Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas

Automorfismos de códigos binarios auto-duales doblemente pares y extremales

Darwin Villar Salinas

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

Director: Dr. rer. nat. Ismael Gutiérrez García

Barranquilla, Noviembre de 2010

Agradecimientos

Le agradezco ante todo a Dios por brindarme la oportunidad de seguir creciendo de manera personal y profesional, dando este paso siguiente en mi formación académica. Por estar siempre a mi lado, a lo largo de este camino e iluminándome en los momentos más necesarios.

A mi familia por su apoyo incondicional, sin ellos nada de lo que he conseguido lo tendría. A mis amigos y compañeros de estudio Rogelio Grau y Rubén Serna, por su colaboración al ayudarme a adaptarme rápidamente al mundo de la matemática pura.

Al MSc. Javier de la Cruz, por su disposición y sugerencias compartidas. A mi tutor y amigo Dr. rer. nat. Ismael Gutiérrez García por su apoyo y guía constante, y gracias a quién tuve la oportunidad de conocer mejor la matemática y sus aplicaciones.

Finalmente a todos mis profesores, quienes me ayudaron a madurar y a formar en mí el ser humano que soy, ojalá un ejemplo a seguir de las generaciones por venir.

Introducción

Con el interés, cada vez más creciente, en almacenamiento y transmisión de información, uno de los objetivos principales es conseguir la correcta reconstrucción de ésta a partir de los datos leídos o recibidos de una fuente. Esto con el fin de garantizar una comunicación eficaz.

En esta tarea juega un papel vital la teoría de la información y más precisamente la teoría de códigos, cuyo fin esencial es detectar y corregir errores que puedan suceder durante el proceso de transmisión o lectura de los datos, dependiendo del caso. Así, es de interés contar con códigos que tengan la mayor capacidad posible, fijados unos parámetros, de corregir errores.

Específicamente, en el caso de códigos binarios lineales existe una clase que, entre los códigos de bloque, posee la mayor capacidad de detección y corrección de errores. Éstos son los códigos doblemente pares extremales, que si además cuentan con la condición de ser auto-duales, los automorfismos que se puedan definir sobre este espacio vectorial se comportan de una manera particular, permitiendo así incluso obtener el código a partir de la información proporcionada por el grupo de automorfismos correspondiente.

Por esta razón en el presente trabajo de grado se proporcionan inicialmente algunas definiciones básicas y resultados fundamentales para la teoría de códigos en general, con el fin de estudiar con cuidado las técnicas introducidas por Huffman[1] y trascendidas por Yorgov[2], para caracterizar automorfismos de códigos extremales tipo II, que son los de nuestro interés. Resultados que son necesarios para el desarrollo mostrado en el segundo capítulo dedicado a obtener algunas condiciones necesarias, dado el tipo $p-(c,f)$ de un automorfismo de un código extremal tipo II, con p un primo impar.

Estas Condiciones son empleadas en el capítulo 2 para excluir algunos

de los tipos de una lista de posibilidades para cada uno de los códigos analizados, estos son los de parámetros [24,12,8], [48,24,12] y [120, 60, 24], todos extremales tipo II.

Finalmente, en el capítulo 3 de la lista resultante se determina si es posible que exista un código auto-dual, doblemente par y extremal con automorfismos del tipo estudiado en cada caso particular. Lo que al final nos lleva a obtener el código en sí, para los casos en los cuales no se llega a una contradicción.

Índice general

Capítulo 1

Preliminares

1.1. Generalidades

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

Recordemos que K^n es el producto cartesiano de n copias de K. Es decir,

$$K^n = \{(a_1, \ldots, a_n) \mid a_j \in K\}.$$

Como ejemplo de alfabeto K, con $|K| = q$ podemos considerar el conjunto de las clases residuales módulo q. Es decir, $K = \{0, 1, \ldots, q-1\}$. Sobre este conjunto puede definirse una suma de tal forma que se obtiene la estructura de grupo abeliano. Mas aún, si q es un número primo, entonces $\mathbb{Z}_q$ es un cuerpo. Un código binario corresponde entonces a un código definido sobre el cuerpo $\mathbb{Z}_2$ y un ternario a uno definido sobre el cuerpo $\mathbb{Z}_3$.

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

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

Para los vectores $u = (1, 1, 0, 0, 1)$, $v = (0, 1, 1, 1, 0) \in \mathbb{Z}_2^5$ se verifica que $\mathrm{d}(u, v) = 4$.

