sumando el primer renglón al cuarto se obtiene el renglón número cinco, así que se suprime el cuarto renglón. En esta nueva matriz, se suman el segundo renglón y el sexto, nuevamente resultan dos renglones iguales, después de descartar uno de ellos es claro que la matriz que resulta es una de chequeo de paridad de un $[7,4,3]$ código binario de Hamming.

Ejemplo 3.10 Consideremos el código BCH binario de longitud 7, con $\delta = 5$ y $b = 1$. Su polinomio generador $g(x)$ es el producto de los polinomios minimales $m_1(x)$ y $m_3(x)$, esto es, $g(x) = (x^3+x+1)(x^3+x^2+1) = \sum_{i=0}^{6} x^i$. La matriz de chequeo de paridad correspondiente es

$$H = \begin{pmatrix} 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^2 & \omega^4 & \omega^5 & \omega^4 \end{pmatrix}$$

o haciendo las sustituciones respectivas

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

Ejemplo 3.11 Las clases ciclotómicas de 2 módulo 25 son:

$C_0 = \{0\}$,
$C_1 = \{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24\}$,
$C_5 = \{5,10,15,20\}$.

Sea $B = B_2(25,1,\omega)$ un código BCH. Los ceros del código dual $B^\perp$ son los recíprocos de los no ceros de B. Por lo tanto los ceros de $B^\perp$ son: $\{\omega^0,\omega^5,\omega^{10},\omega^{15},\omega^{20}\}$. Esto muestra que $B^\perp$ no es un código BCH, de ahí que el código dual de un código BCH no necesariamente es un código BCH.

3.6 Códigos de Reed-Solomon

Definición 3.6 *Para cada potencia de un primo q ($q > 2$), el código q-ario de* **Reed-Solomon**, *denotado RS, es el código BCH de longitud $q-1$.*

Como veremos más adelante, la propiedad de que su longitud sea precisamente $q-1$ hace que los códigos RS sean considerablemente prácticos.

Ya que las raices del polinomio $x^{q-1}-1$ son precisamente los elementos no cero del campo base $\mathbf{F}_q$,

$$x^n - 1 = x^{q-1} - 1 = \prod_{\beta \in \mathbf{F}_q^*} (x - \beta).$$

Y como $iq \equiv i \pmod{q-1}$ para todo i, se sigue que $m_i(x) = x - \omega^i$, con ω un generador del grupo multiplicativo $\mathbf{F}_q^*$. Por lo tanto un código RS de longitud $q-1$ y distancia designada δ tiene polinomio generador

$$g(x) = (x - \omega^b)(x - \omega^{b+1}) \cdots (x - \omega^{b+\delta-2}).$$

Ejemplo 3.12 $\omega = 2$ es un elemento primitivo de $\mathbf{F}_5$, el código RS sobre $\mathbf{F}_5$ con $b = 1$, longitud 4 y distancia designada 3 tiene polinomio generador

$$g(x) = (x-2)(x-4)(x-3) = (x+3)(x+1)(x+2).$$

Y el código es

$$C = \{(c_0 + c_1 x + c_2 x^2 + c_3 x^3) g(x) : c_i \in \mathbf{F}_5\}.$$

La dimensión del código RS es $n - \text{grad}(g(x)) = n - \delta + 1$, donde n es la longitud del código. La distancia mínima es, por la cota BCH, al menos $\delta = n - k + 1$. Sin embargo por la cota Singleton, proposición 2.4, la distancia mínima no puede ser mayor que δ, y por lo tanto aquella es exactamente $n - k + 1$ y los códigos RS son distancia máxima separables (MDS).

Damos ahora dos ejemplos de como transformar un código 2^m-ario a otro sobre el campo binario. En general esta transformación lleva códigos lineales a códigos lineales, sin embargo no siempre lleva códigos cíclicos a códigos cíclicos; de este hecho sólo se conoce un ejemplo, el cual mostramos como aparece en [45] en el ejemplo 3.14.

Ejemplo 3.13 Considérese el código [3, 2, 2] de Reed-Solomon sobre el campo $\mathbf{F}_4 = \{0, 1, \omega, \omega^2\}$, donde $\omega^2 + \omega + 1 = 0$. El polinomio generador de este código es $g(x) = x - \omega$, por lo que el código es

$$C = \{\psi^{-1}(p(x)(x - \omega)) : \text{grad}(p(x)) \leq 1\},$$

donde $\psi : \mathbf{F}_4^3 \to R_3$ es la función definida en la página 26.

Las palabras de este código son:

0	0	0	ω	1	0	ω^2	ω	0	1	ω^2	0
1	0	ω	ω^2	1	ω	ω	ω	ω	0	ω^2	ω
ω	0	ω^2	0	1	ω^2	1	ω	ω^2	ω^2	ω^2	ω^2
ω^2	0	1	1	1	1	0	ω	1	ω	ω^2	1

La pareja $\{1, \omega\}$ es una base de $\mathbf{F}_4$ sobre $\mathbf{F}_2$ y bajo esta base

$$0 \mapsto 00, \quad 1 \mapsto 10, \quad \omega \mapsto 01, \quad \omega^2 \mapsto 11,$$

y el código puede transformarse en un $[3(2), 2(2)]$ código binario, digamos $\mathcal{C}$, cuyas palabras resultan ser:

000000	011000	110100	101100
100001	111001	010101	001101
010011	001011	100111	111111
110010	101010	000110	011110

Como puede verse esta transformación *no* lleva un código cíclico en un código cíclico, pues por ejemplo la palabra 0110000 está en $\mathcal{C}$, pero 001100 no.

Ejemplo 3.14 Tomemos la base $\{1, \omega, \omega^6\}$ de $\mathbf{F}_8$ sobre el campo $\mathbf{F}_2$. Bajo esta base tenemos la siguiente tabla,

$0 \mapsto 000$	$\omega^2 \mapsto 101$	$\omega^5 \mapsto 011$
$1 \mapsto 100$	$\omega^3 \mapsto 110$	$\omega^6 \mapsto 001$
$\omega \mapsto 010$	$\omega^4 \mapsto 111$	

El polinomio

$$g(x) = (x + \omega^5)(x + \omega^6) = \omega^4 + \omega x + x^2$$

es el generador del $[7, 5, 3]$ código de Reed-Solomon sobre $\mathbf{F}_8$. Este código es transformado en el $[21, 15, 3]$ código BCH binario con polinomio generador

$$g(y) = m_1(y) = 1 + y + y^2 + y^4 + y^6.$$

Este es el único ejemplo no trivial conocido de un código cíclico que es transformado de esta manera en un código cíclico.

En [45;372] se describe un método general para transformar un código $[n, k, d]$ 2^m-ario, para algún entero m, en un $[nm, mk, \geq d]$ código binario.

Teorema 3.12 [45;296] *Sea C un $[q^m - 1, k, d]$ código RS, sobre $\mathbf{F}_q$, con polinomio generador*

$$g(x) = (x - \omega)(x - \omega^2) \cdots (x - \omega^{d-1}).$$

Entonces el código extendido $\hat{C}$ es un $[q^m, k, d + 1]$ código.

En la pasada sección notamos que el dual a un código BCH en general no es un código del mismo tipo. Con los códigos de Reed-Solomon no sucede esto, como lo muestra el siguiente

Teorema 3.13 *El código dual a un código de Reed-Solomon es un código de Reed-Solomon.*

Demostración: Sea ω un generador del grupo multiplicativo $\mathbf{F}_q^*$. Supóngase que $g(x) = (x - \omega^b)(x - \omega^{b+1})(x - \omega^{b+\delta-2})$ es el polinomio generador de un código de Reed-Solomon dado, digamos C. Aplicando el teorema 3.4 encontramos que

$$g^{\perp}(x) = (x - \omega^a)(x - \omega^{a+1})(x - \omega^{a+\delta-2}),$$

con $a = 2 - \delta - b$, es el polinomio generador para $C^{\perp}$. □

El método original de codificación de Reed-Solomon tiene ventajas prácticas como se muestra a continuación:

Sea $\bar{u} = (u_0, u_1, \ldots, u_{k-1}), u_i \in \mathbf{F}_q$ el mensaje a ser codificado, y sea

$$u(x) = \sum_{i=0}^{k-1} u_i x^i.$$

Se codifica $\bar{u}$ como el vector $\bar{c}$ cuyo polinomio de Mattson-Solomon es $(q - 1)u(x)$, por lo tanto

$$\bar{c} = (u(1), u(\omega), \ldots, u(\omega^{n-1})),$$

donde ω es una raíz $(q-1)$-ésima primitiva de la unidad. Podemos entonces recuperar el polinomio $c(x)$ a partir de su polinomio de Mattson-Solomon $c_{ms}(x) = (q - 1)u(x)$.

$$c(x) = \frac{1}{q-1} \sum_{i=0}^{q-2} c_{ms}(\omega^i) x^i = \frac{1}{q-1} [c_{ms}(1) + c_{ms}(\omega)x^2 + \cdots + c_{ms}(\omega^{q-2})x^{q-2}].$$

Haciendo sustituciones adecuadas

$$c(x) = u(1) + u(\omega)x^2 + \cdots + u(\omega^{q-2})x^{q-2}.$$

Sólo resta probar que $\bar{c}$ está en el código RS. Para esto se verifica que $\omega, \omega^2, \ldots, \omega^{\delta-1}$ son ceros de $c(x) = \sum_{i=0}^{q-2} c_i x^i$.

El polinomio de Mattson-Solomon de $c(x)$ es:

$$c_{ms}(x) = \sum_{i=0}^{q-2} c(\omega^{-i})x^i = (q-1)\sum_{i=0}^{k-1} u_i x^i = \sum_{i=0}^{k-1}(q-1)u_i x^i.$$

Igualando coeficientes y tomando en cuenta que $q - 1 = -1$ en $\mathbf{F}_q$, tenemos:

$$c(1) = -u_0,\ c(\omega^{-1}) = -u_1, \ldots, c(\omega^{-(k-1)}) = -u_{k-1}.$$

Además, por ser distintos los grados de los polinomios

$$c(\omega^{-k}) = c(\omega^{-(k+1)}) = \cdots = c(\omega^{-(q-2)}) = 0,$$

lo cual puede reescribirse, usando el hecho de que ω es una raíz $(q-1)$-ésima primitiva de la unidad, como

$$c(\omega^{\delta-1}) = \cdots = c(\omega^2) = c(\omega) = 0.$$

4 Diseños

Aquí nos apartamos por un momento del estudio de los códigos lineales, ahora dedicaremos nuestra atención al estudio de las geometrías finitas, vistas como diseños. Más tarde estableceremos una correspondencia entre aquellos y estos. Veremos que los llamados códigos de Reed-Muller surgen naturalmente como códigos binarios asociados a las geometrías finitas. Notaremos además cómo los parámetros de estos códigos pueden ser obtenidos a partir de la estructura combinatoria de estas geometrías.

4.1 Conceptos generales

Definición 4.1 *Una* **estructura de incidencia** *es una pareja de conjuntos* $\mathbf{S} = (\mathbf{P}, \mathbf{B})$, *donde* $\mathbf{B}$ *es una familia de subconjuntos de* $\mathbf{P}$. *En caso de que* $\mathbf{P}$ *sea finito se dice que la estructura de incidencia es* **finita**.

Los elementos de $\mathbf{P}$ son llamados **puntos** o **variedades**, (este último término se debe a que el origen de estas nociones se encuentra en la agricultura pues las estructuras de incidencia se utilizan para examinar efectos de algunos fertilizantes) y los miembros de $\mathbf{B}$ se denominan **bloques**. Cuando el punto p está en el bloque B se dice que p y B son **incidentes**, (o que p es incidente con B, o que B es incidente con p.)

Si X es un conjunto cualquiera denotaremos por $P_t(X)$ a la subfamilia del conjunto potencia de X, $P(X)$, de todos los subconjuntos de X con t elementos. A cada elemento de $P_t(X)$ le llamaremos t-**conjunto**

Como nuestro interés se centra en las estructuras de incidencia finita de aquí en adelante al hablar de una estructura de incidencia supondremos que es finita.

Definición 4.2 *Sean* v, k, t *y* λ *enteros positivos. Diremos que una estructura de incidencia* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *es un* t-(v, k, λ) **diseño,** (*o bien un* t-*diseño con* v *puntos, con medida de bloque* k *e índice* λ), *si*

i) existen v *puntos, i.e.,* $\mid \mathbf{P} \mid = v$.

ii) cualquier bloque B *es incidente con exactamente* k *puntos, en símbolos:* $\forall B \in \mathbf{B}. \mid B \mid = k$.

iii) para todo conjunto T *de* t *puntos, existen exactamente* λ *bloques incidentes con todos los puntos de* T, *i.e.,*

$$T \in P_t(\mathbf{P}) \;\Rightarrow\; \mid \{B : B \in \mathbf{B}, T \subseteq B\} \mid = \lambda.$$

Es común escribir un t-(v, k, λ) diseño como $S_\lambda(t, k, v)$. Cuando $\lambda = 1$ el subíndice correspondiente es suprimido, y a los diseños de esta clase se les llama **sistemas de Steiner**. En particular los diseños $S(2, 3, v)$ son llamados **sistemas triples de Steiner,** mientras que los $S(3, 4, v)$ se conocen como **sistemas cuádruples de Steiner.**

Ejemplo 4.1 Sean $\mathbf{P} = \{1, 2, 3, 4, 5, 6, 7\}$ y

$$\mathbf{B} = \{\{1, 2, 3\}, \{1, 4, 7\}, \{1, 5, 6\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 5\}, \{3, 6, 7\}\}.$$

Entonces $(\mathbf{P}, \mathbf{B})$ forma un 2-$(7, 3, 1)$ diseño, y escribimos $(\mathbf{P}, \mathbf{B}) = S(2, 3, 7)$. Este sistema triple de Steiner es conocido como **plano de Fano** y es el menor diseño que surge de la geometría proyectiva, como veremos más adelante. Puede ser representado con el diagrama mostrado en la siguiente figura

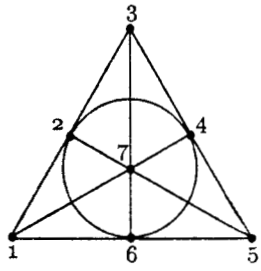

Figura 2. El plano de Fano $\mathcal{F}$.

Ejemplo 4.2 Sea $\mathbf{P}$ el conjunto de puntos de las 16 posiciones del arreglo 4×4, i.e. $\mathbf{P} = \{(1,1), (1,2), \ldots, (4,3), (4,4)\}$. Para cada par (i, j) defínase el bloque $B_{ij} = \{(i, k), (k, j)\}_{k=1}^{4} - \{(i, j)\}$ (en la figura 3 se muestra uno de estos bloques). Entonces el número de bloques es el mismo que el de puntos y cualesquiera dos puntos son incidentes con dos bloques, así que $(\mathbf{P}, \mathbf{B})$ es un 2-$(16, 6, 2)$ diseño conocido como **biplano de orden 4.**

		*	
*	*		*
		*	
		*	

Figura 3. El bloque B_{23}

Ejemplo 4.3 Un 2-$(n^2+n+1, n+1, 1)$ diseño, $n \geq 2$, es llamado **plano proyectivo de orden** n.

Originalmente los diseños surgieron como una necesidad al realizar experimentos biológicos y en agricultura, en la rama de la estadística conocida como diseño de experimentos (cf. [37], [40]). Por ejemplo supóngase que se desean comparar los efectos de v variedades de fertilizantes en b diferentes cultivos. Lo ideal sería probar cada cultivo con cada una de las variedades de fertilizante, con lo cual obtendríamos b bloques de tierra, (uno por cada cultivo), y en cada uno se probarían los v fertilizantes. Este es un 2-(v, v, b) diseño conocido como diseño **completo**. Obviamente esto no es posible hacerlo, por razones económicas, así que lo que se hace es probar cada cultivo con sólo k de las variedades de fertilizante, de tal forma que cualesquiera dos fertilizantes sean utilizados simultaneamente, en el mismo cultivo, un número constante λ de veces. Este es un 2-(v, k, λ) diseño con b bloques, es **incompleto** si $k < v$, también se dice que el diseño es **balanceado** porque así es la comparación entre los pares de fertilizantes. En general un 2-diseño no trivial es conocido como **diseño de bloques balanceado incompleto (DBBI)** si $k < v$.

Si un diseño tiene tantos puntos como bloques se dice que es un **diseño simétrico.** Un diseño **trivial** es aquel en el cual todo conjunto de k puntos es incidente con un bloque, en cuyo caso el número de bloques es $\begin{pmatrix} v \\ k \end{pmatrix}$. Un 1-diseño es llamado una **configuración táctica.** Cuando $k = 2$ un t-(v, k, λ) diseño resulta ser una *gráfica* no dirigida y sin lazos; donde los puntos son los vértices y los bloques las aristas. La gráfica será *completa* si $t = 2$, o sea, si todas las aristas posibles están presentes.

Proposición 4.1 [5;7], [11;2], [57;20] *Sea* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *un* t-(v, k, λ) *diseño. El número de bloques en* $\mathbf{D}$, *que denotaremos por* b. *viene dado por*

$$b = \lambda \begin{pmatrix} v \\ t \end{pmatrix} / \begin{pmatrix} k \\ t \end{pmatrix}.$$

Demostración: Sea $N = \mid \{(T, B) \in P_t(\mathbf{P}) \times \mathbf{B} : T \subseteq B\} \mid$. Ya que

$$\mid \{T : T \in P_t(\mathbf{P})\} \mid = \begin{pmatrix} v \\ t \end{pmatrix}.$$

por el tercer axioma de t-diseños se tiene que

$$N = \lambda \begin{pmatrix} v \\ t \end{pmatrix}.$$

Sean $B_0 \in \mathbf{B}$ un bloque fijo y

$$N_0 = \mid \{(T, B_0) \in P_t(\mathbf{P}) \times \mathbf{B} : T \subseteq B_0\} \mid,$$

entonces $N_0 = \begin{pmatrix} k \\ t \end{pmatrix}$, por lo tanto

$$N = b \begin{pmatrix} k \\ t \end{pmatrix}.$$

Igualando los valores obtenidos de N y despejando b se obtiene el resultado deseado. □

Proposición 4.2 [57;21] *Dado $S \in P_s(\mathbf{P})$, $0 \leq s \leq t$, se denotará por $\mathbf{D}_S$ a la subestructura de $\mathbf{D}$ con puntos $\mathbf{P} - S$ y bloques $\mathbf{B}_S = \{B \in \mathbf{B} : S \subseteq B\}$. Entonces $\mathbf{D}_S$ es un $(t-s)$-$(v-s, k-s, \lambda)$ diseño. Si $S = \{p\}$, denotaremos al diseño $\mathbf{D}_{\{p\}}$ simplemente como $\mathbf{D}_p$ y le llamaremos la* **contracción** *de $\mathbf{D}$ en el punto p.*

Demostración: Sea $B \in \mathbf{B}_S$, entonces B, como bloque en $\mathbf{B}$, es incidente con exactamente k puntos, así que en $\mathbf{D}$

$$k = \mid B \mid = \mid (B - S) \cup S \mid = \mid B - S \mid + \mid S \mid.$$

Por lo tanto $\mid B - S \mid = k - s$. Por último, elijamos $T \in P_{t-s}(\mathbf{P} - S)$; entonces $T \cup S$ tiene cardinalidad t, así que $\mid \{B \in \mathbf{B} : T \cup S \subseteq B\} \mid = \lambda$. □

Aplicando la proposición anterior a $\mathbf{D}_S$ tenemos la siguiente

Proposición 4.3 [5;6],[11;2],[57;21] *Para todo s, $0 \leq s \leq t$, el número de bloques de un t-(v, k, λ) diseño, incidentes con todos los puntos de un conjunto de cardinalidad s, es exactamente*

$$\lambda_s = \lambda \begin{pmatrix} v - s \\ t - s \end{pmatrix} / \begin{pmatrix} k - s \\ t - s \end{pmatrix}.$$

Esto es, todo t-(v, k, λ) diseño es también un s-diseño para $s \leq t$. a saber, un s-(v, k, λ_s) diseño.

De la proposición anterior es claro que el número de bloques incidentes con un punto, arbitrario pero fijo, es independiente del punto elegido, a saber λ_1. Este número será denotado como r y le llamaremos el **número de repetición.** El siguiente resultado se desprende inmediatamente de la misma proposición:

Corolario 4.1 [5; 7] *Una condición necesaria para la existencia de un* t-(v, k, λ) *diseño es que los números* $b = \lambda_0, r = \lambda_1, \lambda_2, \ldots, \lambda_t = \lambda$ *sean enteros.*

Se ha conjeturado que para cualesquiera t, k y λ dados satisfaciendo estas condiciones y v suficientemente grande, existe un t-(v, k, λ) diseño, sin embargo esto sólo ha sido probado para $t = 2$ y no se conoce ningún diseño con $t > 5$, (cf. [54], [55], [56]).

Haciendo $\lambda_t = \lambda$ en la proposición precedente se encuentra una manera recursiva de calcular los valores λ_s, notemos que

$$\frac{v-s}{k-s}\lambda_{s+1} = \lambda\frac{v-s}{k-s}\frac{[v-(s+1)][v-(s+1)-1]\cdots[v-t+1]}{[k-(s+1)][k-(s+1)-1]\cdots[k-t+1]}$$

lo cual resulta del lado derecho, después de hacer las cancelaciones correspondientes, λ_s, por lo tanto

$$\lambda_s = \frac{v-s}{k-s}\lambda_{s+1}.$$

En particular cuando $s = 0$ (recuérdese que $\lambda_0 = b$ y $\lambda_1 = r$) obtenemos

$$bk = vr;$$

y cuando $t = 2$, tomando $s = 1$, se obtiene

$$r(k-1) = \lambda(v-1).$$

Estas ecuaciones muestran que los parámetros de un diseño no son independientes, es más, tienen restricciones de divisibilidad impuestas por la necesidad de que los valores λ_s sean enteros.

Existen otros valores λ's asociados a un t-diseño, los cuales fueron discutidos explícitamente en primer lugar por Richard M. Wilson. Supóngase que i y j son enteros no negativos. Entonces para conjuntos ajenos de puntos I y J, con $\mid I \mid = i$ y $\mid J \mid = j$, el número de bloques que contienen a I y son ajenos

a J, es independiente de estos conjuntos de puntos siempre que $i+j \leq t$ y se denota como λ_i^j. A fin de probar la independencia de este valor respecto a los conjuntos I y J se construye un análogo al triángulo de Pascal con λ_i^j en la (i,j)-ésima posición. (Debe notarse que para $0 \leq i \leq t$, $\lambda_i^0 = \lambda_i$). En este triángulo se satisface la recursión:

$$\lambda_i^j = \lambda_{i+1}^j + \lambda_i^{j+1}.$$

En efecto pues

$$\lambda_i^j = \mid \{B \in \mathbf{B} : I \subseteq B, B \cap J = \emptyset\} \mid,$$

por lo que para todo x que no esté ni en I ni en J, y para todo bloque B, $I \cup \{x\} \subseteq B$ o $B \cap (J \cup \{x\}) = \emptyset$. Notemos ahora que $\lambda_{i+1}^j = \mid \{B \in \mathbf{B} : I \cup \{x\} \subseteq B, x \in (I \cup J)^c, B \cap J = \emptyset\} \mid$, análogamente para λ_i^{j+1}. De estas observaciones se concluye la recursión deseada la cual nos da la independencia de los valores λ_i^j. El arreglo triangular construido se ve así

$$\begin{array}{ccccccc}
 & & & \lambda_0^0 & & & \\
 & & \lambda_1^0 & & \lambda_0^1 & & \\
 & \lambda_2^0 & & \lambda_1^1 & & \lambda_0^2 & \\
\lambda_3^0 & & \lambda_2^1 & & \lambda_1^2 & & \lambda_0^3
\end{array}$$

donde, de acuerdo a la fórmula de recursión:

$$\begin{array}{ll}
\lambda_0^0 = \lambda_0 & \lambda_0^2 = \lambda_0 - 2\lambda_1 + \lambda_2 \\
\lambda_1^0 = \lambda_1 & \lambda_3^0 = \lambda_3 \\
\lambda_0^1 = \lambda_0 - \lambda_1 & \lambda_2^1 = \lambda_2 - \lambda_3 \\
\lambda_2^0 = \lambda_2 & \lambda_1^2 = \lambda_1 - 2\lambda_2 + \lambda_3 \\
\lambda_1^1 = \lambda_1 - \lambda_2 & \lambda_0^3 = \lambda_0 - 3\lambda_1 + 3\lambda_2 - \lambda_3
\end{array}$$

Por fortuna no es necesario construir este triángulo cada vez que necesitemos calcular un λ_i^j particular; Ray-Chaudhuri y R. Wilson calcularon una fórmula que nos evita este trabajo, esto es lo que nos dice la

Proposición 4.4 [5;9] *Para i y j enteros no negativos con $i+j \leq t$, el número de bloques de un t-(v,k,λ) diseño que contienen un i-conjunto ajeno de un j-conjunto es*

$$\lambda_i^j = \lambda \binom{v-i-j}{k-i} / \binom{v-t}{k-t}$$

Demostración: Basta probar que el lado derecho de la igualdad satisface las condiciones iniciales $\lambda_i^0 = \lambda_i$, y la recursión $\lambda_i^j = \lambda_{i+1}^j + \lambda_i^{j+1}$. Las condiciones iniciales son claramente satisfechas y la fórmula de recursión se satisface por la recursión de los coeficientes binomiales. □

Al calcular el triángulo correspondiente a un diseño particular comenzamos con el vértice inferior izquierdo y ascendemos al vértice superior utilizando la recursión $\lambda_s = \frac{v-s}{k-s}\lambda_{s+1}$, y enseguida se completa el triángulo con la recursión $\lambda_i^j = \lambda_i^{j+1} + \lambda_{i+1}^j$. Por ejemplo para el plano de Fano tenemos

$$\begin{array}{ccccc} & & 7 & & \\ & 3 & & 4 & \\ 1 & & 2 & & 2 \end{array}$$

Una de estas diferencias de λ_i^j's tiene gran importancia en el presente trabajo, así que se le asigna un nombre especial

Definición 4.3 *Si $t \geq 2$ el* **orden** *del t-diseño* $\mathbf{D}$ *es $n = \lambda_1^1 = r - \lambda_2$. En particular si $t = 2$ entonces $n = r - \lambda$.*

El orden del plano de Fano es 2 y el del biplano del ejemplo 4.2 es 4. En general para un 2-diseño el triángulo de Pascal correspondiente es

$$\begin{array}{ccccc} & & b & & \\ & r & & b-r & \\ \lambda & & n & & b-r-n \end{array}$$

Al estudiar códigos asociados a diseños veremos que el orden de este nos permitirá determinar si tal código puede tener o no algunas propiedades que nos interesan.

Al igual que con las estructuras, algebraicas en la teoría de diseños también puede hablarse de diseños *esencialmente iguales* a través de un isomorfismo el cual no distinga los papeles de puntos y bloques.

Definición 4.4 *Sean* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *y* $\mathbf{D}' = (\mathbf{P}', \mathbf{B}')$ *dos estructuras de incidencia, y sea*

$$\phi : \mathbf{P} \cup \mathbf{B} \longrightarrow \mathbf{P}' \cup \mathbf{B}'$$

una función biyectiva tal que

$$\phi(\mathbf{P}) = \mathbf{P}', \qquad \phi(\mathbf{B}) = \mathbf{B}.'$$

Entonces ϕ se denomina un **isomorfismo** *de* $\mathbf{D}$ *a* $\mathbf{D}'$. *Si* $\mathbf{D} = \mathbf{D}'$, ϕ *se conoce como* **automorfismo** *o* **colineación**.

El grupo de automorfismos de $\mathbf{D}$ se denotará como $Aut(\mathbf{D})$.

Ejemplo 4.4 (1) La permutaciónes (1762)(34) y (123)(456) son automorfismos del plano de Fano de la figura 2 pag. 53.

