Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas

El defecto en la teoría clásica de códigos lineales

Luis Alfonso Pinedo Sandoval

Trabajo presentado como requisito parcial para optar al título de Magíster en Matemáticas

Director: Prof. Dr. Ismael Gutiérrez Garcia

Barranquilla, Noviembre de 2013

Dedicatoria

A mi madre Lola Sandoval y a mi Guajira hermosa

Agradecimientos

Deseo expresar mis agradecimientos a todos los profesores del postgrado en Matemáticas de la Universidad del Norte por sus valiosas enseñanzas durante estos años. Especialmente al Prof. Dr. Ismael Gutiérrez García por las interesantes reuniones y discusiones a lo largo de este trabajo.

Introducción

En las últimas décadas el uso de la información y en particular el manejo seguro de la misma ocupa un punto central en las investigaciones relacionadas con aplicaciones del álgebra en la teoría de la información.

Dos aspectos importantes son el cifrado de la información para protegerla de intrusos y la detección y corrección de errores ocurridos durante la transmisión por ruido en el canal. El primero está asociado a la criptografía y el segundo a la teoría de códigos lineales sobre cuerpos finitos.

Los parámetros de un código lineal C sobre el cuerpo finito $\mathbb{F}_q$ están dados por $[n, k, d]$, donde n indica la longitud, k la dimensión y d la distancia mínima de C. En la construcción de códigos lineales las cotas para el número de elementos del código juegan un papel importante.

Uno de los problemas centrales de la teoría de códigos es encontrar *buenos* códigos para una longitud n dada. Es decir, se desea, por una parte, que este tenga una buena rata de información, o equivalentemente, que el número de codewords sea grande y por otro lado, resulta interesante poder detectar y corregir una gran cantidad de errores. Esto es, tener una distancia mínima grande. Estas exigencia claramente se contradicen mutuamente, ya que una gran cantidad de codewords implica una distancia mínima pequeña.

Una de las cotas superiores importantes en la teoría de códigos lineales es la cota de Singleton, la cual establece que $d \leq n - k + 1$. Un código C es denominado un MDS-*código*, si alcanza la cota de Singleton. Es decir, si $d = n - k + 1$. Este nombre se deriva de su sigla en ingles *Maximum Distance Separable*.

Lamentablemente, los parámetros de un MDS-código están muy limitados por el tamaño q del cuerpo. Por lo tanto, resulta de especial interés encontrar códigos que tengan la distancia mínima lo más cerca posible de la cota de Singleton. Son de particular interés los casi MDS-códigos, es decir, aquellos cuya distancia mínima dista una unidad de dicha cota. Esto es, códigos para los cuales $d = n - k$.

En general, la medida de la separación de la cota de Singleton se llama el defecto de un código. Este concepto fue presentado por A. Faldum y W. Willems en [2], y es el tema central de este trabajo. La tesis presente es de carácter monográfico. En ella se presentan múltiples detalles omitidos en los resultados del artículo citado, además una gran cantidad de ejemplos que permitan a los próximos estudiantes una lectura mas fácil de este tema.

Índice general

Capítulo 1

Preliminares

A lo largo del trabajo usamos la palabra *alfabeto* para denotar un conjunto K en el cual se toman los caracteres que conforman los codewords usados. En general nuestro alfabeto K está representado por el cuerpo finito $\mathbb{F}_q$ o por una extensión de éste, digamos $\mathbb{F}_{q^e}$.

1.1 Algunos conceptos y resultados básicos

1.1.1 Definición. Sea K un alfabeto de q elementos y $n \in \mathbb{N}$. Un subconjunto no vacío C de K^n se denomina un *código de bloque* ó simplemente un código de longitud n sobre el alfabeto K. Los elementos de C se denominarán *codewords*. Si $q = 2$ ó $q = 3$, entonces llamamos a C un *código binario* ó ternario respectivamente.

1.1.2 Definición. Sean K un cuerpo y $n \in \mathbb{N}$. Para $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in K^n$ definimos la *distancia de Hamming* d entre u y v de la siguiente manera

$$d(u, v) := |\{j | u_j \neq v_j, j = 1, \ldots, n\}|.$$

1.1.3 Definición. Sean C un código de longitud n sobre un alfabeto K.

(a) Si $|C| > 1$, entonces llamamos a

$$d(C) := \min\{d(c, c') | c, c' \in C,\ c \neq c'\}$$

la *distancia mínima* de C y si $|C| = 1$, entonces definimos $d(C) := 0$.

(b) Si $d(C) = d$ y $M = |C|$, entonces diremos que C es un (n, M, d) código sobre K. Llamamos a (n, M, d) los párametros de C.

1.1.4 Definición. Sea K un cuerpo finito y $n \in \mathbb{N}$. Un *código lineal* C es un subespacio vectorial del espacio K^n. Escribiremos para ello $C \leq K^n$.
Si $dim_K(C) = k$ y $d(C) = d$, entonces diremos que C es $[n, k]$-*código* ó más exactamente un $[n, k, d]$-*código* sobre K. Llamamos a $[n, k, d]$ los *parámetros* de C. Si $|K| = q$, entonces es usual decir que C es un $[n, k, d]_q$-código.

1.1.5 Definición. Sean K un cuerpo finito, $n \in \mathbb{N}$ y $C \subseteq K^n$.

(a) Para $x = (x_1, \ldots, x_n) \in K^n$ definimos

$$\mathrm{wt}(x) := d(x, 0) = |\{j | x_j \neq 0\}|$$

y lo llamamos el peso de x.

(b) Si $C \neq \{0\}$, entonces se define el peso mínimo de C, notado con $\mathrm{wt}(C)$, de la siguiente manera

$$\mathrm{wt}(C) := \min\{\mathrm{wt}(x) | 0 \neq x \in C\}$$

Para $C = \{0\}$ se define $\mathrm{wt}(C) = 0$.

(c) El *soporte* de $x = (x_1, \ldots, x_n) \in K^n$ se nota y define mediante

$$\mathrm{sop}(x) := \{j | x_j \neq 0\}$$

Para $U \subseteq K^n$ definimos además $\mathrm{sop}(U) := \cup_{u \in U} \mathrm{sop}(u)$. En particular $\mathrm{wt}(u) = |\mathrm{sop}(u)|$ y

$$\mathrm{sop}(U) = \{j \mid \exists u = (u_1, \ldots, u_n) \in U, \quad \text{con} \quad u_j \neq 0\}.$$

1.1.6 Teorema. Sea K un cuerpo finito $n \in \mathbb{N}$ y $C \leq K^n$. Entonces $d(C) = \mathrm{wt}(C)$.

Demostración. Supongamos que $C \neq \{0\}$.

$$\begin{aligned}
d(C) &= \min\{d(c, c') | c, c' \in C,\ c \neq c'\} \\
&= \min\{d(c - c, c' - c) | c, c' \in C,\ c \neq c'\} \\
&= \min\{d(0, c' - c) | c, c' \in C,\ c \neq c'\} \\
&= \min\left\{d(0, c'') | c'' \in C - \{0_c\}\right\} \\
&= \min\left\{wt(c'') | c'' \in C - \{0_c\}\right\} \\
&= \mathrm{wt}(C).
\end{aligned}$$

1.1.7 Definición. Sea C un $[n,k]$-código sobre un cuerpo finito K. Una matriz $G \in \mathrm{Mat}(k \times n, K)$ cuyas filas forman una base para C, se denomina *matriz generadora* de C.

1.1.8 Definición. Sea C un $[n,k]$-código sobre un cuerpo finito K, con $k < n$. Diremos que $H \in \mathrm{Mat}(n-k \times n, K)$ es una matriz de control para C, si:

$$C = \{u \in K^n | Hu^t = 0\}$$

1.1.9 Lema. Sea C un $[n,k]$-código sobre un cuerpo finito K. Entonces $G \in \mathrm{Mat}(k \times n, K)$ es una matriz generadora de C, si y sólo si

$$C = \{uG \mid u \in K^k\}.$$

Demostración. Note inicialmente que, si $u = (u_1, \ldots, u_k) \in K^k$ y

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in \mathrm{Mat}(k \times n, K),$$

entonces

$$uG = \sum_{j=1}^{k} u_j g_j \in K^n. \tag{1.1}$$

Supongamos inicialmente que G es una matriz generadora para C. Dado que cada $g_j \in C$, de (1.1) se sigue que $uG \in C$, para todo $u \in K^k$. Esto demuestra que $\{uG \mid u \in K^k\} \subseteq C$.

Por otro lado, si $c \in C$, entonces existen $c_1, \ldots, c_n \in K$ tales que

$$c = \sum_{j=1}^{k} c_j g_j.$$

En consecuencia de (1.1) se sigue que $c = uG$, con $u = (c_1, \ldots, c_k) \in K^k$. Esto demuestra que $C \subseteq \{uG \mid u \in K^k\}$ y se tiene la afirmación.

Recíprocamente, supongamos que $C = \{uG \mid u \in K^k\}$, con

$$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} \in \mathrm{Mat}(k \times n, K).$$

Sea $B = (e_j \mid j = 1, \ldots, k)$ la base canónica de K^k. Entonces para todo $j = 1, \ldots, k$ se verifica que

$$e_j G = g_j$$

y en consecuencia las filas de G pertenecen a C.

Nuevamente de (1.1) y de la hipótesis se sigue que, si $c \in C$, entonces existen $c_1, \ldots, c_n \in K$ tales que $c = \sum_{j=1}^{k} c_j g_j$. Es decir, $C = \langle g_1, \ldots, g_k \rangle$. Dado que $\dim_K C = k$, se sigue que $(g_1, \ldots, g_k)$ es una base para C y consecuentemente G es una matriz generadora para C. □

1.1.10 Teorema. Sea C un $[n, k]$-código sobre un cuerpo K, con $k > 1$ y $H \in \mathrm{Mat}(n-k \times n, K)$ una matriz de control para C. Definamos los siguientes conjuntos:

- $A(r)$ denota el conjunto de todos los $r \in \mathbb{N}$ para los cuales existen r columnas de H que son linealmente dependientes.
- $B(r)$ denota el conjunto de todos los $r \in \mathbb{N}$ tales que cualquier $r - 1$ columnas de H son linealmente independientes.

Entonces

$$d(C) = \mathrm{wt}(C) = \min_{1 \leq r \leq n} A(r) = \max_{1 \leq r \leq n} B(r).$$

Demostración. Sean $s_1, \ldots, s_n \in K^{n-k}$ las columnas de H. Dado que $\dim_K C = k > 1$, se sigue que $n > n - k$. Por lo tanto $\{s_1, \ldots, s_n\} \subseteq K^{n-k}$ es un conjunto linealmente dependiente.

Sea $1 \leq m \leq n$ minimal con respecto a la propiedad de existir m columnas de H linealmente dependientes, digamos $s_{i_1}, \ldots, s_{i_m}$, con $i_j \in \{1, \ldots, n\}$. Entonces existen $c_j \in K$ tales que

$$\sum_{j=1}^{n} c_j s_j = 0,$$

y $c_j \neq 0$ exactamente para $j \in \{i_1, \ldots, i_m\}$.

Si definimos $c = (c_1, \ldots, c_n)$, entonces se verifica que $Hc^t = 0$ y $\mathrm{wt}(c) = m$. En consecuencia $c \in C$ y $\mathrm{wt}(C) \leq m$.

Supongamos que existiese $0 \neq x \in C$ con $m' = \mathrm{wt}(x) < m$. Entonces se tendría que $Hx^t = 0$, lo cual implicaría la existencia de m' columnas de H linealmente dependiente, lo cual contradice la elección de m. Por lo tanto $\mathrm{wt}(C) = m$. Usando el teorema 1.1.6 se tiene la conclusión. □

1.1.11 Definición. Sean C un $[n,k]$-código sobre un cuerpo finito K, con $n \geq 2$ y $|K| = q$.

(a) Para $1 \leq i \leq n$. Definimos

$$\breve{C}(i) = \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \mid (c_1, \ldots, c_{i-1}, 0, c_{i+1}, \ldots, c_n) \in C\}$$

y lo llamamos la **reducción** de C en la i-ésima coordenada.

(b) Para $1 \leq i \leq n$. Definimos

$$\overset{\circ}{C}(i) = \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \mid \exists c_i \in K \ (c_1, \ldots, c_n) \in C\}$$

y lo llamamos la **perforación** de C en la i-ésima coordenada.

1.1.12 Ejemplos. Sea C el $[4,2,2]$-código binario dado por

$$C = \{0000, 1011, 0110, 1101\}.$$

Entonces

(1) $\overset{\circ}{C}(1) = \{000, 011, 110, 101\}$.

(2) $\overset{\circ}{C}(2) = \{000, 111, 010, 101\}$.

(3) $\breve{C}(1) = \{000, 110\}$.

(4) $\breve{C}(2) = \{000, 111\}$.

1.1.13 Teorema. Sean C un $[n,k,d]$-código sobre un cuerpo finito K, con $|K| = q$, $n \geq 2$ y $k \geq 1$. Entonces

(a) $\breve{C}(i)$ y $\overset{\circ}{C}(i)$ son códigos lineales de longitud $n-1$ y $\breve{C}(i) \subseteq \overset{\circ}{C}(i)$.

(b) $k - 1 \leq \dim_K \breve{C}(i) \leq \dim_K \overset{\circ}{C}(i) \leq k$.

(c) Si $\breve{C}(i) \neq \{0\}$, entonces $d(\breve{C}(i)) \geq d(\overset{\circ}{C}(i))$.

(d) $\dim_K \breve{C}(i) = k - 1$ si y solo si existe $(c_1, \ldots, c_n) \in C$, con $c_i \neq 0$.

(e) $\dim_K \overset{\circ}{C}(i) = k-1$ si y solo si existe $(0, \ldots, 0, c_i, 0 \ldots, 0) \in C$, con $c_i \neq 0$. En particular, si $d \geq 2$, entonces $\dim_K \overset{\circ}{C}(i) = k$.

(f) $\breve{C}(i) = \overset{\circ}{C}(i)$ si y solo si existe $(0, \ldots, 0, c_i, 0 \ldots, 0) \in C$, con $c_i \neq 0$ o para todo $(c_1, \ldots, c_n) \in C$, se verifica que $c_i = 0$.

(g) Si $\breve{C}(i) \neq \{0\}$, entonces $d(\breve{C}(i)) \geq d$.

(h) Si $\dim_K \overset{\circ}{C}(i) = k$, entonces $d - 1 \leq d(\overset{\circ}{C}(i)) \leq d$.

Demostración.

(a) Se sigue inmediatamente de la definición 1.1.11.

(b) De (a) se sigue que

$$\dim_K \breve{C}(i) \leq \dim_K \overset{\circ}{C}(i) \leq k.$$

Si $c_i = 0$, para todo $c = (c_1, \ldots, c_n) \in C$, entonces

$$\dim_K \breve{C}(i) = \dim_K \overset{\circ}{C}(i) = k.$$

Sea $v_1 = (c_1, \ldots, c_n) \in C$, con $c_i \neq 0$. Entonces existe una base para C que contiene a v_1, digamos $B = (v_1, \ldots, v_k)$. Además existen escalares $\lambda_2, \ldots, \lambda_k \in K$ tales que cada uno de los vectores

$$v_2 - \lambda_2 v_1, \ldots, v_k - \lambda_k v_1$$

tiene un cero en la i-ésima posición. Es claro que el conjunto

$$\{v_2 - \lambda_2 v_1, \ldots, v_k - \lambda_k v_1\}$$

es linealmente independiente. Por lo tanto

$$\dim_K \breve{C}(i) \geq k - 1.$$

(c) Se sigue de (a).