(2) Un automorfismo del biplano del ejemplo 4.2 es cualquier elemento del grupo $S_4 \times S_4$ con el primer factor operando en los renglones y el segundo en las columnas. Esto puede verificarse notando que $(\sigma, \tau) \in S_4 \times S_4$ implica que $(\sigma, \tau)B_{ij} = B_{\sigma(i),\tau(j)}$

Definición 4.5 *Una estructura de incidencia* $S^* = (\mathbf{P}^*, \mathbf{B}^*)$ *es una* **extensión** *de la estructura* $S = (\mathbf{P}, \mathbf{B})$ *si existe un punto* $p \in \mathbf{P}^*$ *tal que la contracción* S_p^* *es isomorfa a* S.

Proposición 4.5 [5; 16] *Si un* t-(v, k, λ) *diseño* $\mathbf{D}$ *tiene una extensión entonces* $(k+1)$ *divide a* $b(v+1)$.

Demostración: Sea $\mathbf{E}$ es una extensión de $\mathbf{D}$, entonces $\mathbf{E}$ es un $(t+1)$-$(v+1, k+1, \lambda)$ diseño y, el valor λ_1 de este diseño es b, el número de bloques de $\mathbf{D}$. Denotemos por b^* el número de bloque de $\mathbf{E}$, entonces por la recursión que relaciona a las λ_s se tiene

$$b^* = \lambda_1(v+1)/(k+1) = b(v+1)/(k+1). \square$$

Ejemplo 4.5 El plano de Fano, $\mathcal{F}$, puede ser construido de la siguiente manera: considérese la gráfica completa de cuatro vértices, esto es un cuadrado junto con su diagonales. Tomemos como el conjunto de puntos $\mathbf{P}$ a las seis aristas, o sea cada línea que une dos vértices distintos, junto con un punto adicional el cual denotaremos por ∞. Los bloques que contendrán a ∞ serán cada pareja de aristas ajenas junto con el punto ∞, y los bloques que no contengan a este punto serán aquellos cuyos puntos forman un triángulo de la gráfica completa.

$\mathcal{F}$ se extiende a un 3-$(8,4,1)$ diseño de la siguente manera: el conjunto de puntos será el de los puntos de $\mathcal{F}$ junto con un punto adicional; los bloques que no contienen a este punto serán aquellos cuyos puntos son los que no se encuentran en un bloque de $\mathcal{F}$, siete en total; y los bloques que contienen al punto adicional serán los formados por los bloques del plano $\mathcal{F}$ a los cuales se les ha agregado el punto adicional. Puede verificarse directamente que este diseño así construido también es un 2-$(8,4,3)$ diseño.

Otra forma de describir una estructura de incidencia finita es a través de una matriz asociada la cual recibe el nombre de **matriz de incidencia.** Esta matriz permitirá definir códigos lineales considerando su espacio renglón sobre un campo finito dado.

Definición 4.6 *Sea* $\mathbf{S} = (\mathbf{P}, \mathbf{B})$, *una estructura de incidencia con* $\mathbf{P} = \{p_1, p_2, \ldots, p_v\}$ *y* $\mathbf{B} = \{B_1, B_2, \ldots, B_b\}$. *Una* **matriz de incidencia** *para* $\mathbf{S}$ *es una matriz* $A = (a_{ij})$ *de* $b \times v$ *tal que* $a_{ij} = \chi_{B_i}(p_j)$, *donde* χ_X *denota la función característica del conjunto* X.

En particular cuando $\mathbf{S}$ resulte ser un diseño, la matriz de incidencia de $\mathbf{S}$ tendrá k entradas igual a 1 en cada renglón, y r entradas igual a 1 en cada columna.

Ejemplo 4.6 Los renglones de la matriz de incidencia del plano de Fano de la figura 2, pag. 53, son precisamente las palabras codificadas de la segunda columna de la figura 1, pag. 39.

Definición 4.7 *Sean* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *un* 2-(v, k, λ) *diseño y* $S \in P(\mathbf{P})$, *si cualesquiera tres puntos de* S *no están contenidos en un bloque, llamaremos a* S *un* s-**arco.** *Un bloque* $B \in \mathbf{B}$ *se llama*

1) **tangente a** S *si* B *intersecta a* S *en un único punto.*
2) **secante a** S *si* B *intersecta a* S *en dos puntos.*
3) **exterior a** S *si* B *es ajeno a* S.

Ejemplo 4.7 En el plano de Fano de la figura 2, pag. 53, $S = \{1,3,4,6\}$ es un 4-arco, las líneas $\{1,2,3\}$ y $\{2,5,7\}$, son secante y exterior respectivamente, no existen tangentes.

Teorema 4.1 [5; 19] (**Andriamanalimanana**) *Sea* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *un diseño* $S_\lambda(2, k, v)$ *de orden* n, *donde* $k \geq 3$, *y sea* S *un* s*-arco de* $\mathbf{D}$. *Entonces*

i) $s \leq \frac{r+\lambda-1}{\lambda}$, *si* n *es impar, o* n *es par y* λ *no divide a* r.

ii) $s \leq \frac{r+\lambda}{\lambda}$, *si* n *es par y* λ *divide a* r.

Demostración Sea p un punto fijo en S, ya que un bloque puede intersectar a S en a lo más un punto distinto de p y existen r bloques que contienen a p, calculando la cardinalidad del conjunto $\{(q, B) : q \in S - \{p\}, p, q \in B \in \mathbf{B}\}$ se obtiene

$$(s-1)\lambda = \sum_{B:p\in B} \mid B \cap (S - \{p\}) \mid \leq r.$$

Por lo tanto $s \leq (r+\lambda)/\lambda$, para cualquier orden de $\mathbf{D}$.

Ahora se probará que si n es impar o si es par y λ no divide a r entonces S tiene una tangente. Supóngase que no es así , esto es, supóngase que S carece de tangentes. Entonces $\mid B \cap (S - \{p\}) \mid = 1$, para todo bloque que contenga a p, y así $s = (r+\lambda)/\lambda$, esto implica que λ divide a r. Ya que $k \geq 3$, es posible elegir un punto u fuera de S. Supongamos que existen m secantes a S a través de u, evaluando la cardinalidad de $\{(q, B) : q \in S,\ u, q \in B\}$ en dos formas se obtiene $2m = s\lambda = \lambda(r+\lambda)/\lambda$, esto es $r + \lambda = 2m$ así que $n = r - \lambda = 2m - 2\lambda$ y n es par.

Si S tiene una tangente B en un punto p entonces $\mid B \cap (S - \{p\}) \mid = 0$, por lo que $\lambda(s-1) \leq r - 1$, de donde $s \leq (r - 1 + \lambda)/\lambda$. □

Los arcos de longitud máxima serán de interés en nuestro trabajo por lo que les damos un nombre especial

Definición 4.8 *Sea* $\mathbf{D}$ *un* 2-(v, k, λ) *diseño de orden* n. *Un* **óvalo en** $\mathbf{D}$ *es un* s*-arco de cardinalidad máxima* m, *donde*

1) $m = (r + \lambda - 1)/\lambda$ *si* n *es impar, o si* n *es par y* λ *no divide a* r.

2) $m = (r + \lambda)/\lambda$ *si* n *es par y* λ *divide a* r.

Ejemplo 4.8 Es sencillo verificar que la estructura de incidencia cuyos bloques son los óvalos del plano de Fano forman un diseño simétrico. Este diseño también puede ser obtenido con el mismo conjunto de puntos del ejemplo 4.5, pero ahora tomando los bloques que contienen a ∞ consistentes de ∞ junto con los tres lados incidentes con un vértice de la gráfica, uno por cada vértice. Los bloques que no contienen a ∞ consisten de las aristas de un cuadrado de la gráfica (esto es de un ciclo cerrado de longitud cuatro de la gráfica). Es sencillo verificar que este es un 2-$(7, 4, 2)$ diseño.

4.2 Diseños asociados a códigos

Ya se ha mostrado una forma de asociar un código lineal a un diseño dado, por medio de una matriz de incidencia del diseño. En esta sección se mostrará que los vectores de algunos códigos lineales, con un cierto peso fijo, determinan un t-diseño, con esto se establece una relación entre diseños y códigos lineales que permite "trasladar" algunos resultados de una de estas ramas de la matemática a otra. Comenzamos con algunas definiciones

Definición 4.9 *Sean $\bar{x}, \bar{y} \in \mathbf{F}_q^n$. El conjunto $S_{\bar{x}}$ de posiciones en las cuales $\bar{x}$ tiene entradas no cero es llamado el* **soporte de** *$\bar{x}$. Decimos que $\bar{x}$* **cubre** *a $\bar{y}$ si $S_{\bar{y}} \subseteq S_{\bar{x}}$*

Por ejemplo el soporte de $12020 \in \mathbf{F}_3^5$ es $\{1, 2, 4\}$.

Definición 4.10 *Sea S_w el conjunto de palabras de peso w del $[n, k]$ código lineal C. Se dice que S_w* **sostiene** *un t-(n, w, λ) diseño si los soportes de las palabras codificadas en S_w forman los bloques de un t-(n, w, λ) diseño; o equivalentemente si para cualquier t-conjunto $T \subseteq \{1, 2, \ldots, n\}$ existen exactamente λ palabras codificadas en C, de peso w, con las entradas en las posiciones dadas por T distintas de cero.*

De particular importancia resultan los códigos perfectos (ver definición 2.6) para obtener diseños a partir de ellos, como nos lo indican los siguientes resultados:

Teorema 4.2 [34; 63] *Sea C un $[n, k, d = 2t + 1]$ código binario perfecto. Entonces S_d sostiene un sistema de Steiner $S(t + 1, d, n)$.*

Demostración: Ya que el código C es perfecto, las esferas de radio t centradas en las palabras codificadas forman una cubierta ajena de $\mathbf{F}_2^n$. Así que la palabra $\bar{x} \in \mathbf{F}_2^n$ de peso $t + 1$ está contenida en sólo una de estas esferas, digamos en aquella de centro en $\bar{c}$. Entonces,

$$ps(\bar{c}) = d(\bar{c}, 0) \leq d(\bar{c}, \bar{x}) + d(\bar{x}, 0) = d(\bar{c}, \bar{x}) + ps(\bar{x}) \leq t + t + 1 = d,$$

esto es $\bar{c} \in S_d$.

Tenemos $ps(\bar{x}) = t+1$, $ps(\bar{c}) = 2t+1$ y $d(\bar{x},\bar{c}) \leq t$; aplicando estas expresiones en la igualdad

$$d(\bar{x},\bar{y}) = ps(\bar{x}) + ps(\bar{y}) - 2ps(\bar{x} * \bar{y}),$$

mencionada en el ejemplo 2.4, obtenemos

$$2ps(\bar{x} * \bar{c}) = ps(\bar{x}) + ps(\bar{c}) - d(\bar{x},\bar{c}) \geq 2t+2$$

esto es $ps(\bar{x} * \bar{c}) \geq t+1 = ps(\bar{x})$, lo que significa que $\bar{c}$ cubre a $\bar{x}$. □

Ejemplo 4.9 Las palabras codificadas de peso 3 en el código binario de Hamming $\mathcal{H}_r$ sostienen un sistema triple de Steiner $S(2,3,2^r-1)$.

Corolario 4.2 *Sea C un $[n,k,d=2t+1]$ código binario perfecto. Entonces el número de palabras codificadas de peso d es*

$$\mathcal{A}_d = \begin{pmatrix} n \\ t+1 \end{pmatrix} / \begin{pmatrix} d \\ t+1 \end{pmatrix}.$$

Demostración: Por el teorema precedente S_d sostiene un $(t+1)$-$(n,d,1)$ diseño, y el número de bloques de este diseño es, de acuerdo a la proposición 4.1, precisamente $\mathcal{A}_d$. □

Ejemplo 4.10 Para el código de Hamming $\mathcal{H}_r$

$$\mathcal{A}_3 = \frac{(2^r-1)(2^{r-1}-1)}{3}.$$

También podemos probar un resultado acerca de diseños asociados con códigos extendidos:

Teorema 4.3 [34;63] *Sea C un código binario perfecto de longitud n y distancia mínima $d = 2t+1$. Sea $\hat{C}$ código extendido de C. Entonces las palabras codificadas de peso $2t+2$ en $\hat{C}$ forman un diseño $S(t+2, 2t+2, n+1)$.*

Demostración: Se desea probar que todo vector $\bar{u} \in \mathbf{F}_2^{n-1}$ de peso $t+2$ es cubierto por una única palabra codificada, en $\hat{C}$, de peso $2t+2$.

Sean $\bar{c}$ y $\bar{c}'$ son dos palabras codificadas de peso $2t+2$ en $\hat{C}$, las cuales cubren al vector $\bar{u} \in \mathbf{F}_2^{n+1}$ de peso $t+2$. Por la igualdad mostrada en el ejemplo 2.4,

$$d(\bar{c}, \bar{u}) = ps(\bar{c}) + ps(\bar{u}) - 2ps(\bar{c} * \bar{u}) = (2t+2) + (t+2) - 2(t+2) = t.$$

Entonces $\bar{u}$ está en la esfera con centro en $\bar{c}$ y radio t, $B_t(\bar{c})$. Igualmente se prueba que $\bar{u}$ también está en $B_t(\bar{c}')$, lo cual contradice que el código sea perfecto. Esto muestra la unicidad de la palabra codificada de peso $2t+2$ en $\hat{C}$.

Supóngase que la $(n+1)$-ésima posición coordenada de las palabras codificadas en $\hat{C}$ es el chequeo de paridad total, que se agregó al código C para formar a $\hat{C}$.

Sea $\bar{u} \in \mathbf{F}_2^{n+1}$ un vector de peso $t+2$ con 1's en las entradas $i_1, i_2, \ldots, i_{t+2}$, con $i_1 < \cdots < i_{t+2}$. Se denotará como $\bar{u}'$ al vector que resulta cuando se suprime de $\bar{u}$ la última posición coordenada. Para garantizar la existencia de la palabra codificada en $\hat{C}$ de peso $2t+2$ se consideran dos casos:

Si $i_{t+2} = n+1$ entonces $\bar{u}'$ es de peso $t+1$. Ya que C es perfecto y corrige t errores de transmisión existe una palabra $\bar{c} \in C$ tal que $d(\bar{u}', \bar{c}) \leq t$. Así pues se tiene

$$\begin{aligned} t &\geq d(\bar{u}', \bar{c}) = ps(\bar{c}) + ps(\bar{u}') - 2ps(\bar{u}' * \bar{c}) \\ &\geq ps(\bar{c}) + (t+1) - 2ps(\bar{u}' * \bar{c}). \end{aligned}$$

Esto siginfica que $2ps(\bar{u}' * \bar{c}) \geq ps(\bar{c}) + 1 \geq 2t+2$, por lo tanto se cumplen ambas igualdades y $\bar{c}$ cubre a $\bar{u}'$. Este argumento prueba además que $\bar{c}$ es de peso $2t+1$, entonces $\mid \bar{c} \mid 1 \mid$ está en $\hat{C}$ cubre a $\bar{u}$ y es de peso $2t+2$.

Un razonamiento análogo para el caso $i_{t+2} < n+1$ muestra que $\bar{u}'$ es cubierto por una palabra $\bar{c}$ en C de peso $2t+1$ ó $2t+2$. Al agregarle a esta palabra codificada el chequeo de paridad total se obtiene el resultado deseado. □

Corolario 4.3 *El número de palabras codificadas de peso 4 en $\hat{\mathcal{H}}_r$ es*

$$\binom{2^r}{3} / \binom{4}{3} = \frac{2^{r-2}(2^r-1)(2^{r-1}-1)}{3}.$$

Teorema 4.4 [5;85], [34;177] (**Assmus-Mattson**) *Sea C un $[n,k,d]$ código q-ario y sea $d^\perp$ la distancia mínima de $C^\perp$. Sea $w=2$ cuando $q=2$, en otro caso el mayor entero w tal que*

$$w-(w+q-2)/(q-1)<d,$$

y defínase $w^\perp$ similarmente. Supóngase que existe un entero t con $0<t<d$ que satisface la siguiente condición: si el polinomio enumerador de peso de $C^\perp$ es $W_C^\perp(x)=\sum_{i=1}^n A_i x^i$, entonces a lo más $d-t$ de los $A_1,\ldots,A_{n-t}$ son no cero. Entonces para cada i con $d\leq i\leq w$ los soportes de los vectores de peso i de C, si existen, sostienen un t-diseño. Similarmente, para cada j con $d^\perp\leq j\leq min\{w^\perp,n-t\}$ los soportes de los vectores de peso j en $C^\perp$, si existen, forman un t-diseño.

4.3 Geometría Afín

Sea $V=\mathbf{F}_q^n$. La **geometría afín finita** de dimensión n sobre $\mathbf{F}_q$, $GA(V)=GA(n,q)$ es aquella cuyos **puntos** son los vectores de V, y si U es un subespacio de V de dimensión t, un t-plano de $GA(V)$ es $\bar{v}+U$, donde $\bar{v}\in V$. La estuctura de $GA(V)$ es dada por la contención como conjuntos. Por lo tanto un punto es un 0-plano, los 1-planos son **líneas** de la geometría, a los 2-planos se les llama **planos** y los $(n-1)$-planos se conocen como **hiperplanos** en $GA(V)$.

Un m-plano y un l-plano en $GA(V)$, $\bar{x}+U$ y $\bar{y}+W$, respectivamente se dicen **paralelos** si $U\subseteq W$ o $W\subset U$.

Un subespacio U de dimensión t de $V=\mathbf{F}_q^n$ es un código lineal, por lo tanto tiene una matriz de chequeo de paridad H, de $(n-t)\times n$ que cumple

$$\bar{x}\in U \text{ si y sólo si } H\bar{x}^t=0.$$

Sea $\bar{v}+U$ un t-plano de $GA(\mathbf{F}_q^n)$, entonces $\bar{x}\in\bar{v}+U$ si y sólo si $\bar{x}-\bar{v}\in U$, lo cual equivale a pedir que $H(\bar{x}-\bar{v})^t=\mathbf{0}$, esto es

$$\bar{x}\in\bar{v}+U \text{ si y sólo si } H\bar{x}^t=H\bar{v}^t.$$

Esto significa que los vectores en $\bar{v}+U$ son precisamente las soluciones de un sistema de $n-t$ ecuaciones lineales independientes en n indeterminadas (si el sistema es homogéneo su conjunto de soluciones es U, en caso contrario es un t-plano que no contiene a $\mathbf{0}\in V$).

Nuestra intención es ver a las geometrías finitas como diseños de bloques, para lo cual es necesaria la siguiente información:

Todo l-plano en $GA(n,q)$ satisface $n-l$ ecuaciones lineales independientes de la forma

$$\sum_{j=1}^{m} a_{ij}x_j = b_i, \quad i = 1,\ldots,(n-l) \quad a_{ij}, b_i \in \mathbf{F}_q,$$

Cuando $b_i = 0$ para todo i las ecuaciones definen un espacio vectorial de dimensión l de $\mathbf{F}_q^n$, y ya que para cada uno de los sistemas de ecuaciones anteriores los b_i pueden ser elegidos de q^{n-l} maneras distintas, por el teorema 2.7 el número de l-planos en $GA(n,q)$ es

$$q^{n-l}\begin{bmatrix} n \\ l \end{bmatrix}_q = q^{n-l}\prod_{t=0}^{l-1}\frac{q^{n-t}-1}{q^{l-t}-1}.$$

Se ha probado el siguiente:

Teorema 4.5 [34; 699] *El número de geometrías afines $GA(l,q)$ en una geometría $GA(n,q)$ dada, es*

$$q^{n-l}\begin{bmatrix} n \\ l \end{bmatrix}_q = q^{n-l}\prod_{t=0}^{l-1}\frac{q^{n-t}-1}{q^{l-t}-1}.$$

En particular existen

$$q^{n-1}\frac{q^n-1}{q-1}$$

líneas en $GA(n,q)$ y por la forma en que se definieron cada línea contiene q puntos.

Sea $\bar{v}+W$ un l-plano de la geometría $GA(n,q)$, ya que todo m-plano de la geometría que lo contenga puede ser escrito como $\bar{v}+U$, donde W es un subespacio vectorial de U, el número de m-planos conteniendo un l-plano dado en $GA(n,q)$ es justo el de $(m-l)$-subespacios en un $(n-l)$-espacio. Por ejemplo si V, U y W son espacios vectoriales de dimensión n, m y l, respectivamente, entonces $V = W \oplus X$ y $U = W \oplus Y$, donde X y Y son espacios vectoriales de dimensión $n-l$ y $m-l$, respectivamente.

Resumiendo, tenemos el siguiente

Teorema 4.6 [34;699] *Sean l, m y n enteros positivos tales que $l < m < n$. El número de $GA(m,q)$ que contienen una $GA(l.q)$ dada, en $GA(n,q)$, es*

$$\begin{bmatrix} n-l \\ m-l \end{bmatrix}_q = \prod_{k=l+1}^{m} \frac{q^{n-k+1}-1}{q^{m-k+1}-1}.$$

Sea W un espacio vectorial de dimensión n, el grupo de transformaciones lineales invertibles de W en sí mismo, denotado como $GL(W)$, se conoce como el **grupo lineal general** de W. Ya que un espacio vectorial de dimensión finita queda determinado de manera única, salvo isomorfismo, por su dimensión y su campo de escalares, en algunas ocasiones el grupo $GL(W)$ será denotado como $GL(n,q)$, si W es un espacio vectorial de dimensión n sobre $\mathbf{F}_q$. Para calcular el orden de este grupo debe notarse que es exactamente el número de formas en las cuales se puede enviar una base de W a otra de sus bases. Este es el número maneras de elegir, de W, n vectores linealmente independientes, el cual es, de acuerdo a la demostración del teorema 2.7:

$$\mid GL(n,q) \mid = (q^n-1)(q^n-q)\cdots(q^n-q^{k-1}) = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1).$$

El subgrupo de $GL(V)$ de las transformaciones lineales con determinante 1 es llamado el **grupo lineal especial** o **unimodular**, se denota por $SL(W)$, o en el caso de que W es un espacio sobre $\mathbf{F}_q$ como $SL(n,q)$. El orden de $SL(n,q)$ es $\frac{1}{q-1} \mid GL(n,q) \mid$, pues si $T \in SL(n.q)$ y $\alpha \in \mathbf{F}_q^*$ entonces $\alpha T \in GL(n,q)$, esto es por cada elemento de $SL(n.q)$ existen $q-1$ elementos en $GL(n,q)$.

Definición 4.11 *Sean i, j dos enteros distintos. $1 \leq i.j \leq n$ y 1_{ij} la matriz que tiene un 1 en la entrada i,j y cero en las restantes. Una matriz de $n \times n$ se dice* **elemental** *si es de la forma $I + c1_{ij}$, donde $c \in \mathbf{F}_q$ e I es la matriz identidad $n \times n$. Definimos $E_{ij}(c) = I + c1_{ij}$.*

Es inmediato verificar que el determinante de una matriz elemental es 1, y que si A es cualquier matriz de $n \times n$, la multiplicación $E_{ij}(c)A$ añade c veces el j-ésimo renglón de A al i-ésimo, y que $AE_{ij}(c)$ equivale a sumar c veces la i-ésima columna de A a su j-ésima columna. Para i fijo, diferente de j, la función del grupo aditivo $\mathbf{F}_q$ en el grupo multiplicativo $GL(V)$ dada por $c \mapsto E_{ij}(c)$ es un homomorfismo como puede verificarse inmediatamente.

Proposición 4.6 [32; 541] *El grupo $SL(V)$ es generado por las matrices elementales. Si $A \in GL(V)$ entonces $A = SD$, donde $S \in SL(V)$ y D es una matriz diagonal de la forma*

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d \end{pmatrix}.$$

Demostración: Sea $A = (a_{ij}) \in GL(V)$. La primera entrada de algún renglón de A es distinta de cero, (pues de no ser así A sería singular), y por una operación elemental de renglones es posible hacer a_{11} diferente de cero. Añadiendo un múltiplo adecuado del primer renglón al segundo puede hacerse a_{21} distinto de cero, y enseguida sumar un múltiplo del segundo renglón al primero para obtener $a_{11} = 1$. Después se suman múltiplos del primer renglón a los restantes para que la primera columna de A ahora sólo contenga un 1 en la primera entrada y 0 en las restantes.

Repitiendo el procedimiento con el segundo renglón y columna hacemos $a_{22} = 1$ y $a_{i2} = 0$ si $i > 2$. Entonces puede hacerse $a_{12} = 0$ sumando un múltiplo adecuado del segundo renglón al primero, y se obtiene $a_{i2} = 0$ para i diferente de 2.

Continuamos con este procedimiento hasta obtener $a_{nn} = d$, un elemento no nulo, y $a_{nj} = 0$ para j distinto de n. Entonces añadiendo un múltiplo del último renglón a los restantes se obtiene la matriz D, y la prueba está completa. □

Ejemplo 4.11 $SL(\mathbf{F}_2^3) = SL(2,3)$ es generado por las matrices

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

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

Teorema 4.7 [32; 541] *Para $n \geq 3$. $SL(V)$ es igual a su propio grupo conmutador.*

Demostración: Ya que $n \geq 3$ pueden elegirse tres enteros distintos i, j, k entre 1 y n. Entonces

$$E_{ij}(c) = E_{ik}(c)E_{kj}(1)E_{ik}(-c)E_{kj}(-1)$$

esto es, $E_{ij}(c)$ es un conmutador. □

Si G es un grupo de permutaciones sobre el conjunto A, con $\mid A \mid = k$, se dice que G es de **grado** k. Además diremos que G es t-**transitivo** si para cualesquiera dos t-adas ordenadas de elementos distintos de A, digamos $(a_1, a_2 \ldots, a_t)$,$(b_1, b_2, \ldots, b_t)$ existe $\sigma \in G$ tal que $a_i\sigma = b_i$; $i = 1, 2, \ldots, t$. A los grupos t-transitivos también se les conoce como **doblemente transitivos** si $t = 2$, **triplemente transitivos** cuando $t = 3$, y así sucesivamente. (cf. [23])

El grupo, bajo la composición, consistente de las transformaciones de la forma $\bar{y} = A\bar{x} + \bar{v} = (A, \bar{v})\bar{x}$ definidas operando de $\mathbf{F}_q^n$ en sí mismo, con $A \in GL(n, q)$, es llamado el **grupo lineal general no homogéneo** o **grupo lineal general afín**,denotado por $GLA(n, q)$.

Cada una de tales transformaciones se denomina **transformación afín**. El orden de este grupo es fácil de calcular pues ya conocemos el orden de $GL(n, q)$ y el vector $\bar{v}$ puede ser elegido de q^n formas así que

$$\mid GLA(n, q) \mid = q^{n+[n(n-1)/2]} \prod_{i=0}^{n} (q^i - 1).$$

Todo elemento de $GLA(n, q)$ preserva clases de espacios vectoriales, y por lo tanto actúa en $GA(n, q)$. La composición está dada por $(A, \bar{v})(B\bar{w}) = (AB, \bar{v}B + \bar{w})$.

El grupo $GLA(1, q)$, llamado frecuentemente **grupo afín**, consta de las transformaciones de la forma $\bar{y} = a\bar{x} + b$. con $a, b \in \mathbf{F}_q$ y a no cero, este es un grupo de orden $q(q-1)$ y grado q. $GLA(1, q)$ permuta los elementos de $\mathbf{F}_q$, pues si $\bar{y} = a\bar{x} + b = a\bar{z} + b$ entones $\bar{x} = \bar{z}$. Es más, este grupo es 2-transitivo o doblemente transitivo, en efecto elijamos dos parejas ordenadas $(a_1, a_2), (b_1, b_2)$ de elementos de A, con la condición de que la primera entrada no coincida con la segunda, entonces las ecuaciones

$$b_1 = aa_1 + b, \text{ y } b_2 = aa_2 + b$$

pueden resolverse para a y b de forma única, obteniendo

$$a = \frac{b_1 - b_2}{a_1 - a_2}, \quad b = \frac{a_1 b_2 - a_2 b_1}{a_1 - a_2}.$$

Definición 4.12 *Sean V y W espacios vectoriales sobre el campo $\mathbf{F}_q$. Una* **transformación semilineal** *de V en W es una función $T : V \to W$ junto con un automorfismo, σ, del campo $\mathbf{F}_q$, tales que se satisface:*

$$T(\bar{u} + \bar{v}) = T\bar{u} + T\bar{v}, \quad \forall\, \bar{u}, \bar{v} \in V$$
$$T(a\bar{v}) = \sigma(a)T(\bar{v}) \quad \forall\, a \in \mathbf{F}_q,\ \forall\, \bar{v} \in V.$$

Utilizaremos la notación (σ, T) para la transformación semilineal T cuando deseemos enfatizar que σ es su automorfismo asociado. Resulta claro que una transformación semilineal lleva subespacios en subespacios preservando contenciones. La composición de transformaciones semilineales es otra vez semilineal, de la definición es sencillo verificar que $(\mu, S)(\sigma, T) = (\mu\sigma, ST)$. Esto es cuando $V = W$ el conjunto de los isomorfismos semilineales forma un grupo, denotado como $\Gamma L(V)$, y la función $\psi : (\sigma, T) \mapsto \sigma$ es un homomorfismo de $\Gamma L(V)$ al grupo de Galois de $\mathbf{F}_q$ (el grupo de automorfismos de $\mathbf{F}_q$). Ya que una transformación semilineal es lineal precisamente cuando el automorfismo asociado es la identidad, el núcleo del homomorfismo ψ es claramente el grupo $GL(V)$.

Expresemos matricialmente a las transformaciones semilineales. Sean $\{\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_m\}$ y $\{\bar{w}_1, \bar{w}_2, \ldots, \bar{w}_n\}$, bases ordenadas de V y W respectivamente. Si $T(\bar{v}_i) = \sum_{j=1}^{n} a_{ij} w_j$, $A = (a_{ij})$ entonces, utilizando el isomorfismo natural entre V y $\mathbf{F}_q^m$ así como entre W y $\mathbf{F}_q^n$

$$T : (x_1, x_2, \ldots, x_m) \mapsto A(\sigma(x_1), \sigma(x_2), , \ldots, \sigma(x_m))^t$$

Es fácil verificar que matricialmente la composición de las transformaciones semilineales (σ, A) y (ρ, B) resulta $(\rho\sigma, B A^{\rho})$, donde A^{ρ} denota la matriz (ρa_{ij}). Es claro que cualquier matriz invertible A, y cualquier automorfismo σ producen una transformación semilineal. por lo tanto si $V = W$ la función $\psi : (\sigma, T) \mapsto \sigma$, es un homomorfismo *sobre* el grupo de Galois de $\mathbf{F}_q$. Por lo tanto, para un espacio vectorial dado, digamos V, el grupo de isomorfismos semilineales de V contiene a $GL(V)$ como subgrupo normal (por ser el núcleo de ψ), siendo el grupo cociente el grupo de Galois de $\mathbf{F}_q$ (por el primer teorema del homomorfismo), el cual es cíclico (ver [17;420]).

Hemos visto que el grupo $\Gamma L(V)$ envía subespacios en subespacios. Para que pueda actuar sobre la geometría afín de V debe de tenerse además a V mismo actuando por translación. Por esto se define el **grupo semilineal afín** $\Gamma LA(n,q)$ como el grupo de las transformaciones $(T,\bar{v})$ definidas, para cada $\bar{x} \in V$, de la siguiente manera:

$$(T,\bar{v})(\bar{x}) = T(\bar{x}) + \bar{v}, \quad T \in \Gamma L(V),\ \bar{v} \in V.$$

La composición de estas funciones está dada como $(T,\bar{v})(S,\bar{w}) = (TS, T\bar{w} + v)$. Es inmediato verificar que la acción de estas transformaciones es doblemente transitiva, sobre los puntos de $GA(V)$, cuando son vistas como grupo de permutaciones sobre la geometría.

Sea $\{\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_n\}$ una base ordenada de V. Si $\bar{v} = \sum_{i=1}^{n} b_i \bar{v}_i$ y $(T,\bar{v})$ es un elemento de $\Gamma LA(V)$ con $T(\bar{v}_i) = \sum_{j=1}^{n} a_{ij}\bar{v}_j$ se define la matriz $A = (a_{ij})$. Para una automorfismo σ de $\mathbf{F}_q$, asociado a T se tiene

$$(T,\bar{v}) : (x_1, \ldots, x_n) \mapsto A(\sigma(x_1), \ldots, \sigma(x_n))^t + (b_1, \ldots, b_n).$$

Denotando esta transformación matricial como la tripleta

$$(\sigma, A, (b_1, \ldots, b_n)),$$

podemos reescribir la composición de la siguiente manera:

$$(\tau, B, (c_1, \ldots, c_n))(\sigma, A, (b_1, \ldots, b_n)) = (\tau\sigma, BA^{\tau}, (\tau(b_1) + c_1, \ldots, \tau(b_n) + c_n)).$$

Definición 4.13 *Sean V y W dos espacios vectoriales de dimensión finita sobre el mismo campo finito. Se dice que las geometrías $GA(V)$ y $GA(W)$ son* **isomorfas** *si existe una trasformación biyectiva $\phi : GA(V) \to GA(W)$, tal que para $U, U' \in GA(V)$, se cumple $U \subseteq U'$, si y sólo si $\phi(U) \subseteq \phi(U')$. Si $V = W$ tal función se denomina* **automorfismo** *de V.*

El *teorema fundamental de la geometría afín* afirma que si V es un espacio vectorial de dimensión al menos 2 entonces $Aut(GA(V)) = \Gamma LA(V)$. (La prueba se difiere a la siguiente sección).

Para cada subespacio U de V defínase la geometría afín $GA(\bar{x}+U)$ como aquella formada por los t-planos en $GA(V)$ contenidos en $\bar{x} + U$. Entonces $GA(\bar{x} + U)$ es isomorfa a $GA(U)$ pues todo elemento de $GA(\bar{x} + U)$ puede escribirse de la forma $\bar{x} + U'$ para un subespacio U' de U.

4.4 Geometría Proyectiva

Los fundamentos para la Geometría Proyectiva fueron propuestos primero por el italiano Gino Fano, en 1892, (cf. [16]). Fano describió una geometría de dimensión 2 en la cual el número de puntos es $p+1$, para un primo fijo p. En 1906 O. Veblen y W.H. Bussey denotaron a esta geometría como $PG(2,p)$, dando además una extensión a $PG(n,q)$, donde n es un entero positivo y q es una potencia de un primo p (ver [52]). Más tarde, en 1938, O. Veblen y J.W. Young escribieron el primer libro sobre este tema, presentando un estudio extenso sobre estas geometrías (cf. [53]), las cuales denotaremos, en el presente escrito, como $GP(n,q)$.

Si V es un espacio vectorial de dimensión $n+1$ sobre el campo finito de orden q, la **geometría proyectiva finita** de V, denotada $GP(V) = GP(n,q)$, es aquella cuyos elementos son los subespacios de V a los cuales se les ha suprimido el punto de coordenadas $(0,0,\ldots,0)$ y su estructura es dada por la contención como conjuntos. La dimensión de $GP(V)$ se define como n, similarmente la **dimensión proyectiva** de un *subespacio proyectivo*, esto es un subespacio de V sin el origen, es definido como una unidad menor que la dimensión del subespacio (visto como subespacio de V).

Con esta definición tenemos por ejemplo que: los puntos de $GP(V)$ son los subespacios de dimensión 1 de V, las **líneas** son los subespacios de dimensión 2 de V, los **planos** los subespacios de V de dimensión 3, y los **hiperplanos** los subespacios de dimensión n de V; todos estos subespacios proyectivos sin el origen, como se han definido.

Existe otra manera de definir una geometría proyectiva: considérese al espacio vectorial V de dimensión $n+1$ sobre $\mathbf{F}_q$. Identifiquemos los vectores no cero de este espacio módulo la relación de equivalencia

$$\bar{u} \equiv \bar{v} \quad \Longleftrightarrow \quad \bar{u} = \lambda \bar{v}.\ \lambda \in \mathbf{F}_q,$$

a cada clase de equivalencia le llamaremos **punto.** Para las **líneas** conteniendo dos puntos distintos $p_1 = (a_1, a_2, \ldots, a_{n+1})$ y $p_2 = (b_1, b_2, \ldots, b_{n+1})$ se toma al conjunto de puntos

$$\alpha p_1 + \beta p_2 = (\alpha a_1 + \beta b_2, \ldots, \alpha a_{n+1} + \beta b_{n+1})$$

donde α y β son elementos de $\mathbf{F}_q$ tales que por lo menos uno de ellos es distinto de cero. La definición de los subespacios proyectivos se hace de manera

similar a la definición dada anteriormente. Claramente ambas definiciones son equivalentes.

Una geometría proyectiva también puede definirse axiomaticamente, como se hace en [9], [12] y [34], pero para los fines de este trabajo es suficiente con la definición dada.

Ejemplo 4.12 El plano de Fano es una geometría proyectiva $GP(2,2)$, en efecto si etiquetamos los puntos de esta geometría de la siguiente forma

$$\begin{array}{llll} 011 \mapsto 1 & 001 \mapsto 2 & 010 \mapsto 3 & 110 \mapsto 4 \\ 100 \mapsto 5 & 111 \mapsto 6 & 101 \mapsto 7 & \end{array}$$

resulta el plano de Fano mostrado en la figura 2 de la página 53.

Como en la pasada sección calcularemos la cardinalidad de ciertos conjuntos de subespacios, los cuales nos permitirán asociar un diseño a cada geometría proyectiva finita:

Teorema 4.8 [34;696] *El número de geometrías proyectivas de dimensión m sobre $\mathbf{F}_q$, $GP(m,q)$, contenidas en una geometría proyectiva dada de dimensión n sobre el mismo campo, $GP(n,q)$, es*

$$\left[\begin{array}{c} n+1 \\ m+1 \end{array} \right]_q = \prod_{t=0}^{m} \frac{q^{n+1-t}-1}{q^{m+1-t}-1}.$$

Demostración: Por definición de geometría proyectiva finita, el número que se busca es precisamente el número de subespacios vectoriales de dimensión $m+1$, contenidos en un espacio vectorial de dimensión n. Por lo tanto esta cantidad es el coeficiente binomial gaussiano mostrado en el teorema. □

Teorema 4.9 [34;698] *Sean l, m y n enteros positivos tales que $l < m < n$. El número de geometrías proyectivas de dimensión m sobre $\mathbf{F}_q$, $GP(m,q)$, que contienen una geometría proyectiva de dimensión l sobre el mismo campo, $GP(l,q)$, ambas contenidas en la geometría $GP(n,q)$, es*

$$\left[\begin{array}{c} n-l \\ m-l \end{array} \right]_q = \prod_{k=l+1}^{m} \frac{q^{n-k-1}-1}{q^{m-k-1}-1}.$$

Demostración: Es la misma que la prueba que se dió para el resultado análogo en el caso afín. □

Para examinar cuándo dos geometrías proyectivas son esencialmente las mismas, debemos de poner atención en las funciones que preserven incidencias, esto es si $\phi : GP(V) \rightarrow GP(W)$, entonces para cualesquiera subespacios U y U' de V tales que $U \subseteq U'$ debemos de tener $\phi(U) \subseteq \phi(U')$. Con esto en mente enunciamos la

Definición 4.14 *Si V y W son espacios vectoriales de dimensión finita, sobre el mismo campo finito, entonces las geometrías $GP(V)$ y $GP(W)$ son* **isomorfas** *si existe una biyección*

$$\phi : GP(V) \longrightarrow GP(W)$$

tal que, para $U, U' \in GP(V)$, $U \subseteq U'$ si y sólo si $\phi(U) \subseteq \phi(U')$. Cuando $W = V$ tal función ϕ se denomina **automorfismo** *o* **colineación** *de $GP(V)$.*

La dimensión de $GP(n, q)$ es igual a la longitud de la mayor cadena $U_1, U_2, \ldots, U_k$ de subespacios no cero de $V = \mathbf{F}_q^{n+1}$, distintos de V, tales que $U_1 \subset U_2 \subset \ldots \subset U_k$, con la contención estricta, se sigue que geometrías isomorfas tienen la misma dimensión proyectiva. Obviamente toda transformación lineal invertible, de V en W, inducirá un isomorfismo, pero estas no son las únicas; como veremos más adelante todo automorfismo es inducido por una transformación semilineal, este es el teorema fundamental de la geometría proyectiva.

Resulta claro que una transformación semilineal T (ver la sección anterior), lleva subespacios en subespacios preservando contenciones, y así induce una función que preserva incidencias en las geometrías proyectivas. Será un isomorfismo de espacios proyectivos si T es un isomorfismo de la estructura aditiva de V, siendo T^{-1} su inversa, y el automorfismo asociado de este será el inverso del automorfismo asociado a T.

Recuérdese que $GL(V)$ es el grupo de transformaciones lineales invertibles de V en sí mismo. Identificando las transformaciones de este grupo que son múltiplos escalares no cero una de la otra, resulta un grupo, denotado como $P(V)$, denominado **grupo proyectivo**. En el caso de que V sea un espacio vectorial de dimensión n sobre el campo $\mathbf{F}_q$ este grupo también se escribirá como $P(n, q)$, su orden es

$$\mid P(n,q) \mid = \frac{1}{q-1} \mid GL(n+1,q) \mid .$$

Cada elemento de $P(n,q)$ es una transformación inyectiva de $GP(n,q)$ sobre sí misma. Además cada elemento de $P(n,q)$ envía una línea en $GP(n,q)$ en una línea. Ya que cada elemento de $P(n,q)$ permuta los puntos de $GP(n,q)$, este grupo se puede representar naturalmente como un grupo de permutaciones con grado $1+q+\cdots+q^n$, esto es un grupo de permutaciones sobre un conjunto de cardinalidad $1+q+\cdots+q^n$.

Proposición 4.7 [9; 104] *El grupo $P(n,q)$ es doblemente transitivo.*

Demostración: Sean $\{\beta,\gamma\}$ y $\{\beta',\gamma'\}$ dos conjuntos de puntos de la geometría $GP(n-1,q)$. Por la definición de geometría proyectiva, estos conjuntos son linealmente independientes cuando son vistos en $\mathbf{F}_q^n$. Por lo tanto puede completarse cada uno de ellos a una base del espacio $\mathbf{F}_q^n$. Así existe una transformación lineal invertible que envía β en β' y γ en γ'. □

Es obvio que todo isomorfismo semilineal de V induce un isomorfismo de $GP(V)$. Las trasformaciones escalares inducen el isomorfismo identidad, es más, estas son las únicas con esta propiedad como lo muestra la

Proposición 4.8 [5; 93] *Sea V un espacio de dimensión finita sobre el campo $\mathbf{F}_q$. Si un isomorfismo semilineal T induce el isomorfismo identidad en $GP(V)$, entonces T es una función escalar.*

Demostración: Que T sea la identidad en $GP(V)$ significa que $T(U)=U$, para todo subespacio U de V. En particular $T(\bar{v}_i)=a_i\bar{v}_i$ para todo $\bar{v}_i$ en una base de V, con $a_i\in\mathbf{F}_q$, además para $\bar{v}_i,\bar{v}_j\in V$ existe un elemento $a\in\mathbf{F}_q$ tal que $(\bar{v}_i+\bar{v}_j)T=a(\bar{v}_i+\bar{v}_j)$. Utilizando la aditividad de T se concluye que $a_i=a=a_j$. □

Es posible mostrar más sobre estas transformaciones escalares. Supóngase que una matriz $M=(a_{ij})$ conmuta con toda matriz invertible, entonces conmuta con toda matriz elemental $I+c1_{ij}$, así que $M1_{ij}=1_{ij}M$. Si $M1_{ij}=(c_{lm})$, de la última igualdad tenemos las relaciones

$$\begin{aligned} c_{ik} &= a_{jk}, \quad 0\le k\le n \\ c_{kj} &= a_{ki}, \quad 0\le k\le n \\ c_{lm} &= 0 \quad \text{en otro caso} \end{aligned}$$

además $a_{jk} = 0$ si k es distinto de i y $a_{kj} = 0$ si k es diferente de j. De ahí que $M1_{ij} = c_{ij}1_{ij}$, pero $c_{ij} = a_{jj} = a_{ii}$ por lo tanto $M = aI$, $a \in \mathbf{F}_q$. Esto muestra que el centro de $GL(V)$ es el grupo de matrices escalares. En particular si $M \in SL(V)$ entonces $\mid M \mid = 1 = a^n$ y el centro de $SL(V)$ consta de todas las matrices en $\mu_n(\mathbf{F}_q)I$, donde $\mu_n(\mathbf{F}_q)$ es el conjunto de las raices n-ésimas de la unidad en $\mathbf{F}_q$. El grupo cociente de $GL(V)$ y su centro es llamado el **grupo proyectivo lineal general,** es denotado por $GLP(V)$, y cuando V es el espacio vectorial de dimensión n sobre el campo finito de orden q se denotará como $GLP(n, q)$. El orden de este grupo es

$$\mid GLP(n,q) \mid = \frac{1}{q-1} \mid GL(n,q) \mid,$$

pues si N es un subgrupo normal del grupo M se cumple que $\mid M/N \mid$ es precisamente $\mid M \mid / \mid N \mid$ (cf. [17; 113]). Si Z es el centro de $SL(V)$ se define el **grupo proyectivo lineal especial** $PSL(V)$ como $PSL(V) = SL(V)/Z$, y en el caso de que V sea de dimensión n sobre $\mathbf{F}_q$ se denotará como $PSL(n, q)$

Teorema 4.10 [32; 544] *El grupo $PSL(n, q)$ es simple para $n \geq 3$.*

El centro de $GL(V)$ es un subgrupo normal en $\Gamma L(V)$, su cociente se denota como $\Gamma LP(V)$, y se denomina **grupo proyectivo semilineal.**

Todas las colineaciones de $GP(V)$ son inducidas por transformaciones semilineales; como lo afirma el siguiente

Teorema 4.11 [2; cap. 2] **(Teorema Fundamental de la Geometría Proyectiva)** *Sea V un espacio vectorial de dimenión al menos tres sobre el campo K. Entonces el grupo de automorfismos de $GP(V)$ coincide con $\Gamma LP(V)$.*

Demostración: En la prueba se hará uso frecuentemente de que si U es un subespacio de V tal que $U = L_1 + L_2 + \cdots + L_r$, donde cada L_i es una recta en V, y σ es un automorfismo de $GP(V)$ entonces $\sigma(U) = \sigma(L_1) + \cdots + \sigma(L_r)$; esto es, σ está completamente determinado si se conoce su restricción a cada recta de V. Para una mejor comprensión la prueba se dividide en doce puntos.

Paso 1: Se probará por inducción sobre r que $L \subset L_1 + \cdots + L_r$ implica que $\sigma L \subset \sigma L_1 + \cdots + \sigma L_r$. En el caso $L = L_r$ no hay nada que probar.

supóngase pues que L no es L_r. L es generado por un vector $\bar{u}+\bar{v}$, donde $\bar{u}\in L_1+\cdots+L_{r-1}$, $\bar{u}$ no nulo y $\bar{v}\in L_r$. Entonces

$$\sigma\langle\bar{u}\rangle\subset\sigma L_1+\cdots+\sigma L_{r-1}$$

por hipótesis de inducción. Como $L\subset\langle\bar{u}\rangle+L_r$ se tiene $\sigma L\subset\sigma\langle\bar{u}\rangle+\sigma L_r$.

Paso 2: Ya que se utilizará frecuentemente el razonamiento anterior lo abstraemos aquí: Sean $\bar{c}$ y $\bar{d}$ vectores linealmente independientes, y sea $L\subset\langle\bar{c}\rangle+\langle\bar{d}\rangle$, con L distinto de $\langle\bar{d}\rangle$. Bajo estas condiciones L es generado por un vector de la forma $a\bar{c}+b\bar{d}$ con $\bar{a}$ no nulo, para más comodidad se toma al vector $\bar{c}+a^{-1}b\bar{d}=\bar{c}+e\bar{d}$, como el generador, el elemento d es por lo tanto determinado de manera única por L.

Paso 3: Sean $\{\bar{v}_i\}_{i=1}^n$ una base de V y $L_i=\langle\bar{v}_i\rangle$, entonces $V=L_1+\cdots+L_n$. Ya que σ es biyectiva, $\sigma L_i=\langle\bar{v}_i'\rangle$ es también una base de V. La recta $\sigma\langle\bar{v}_1+\bar{v}_i\rangle\subset\langle\bar{v}_1'\rangle+\langle\bar{v}_i'\rangle$ es distinta de $\langle\bar{v}_i'\rangle$ si $i\geq 2$, por lo que $\sigma\langle\bar{v}_1+\bar{v}_i\rangle=\langle\bar{v}_1'+b_i\bar{v}_i'\rangle$, donde b_i no es cero pues $\langle\bar{v}_1+\bar{v}_i\rangle$ es distinto de $\langle\bar{v}_1\rangle$. Reemplazando $\bar{v}_i$ por $b_i\bar{v}_i'$ se obtiene $\sigma\langle\bar{v}_i\rangle=\langle\bar{v}_i'\rangle$ y $\sigma\langle\bar{v}_1+\bar{v}_i\rangle=\langle\bar{v}_1'\rangle+\langle\bar{v}_i'\rangle$ para $i\geq 2$.

Paso 4: Sea $x\in K$; $\langle\bar{v}_1+x\bar{v}_2\rangle$ y $\langle\bar{v}_1+x\bar{v}_2\rangle$ diferentes de $\langle\bar{v}_2\rangle$. Existe una única $x'\in K$ tal que $\sigma\langle\bar{v}_1+x\bar{v}_2\rangle=\langle\bar{v}_1'+x'\bar{v}_2'\rangle$ y, ya que si x es distinto de y; $\langle\bar{v}_1+x\bar{v}_2\rangle$ no es igual a $\langle\bar{v}_1+y\bar{v}_2\rangle$ tenemos x' diferente de y'. Se ha construido una función inyectiva de K en sí mismo dada por $x\mapsto x'$ de la cual se probará que es biyectiva. Por el paso (3) es claro que esta función envía los elementos neutros, tanto aditivo como multiplicativo, del campo sobre sí mismos, esto es $0'=0$ y $1'=1$.

Análogamente se puede construir una aplicación $x\mapsto x''$ tal que $\sigma\langle\bar{v}_1+x\bar{v}_3\rangle=\langle\bar{v}_1'+x''\bar{v}_3\rangle$, se probará que $x'\mapsto x''$, para todo $x\in K$. Puede suponerse que x es no nulo. La recta $\langle x\bar{v}_2-x\bar{v}_3\rangle$ está en los planos $\langle\bar{v}_2\rangle+\langle\bar{v}_3\rangle$ y $\langle\bar{v}_1+x\bar{v}_2\rangle+\langle\bar{v}_1+x\bar{v}_3\rangle$. Así que la imágen de la recta está contenida en los planos $\langle\bar{v}_2'\rangle+\langle\bar{v}_3'\rangle$ y $\langle\bar{v}_1'+x'\bar{v}_2'\rangle+\langle\bar{v}_1'+x''\bar{v}_3'\rangle$. La única posibilidad para la imagen de la recta es $\langle x'\bar{v}_2-x''\bar{v}_3\rangle$. Pero $\langle x\bar{v}_2-x\bar{v}_3\rangle=\langle\bar{v}_2-\bar{v}_3\rangle$ cuya imagen es, después del mismo razonamiento, $\langle 1'\bar{v}_2'-1''\bar{v}_3'\rangle=\langle\bar{v}_2'-\bar{v}_3'\rangle$, de donde resulta $x'=x''$. En lugar de $\bar{v}_3$ puede tomarse otro vector $\bar{v}_i$ con $i\geq 3$, por lo tanto existe una función $x\mapsto x'$ tal que para $i\geq 2$

$$\sigma\langle\bar{v}_1+x\bar{v}_i\rangle=\langle v_1'+x'\bar{v}_i'\rangle.$$

Paso 5: Se prueba por inducción que

$$\sigma\langle\bar{v}_1+x_2\bar{v}_2+\cdots+x_n\bar{v}_n\rangle=\langle\bar{v}_1'+x_2'\bar{v}_2'+\cdots+x_n'\bar{v}_n'\rangle.$$

Supóngase que

$$\sigma\langle \bar{v}_1 + x_2\bar{v}_2 + \cdots + x_{r-1}\bar{v}_{r-1}\rangle = \langle \bar{v}'_1 + x'_2\bar{v}'_2 + \cdots + x'_{r-1}\bar{v}'_{r-1}\rangle.$$

La recta $\langle \bar{v}_1 + x_2\bar{v}_2 + \cdots + x_r\bar{v}_r\rangle$ está en

$$\langle \bar{v}_1 + x_2\bar{v}_2 + \cdots + x_{r-1}\bar{v}_{r-1}\rangle + \langle \bar{v}_r\rangle,$$

y es distinta de $\langle \bar{v}_r\rangle$. Su imagen por consiguiente es generada por un vector de la forma

$$\bar{v}'_1 + x'_2\bar{v}'_2 + \cdots + x'_{r-1}\bar{v}'_{r-1} + u\bar{v}'_r.$$

La recta también está en

$$\langle \bar{v}_1 + x_r\bar{v}_r\rangle + \langle \bar{v}_2\rangle + \cdots + \langle \bar{v}_{r-1}\rangle$$

por lo que su imágen está en

$$\langle \bar{v}'_1 + x'_r\bar{v}'_r\rangle + \langle \bar{v}'_2\rangle + \cdots + \langle \bar{v}'_{r-1}\rangle.$$

Ya que en la expresión de la recta debe aparecer $\bar{v}'_1$ se tiene $u = x'_r$. Por lo tanto

$$\sigma\langle \bar{v}_1 + x_2\bar{v}_2 + \cdots + x_n\bar{v}_n\rangle = \langle \bar{v}'_1 + x'_2\bar{v}'_2 + \cdots + x'_n\bar{v}'_n\rangle.$$

Paso 6: La imágen de la recta $\langle x_2\bar{v}_2 + \cdots + x_n\bar{v}_n\rangle$ está en $\langle \bar{v}'_2\rangle + \cdots + \langle \bar{v}'_n\rangle$. La recta está también en $\langle \bar{v}_1 + x_2\bar{v}_2 + \cdots + x_n\bar{v}_n\rangle + \langle \bar{v}_1\rangle$, por lo que su imagen está en $\langle \bar{v}'_1 + x'_2\bar{v}'_2 + \cdots + x'_n\bar{v}'_n\rangle + \langle \bar{v}'_1\rangle$. De donde

$$\sigma\langle x_2\bar{v}_2 + \cdots + x_n\bar{v}_n\rangle = \langle x'_2\bar{v}'_2 + \cdots + x'_n\bar{v}'_n\rangle.$$

Paso 7: Por el paso anterior una recta de V de la forma $\langle \bar{v}'_1 + y\bar{v}'_2\rangle$ no es imagen de una recta en $\langle \bar{v}_2\rangle + \cdots + \langle \bar{v}_n\rangle$, debe ser la imagen de una recta

$$\langle \bar{v}_1 + x_2\bar{v}_2 + \cdots + x_n\bar{v}_n\rangle,$$

esto implica que $x'_2 = y$ por lo que la función $x \mapsto x'$ es suprayectiva.

Paso 8:

$$\sigma\langle \bar{v}_1 + (x+y)\bar{v}_2 + \bar{v}_3\rangle = \langle \bar{v}'_1 + (x+y)'\bar{v}'_2 + \bar{v}'_3\rangle.$$

pero

$$\langle \bar{v}_1 + (x+y)\bar{v}_2 + \bar{v}_3\rangle \subset \langle \bar{v}_1 + x\bar{v}_2\rangle + \langle y\bar{v}_2 + \bar{v}_3\rangle.$$

por lo que

$$\langle \bar{v}_1' + (x+y)'\bar{v}_2' + \bar{v}_3' \rangle \subset \langle \bar{v}_1' + x'\bar{v}_2' \rangle + \langle y'\bar{v}_2' + \bar{v}_3' \rangle.$$

Por lo tanto $(x+y)' = x' + y'$.