(d) Es claro que

$$\dim_K \breve{C}(i) = k - 1 \Leftrightarrow |\breve{C}(i)| = q^{k-1} < q^k = |C|.$$

Por lo tanto

$$\dim_K \breve{C}(i) = k - 1 \Leftrightarrow \exists\ (c_1, \ldots, c_n) \in C, \text{ con } c_i \neq 0.$$

(e) Consideremos la proyección sobre la i-ésima coordenada

$$\pi : C \longrightarrow \overset{\circ}{C}(i)$$

definida por

$$\pi(c_1, \ldots, c_n) := (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n).$$

Claramente π es un epimorfismo de espacios vectoriales y además

$$\ker(\pi) = C \cap \{(0, \ldots, 0, c_i, 0 \ldots, 0) \mid c_i \in K\}.$$

Del primer teorema de isomorfía para espacios vectoriales se sigue que

$$k - \dim_K \ker(\pi) = \dim_K C - \dim_K \ker(\pi) = \dim_K \overset{\circ}{C}(i).$$

Entonces

$$\begin{aligned} \dim_K \overset{\circ}{C}(i) = k - 1 &\Leftrightarrow \dim_K \ker(\pi) = 1 \\ &\Leftrightarrow \exists\ (0, \ldots, 0, c_i, 0 \ldots, 0) \in C, \text{ con } c_i \neq 0. \end{aligned}$$

Si en particular $d \geq 2$, entonces no existe $(0, \ldots, 0, c_i, 0 \ldots, 0) \in C$ con $c_i \neq 0$. Por lo tanto de (b) se sigue que $\dim_K \overset{\circ}{C}(i) = k$.

(f) Dado que $\breve{C}(i) \subseteq \overset{\circ}{C}(i)$, se tiene que

$$\begin{aligned} \breve{C}(i) = \overset{\circ}{C}(i) &\Leftrightarrow \dim_K \breve{C}(i) = \dim_K \overset{\circ}{C}(i) \\ &\Leftrightarrow \dim_K \breve{C}(i) = k \ \vee \ \dim_K \overset{\circ}{C}(i) = k - 1. \end{aligned}$$

El resto se sigue de (d) y (e).

(g) Sea $0 \neq c = (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \in \breve{C}(i)$ con $\mathrm{wt}(c) = d(\breve{C}(i))$. Entonces $c' = (c_1, \ldots, c_{i-1}, 0, c_{i+1}, \ldots, c_n) \in C$ y se tiene que

$$d \leq \mathrm{wt}(c') = \mathrm{wt}(c) = d(\breve{C}(i)).$$

(h) Supongamos que $\dim_K \overset{\circ}{C}(i) = k$ y sea $0 \neq c = (c_1, \ldots, c_n) \in C$ con $\mathrm{wt}(c) = d$. Si definimos $c' := (c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n)$, entonces $c' \in \overset{\circ}{C}(i)$ y $c' \neq 0$, ya que de lo contrario para la proyección π de (e) se

verificaría que $\ker(\pi) \neq \{0\}$, lo cual contradice el hecho que $\dim_K \overset{\circ}{C}(i) = k$. Entonces

$$d(\overset{\circ}{C}(i)) \leq \mathrm{wt}(c') \leq \mathrm{wt}(c) = d. \tag{1.2}$$

Por otro lado, sea $0 \neq x' = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in \overset{\circ}{C}(i)$ con $\mathrm{wt}(x') = d(\overset{\circ}{C}(i))$. Entonces dado que $\dim_K \overset{\circ}{C}(i) = k$ se tiene que existe

$$0 \neq x = (x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \in C$$

y se sigue que

$$d \leq \mathrm{wt}(x) \leq \mathrm{wt}(x') + 1 = d(\overset{\circ}{C}(i)) + 1. \tag{1.3}$$

De (1.2) y (1.3) se sigue la afirmación. □

1.2 Algunos códigos importantes

1.2.1 Los códigos de Hamming

Con ayuda de la definición de matriz de control presentamos a continuación una familia importante de códigos perfectos.

1.2.1 Teorema. Sea K un cuerpo finito, con $|K| = q$ y sean $k \in \mathbb{N}$ con $k \geq 2$ y $n = \frac{q^k - 1}{q-1}$. Entonces existe un $[n, n-k, 3]$-código perfecto sobre K, el cual llamamos **código de Hamming**.

Demostración. Todo vector no nulo $u \in K^k$ define una recta, que pasa por el vector cero. Es decir, define un subespacio vectorial de dimensión uno, generado por u. Esta recta está dada por

$$\langle u \rangle = \{ku \mid k \in K\}.$$

El espacio vectorial K^k tiene $q^k - 1$ vectores no nulos y dado un vector no nulo $u \in K^k$ existen $q - 1$ múltiplos escalares no nulos de u.
Dado que cualquier vector de la forma ku, con $k \in K^\times$ define la misma recta que u, se sigue que existen exactamente

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

rectas distintas en K^k.

Sean $\langle h_1\rangle, \ldots, \langle h_n\rangle$ estas rectas y sea $H \in \mathrm{Mat}(k \times n, K)$ la matriz cuyas columnas son precisamente los vectores h_j. Esto es, $H = (h_1 \cdots h_n)$.
El código C con matriz de control H, es decir,

$$C = \{c \in K^n \mid Hc^t = 0\},$$

se denomina un **código de Hamming**. Las columnas $h_1, \ldots, h_k$ puede elegirse de tal manera que $B = (h_1, \ldots, h_k)$ sea una base para K^k. Entonces $\mathrm{Rang}(H) = k$ y se tiene que $\dim(C) = n - k$. Es decir, $|C| = q^{n-k}$.
Por otro lado, cualquier par de columnas de H son linealmente independiente, pero de manera adecuada tres columnas resultan linealmente dependiente. Usando los teoremas 1.1.6 y 1.1.10 se sigue que $\mathrm{wt}(C) = d(C) = 3$.
Con esto podemos afirmar que C tiene los parámetros $[n, n-k, 3]$. En particular, se sigue que C puede corregir un error.
Demostramos ahora que C es un código perfecto. Para ello, note que

$$\sum_{j=0}^{1} \tbinom{n}{j}(q-1)^j = 1 + n(q-1) = 1 + \tfrac{q^k-1}{q-1}(q-1) = q^k.$$

Por lo tanto

$$\frac{q^n}{\sum_{j=0}^{1} \binom{n}{j}(q-1)^j} = \frac{q^n}{q^k} = q^{n-k} = |C|,$$

con lo cual se demuestra la perfección de C. □

En la construcción de C hemos elegido aleatoriamente, de un lado los representantes h_j en los subespacios vectoriales de dimensión uno y por otro lado, la ubicación de los h_j en la matriz H. Otras elecciones no suministran resultados esencialmente distintos, lo cual está asociado al concepto de **códigos equivalentes**. Esto nos permite hablar sin ambigüedades del $[\frac{q^k-1}{q-1}, n-k, 3]$-código de Hamming sobre K. En adelante usamos la notación $\mathrm{Ham}_q(k)$ para referirnos a este código.

1.2.2 Ejemplos. (a) Sean $q = 2$ y $k = 2$ Entonces tenemos el $[3, 1]$-código binario de Hamming. Una matriz de control H es

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

Además

$$C = \{000, 111\}.$$

(b) Sean $q = 2$ y $k = 3$. Entonces tenemos el $[7, 4]$-código binario de Hamming. Una matriz de control H es

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

(c) Sean $q = 2$ y $k = 4$. Entonces tenemos el $[15, 11]$-código de Hamming binario. La matriz de control H es por ejemplo

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

(d) Sean $q = 3$ y $k = 3$. Entonces tenemos el $[13, 10]$-código de Hamming ternario. Además

$$H = \begin{pmatrix} 1\,0\,0\,1\,2\,0\,0\,1\,2\,1\,2\,1\,1 \\ 0\,1\,0\,1\,1\,1\,2\,0\,0\,1\,1\,2\,1 \\ 0\,0\,1\,0\,0\,1\,1\,1\,1\,1\,1\,1\,2 \end{pmatrix}.$$

(e) Sean $q = 5$ y $k = 3$. Entonces tenemos el $[31, 26]$-código de Hamming sobre $\mathbb{F}_5$. Una matriz de control es

$$H = \begin{pmatrix} 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,2\,2\,2\,2\,2\,2\,3\,3\,3\,3\,3\,4\,4\,4\,4\,4 \\ 1\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4 \end{pmatrix}.$$

1.2.2 Los códigos de Reed - Solomon

Los códigos de Reed-Solomon fueron presentados en 1960 por I. S. Reed[1] y G. Solomon [2] en [8] siendo estos investigadores del Instituto Tecnológico de Massachussets. Estos códigos has sido utilizados en la codificación de información en los CD's, los DVD's y en los discos Blu-ray, así como en sistemas de comunicaciones DSL, WiMAX, DVB y ATSC. En la década de los ochenta las multinacionales Philips y Sony establecieron el CIRC (*Cross Interleaved Reed - Solomon Code*) como un estándar en la detección y corrección de errores en el sistema de audio para discos compactos.

[1] Irving S. Reed (Seattle, 1923 -). Matemático e ingeniero americano. Reed ha contribuido grandemente en el área de la ingeniería incluyendo radar, procesamiento digital de señales e imágenes.

[2] Gustave Solomon (Brooklyn, 1930 - California, 1996). Matemático e ingeniero americano coinventor de la teoría algebraica de la corrección de errores.

1.2.3 Definición. Sea K un cuerpo finito, digamos $|K| = q$. Sean $k, n \in \mathbb{N}$ con $1 \leq k \leq n \leq q$ y además

$$K[x]_k := \{f \in K[x] \mid \text{grad}(f) < k\}.$$

Es decir, $K[x]_k$ denota el conjunto de todos los polinomios con coeficientes en K con grado estrictamente menor que k.

Sea $A = \{a_1, \ldots, a_n\} \subseteq K$, con $a_i \neq a_j$ para $i \neq j$. Definamos

$$C(A) := \{(f(a_1), \ldots, f(a_n)) \mid f \in K[x]_k\} \subseteq K^n.$$

Se verifica sin dificultades que $C(A) \leq K^n$. Este subespacio se denomina **código de Reed - Solomon** o simplemente un RS-código.

Determinamos a continuación los parámetros de $C(A)$.

1.2.4 Teorema. Sean K un cuerpo finito, con $|K| = q$ y $1 \leq k \leq n \leq q$. Entonces $C(A)$ es un $[n, k, n-k+1]$-código sobre K.

Demostración. Claramente $C(A)$ tiene longitud n. Consideremos ahora la función

$$\alpha : K[x]_k \longrightarrow C(A)$$

definida por

$$\alpha(f) := (f(a_1), \ldots, f(a_n)).$$

Se verifica sin dificultades que α es un epimorfismo entre espacios vectoriales. Demostramos ahora que α es inyectiva, por lo tanto un isomorfismo. Si $f \in \ker(\alpha)$, entonces

$$\alpha(f) = (f(a_1), \ldots, f(a_n)) = (0, \ldots, 0).$$

Dado que $\text{grad}(f) < k \leq n$, se sigue que f tiene a lo mas $k-1$ raíces distintas. Por lo tanto la igualdad anterior se verifica si y solo si $f = 0$.
Es claro que $B = (1, x, \ldots, x^{k-1})$ es una base para $K[x]_k$. Por consiguiente

$$\dim_K K[x]_k = k = \dim_K C(A).$$

Para calcular $d(C(A))$, consideremos dos elementos cualesquiera de $C(A)$, digamos $c_f = (f(a_1), \ldots, f(a_n))$ y $c_g = (g(a_1), \ldots, g(a_n))$ y supongamos que $d(c_f, c_g) = t$. Entonces c_f y c_g coinciden en $n - t$ posiciones, por lo tanto el polinomio $f - g$ tiene $n - t$ raíces. Sabemos que $n - t \leq k - 1$. En consecuencia

$$n - k + 1 \leq t.$$

Esto significa que $n-k+1$ es una cota inferior del conjunto

$$\{d(c_f, c_g) \mid f, g \in K[x]_k\}.$$

Dado que $d(C(A))$ es la mayor cota inferior, se tiene que $n-k+1 \leq d(C(A))$. Para el polinomio

$$f = \prod_{j=1}^{k-1}(x - a_j)$$

se verifica que $\mathrm{wt}(c_f) = n-k+1$. Por lo tanto

$$d(C(A)) = n-k+1.$$

Con esto se concluye que $C(A)$ es un $[n, k, n-k+1]$-código sobre K.□
Los códigos de Reed - Solomon forman parte de los códigos mas importantes ya que

(a) Alcanzan la cota de Singleton y por lo tanto es posible detectar un mayor número de errores.

(b) Existen algoritmos rápidos de decodificación.

(c) Se utilizan en aplicaciones importantes como en el CD-*player*. En éstos se utilizan RS-códigos con parámetros $[32, 28, 5]$ o $[28, 24, 5]$ sobre el cuerpo finito $\mathbb{F}_{2^8}$.

1.2.5 Teorema. Sean K un cuerpo finito, con $|K| = q$, $A = \{a_1, \ldots, a_n\} \subseteq K$, con $a_i \neq a_j$ para $i \neq j$ y $1 \leq k \leq n \leq q$. Entonces la matriz generadora de un $[n, k]$-código de Reed - Solomon está dada por la matriz de Vandermonde

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}.$$

Demostración. Note que

$$\begin{aligned} c_f \in C(A) &\Leftrightarrow \exists f \in K[x]_k \text{ tal que } c_f = (f(a_1), \ldots, f(a_n)) \\ &\Leftrightarrow \exists c_0, \ldots, c_{k-1} \in K \text{ tales que } c_f = \Big(\sum_{j=0}^{k-1} c_j a_1^j, \ldots, \sum_{j=0}^{k-1} c_j a_n^j\Big) \\ &\Leftrightarrow c_f = (c_0, \ldots, c_{k-1})G \\ &\Leftrightarrow c_f \in K^k G. \end{aligned}$$

Usando el lema 1.1.9 se sigue la afirmación. □

1.2.6 Ejemplo. Sea C un $[3,2]$-código ternario de Reed - Solomon con $A = \{0,1,2\}$. Entonces

$$C(A) = \{(f(0), f(1), f(2)) \mid f \in K[x]_2\}.$$

Note que

$$K[x]_2 = \{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\}.$$

Por lo tanto

$$C(A) = \{000, 012, 021, 111, 120, 102, 222, 201, 210\}.$$

Note que $d(C(A)) = 2$.
Otra alternativa para la construcción es utilizar el teorema anterior. En este caso una matriz generadora para C esta dada por

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix},$$

y se tiene nuevamente que

$$C(A) = \mathbb{F}_3^2 G = \{000, 012, 021, 111, 120, 102, 222, 201, 210\}.$$

1.2.3 Los códigos binarios de Reed - Muller

1.2.7 Teorema. (Construcción de Plotkin) Para $j = 1, 2$ sean C_j dos $[n, k_j, d_j]$-códigos sobre un cuerpo finito K , con $|K| = q$. Entonces

$$C = C_1 \propto C_2 := \{(c_1, c_1 + c_2) \mid c_j \in C_j,\ j = 1, 2\} \subseteq K^{2n}$$

es un $[2n, k_1 + k_2, d]$-código sobre K, donde $d = \min\{2d_1, d_2\}$.

Demostración. Claramente C es un código de longitud $2n$ sobre K. Consideremos ahora la función $\varphi : C_1 \oplus C_2 \longrightarrow C$ definida por

$$\varphi(x_1, x_2) := (x_1, x_1 + x_2).$$

Se verifica sin dificultades que φ es isomorfismo entre espacios vectoriales. Entonces se tiene que

$$\dim_K C = \dim_K C_1 \oplus C_2 = k_1 + k_2.$$

Resta demostrar la afirmación sobre la distancia mínima. Si C es el espacio vectorial nulo, entonces $d_1 = d_2 = 0$. Supongamos entonces que $C \neq \{0\}$ y sea $0 \neq c = (c_1, c_1 + c_2) \in C$. Dado que $\mathrm{wt}(c_1) \geq |\mathrm{sop}(c_1) \cap \mathrm{sop}(c_2)|$ se sigue que

$$\begin{aligned} \mathrm{wt}(c) &= \mathrm{wt}(c_1) + \mathrm{wt}(c_1 + c_2) \\ &= \mathrm{wt}(c_1) + \mathrm{wt}(c_1) + \mathrm{wt}(c_2) - 2|\mathrm{sop}(c_1) \cap \mathrm{sop}(c_2)| \\ &\geq \mathrm{wt}(c_2). \end{aligned}$$

Si $c_2 \neq 0$, entonces dado que $\mathrm{wt}(c_2) \geq d_2$, se tiene que $\mathrm{wt}(c) \geq d_2$. Si $c_2 = 0$, entonces dado que $c \neq 0$, se tiene que $\mathrm{wt}(c) = 2\mathrm{wt}(c_1) \geq 2d_1$. En resumen se tiene

$$d \geq \min\{2d_1, d_2\}.$$

Con $c_1 = 0$ y c_2 con peso mínimo o lo contrario, se alcanza el mínimo. □

1.2.8 Ejemplo. Sean C_1 el $[7, 4, 3]$-código binario de Hamming y C_2 el $[7, 1, 7]$-código binario de repetición. Entonces

(*a*) $C_1 \propto C_2 = \{(c_1, c_1), (c_1, \overline{c}_1) \mid c_1 \in C_1\}$ es un $[14, 5, 7]$-código binario, donde $\overline{c}$ es el vector que resulta al intercambiar ceros y unos en c.