Paso 9:

$$\sigma\langle \bar{v}_1 + xy\bar{v}_2 + x\bar{v}_3 \rangle = \langle \bar{v}_1' + (xy)'\bar{v}_2' + x'\bar{v}_3' \rangle.$$

y

$$\langle \bar{v}_1 + xy\bar{v}_2 + x\bar{v}_3 \rangle \subset \langle \bar{v}_1 \rangle + \langle y\bar{v}_2 + \bar{v}_3 \rangle,$$

de donde

$$\langle \bar{v}_1' + (xy)'\bar{v}_2' + x'\bar{v}_3' \rangle \subset \langle \bar{v}_1' \rangle + \langle y'\bar{v}_2' + \bar{v}_3' \rangle.$$

De ahí que $(xy)' = x'y'$. Por lo tanto la función $x \mapsto x'$ es un automorfismo μ de K.

Si $x_1 = 0$ ó 1 en la recta $\langle x_1\bar{v}_1 + \cdots + x_n\bar{v}_n \rangle$ entonces su imagen es

$$\langle \mu(x_1)\bar{v}_1' + \cdots + \mu(x_n)\bar{v}_n' \rangle.$$

Si x_1 no es cero esta recta es la misma que

$$\langle \bar{v}_1 + x_1^{-1}x_2\bar{v}_2 + \cdots + x_1^{-1}x_n\bar{v}_n \rangle,$$

y su imagen

$$\langle \bar{v}_1' + \mu(x_1^{-1}x_2)\bar{v}_2' + \cdots + \mu(x_1^{-1}x_n)\bar{v}_n' \rangle,$$

es la misma recta que

$$\langle \mu(x_1)\bar{v}_1' + \cdots + \mu(x_n)\bar{v}_n' \rangle.$$

Paso 10: Sea λ el automorfismo semilineal de V, cuyo automorfismo de campo asociado es μ, el cual envía $\bar{v}_i$ en $\bar{v}_i'$. Para toda recta L de V se ha mostrado que $\sigma L = \lambda L$.

Paso 11: Supóngase que λ_1 es otro automorfismo semilineal de V que transforma las rectas de la misma manera que λ. Entonces $\lambda^{-1}\lambda$ es una función biyectiva de V en sí mismo que deja fija cada recta de V. Esta función envía cada vector no nulo $\bar{v}$ de V sobre un múltiplo escalar no nulo de $\bar{v}$. Si $\bar{v}$ y $\bar{u}$ son vectores linealmente independientes de V entonces los tres vectores $\bar{v}, \bar{u}$ y $\bar{v} + \bar{u}$ son transformados respectivamente en $a\bar{v}, b\bar{u}$ y $c(\bar{v} + \bar{u})$. Pero

$$\lambda_1^{-1}\lambda(\bar{v} + \bar{u}) = \lambda_1\lambda(\bar{v}) + \lambda_1^{-1}\lambda(\bar{u}) = a\bar{v} + b\bar{u}.$$

De donde $a = b$. Si $\bar{x}$ y $\bar{y}$ son linealmente dependientes pero no nulos y $\bar{w}$ es un tercer vector linealmente independiente de $\bar{x}$, entonces cuando $\bar{v}$ y $\bar{u}$ son transformados por $\lambda^{-1}\lambda_1$ aparecen multiplicados por el mismo factor que $\bar{w}$. Por lo tanto $\lambda^{-1}\lambda_1(\bar{v}) = a\bar{v}$, entonces la misma a funciona para todo vector de V por lo tanto $\lambda_1(\bar{v}) = \lambda(a\bar{v})$.

Paso 12: Sea a distinto de cero. Defínase la aplicación λ_1 por $\lambda_1(\bar{v}) = \lambda(x\bar{v})$. Para cualquier $b \in K$ se tiene

$$\lambda_1(b\bar{v}) = \lambda(ab\bar{v}) = \lambda(aba^{-1}a\bar{v}) = \mu(aba^{-1})\lambda_1(\bar{v}).$$

Por lo tanto λ_1 es semilineal y su isomorfismo asociado μ_1 está dado por $\mu_1(\bar{v}) = \mu(a\bar{v}a^{-1})$. Si $\bar{v}$ no es cero entonces $\lambda_1(\bar{v}) = \lambda(a\bar{v}) = \mu(a)\lambda(\bar{v})$, esto es, $\lambda_1\langle\bar{v}\rangle = \lambda\langle\bar{v}\rangle$ por lo que λ y λ_1 inducen la misma colineación. Con esto concluye la demostración del teorema. □

Entre los automorfismos de $GP(n, q)$ existe siempre un elemento de orden $v = (q^{n+1} - 1)/(q - 1)$ que permuta los puntos de la geometría en un único cíclo de longitud v, llamado el **ciclo de Singer**. La manera de construirlo es la siguiente:

Si ω es un elemento primitivo de $K = \mathbf{F}_{q^{n+1}}$, entonces K puede ser visto como un espacio vectorial de dimensión $n + 1$ sobre $F = \mathbf{F}_q$ con base $1, \omega, \ldots, \omega^n$. El orden de ω^v es $q^{n+1} - 1/\text{mcd}\{q^{n-1}, v\} = q - 1$, donde $\text{mcd}\{a, b\}$ denota el máximo común divisor de a y b (ver [17; 62]), esto significa que ω^v es un elemento primitivo de F. Por la estructura de campo, la multiplicación por ω induce una transformación lineal en K. Esta transformación induce un automorfismo de $GP(n, q)$ que actúa como un ciclo de longitud v en los v puntos de la geometría. En efecto

$$F = \{0, 1, \omega^v, \omega^{2v}, \ldots, \omega^{v(q-2)}\}$$

y los subespacios de dimensión 1 generados por los vectores $1, \omega, \ldots, \omega^{v-1}$ representan todos los puntos de $GP(n+1, q^{n+1})$. En efecto, si $\langle\alpha\rangle$ representa el espacio vectorial generado por α entonces:

$$\begin{array}{rcl}
\langle 1\rangle & = & \{0, 1, \omega^v, \omega^{2v}, \ldots \omega^{(q-1)v}\} \\
\langle\omega\rangle & = & \{0, \omega, \omega^{v+1}, \omega^{2v+1}, \ldots, \omega^{(q-1)v+1}\} \\
\langle\omega^2\rangle & = & \{0, \omega^2, \omega^v + 2, \omega^{2v+2}, \ldots, \omega^{(q-1)v+2}\} \\
\vdots & & \vdots \\
\langle\omega^{v-1}\rangle & = & \{0, \omega^{v-1}, \omega^{2v-1}, \omega^{3v-1}, \ldots, \omega^{(q-1)v+v-1}\}
\end{array}$$

Ahora la prueba del teorema fundamental de la geometría afín enunciado en la sección anterior es inmediata del teorema anterior y el teorema **fundamental de inmersión**, el cual se enuncia enseguida.

Teorema 4.12 [21;32] *Sean V un espacio vectorial sobre $\mathbf{F}_q$, H un hiperplano de V, (esto es un subespacio de codimensión 1 de V), $\bar{x} \in V - H$, $GP(V)_H$ el conjunto de subespacios de la geomtría $GP(V)$ no contenidos en H, y ϕ la función*

$$\phi : GA(\bar{x} + H) \longrightarrow GP(V)$$

definida por $N \mapsto \langle N \rangle$, para cualquier t-plano $N \in GA(\bar{x} + H)$. Entonces ϕ es una función inyectiva,

$$\phi(GA(\bar{x} + H)) = GP(V)_H \qquad y \qquad \phi^{-1}(U) = U \cap (\bar{x} + H),$$

para todo $U \in GP(V)_H$.

Demostración: Si $S = \bar{v}+M \in GA(\bar{x}+H)$, entonces $\bar{v} \in \bar{v}+M \subseteq \bar{x}+H$, por lo que $\bar{v} = \bar{x}+\bar{h}$, para alguna $\bar{h} \in H$, y $\bar{v}+H = (\bar{x}+\bar{h})+H = \bar{x}+(\bar{h}+H) = \bar{x} + H$.

Si $a\bar{v} + \bar{m} = \bar{v} + \bar{h}$, con $\bar{m} \in M$ y $\bar{h} \in H$, entonces $(a-1)\bar{v} = \bar{h} - \bar{m} \in H$. De ahí que $\bar{v} \in V - H$ pues $\bar{x} + H = \bar{v} + H$ y $\bar{x} \in V - H$, por lo tanto $a = 1$ y $\bar{h} = \bar{m}$. Así pues $\langle S \rangle \cap \langle \bar{x} + H \rangle = S$. Esto muestra que la función ϕ es inyectiva y también que su inversa, al restringir el codominio a su imagen, es

$$\langle S \rangle \mapsto \langle S \rangle \cap \langle \bar{x} + H \rangle.$$

Si U es un subespacio de V, no contenido en H. entonces $U + H = V$, ya que H es un hiperplano en V, y así

$$\dim(U \cap H) = \dim U + \dim H - \dim V = \dim U - 1.$$

Por lo tanto $U \cap H$ es un hiperplano en U. Sea $\bar{u} \in U - H$. Entonces $U = \bar{u} \oplus \langle U \cap H \rangle$. Ya que $H + \langle \bar{u} \rangle = V$, se sigue que $\bar{c}$ es de la forma $b\bar{u} + \bar{h}$. y así $b\bar{u} \in \bar{x} + H$. Pongamos $\bar{v} = b\bar{u}$ y $M = U \cap H$. Entonces $U = \langle \bar{v} \rangle + M$. donde $\bar{v} + M \in GA(\bar{x} + H)$. Esto muestra que ϕ es sobre. □

Es conveniente visualizar este teorema como la proyección de subespacios de un espacio vectorial dado sobre un hiperplano que no contiene al origen, como se ilustra en [21;34].

4.4.1 El plano de Fano

Aún cuando el plano de Fano $\mathcal{F}$ (fig. 2, pag. 53) es la más simple de las geometrías proyectivas finitas, su gran variedad de propiedades nos obliga a dedicarle especial atención. Ya se han mostrado algunas propiedades de esta geometría, aquí se prueban otras más. De la lista de propiedades de $\mathcal{F}$, enunciadas enseguida aquellas de los incisos 5,6 y 9 son resultados propios, las de los incisos 7 y 8 aunque no son originales no se encontró, en la bibliografía revisada, calculado explícitamente el grupo de automorfismos del plano de Fano o de otra geometría proyectiva finita, el resto de los incisos enuncian propiedades de $\mathcal{F}$ ya conocidas.

Acordemos denotar las líneas del plano de Fano de la siguiente manera:

$$L_1 = \{1,2,3\}, \quad L_2 = \{2,5,7\}, \quad L_3 = \{1,4,7\}, \quad L_4 = \{3,6,7\},$$
$$L_5 = \{1,5,6\}, \quad L_6 = \{2,4,6\}, \quad L_7 = \{3,4,5\}.$$

A continuación se resumen algunas de las principales propiedades de este diseño:

Teorema 4.13 *Sea $\mathcal{F} = (\mathbf{P}, \mathbf{B})$ el plano de Fano, entonces*

1) *$\mathcal{F}$ es un diseño $S(2,3,7)$.*

2) *$C_2(\mathcal{F}) = \mathcal{H}_3$, $C_3(\mathcal{F}) = (\mathbf{F_3}1)^{\perp}$ y $C_p(\mathcal{F}) = \mathrm{F}_p^7$ si $p \geq 5$.*

3) *Las palabras codificadas de peso tres en $\mathcal{H}_3$ sostienen a $\mathcal{F}$, mientras que las de peso cuatro sostienen un $S_2(2,4,7)$ el cual es el diseño de puntos y óvalos $\mathcal{O}$ de $\mathcal{F}$.*

4) *$C_2(\mathcal{O}) = \mathcal{H}_3^{\perp}$.*

5) *Sean $B_i \in \mathbf{B}$, $i = 1,2,3,4$. $\{v^{B_i}\}_{i=1}^4$ es una base de $\mathcal{H}_3$ si y sólo si $\mathbf{P} = \cup_{i=1}^4 B_i$.*

6) *Sean O_i, $i = 1,2,3$ tres óvalos de $\mathcal{F}$. $\{v^{O_i}\}_{i=1}^3$ es una base de $\mathcal{H}_3^{\perp}$ si y sólo si $\mathbf{P} = \cup_{i=1}^3 O_i$.*

7) *$Aut(\mathcal{F})$ es un grupo:*

- *de orden* 168
- *no conmutativo*
- *simple*
- *doblemente transitivo*

- *generado por*

$$\sigma_1 = (16)(34), \quad \sigma_2 = (16)(27),$$
$$\sigma_3 = (45)(67), \quad \sigma_4 = (12)(67),$$
$$\sigma_5 = (46)(57), \quad \sigma_6 = (13)(46).$$

8) *Es más, si* $\tilde{\sigma}_i$ *es la acción de* σ_i, $i = 1, 2, \ldots, 6$ *sobre las líneas de* $\mathcal{F}$ *entonces:*

$$\tilde{\sigma}_1 = (L_1L_6)(L_3L_4), \quad \tilde{\sigma}_2 = (L_1L_4)(L_3L_6),$$
$$\tilde{\sigma}_3 = (L_2L_6)(L_3L_5), \quad \tilde{\sigma}_4 = (L_2L_5)(L_3L_6),$$
$$\tilde{\sigma}_5 = (L_3L_5)(L_4L_7), \quad \tilde{\sigma}_6 = (L_3L_4)(L_5L_7).$$

9) *Existen precisamente* 30 *distintos códigos binarios de Hamming* $\mathcal{H}_3$ *(todos equivalentes).*

Demostración: Ya se han probado los incisos (1)-(4). La parte "si" del inciso (5) es obvia, y la prueba de la contrapositiva de la parte "sólo si" es directa. Igualmente se prueba el inciso (6).

(7)-(8). Ahora calculemos el grupo de automorfismos del plano de Fano. Este grupo es, por el teorema fundamental de la geometría proyectiva, el grupo de todas las matrices invertibles 3×3 con entradas en $\mathbf{F}_2$, el cual es calculado en el ejemplo 4.11. Ya que cada elemento del grupo es una transformación lineal de $\mathbf{F}_2^3$ sobre sí mismo, queda completamente determinado por su valor en una base de este espacio. Supongamos que $\bar{u}, \bar{v}$ y $\bar{w}$ son los vectores de una base de $\mathbf{F}_2^3$, y que $A \in SL(3,2)$; el punto $A\bar{u}^t$ puede ser elegido de 7 formas distintas (el vector cero no puede ser elegido), enseguida el punto $A\bar{v}^t$ sólo puede elegirse 6 maneras distintas, por último el punto $A\bar{w}^t$ debe elegirse de tal forma que sea linealmente independiente de estos dos puntos escogidos anteriormente, lo cual sólo puede hacerse de 4 formas distintas, por lo tanto el orden del grupo de automorfismos es $7 \times 6 \times 4 = 168$.

Ya que cada una de estas matrices induce una permutación en los puntos del plano de Fano podemos decir que su grupo de automorfismos es generado por las permutaciones que se muestran en el enunciado del teorema. Este es un grupo no conmutativo, (pues $\sigma_1\sigma_2\sigma_3$ y $\sigma_3\sigma_1\sigma_2$ son distintos), simple (teorema 4.10) y doblemente transitivo (proposición 4.7). Es más si $\tilde{\sigma}_i$ es la acción de σ_i en las líneas del plano de Fano, entonces cada una de estas $\tilde{\sigma}_i$ es una permutación de las líneas de $\mathcal{F}$, y la acción de estas permutaciones es como se describe en el teorema.

(9). Para cada permutación $\rho : \mathbf{P} \to \mathbf{P}$ sea $\mathbf{B}_\rho = \{\rho(B) : B \in \mathbf{B}\}$, entonces $\mathcal{F}_\rho = (\mathbf{P}, \mathbf{B}_\rho)$ es un plano de Fano, que sólo difiere de $\mathcal{F}$ en la enumeración de sus puntos. Además es claro que si

$$B \in \mathbf{B}, \text{ y } v^B \in C_2(\mathcal{F}) \text{ entonces } v^{\rho(B)} \in C_2(\mathbf{P}, \mathbf{B}_\rho).$$

Por otra parte existen $7! = 5040$ funciones biyectivas de $\mathbf{P}$ en sí mismo (cf. [20;72]). Si ρ es una de estas funciones entonces

$$\mathcal{F}_\rho = \mathcal{F}_{\sigma\rho}, \quad \forall \sigma \in Aut(\mathcal{F}).$$

Por lo tanto existen precisamente $5040/168 = 30$ funciones que inducen, cada una de ellas, una distinta enumeración de los puntos del plano de Fano. De ahí que este sea el número total de $[7, 4, 3]$ códigos binarios de Hamming distintos, pero equivalentes (un automorfismo del plano de Fano es un automorfismo de $\mathcal{H}_3$). □

4.5 Diseños asociados a geometrías finitas

Recuérdese que, en un 2-(v, k, λ) diseño de orden n, se verifican las siguientes ecuaciones

$$bk = vr, \quad r(k-1) = \lambda(v-1), \text{ y } n = r - \lambda.$$

Considérese el conjunto de w-subespacios, $1 \leq w \leq m-1$, de la geometría $GP(m, q)$. Puede verificarse que este conjunto forma un 2-diseño con parámetros

$$v = \tfrac{q^{m+1}-1}{q-1}, \qquad k = \tfrac{q^{w+1}-1}{q-1},$$

$$b = \begin{bmatrix} m+1 \\ w+1 \end{bmatrix}_q, \qquad r = \tfrac{(q^{w+1}-1)}{(q^{m+1}-1)} \begin{bmatrix} m+1 \\ w+1 \end{bmatrix}_q,$$

$$\lambda = \tfrac{(q^{w+1}-1)(q^w-1)}{(q^{m+1}-1)(q^m-1)} \begin{bmatrix} m+1 \\ w+1 \end{bmatrix}_q, \qquad n = \tfrac{q^w(q^{w+1}-1)(q^{m-w}-1)}{(q^{m+1}-1)(q^m-1)} \begin{bmatrix} m+1 \\ w+1 \end{bmatrix}_q.$$

Similarmente considerando los w-planos, $1 \leq w \leq m-1$, de la geometría afín $GA(m, q)$ obtenemos un 2-diseño de bloques con parámetros

$$v = q^m, \qquad k = q^w,$$

$$b = q^{m-w} \begin{bmatrix} m \\ w \end{bmatrix}_q, \qquad r = \begin{bmatrix} m \\ w \end{bmatrix}_q,$$

$$\lambda = \frac{q^w - 1}{q^m - 1} \begin{bmatrix} m \\ w \end{bmatrix}_q, \qquad n = \frac{q^w(q^{m-w} - 1)}{q^m - 1} \begin{bmatrix} m \\ w \end{bmatrix}_q.$$

Definición 4.15 *Se denotará al diseño de puntos y w-subespacios de la geometría $GP(m, q)$ como*

$$GP(m, w, q).$$

Análogamente $GA(m, w, q)$ expresa el diseño de puntos y w-planos de la geometría afín $GA(m, q)$.

5 Códigos asociados a diseños

Este es el capítulo principal del presente trabajo, pues se establece una correspondencia entre las geometrías finitas, tanto afín como proyectiva, y la teoría algebraica de los códigos. Se muestra que los códigos naturalmente asociados a estas geometrías corresponden a un tipo de códigos conocidos como códigos de Reed-Muller, y que los parámetros de éstos quedan determinados por la estructura combinatoria de aquellas.

5.1 Conceptos generales

Definición 5.1 *Sea* $\mathrm{S} = (\mathrm{P}, \mathrm{B})$ *una estructura de incidencia finita, con* $\mathrm{P} = \{p_1, p_2, \ldots, p_t\}$. *Para cualquier subconjunto* A *de* P *el* **vector de incidencia** *de* A *es*

$$v^A = (\chi_A(p_1), \chi_A(p_2), \ldots, \chi_A(p_t)).$$

Definición 5.2 *El* **código asociado a la estructura de incidencia** S *sobre el campo* F_q, $C_q(\mathrm{S})$, *es el* F_q*-espacio vectorial generado por los vectores de incidencia de los bloques de* S. *En otras palabras*

$$C_q(\mathrm{S}) = \langle v^B : B \in \mathrm{B} \rangle.$$

Ejemplo 5.1 Sea $\mathcal{F}$ el plano de Fano. Entonces $C_2(\mathcal{F})$ es el $[7, 4, 3]$ código binario de Hamming de la figura 1, pag. 39

Definición 5.3 *Para cualquier estructura de incidencia* S *y todo primo* p *se define el* p**-rango de** S *como la dimensión del código* $C_p(\mathrm{S})$ *y lo denotamos*

$$\mathrm{rang}_p(\mathrm{S}) = \dim(C_p(S)).$$

Debe notarse que el rango de una matriz de incidencia sobre el campo de orden p^r, para cualquier entero r, es precisamente el p-rango. Con estas nociones podemos enunciar ya el primer resultado de esta sección

Teorema 5.1 [5; 42] *Sea* D *un* 2-(v, k, λ) *diseño no trivial de orden* n. *Si* p *es un primo que no divide a* n *entonces*

$$\mathrm{rang}_p(\mathrm{D}) \geq v - 1$$

La igualdad se cumple si y sólo si p *divide a* k. *En caso de igualdad tenemos que* $C_p(\mathrm{D}) = (\mathbf{F}_p \mathbf{1})^{\perp}$, *donde* $\mathbf{1}$ *es el vector todo-uno, o sea el que tiene todas sus entradas igual a* 1, *y en el caso de desiguladad estricta* $C_p(\mathrm{D}) = \mathbf{F}_p^v$.

Demostración: Supóngase que $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ y sean p un primo que no divide a n y $C = C_p(\mathbf{D})$. Para $x \in \mathbf{P}$ sea $\bar{v} = \sum\{v^B : B \in \mathbf{B},\ x \in B\}$, entonces $\bar{v}$ tiene al número r en la entrada correspondiente a x y λ en las restantes. Ya que para un 2-diseño $n = r - \lambda$ se tiene:

$$\sum_{B \in \mathbf{B}} v^B - \bar{v} = r\mathbf{1} - \bar{v} = n(\mathbf{1} - v^x) \in C.$$

Por lo tanto $\mathbf{1} - v^x \in C$ para todo punto x, así que $v^x - v^y \in C$ para cada par de puntos x, y; esto da la contención $C \supseteq (\mathbf{F}_p\mathbf{1})^\perp$, por lo que $\text{rang}_p(\mathbf{D}) \geq v-1$. Por otra parte p divide a k si y sólo si $v^B \cdot \mathbf{1} = k = 0$, para cada bloque B, lo cual ocurre si y sólo si $v^B \in (\mathbf{F}_p\mathbf{1})^\perp$, esto es si y sólo si $C = (\mathbf{F}_p\mathbf{1})^\perp$. □

Ejemplo 5.2 Por el teorema anterior si $\mathcal{F}$ es el plano de Fano entonces $C_3(\mathcal{F}) = (\mathbf{F}_3\mathbf{1})^\perp$; $C_p(\mathcal{F}) = \mathbf{F}_p^7$ para cada primo $p \geq 5$ y como vimos antes $C_2(\mathcal{F})$ es el menor código de Hamming, $\mathcal{H}_3$.

Elijamos un primo p que no divida a nk, entonces $b \geq \text{rang}_p(\mathbf{D}) \geq v$. Esto es, $b \geq v$, o sea un 2-diseño, y por lo tanto en un t-diseño, $t \geq 2$, el número de puntos no puede exceder al número de bloques, esto se conoce como la **desigualdad de Fisher.**

Teorema 5.2 [15] *Sea S un sistema triple de Steiner con v puntos, i.e. un 2-$(v, 3, 1)$ diseño.*

i) $\text{rang}_2(S) \geq v - log_2(v+1)$. *La igualdad se cumple si y sólo si* $v = 2^d - 1$ *y* $S = GP(d-1, 1, 2)$.

ii) $\text{rang}_3(S) \geq v - log_3(v) - 1$. *La igualdad se cumple si y sólo si* $v = 3^d$ *y* $S = GA(d, 1, 3)$.

iii) Para todo primo $p > 3$ *se tiene* $\text{rang}_p(S) = v$.

5.2 Códigos (binarios) de Reed-Muller

La clase de los códigos binarios conocidos como de Reed-Muller se deben a I.S. Reed (véase [41]), y a D.E. Muller (consúltese [38]), mientras que los códigos de Reed-Muller no binarios fueron descubiertos independientemente por varias personas, entre ellos están P. Delsarte (ver [14]), T. Kasami, S. Lin y W.W. Peterson (cf. [29]), J.L. Massey, D.J. Costello y J. Justensen (consultar [33]), etc.

A lo largo de esta sección F denotará el campo binario y V el espacio vectorial F^m de dimensión m sobre F.

Lema 5.1 [5; 142] *Sean* $K = \{1, 2, \ldots, m\}$, $\bar{w} = (w_1, \ldots, w_m) \in V$ *y* $Sop(\bar{w})$ *el soporte de este vector. Entonces la función característica de* $\bar{w}$ *está dada por*

$$\chi_{\bar{w}}(x_1, \ldots, x_m) = \prod_{k=1}^{m}(x_k + 1 + w_k) = \sum_{J}\{\prod_{j \in J} x_j : Sop(\bar{w}) \subseteq J \subseteq K\}.$$

Demostración: Es sencillo comprobar que el primer polinomio define la función característica del vector $\bar{w}$, desarrollando el producto se obtiene la suma de la derecha. □

Ejemplo 5.3 1) $\chi_{(1,1,\ldots,1)}(x_1, \ldots, x_m) = x_1 x_2 \cdots x_m$

2) $\chi_{(0,0,\ldots,0)}(x_1, \ldots, x_m) = \sum_{J \subseteq K} \prod_{j \in J} x_j = \sum_{f \in M} f$, donde M es el conjunto de monomios en $x_1, x_2, \ldots, x_m$ donde toda indeterminada aparece a lo más a la primer potencia.

Por el lema anterior, toda función de F^m en F es polinomial. Ya que los dos elementos de F satisfacen la ecuación $x^2 = x$, estas funciones pueden ser reducidas módulo $x_i^2 - x_i$. Entonces el conjunto de 2^m monomios

$$M = \{x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} : i_k = 0 \text{ ó } 1, 1 \leq k \leq m\}$$

forma un base para el espacio vectorial de las funciones de F^m en F reducidas módulo $x_i^2 - x_i$. Para cada entero no negativo $r \leq m$, se denotará al espacio vectorial sobre F generado por los monomios en M de grado a lo más r como M_r es decir

$$M_r = \langle \{x_1^{i_1} \cdots x_m^{i_m} : 0 \leq i_k \leq 1, \sum i_k \leq r, \ 1 \leq k \leq m\} \rangle.$$

Ahora ya se tiene la nomenclatura necesaria para enunciar la definición de los códigos binarios de Reed-Muller:

Definición 5.4 *Para cualesquiera dos enteros* m *y* r, $0 \leq r \leq m$, *el* **código de Reed-Muller de orden** r, *sobre* F, *denotado como* $RM(r, m)$, *es la imágen de la función evaluación* $ev : M_r \longrightarrow F^{2^m}$, *definida como*

$$ev(f(x_1, \ldots x_m)) = (f(p_1), \ldots, f(p_{2^m})),$$

donde $p_1, \ldots, p_{2^m}$ *son los distintos puntos de* $GA(m, 2)$.

Ejemplo 5.4 1) $RM(0,m) = F\mathbf{1}$, $RM(m,m) = F^{2^m}$. Más adelante se muestra que

$$RM(m-1,m) = (F\mathbf{1})^{\perp}.$$

2) Para $m = 3$ y $r = 2$, $RM(2,3)$ es la imagen bajo la función evaluación, del subespacio M_2 el cual tiene como base

$$1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3.$$

3) La preimagen del código de Reed-Muller de primer orden $RM(1,m)$ consiste de todas las combinaciones lineales de los monomios x_i y 1, por lo tanto toda palabra codificada, exepto **0** y **1**, es imagen de un funcional lineal no cero en V, o bien, de 1 más un funcional lineal no cero. Ya que todo funcional lineal tiene 2^{m-1} ceros todo vector de $RM(1,m)$, tiene peso 2^{m-1} o bien es el vector **0** ó **1**. Calculemos una matriz generadora para $RM(1,m)$, en la base ordenada $\{x_1, x_2, \ldots, x_m, 1\}$. En las primeras $2^m - 1$ columnas y m renglones coloquemos las representaciones binarias de los números entre 1 y $2^m - 1$, enseguida coloquemos una columna de m ceros y por último un renglón con todas sus entradas igual a 1. Claramente esta es una matriz generadora para el ortogonal del código extendido de Hamming, por lo tanto

$$RM(1,m) = (\hat{\mathcal{H}}_m)^{\perp}.$$

En particular $RM(1,3)$ es la imagen del subespacio $\langle 1, x_1, x_2, x_3\rangle$. Este código se muestra en la siguiente figura

00000000	01101001	01010101	11000011
11111111	11110000	00111100	10100101
00001111	11001100	01011010	10011001
00110011	10101010	01100110	10010110

Figura 4. $RM(1,3)$

De la definición de M_r es claro que

$$\dim(RM(r,m)) = \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}.$$

En particular

$$\dim(RM(1,m)) = 1 + m.$$

Lema 5.2 [9;69] *Sea f un polinomio en m variables y coeficientes en F, de grado menor que m entonces*

$$\sum_{\bar{w}\in V} f(\bar{w}) = 0.$$

Demostración: La función caracterísitica de $\bar{w} = (w_1, \ldots, w_m) \in V$ es

$$\chi_{\bar{w}}(x_1, \ldots, x_m) = \prod_{i=0}^{m} [1 + x_i + w_i].$$

Entonces el coeficiente del monomio de grado m de esta función es 1, por lo que

$$\begin{aligned} f(\bar{x}) &= \textstyle\sum_{\bar{w}\in V} f(\bar{w})\chi_{\bar{w}}(\bar{x}) \\ &= \textstyle\sum_{\bar{w}\in V} f(\bar{w})[x_1 \cdots x_m + g(x_1, \ldots, x_m)], \end{aligned}$$

donde el grado de $g(\bar{x})$ es menor que m. Comparando los coeficientes del monomio de grado m en esta igualdad se obtiene el resultado deseado. □

Mencionamos anteriormente que $RM(0,m)^{\perp} = RM(m-1,m)$. Este sólo es un caso particular del siguiente

Teorema 5.3 [5;144] *Para cualesquiera m y r con $0 \leq r < m$*

$$RM(r,m)^{\perp} = RM(m-r-1,m).$$

Demostración: Sean $\bar{f} \in RM(m-r-1,m)$ y $\bar{g} \in RM(r,m)$ dos palabras codificadas que son imagen bajo la función ev, de los polinomios $f(\bar{x})$ y $g(\bar{x})$ respectivamente. Entonces f es un polinomio de grado a lo más $m-r-1$ y g es un polinomio de grado a lo más r, por lo tanto su producto tiene grado a lo más $m-1$, y su imagen está en $RM(m-1,m)$. Por el lema anterior $\bar{f}$ y $\bar{g}$ son ortogonales de ahí que

$$RM(m-r-1,m) \subseteq RM(r,m)^{\perp}.$$

Ya que la dimensión del código $RM(m-r-1,m)$ es igual a

$$\begin{aligned}
&\binom{m}{0}+\binom{m}{1}+\binom{m}{2}+\cdots+\binom{m}{m-r-1}\\
&=2^m-\left[\binom{m}{m-r}+\cdots+\binom{m}{m-1}+\binom{m}{m}\right]\\
&=2^m-\left[\binom{m}{r}+\cdots+\binom{m}{1}+\binom{m}{0}\right]\\
&=2^m-\dim(RM(r,m))\\
&=\dim(RM(r,m)^{\perp})
\end{aligned}$$

se obtiene el resultado deseado. □

Ejemplo 5.5 Del teorema anterior se sigue inmediatamente que:

$$RM(1,m)^{\perp}=\hat{\mathcal{H}}_m=RM(m-2,m).$$

En el estudio de los códigos asociados a geometrías finitas será de gran utilidad el siguiente concepto:

Definición 5.5 *Para* $0\leq r<m$ *el código* **agujerado** *de Reed-Muller de orden* r, $RM(r,m)^*$, *es el código obtenido de* $RM(r,m)$ *suprimiendo la posición coordenada correspondiente al vector* $\mathbf{0}$.

Ejemplo 5.6 $RM(1,3)^*$ es un $[7,4,3]$-código, el código de Hamming $\mathcal{H}_3$.

Proposición 5.1 [5;145] *Para* $0\leq r<m$, $RM(r,m)^*$ *es un código de longitud* 2^m-1, *y su dimensión es la misma que la de* $RM(r,m)$

Demostración: La dimensión debe ser la de $RM(r,m)$ ya que todos los vectores en el código son de peso par y la proyección natural de $RM(r,m)$ en $RM(r,m)^*$ no puede tener un núcleo. □

Del lema 5.2 se sigue que si $r<m$ todo polinomio $f\in M_r$ satisface la igualdad $f(\mathbf{0})=\sum f(\bar{w})$, donde la suma se toma sobre todos los elementos $\bar{w}$ no nulos de V, $RM(r,m)$ es el código extendido del código $RM(r,m)^*$.

5.3 Códigos de Reed-Muller asociados a geometrías

El polinomio x_i toma valor de 1 precisamente en aquellos vectores de $V = F^m$ que tienen un 1 en la posición i; por lo tanto $1 + x_i$ es la función característica para el hiperplano de ecuación $x_i = 0$. Similarmente el polinomio x_i es la función característica del complemento de este hiperplano, que es el $(m-1)$-plano que satisface la ecuación $x_i = 0$. Siguiendo con este razonamiento tenemos que el polinomio $x_i(1 + x_j)$, con i distinto de j es la función característica de la intersección de los $(m-1)$-planos correspondientes a las funciones características x_i y $1 + x_j$, un $(m-2)$-plano. En general todo monomio es la función característica de un l-plano y $RM(r, m)$ es generado por los vectores de incidencia de los $(m-s)$-planos $0 \leq s \leq r$ de la geometría $GA(m, 2)$. Nuestro propósito es demostrar que $RM(r, m)$ es el código generado por los vectores de incidencia de los $(m-r)$-planos de $GA(m, 2)$. Ya que las ecuaciones lineales definen un $(m-1)$-plano y $RM(1, m)$ es imagen de $2^m(2^m - 1)$ polinomios lineales, que es el número de $(m-1)$-planos en $GA(m, 2)$, tenemos que

$$C_2[GA(m, m-1, 2)] = RM(1, m).$$

Para el caso general primero se prueba que los vectores de incidencia de los $(m-r)$-planos están en el código de Reed-Muller.

Proposición 5.2 [5; 146] *Los vectores de incidencia de los $(m-r)$-planos de la geometría afín $GA(m, 2)$ están todos en $RM(r, m)$.*

Demostración: Ya que los puntos de todo $(m-r)$-plano en $GA(m, 2)$, $\bar{x} = (x_1, \ldots, x_m)$ son aquellos que satisfacen las r ecuaciones lineales

$$\sum_{j=1}^{m} a_{ij} x_j = b_i, \quad i = 1, 2, \ldots, r, \quad a_i, b_i \in F,$$

el polinomio

$$\prod_{i=1}^{r} (b_i + 1 + \sum_{j=1}^{m} a_{ij} x_j),$$

tiene grado a lo más r y por lo tanto su imagen está en $RM(r, m)$. Además este polinomio es el vector de incidencia del $(m-r)$-plano definido por las ecuaciones anteriores. □

La prueba muestra más, a saber, que los vectores de incidencia de los $(m-s)$-planos están en $RM(r,m)$ para cualquier $s \leq r$.

Es inmediato probar que la función característica de cualquier $(t+1)$-plano es la suma de dos t-planos paralelos contenidos en él. De ahí que, como puede verificarse por inducción sobre s, el código binario asociado al diseño $GA(m, m-r, 2)$ contiene las funciones características de todos los $(m-r)$-planos para $0 \leq s \leq r$, por lo tanto el código de este diseño es $RM(r,m)$. Invirtiendo los papeles de r y $m-r$ se tiene

Teorema 5.4 [5; 147] *Si r y m son enteros tales que $0 \leq r \leq m$, entonces*

$$C_2[GA(m,r,2)] = RM(m-r,m).$$

Las funciones características de los r-planos son vectores de peso 2^r. Se probará que estas funciones son las únicas con esta propiedad y que la distancia mínima de $RM(m-r,m)$ es precisamente esta cantidad.

Un subespacio de F^m de dimensón r será denotado como $\prod_r$, y el subespacio proyectivo correspondiente $\prod_r - \{\mathbf{0}\}$ como $\prod_r^*$.

Se mostrará que $C_2[GP(m-1,r,2)] = RM(m-r-1,m)^*$:
Sea $C = C_2[GP(m-1,r,2)]$. Un r-subespacio proyectivo $\prod_r^*$ satisface $m-1-r$ ecuaciones lineales, su función característica es un polinomio de grado $m-r-1$ en m variables, y ya que $\mathbf{0}$ no está en $GP(m-1,2)$ la función característica de $\prod_r^*$ está en $RM(m-r-1,m)^*$.

Extiéndase a C por un chequeo de paridad total al código $\hat{C}$. Un bloque de $GP(m-1,r,2)$ es un $\prod_{r+1}^*$, entonces su peso es $2^{r+1}-1$ y ya que el peso de $\prod_{r+1}$ es 2^r, los vectores de incidencia de los $(r+1)$-subespacios de F^m generan a $\hat{C}$. Ya que $\prod_{r+1}$ satisface $m-1-r$ ecuaciones lineales su función característica es un polinomio de grado $m-r-1$, por lo tanto $\hat{C} \subseteq RM(m-r-1,m)$.

El número de repetición $r = \lambda_1$ para un diseño de puntos e hiperplanos de una geometría proyectiva es congruente con 1 módulo 2 (véase pag. 85), y como en todo diseño $(\mathbf{P},\mathbf{B})$,

$$\sum_{B \in \mathbf{B}} v^B = r\mathbf{1}$$

el vector todo-uno siempre está en el código binario de un diseño de puntos e hiperplanos de una geometría proyectiva. Ya que los $(r+1)$-subespacios

contenidos en un $(r+2)$-espacio forman un diseño $GP(r+1,r,2)$, el vector de incidencia de todo $(r+2)$-subespacio de F^m es la suma de todos los vectores de incidencia de los $(r+1)$-subespacios que contiene.

Notemos que en F, si $\bar{w}$ es un elemente fijo de $\prod_{r+2} - \prod_{r+1}$, entonces se tiene que $\prod_{r+2} - \prod_{r+1} = \{\bar{h} + \bar{w} : \bar{h} \in \prod_{r+1}, \bar{w} \in \prod_{r+2}\} = \prod_{r+1} + \bar{w}$, entonces en $C_2[GA(m, r+1, 2)]$ el vector de incidencia de un $(r+1)$-plano es la suma de los vectores de incidencia de un $(r+2)$-subespacio y un $(r+1)$-subespacio. Por lo tanto todos los $(r+1)$-planos de F^m están en $\hat{C}$, esto es

$$C_2[GA(m, r+1, 2)] = RM(m-r-1, m) \subseteq \hat{C},$$

de ahí que $\hat{C} = RM(m-r-1, m)$ y $C = RM(m-r-1, m)^*$. Se ha probado la siguiente

Proposición 5.3 [6; 147] $C_2[GP(m-1, r, 2)] = RM(m-r-1, m)^*$. *En particular* $C_2[GP(d, 1, 2)] = \mathcal{H}_{d+1}$.

Ejemplo 5.7 El diseño $GP(d, 1, 2)$ se extiende naturalmente a $GA(d+1, 2, 2)$ y como se ha visto $C_2[GP(d, 1, 2)] = \mathcal{H}_{d+1}$ mientras que $C_2[GA(d+1, 2, 2)] = \hat{\mathcal{H}}_{d+1}$, un código extendido de Hamming.

Teorema 5.5 [6; 18] *Cualquier inmersión de* $GP(m-1, 2)$ *en* $GP(m, 2)$ *induce las siguientes sucesiones exactas cortas:*

$$0 \to RM(m-r-1, m)^* \to RM(m-r, m+1)^* \to RM(m-r, m) \to 0,$$

$$0 \to RM(m-r-1, m) \to RM(m-r, m+1)^* \to RM(m-r, m)^* \to 0.$$

Demostración: Sea $W = F^{m+1}$. La imagen de cualquier inmersión de $GP(m-1, 2)$ en $GP(m, 2)$ es un hiperplano de $GP(m, 2)$ y por lo tanto podemos asociarle un hiperplano H de W. Además $\bar{H} = W - H = GA(m, 2)$, entendiendo esta igualdad como isomorfismo según se definió al final de la sección sobre geometría afín. Si $\bar{w}$ es un vector fijo en $\bar{H}$ entonces $\bar{H} = \{\bar{h} + \bar{w} : \bar{w} \in W, \bar{h} \in H\} = H + \bar{w}$. Si $\prod_{r+1}$ es un $(r+1)$-espacio que corta a H en un r-espacio $\prod_r$. y $\bar{w}$ es un elemento de $\prod^*_{r+1}$ que no está en $\prod^*_r$ entonces $\prod^*_{r+1} \cap \bar{H} = \prod^*_{r+1} - \prod_r = \{\bar{w} + h : h \in \prod^*_r\} = \bar{w} + \prod_r$.

Sea $\mathbf{D}$ el diseño $GP(m, r, 2)$; de $GP(H)$ constrúyase el diseño $\mathbf{D}_1 = GP(m-1, r, 2)$ y de $GA(\bar{H})$ el diseño $\mathbf{D}_2 = GA(m, r, 2)$. Entonces

$$C_2(\mathbf{D}) = RM(m-r, m+1),\ C_2(\mathbf{D}_1) = RM(m-r-1, m)^*, \text{ y}$$
$$C_2(\mathbf{D}_2) = RM(m-r, m).$$

Un bloque de $\mathbf{D}$ es un subespacio $\prod_{r+1}^{*}$, y $\prod_{r+1}^{*} \subset H$ o $\prod_{r+1}^{*} \cap H = \prod_{r}^{*}$. Entonces $\prod_{r+1}^{*} \cap \bar{H} = \emptyset$ o $\bar{w} + \prod_{r}$. Todo r-plano de $GA(\bar{H})$ surge de esta manera; por lo tanto la proyección $\pi_{\bar{H}}$ de las posiciones coordenadas de $C_2(\mathbf{D})$ sobre las posiciones coordenadas de $\bar{H}$ tiene por imágen a $C_2(\mathbf{D}_2)$ y $C_2(\mathbf{D})$ está en su núcleo. Se tiene entonces que

$$\dim(C_2(\mathbf{D}_1)) \leq \dim(C_2(\mathbf{D})) - \dim(C_2(\mathbf{D}_2)),$$

esto es

$$\sum_{i=1}^{m-r-1} \begin{pmatrix} m \\ i \end{pmatrix} \leq \sum_{i=1}^{m-r} \begin{pmatrix} m+1 \\ i \end{pmatrix} - \sum_{i=1}^{m-r} \begin{pmatrix} m \\ i \end{pmatrix},$$

entonces utilizando repetidamente la igualdad $\begin{pmatrix} n+1 \\ i+1 \end{pmatrix} = \begin{pmatrix} n \\ i+1 \end{pmatrix} + \begin{pmatrix} n \\ i \end{pmatrix}$ puede concluirse que se cumple la igualdad y por lo tanto $C_2(\mathbf{D}_1)$ es el núcleo de la proyección, con esto se obtiene la primera sucesión.

Para probar la segunda sucesión se toma ahora la proyección sobre $H - \{0\}$. Constrúyanse los diseños $\mathbf{E}_2 = GP(m-1, r-1, 2)$ y $\mathbf{E}_1 = GA(m, r+1, 2)$ a partir de $GP(H)$ y $GA(\bar{H})$ respectivamente y sea $\mathbf{D}$ el diseño considerado anteriormente.

Ya que todo r-subespacio proyectivo de $GP(W)$ intersecta a H en un $(r-1)$-subespacio proyectivo o está contenido en él y todo $(r-1)$-subespacio proyectivo puede ser obtenido de esta forma la imagen de la proyección es $C_2(\mathbf{E}_2)$.

Si dos r-subespacios de $GP(W)$ intersectan a $GP(H)$ en el mismo $(r-1)$-subespacio proyectivo entonces sus intersecciones en $\bar{H}$ son ajenas por lo que forman dos clases del mismo r-subespacio de $GA(\bar{H})$. La unión de estas clases forma un $(r+1)$-plano de $GA(m, 2)$ por lo que $C_2(\mathbf{E}_1)$ está en el núcleo de la proyección. Por un argumento respecto a las dimensiones puede concluirse que este código es precisamente el núcleo. □

Corolario 5.1 [6: 19] *La distancia mínima del código $RM(m-r, m)$ es 2^r y los vectores de peso mínimo son los vectores de incidencia de los r-planos de la geometría $GA(m, 2)$. El peso mínimo de $RM(m-r, m)^*$ es $2^r - 1$ y los vectores de peso mínimo son los vectores de incidencia de los $(r-1)$-subespacios proyectivos de la geometría proyectiva $GP(m-1, 2)$. En particular los vectores de peso mínimo de $\mathcal{H}_{d+1}$ son los vectores de incidencia de las rectas de $GP(d, 2)$.*

Demostración: Ya se ha probado que los vectores de incidencia de los r-planos de $GA(m,2)$ están en $RM(m-r,m)$, como su peso es 2^r, si los vectores de incidencia de los r-planos son los vectores de peso mínimo en $RM(m-r,m)$ entonces el peso mínimo de $RM(m-r,m)^*$ es 2^r-1. Inversamente si el peso mínimo de $RM(m-r,m)^*$ es 2^r-1, el de $RM(m-r,m)$ es 2^r pues este código es obtenido de aquel añadiendo un chequeo de paridad total.

Se probará el corolario por inducción en m utilizando la misma notación que en el teorema anterior. La hipótesis de inducción es que el corolario es válido para m y todo $r<m$.

Si $r=0$ el resultado es trivial. Supóngase pues que $r>0$ y que la dimensión es $m+1$. Si $r=m$ tenemos el código $RM(1,m+1)$ y el corolario es válido en este caso; entonces puede suponerse que $0<r<m$.

Fijemos una inmersión de $GP(m-1,2)$ en $GP(m,2)$ como en el teorema y sea $\bar{v}$ un vector de peso mínimo $C_2(\mathbf{D})$. Si $\bar{v}$ tiene coordenadas cero en las entradas correspondientes a $\bar{H}$, entonces puede pensarse como un vector de $C_2(\mathbf{D}_1)$ y, por hipótesis de inducción, tendrá peso $2^{r+1}-1$, es el vector de incidencia de un r-subespacio de $GP(m-1,2)$ y por lo tanto de $GP(m,2)$. Si $\bar{v}$ tiene entradas cero en los coordenadas correspondientes a $H^*=H-\{\mathbf{0}\}$ entonces puede pensarse como vector de $RM(m-r-1,m)$ y, por hipótesis de indución, su peso es no mayor que 2^{r-1}, lo cual es imposible pues el peso mínimo está acotado por $2^{r+1}-1$. Ahora sólo resta considerar aquellos vectores $\bar{v}$ de peso mínimo tales que ninguna de sus proyecciones sea el vector cero, por lo tanto el peso mínimo de $\bar{v}$ es, por inducción, al menos $2^r-1-2^r=2^{r+1}-1$, además cuando tal vector de peso $2^{r+1}-1$ es proyectado sobre las coordenadas correspondientes a H^*, es el vector de incidencia de un $(r-1)$-subespacio del espacio proyectivo inmerso. Se desea mostrar que $\bar{v}$ es el vector de incidencia de un r-subespacio proyectivo de $GP(m,2)$; para esto se construye un r-subespacio de esta geometría cuyo vector de incidencia $\bar{w}$ coincide con $\bar{v}$ en las coordenadas correspondientes a H^* y tiene por lo menos una entrada en común con $\bar{v}$ en las coordenadas de $\bar{H}$. Entonces $ps(\bar{v}*\bar{w})\geq(2^r-1)+1$, donde $\bar{v}*\bar{w}$ denota la intersección de $\bar{v}$ y $\bar{w}$ definida en el ejemplo 2.4. Así que $ps(\bar{v}*\bar{w})\leq 2^{r-1}-2<2^{r+1}-1$, y $\bar{v}=\bar{w}$. Con esto tenemos el resultado proyectivo, del cual se sigue el resultado afín. □

Ejemplo 5.8 [6;21] Una base para el código $RM(m-2,m)=\mathcal{H}_m$, consistente de vectores de incidencia de líneas de $GP(m,2)$, puede encontrarse como se describe a continuación: tómese cualquier línea e inclúyase su vector

de incidencia como un vector de la base. A continuación elíjase cualquier punto no incidente con esta línea, e inclúyanse los tres vectores de incidencia de las tres líneas que contienen este nuevo punto y un punto de la primera línea. Se continua de esta manera hasta que no hay más puntos que elegir. Es decir, si existe un punto que aún no es incidente con alguna de las líneas elegidas hasta el momento, se agregan a la base los vectores de incidencia de las líneas que contienen a este punto y algún otro de los ya elegidos. Esta manera de construir vectores claramente garantiza su independencia lineal, y es sencillo calcular que el número de vectores que se obtienen es precisamente la dimensión de $\mathcal{H}_m$, de ahí que formen una base.

Ejemplo 5.9 El diseño $GA(3,1,2)$ puede ser visto como un octágono regular junto con todas sus diagonales, (esto es, una gráfica completa de ocho vértices), en la cual los vértices del octágono son los puntos y cada línea es un bloque (debe notarse que sin importar cómo etiquetemos cada vértice del octágono el diseño es exactamente el mismo.)

Como sabemos, este código es precisamente $RM(2,3) = (\mathbf{F}_2\mathbf{1})^{\perp}$, un código de longitud 8 y dimensión 7 el cual es generado por

$$\begin{array}{ll} 11111111 & 00010001 \\ 00001111 & 00000101 \\ 00110011 & 00000011 \\ 01010101 & \end{array}$$

Y como vimos antes este código es generado por los vectores de peso que tienen todas sus entradas, excepto dos, iguales a cero, una de las cuales es 1 y la otra -1, los cuales en este caso, ya que $-1 = 1$ en F, son los vectores de incidencia de las líneas de $GA(3,2)$.

Por otra parte el código $RM(1,3)$ mostrado en la figura 4, pag. 89, es el código binario asociado al diseño $GA(3,2.2)$, el cual es un sistema cuádruple de Steiner $S(3,4,8)$, y todos sus vectores excepto $\mathbf{0}$ y $\mathbf{1}$, son vectores de incidencia de 2-planos de $GA(3,2)$. Por ejemplo al ordenar los puntos de la geometría de la siguiente manera

$$\begin{array}{llll} 100 \mapsto p_1, & 000 \mapsto p_2, & 110 \mapsto p_3, & 010 \mapsto p_4, \\ 101 \mapsto p_5, & 001 \mapsto p_6, & 111 \mapsto p_7, & 011 \mapsto p_8. \end{array}$$

las palabras codificadas 01010101, 00110011, 11001100 y 11000011 son los vectores de incidencia de los 2-planos de $GA(3,2)$ que satisfacen las ecuaciones $x_1 = 0$, $x_2 = 1$, $x_2 = 0$ y $x_2 + x_3 = 0$ respectivamente.

Agujerar este código equivale a suprimir la primera posición coordenada y el código que resulta es el código binario de Hamming $\mathcal{H}_3$. Si después de agujerar, como se indica, el código de la figura 4, pag. 89, se aplica la permutación (17)(35)(46) a las columnas el código que se obtiene es precisamente el mostrado en la figura 1, pag. 39.

5.4 Sistemas triples y cuádruples de Steiner

Esta sección está basada en [30], por lo que se suprimen las referencias al principio de cada proposición. Recordemos que un sistema triple de Steiner es un diseño $S(2,3,v)$, mientras que un sistema cuádruple de Steiner es un 3-$(v,4,1)$ diseño.

Si en un código C toda palabra codificada tiene coordenada 0 en una posición particular, entonces el código obtenido de C suprimiendo esa posición coordenada se llama **código acortado** de C.

Puede probarse inmediatamente que un sistema triple de Steiner con v puntos satisface $v \equiv 1$ ó 3 $(mod\ 6)$; y v es siempre un número impar. Denotaremos el tercer punto en el bloque que contiene a los puntos distintos x y y por $x * y$ y al bloque por xy. Es sencillo probar que la operación $*$ induce las propiedades de grupo abeliano en un sistema triple de Steiner, excepto la asociatividad. Cuando le agregamos un elemento al conjunto de puntos, lo definimos como el elemento neutro y suponemos que todo elemento es de orden 2; entonces $*$ es una operación de grupo abeliano, es más la asociatividad se cumple sólo cuando el diseño proviene de una geometría proyectiva sobre el campo binario.

Sea $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ un sistema triple de Steiner. Un subconjunto $\mathbf{P}'$ de $\mathbf{P}$ es llamado **subsistema** de $\mathbf{D}$ si tiene al menos tres elementos y si los puntos distintos x y y están en $\mathbf{P}'$ entonces también lo está el punto $x * y$. $\mathbf{P}'$ forma un diseño $S(2,3,v')$ donde v' es la cardinalidad de $\mathbf{P}'$ y los bloques de este diseño son aquellos de $\mathbf{D}$ contenidos en el subsistema. Un subsistema propio es llamado un **hiperplano proyectivo** de $\mathbf{D}$ si todo bloque de $\mathbf{D}$ intersecta al hiperplano.

Supóngase que S es un subsistema de cardinalidad $\frac{v-1}{2}$. Para cada punto fijo fuera de S existen $\frac{v-1}{2}$ bloques a través del punto que no son ajenos de S, ya que cada uno de estos sólo puede tener un punto en S. Por ser S un subsistema el número total de puntos en bloques que contienen un punto fijo exterior a S es $3 + 2 + 2 + \cdots + 2 = 1 + 2 + 2 + \cdots + 2$, donde en el

miembro izquierdo tenemos $\frac{v-1}{2}$ sumandos iguales a 2, por lo que esta suma es presisamente v; así que no existe un bloque que no corta a S. Resumiendo, si un subsistema tiene $(v-1)/2$ puntos entonces es un hiperplano proyectivo. Es sencillo verificar que un hiperplano de la geometría $GP(n,2)$, es un hiperplano proyectivo. Similarmente, un subsistema propio no vacío S es un **hiperlplano.afín** si para todo punto x fuera de S la unión de todos los bloques que contienen este punto y que son ajenos de S forma un subsistema S' y todo bloque que intersecta a S en un punto también corta a S'. Entonces $S'' = \mathbf{P} - (S \cup S')$ es también un subsistema, y los tres subsistemas forman un conjunto de subsistemas mutuamente ajenos.

Las geometrías finitas nos proveen de los diseños que nos interesan, en particular $GP(d,1,2) = S(2,3,2^{d+1}-1)$ y $GA(d,1,2) = S(2,3,3^d)$, como puede verificarse inmediatamente.

5.4.1 Palabras codificadas de peso mínimo

Recuérdese que para cada primo p el p-rango del diseño $\mathbf{D}$, denotado como $\text{rang}_p(\mathbf{D})$, es la dimensión del código p-ario asociado a $\mathbf{D}$.