(*b*) $C_2 \propto C_1 := \{(0, \ldots, 0, c_1), (1, \ldots, 1, \overline{c}_1) \mid c_1 \in C_1\}$ es un $[14, 5, 3]$-código binario.

Presentamos ahora una extensión de la definición de los códigos de Reed - Solomon, en la cual se utilizan polinomios en m indeterminadas. Estos códigos se denominaron de códigos de Reed - Muller después que D. E. Muller[3] los descubriera y que I. S. Reed presentara un procedimiento de decodificación en la década de los cincuenta [6], [7].

1.2.9 Definición. Sean $K = \mathbb{F}_2$ y $r, m \in \mathbb{N}_0$, con $0 \leq r \leq m$. Definamos

$$\begin{aligned} \mathrm{RM}(0, m) &= [2^m, 1] - \text{código de repetición} \\ &= \{(0, \ldots, 0), (1, \ldots, 1)\}. \end{aligned}$$

$$\mathrm{RM}(m, m) = \mathbb{F}_2^{2^m}.$$

[3] D. E. Muller. (1924 - 2008) Matemático e informático Norteamericano. Desarrolló e introdujo el ahora estándar Lenguaje de Transferencia de Registros entre la comunidad informática mientras trabajaba en el Lincoln Laboratory del MIT.

Para $m \geq 2$ y $1 \leq r \leq m-1$ sea recursivamente

$$\mathrm{RM}(r,m) = RM(r,m-1) \propto \mathrm{RM}(r-1,m-1).$$

Llamamos a estos **códigos binarios de Reed-Muller** de orden r.

Note que en particular

$$\begin{aligned}\mathrm{RM}(0,0) &= \mathbb{F}_2\\ \mathrm{RM}(0,1) &= \{(0,0),(1,1)\}\\ \mathrm{RM}(1,1) &= \mathbb{F}_2^2.\end{aligned}$$

1.2.10 Teorema. Sean $r, m \in \mathbb{N}_0$, con $0 \leq r \leq m$. Entonces $\mathrm{RM}(r,m)$ es un $[2^m, \sum_{j=0}^{r}\binom{m}{j}, 2^{m-r}]$-código binario.

Demostración.

(a) Si $r = 0$ o $r = m$, entonces la longitud de $\mathrm{RM}(r,m) = 2^m$. Para el caso general se procede por inducción sobre $r+m$ y se tiene que la longitud de $\mathrm{RM}(r,m) = 2^{m-1} + 2^{m-1} = 2^m$.

(b) Para el cálculo de la dimensión tenemos:

$$\dim_K(\mathrm{RM}(0,m)) = 1 = \sum_{j=0}^{0}\tbinom{m}{j}$$

$$\dim_K(\mathrm{RM}(m,m)) = 2^m = \sum_{j=0}^{m}\tbinom{m}{j}$$

Para el caso general nuevamente se procede por inducción sobre $r+m$ y se tiene que

$$\begin{aligned}\dim_K(\mathrm{RM}(r,m)) &= \dim_K(\mathrm{RM}(r,m-1)) + \dim_K(\mathrm{RM}(r-1,m-1))\\ &= \sum_{j=0}^{r}\tbinom{m-1}{j} + \sum_{j=0}^{r-1}\tbinom{m-1}{j}\\ &= 1 + \sum_{j=0}^{r-1}\left(\tbinom{m-1}{j+1} + \tbinom{m-1}{j}\right)\\ &= 1 + \sum_{j=0}^{r-1}\tbinom{m}{j+1}\\ &= \sum_{j=0}^{r}\tbinom{m}{j}.\end{aligned}$$

(*c*) Si $r = 0$, entonces $d(\mathrm{RM}(0,m)) = 2^m = 2^{m-0}$ y si $r = m$, entonces $d(\mathrm{RM}(m,m)) = 1 = 2^{m-m}$. Para el caso general se procede por inducción y se tiene que

$$d(\mathrm{RM}(r,m)) = \min\{2 \cdot 2^{m-1-r}, 2^{(m-1)-(r-1)}\} = 2^{m-r},$$

con lo cual se completa la demostración. □

1.2.11 Ejemplo. Códigos binarios de Reed - Muller.

(*a*) $\mathrm{RM}(1,2)$ es un $[4,3,2]$-código binario. Note además que

$$\begin{aligned}\mathrm{RM}(1,2) &= \mathrm{RM}(1,1) \propto \mathrm{RM}(0,1)\\ &= \mathbb{F}_2^2 \propto \{00,11\}\\ &= \{0000,0011,1111,1100,0101,0110,1010,1001\}.\end{aligned}$$

(*b*) $\mathrm{RM}(1,3)$ es un $[8,4,4]$-código binario. Es claro que $|C| = 16$.

$$\begin{aligned}\mathrm{RM}(1,3) &= \mathrm{RM}(1,2) \propto \mathrm{RM}(0,2)\\ &= \mathrm{RM}(1,2) \propto \{0000,1111\}.\end{aligned}$$

(*c*) $\mathrm{RM}(1,4)$ es un $[16,5,8]$-código binario.

(*d*) $\mathrm{RM}(1,5)$ es un $[32,6,16]$-código binario. Este código fue utilizado por la expedición Mariner 6, 7 y 9 hacia marte entre los años 1969 - 1972 para enviar fotografías hacia la tierra. Los $2^6 = 64$ codewords corresponden a la claridad (escala de grises) de un punto de la imagen. Dado que la distancia mínima es 16, pueden ser corregidos hasta 7 errores en un codeword (de longitud 32).

1.3 La cota de Singleton y la cota de Griesmer

1.3.1 Teorema. (Cota de Singleton) Sea C un código de longitud n sobre un alfabeto K con $|K| = q$ y distancia mínima d. Entonces $d \leq n - \log_q |C| + 1$ o equivalentemente $|C| \leq q^{n-d+1}$

Demostración. Consideramos la función $f : K^n \to K^{n-d+1}$ definida por $f(x_1,\ldots,x_n) := (x_1,\ldots,x_{n-d+1})$. Dado que dos codewords distintos tienen distancia por lo menos d, se tiene que la restricción de f a C es inyectiva. En efecto, sean $x, y \in K^n$, digamos $x = (x_1,\ldots,x_n)$ y $y = (y_1,\ldots,y_n)$. Si $x \neq y$, entonces forzosamente $(x_1,\ldots,x_{n-d+1}) \neq (x_1^1,\ldots,x_{n-d+1}^1)$, ya que de

lo contrario se tendría que $d(x_1, x^1) \leq d-1$, lo cual es contradictorio.

Por lo tanto
$$|C| = |f(C)| \leq |K^{n-d+1}| = q^{n-d+1.}$$

En consecuencia $\log_q |C| \leq n-d+1$ y se tiene que $d \leq n - \log_q |C| + 1$. □

1.3.2 Definición. Sea C un código de longitud n sobre un alfabeto K, con $|K| = q$ y distancia mínima d. Diremos que C es un MDS-código, si C alcanza la cota de Singleton. Es decir, si $|C| = q^{n-d+1}$.

En el contexto de los códigos lineales, C es un MDS-código si y solo si $d = n-k+1$.

1.3.3 Teorema. (Cota de Griesmer) Sea C un $[n,k,d]$-código sobre el cuerpo K con q elementos. Entonces
$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$
donde $\lceil x \rceil$ denota el menor entero que es mayor o igual que el número real x.

Demostración. Ver [4, Theorem 3.2.2]. □

1.3.4 Teorema. Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$ con matriz de paridad H y matriz generadora G. Entonces C es un MDS-código si y solo si cada $n-k$ columnas de H son linealmente independiente.

Demostración. Ver [5, Theorem 1. Chapter 11]. □

1.3.5 Teorema. Si C es un MDS-código, entonces su código dual $C^{\perp}$ también lo es.

Demostración. H es una matriz generadora para $C^{\perp}$. Del teorema 1.3.4, unas $n-k$ columnas de H son linealmente independiente, así unicamente el codeword cero es cero en mas de $n-k$ coordenadas. Por consiguiente $C^{\perp}$ tiene distancia mínima por lo menos $k+1$. Es decir, tiene parámetros $[n, n-k, k+1]$, con lo que $C^{\perp}$ es un MDS-código.

1.4 Los teoremas de la dualidad e identidad de MacWilliams

1.4.1 Definición. Un *producto interior* sobre un espacio vectorial V es una función que asocia un número real $(u|v)$ a cada pareja $u = (u_1, \ldots, u_n)$ y $v = (v_1, \ldots, v_n)$

$$(u|v) = u_1v_1 + \cdots + u_nv_n = \sum_{i=1}^{n.} u_iv_i.$$

Si $(u|v) = 0$, entonces decimos que u y v son ortogonales.

1.4.2 Definición. Sea C un $[n, k]$-código sobre un cuerpo finito K.

(a) El *código dual* de C, notado con $C^{\perp}$, se define de la siguiente manera:

$$C^{\perp} := \{u \in K^n \mid (u|c) = 0, \forall c \in C\}.$$

(b) C se denomina auto-ortogonal, si $C \subseteq C^{\perp}$.

(c) C se denomina auto-dual, si $C = C^{\perp}$.

1.4.3 Teorema. Sea C un $[n, k]$-código sobre un cuerpo finito K, $|K| = q$. Entonces

(a) $C^{\perp}$ es un $[n, n-k]$-código sobre K.

(b) $(C^{\perp})^{\perp} = C$.

(c) G es una matriz generadora de C si y solo si G es una matriz de control de $C^{\perp}$.

(d) H es una matriz de control de C si y solo si H es una matriz generadora de $C^{\perp}$.

(e) Si $(I_k \mid A)$ es una matriz generadora de C (en forma estándar), entonces $(-A^t \mid I_{n-k})$ es una matriz generadora de $C^{\perp}$, por lo tanto una matriz de control de C.

(f) Si C es auto-dual, entonces $n = 2k$. En particular, todo código auto-dual tiene longitud par.

Demostración.

(a) Sea G una matriz generadora para C, cuyas filas están dadas por

$$f_j = (g_{j1}, \ldots, g_{jn}),\ j = 1, \ldots, k.$$

Entonces

$$\begin{aligned} x \in C^{\perp} &\Leftrightarrow (x|c) = 0, \text{ para todo } c \in C. \\ &\Leftrightarrow (x|v_j) = 0, \text{ para una base } B = (v_1, \ldots, v_k) \text{ de } C. \\ &\Leftrightarrow (x|f_j) = 0. \\ &\Leftrightarrow Gx^t = 0, \end{aligned}$$

con lo cual se demuestra que G es una matriz de control de C. Del álgebra lineal sabemos que

$$n = \text{Rang}(G) + \dim_K \ker(G).$$

Es decir,

$$n = \text{Rang}(G) + \dim_K C^{\perp}.$$

De donde se sigue que $\dim_K C^{\perp} = n - k$.

(b) Es claro que $C \subseteq (C^{\perp})^{\perp}$. En efecto, si $x \in C$ y $v \in C^{\perp}$, entonces $(x|v) = 0$. Por lo tanto $x \in (C^{\perp})^{\perp}$.

Por otro lado, de (a) se sigue que

$$\dim_K (C^{\perp})^{\perp} = n - (n - k) = k = \dim_K C.$$

Con lo cual se tiene la igualdad.

(c) En (a) se demostró que si G es una matriz generadora de C, entonces G es una matriz de control de $C^{\perp}$.

Recíprocamente, sea G una matriz de control de $C^{\perp}$. Dado que $C^{\perp}$ es un $[n, n-k]$-código sobre K, se verifica que toda matriz generadora de $C^{\perp}$ tiene $n - k$ filas. Por lo tanto cualquier matriz de control de $C^{\perp}$ tiene $n-(n-k) = k$ filas. Supongamos entonces que las filas de G están dadas por

$$f_j = (g_{j1}, \ldots, g_{jn}), \quad j = 1, \ldots, k.$$

Entonces $(y|f_j) = 0$, para todo $y \in C^{\perp}$ y todo $j = 1, \ldots, k$. Es decir, $f_j \in (C^{\perp})^{\perp} = C$, para todo $j = 1, \ldots, k$.

Dado que las filas de G son linealmente independientes y además

$$\dim_K C = n - (n - k) = k,$$

con k el número de filas de G, se tiene que G es una matriz generadora de C.

(d) Usando (b) y (c) tenemos:

H es una matriz generadora de $C^\perp$ si y solo si H es una matriz de control de $(C^\perp)^\perp = C$.

(e) Se verifica que

$$(-A^t \mid I_{n-k})(I_k \mid A)^t = (-A^t \mid I_{n-k})\begin{pmatrix} I_k \\ A^t \end{pmatrix} = -A^t I_k + I_{n-k}A^t = 0.$$

Se sigue entonces que $(-A^t \mid I_{n-k})$ es una matriz de control de C y consecuentemente una matriz generadora de $C^\perp$.

(f) Si C es auto-dual, entonces C y $C^\perp$ tienen la misma dimensión sobre K. Por lo tanto $n - k = k$ y se tiene la afirmación. □

El código Simplex

El código dual del código de Hamming se denomina *código simplex* y lo notamos con $\mathrm{Sim}_q(m)$

1.4.4 Lema. (a) Todo codeword no nulo de $\mathrm{Sim}_q(m)$ tiene peso q^{m-1}.

(b) $\mathrm{Sim}_q(m)$ es un $[\frac{q^m-1}{q-1}, m, q^{m-1}]$-código sobre $\mathbb{F}_q$.

Demostración. Sea H una matriz de control de $\mathrm{Ham}_q(m)$, con filas $f_1, \ldots, f_m$. Sea además $0 \neq c = (c_1, \ldots, c_n) \in \mathrm{Sim}_q(m)$. Dado que H es una matriz generadora de $\mathrm{Sim}_q(m)$ se tiene que $B = (f_1, \ldots, f_m)$ es una base para $\mathrm{Sim}_q(m)$. Por lo tanto

$$c = \sum_{j=1}^{m} a_j f_j = \sum_{j=1}^{m} a_j (f_{j1}, \ldots, f_{jn}), \quad a_j \in \mathbb{F}_q.$$

Sean $h_i := (f_{1i}, \ldots, f_{mi})^t$ la i-ésima columna de H, $a := (a_1, \ldots, a_m) \in \mathbb{F}_q^m$ y definamos el conjunto $U(a)$ de la siguiente manera:

$$U(a) := \left\{ (b_1, \ldots, b_m)^t \mid b_j \in \mathbb{F}_q, \ \sum_{j=1}^{m} a_j b_j = 0 \right\} \subseteq \mathbb{F}_q^m.$$

Se verifica inmediatamente que $U(a) = \langle a \rangle^\perp$. Por lo tanto

$$\dim_{\mathbb{F}_q} U(a) = \dim_{\mathbb{F}_q} \langle a \rangle^\perp = m - \dim_{\mathbb{F}_q} \langle a \rangle = m - 1.$$

En consecuencia $U(a)$ tiene $\frac{q^{m-1}-1}{q-1}$ columnas h_i de H. Note que

$$c_i = 0 \Leftrightarrow \sum_{j=1}^{m} a_j f_{ji} = 0 \Leftrightarrow (f_{1i}, \ldots, f_{mi})^t \in U(a).$$

Esto demuestra que en c ha y exactamente $\frac{q^{m-1}-1}{q-1}$ ceros. Entonces

$$\mathrm{wt}(c) = n - \frac{q^{m-1}-1}{q-1} = \frac{q^m-1}{q-1} - \frac{q^{m-1}-1}{q-1} = q^{m-1}.$$

El resto del lema es claro. □

1.4.5 Definición. Sea C un código de longitud n sobre un cuerpo finito K. Para $0 \leq j \leq n$ denotamos con A_j el número de codewords con peso j. Esto es:

$$A_j := |\{c \in C \mid \mathrm{wt}(c) = j\}|$$

Entonces, el polinomio definido por:

$$A(x) = \sum_{j=0}^{n} A_j x^j \in \mathbb{Z}[x]$$

se denomina polinomio enumerador de pesos de C, y el vector $(A_0, A_1, \ldots, A_n)$ se denomina *la distribución de pesos* de C.
El polinomio entero en dos variables dado por:

$$A(x,y) = x^n A\left(\frac{y}{x}\right) = \sum_{j=0}^{n} A_j x^{n-j} y^j \in \mathbb{Z}[x,y]$$

se denomina polinomio *enumerador de pesos homogéneo* de C.