Si el código de un sistema triple de Steiner con v puntos tiene dimensión v entonces sus vectores de peso mínimo son todos los vectores de peso 1; por lo tanto, de acuardo al teorema 5.2, sólo se consideran los códigos binarios y ternarios.

Proposición 5.4 *Sea* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *un* 2-$(v,3,1)$ *diseño y sea* $C = C_p(\mathbf{D})$ *con* $p = 2$ *ó* 3, *su código asociado. Supóngase que el peso mínimo de* C *es tres. Si* $p = 2$ *entonces los vectores de peso mínimo son los vectores de incidencia de los bloques de* $\mathbf{D}$, $v = 2^d - 1$ *para algún entero* $d \geq 2$, $\mathbf{D} = GP(d-1,1,2)$ *y* $C = \mathcal{H}_d$. *Si* $p = 3$ *entonces* $v = 3^d$ *para algún* $d \geq 1$ *y* $\mathbf{D} = GA(d,1,2)$.

Demostración: Si $p = 2$ la cota por empaquetamiento con esferas. proposición 2.5, implica que $k \leq v - log_2(1+v)$. Por el teorema 5.2 se tiene $k \geq v - log_2(v+1)$ con la igualdad si y sólo si $\mathbf{D}$ es el diseño de puntos y líneas de una geometría proyectiva.

Si $p = 3$ la cota por empaquetamiento nos da $k \leq v - log_3(1+2v) \leq v$. Supóngase que $v \in [3^d, 3^{d+1}-1)$. Por el teorema 5.2 puede mostrarse que $k = v - d - 1$ y que $\mathbf{D} = GP(d,1,3)$. Por ejemplo supongamos que $\frac{3^{d+1}}{2} \leq v < 3^d$, de la primera desigualdad puede deducirse que $d+1 \leq log_3(2v+1)$.

esto es, que $v - d - 1 \geq v - log_3(2v + 1)$ por lo que $k \leq v - d - 1$. Por otra parte la segunda desigualdad implica que $v - log_3(v) > v - d - 2$ y por el teorema 5.2 $k > v - d - 2$ por lo tanto $k = v - d - 1$ y $\mathbf{D} = GA(d, 1, 2)$. El código de este diseño es un código de una clase conocida como códigos generalizados de Reed-Muller, los cuales se definen en la siguiente sección, la prueba de esto va más allá del alcance de este trabajo. Puede consultarse [5; cap. 5] para una prueba. □

En la prueba de esta proposición, los autores de la referencia mencionada al principio de la sección utilizan la afirmación de que si $3^d \leq v < 3^{d+1}$ entonces $d < log_3(1 + 2v) < d + 1$, donde v es un entero positivo congruente con 1 ó 3 módulo 6, lo cual es falso pues tomando $v = 75$ y $d = 3$, ya que $3^4 = 81$, debemos de tener $log_3[1 + 2(75)] > 4$.

Corolario 5.2 *Sea* $\mathbf{D}$ *un* $2 - (v, 3, 1)$ *diseño, y sea* G *su grupo de automorfismos. Si* G *es transitivo en los puntos entonces* $\text{rang}_2(\mathbf{D}) = v$ *o* $\mathbf{D}$ *es un diseño* $GP(d, 1, 2)$ *para algún entero* d.

Demostración: Si $\mathbf{D}$ no es el diseño de puntos y líneas de una geometría proyectiva es porque su distancia mínima no es tres, entonces esta debe ser uno, por lo tanto todos los vectores de peso 1 están en el código. □

Corolario 5.3 *Si la distancia mínima del código binario del diseño* $\mathbf{D} = S(3, 4, v)$ *es* 4 *entonces* $v = 2^d$, *para algún* d, $\mathbf{D} = GA(d, 2, 2)$ *y* $C_2(\mathbf{D}) = RM(d - 2, d)$.

Demostración: La cota por empaquetamiento con esferas implica que

$$k \leq v - log_2(1 + v).$$

Sea x un punto fijo de $\mathbf{D}$ entonces $\mathbf{D}_x$, la contracción de $\mathbf{D}$, es un diseño $S(2, 3, v - 1)$. El código $C_2(\mathbf{D}_x)$ tiene peso mínimo 3 por lo que es un código binario de Hamming: de ahí que $v - 1 = 2^d - 1$ para algún d. y $\mathbf{D}_x = GP(d - 1, 1, 2)$, por lo que $v = 2^d$ y $\dim(C_2(\mathbf{D}_x)) = 2^d - d - 1$. De la desigualdad $2^d < 2^d + 1$ se deduce

$$2^d - d > 2^d - log_2(1 + 2^d) \geq k$$

por lo que $k = 2^d - d - 1$. Así $C_2(\mathbf{D})$ es un $[2^d, 2^d - d - 1, 4]$ código binario, este es el código extendido de Hamming y $\mathbf{D} = GA(d, 2, 2)$. □

Proposición 5.5 *Sean* $\mathbf{D} = (\mathbf{P}, \mathbf{B}) = S(2, 3, v)$ *y* $C = C_p(\mathbf{D})$, *donde* $p = 2$ *ó* 3 *y* p *divide al orden* $n = (v-3)/2$ *del diseño. Si* $p = 2$ *entonces todo vector no cero del código ortogonal tiene peso* $(v+1)/2$ *y el complemento de los soportes forma los puntos de un hiperplano proyectivo. Cada soporte forma un óvalo para* $\mathbf{D}$. *Inversamente el conjunto de puntos fuera de un hiperplano proyectivo forma el soporte de un vector en* $C^{\perp}$. *Si* v *además es de la forma* $8a+7$, *con* $a \equiv 0$ *ó* $1 \pmod 3$, *entonces* $C^{\perp} \subseteq C$.

Si $p = 3$ *entonces todo vector de* $C^{\perp}$ *excepto* $0, \mathbf{1}$ *y* $-\mathbf{1}$ *tiene peso* $2v/3$ *y es la diferencia de los vectores de incidencia de dos hiperplanos paralelos afines. Inversamente cualquiera de tales vectores está en* $C^{\perp}$. *Se tiene además* $C^{\perp} \subseteq C$.

Demostración: Sean $\bar{w}$ un vector no cero de $C^{\perp}$ y S su soporte. Denotaremos por w_x la entrada de $\bar{w}$ en la posición coordenada correspondiente al punto x. Si x, y son dos puntos y $w_x = 1$ entonces $v^{xy} \cdot \bar{w} = 0$ implica que w_y es distinto de w_{x*y}, lo que significa que después de suprimir de $\bar{w}$ la coordenada x exactamente la mitad de las entradas restantes serán cero, por lo tanto

$$| S | = 1 + \frac{v-1}{2} = \frac{v+1}{2}.$$

Además todo bloque que intersecta a S lo hace exactamente dos veces, por lo que $\mathbf{P} - S$ es un hiperlano proyectivo, digamos H, y $v^H = v^{\mathbf{P}} + v^S$. Ya que $\sum_{B \in \mathbf{B}} v^B = r\mathbf{1}$, $n = r - 1$ y n es par, el vector de incidencia de $\mathbf{P}$ está en el código. Por otra parte, ya que H es un 2-$(\frac{v-1}{2}, 3, 1)$ diseño,

$$\sum v^B = \frac{v-3}{4} v^H = \frac{n}{2} v^H,$$

donde la suma se toma sobre todos los $B \in \mathbf{B}$ tales que $B \subset H$. Esto muestra $v^H \in C$ si y sólo si $n/2 \equiv 1 \pmod 2$ y $n \equiv 0 \pmod 2$, esto es si y sólo si $v = 8a + 7$, para $a \in \mathbf{Z}$. La condición $a \equiv 0$ ó $1 \pmod 3$ se obtiene al considerar sólo aquellos valores de v congruentes con 1 ó 3 módulo 6.

Supóngase ahora que $p = 3$. Ya que para todo bloque xy se cumple $\mathbf{1} \cdot v^{xy} = 1 + 1 + 1 = 0$ el vector todo-uno está en $C^{\perp}$. Elíjase un vector $\bar{w}$ diferente de $0, \mathbf{1}, -\mathbf{1}$, entonces para todo bloque xy, $w_x + w_y + w_{x*y} = 0$. Para todo $\alpha \in \mathbf{F}_3$, se denotará por S_α al conjunto de puntos x tales que $w_x = \alpha$. Si $S_0 = \emptyset$, sea x un punto tal que w_x es no nulo, sin pérdida de generalidad puede suponerse que $w_x = 1$. Para todo punto y, distinto de x, se

tiene $w_y + w_{x*y} = 2$ de ahí que $w_x = w_y = w_{x*y} = 1$. Ya que esto sucede para todo punto y diferente de x, $\bar{w} = \mathbf{1}$, lo cual es una contradicción, entonces S_0 es no vacío. Elíjase un punto $x \in S_0$, y un punto y distinto de x, $w_y = -w_{x*y}$, entonces $\mid S_1 \mid = \mid S_{-1} \mid$. Ya que $\mathbf{1}$ está en $C^{\perp}$, $\bar{w} + \mathbf{1} \in C^{\perp}$. Definiendo los conjuntos S'_i como para $\bar{w}$ se tiene $\mid S'_1 \mid = \mid S'_{-1} \mid$, $S'_1 = S_0$ y $S'_{-1} = S_1$, entonces

$$\mid S_0 \mid = \mid S'_1 \mid = \mid S'_{-1} \mid = \mid S_1 \mid = \mid S_{-1} \mid . \square$$

No se da la prueba de los siguientes resultados, las pruebas respectivas se encuentran en la referencia [30].

Teorema 5.6 *Sea* $\mathbf{D}$ *un sistema triple de Steiner con* $v \geq 7$ *puntos. Supóngase que* d *es un entero tal que* $2^d - 1 \leq v < 2^{d+1} - 1$. *Entonces el código binario* $C_2(\mathbf{D})$ *contiene un subcódigo, digamos* C, *que puede ser acortado al código binario de Hamming,* $\mathcal{H}_d$, *suprimiendo* $v - (2^d - 1)$ *posiciones coordenadas donde las entradas de las palabras codificadas de* C *son todas cero. Equivalentemente* $C_2(\mathbf{D})$ *contiende un conjunto de vectores de peso* 3 *que sostienen al diseño* $GP(d-1, 1, 2)$.

En particular si $v = 2^d - 1$ *entonces* $\mathcal{H}_d \subseteq C_2(\mathbf{D})$.

Corolario 5.4 *Sea* $\mathbf{D}$ *un sistema cuádruple de Steiner con* $v \geq 7$ *puntos. y supóngase que* d *es un entero tal que* $2^d \leq v < 2^{d+1}$. *Entonces el código binario* $C_2(\mathbf{D})$ *contiene un subcódigo* C *que puede ser acortado al código de Reed-Muller* $RM(d-2, d)$.

En particular si $v = 2^d$ *entonces* $RM(d-2, d) \subseteq C_2(\mathbf{D})$ *y* $C_2(\mathbf{D})^{\perp} \subseteq RM(1, d)$.

5.5 Códigos generalizados de Reed-Muller

Ahora consideraremos los códigos que resultan de evaluar ciertas fuciones en los puntos de una geometría afín.

Lema 5.3 [5; 153] *Si* $\bar{w} = (w_1, \ldots, w_m) \in \mathrm{F}_q^m$, *entonces su función característica viene dada por*

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

Demostración: Esto es claro notando que cualquier elemento no cero de $\mathbf{F}_q^m$ satisface la ecuación $a^{q-1} = 1$ por lo que la expresión entre corchetes es cero a menos que $x_i = w_i$ para todo i. □

Nótese que $\omega \in \mathbf{F}_q$ implica $x^q - x = [(x-\omega)^{q-1} - 1](x-\omega)$, de ahí que $\prod_{\alpha \in \mathbf{F}_q - \{\omega\}}(x-\alpha) = (x-\omega)^{q-1} - 1$. Evaluando en $x = \omega$ se sigue que el producto de todos los elementos no cero de un campo finito es -1; lo cual generaliza al teorema de Wilson: $(p-1)! \equiv -1 \ (mod\, p)$.

Ejemplo 5.10 El polinomio $1 - (x_i - a)^{q-1}$ es la función característica del $(m-1)$-plano en $\mathbf{F}_q^m$ que satisface la ecuación $x_i = a$.

El lema anterior muestra que toda función de $\mathbf{F}_q^m$ en $\mathbf{F}_q$ es polinomial. Pero como todo elemento de $\mathbf{F}_q$ satisface la ecuación $x^q = x$ estos polinomios pueden ser reducidos módulo $x_i^q - x_i$ y entonces el conjunto de q^m monomios

$$M = \{x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} : \ 0 \leq i_k \leq q-1, \ k = 1, 2, \ldots, m\}$$

forma una base para estas funciones. Obviamente un monomio de M tiene grado a lo más $m(q-1)$. Si ρ es un entero tal que $0 \leq \rho \leq m(q-1)$ denotaremos por M_ρ al espacio vectorial sobre $\mathbf{F}_q$ generado por los monomios en M de grado a lo más ρ, esto es

$$M_\rho = \langle \{x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} : \ 0 \leq i_k \leq q-1, \ \sum i_k \leq \rho, \ k = 1, 2, \ldots, m\} \rangle.$$

Ahora estamos en condiciones de dar la definición de los códigos generalizados de Reed-Muller:

Definición 5.6 *Si m es 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 $\mathbf{F}_q$, denotado por $RM_q(\rho, m)$, es la imagen de la función*

$$ev : M_\rho \longrightarrow \mathbf{F}_q^{q^m},$$

definida por

$$ev(f(x_1, \ldots, x_m)) = (f(p_1), f(p_2), \ldots . f(p_{q^m})),$$

donde $p_1, p_2, \ldots, p_{q^m}$ son los distintos puntos de la geometría afín $GA(m, q)$.

Ejemplo 5.11 Obviamente esta es una generalización de los códigos de Reed-Muller, además $RM_q(0,m) = \mathbf{F}_q\mathbf{1}$ y $RM_q(m(q-1),m) = \mathbf{F}_q^{q^m}$.

Para calcular la dimensión de estos códigos se utilizará el siguiente resultado:

Teorema 5.7 [1;67], [20;184] **(Principio de inclusión exclusión)** *Sea S un conjunto finito de cardinalidad N, y sean $c_1, \ldots, c_t$, t condiciones sobre algunos de los elementos de S. Denotemos por $N(c_{i_1}c_{i_2}\cdots c_{i_k})$ el número de elementos de S que satisfacen las condiciones c_{i_j}, $j = 1, 2, \ldots, k$. Entonces el número de elementos de S que no satisfacen ninguna de las condiciones, $\bar{N}$, está dado por*

$$\bar{N} = N - \sum_i N(c_i) - \sum_{1\le i<j\le t} N(c_ic_j) + \cdots + (-1)^t N(c_1\cdots c_t).$$

Demostración: Basta con calcular las aportaciones de cada punto de S en ambos miembros de la igualdad anterior. □

Podemos ahora calcular la dimensión de los códigos que nos interesan

Teorema 5.8 [5;154] *Para todo entero ρ, $0 \le \rho \le m(q-1)$*

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

Demostración: Sea S_i el conjunto de monomios en m variables de grado i, $0 \le i \le \rho$, y sea c_k la siguiente condición sobre los elementos de S_i : x_k aparece por lo menos q veces en el monomio, $0 \le k \le m$.

Con la notación del teorema anterior $N(c_1)$ es el número de maneras de elegir $i-q$ objetos de entre m objetos, permitiendo repeticiones, esto es $\binom{(i-q)+m-1}{i-q}$; $N(c_1c_2)$ es el número de formas distintas en las que se pueden tomar $i-2q$ objetos con repetición de entre m objetos, esto es $\binom{(i-2q)+m-1}{i-2q}$, se sigue de esta forma hasta obtener que $N(c_1\cdots c_m)$ es $\binom{(i-mq)+m-1}{i-mq}$, por lo tanto el número de monomios de grado i que son elementos de M_ρ es precisamente la suma interior del teorema, sumando sobre i se obtiene el resultado deseado. □

Ejemplo 5.12 Para $\rho = 1$ se tiene que $\dim(RM_q(1,m)) = 1+m$. Ya que todo polinomio lineal no constante en m variables tiene q^{m-1} ceros, estos códigos tienen peso mínimo $q^m - q^{m-1} = q^{m-1}(q-1)$, y todos los vectores excepto los múltiplos escalares del vector todo-uno tienen este peso.

En el caso $m = 1$ podemos obtener que $\dim(RM_q(\rho,1)) = 1+\rho$, y además como un polinomio en una variable de grado a lo más ρ puede tener a lo más ρ raices distintas, ya que $0 \leq \rho \leq q-1$, tenemos un polinomio de grado ρ con ρ raices distintas por lo que el peso mínimo de este código es $q-\rho$, y es un código de máxima distancia separable (MDS).

Generalizando el caso anterior, si $\rho \leq q-1$ no es necesario utilizar un argumento de inclusión exclusión y puede probarse que en este caso

$$\dim(RM_q(\rho,m)) = \begin{pmatrix} \rho+m \\ m \end{pmatrix}.$$

Lema 5.4 [8;69] *Sea f un polinomio en m variables de grado menor que $m(q-1)$. Entonces*

$$\sum_{\bar{w}\in\mathbf{F}_q^m} f(\bar{w}) = 0.$$

Demostración: Ya que

$$f(\bar{x}) = \sum_{\bar{w}\in\mathbf{F}_q^m} p(\bar{w})\chi_{\bar{w}}(\bar{x})$$

y el coeficiente del monomio de grado $m(q-1)$ en $\chi_\alpha(\bar{x})$ es $(-1)^m$ debemos de tener, por hipótesis, que el coeficiente de este monomio en $f(\bar{x})$ es cero. □

Teorema 5.9 [5;156] *Si $\rho \leq m(q-1)$*

$$RM_q(\rho,m)^\perp = RM(m(q-1)-1-\rho,m).$$

Demostración: Sean $f \in M_\rho$ y $g \in M_{m(q-1)-1-\rho}$, entonces $fg \in M_{m(q-1)}$ y $\sum_{\bar{w}\in\mathbf{F}_q^m} f(\bar{w})g(\bar{w}) = 0$, pero esta expresión es el producto interior de las palabras codificadas correspondientes a f y g, por lo tanto estas palabras son ortogonales, y

$$RM(m(q-1)-1-\rho,m) \subseteq RM(\rho,m).$$

Se define una permutación de M enviando el elemento $x_1^{i_1} \cdots x_m^{i_m}$ al monomio $x_1^{q-1-i_1} \cdots x_m^{q-1-i_m}$, esta función garantiza que el número de monomios de grado $\leq \rho$ es el número de monomios de grado $> m(q-1) - 1 - \rho$, y de ahí que la dimensión del código $RM_q(m(q-1)-1-\rho, m)$ es $q^m - \dim(RM_q(\rho, m))$. □

Teorema 5.10 [5;156] *Si* $0 \leq \rho \leq m(q-1)$ *entonces*

$$GLA(m,q) \subseteq Aut[RM_q(\rho, m)].$$

Demostración: Recuérdese que un automorfismo de un código es una permutación del conjunto de posiciones coordenadas que preserva al código, en este caso, si $(f(\alpha))_{\alpha \in \mathbf{F}_q^m}$ es una palabra codificada y σ es una permutación de $\mathbf{F}_q^m$ entonces

$$((f(\alpha))_{\alpha \in \mathbf{F}_q^m})\sigma = (f(\alpha\sigma))_{\alpha \in \mathbf{F}_q^m}$$

es una palabra codificada.

Si $f \in M_\rho$ y $A\bar{x} + \bar{v} \in GLA(m,q)$, entonces $f(A\bar{x} + \bar{v}) \in M_\rho$. □

Teorema 5.11 [5;157] *Para* $0 \leq r \leq m$ *y* $r(q-1) \leq \rho$

$$C_q[GA(m, m-r, q)] \subseteq RM_q(\rho, m).$$

Demostración: Ya que el grupo lineal afín $GLA(m,q)$ es transitivo en los t-planos, y el código $RM_q(\rho, m)$ es invariante bajo este grupo, basta con garantizar que el código contiene el vector de incidencia de un $(m-r)$-plano para obtener el resultado deseado.

El polinomio

$$p(x_1, \ldots, x_m) = \prod_{i=1}^{r} (1 - x_i^{q-1})$$

es de grado $r(q-1)$ y se anula fuera del conjunto de puntos que satisfacen las ecuaciones $x_i = 0$, para $i = 1, \ldots, r$. Por lo tanto este es el vector de incidencia del $(m-r)$-plano definido por estas ecuaciones. □

Como en el caso binario, el código generalizado de Reed-Muller contiene los vectores de incidencia de los $(m-s)$-planos para $0 \leq s \leq r$, como puede verse de la demostración del teorema anterior. Usando un proceso inductivo se puede ver que el subcódigo del código generalizado de Reed-Muller generado por los vectores de incidencia de los $(m-r)$-planos contiene a los vectores de incidencia de los $(m-s)$-planos, $0 \leq s \leq r$.

Definición 5.7 *Para* $0 \leq \rho < m(q-1)$ *el código* **generalizado agujerado de Reed-Muller de** ρ**-ésimo orden**, *denotado* $RM_q(\rho, m)^*$, *es el código de longitud* $q^m - 1$ *obtenido de* $RM_q(\rho, m)$ *suprimiendo la posición coordenada correspondiente al vector* $\mathbf{0}$.

Teorema 5.12 [5;159] $GL(m,q) \subseteq Aut[RM_q(\rho, m)^*]$, *y* $RM_q(\rho, m)^*$ *es un código cíclico.*

Demostración: Ya que el estabilizador de $\mathbf{0}$ en $GLA(m,q)$ es $GL(m,q)$ este último actúa en $RM_q(m,q)^*$.

Sean $K = \mathbf{F}_{q^m}$, ω un elemento primitivo en K y $p(x) = \sum_{i=0}^{m} \omega_i x^i$ el polinomio irreducible de ω sobre $\mathbf{F}_q = E$. Viendo a K como un espacio vectorial sobre E con base $1, \omega, \ldots, \omega^{m-1}$, la multiplicación por ω simplemente cicla sus elementos y es una transformación lineal de orden $q^m - 1$ dada por la matriz compañera de $p(x)$, esto es, por

$$S = \begin{pmatrix} 0 & 0 & \cdots & 0 & -\omega_0 \\ 1 & 0 & \cdots & 0 & -\omega_1 \\ 0 & 1 & \cdots & 0 & -\omega_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\omega_{m-1} \end{pmatrix}.$$

Si $\bar{e} = \bar{e}_1^t = (1, 0, 0, \ldots, 0)^t$, digamos, ordenando las posiciones coordenadas de tal forma que la palabra codificada correspondiente a $f \in M_\rho$ sea

$$(f(\bar{e}^t), f((S\bar{e})^t), f((S^2\bar{e})^t), \ldots, f((S^{q^m-2}\bar{e})^t))),$$

se muestra que el código es cíclico. □

Corolario 5.5 [5;160] *Si* $\rho < m(q-1)$, $RM_q(\rho, m)$ *es un código cíclico extendido, y su dimensión es la misma que el correspondiente código cíclico* $RM_q(\rho, m)^*$.

Demostración: Se sigue del hecho de que si $f \in M_{m(q-1)-1}$

$$f(\mathbf{0}) = -\sum\{f(\bar{w}) : \bar{w} \in \mathbf{F}_q^m - \{\mathbf{0}\}\}. \square$$

Definición 5.8 *Si la representación q-ária del entero positivo u es*

$$u = \sum_{0}^{\infty} u_i q^i,$$

donde $0 \leq u_i \leq q-1$, *definimos el* **q-peso** *de* u, *denotado* $w_q(u)$, *por*

$$w_q(u) = \sum_{0}^{\infty} u_i.$$

Lema 5.5 [5; 161] *Sean* $\rho < m(q-1)$, $\mu = m(q-1)-1-\rho$, $f \in M_\rho$, $u \in \mathbf{N}$, *con* $w_q(u) \leq \mu$, L *un campo de extensión de* $\mathbf{F}_q$, *y* $\bar{a} \in L^m$. *Entonces*

$$\sum_{\bar{w} \in \mathbf{F}_q^m} (\bar{w}, \bar{a})^u f(\bar{w}) = 0,$$

donde $(\cdot,\cdot)$ *denota el producto interior estándard en* L^m.

Demostración: Supóngase que $\bar{w} = (w_1, \ldots, w_m) \in \mathbf{F}_q^m$ y que $\bar{a} = (a_1, \ldots, a_m)$. Sean $u = \sum_0^s u_k q^k$ y

$$g(x_1, \ldots, x_m) = \prod_k (\sum_{i=1}^{m} a_i^{q^k} x_i)^{u_k}.$$

Fijando u_k, cada sumando en el producto anterior es de la forma $c(\bar{a}) x_1^{i_1} \cdots x_m^{i_m}$ con $\sum_{j=1}^m i_j \leq u_k$, y $c(\bar{a})$ una constante que depende de $\bar{a}$. Después de realizar el producto, cada sumando resulta de la forma $c'(\bar{a}) x_1^{i_1} \cdots x_m^{i_m}$ con $\sum_{j=1}^m i_j \leq \sum u_k = w_q(u) \leq \mu$. Entonces $\operatorname{grad}(g(\bar{x}) f(\bar{x})) \leq \rho + \mu < m(q-1)$.

Por otra parte, por el lema 5.4, se tiene

$$\begin{aligned} \textstyle\sum_{\bar{w} \in \mathbf{F}_q^m} (\bar{w}, \bar{a})^u f(\bar{w}) &= \textstyle\sum_{\bar{w} \in \mathbf{F}_q^m} (\sum_{i=1}^m a_i w_i)^{\sum_k u_k q^k} f(\bar{w}) \\ &= \textstyle\sum_{\bar{w} \in \mathbf{F}_q^m} \prod_k (\sum_{i=1}^m a_i^{q^k} w_i)^{u_k} f(\bar{w}) \\ &= \textstyle\sum_{\bar{w} \in \mathbf{F}_q^m} g(\bar{w}) f(\bar{w}) = 0. \ \square \end{aligned}$$

Teorema 5.13 [5; 161] *Si* $K = \mathbf{F}_{q^m}$, $E = \mathbf{F}_q$ *y* ω *es un elemento primitivo de* K, *entonces para* $0 \leq u \leq q^m - 2$, ω^u *es una raíz del código* $RM_q(\rho, m)^*$ *si y sólo si* $0 < w_q(u) \leq m(q-1) - 1 - \rho$.