1.4.6 Teorema. (Dualidad de MacWilliams) Sea C un código lineal $[n,k]$ sobre $K = F_q$ con el polinomio enumerador de pesos $A(z)$. Notemos con $A^{\perp}(z)$ el polinomio enumerador de pesos de $C^{\perp}$. Entonces

$$A^{\perp}(z) = \frac{1}{q^k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

Demostración. Ver [12, Theorem 3.2.2]. □

1.4.7 Ejemplos. (a) Si C es el $[7,4,3]$-código binario de *Hamming*, entonces el polinomio enumerador de pesos de C está dado por

$$A(z) = 1 + 7z^3 + 7z^4 + z^7.$$

(b) Sea C el $[7,3,4]$-código simplex. Entonces el polinomio enumerador de pesos de C está dado por

$$\begin{aligned} A^{\perp}(z) &= \frac{1}{q^k}(1+z)^n A\left(\frac{1-z}{1+z}\right) \\ &= \frac{1}{2^4}[(1+z)^7 + 7(1+z)^4(1-z)^3 + 7(1+z)^3(1-z)^4 + (1-z)^7] \\ &= 1 + 7z^4. \end{aligned}$$

1.4.8 Teorema. (Identidad de MacWilliams) Sea C un $[n,k]$- código sobre $\mathbb{F}_q$ con polinomio enumerador de pesos

$$A(z) = \sum_{i=0}^{n} A_i z^i.$$

Sea

$$A^{\perp}(z) = \sum_{i=0}^{n} A_i^{\perp} z^i$$

el polinomio enumerador de pesos de $C^{\perp}$. Entonces para todo $r = 0, \ldots, n$ se tiene la identidad

$$\sum_{i=0}^{n-r} \binom{n-i}{r} A_i = q^{k-r} \sum_{j=0}^{r} \binom{n-j}{r-j} A_j^{\perp}$$

Demostración. Si cambiamos C y $C^{\perp}$ en la dualidad de MacWilliams, entonces obtenemos:

$$\begin{aligned} A(\tfrac{1}{z}) &= q^{-(n-k)} \left(\frac{z+(q-1)}{z}\right)^n A^{\perp}\left(\frac{1-\frac{1}{z}}{1+\frac{(q-1)}{z}}\right) \\ &= q^{-(n-k)} \left(\frac{z+(q-1)}{z}\right)^n A^{\perp}\left(\frac{z-1}{z+q-1}\right) \end{aligned}$$

Entonces

$$z^n A(\tfrac{1}{z}) = q^{-(n-k)}(z+(q-1))^n A^{\perp}\left(\frac{z-1}{z+q-1}\right).$$

Utilizando el hecho que:

$$A(z) = \sum_{i=0}^{n} A_i z^i = \sum_{c \in C} z^{\mathrm{wt}(c)}$$

obtenemos:

$$\sum_{i=0}^{n} A_i z^{n-i} = q^{-(n-k)} \sum_{j=0}^{n} A_j^{\perp} (z+q-1)^{n-j} (z-1)^j.$$

Utilizando la fórmula de *Leibnitz* de la derivada n-ésima para z obtenemos:

$$\sum_{l=0}^{n-r} \binom{n-j}{r} r! z^{n-i-r} =$$

$$q^{-(n-k)} \sum_{j=0}^{n} A_{\perp}^{j} \sum_{l=0}^{n} \binom{r}{l} \binom{n-j}{l} l! (z+q-1)^{n-j-l} \binom{j}{r-l} (r-l)! (z-1)^{j-(r-l)}.$$

Si hacemos $z = 1$, y consideramos solo en el lado derecho de la ecuación para $j = r - l$, se obtiene:

$$\begin{aligned}
\sum_{i=0}^{n-r} A_i \binom{n-i}{r} &= \frac{1}{r!} q^{-(n-k)} \sum_{j=0}^{n} A_j^{\perp} \binom{r}{r-j} \binom{n-j}{r-j} (r-j)! q^{n-r} j! \\
&= \frac{1}{r!} q^{-(n-k)} \sum_{j=0}^{r} A_j^{\perp} \frac{r!}{(r-(r-j))!(r-j)!} (r-j)! j! \binom{n-j}{r-j} q^{n-r} \\
&= q^{-(n-k)} q^{n-r} \sum_{j=0}^{n} A_j^{\perp} \binom{n-j}{r-j} \\
&= q^{k-r} \sum_{j=0}^{r} A_j^{\perp} \binom{n-j}{r-j}. \quad \square
\end{aligned}$$

1.5 Los códigos de Golay

1.5.1 Los códigos binarios de Golay

1.5.1 Definición. Sea $r \in \mathbb{N}$. Un código C se denomina **r-divisible**, si para todo $c \in C$ se verifica que $r \mid \mathrm{wt}(c)$. En particular, si $2 \mid \mathrm{wt}(c)$, para todo $c \in C$, entonces C se denomina **par** y si $4 \mid \mathrm{wt}(c)$, para todo $c \in C$, entonces C se denomina **doblemente par**.

1.5.2 Lema. (Divisibilidad) Sea C un código binario auto-dual de longitud n. Entonces

(a) C es par.

(b) Si $4 \mid \mathrm{wt}(c)$, para todo c en una base de C, entonces C es un código doblemente par.

Demostración.

(a) Sea $c = (c_1, \ldots, c_n) \in C$. Dado que la característica de K es 2, se tiene que

$$0 = (c|c) = \sum_{j=1}^{k} c_j^2 = \sum_{c_j \neq 0} 1 = \mathrm{wt}(c) \cdot 1.$$

Por lo tanto C es par.

(b) Es suficiente demostrar que si $c, c' \in C$, $4 \mid \mathrm{wt}(c)$ y $4 \mid \mathrm{wt}(c')$, entonces $4 \mid \mathrm{wt}(c + c')$. Note inicialmente que

$$\mathrm{wt}(c + c') = \mathrm{wt}(c) + \mathrm{wt}(c') - 2\ |\mathrm{sop}(c) \cap \mathrm{sop}(c')| \tag{1.4}$$

De la auto-dualidad de C se sigue que

$$0 = (c|c') = \sum_{j=1}^{k} c_j c'_j = \sum_{c_j = c'_j} 1 = |\mathrm{sop}(c) \cap \mathrm{sop}(c')| \cdot 1.$$

Es decir, $2 \mid |\mathrm{sop}(c) \cap \mathrm{sop}(c')|$. Por lo tanto, si $4 \mid \mathrm{wt}(c)$ y $4 \mid \mathrm{wt}(c')$, usando (1.4) se sigue que $4 \mid \mathrm{wt}(c + c')$. □

1.5.3 Ejemplo. (**El** $[8, 4, 4]$**-código extendido de Hamming**) La matriz

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

es una matriz generadora de $\mathrm{Ham}_2(3)$. El código extensión de $\mathrm{Ham}_2(3)$, también llamado **código de Hamming extendido**, esta dado por

$$\widehat{C} = \left\{ (c_1, \ldots, c_8) \mid (c_1, \ldots, c_7) \in \mathrm{Ham}_2(3),\ \sum_{j=1}^{8} c_j = 0 \right\}$$

y tiene matriz generadora

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

Notemos sus filas con f_1, f_2, f_3, f_4.
Dado que $(f_i|f_j) = 0$, para todo $i, j = 1, \ldots, 4$, se sigue que $\widehat{C} \subseteq \widehat{C}^{\perp}$. Por otro lado,

$$4 = \dim_{\mathbb{F}_2} \widehat{C} \leq \dim_{\mathbb{F}_2} \widehat{C}^{\perp} = 8 - \dim_{\mathbb{F}_2} \widehat{C} = 4.$$

Por lo tanto $\widehat{C} = \widehat{C}^{\perp}$. Además las filas de $\widehat{G}$ tienen peso 4, por lo tanto del lema de divisibilidad se sigue que $\widehat{C}$ es un código 4-divisible. Por consiguiente sus parámetros son $[8, 4, 4]$.

1.5.4 Ejemplo. (Código binario extendido de Golay) Sea C_1 el código extendido de Hamming del ejemplo anterior y sea $C_2 \leq \mathbb{F}_2^8$ generado por la matriz

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

Note que G_2 se obtuvo a partir de $\widehat{G}$ mediante la permutación

$$(c_1, c_2, \ldots, c_7, c_8) \mapsto (c_7, c_6, \ldots, c_1, c_8).$$

Se verifica entonces que C_2 es también un $[8, 4, 4]$-código binario auto-dual. Se deja como ejercicio verificar que

$$C_1 \cap C_2 = \{(0, \ldots, 0), (1, \ldots, 1)\}. \tag{1.5}$$

Definamos ahora

$$C := \left\{(c_1 + c_2, c_1' + c_2, c_1 + c_1' + c_2) \mid c_1, c_1' \in C_1,\ c_2 \in C_2\right\} \leq \mathbb{F}_2^{24}.$$

Dado que los codewords

$$(c_1, 0, c_1), (0, c_1', c_1') \text{ y } (c_2, c_2, c_2) \tag{1.6}$$

contienen una base para C, se verifica que $\dim_{\mathbb{F}_2} C = 12$. Con base en lo anterior, se tiene que los vectores (1.6) son ortogonales dos a dos. Es decir, C

es un código binario, auto-dual con parámetros $[24, 12, d]$.

Demostramos a continuación que $d = 8$. Para ello note que los vectores (1.6) son todos 4-divisibles, por lo tanto del lema anterior se tiene que C es también 4-divisible. Demostramos entonces que C no admite un codeword de peso 4. Dado que para todo $x, y \in \mathbb{F}_2^8$ se verifica que

$$\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2|\mathrm{sop}(x) \cap \mathrm{sop}(y)|,$$

podemos afirmar que las componentes $c_1 + c_2$, $c_1' + c_2$ y $c_1 + c_1' + c_2$ en

$$0 \neq c = (c_1 + c_2, c_1' + c_2, c_1 + c_1' + c_2)$$

tiene un peso par.

Si las tres componentes son todas distintas de cero, entonces se tiene que $\mathrm{wt}(c) \geq 8$, ya que C es un código 4-divisible. Supongamos entonces que por lo menos una de las tres componentes es cero.
La condición (1.5) implica que $c_2 = (0, \ldots, 0)$ o $c_2 = (1, \ldots, 1)$. En ambos casos se sigue inmediatamente que $\mathrm{wt}(c) \geq 8$. Dado que C tiene codewords con peso 8, se sigue que C es un $[24, 12, 8]$-código auto-dual. Éste se llama el código binario extendido de Golay y se nota con G_{24}.

1.5.5 Ejemplo. (Código binario de Golay) Si en el código binario extendido de Golay C del ejemplo anterior perforamos en la última coordenada se tiene un nuevo código de longitud 23. De la construcción de C_1, C_2 y C de los ejemplos anteriores se sigue que este código tiene parámetros $[23, 12, 7]$, el cual notamos con G_{23} y lo llamamos **código binario de Golay**.
Se verifica que éste es perfecto. En efecto,

$$2^{23} = |\mathbb{F}_2|^{23} = |G_{23}| \sum_{j=0}^{3} \tbinom{23}{j} = 2^{12}(1 + \tbinom{23}{1} + \tbinom{23}{2} + \tbinom{23}{3}) = 2^{12} \cdot 2^{11}.$$

1.5.2 Los códigos ternarios de Golay

1.5.6 Definición. El código ternario de Golay G_{12} está definido por la matriz generadora

$$G = (I_6 \mid B) \in \mathrm{Mat}(6 \times 12, \mathbb{F}_3),$$

donde

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Perforando G_{12} en la última coordenada se obtiene el código de Golay ternario perforado $G_{11} = G_{12}^*$

1.5.7 Teorema. El código ternario de Golay G_{12} satisface las siguientes propiedades:

(a) G_{12} es auto-dual.

(b) B es simétrica y G_{12} está generado por la matriz $G = (B \mid I_6)$.

(c) G_{12} es un $[12, 6, 6]$-código ternario.

(d) El código G_{11} obtenido perforando G_{12} en la ultima coordenada tiene parámetros $[11, 6, 5]$ y es además perfecto.

Demostración.

(a) Sea G la matriz generadora de G_{12}. Entonces todo par de codewords en G_{12} son ortogonales. Así $G_{12} \subseteq G_{12}^{\perp}$, luego $\dim_{\mathbb{F}_3} G_{12} \leq \dim_{\mathbb{F}_3} G_{12}^{\perp}$.

Ahora

$$6 = \dim_{\mathbb{F}_3} G_{12} \leq \dim_{\mathbb{F}_3} G_{12} = 12 - 6 = 6.$$

Luego

$$\dim_{\mathbb{F}_3} G_{12} = \dim_{\mathbb{F}_3} G_{12}^{\perp},$$

con lo que $G_{12} = G_{12}^{\perp}$.

(b) Del hecho que $B^t = B$, y que $(I_6 \mid B)$ es una matriz generadora de G_{12}, se sigue que $(-B^t \mid I_{n-k})$ es una matriz generadora de $G_{12}^{\perp}$, por lo tanto una matriz de control para G_{12}. Como $G_{12} = G_{12}^{\perp}$ y $B^t = B$ entonces $(B \mid I_k)$.

(c) Sea $x = (i \mid d) \in G_{12}$, con $\mathrm{wt}(x) \leq 5$. Entonces $\mathrm{wt}(i) \leq 2$ ó $\mathrm{wt}(d) \leq 2$.

Sí $\mathrm{wt}(i) \leq 2$, entonces se tendría

$$\begin{aligned} x &= \lambda_1\,(1000000\; b_{11}\; b_{12} \cdots b_{16}) + \lambda_2\,(0100000\; b_{21}\; b_{22} \cdots b_{26}) + \cdots + \\ &\quad \lambda_6\,(0000001\; b_{61}\; b_{62} \cdots b_{66}). \end{aligned}$$

Es decir x sería combinación lineal de a lo más dos filas de G. Como el peso de las filas de G es 6, no puede ser proporcional a una de ellas, así que ó es la suma de dos de ellas, ó es la suma de una o mas 2 por la otra ó 2 por una mas 2 por la otra.

Note que cualquiera de estos casos no es posible.

Se procede de manera similar si $\mathrm{wt}(d) \leq 2$, considerando como matriz generadora $(-B \mid I_6)$.

(d) Demostramos que G_{11} es un código perfecto. En efecto, dado que G_{11} es un $[11, 6, 5]$-código ternario, de la cota de *Hamming* se sigue que

$$\begin{aligned}\sum_{i=0}^{2} \tbinom{11}{i}(3-1)^i &= 2^0\tbinom{11}{0} + 2\tbinom{11}{1} + 2^2\tbinom{11}{2} \\ &= 1 + 22 + 4 \cdot 5 \cdot 11 \\ &= 23 + 220 \\ &= 243 \\ &= 3^5,\end{aligned}$$

con lo cual se tiene la afirmación. □

Capítulo 2

El defecto de un código lineal

La definición del defecto de un código lineal C establece una medida de que tan lejos está C de ser un MDS-código. El defecto restringe los parámetros n, k y d de C, debido al tamaño q del cuerpo. Uno de los resultados importantes de esta sección muestra la relación que existe entre el defecto de un código C y el de su dual $C^{\perp}$.

Todos los códigos considerados se suponen definidos sobre el alfabeto $\mathbb{F}_q$. Si C es un código de longitud n sobre $\mathbb{F}_q$ y D es un subespacio de C, entonces decimos que D es un subcódigo de C y escribimos para denotarlo $D \leq C$.

2.1 La jerarquia de pesos de un código

Los resultados de esta sección fueron demostrados por V. wei en [11]. Se destaca por ejemplo una generalización de la cota de Singleton.

2.1.1 Definición. Sea C un $[n, k, d]$-código.

(a) Para $r \in \{1, \ldots k\}$ el r-ésimo peso generalizado de *Hamming* de C está definido por

$$d_r := d_r(C) := \min\{|\mathrm{sop}(D)| \mid D \text{ es un subcódigo } r\text{-dimensional de } C\},$$

donde como se definió antes,

$$\mathrm{sop}(D) = \{i \mid \exists\ (x_1, \ldots, x_n) \in D \text{ con } x_i \neq 0\}$$

es el soporte de D.

(b) La secuencia $d_1 \leq d_2 \leq \ldots \leq d_k$ se llama la jerarquía de pesos de C. Notamos que $d_1 = d$ es la distancia mínima de C. Además se verifica que $d_1 < d_2 < \ldots < d_k$.

2.1.2 Observación. Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$. Probamos que $d(C) = d_1(C)$.

$$d_1(C) = \min\{|\text{sop}(D)| \mid D \leq C, \text{ con } \dim(D) = 1\}$$

Si $D \leq C$ y $\dim(D) = 1$, entonces existe $y = (y_1, \ldots, y_n) \neq 0$ tal que

$$\begin{aligned} D &= \langle (y_1, \ldots, y_n) \rangle \\ &= \{\alpha(y_1, \ldots, y_n) \mid \alpha \in \mathbb{F}_q\} \\ &= \{(\alpha y_1, \ldots, \alpha y_n) \mid \alpha \in \mathbb{F}_q\}. \end{aligned}$$

Note que

$$\begin{aligned} \text{sop}(\langle y \rangle) &= \{i \in \{1, \ldots, n\} \mid \alpha\, y_i \neq 0\} \\ &= \{i \in \{1, \ldots, n\} \mid y_i \neq 0\} \\ &= \text{sop}(y). \end{aligned}$$

Además

$$\mathcal{D} := \{D \leq C \mid \dim(D) = 1\} = \{\langle y \rangle \mid 0 \neq y \in C\}.$$

Por otro lado,

$$\begin{aligned} \{|\text{sop}(D)| \mid D \in \mathcal{D}\} &= \{|\text{sop}(\langle y \rangle)| \mid y \in C\} \\ &= \{|\text{sop}(y)| \mid 0 \neq y \in C\}. \end{aligned}$$

Entonces

$$\min\{|\text{sop}(D)| \mid D \in \mathcal{D}\} = \{|\text{sop}(y)| \mid 0 \neq y \in C\}.$$

Por lo tanto,

$$d_1(C) = d(C),$$

con lo cual se tiene la afirmación. □

2.1.3 Teorema. (Monotonía de la jerarquía) Para un $[n, k]$-código lineal C con $k > 0$, tenemos.

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Demostración. Es claro que $d_{r-1}(C) \leq d_r(C)$. En consecuencia resta demostrar que la desigualdad es estricta. Sea D el subcódigo de C con las siguientes propiedades: $|\mathrm{sop}(D)| = d_r(C)$ y $\dim_{\mathbb{F}_q} D = r$.

Sea $i \in \mathrm{sop}(D)$ y $D_i := \{x \in D \mid x_i = 0\}$. Entonces

$$\dim_{\mathbb{F}_q} D_i = r - 1.$$

De la definición de peso generalizado de Hamming tenemos que

$$d_{r-1}(C) \leq |\mathrm{sop}(D_i)| \leq |\mathrm{sop}(D)| - 1 = d_r(C) - 1,$$

con lo cual se tiene el resultado. □

2.1.4 Teorema. (Cota de Singleton generalizada) Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$. Entonces $d_r \leq n - k + r$, para $1 \leq r \leq k$. Note que en el caso $r = 1$ se tiene la cota de Singleton.

Demostración. La prueba se sigue por inducción sobre $k - r$. Cuando $k - r = 0$, $d_r = d_k \leq n = n - k + r$ por el teorema de la monotonía.
Asumimos ahora que $d_r \leq n - k + r$ para algún $r \leq k$. Entonces por el mismo teorema se sigue que

$$d_{r-1} \leq d_r - 1 \leq n - k + (r - 1),$$

teniendo así el resultado. □

2.1.5 Lema. Sea C un $[n, k]$-código sobre $\mathbb{F}_q$. Para un entero positivo $s < n$, sea r el entero mas grande tal que C tiene una matriz generadora G de la forma

$$G = \begin{pmatrix} G_1 & 0 \\ G_2 & G_3 \end{pmatrix},$$

donde $G_1 \in \mathrm{Mat}(r \times s, \mathbb{F}_q)$ de rango r y $G_3 \in \mathrm{Mat}((k - r) \times (n - s), \mathbb{F}_q)$. Entonces C tiene una matriz de control de la forma

$$H = \begin{pmatrix} H_1 & H_2 \\ 0 & H_3 \end{pmatrix},$$

donde $H_1 \in \mathrm{Mat}((s - r) \times s, \mathbb{F}_q)$ de rango $s - r$ y $H_3 \in \mathrm{Mat}((n - k - s + r) \times (n - s), \mathbb{F}_q)$ es de rango $n - k - s + r$. Además, $n - k - s + r$ es la dimensión más grande de un subespacio de $C^{\perp}$ con soporte contenido en las últimas $n - s$ coordenadas.

Demostración. Ver [4, Lemma 7.10.3]. □

2.1.6 Teorema. (Dualidad de Wei) Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$. Entonces

$$\{d_r(C) \mid 1 \leq r \leq k\} = \{1, 2 \ldots, n\} \setminus \{n + 1 - d_r(C^\perp) \mid 1 \leq r \leq n - k\}.$$

Demostración. Sea $s = d_r(C^\perp)$, para algún $r \in \{1, \ldots, n - k\}$. Es suficiente demostrar que no existe t con $1 \leq t \leq k$ tal que $d_t(C) = n + 1 - s$.

Dado que $s = d_r(C^\perp)$, existe un conjunto de s coordenadas que soportan un subcódigo r-dimensional de $C^\perp$. Reordenamos las columnas de tal forma que éstas sean las primeras s coordenadas. Así $C^\perp$ tiene una matriz generadora de tamaño $(n - k) \times n$ y de la forma

$$H = \begin{pmatrix} H_1 & 0 \\ H_2 & H_3 \end{pmatrix},$$

donde $H_1 \in \mathrm{Mat}(r \times s, \mathbb{F}_q)$ de rango r.

Como $d_r(C^\perp) < d_{r+1}(C^\perp)$ por el teorema de la monotonía, ningun subcódigo más grande tiene soporte en éstas coordenadas. Aplicando el lema 2.1.5, con $C^\perp$ en lugar de C y $n - k$ en lugar de k, se tiene que existe un subcódigo de C con dimensión $(k - s + r)$, el cual es cero en las primeras s coordenadas.

Por consiguiente

$$d_{k-s+r}(C) \leq n - s. \tag{2.1}$$

Si asumimos que no existe un t con $d_t(C) = n + 1 - s$, entonces de (2.1) se sigue que

$$t > k - s + r. \tag{2.2}$$

Reemplazando C por un código equivalente por permutación, sí fuese necesario, se sigue que C tiene una matriz generadora de la forma

$$G = \begin{pmatrix} G_1 & 0 \\ G_2 & G_3 \end{pmatrix},$$

donde $G_1 \in \mathrm{Mat}(t \times (n + 1 - s), \mathbb{F}_q)$ de rango t.

Por otra parte, como $d_t(C) < d_{t+1}(C)$ podemos aplicar el lema 2.1.5 con t en lugar de r y $n + 1 - s$ en lugar de s. En consecuencia existe un subcódigo de $C^\perp$ con dimensión $(s - 1 - k + t)$, el cual es cero en las primeras $n + 1 - s$ posiciones. Dado que $s = d_r(C^\perp)$, tenemos que $s - 1 - k + t < r$, lo cual contradice (2.2). □

En lo que sigue se establecen resultados sobre la jerarquía de pesos de los códigos especiales considerados en el primer capítulo.

2.1.7 Teorema. (Código de Reed-Muller) Sea C un código binario de Reed-Muller de orden 1. Es decir, C tiene longitud 2^m y dimensión $m+1$. Entonces para $1 \leq r \leq m$ se verifica que

$$d_r(C) = 2^{m-1} + 2^{m-2} + \cdots + 2^{m-r},$$

y $d_{m+1}(C) = 2^m$.

Demostración. Del teorema 1.2.10 se sigue que $d(C) = d_1 = 2^{m-1}$. Sea D un subcódigo con dimensión r y soporte $d_r(C)$. Por la cota de Griesmer

$$d_r(C) = |\mathrm{sop}(D)| \geq \sum_{i=0}^{r-1} 2^{m-1-i}.$$

Por otro lado, no es difícil construir un subcódigo de dimensión r con éste soporte. Por ejemplo, tomando cualesquiera r filas (no todas llenas de 1) es una matriz generadora en forma estandar. □

2.1.8 Corolario (Código Simplex) Sea C un código binario Simplex de longitud $2^m - 1$ y dimensión m. Entonces para $1 \leq r \leq m$ se verifica que

$$d_r(C) = 2^{m-1} + 2^{m-2} + \cdots + 2^{m-r}.$$

Demostración. Es conocido que el código Simplex es el subcódigo de un código de Reed-Muller de orden 1, sin el vector lleno de unos. Por consiguiente no es difícil demostrar que los pesos generalizados para los dos códigos son iguales, excepto aquel código Simplex no tiene el último peso de el código de Reed-Muller. □

2.1.9 Corolario (Código de Hamming) Sea C un código binario de Hamming de longitud $n = 2^m - 1$ y dimensión $k = 2^m - m - 1$. Entonces

$$\{d_r(C) \mid 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{2^i \mid 0 \leq i < m\}.$$

Demostración. Se sigue inmediatamente de los dos corolarios anteriores y del teorema de la dualidad de Wei. □

2.1.10 Ejemplos. (a) Código binario de Reed-Muller.
Sea C el RM$(1,3)$. Entonces C es un $[8,4,4]$-código binario, con $m = 3$. Por lo tanto del teorema 2.1.7 se sigue que

$$\begin{aligned} d_1(C) &= 4 \\ d_2(C) &= 2^2 + 2^1 = 6 \\ d_3(C) &= 2^2 + 2^1 + 1 = 7 \\ d_4(C) &= 2^3 = 8. \end{aligned}$$

(b) Código Simplex.
Sea C el $[7, 3, 4]$-código binario Simplex. Entonces $m = 3$ y por el corolario 2.1.8 la jerarquía de pesos para C está dada por

$$\begin{aligned} d_1(C) &= 4 \\ d_2(C) &= 2^3 + 2^2 = 12 \\ d_3(C) &= 2^3 + 2^2 + 2^1 = 14. \end{aligned}$$

(c) Código binario de Hamming.
Sea C el $[7, 4, 3]$-código binario de Hamming. Entonces $m = 3$ y $k = 4$ y por el corolario 2.1.9 la jerarquía de pesos para C está dada por

$$\begin{aligned} \{d_1(C), d_2(C), d_3(C), d_4(C)\} &= \{1, 2, \ldots, 7\} \setminus \{2^0, 2^1, 2^2\} \\ &= \{1, 2, \ldots, 7\} \setminus \{1, 2, 4\} \\ &= \{3, 5, 6, 7\}. \end{aligned}$$

(d) Código binario de Golay.
Sea C el $[24, 12]$-código binario de Golay. Entonces C tiene jerarquía de pesos

$$\{8, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 24\}.$$

En efecto, es conocido que C es auto-dual y que su distancia mínima es $d_1 = 8$. Entonces por la cota de Griesmer $d_2 \geq 12$. Por el teorema de la dualidad de Wei el conjunto

$$\{14, 15, 16, 18, 19, 20, 21, 22, 23, 24\}$$

es un subcojunto de la jerarquía de pesos. Puesto que el código tiene solamente codewords de pesos $0, 8, 12, 16$ y 24. esto trae como consecuencia que $d_2 \neq 13$ y $d_2 = 12$. Completando así la jerarquía de pesos. □

2.1.11 Ejemplos. [Dualidad de Wei]

(a) Sea C el $[15, 11]$-código de Hamming. Calculemos inicialmente la jerarquía de pesos del código Simplex de dimensión m. Entonces $d_r(C^\perp) = 2^{m-1} + 2^{m-2} + \cdots + 2^{m-r}$ para $1 \leq r \leq m$.
Para $m = 4$. Tenemos

$$\begin{aligned} d_1(C^\perp) &= 2^{m-1} = 2^3 = 8 \\ d_2(C^\perp) &= 2^{m-1} + 2^{m-2} = 2^3 + 2^2 = 12 \\ d_3(C^\perp) &= 2^{m-1} + 2^{m-2} + 2^{m-3} = 2^3 + 2^2 + 2 = 14 \\ d_4(C^\perp) &= 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{m-4} = 2^3 + 2^2 + 2 + 2^0 = 15 \end{aligned}$$

Entonces $d_r(C^\perp) = \{8, 12, 14, 15\}$. Ahora la jerarquía de pesos de C está dada por

$$\begin{aligned}
\{d_r(C) : 1 \leq r \leq 11\} &= \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \leq r \leq n - k\} \\
\{d_r(C) : 1 \leq r \leq 11\} &= \{1, 2, \ldots, 15\} \setminus \{1, 2, 4, 8\} \\
\{d_r(C) : 1 \leq r \leq 11\} &= \{3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15\}
\end{aligned}$$

(b) Sea C el $[31, 26, 3]$-código de Hamming sobre $\mathbb{F}_5$. Entonces

$$\begin{aligned}
d_1(C^\perp) &= 2^{m-1} = 2^4 = 16 \\
d_2(C^\perp) &= 2^{m-1} + 2^{m-2} = 2^4 + 2^3 = 16 + 8 = 24 \\
d_3(C^\perp) &= 2^{m-1} + 2^{m-2} + 2^{m-3} = 2^4 + 2^3 + 2^2 = 28 \\
d_4(C^\perp) &= 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{m-4} = 2^4 + 2^3 + 2^2 + 2^1 = 30 \\
d_5(C^\perp) &= 2^{m-1} + 2^{m-2} + 2^{m-3} + 2^{m-4} + 2^{m-5} = 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 31
\end{aligned}$$

Entonces $d_r(C^\perp) = \{16, 24, 28, 30, 31\}$

$$\begin{aligned}
\{d_r(C) : 1 \leq r \leq 26\} &= \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r(C^\perp) : 1 \leq r \leq n - k\} \\
\{d_r(C) : 1 \leq r \leq 26\} &= \{1, 2, \ldots, 31\} \setminus \{1, 2, 4, 8, 16\} \\
\{d_r(C) : 1 \leq r \leq 26\} &= \{3, 5, 6, 7, 9, 10, 11 \ldots, 30, 31\}
\end{aligned}$$

2.2 El defecto de un código

2.2.1 Definición. Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$.

(a) $def(C) := n + 1 - k - d$ es llamado el defecto de C.

(b) Decimos que C es un $A^s MDS$ código, si $s = def(C)$.

2.2.2 Definición. Un código C de defecto 1 se denomina un casi MDS-código, y un $A^o MDS$-código es un MDS-código. Es decir, un código de defecto 0.

2.2.3 Ejemplos. [Defectos de códigos]

(a) Sea C el $[7, 4, 3]$-código binario de *Hamming*. Entonces

$$\begin{aligned}
\text{def}(C) &= s = n - k + 1 - d \\
\text{def}(C) &= 7 - 4 + 1 - 3 \\
\text{def}(C) &= 1.
\end{aligned}$$

Luego C es un casi MDS-código.

(b) Sea C el $[7,3,4]$-código binario Simplex. Entonces $def(C) = s = 1$. Entonces C es un casi MDS-código.

(c) Sea C el $[5,2,2]$-código binario dado por $C = \{11111, 11000, 00111, 00000\}$. Entonces

$$\text{def}(C) = n - k + 1 - d = 2.$$

(d) El $[3,2,2]$-código ternario de Reed-Solomon C tiene defecto dado por $def(C) = n - k + 1 - d = 0$. Es decir, C es un MDS-código.

2.2.4 Lema. Sea C un $[n,k,d]$-A^sMDS código sobre $\mathbb{F}_q$. Entonces tenemos:

(a) Si $k \geq 2$, entonces $d \leq q(s+1)$.

(b) Si $k \geq 3$ y $d = q(s+1)$, entonces $s+1 \leq q$

Demostración.