Demostración: Con la notación de la demostración del teorema 5.12 consideremos a K como un espacio vectorial sobre E. Sea $\bar{a} = (1, \omega, \ldots, \omega^{m-1})^t$ un vector en K^m. Entonces $(S^i\bar{e}, \bar{a}) = \omega^i$ para $i = 0, 1, \ldots, q^m - 2$. Para $f \in M_\rho$ la palabra codificada

$$(f(\bar{e}^t), f((S\bar{e})^t), \ldots, f((S^{q^m-2}\bar{e})^t))$$

en $RM_q(\rho, m)^*$ corresponde, por la relación entre un código cíclico y el ideal de polinomios asociado, al polinomio

$$f(x) = \sum_{i=0}^{q^m-2} f((S^i\bar{e})^t)x^i.$$

Por el lema anterior

$$\begin{aligned} f(\omega^u) &= \textstyle\sum_{i=0}^{q^m-2} f((S^i\bar{e})^t)(\omega^u)^i = \sum_{i=0}^{q^m-2} f((S^i\bar{e})^t)(S^i\bar{e}, \bar{a})^u \\ &= \textstyle\sum\{f(\bar{w}) : \bar{w} \in \mathbf{F}_q^m - \{\mathbf{0}\}\} = 0 \end{aligned}$$

para $0 < w_q(u) \leq m(q-1) - 1 - \rho = \mu$. Pero como $w_q(u) = m(q-1) - w_q(q^m - 1 - u) > \mu$ si y sólo si $w_q(q^m - 1 - u) \leq \rho$, el número de enteros u con $u = 0$ o $w_q(u) > \mu$ es la dimensión de $RM_q(\rho, m)$, pues la función que envía el número

$$q^m - 1 - u = \sum_{i=0}^{m-1} v_i q^i \quad \text{a} \quad x_0^{v_0} \cdots x_{m-1}^{v_{m-1}}$$

es biyectiva, esto muestra que tenemos exactamente las raices del polinomio generador. □

Corolario 5.6 [5; 163] *Sean* $0 \leq \rho < m(q-1)$, $\mu + \rho = m(q-1) - 1$ *y* ω *un elemento primitivo de* $\mathbf{F}_{q^m}$ *entonces*

a) El código $RM_q(\rho, m)^*$ *es cíclico y su polinomo generador es* $g(x) = \prod(x - \omega^u)$, *donde* $0 < u < q^m - 1$, *y* $w_q(u) \leq \mu$.

b) El código $(RM_q(\rho, m)^*)^\perp$ *es un código cíclico y su polinomio generador es* $g^\perp(x) = \prod(x - v)$, *donde* $0 \leq v < q^m - 1$, *y* $w_q(u) \leq \rho$.
Además

$$(RM_q(\rho, m)^*)^\perp = RM_q(\mu, m)^* \cap (\mathbf{F}_q\mathbf{1})^\perp.$$

c) La dimensión del código $RM_q(\rho, m)$, *(o bien de* $RM_q(\rho, m)^*$*) está dada por*

$$| \{u : 0 \leq u \leq q^m - 1, \ w_q(u) \leq \rho\} | .$$

Demostración: El inciso (a) es una consecuencia inmediata del teroema anterior, y (c) simplemente es otra manera de contar los generadores de M_ρ. La primera parte de (b) se sigue del la forma en la cual se calcula el polinomio generador del código dual a un código cíclico, mientras que la segunda parte se obtiene de (a) y notando además que el factor $(x-1)$ obliga que nuestro código sea un subcódigo de $(\mathbf{F}_q\mathbf{1})^\perp$. □

Teorema 5.14 [5;164] *Si $\rho = r(q-1)+s$, $0 \leq s < q-1$, entonces el código $RM_q(\rho, m)^*$ es un subcódigo de un código BCH de longiud $q^m - 1$ sobre $\mathbf{F}_q$ con distancia designada $(q-s)q^{m-r-1}$.*

Demostración: Pongamos como antes $\mu = m(q-1) - \rho - 1$ y sea δ el menor entero con $w_q(\delta) = \mu + 1$. Ya que $\mu + 1 = (m-r)(q-1) - s = (m-r-1)(q-1) + (q-1-s)$ se tiene

$$\delta = (q-s-1)q^{m-r-1} + \sum_{i=0}^{m-r-2} (q-1)q^i = (q-s)q^{m-r-1} - 1.$$

De esta forma todo entero positivo menor que δ tiene q-peso menor o igual que μ, por lo que los elementos ω, $\omega^2, \ldots, \omega^{\delta-1}$ son todos los ceros del código $RM_q(\rho, m)^*$. □

Ahora se probará que los códigos de Reed-Muller tienen distancia mínima igual a la distancia designada del código BCH en el cual están inmersos.

Teorema 5.15 [5;165] *Si $0 \leq \rho < m(q-1)$, y $\rho = r(q-1)+s$ con $0 \leq s < q-1$, entonces $RM_q(\rho, m)$ tiene vectores de peso $(q-s)q^{m-r-1}$ que consisten de la suma de múltiplos de los vectores de incidencia de $(q-s)$, $(m-r-1)$-planos paralelos, todos contenidos en un $(m-r)$-plano.*

Demostración: Elíjanse r elementos arbitrarios $w_i \in \mathbf{F}_q$, no necesariamente distintos, y s elementos distintos w'_j del mismo campo. Entonces el polinomio $p(x_1, \ldots, x_m)$

$$\prod_{i=1}^{r} [1 - (x_i - w_i)^{q-1}] \prod_{j=1}^{s} (x_{r-1} - w'_{r+1})$$

tiene grado $r(q-1)+s=\rho$ y es cero en los puntos de $\mathbf{F}_q^m$ que no satisfacen las ecuaciones

$$x_i = w_i \quad \text{para i} = 1,\ldots,\text{r};$$
$$x_{r+1} = a,$$

donde a es distinto de los w_j' para $j = 1,\ldots,s$; $(q-s)q^{m-r-1}$ vectores en $\mathbf{F}_q^m$ satisfacen estas ecuaciones y la palabra codificada correspondiente a $p(\bar{x})$, $\bar{x}=(x_1,\ldots,x_m)$, tiene este peso.

Ahora considérense los q^{m-r-1} puntos de $\mathbf{F}_q^m$ satisfaciendo las primeras r ecuaciones anteriores y además la ecuación $x_{r+1}=c$, donde c es un elemento de $\mathbf{F}_q$ distinto de los w_i'. Entonces todos estos puntos están en un $(m-r-1)$-plano y las posiciones coordenadas correspondientes en la palabra codificada de $p(\bar{x})$ tienen el valor constante $\prod_{j=1}^{s}(c-w_j')$ en dichos puntos. Ya que esto sucede con cada uno de los $q-s$ elementos de $\mathbf{F}_q$ distintos de los w_j' se obtiene un vector en la forma enunciada. □

Notemos que $RM_q(\rho,1)^*$ es un $[q-1,\rho+1,q-\rho-1]$ código q-ario de Reed-Solomon, el cual es máxima distancia separable, i.e., un código MDS.

Corolario 5.7 [5;166] *Si* $\rho = r(q-1)+s < m(q-1)$ *con* $0 \le s < q-1$ *entonces* $RM_q(\rho,m)$ *tiene distancia mínima* $(q-s)q^{m-r-1}$ *y* $RM_q(\rho,m)^*$ *tiene distancia mínima* $(q-s)q^{m-r-1}-1$.

Demostración: Con la notación anterior tómese $w_i=0$ para $i=1,\ldots,r$ y los w_j' todos distintos de cero, entonces el vector $\mathbf{0}$ no es un cero del correspondiente polinomio, así que la palabra codificada correspondiente en $RM_q(\rho,m)^*$ tiene peso $(q-s)q^{m-r-1}$; esta es entonces la distancia mínima del código, por el teorema anterior. Entonces la distancia mínima del código $RM_q(\rho,m)$ es $(q-s)q^{m-r-1}$ pues tiene vectores de este peso. □

Corolario 5.8 [5;166] *Sea* p *un primo. Entonces la distancia mínima del código* $C_p[GA(m,r,p^t)]$ *es* p^{tr}.

Demostración: Sea $q=p^t$, ya que

$$C_p[GA(m,r,p^t)] \subseteq RM_q((m-r)(q-1),m)$$

y la distancia mínima del código de Reed-Muller es q^r, la distancia mínima del código del diseño es al menos esta cantidad, pero este último tiene vectores de este peso. □

Ejemplo 5.13 El código de Reed-Muller $RM_3(1,2)$ es

000000000	111202002	021211200	021120012
111111111	111020220	102022011	210100122
222222222	201220101	201102210	012122100
012001212	222010110	210012201	102201120
000121221	210221010	201011022	120021102
021002121	000212112	222101001	120200211
120112020	102110202	012210021	

Figura 5. $RM_3(1,2)$.

Entonces el código $(RM_3(1,2)^*)^\perp$ es precisamente $RM_3(2,2)^* \cap (\mathbf{F}_3\mathbf{1})^\perp$.

Construyamos el campo de orden 9 como el conjunto de polinomios en el anillo $\mathbf{F}_3[x]$ reducidos módulo x^2+1. La clase de $1+x$, que denotaremos por ω, es un elemento primitivo del campo. Ya que los enteros positivos menores que ocho con 3-peso menor que 2 son $1, 2, 3, 4$ y 6, el polinomio generador del código $RM_3(1,2)^*$ es

$$\begin{aligned} g(x) &= (x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4)(x-\omega^6) \\ &= x^5 + 2x^4 + x^3 + x^2 + x + 2. \end{aligned}$$

Similarmente encontramos que el polinomio generador para $(RM_3(1,2)^*)^\perp$ es $g^\perp(x) = x^3 + x + 2$.

Utilizando el primer polinomio podemos construir una matriz generadora para $RM_3(1,2)^*$ y entonces utilizarla para obtener una matriz generadora para $RM_3(1,2)$. La distancia mínima de éste último código es 6 y todo vector de peso mínimo es la diferencia de dos vectores de incidencia de líneas de $GA(2,3)$, las cuales son

$$\begin{array}{lll} l_1 = \{1,4,5\} & l_2 = \{2,6,8\} & l_3 = \{3,7,9\} \\ l_4 = \{1,2,3\} & l_5 = \{4,6,9\} & l_6 = \{5,7,8\} \\ l_7 = \{1,8,9\} & l_8 = \{2,4,7\} & l_9 = \{3,5,6\} \\ l_{10} = \{1,6,7\} & l_{11} = \{2,5,9\} & l_{12} = \{3,4,8\} \end{array}$$

Si denotamos por v_i al vector de incidencia de l_i entonces, por ejemplo, los vectores

$$v_2 - v_3,\ v_5 - v_6,\ v_3 - v_2,\ v_6 - v_5,\ v_1 - v_2,\ v_4 - v_5,\ v_1 - v_3, \ldots$$

son algunas de las palabras codificadas de peso mínimo en $RM_3(1,2)$.

También es posible definir códigos de Reed- Muller asociados a geometrías proyectivas finitas, y se puede hacer un análisis similar al anterior, es decir, determinar su dimensión, su distancia mínima, el código dual, y el hecho de que este código también es cíclico. (cf. [31], [50])

En la referencia [44] se estudian los códigos de Reed-Muller (generalizados y proyectivos) usando técnicas de álgebra conmutativa, como son ideales de puntos, la función de Hilbert, resoluciones proyectivas, etc.

6 Gráficas y conjuntos diferencia

En este capítulo se presenta un estudio de códigos asociados a algunas gráficas, cuando estas son vistas como estructuras de incidencia. En particular se clasifican los códigos asociados a las gráficas completas.

También se introduce el concepto de conjunto diferencia, los cuales están naturalmente asociados a diseños que tiene el mismo número de puntos que de bloques, esto es simétricos. Se muestra que los puntos en un hiperplano de la geometría proyectiva $GP(n,q)$ determina uno de estos conjuntos. Por último se estudian los códigos binarios asociados a un 2-$(16,6,2)$ diseño; pues los diseños con estos parámetros pueden ser naturalmente asociados con un conjunto diferencia.

La primera sección de este capítulo es la única del presente trabajo en la que todos los resultados son propios.

6.1 Gráficas como estructuras de incidencia

En esta sección K_n denotará a la gráfica completa de n vértices. Recuérdese que, si $\mathbf{S}$ es una estructura de incidencia finita, el código asociado a $\mathbf{S}$ sobre $\mathbf{F}_q$ se denota como $C_q(\mathbf{S})$.

Teorema 6.1 *Sean $n \geq 2$ y F un campo finito de orden q. Si la característica de F es dos entonces $C_q(K_n)$ es $(F\cdot\mathbf{1})^{\perp}$; en cualquier otro caso $C_q(K_n) = F^n$.*

Si q es una potencia de 2, una base del código está dada fijando un punto de la gráfica y tomando los vectores de incidencia de los arcos que contienen dicho punto. En particular si n es par el vector todo uno $\mathbf{1}$ está en el código y si $n = 2^m$, K_n es el diseño de de puntos y líneas del la geometría afín $GA(m,2)$ y $C_2(K_{2^m}) = RM(m-1,m)$.

Demostración: Denotemos por $\bar{e}_i$ al vector de longitud n con un 1 en la i-ésima posición y cero en las demás. Una base para $(F\cdot\mathbf{1})^{\perp}$ está dada por los vectores $\bar{e}_i + \bar{e}_n$, $1 \leq i \leq n-1$. Mostraremos que a menos que $\mathrm{car}(F) = 2$ podemos extender este conjunto de vectores a una base de F^n.

Consideremos $a_k \in F$, $\bar{e}_k$, $k = 1, \ldots, n$ y elijamos $i < j < n$ Supongamos que

$$\sum_{k=1}^{n-1} a_k(\bar{e}_k + \bar{e}_n) + a_n(\bar{e}_i + \bar{e}_j) = 0.$$

Ya que el coeficiente de $\bar{e}_n$ es $\sum_{k=1}^{n-1} a_k$, esta cantidad debe ser cero por lo que $a_k = 0$ si k es distinto de i y j y $a_i = a_j = -a_n$, pero entonces $a_i = a_j = -a_i$ de ahí que si $\text{car}(F) > 2$ debemos de tener $a_i = a_j = a_n = 0$ por lo que

$$\{\bar{e}_i + \bar{e}_n : 1 \leq i \leq n-1\} \cup \{\bar{e}_i + \bar{e}_j\}$$

es una base para F^n. Cuando F es de característica 2 este conjunto es linealmente dependiente, esto prueba el teorema. □

Un **camino** de longitud n, en una gráfica, es una sucesión finita de aristas $a_1, \ldots, a_n$ junto con una sucesión de vértices $p_1, \ldots, p_{n+1}$, tales que la i-ésima arista es adyacente a los vértices p_i y p_{i+1}. Una gráfica es **conexa** si todo par de vértices distintos está unido por un camino. Un camino es **simple** si todas sus aristas son diferentes. Si el camino $\{x_1, x_2\} \cdots \{x_{n-1}, x_n\}$ es simple entonces el camino $\{x_1, x_2\} \cdots \{x_n, x_1\}$ se denomina **ciclo.**

Corolario 6.1 *Para todo entero m tal que $2^m \leq n < 2^{m+1}$, $C_2(K_n)$ contiene un código que puede ser acortado al código $RM(m-1, m) = (\mathbf{F}_2\mathbf{1})^\perp$.*

Además si T es un camino de longitud $n-1$ entonces $C_q(T) = (\mathbf{F}_q\mathbf{1})^\perp$, para cualquier potencia q de 2.

Demostración: La primera parte se sigue del teorema anterior y del hecho de que K_n contiene una subgráfica K_{2^m}.

Supóngase ahora que T es el camino $\{x_1x_2\}\{x_2x_3\} \cdots \{x_{n-1}x_n\}$. Entonces el vector de incidencia de los vértices x_i y x_j, $i < j$, es la suma de los vectores de incidencia de las aristas $\{x_ix_{i+1}\}\{x_{i+1}x_{i+2}\} \cdots \{x_{j-1}x_j\}$ y por lo tanto está en $C_q(T)$. Se tienen entonces todos los vectores de incidencia de cualquier par de vértices. □

Una **gráfica bipartita** G consiste de la unión ajena de dos conjuntos no vacíos, V_1, V_2 de vértices tales que toda arista de G une un vértice de V_1 con un vértice de V_2.

Corolario 6.2 *Si $G = G_1 \cup G_2$ es una gráfica bipartita entonces $C_2(G) = (\mathbf{F}_2\mathbf{1})^\perp$.*

Demostración: Sin pérdida de generalidada puede suponerse que G_2 tiene al menos tantos puntos como G_1. Procedamos entonces por inducción

sobre el número de vértices m de G_1 : para $m = 1$ el resultado es claro de la demostración del teorema precedente, supóngase pues el resultado para m. En el caso $m+1$ elijamos m puntos, por hipótesis de inducción y el teorema anterior una base para este código está dada por los vectores de incidencia de cada par de vértices con uno de ellos fijo. Supongamos por ejemplo que el vértice fijo, x, es uno de los m elegidos. Entonces sólo nos resta probar que si y es el punto de G_1 que no fue elegido, el vector de incidencia de x y y está en el código. Elijamos un punto cualquiera z de G_2 entonces $v^{\{x,z\}} + v^{\{z,y\}}$ es el vector deseado. □

Una subgráfica T de la gráfica conexa G se llama **árbol generador** si T es una gráfica conexa, sin ciclos e incluye todos los vértices de G.

Corolario 6.3 *Sea q una potencia de 2. El código q-ario de un árbol generador de una gráfica completa G es $C_q(G)$.* □

Proposición 6.1 *El código q-ario de longitud impar de un camino simple es un código cíclico generado por $1+x$. En particular $RM(m-1,m) = \langle 1+x \rangle$.*

Demostración: Se sigue del hecho de que $x+1$ divide a $x^n - 1$ si n es par, y de que una matriz generadora para el código está dada por

$$G = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}. \square$$

Proposición 6.2 *Sea K_{2m} la gráfica completa de $2m$ lados, $m \geq 3$. Considérese la estructura de incidencia* S *cuyo conjunto de puntos,* P, *es el conjunto de vértices de la gráfica y, teniendo etiquetados los vértices en el sentido de las manecillas de un reloj, tomaremos como bloques a los conjuntos*

$$\{1, m, m+1, m+2\}, \{2, m+1, m+2, m+3\} \ldots \{m-1, 2m-2, 2m-1, 2m\}.$$

Entonces, para cada potencia q de un primo, el código q-ario de S *es un $[2m, m-1, 4]$ código.*

Demostración: Es claro que la longitud y la dimensión del código $C_q(\mathbf{S})$ es $2m$ y $m-1$, respectivamente. Para ver que su distancia mínima es 4 basta con aplicar directamente el teorema 2.2. □

Ejemplo 6.1 *El código correspondiente al octágono, como se describe en la proposición, tiene matriz generadora*

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

Proposición 6.3 *Sean G y $\mathbf{P}$ como en la proposición anterior, pero por conjunto de bloques tómense los anteriores junto con $\{1, m, 2m-1, 2m\}$, $m \geq 5$. Si q no es una potencia de 2 entonces $C_q(G)$ es un $[2m, m, 4]$ código.*

Demostración: Si se aplica la permutación $(1, m+1)(m, 2m)$ a las columnas de la matriz de incidencia de G puede ser transformada en una matriz en la forma estándard con m renglones. La prueba sobre la distancia mínima es similar a la de la proposición precedente. □

En [43] se hace un análisis más detallado de códigos asociados a gráficas.

6.2 Conjuntos diferencia

Definición 6.1 *Un 2-(v, k, λ) diseño simétrico es llamado* **cíclico** *si tiene un automorfismo que permuta los puntos y también los bloques en un un ciclo de longitud v.*

Definición 6.2 *Sea G un grupo de orden v. Se dice que un 2-(v, k, λ) diseño $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ admite a G como* **grupo regular de automorfismos**, *si para un punto fijo u y un bloque particular B, se cumple*

$$\mathbf{P} = \{(u)g : g \in G\} \quad y \quad \mathbf{B} = \{(B)g : g \in G\}.$$

Llamaremos a u y a B **punto base** *y* **bloque base** *respectivamente.*

Si $y = (u)g_1$ es otro punto entonces $(u)g = (y)g_1^{-1}g$, por lo tanto podemos identificar los puntos con los elementos del grupo y un cambio de punto base reemplaza g por $g_1 g$ para un g_1 adecuado.

Definición 6.3 *Un k-subconjunto $D = \{a_1, \ldots, a_k\}$ de un grupo G de orden v es llamado un (v, k, λ)* **conjunto diferencia** *si para todo elemento d de G, excepto la identidad, existen precisamente λ pares ordenados $(a_i, a_j) \in D \times D$, que satisfacen una de las condiciones siguientes:*

1) $a_i a_j^{-1} = d$.
2) $a_i^{-1} a_j = d$.

Ejemplo 6.2 Sea $\mathbf{Z}_m$ el grupo aditivo de los enteros módulo m. Puede comprobarse fácilmente que los subconjuntos $D_1 = \{1, 2, 4, 10\} \subset \mathbf{Z}_{13}$ y $D_2 = \{0, 1, 6, 8, 18\} \subset \mathbf{Z}_{21}$ forman $(13, 4, 1)$ y $(21, 5, 1)$ conjuntos diferencia respectivamente.

Teorema 6.2 [22; 149] *Las condiciones* (1) *y* (2) *de la definición anterior son equivalentes. Si* $\mathbf{D}$ *es un* 2-(v, k, λ) *diseño simétrico que admite al grupo* G *como grupo regular de automorfismos y si* $(u)a_1, \ldots, (u)a_k$ *son los puntos de un bloque de* $\mathbf{D}$, *entonces* $D = \{a_1, \ldots, a_k\}$ *es un* (v, k, λ) *conjunto diferencia. Inversamente si* $D = \{a_1, \ldots, a_k\}$ *es un* (v, k, λ) *conjunto diferencia de elementos de un grupo* G *de orden* v, *entonces la familia*

$$\{(D)g = \{a_1 g, \ldots, a_k g\} : g \in G\}$$

es el conjunto de bloques de un 2-(v, k, λ) *diseño simétrico que admite a* G *como grupo regular de automorfismos; este diseño recibe el nombre de* **desenvolvimiento de** D.

Demostración: Sea $\mathbf{D}$ un 2-(v, k, λ) diseño que admite al grupo G de orden v como grupo regular de automorfismos. Sea u un punto base; entonces $\mathbf{P} = \{(u)g : g \in G\}$ y el punto $(u)g$ puede ser identificado con g. Si los puntos de un bloque base D son $a_1, \ldots, a_k$ entonces todo bloque es de la forma $(D)g = \{a_1 g, \ldots, a_k g\}$. Para cada elemento d de G, distinto de la identidad e, existen exactamente λ pares ordenados $(a_i, a_j) \in D \times D$ tales que para algún $g \in G$, $a_i g = d$ y $a_j g = e$, de ahí que $d = a_i a_j^{-1}$. Por lo tanto $D = \{a_1, \ldots, a_k\}$ es un (v, k, λ) conjunto diferencia que satisface la condición (1).

Inversamente sea $D = \{a_1, \ldots, a_k\}$ es un (v, k, λ) conjunto diferencia de elementos del grupo G de orden v que satisface (1). Sean x, y dos elementos distintos de G, entonces $xy^{-1} = d$ es distinto de e, por lo tanto existen λ parejas ordenadas (a_i, a_j) tales que $a_i a_j^{-1} = d = xy^{-1}$, de ahí que $a_i^{-1} x = a_j^{-1} y = g$ y por lo tanto $\{x, y\} \subset (D)g$. La desigualdad de Fisher, probada en el último párrafo de la sección 5.1, garantiza que el diseño es simétrico.

Probemos ahora que la condición (1) implica a la condición (2). Sea M la matriz de incidencia del diseño del desenvolvimiento de D. Si d es diferente de e, ya que el desenvolvimiento de D es un 2-diseño, cualesquiera dos bloques tienen exactamente λ puntos en común (como puede verse calculando $MM^t = (r - \lambda)I + \lambda \mathbf{1}$, donde I es la matriz identidad y $\mathbf{1}$ es la matriz

que tiene todas sus entradas iguales a 1) por lo que existen exactamente λ bloques del desenvolvimiento de D incidentes con d y con e. Se obtienen entonces exactamente λ parejas ordenadas (a_i, a_j) tales que $a_i d = a_j$, por lo tanto $d = a_i^{-1} a_j$. Esto prueba que la condición (1) implica la condición (2). Inversamente si suponemos la propiedad (2), los conjuntos $\{a_1 r, \ldots, a_k r\}$ y $\{a_1 s, \ldots, a_k s\}$ tienen exactamente λ elementos en común. Por lo tanto estos conjuntos son los bloques de un 2-(v, k, λ) diseño. □

Ejemplo 6.3 Puede verificarse directamente que el desenvolvimiento del conjunto diferencia $D = \{1, 2, 4\}$ en el grupo aditivo $\mathbf{Z}_7 = \{1, 2, 3, 4, 5, 6, 7\}$ es el plano de Fano $\mathcal{F}$, que difiere del que se ha mencionado anteriormente sólo por la numeración de sus puntos. Aplicando la permutación (473) a los puntos del desenvovimiento del conjunto diferencia obtenemos este diseño tal y como se había construido anteriormente.

Similarmente el diseño de puntos $\mathbf{Z}_7$, y bloques la familia de transladados del conjunto diferencia $\{1, 2, 3, 5\}$, resulta ser el diseño de puntos y óvalos de $\mathcal{F}$.

Conviene recordar que de acuerdo a la sección 4.1 un 2-(v, k, λ) diseño simétrico satisface las ecuaciones

$$b = v, \quad k = r, \quad k(k-1) = \lambda(v-1).$$

No es difícil convencerse de que si G es un grupo abeliano de orden v y $D = \{a_1, \ldots, a_k\}$ es un k-conjunto de G, con $v = k(k-1)+1$, entonces D es un $(v, k, 1)$ conjunto diferencia si y sólo si $a_i a_j$ es diferente de $a_l a_m$, para cualesquiera cuatro elementos distintos a_i, a_j, a_l, a_m de D con $i \leq j$ y $l \leq m$.

Además si a y b son dos elementos distintos de $\mathbf{F}_7$ entonces $D = \{a, b, 2b-a, 4b-3a\}$ es un $(7, 4, 2)$ conjunto diferencia y su desenvolvimiento es isomorfo al diseño de puntos y óvalos del plano de Fano. Si a y b son dos elementos distintos del grupo $\mathbf{F}_{11}$ entonces $D = \{a, b, 5a-4b, 2b-a\}$ es un $(11, 5, 2)$ conjunto diferencia.

Teorema 6.3 [5; 122] **(Brauer)** *Sea* $\mathbf{S} = (\mathbf{P}, \mathbf{B})$ *una estructura de incidencia con el mismo número de puntos que de bloques y supóngase que la matriz de incidencia es no singular. Entonces todo automorfismo de* $\mathbf{S}$ *fija tantos puntos como bloques y tiene la misma estructura cílica en* $\mathbf{P}$ *que en* $\mathbf{B}$. *Además si* G *es cualquier subgrupo de* $Aut(\mathbf{S})$ *entonces* G *tiene el mismo número de órbitas en los puntos que en los bloques.*

Demostración: Sea A una matriz de incidencia para $\mathbf{S}$, no singular. Cada automorfismo de $\mathbf{S}$ actúa como una permutación en $\mathbf{P}$ y en $\mathbf{B}$. Sean P y R, respectivamente, las matrices de permutación que repersentan dichas operaciones. Entonces $AP = RA$ y, como A es no singular, $A^{-1}RA = P$; por lo tanto P y R son matrices similares. Ya que el número de puntos fijos de una matriz de permutación es su traza, y matrices similares tienen la misma traza, se sigue la afirmación del teorema sobre los puntos fijos.

Sean n_i y m_i el número órbitas de puntos y de bloques, respectivamente, de longitud i. Hemos mostrado que $n_1 = m_1$. Ahora probamos por inducción que $n_i = m_i$: supóngamos que $n_i = m_i$, para $1 \leq i \leq k$. Si ψ es un automorfismo de $\mathbf{S}$, entonces ψ^k fija $\sum tn_t$ puntos y $\sum tm_t$ bloques, donde la suma se toma sobre todos los divisores t de k. Pero las matrices de permutación en puntos y bloques, asociadas naturalmente a ψ^k son P^k y R^k, respectivamente, estas matrices son similares, por lo que tienen la misma traza. Por lo tanto $\sum tn_t = \sum tm_t$, así que, por hipótesis de inducción $kn_k = km_k$, de ahí que $n_k = m_k$.

Por último, si G es un subgrupo de $Aut(\mathbf{S})$, por el teorema de Burnside (el número de órbitas de un grupo de permutación sobre un conjunto finito es el número de puntos fijos, por los elementos del grupo, dividido por la cardinalidad del grupo, cf. [17; 163]) y la primera afirmación implican que el número de órbitas en puntos es el mismo que el de órbitas en bloques. □

Aunque el problema de la enumeración de todos los conjuntos diferencia aún continua abierto existen dos métodos bien conocidos de construir conjuntos diferencia, (cf. [9; 150], [22; 170]), uno se describe aquí con detalle, en el siguiente teorema. El otro método utiliza el concepto de residuo cuadrático, por lo que está fuera de la línea del presente trabajo.