(a) Supongamos que $d > q(s+1)$, entonces por la cota de Griesmer tenemos

$$\begin{aligned} n &\geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \\ &= \left\lceil \frac{d}{q^0} \right\rceil + \left\lceil \frac{d}{q} \right\rceil + \left\lceil \frac{d}{q^2} \right\rceil + \left\lceil \frac{d}{q^3} \right\rceil + \cdots + \left\lceil \frac{d}{q^{k-1}} \right\rceil \\ &= d + \left\lceil \frac{d}{q} \right\rceil + \sum_{i=1}^{k-2} \left\lceil \frac{d}{q^{i+1}} \right\rceil \\ &\geq d + s + 2 + k - 2 = \\ &= n + 1 - k - s + s + 2 + k - 2 \\ &= n + 1, \end{aligned}$$

lo cual es una contradicción.

(b) Si $k \geq 3$ y $d = q(s+1)$, entonces

$$d + k + s - 1 = n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = d + \left\lceil \frac{d}{q} \right\rceil + \left\lceil \frac{d}{q^2} \right\rceil + \cdots + \left\lceil \frac{d}{q^{k-1}} \right\rceil.$$

En consecuencia

$$d + k + s - 1 \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = d + s + 1 + \left\lceil \frac{s+1}{q} \right\rceil + \sum_{i=1}^{k-3} \left\lceil \frac{d}{q^{i+2}} \right\rceil.$$

Por lo tanto

$$\begin{aligned} d+k+s-1 &\geq d+s+1+\left\lceil \frac{s+1}{q} \right\rceil + k - 3 \\ -1 &\geq \left\lceil \frac{s+1}{q} \right\rceil - 2 \\ -1+2 &\geq \frac{s+1}{q} \\ 1 &\geq \frac{s+1}{q} \\ s+1 &\leq q. \qquad \square \end{aligned}$$

2.2.5 Proposición. Sea C un $[n,k,d]$-código. Sea $d_1 < d_2 < \ldots < d_k$ es la jerarquía de peso de C, entonces $C^{\perp}$ tiene defecto

$$s(C^{\perp}) = \min\{s \mid s \in \mathbb{N}, d_j = n-k+j,\ \forall j \geq s\} - 1.$$

Es decir, si $r_0 := \min\{s \mid s \in \mathbb{N}, d_j = n-k+j,\ \forall j \geq s\} - 1$, entonces $C^{\perp}$ es un código $A^{r_0}MDS$.

Demostración. Definamos

$$r_0 := \min\{s \in \mathbb{N} \mid d_j = n-k+j, \quad \forall j \geq s\} - 1.$$

Sea $\{d_1^{\perp}, \ldots, d_{n-k}^{\perp}\}$ la jerarquía de pesos de $C^{\perp}$. Entonces del teorema de la dualidad de Wei se tiene que

$$\{d_1^{\perp}, \ldots, d_{n-k}^{\perp}\} = \{1, \ldots, n\} \setminus \{n+1-d_j \mid j = 1, \ldots, k\},$$

de la definición de r_0 se sigue que $d_1^{\perp} = n+1-(n-k+r_0) = k+1-r_0$.

Por otro lado, de la definición de defecto se tiene que $d_1^{\perp} = n-(n-k)+1-s(C^{\perp}) = k+1-s(C^{\perp})$. Luego $s(C^{\perp}) = r_0$. Por consiguiente $C^{\perp}$ es un $A^{r_0}MDS$ código. $\square$

2.2.6 Corolario Sea C un $[n,k,d]$-código con $\text{def}(C) \geq 1$. Entonces $C^{\perp}$ es un casi MDS-código si y solo si $d_2 = d + \text{def}(C) + 1$.

Demostración. Sea $C^{\perp}$ un casi MDS-código, entonces por la proposición anterior

$$s(C^{\perp}) = \min\{s | s \in \mathbb{N},\ d_j = n-k+j, \text{ para todo } j \geq s\} - 1.$$

En particular $d_2 = n - k + 2$, por definición de defecto

$$d_2 = n - k + 2 = d + \text{def}(C) + 1.$$

Reciprocamente, si

$$d_2 = d + \text{def}(C) + 1 = n - k + 2,$$

entonces $d_i = n - k + i$ para todo $i \in \{2, \ldots, k\}$. La proposición 2.2.5, quiere decir que el defecto de $C^\perp$ es menor ó igual a 1.

Como $\text{def}(C) \geq 1$, entonces C no es un MDS-código, con lo que $C^\perp$ no es un MDS-código. Por consiguiente el $\text{def}(C^\perp)$ es 1, entonces $C^\perp$ es un casi MDS-código. □

2.2.7 Corolario Sea C un $[n, k, d]$-casi MDS-código. Entonces $C^\perp$ es un casi MDS-código si y solo si $d_2 = d + 2$.

Demostración. Si C es un casi MDS-código, entonces $\text{def}(C) = 1$. Del corolario anterior, $C^\perp$ es un casi MDS-código si y solo si

$$d_2 = d + \text{def}(C) + 1 = d + 1 + 1 = d + 2.$$

En consecuencia $d_2 = d + 2$. □

2.2.8 Teorema. Sea C un $[n, k, d]$-A^sMDS código sobre $\mathbb{F}_q$ con $s \geq 1$. Si $d > qs$, entonces $C^\perp$ es un casi MDS-código.

Demostración. De la cota generalizada de Singleton

$$\begin{aligned} d_2 \leq n - (k - 2) &= n - k + 2 \\ &= n - k + 1 + 1 \\ &= d + s + 1. \end{aligned}$$

Supongamos que $d_2 \leq d + s$. Sea D un subcódigo de C con $d_2 = |\text{sop}(D)|$. Entonces D es un $[|\text{sop}(D)|, 2, d^*]$-código con $d^* \geq d$, y

$$\text{def}(D) = |\text{sop}(D)| + 1 - 2 - d^* \leq d + s - 1 - d = s - 1.$$

Por el lema 2.2.4,

$$d^* \leq q((s - 1) + 1) \leq qs,$$

luego $d^* \leq qs$; contradiciendo la condición $d > qs$. Esto prueba que

$$d_2 = d + s + 1 = d + \text{def}(C) + 1,$$

por el corolario 2.2.6 $C^\perp$ es un casi MDS-código. □

2.2.9 Corolario Sea C un $[n,k,d]$-A^sMDS código sobre $\mathbb{F}_q$. Supóngase $k \geq 2$ y $d > qs$. Entonces

(a) $n \leq d + 2q$ para $s = 1$ y

(b) $k \leq q,\ n \leq (q+1)(s+2) - 3$ para $s \geq 2$.

Demostración.

(a) Sea $s \geq 1$, por el teorema 2.2.8, $C^{\perp}$ es un casi MDS-código, es decir $s^{\perp} = 1$. Supongamos que $s = 1$, entonces $1 = \text{def}(C) = n - k + 1 - d$ luego, $n - k = d > q \geq 2$ con lo que $d^{\perp} \leq 2q$, por tanto $k \leq 2q$. Concluimos que $n = k + d + s - 1 \leq 2q + d$.

(b) Sea $s \geq 2$. Demostramos inicialmente que $k \leq q$. Supongamos que $k > q$. Dado por hipótesis $d > qs$, usando el teorema 2.2.8. se tiene que $C^{\perp}$ es un casi MDS-código, entonces $d^{\perp} = k > q = qs^{\perp}$. De $(C^{\perp})^{\perp} = C$ es un casi MDS-código, es decir $s = 1$ contradiciendo la suposición $k > q$. De modo que $k \leq q$.

Por otro lado, supóngase $k \leq q$ por el lema 2.2.4. obtenemos

$$\begin{aligned} n = k + d + s - 1 &\leq q + q(s+1) + s - 1 \\ &= q + qs + q + s - 1 + 3 - 3 \\ &= qs + 2q + s + 2 - 3 \\ &= q(s+2) + (s+2) - 3 \\ &= (q+1)(s+2) - 3. \end{aligned}$$

Entonces $n \leq (q+1)(s+2) - 3$. □

2.2.10 Lema. Si $M \in \text{Mat}(k+1 \times k+1, \mathbb{F}_q)$ está dada por

$$M = \left(\binom{j}{i} \right)_{i,j=0,1,\ldots,k}$$

Entonces

$$M^{-1} = \left((-1)^{j-1} \binom{j}{i} \right)_{i,j=0,1,\ldots,k}$$

Donde i representa las filas y j las columnas.

Demostración. Tenemos que probar que $MM^{-1} = I$. Esto es equivalente a demostrar que

$$\sum_{r=0}^{k}(-1)^{r-i}\binom{r}{i}\binom{j}{r} = \delta_{ij},$$

para todo $i, j = 0, 1 \ldots, k$.
Ahora si $z = y + 1$, entonces

$$z^j = (y+1)^j = \sum_{r=0}^{j}\binom{j}{r}y^r = \sum_{r=0}^{j}\binom{j}{r}(z-1)^r = \sum_{r=0}^{j}\sum_{i=0}^{r}\binom{j}{r}\binom{r}{i}(-1)^{r-i}z^i.$$

Comparando los coeficientes de los lados derechos e izquierdos se tiene la afirmación. □

2.2.11 Teorema. Sean C un $[n, k, d]$-A^sMDS código y $C^\perp$ un $[n, n-k, d^\perp]$-$A^{s^\perp}$MDS código sobre $\mathbb{F}_q$. Supóngase que $s \geq 1$. Entonces la distribución de pesos $A_0, A_1, \ldots, A_n$ de C satisface.

$$\begin{aligned} A_{n-d^\perp+r} &= \sum_{j=d^\perp}^{n-d}\binom{j}{d^\perp - r}\left(\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\binom{j-d^\perp+r}{j-1}\right)A_{n-j} \\ &+ \binom{n}{d^\perp - r}\sum_{i=0}^{r-1}(-1)^i\binom{n-d^\perp+r}{i}(q^{k-d^\perp+r-i}-1). \end{aligned}$$

Para $r = 1, \ldots, d^\perp$. En particular, $A_d, \ldots, A_{n-d^\perp}$ determina completamente la distribución de pesos de C.

Demostración. Sea $1 \leq r \leq d^\perp$. Por tanto $A^\perp_{i=0}$, para $1 \leq i \leq r$. Por las identidades de *MacWilliams* se sabe

$$\sum_{i=0}^{n-r}\binom{n-i}{r}A_i = q^{k-r}\sum_{i=0}^{r}\binom{n-i}{n-r}A_i^\perp, \tag{2.3}$$

para todo $0 \leq r \leq n$. En particular para $0 \leq r \leq d^\perp$.

Además

$$\sum_{i=0}^{n-r}\binom{n-i}{r}A_i = \sum_{i=0}^{d-1}\binom{n-i}{r}A_i + \sum_{i=d}^{n-r}\binom{n-i}{r}A_i$$

Por lo tanto de (2.3) se tiene que:

$$\begin{aligned}\sum_{i=d}^{n-r}\binom{n-i}{r}A_i &= q^{k-r}\sum_{i=0}^{r}\binom{n-i}{n-r}A_i^{\perp}-\sum_{i=0}^{d-1}\binom{n-i}{r}A_i\\ &= q^{k-r}\sum_{i=0}^{r}\binom{n-i}{n-r}A_i^{\perp}-\binom{n}{r}\\ &= q^{k-r}\left[\binom{n}{n-r}+\binom{n-1}{n-r}A_1^{\perp}+\cdots+\binom{n-r}{n-r}A_r^{\perp}\right]-\binom{n}{r},\end{aligned}$$

para todo $0\leq r\leq d^{\perp}$.

Pero $A_r^{\perp}=0$, para todo $0<r\leq d^{\perp}-1$, entonces

$$\sum_{i=d}^{n-r}\binom{n-i}{r}A_i = q^{k-r}\binom{n}{r}-\binom{n}{r}=(q^{k-r}-1)\binom{n}{r}, \tag{2.4}$$

para todo $0\leq r\leq d^{\perp}-1$.

Notamos que

$$d^{\perp}-1=n-(n-k)-s^{\perp}=k-s^{\perp}\leq k=n+1-d-s\leq n-d.$$

En términos de matrices tenemos:

$$\left(\left(\binom{j}{r}\right)_{r,j=0,\ldots,d^{\perp}-1}\middle|\left(\binom{j}{r}\right)_{\substack{r=0,\ldots,d^{\perp}-1\\ j=d^{\perp},\ldots,n-d}}\right)\begin{pmatrix}A_n\\ \vdots\\ A_d\end{pmatrix}=\begin{pmatrix}(q^k-1)\binom{n}{0}\\ \vdots\\ (q^{k-d^{\perp}+1}-1)\binom{n}{d^{\perp}-1}\end{pmatrix},$$

donde j representa las columnas y r las filas de las correspondientes matrices.

$$\overbrace{d^{\perp}\left\{\left(\begin{array}{cccc|cccc}\binom{0}{0} & \binom{1}{0} & \cdots & \binom{d^{\perp}-1}{0} & \binom{d^{\perp}}{0} & \binom{d^{\perp}+1}{0} & \binom{d^{\perp}+2.}{0} & \cdots & \binom{n-d}{0}\\ \binom{0}{1} & \binom{1}{1} & \cdots & \binom{d^{\perp}-1}{1} & \binom{d^{\perp}}{1} & \binom{d^{\perp}+1}{1} & \binom{d^{\perp}+2.}{1} & \cdots & \binom{n-d}{1}\\ \vdots & & & & \vdots & \vdots & \vdots & & \vdots\\ \binom{0}{d^{\perp}-1} & \binom{1}{d^{\perp}-1} & \cdots & \binom{d^{\perp}-1}{d^{\perp}-1} & \binom{d^{\perp}}{d^{\perp}-1} & \binom{d^{\perp}+1}{d^{\perp}-1} & \binom{d^{\perp}+2.}{d^{\perp}-1} & \cdots & \binom{n-d}{d^{\perp}-1}\end{array}\right)\right.}^{n-d}\begin{pmatrix}A_n\\ \\ \vdots\\ \\ A_d\end{pmatrix}$$

Si definimos, $A := \left((-1)^{j-r}\binom{j}{r}\right)_{r,j=0,\ldots,d^\perp-1}$ y $B = \left(\binom{j}{r}\right)_{\substack{r=0,\ldots,d^\perp-1 \\ j=d^\perp,\ldots,n-d}}$, entonces aplicando el lema 2.2.10 produce la ecuación

$$(I_{d^\perp}|AB)\begin{pmatrix} A_n \\ \vdots \\ A_d \end{pmatrix} = A\begin{pmatrix} (q^k-1)\binom{n}{0} \\ \vdots \\ (q^{k-d^\perp+1}-1)\binom{n}{d^\perp-1} \end{pmatrix}.$$

Para $0 \leq r < d^\perp \leq j \leq n-d$ la entrada en la posición (r,j) en la matriz $(I_{d^\perp}|AB)$ es

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

Entonces

$$\begin{aligned}\sum_{i=0}^{d^\perp-1}(-1)^{i-r}\binom{i}{r}\binom{j}{i} &= \sum_{i=0}^{n-d}(-1)^{i-r}\binom{i}{r}\binom{j}{i} - \sum_{i=d^\perp}^{n-d}(-1)^{i-r}\binom{i}{r}\binom{j}{i} \\ &= \delta_{r,j} - \sum_{i=d^\perp}^{n-d}(-1)^{i-r}\binom{i}{r}\binom{j}{i} \\ &= -\sum_{i=d^\perp}^{j}(-1)^{i-r}\binom{i}{r}\binom{j}{i}.\end{aligned}$$

Así para $r = 0,\ldots,d^\perp-1$, obtenemos:

$$A_{n-r} + \sum_{j=d^\perp}^{n-d}\left(-\sum_{i=d^\perp}^{j}(-1)^{i-r}\binom{i}{r}\binom{j}{i}\right)A_{n-j} = \sum_{i=0}^{d^\perp-1}(-1)^{i-r}\binom{j}{r}\binom{n}{j}(q^{k-j}-1)$$

$$A_{n-r} = \sum_{j=d^\perp}^{n-d}\left(\sum_{i=d^\perp}^{j}(-1)^{i-r}\binom{i}{r}\binom{j}{i}\right)A_{n-j} + \sum_{i=0}^{d^\perp-1}(-1)^{i-r}\binom{j}{r}\binom{n}{j}(q^{k-j}-1)$$

ó equivalentemente

$$\begin{aligned}
A_{n-d^\perp+r} &= \sum_{j=d^\perp}^{n-d}\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\binom{i}{d^\perp-r}\binom{j}{i}A_{n-j}+\\
&\quad+\sum_{j=0}^{d^\perp-1}(-1)^{j-d^\perp+r}\binom{j}{d^\perp-r}\binom{n}{j}(q^{k-j}-1)\\
&= \sum_{j=d^\perp}^{n-d}\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\binom{i}{d^\perp-r}\binom{j}{i}A_{n-j}+\\
&\quad+\sum_{i=0}^{r-1}(-1)^{i}\binom{d^\perp-r+i}{d^\perp-r}\binom{n}{d^\perp-r+i}(q^{k-d^\perp+r-i}-1)\\
&= \sum_{j=d^\perp}^{n-d}\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\left(\frac{i!}{(i-d^\perp+r)!(d^\perp-r)!}\right)\left(\frac{j!}{(j-i)!\,i!}\right)A_{n-j}\\
&\quad+\sum_{i=0}^{r-1}(-1)^{i}\left(\frac{(d^\perp-r+i)!}{(d^\perp-r+i-d^\perp+r)!(d^\perp-r)!}\right)\cdot\\
&\qquad\qquad\cdot\left(\frac{n!}{(n-d^\perp+r-i)!(d^\perp-n+i)!}\right)(q^{k-d^\perp+r-i}-1)\\
&= \sum_{j=d^\perp}^{n-d}\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\frac{j!}{(j-d^\perp+r)!(d^\perp-r)!}\frac{(j-d^\perp+r)!}{(j-d^\perp+r-(j-i))!(j-i)!}+\\
&\quad+\sum_{j=d^\perp}^{r-1}(-1)^{i}\frac{n!}{(n-d^\perp+r)!(d^\perp-r)!}\frac{(n-d^\perp+r)!}{(n-d^\perp+r-i)!\,i!}(q^{k-d^\perp+r-i}-1)\\
&= \sum_{j=d^\perp}^{n-d}\binom{j}{d^\perp-r}\left(\sum_{i=d^\perp}^{j}(-1)^{i-d^\perp+r}\binom{j-d^\perp+r}{j-i}\right)A_{n-j}+\\
&\quad+\binom{n}{d^\perp-r}\sum_{i=0}^{r-1}(-1)^{i}\binom{n-d^\perp+r}{i}(q^{k-d^\perp+r-i}-1)\qquad\square
\end{aligned}$$

2.2.12 Definición. Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$. Entonces definimos el código extensión C_e como el código generado por C sobre la extensión del cuerpo $\mathbb{F}_{q^e}$.

2.2.13 Proposición. C y C_e tienen los mismos parámetros n, k y d.

Demostración. Dado que que el rango de una matriz no cambia por la extensión del cuerpo, se tiene que una matriz generadora de C es también una matriz generadora de C_e. En consecuencia

$$\dim_{\mathbb{F}_q} C = \dim_{\mathbb{F}_{q^e}} C_e.$$

Por lo tanto $C = \mathbb{F}_q^k G$ y $C_e = \mathbb{F}_{q^e}^k G$, siendo G la matriz generadora de C. Una matriz de control H de C es también una matriz de control de C_e. Dado que d es el número natural r mas grande tal que cada submatriz de H de tamaño $(n-k) \times (r-1)$ tiene rango $r-1$, se verifica que r es el máximo número de columnas linealmente independientes. Por lo tanto del teorema 1.1.10, se sigue que la distancia mínima de C_e es d. Por consiguiente C y C_e tienen los mismos parámetros. □

2.3 Dualidad en los casi MDS-códigos

2.3.1 Definición. Un código C es llamado dualmente casi MDS-código, si $def(C) = def(C^\perp) = 1$.

2.3.2 Ejemplo. El $[7, 4, 3]$-código binario de Hamming C tiene defecto $s = 1$ y su código dual el $[7, 3, 4]$-código Simplex tiene defecto $s^\perp = 1$. Con lo cual C es dualmente casi MDS-código.

2.3.3 Proposición. Sea C dualmente casi MDS-código. Entonces para cada vector de peso mínimo c en C, existe salvo un múltiplo, un vector único de peso mínimo $c^\perp$ en $C^\perp$ tal que

$$\mathrm{sop}\langle c\rangle \cap \mathrm{sop}\langle c^\perp\rangle = \emptyset.$$

En particular el número de codewords con peso mínimo en C y $C^\perp$ son iguales.

Demostración. Sea $[n, k, d]$ los parámetros de C. En consecuencia $d = n - k$. Denotemos con $h_1, \ldots, h_n$ las columnas de una matriz de control H para C.

Sea $c = (c_1, \ldots, c_n)$ con $c_j \neq 0$, para exactamente $j \in \{j_1, \ldots, j_d\}$. Esto implica que las columnas $h_{j_1}, \ldots, h_{j_d}$ son linealmente independiente. Como rango de $H = n - k = d$, hallamos una columna $h_l \notin \{h_{j_1}, \ldots, h_{j_d}\}$ tal que

$$\dim\langle h_{j_1}, \ldots, h_{j_d}\rangle = d.$$

Así, existe $c^\perp = (c_1^\perp, \ldots, c_n^\perp) \in C^\perp$ con $c_1^\perp = 1$ y $c_{j_1}^\perp = \cdots = c_{j_{d-1}}^\perp = 0$. Dado que $c_i = 0$ para $i \notin \{j_1, \ldots, j_d\}$, al efectuar el producto interior de c con $c^\perp$ obtenemos

$$0 = (c|c^\perp) = \sum_{i=1}^{n} c_i c_i^\perp = c_{j_1} c_{j_1}^\perp + c_{j_2} c_{j_2}^\perp + \cdots + c_{j_{d-1}} c_{j_{d-1}}^\perp + c_{j_d} c_{j_d}^\perp = c_{j_d} c_{j_d}^\perp.$$

De esto se sigue que $c_{j_d}^\perp = 0$, ya que $c_{j_d} \neq 0$. Además, como $c_{j_1}^\perp = \cdots = c_{j_{d-1}}^\perp = 0$, se sigue que

$$\operatorname{sop}\langle c^\perp \rangle \subseteq \{1, \ldots, n\} \setminus \{j_1, \ldots, j_d\}.$$

Dado que C y $C^\perp$ son casi MDS-códigos, tenemos que la distancia mínima $d^\perp = n - (n-k) = k$, por lo que el vector $0 \neq c^\perp \in C^\perp$ es un vector de peso mínimo de $C^\perp$.

Por otro lado $\operatorname{sop}\langle c \rangle \subseteq \{j_1, \ldots, j_d\}$, por consiguiente

$$\operatorname{sop}\langle c \rangle \cap \operatorname{sop}\langle c^\perp \rangle = \emptyset,$$

con lo cual se tiene la afirmación. □

2.3.4 Ejemplo. Sea C un $[7, 4, 3]$-código binario de Hamming con matriz generadora.

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

Listamos a continuación todos los elementos de C

0000000	0001101	1111111	1110010
1101000	1000110	0010111	0111001
0110100	0100011	1001011	1011100
0011010	1010001	1100101	0101110

Para el $[7, 3, 4]$-código Simplex, con matriz generadora

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

Los codewords del código Simplex están dados por

0000000	1110010
1011100	1001011
0101110	0111001
0010111	1100101

Note que para cada $c \in C$, existe un único vector de peso mínimo $c^{\perp} \in C^{\perp}$ tal que

$$\mathrm{sop}\langle c\rangle \cap \mathrm{sop}\langle c^{\perp}\rangle = \emptyset,$$

como lo indica la proposicion anterior.

2.3.5 Corolario Sea C dualmente casi MDS-código sobre $\mathbb{F}_q$ con parámetros $[n, k, d]$. Entonces

$$A_{d+r} = \binom{n}{k-r} \sum_{i=0}^{r-1} (-1)^i \binom{d+r}{i} (q^{r-i} - 1) + (-1)^r \binom{k}{r} A_d,$$

para $r = 1, \ldots, k$

Demostración. En el caso dualmente casi MDS-códigos, se verifica que $s = s^{\perp} = 1$. Además $n - k = d$ y $d^{\perp} = k$. Es decir, $n - d = d^{\perp} = k$. Por lo tanto del teorema 2.2.11 tenemos que

$$\begin{aligned}
A_{d+r} &= \sum_{j=k}^{k} \binom{j}{k-r} \left(\sum_{i=k}^{j} (-1)^{i-k+r} \binom{j-k+r}{j-1} \right) A_{n-j} \\
&+ \binom{n}{k-r} \sum_{i=0}^{r-1} (-1)^i \binom{d+r}{i} (q^{r-i} - 1) \\
&= \binom{k}{k-r} (-1)^r \binom{r}{k-1} A_{n-k} + \binom{n}{k-r} \sum_{i=0}^{r-1} (-1)^i \binom{d+r}{i} (q^{r-i} - 1) \\
&= \binom{n}{k-r} \sum_{i=0}^{r-1} (-1)^i \binom{d+r}{i} (q^{r-i} - 1) + (-1)^r \binom{k}{r} A_d,
\end{aligned}$$

con lo cual se tiene el resultado. □

2.3.6 Corolario Sea C dualmente casi MDS-código sobre $\mathbb{F}_q$ con parámetros $[2d, d, d]$. Entonces C es un código formalmente auto-dual. Es decir, las distribuciones de pesos de C y $C^{\perp}$ son iguales.

Demostración. Sean $\{A_i \mid i = 0, 1, \ldots, n\}$ la distribución de pesos de C y $\{A_i^{\perp} \mid i = 0, 1, \ldots, n\}$ la distribución de pesos de $C^{\perp}$. De la identidad de MacWilliams se tiene que

$$\sum_{i=0}^{n-r} \binom{n-i}{r} A_i = q^{k-r} \sum_{i=0}^{r} \binom{n-i}{r-j} A_i^{\perp}.$$

Demostramos que la distribución de pesos de C y $C^{\perp}$ coinciden cuando $n = 2d$ y $r = d$. En efecto $A_i = 0$, para $1 \leq i \leq d$, y $A_i^{\perp} = 0$ para $1 \leq i \leq d$. Entonces

$$\begin{aligned} \sum_{i=0}^{2d-d} \binom{2d-i}{d} A_i &= q^{d-d} \sum_{i=0}^{d} \binom{2d-i}{d-i} A_i^{\perp} \\ \sum_{i=0}^{d} \binom{2d-i}{d} A_i &= q^{0} \sum_{i=0}^{d} \binom{2d-i}{d-i} A_i^{\perp} \end{aligned}$$

Por lo tanto

$$\tbinom{2d}{d} A_0 + \tbinom{2d-1}{d} A_1 + \cdots + \tbinom{2d-d}{d} A_d = \tbinom{2d}{d} A_0^{\perp} + \tbinom{2d-1}{d-1} A_1^{\perp} + \cdots + \tbinom{2d-d}{d} A_d^{\perp}.$$

Entonces

$$\binom{2d}{d} + A_d = \binom{2d}{d} + A_d^{\perp}$$

y se tiene que $A_d = A_d^{\perp}$. □

2.3.7 Proposición. Sea C dualmente casi MDS-código sobre $\mathbb{F}_q$ con parámetros $[n, k, d]$. Dadas cualesquiera $d + 1$ posiciones, entonces existe, salvo un múltiplo, exactamente un codeword de peso d ó $d + 1$ con soporte en las posiciones dadas.

Demostración. Según el corolario 2.2.7, se tiene que $d_2 = d + 2$. Por consiguiente dos codewords no linealmente independiente con soporte en $d + 1$ posiciones pueden ser encontrados.

Del corolario 2.3.5 sabemos que

$$A_{d+1} = \binom{n}{k-1}(q-1) - kA_d.$$

Por otro lado,

$$\begin{aligned}
\binom{n}{k-1} &= \tfrac{1}{q-1}(kA_d + A_{d+1}) \\
&= |\{\{j_1 \ldots, j_{d+1}\} \mid \exists\ 0 \neq c \in C \text{ con } \operatorname{sop}\langle c\rangle \subseteq \{j_1 \ldots, j_{d+1}\}\}| \\
&\leq |\{\{j_1 \ldots, j_{d+1}\} \mid |\{j_1 \ldots, j_{d+1}\}| = d+1\}| \\
&= \binom{n}{d+1} \\
&= \binom{n}{n-(d+1)} \\
&= \binom{n}{k-1},
\end{aligned}$$

lo cual prueba lo afirmado en la proposición. □

2.3.8 Definición. Sea X un conjunto con n elementos. Sea $\mathcal{U}$ un sistema de subconjuntos en el cual cada subconjunto posee d elementos, tal que cualquier conjunto con t elementos en X contiene exactamente un U en $\mathcal{U}$. Entonces este $\mathcal{U}$ es llamado un $U(t, d, n)$ sistema de Steiner superior.

Un ejemplo interesante y sencillo para ilustrar el anterior concepto es el plano de Fano.

2.3.9 Ejemplo. Sea $X = \{1, 2, 3, 4, 5, 6, 7\}$ y como sistema de subconjuntos de X sea

$$\mathcal{U} = \{\{1,2,3\}, \{1,4,7\}, \{1,5,6\}, \{2,4,5\}, \{2,6,7\}, \{3,4,6\}, \{3,5,7\}\}.$$

Enumerando adecuadamente los vértices, se verifica que este es un $U(4, 3, 7)$ sistema de Steiner superior.

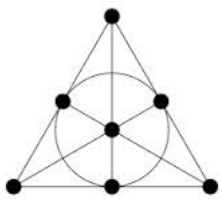

Figura 2.1: Plano de Fano

2.3.10 Lema. Sea $\mathcal{U}$ un $U(d+1,d,n)$ sistema de Steiner superior. Entonces $n < d+p$, donde p denota un primo que divide a $d+1$.

Demostración. Ver [2, Lemma 21]. □

Los sistemas de Steiner juegan un papel importante en la demostración de la siguiente proposición. Todos los detales pueden encontrarse en [2].

2.3.11 Proposición. Sea C dualmente casi MDS-código sobre $\mathbb{F}_q$ con parámetros $[2d,d,d]$. Si C no posee codewords de peso $d+1$, entonces $d+1$ es un número primo.

Demostración. Denotemos con p el número primo más pequeño que divide a $d+1$. Puesto que $2d = n < d+p \leq d+(d+1)$ y dado que $2d$ y $2d+1$ son enteros consecutivos obtenemos que $d+p = 2d+1 = d+(d+1)$. Por consiguiente $p = d+1$, con lo cual se tiene que $d+1$ es primo. □

2.3.12 Proposición. Sea C dualmente casi MDS-código sobre $\mathbb{F}_q$ con parámetros $[n,k,d]$, el cual no admite codewords de peso $d+1$. Si C_e es el código extensión sobre $\mathbb{F}_{q^e}$, entonces C_e es dualmente MDS-código sin codewords de peso $d+1$.

Demostración. Por la proposición 2.2.13 C_e, es dualmente MDS-código. Supongamos que existe un codewords $c_e \in C_e$ con $\mathrm{wt}(c_e) = d+1$. De la proposición 2.3.7 se sigue que existe $c \in C$ tal que

$$\mathrm{sop}\langle c\rangle \subseteq \mathrm{sop}\langle c_e\rangle.$$

Aplicando la proposición 2.3.7 para C_e, se tiene que c es un múltiplo de c_e. Por consiguiente $\mathrm{wt}(c) = d+1$, lo cual es una contradicción. □

2.3.13 Ejemplo. Sea $e \in \mathbb{N}$ con $e \geq 2$. Sea C el $[8,4,4]$-código binario extendido de Hamming. Note que C no tiene codewords de peso 5 y 6. Por la proposición anterior, C_e es un $[8,4,4]$-código auto-dual sobre $\mathbb{F}_{q^e}$ sin codewords de peso 5. Observe que

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

es una matriz generadora de C. Sea $a \in \mathbb{F}_{2^e}$ con $a \neq 0,1$. Entonces la suma de la primera fila con el a-múltiplo de la segunda fila produce un codeword de peso 6.

2.3.14 Ejemplo. Sea $e \in \mathbb{N}$ con $e \geq 2$. Sea C el $[12, 6, 6]$-código ternario extendido de Golay. C no tiene codewords de peso 7 ni de peso 8. Por la proposición anterior, C_e es un $[12, 6, 6]$-código auto-dual sobre $\mathbb{F}_{3^e}$ sin codewords de peso 7. Note que

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

es una matriz generadora de C. Sea $a \in \mathbb{F}_{3^e}$ con $a \neq 0, 1, 2$. Entonces como en el ejemplo anterior encontramos un codewords en C_e de peso 8.