Teorema 6.4 [22; 156] *Los hiperplanos de $GP(n, q)$ forman un 2-diseño simétrico cíclico, además los puntos en cualquier hiperplano determinan un (v, k, λ) conjunto diferencia, donde*

$$v = (q^{n+1} - 1)/(q - 1),\ k = (q^n - 1)/(q - 1),\ y\ \lambda = (q^{n-1} - 1)/(q - 1).$$

Demostración: Sea α un elemento primitivo del campo $\mathbf{F}_q^{n+1}$, y sea $f(x) = \sum_{i=0}^{n+1} c_i x^i$ el polinomio irreducible de α sobre $\mathbf{F}_q$. Toda potencia de α puede ser escrita como $\alpha^i = a_0 + a_1\alpha + \cdots + a_n\alpha^n$, con los a_j en $\mathbf{F}_q$. Ya que el orden de α^v es $q - 1$ tenemos $\mathbf{F}_q = \{0, 1, \alpha^v, \ldots, \alpha^{(q-2)v}\}$.

Ya que para cada entero l, $\alpha^{lv+i} = \alpha^{lv}\alpha^i$ y $\alpha^{lv} \in \mathbf{F}_q$, las potencia α^i, α^j corresppponden al mismo punto en $GP(n,q)$, bajo el isomorfismo canónico entre $\mathbf{F}_{q^{n+1}}$ y $\mathbf{F}_q^{n+1}$, si y sólo si $i \equiv j \ (mod\ v)$.

Definamos la función $\phi : \mathbf{F}_{q^{n+1}} \to \mathbf{F}_{q^{n+1}}$ por la relación $\phi(0) = 0$, $\phi(\alpha^i) = \alpha^{i+1}$. La correspondiente función de $\mathbf{F}_q^{n+1}$ en sí mismo queda entonces determinada por

$$\tilde{\phi} : (a_0, \ldots, a_n) \mapsto (-a_n c_0, a_0 - a_n c_1, \ldots, a_{n-1} - a_n c_n).$$

Esta función biyectiva es lineal, así que envía puntos sobre puntos y t-espacios sobre t-espacios. Ya que $1, \alpha, \ldots, \alpha^{v-1}$ corresponden a puntos distintos de $GP(n,q)$, $\tilde{\phi}$ permuta los v puntos en un único ciclo. Además ya que $v - qk = 1$, v y k son primos relativos. Por lo tanto si $\tilde{\phi}^j$ envía los puntos de un hiperplano en sí mismos entonces los permuta en ciclos cuya longitud es un divisor de k. En efecto, pues si $\prod$ es un hiperplano que fija $\tilde{\phi}^j$ y

$$\tilde{\phi}^j \mid_{\prod} = (a_1 \cdots a_{t_1})(b_1 \cdots b_{t_2}) \cdots (u_1 \cdots u_{t_l}),$$

ya que $\tilde{\phi}^{jk} = 1$, y por la independencia de los ciclos

$$\tilde{\phi}^{jk} \mid_{\prod} = (a_1 \cdots a_{t_1})^k (b_1 \cdots b_{t_2})^k \cdots (u_1 \cdots u_{t_l})^k,$$

y debemos de tener entonces que cada uno de los t_i divide a k. Pero como $\tilde{\phi}^v = 1$, también debe cumplirse que los t_i dividen a v, esto sólo es posible si $t_i = 1$, $i = 1, 2, \ldots, l$. De ahí que ninguna potencia de $\tilde{\phi}$, excepto la identidad, fija un hiperplano, por consiguiente $\tilde{\phi}$ debe permutar los hiperplanos en un ciclo de longitud v. □

Definición 6.4 *Una matriz* **circulante** *es una matriz $n \times n$ cuyo $(i+1)$-ésimo renglón es un corrimiento cíclico del i-ésimo renglón.*

Obviamente si $D \subseteq \mathbf{Z}_v$ es un (v, k, λ) conjunto diferencia, la matriz de incidencia de su desenvolvimiento es una matriz circulante. La afirmación recíproca también es válida. En efecto sea $\mathbf{D}$ un 2-(v, k, λ) diseño simétrico cuya matriz de incidencia es circulante. Supóngase que los puntos son los elementos de $\mathbf{Z}_v$ y denótense los bloques como $B_0, B_1, \ldots, B_{v-1}$. Si $B_0 = \{a_1, \ldots, a_k\}$ entonces, por la propiedad circulante de la matriz de incidencia,

$B_i = \{a_1 + i, \ldots, a_k + i\}$. Para todo elemento d no nulo de $\mathbf{Z}_v$ existen λ bloques que contienen a 0 y a d, esto es, el sistema

$$a_l + j = d, \quad a_m + j = 0$$

tiene λ soluciones, por lo que existen λ parejas (a_l, a_m) tales que $a_l - a_m = d$, lo cual es equivalente a decir que B_0 es un (v, k, λ) conjunto diferencia.

La siguiente proposición indica cómo obtener códigos auto-ortogonales a partir de diseños simétricos.

Proposición 6.4 [46; 120] *Sea M la matriz de incidencia de un 2-(v, k, λ) diseño simétrico $\mathbf{D} = (\mathbf{P}, \mathbf{B})$.*

1) Si $k \equiv \lambda \equiv 0 \ (mod\ p)$ entonces $C_p(\mathbf{D})$ es un código auto-ortogonal.

2) Para $k + 1 \equiv \lambda \equiv 0 \ (mod\ p)$, sea G la matriz $v \times 2v$ cuyas primeras v columnas constituyen la matriz identidad y cuyas últimas v columnas son las columnas de M. Entonces G es la matriz generadora de un $[2v, v]$ código auto-ortogonal.

3) Si λ es impar y k es par sea G la matriz $(v+1) \times (2v+2)$ cuyas primeras $v+1$ columnas constituyen la matriz identidad, cuya columna $(v+2)$ consiste de un cero en el primer renglón y unos en todos los demás, y cuyas últimas v columnas son aquellas de M a las cuales se les ha añadido superiormente un uno. Entonces G es la matriz generadora de un $[2v + 2, v + 1]$ código auto-ortogonal.

Demostración: La prueba de (1) y (2) es clara. para probar (3) basta notar que $k(k-1) = \lambda(v-1)$ implica que v es impar. □

6.2.1 Los 2-(16, 6, 2) diseños.

Sea $G = \mathbf{Z}_2 \times \mathbf{Z}_8$ entonces

$$D = \{00, 01, 02, 05, 10, 16\} \text{ y } E = \{00, 01, 10, 12, 15, 16\}$$

son (16, 6, 2) conjuntos diferencia. Si $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ es el grupo de cuaterniones y $H = Q \times \mathbf{Z}_2$ entonces $D = \{10, i0, j0, k0, 11, -11\}$ también es un (16, 6, 2) conjunto diferencia.

Sea ha probado que, salvo isomorfismo, los anteriores son todos los (16, 6, 2) conjuntos diferencia (ver [27]).

Esta sección está basada en [7] por lo que se omitirán las indicaciones de las referencias.

Si C es un código binario auto-ortogonal, i.e. $C \subseteq C^{\perp}$, entonces la función $\phi : \bar{c} \mapsto (1/2)ps(\bar{c})\ (mod\ 2)$, donde $ps(\cdot)$ es el peso de Hamming, está bien definida. Está función es una transformación lineal de C en $\mathbf{F}_2$, pues para $\bar{c}_1, \bar{c}_2 \in C$ la condición $\bar{c}_1 \cdot \bar{c}_2 = 0$ implica que estos vectores tienen un número par de entradas "1" en común. El núcleo de ϕ es el conjunto de vectores en C cuyo peso es congruente con 0 módulo 4. Este subespacio se denotará por $kerC$. Obviamente $kerC = C$ o $kerC$ es de codimensión 1 en C dependiendo si ϕ es la función cero o no lo es.

En lo que sigue se denotrá como $sop(\bar{x})$ el soporte del vector $\bar{x}$, es decir el conjunto de las posiciones coordenadas donde $\bar{x}$ tiene entradas no cero.

Proposición 6.5 *Sea C el código binario asociado a un 2-$(16, 6, 2)$ diseño, entonces C es auto-ortogonal y su dual tiene distancia mínima al menos igual a 4.*

Demostración: Que el código es auto-ortogonal es inmediato, pues dos bloques distintos en un 2-$(16, 6, 2)$ diseño tienen exactamente 2 puntos en común, como puede verificarse calculando MM^t, con M la matriz de incidencia del diseño (ver la demostración al teorema 6.2). Sea $\bar{v} \in C^{\perp}$ un vector arbitario en el código dual, y sea $p \in sop(\bar{v})$. Cada uno de los seis bloques incidentes con p cortan al soporte de v en un número par de puntos y por lo tanto al menos dos veces. Pero como cualesquiera dos puntos son incidentes con exactamente dos bloques se sigue que $\mid sop(\bar{v}) \mid -1 \geq 3$, y de ahí $\mid sop(\bar{v}) \mid \geq 4$, con esto concluye la prueba. □

Ya que el vector todo-uno, $\mathbf{1}$, está en $C^{\perp}$, ningún vector en $C^{\perp}$ tiene peso 14, pues de lo contrario su suma con el vector todo-uno tendría peso 2 lo cual contradice la proposición anterior.

Lema 6.1 *Sea S un conjunto de tres puntos de un 2-$(16, 6, 2)$ diseño y supóngase que B_1, B_2, B_3 son tres bloques distintos incidentes con exactamente dos puntos de S. Entonces la suma, módulo 2, de los vectores de incidencia de estos tres bloques tiene peso 6 ó 10. Además si S está contenido en un bloque C y el peso es 10 entonces el vector de peso 10 es el vector de inidencia del complemento de C.*

Demostración: La prueba al teorema 6.2 muestra que cualesquiera dos bloques del diseño tienen en común exactamente dos puntos, este hecho se utilizará en la presente demostración.

Sea x_i, $i = 0, 1, 2, 3$ el número de puntos no en S en exactamente i de los tres bloques B_1, B_2, B_3. Entonces

$$x_0 + x_1 + x_2 + x_3 = 13,$$

pues esta ecuación cuenta precisamente los puntos fuera de S. Si $x_3 \geq 3$ entonces existen al menos 2 puntos en tres bloques, lo cual contradice los parámetros del diseño, de ahí que $x_3 = 0$ ó 1. Si $x_3 = 0$, ya que cualesquiera dos bloques se cortan en exactamente $\lambda = 2$ puntos se sigue que $x_2 = 3$; pero $k = 6$ implica que cada bloque tiene 2 puntos en S, y 2 puntos en común con cada uno de los bloques por lo que $x_1 = 6$, y $x_0 = 4$. Supóngase ahora que $x_3 = 1$, repitiendo el razonamiento anterior se obtienen los valores $x_2 = 0$, $x_1 = 9$, $x_0 = 3$. Esto prueba la primera parte del lema.

Si $S \subset C$ y el peso es 10, los tres puntos fuera de los tres bloques es $C - S$ y el vector de peso 10 consiste de lo puntos no incidentes con C. □

Lema 6.2 *Si C es el código binario de un 2-(16, 6, 2) diseño entonces $\mathbf{1} \in C$.*

Lema 6.3 *Si C es el código binario de un 2-(16, 6, 2) diseño entonces C contiene al menos 30 vectores de peso 8.*

Demostración: Si A es un bloque entonces la suma módulo 2 de los vectores de incidencia de A y cualquier otro bloque es un vector de peso 8. Con esto se obtienen 15 vectores de peso 8, pero como $\mathbf{1} \in C$ se obtienen otros 15 vectores del mismo peso, por complementación. Para ver que estos vectores son distintos basta con notar que si B es un bloque distinto de A

$$| sop(v^A + v^B) \cap A | = 4, \text{ y } | sop(v^A + v^B + \mathbf{1}) \cap A | = 2. \square$$

Teorema 6.5 *Sea C el código binario de un 2-(16, 6, 2) diseño, entonces $6 \leq \dim(C) \leq 8$, además existe un único de tales diseños con $\dim(C) = 6$. Lo denotaremos por $\mathcal{B}_6$.*

Demostración: Ya que C es auto-ortogonal su dimensión es no mayor que 8. Por los dos lemas anteriores su dimensión es no menor que 6 (pues tiene

al menos 16 vectores de peso 6, 30 vectores de peso 8, 16 vectores de peso 10, uno por cada uno de peso 6, y además a los vectores cero y todo-uno). Si $\dim(C) = 6$ su distribución de peso queda determinado y el polinomio enumerador de peso de $kerC$ es $x^0 + 30x^8 + x^{16}$. Es sencillo verificar que tanto los códigos binarios de Hamming, y sus códigos extendidos son únicos, salvo equivalencias; y de ahí deducir que el único código con la distribución de peso anterior es el código de Reed-Muller $RM(1,4) = (\mathcal{H}_4)^{\perp}$. Denotemos por H el código dual de $kerC$, el polinomio enumerador de peso de este código es, por la ecuación de MacWilliams descrita en el teorema 2.9, pag. 25:

$$x^0 + 140x^4 + 448x^6 + 870x^8 + 448x^{10} + 140x^{12} + x^{16}.$$

Tómese cualquier vector de peso 6 de H, digamos $\bar{v}$, entonces $\mathbf{F}_2\bar{v} + H^{\perp}$ es un $[16,6]$ código binario. Ya que ningún vector de peso 8 en $H^{\perp}$ tiene su soporte ajeno de $sop(\bar{v})$ (pues ningún vector en H tiene peso 14), cada vector de peso 8 intersecta a $sop(\bar{v})$ en dos o cuatro puntos. Obviamente 15 cortan en 2 puntos y 15 en 4 puntos (pues si $\bar{u}$ corta en 4 entonce $\bar{u} + \mathbf{1}$ intersecta en 2), así se obtienen 15 vectores de peso 6 y 15 de peso 10. Por lo tanto $\mathbf{F}_2\bar{v} + H^{\perp}$ tiene al menos 16 vectores de peso 6, los 15 anteriores y $\bar{v}$, al menos 16 vectores de peso 10 y por el lema anterior, al menos 30 vectores de peso 8. Se tienen entonces todos los vectores de $\mathbf{F}_2\bar{v} + H^{\perp}$ y su polinomio enumerador de peso es

$$x^0 + 16x^6 + 30x^8 + 16x^{10} + x^{16}.$$

Ya que no existen vectores de peso 4 ó 12 los soportes de dos distintos vectores de peso 6 se intersectan exactamente en dos puntos. Se tiene entonces un 2-$(16,6,2)$ diseño y cualquiera de estos es obtenido de esta forma de H, pues el código de cualquiera de estos diseños contiene al código $H^{\perp}$. Ya que el grupo de automorfismos de H es transitivo en los vectores de peso 6 (probado por los autores de la referencia [7]), el 2-$(16,6.2)$ diseño de dimensión 6 es único. □

Corolario 6.4 *Los* 448 *vectores de peso* 6 *de* $ker(C)^{\perp}$ *generan naturalmente* 28, 2-$(16,6,2)$ *diseños isomorfos. Por lo tanto es posible construir explícitamente* 2-$(16,6,\lambda)$ *diseños para* $\lambda = 2i$, $i = 1,2\ldots,28$.

Si $A_6 = C_2(\mathcal{B}_6)$ entonces $H^{\perp} = kerA_6 \subset A_6 \subset A_6^{\perp} \subset H$.

Proposición 6.6 *Sea $\bar{v}$ un vector de peso 6 de $A_6^{\perp} - A_6$. El polinomio enumerador de pesos de $A_7 = A_6 + \mathbf{F}_2\bar{v}$ es*

$$x^0 + 4x^4 + 32x^6 + 54x^8 + 32x^{10} + 4x^{12} + x^{16}.$$

Demostración: Claramente A_7 es auto-ortogonal y de dimensión 7. Por otra parte $sop(\bar{v})$ no puede intersectar a cada uno de los 16 bloques de $\mathcal{B}_6$ exactamente dos veces, pues de lo contrario $t = \lambda = 2$ implicaría que los 15 distintos 2-subconjuntos de $sop(\bar{v})$ están en exactamente $15 \times 2 = 30$ bloques, lo cual es imposible. Entonces existe un vector $\bar{w} \in A_6$ de peso 6 cuyo soporte intersecta a $sop(\bar{v})$ en cero o cuatro puntos. Sea $\bar{b}$ el vector de peso 4 el cual es $\bar{w} + \bar{v}$ o su complemento.

Sea H el código definido en el corolario precedente. Por el teorema de Assmus-Mattson, teorema 4.4, los 30 vectores de peso 8 de $H^{\perp}$ sostienen un 3-$(16, 8, 3)$ diseño, de ahí que cualesquiera tres 1's de $\bar{b}$ determinan tres vectores de peso 8 de $H^{\perp}$, digamos $\bar{v}_1$, $\bar{v}_2$ y $\bar{v}_3$. Estos tres vectores deben tener prescisamente cuatro 1's en común y, además deben de ser precisamente los cuatro 1's correspondientes a $\bar{b}$, pues este vector es ortogonal a cada uno de los tres vectores. Se tienen entonces 4 vectores en A_7 de peso 4, a saber $\bar{b}$, $\bar{b} + \bar{v}_1$, $\bar{b} + \bar{v}_2$ y $\bar{b} + \bar{v}_3$, cuya suma es 1.

Ya que $ker A_7$ es de dimensión 6 y claremente es $\mathbf{F}_2\bar{b} + H^{\perp}$, los cuatro vectores de peso cuatro que encontramos son todos. El polinomio enumerador de pesos de $ker A_7$ resulta entonces:

$$x^0 + 4x^4 + 54x^8 + 4x^{12} + x^{16}.$$

De éste es sencillo calcular que A_7 tiene 54 vectores de peso 8. Además en A_7 existen al menos 32 vectores de peso 6, los 16 de A_6 y los 16 de $\mathbf{F}_2\bar{v} + H^{\perp}$, y por complementación también tiene al menos 32 vectores de peso 10; por lo tanto, todos los vectores de A_7 y su polinomio enumerador de pesos resulta como se enuncia en la proposición. □

Apéndice. Líneas de investigación

Una investigación futura puede estar dirigida hacia las siguientes cuestiones:

1.- Encontrar una relación entre los códigos binarios de Hamming, su código dual, los diseños $GP(r,1,2)$ y el simplejo asociado al código dual.

2.- Es bien conocido que si $0 < r < m$, entonces

$$RM(r,m) = RM(r,m-1) \bigoplus RM(r-1,m-1),$$

donde $\oplus$ denota la construcción $\mid \bar{u} \mid \bar{u} + \bar{v} \mid$, (cf. [45]). Generalizar este hecho al caso q-ario.

3.- Determinar completamente las bases para códigos asociados a geometrías finitas.

4.- Ya que los códigos generalizados agujerados de Reed-Muller son cíclicos encontrar, si existe, una relación ente su polinomio generador y la geometría finita cuyo código contienen.

5.- No parece existir en la literatura un trabajo profundo sobre los conjuntos diferencia y sus códigos, es más ni tan siquiera se han determinado todos los conjuntos diferencia. Puede hacerse investigación en esta dirección y en particular dirigida a determinar bajo que condiciones una matriz circulante es la matriz generadora para un código cíclico y el significado de esta condición en el conjunto diferencia correspondiente, cuando existe tal correspondencia.

6.- Hasta hace poco sólo se conocían los códigos de Reed-Muller y los códigos de Reed-Muller generalizados afines, esto es tales que la función *ev* evalúa ciertos polinomios sobre todos los puntos de una geometría afín. Fue A.B. Sörensen (cf. [50]) quien, en su tésis doctoral, definió los códigos proyectivos de Reed-Muller, en los cuales la función *ev* evalúa polinomios homogéneos sobre los puntos de una geometría proyectiva. Sin embargo aún no se ha estudiado la relación existente entre la geometría proyectiva y estos códigos, como se hizo para los códigos de Reed-Muller afines. Es más en la actualidad se está haciendo investigación sobre otros tipos de códigos de Reed-Muller, en los cuales la función *ev* sólo toma un subconjunto propio ya sea de una geometría afín o proyectiva con alguna propiedad particular, por ejemplo ser el conjunto solución de una ecuación.

REFERENCIAS

[1].-Anderson, I. *A first course in combinatorial mathematics.* Academic Press. 1989.

[2].-Artin, E. *Algèbre géométrique.* Gauthier-Villars, París. 1967.

[3].-Assmus, E.F. Jr., and Key, J.D. *Codes and finite geometries.* Technical report, INRIA 1993.

[4].-Assmus, E.F. Jr., and Key, J.D. *Designs and codes: An up date.* Preprint 1995.

[5].-Assmus, E.F. Jr., and Key, J.D. *Designs and their codes.* Cambridge Univerity Press. 1993.

[6].-Assmus, E.F. Jr., and Key, J.D. *Polynomial codes and finite geometries.* Preprint 1993.

[7].-Assmus, E.F. Jr., and Salwach, C.J. *The* $(16, 6, 2)$ *designs.* Internat. J. Math. Math. Sci., 2(1979) pags. 261-281.

[8].-Atiyah, M.F., and Macdonald, I.G. *Introducción al álgebra conmutativa.* Reverté, 1980.

[9].- Blake, I.F., and Mullin, R.C. *An introduction to algebraic and combinatorial coding theory.* Academic Press. 1976.

[10].-Bose, R.C., and Ray-Chaudhuri, D.K. *On a class of error correcting binary group codes.* Information and Control, 3 (1960) pags. 68-79.

[11].-Cameron, P.J., and Van Lint, J.H. *Graph theory, coding theory and block designs.* London Mathematical Society Lecture Note Series 19. 1975.

[12].-Coexter, H.S.M. *Projective Geometry.* Springer Verlag. Second edition. 1987.

[13].-Cohen, G., Dornstetter, J.L., and Godlewski, Ph. *Codes correcteurs d'erreurs. Une introduction au codage algébrique.* Masson. 1992.

[14].-Delsarte, P., and Goethals, J.-M., and MacWilliams, F.J. *On generalized Reed-Muller codes and their relatives.* Info. and control, 16 (1974), pags. 403-442.

[15].-Doyen, J., Hubaut, X., and Vandensavel, M. *Rank of incidence matrices of Steiner triple systems.* Math. Z. 1978 pags. 251-259.

[16].-Fano, G. *Sui postulati foundamentali delle geometria proiettiva in uno spazio a un numero qualunque di dimensioni.* Giorn. Mat. Battaglini 30 (1892) pags. 106-132.

[17].-Fraleigh, J.B. *Álgebra abstracta.* Addison-Wesley Iberoamericana. 1989.

[18].-Golay, M.J.E. *Notes on digital coding.* Proc. IRE 37, 1949, pag. 657.

[19].-Gorenstein, D.C., and Zierler, N. *A class of error-correcting codes in p^m symbols.* J. Soc. Indus. App. Math., 9 (1961), pags. 207-214.

[20].-Grimaldi, R.P. *Matemáticas discreta y combinatoria.* Addison-Wesley Iberoamericana. 1989.

[21].-Gruenberg, K.W., and Weir, A.J. *Linear geometry.* Springer-Verlag, GTM. 1977.

[22].-Hall, M. Jr. *Combinatorial theory.* John Wiley y Sons. 1986.

[23].-Hall, M. Jr. *Teoría de grupos.* Centro Regional de Ayuda Técnica. Agencia Para el Desarrollo Internacional (A.I.D.) México. 1969.

[24].-Hamming, R.W. *Error detecting and error correcting codes.* Bell System Tech. J. 29 (1950) pags. 147-160.

[25].-Harary, F. *Graph Theory.* Addison-Wesley. 1969.

[26].-Herstein, I.N., and Kaplanski, I. *Matters Mathematical.* Chelsea.1978.

[27].-Hussain, Q.M. *On the totality of the solutions for the symetrical incomplete block designs $\lambda = 2$, $k = 5$ or 6.* Sankhya. 7 (1945) pags. 204-208).

[28].-Hocquenghem, A. *Codes correcteurs d'erreurs.* Chiffers 2 (1959) pags. 147-156.

[29].-Kasami, T., Lin, S., and Peterson, W.W. *Generalized Reed-Muller codes.* Electron. Commun. Japan, 51-C (3) (1968) 96-104.

[30].-Key, J.D., and Sullivan, F.E. *Codes of Steiner triple and quadruple systems.* Designs, Codes and Cryptograhy, 3 (1993) pags. 117-125.

[31].-Lauchaud, G. *The parameters of proyective Reed-Muller codes.* Discrete Mathematics 81 (1990) pags. 217-221.

[32].-Lang, S. *Algebra.* Addison Wesley. 1993. Third Edition.

[33].-Massey, J.L.. Costello, D.J., and Justensen. J. *Polynomial weights and code constructions.* IEEE Trans. Info. Theory. 19 (1973) pags. 101-110.

[34].-MacWilliams, F.J., and Sloane, N.J. *The theory of error-correcting codes.* North-Holland. 1988.

[35].-McEliece. R.J. *Finite fields for computer scientists and engineers.* Klewer Academic Publishers. 1980.

[36].-Mitani. N. *On the transmission of numbers in a sequential computer, delivered at the National Convention of the Inst. of Elec. Engineers of Japan* (November. 1951).

[37].-Montgomery. D.C. *Design and analysis of experiments.* Dover, 1984.

[38].-Muller, D.E. *Application of Boolean algebra to swiching circuit design and error detection.* IEEE Trans. Computers, 3 (1954), pags. 6-12.

[39].-Prange, E. *Cyclic error-correcting codes in two symbols.* Tech. Note AFCRC-TN-57-103, Air Force Cambridge Research Center, Bedford, Mass, 1957.

[40].-Raghavârao, D. *Constructions and combinatorial problems in designs of experiments.* Dover, 1971.

[41].-Reed, I.S. *A class of multiple-error-correcting codes and the decoding scheme.* IEEE Trans. Info.Theory, 4 (1954), pags. 38-49.

[42].-Reed, I.S., and Solomon, G. *Polynomial codes over certain finite fields.* J. Soc. Indust. Appl. Math. (1960) pags. 300-304.

[43].-Rentería, C., and Tapia, H. *A class of binary codes associated with graphs.* Congressus Numeratium 76 (1990) pags. 231-242.

[44].-Rentería, C., and Tapia, H. *Reed-Muller codes: An ideal theory approach.* Preprint 1996.

[45].-Roman, S. *Coding and information theory.* Springer-Verlag (GTM). 1992.

[46].-Salwach, C.J. *Planes, biplanes, and their codes.* American Mathematical Monthly 88 (1981) pags. 106-125.

[47].-Shannon, C.E. *A mathematical theory of communication.* Bell System Tech. J. 27, (1948) pags. 379-423.

[48].-Slepian, D. *A note on two binary signaling alphabets.* IRE Trans. Information Theory, IT-2, (1956) pags. 84-86.

[49].-Singer, J. *A theorem in finite projective geometry and some applications to number theory.* Trans. Amer. Math. Soc. 43 (1938), pags. 377-385.

[50].-Sörensen, A.B. *Projective Reed-Muller Codes.* IEEE Trans. Inform. Theory, 37 (1991) pags. 1567-1576.

[51].-Van Lint, J.H. *Coding theory.* Lecture Notes in Mathematics, 19. Spinger-Verlag. 1973.

[52].-Veblen. O., and Bussey, W.H. *Finite projective geometries.* Trans. Amer. Math. Soc. 7 (1906) pags. 241-259.

[53].-Veblen. O., and Young, J.W. *Projective Geometry.* Ginn & Co., 2 vols., Boston, 1938.

[54].-Wilson, R.M. *An existence theory for pairwise balanced designs.* J. Comb. Theory, 13A (1972) pags. 220-273.

[55].- Wilson, R.M. *An existence theory for pairwise balanced designs: III-Proof of the existence conjetures.* J. Comb. Theory, 18A (1975) pags.

71-79.

[56].-Wilson, R.M. *The necessary conditions for t-designs are sufficient for something.* Utilitas Math., 4 (1973) pags. 207-215.

[57].-Wilson, R.M. *On the theory of t-designs.* Enumeration and design, edited by David M. Jackson and Scott A. Vanstone, Academic Press (1984) pags. 19-49.