2.3.15 Teorema. Sea C dualmente casi MDS-código sobre $\mathbb{F}_q$ con parámetros $[2d, d, d]$. Si C no tiene codewords de peso $d+1$ y $d+2$ entonces C es el $[8, 4, 4]$-código binario extendido de Hamming ó el $[12, 6, 6]$-código ternario extendido de Golay.

Demostración. Por el corolario 2.3.5 tenemos para $r = 1$.

$$\begin{aligned} 0 = A_{d+1} &= \binom{2d}{d-1}(-1)^0\binom{d+1}{0}(q-1) - \binom{d}{1}A_d \\ 0 = A_{d+1} &= \binom{2d}{d-1}(q-1) - dA_d. \end{aligned} \tag{2.5}$$

De igual manera para $r = 2$ obtenemos

$$0 = A_{d+2} = \binom{2d}{d-2}(q^2 - 1 - (d+2)(q-1)) + \binom{d}{2}A_d.$$

Un fácil cálculo produce $d = 2q$.

C y $C^\perp$ tienen defecto $s = 1$ y $s^\perp = 1$ respectivamente y distancia mínima $d = 2q$.

Primero calculemos A_{2q}. Sustituyendo $r = 1$, en el corolario 2.3.5 obtenemos

$$0 \leq A_{2q+1} = \binom{4q}{2q-1}(q-1) - 2qA_{2q}.$$

Por consiguiente

$$A_{2q} \leq \frac{q-1}{2q}\binom{4q}{2q-1}$$

Para $r = 2$ obtenemos

$$\begin{aligned} 0 \leq A_{2q+2} &= \binom{4q}{2q-2}(q^2-1-(q-1)(2q+2)) + \binom{2q}{2}A_{2q} \\ &= \binom{4q}{2q-2}\big((q+1)(q-1)-(2q+2)(q-1)\big) + \binom{2q}{2}A_{2q} \\ &= \binom{4q}{2q-2}(q-1)\big((q+1)-(2q+2)\big) + \binom{2q}{2}A_{2q} \\ &= \binom{4q}{2q-2}(q-1)(-q-1) + \binom{2q}{2}A_{2q} \\ &= -\binom{4q}{2q-2}(q-1)(q+1) + \binom{2q}{2}A_{2q}. \end{aligned}$$

Por lo tanto

$$\binom{2q}{2}A_{2q} \geq \binom{4q}{2q-2}(q-1)(q+1)$$

y se tiene que

$$A_{2q} \geq \frac{\binom{4q}{2q-2}}{\binom{2q}{2}}(q-1)(q+1) = \frac{(q-1)}{2q}\binom{4q}{2q-1} = \frac{q-1}{2q}\binom{4q}{2q-1}.$$

Ahora, para $r = 4$ obtenemos

$$\begin{aligned} 0 \leq \binom{4q}{2q-4}\Bigg[&(q^4-1)-(q^3-1)(2q+4)+(q^2-1)\binom{2q+4}{2} \\ &-(q-1)\binom{2q+4}{3}\Bigg] + \frac{q-1}{2q}\binom{2q}{4}\binom{4q}{2q-1} \end{aligned}$$

Multiplicando esta ecuación por $\binom{4q}{2q-4}^{-1}$ y simplificando obtenemos

$$\begin{aligned} 0 &\leq \big[(q^4-1)-(q^3-1)(2q+4)+\frac{1}{3}(q^2-1)(q+2)(2q+3)\big] + \\ &\quad + \frac{(q^2-1)(q+2)(2q+3)}{6} \\ &= (q^4-1)-(q^3-1)(2q+4)+\frac{1}{2}(q^2-1)(q+2)(2q+3) \end{aligned}$$

La desigualdad anterior es equivalente a $q^2 \leq 4q-3$. Resolviendola nos queda que $q = 2$ ó $q = 3$. Luego C es el $[8,4,4]$-código binario extendido de Hamming ó el $[12,6,6]$-código ternario extendido de Golay. □

2.4 MMD-códigos

Sea C un $[n,k,d]$-código sobre $\mathbb{F}_q$ con defecto s y dimensión $k \geq 2$. El lema 2.2.4 (a) establece una cota superior para la distancia mínima dada por $d \leq q(s+1)$ y si $k \geq 3$, entonces se verifica además que $s \leq q-1$, siempre que $d = (s+1)q$.

2.4.1 Definición. Un $[n,k,d]$-código C sobre $\mathbb{F}_q$ con defecto s y dimensión $k \geq 2$ se denomina un MMD-código, si $d = (s+1)q$.

El nombre de estos códigos deriva del ingles *maximum minimum distance*. Usando la definición del defecto, se puede observar que un MMD-código tiene longitud

$$n = (s+1)q + k + s - 1.$$

Esta clase de códigos alcanza la cota de Griesmer.

Para un determinado q y s los MMD-códigos permiten una posible cantidad grande de corrección de errores. Desafortunadamente, tales códigos son extremadamente raros, como veremos en esta sección.

2.4.2 Lema. Si C es un MMD-código sobre $\mathbb{F}_q$ con defecto $s \geq 1$, entonces $C^{\perp}$ es un casi MDS-código. En particular la distancia mínima de $C^{\perp}$ es $\dim_{\mathbb{F}_q} C$.

Demostración. Se sigue inmediatamente del teorema 2.2.8. □

Para los códigos con defecto 0 se tiene que la distribución del pesos está determinada de mánera única por sus parámetros. Sorprendentemente, para los MMD-códigos la situación es similar, como vemos en el siguiente lema.

2.4.3 Lema. Sea C un MMD-código sobre $\mathbb{F}_q$ con defecto $s \geq 1$ y con parámetros $[n,k,d]$ y $k \geq 3$. Entonces para los coeficientes de pesos A_i se verifica que

$$\begin{aligned}
A_d &= \frac{\binom{n}{k-1}}{\binom{k+s-1}{k-1}}(q-1) \\
A_{d+i} &= 0, \text{ para } \ i = 1, \ldots, s+1, \\
A_{d+s-1+r} &= (-1)^r \frac{s(q-1)n!}{(s-1+r)(r-1)!(k-r)!(s+d)!} + \\
&\quad \binom{n}{k-r} \sum_{i=0}^{r-1} (-1)^i \binom{n-k+r}{i} (q^{r-i}-1), \quad \text{para } r = 1, \ldots, k.
\end{aligned}$$

Note que la fórmula para $A_{d+s-1+r}$ en los casos $r = 1$ y $r = 2$ suministra el valor 0.

Demostración. Demostramos inicialmente que

$$A_d = \frac{\binom{n}{k-1}}{\binom{k+s-1}{k-1}}(q-1)$$

y que

$$A_{d+i} = 0, \text{ para } \ i = 1, \ldots, s+1.$$

Para ello consideremos una matriz generadora de C dada por

$$G = (g_{ij}) = (y_1, \ldots, y_n) \in M_{k\times n}(\mathbb{F}_q),$$

donde cada y_j es un vector de $\mathbb{F}_q^k$ y corresponde a la j-ésima columna de G.

Dado que $s \geq 1$, del lema 2.4.2 se sigue que $d(C^{\perp}) = k$. En consecuencia del lema 1.1.10 se sigue que cualquier conjunto con $k-1$ columnas de G es linealmente independiente. Dado que $n = (s+1)q + k + s - 1$ y $d = d(C) = (s+1)q$, se verifica que un codeword

$$0 \neq c = (c_1, \ldots, c_n) = (\sum_{i=1}^{k} a_i g_{i1}, \ldots, \sum_{i=1}^{k} a_i g_{in})$$

con $a_i \in \mathbb{F}_q$ tiene a lo mas $k+s-1$ posiciones con 0. Asi, $c_j = 0$ si y solo si el vector y_j^t de la matriz generadora G pertenece al hiperplano de $\mathbb{F}_q^k$ definido por

$$\left\{ (x_1, \ldots, x_k) \mid \sum_{i=1}^{k} a_i x_i = 0 \right\}.$$

En consecuencia a lo mas $k+s-1$ vectores y_j^t pertenecen a un hiperplano fijo.

Sea entonces H un hiperplano de $\mathbb{F}_q^k$ que contiene $k-2$ vectores de los n vectores y_j^t. Existen exactamente $q+1$ hiperplanos de $\mathbb{F}_q^k$, que contienen estos $k-2$ vectores linealmente independientes y cada y_j^t pertenece a algúno de estos hiperplanos. Entonces se sigue que

$$n = k + (s+1)q + s - 1 \leq k - 2 + (q+1)(s+1) = n.$$

Esto demuestra que el hiperplano H contiene exactamente $k+s-1$ vectores y_j^t. Por lo tanto $0 \neq c \in C$ tiene un cero en por lo menos $k-2$ posiciones y asi en exactamente $k+s-1$ posiciones y c es un codeword con peso mínimo. En particular se cumple que

$$A_d = \frac{\binom{n}{k-1}}{\binom{k+s-1}{k-1}}(q-1).$$

Dado que $n-(k-2)=d+s+1$ y $n-(k+s-1)=d$ se tiene además que

$$A_{d+1}=A_{d+2}=\cdots=A_{d+s+1}=0$$

y se tienen las primeras afirmaciones.

Para tener completamente determinada la distribución de pesos usamos la fórmula

$$A_{n-d^\perp+r}=(-1)^r r\binom{d^\perp}{r}\sum_{j=d}^{n-d^\perp}\binom{n-j}{d^\perp}\frac{A_j}{n-j-d^\perp+r}+$$
$$\binom{n}{d^\perp-r}\sum_{i=0}^{r-1}(-1)^i\binom{n-d^\perp+r}{i}(q^{k-d^\perp+r-i}-1),$$

para $i=1,\ldots,d^\perp$, la cual se presentó en el teorema 2.2.11. Tenga en cuenta ahora que $d^\perp=k$ y que $n-d^\perp=n-k=d+(s-1)$. Usando la primera parte de la demostración se sigue que $A_{n-j}=0$, para todo $j=d^\perp,\ldots,n-d-1$, con lo cual se tiene la siguiente reducción de la fórmula:

$$A_{d+s-1+r}=(-1)^r r\binom{k}{r}\binom{k+s-1}{k}\frac{A_d}{s-1+r}+$$
$$\binom{n}{d^\perp-r}\sum_{i=0}^{r-1}(-1)^i\binom{n-d^\perp+r}{i}(q^{k-d^\perp+r-i}-1).$$

Si multiplicamos $(-1)^r r\binom{k}{r}\binom{k+s-1}{k}\frac{1}{s-1+r}$ por el valor ya determinado de A_d obtenemos el término

$$(-1)^r\frac{s(q-1)n!}{(s-1+r)(r-1)!(k-r)!(s+d)!}$$

y se obtiene completamente la demostración. □

2.4.4 Lema. Sea C un MMD-código sobre $\mathbb{F}_q$ con defecto $s\geq 1$ y con parámetros $[n,k,d]$. Si $k\geq 4$, entonces $s=q-1$ o $s=q-2$.

Demostración. Del lema 2.2.4 se sigue que $s\leq q-1$. En consecuencia resta demostrar que $s\geq q-2$. Para ello consideremos la fórmula establecida en el lema anterior

$$A_{d+s-1+r}=(-1)^r\frac{s(q-1)n!}{(s-1+r)(r-1)!(k-r)!(s+d)!}+$$
$$\tbinom{n}{k-r}\sum_{i=0}^{r-1}(-1)^i\tbinom{n-k+r}{i}(q^{r-i}-1),\quad \text{para } r=1,\ldots,k,$$

para $r = 4$. Esto es admisible, ya que $k \geq 4$. Entonces tenemos que

$$\begin{aligned} 0 \leq A_{d+s+3} &= \frac{s(q-1)n!}{(s+3)3!(k-4)!(s+d)!} + \tbinom{n}{k-4} \sum_{i=0}^{3} (-1)^i \tbinom{s+d+3}{i} (q^{4-i} - 1) \\ &= \tfrac{n!}{6(k-4)!(s+d)!} \left(\tfrac{s(q-1)}{s+3} + \tfrac{1}{\binom{s+d+3}{3}} \sum_{i=0}^{3} (-1)^i \tbinom{s+d+3}{i} (q^{4-i} - 1) \right). \end{aligned}$$

En consecuencia se sigue que

$$0 \leq s(q-1)\tbinom{s+d+3}{3} + (s+3) \sum_{i=0}^{3} (-1)^i \tbinom{s+d+3}{i} (q^{4-i} - 1). \tag{2.6}$$

Dado que $d = (s+1)q$, la desigualdad (2.6) depende solamente de los parámetros s y q. Al factorizar el lado derecho de la desigualdad aparece el término

$$q(q-1)(qs + s + 1 - q)(s - q + 2),$$

con lo cual se obtiene que $s \geq q + 2$. □

2.4.5 Lema. Sea C un MMD-código sobre $\mathbb{F}_q$ con defecto $s = q-1$. Si $k \geq 4$, entonces C es el $[8, 4, 4]$-código extendido de Hamming.

Demostración. De la definición de MMD-código se sigue que C es un $[q^2 + q - 2 + k, k, q^2]$-código sobre $\mathbb{F}_q$ y del lema 2.4.2 se sigue que $C^\perp$ tiene defecto 1. Haciendo reducción del código C, obtenemos un código C_0 de longitud $q^2 + q + 2$, dimensión 4 y distancia mínima mayor o igual a q^2. En particular se tiene que C_0 es un código con defecto $s_0 \leq q - 1$. Del teorema 2.2.4 se sigue además que $s_0 \geq 1$.

Dado que $q^2 > q^2 - q \geq s_0 q$, del teorema 2.2.8 se sigue que $C_0^\perp$ es un código con defecto 1. Con lo cual podemos concluir que $C_0^\perp$ tiene parámetros $[q^2 + q + 2, q^2 + q - 2, 4]$ sobre $\mathbb{F}_q$. En particular cualesquiera tres columnas de una matriz generadora de C_0 no pueden ser colineales al considerarlas como puntos en el espacio proyectivo $\mathbb{P}_3(q)$. Si $q > 2$, entonces se sigue que

$$q^2 + q + 2 \leq q^2 + 1,$$

lo cual es una contradicción. Para la demostración de este resultado ver del teorema 2.6.12 de [12]. Si $q = 2$, entonces $s = 1$ y con el corolario 2.2.9 (a) se tiene que $k \leq 2q = 4$. Dado que por hipótesis $k \geq 4$, se sigue que $k = 4$ y en consecuencia C es el $[8, 4, 4]$-código extendido de Hamming. □

Bibliografía & Referencias

[1] S.M. Dodunekov and I.N., *Landgev, On near-MDS Codes*, report Linköping University (1994).

[2] A Faldum and W. Willems, *Codes of small defect. Design*, Codes and Cryptography 10,341-350 (1997).

[3] R.Hill, *A First Course in Coding Theory*, Clarendon Press, Oxford Applied Mathematics and Computing Sicence Series, (1986)

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

[5] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland Mathematical Library, Amsterdam, 1988.

[6] D. E. Muller. *Application of boolean algebra to switching circuit design and to error detection.* IEEE Transactions on Electronic Computers, 3, 6-12, 1954.

[7] I. S. Reed. *A class of multiple-error-correcting codes and the decoding scheme.* IEEE Transactions on Information Theory, IT-4, 38 - 49, 1954.

[8] I. S. Reed and G. Solomon. *Polynomial Codes over Certain Finite Fields,* Journal of SIAM, June 1960.

[9] Ricardo A. Podestá. *Algunas aspecto combinatorios de la teoría de códigos.* Trabajos de Matemáticas de Fa MAF, serie C 2006/35, 50 págs.

[10] J.H. Van Lint, *Introduction to Coding Theory*, Springer-Verlag, New York Heidelberg Berlin 1982.

[11] Victor K. Wei, *Generalized Hamming Weights for Linear Codes*, IEEE Transactions on Information Theory, VOL. 37, No. 5, 1991

[12] W. Willems, *Codierungstheorie*, Walter de Gruyter Inc., 1999.

[13] W. Willems, *Codierungstheorie und Kriptographie*, Birkhäuser Verlag, Basel, 2008.