1.1.3 Teorema. La distancia Hamming d es una métrica. Es decir, para todo $u, v, w \in K^n$ se verifican

1. $\mathrm{d}(u, v) \geq 0$ y $\mathrm{d}(u, v) = 0$ si y solo si $u = v$
2. $\mathrm{d}(u, v) = \mathrm{d}(v, u)$ (Simetría)
3. $\mathrm{d}(u, v) \leq \mathrm{d}(u, w) + \mathrm{d}(w, v)$. (Desigualdad triangular)

Además d es invariante bajo traslaciones. Es decir, para todo $u, v, w \in K^n$ se verifica que $\mathrm{d}(u + w, v + w) = \mathrm{d}(u, v)$,

Demostración. La no negatividad y la simetría son inmediatas. Sean $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in K^n$. Para la desigualdad triangular note que si $u_j \neq v_j$, entonces $u_j \neq w_j$ o $v_j \neq w_j$. Con lo cual se sigue la afirmación.

Por otro lado,

$$\begin{aligned} \mathrm{d}(u, v) &= |\{j \mid u_j \neq v_j,\ j = 1, \ldots, n\}| \\ &= |\{j \mid u_j + w_j \neq v_j + w_j,\ j = 1, \ldots, n\}| \\ &= \mathrm{d}(u + w, v + w) \end{aligned}$$

□

1.1.4 Definición. Sea C es un código de longitud n sobre un alfabeto K.

1. Si $|C| > 1$, entonces llamaremos a

   $$\mathrm{d}(C) := \mathrm{mín}\{\mathrm{d}(c, c') \mid c, c' \in C, c \neq c'\}.$$

   la **distancia mínima** de C. Si $|C| = 1$, entonces definimos $\mathrm{d}(C) := 0$.

2. Si $\mathrm{d}(C) = d$ y $M = |C|$, entonces diremos que C es un (n, M, d)-código sobre K. Llamaremos a (n, M, d) los **parámetros** de C.

Si el alfabeto K es un cuerpo, es ampliamente conocido que K^n es un espacio vectorial. Los códigos lineales no son más que subespacios de este espacio vectorial. Estos, contrario a los códigos en general, además de ser un subconjunto de K^n, ofrecen abundantes ventajas. Por ejemplo el codificador y el decodificador no necesita almacenar todos los *codewords* sino solamente una base, ya que todos los *codewords* pueden representarse de manera única en términos de los elementos de ésta. Por otro lado, la distancia mínima puede calcularse de manera más rápida utilizando los pesos de los vectores, concepto que se definirá a continuación. No obstante resulta decisiva la rapidez de algunos algoritmos de decodificación, los cuales aprovechan la estructura de espacio vectorial.

1.1.5 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 la dimensión $\dim_K(C) = k$ y la distancia mínima $\mathrm{d}(C) = d$, entonces diremos que C es un $[n,k]$**-código** o más exactamente un $[n,k,d]$**-código** sobre K. Llamaremos a $[n,k,d]$ o $[n,k,d]_q$, si $|K| = q$, los **parámetros** de C.

Con ayuda de la función peso, la cual describimos a continuación, se puede determinar la distancia mínima de un código lineal con una simplificación considerable en los cálculos.

1.1.6 Definición. Sea K un cuerpo y $n \in \mathbb{N}$.

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

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

   y lo llamaremos el **peso** de x. La función $\mathrm{wt} : K^n \longrightarrow \mathbb{N}_0$ se denomina **función peso** sobre K^n.

2. Si $\{0\} \neq C \subseteq K^n$, entonces se define el **peso minimal de** C, notado con $\mathrm{wt}(C)$, de la siguiente manera

$$\mathrm{wt}(C) := \mathrm{mín}\{\mathrm{wt}(x) \mid 0 \neq x \in C\}.$$

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

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

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

Para $U \subseteq K^n$ definimos además

$$\operatorname{sop}(U) := \bigcup_{u \in U} \operatorname{sop}(u).$$

En particular $\operatorname{wt}(u) = |\operatorname{sop}(u)|$ y

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

1.1.7 Teorema. Si $C \neq \{0\}$ es un código lineal, entonces $\mathrm{d}(C) = \operatorname{wt}(C)$.

Demostración. De la invariancia bajo traslaciones de d se sigue

$$\begin{aligned} \mathrm{d}(C) &= \text{mín}\{\mathrm{d}(c, c') \mid c, c' \in C, \ c \neq c'\} \\ &= \text{mín}\{\mathrm{d}(c - c', 0) \mid c, c' \in C, \ c \neq c'\} \\ &= \text{mín}\{\mathrm{d}(x, 0) \mid x \in C, \ x \neq 0\} \\ &= \operatorname{wt}(C). \end{aligned}$$

□

El teorema anterior reduce considerablemente el costo en el cálculo de la distancia mínima de un código lineal. En efecto, se pasa de calcular $\binom{|C|}{2}$ distancias a determinar $|C| - 1$ pesos. Notemos con $K^{k \times n}$ al conjunto de todas las matrices con entradas en el cuerpo K, que poseen k filas y n columnas. Si $A \in K^{k \times n}$, entonces notaremos con A^T la matriz **transpuesta** de A y con $\operatorname{Rang}(A)$ el **rango** de A. Si f es un vector fila, entonces f^T denotará un vector columna.

1.1.8 Definición. Sea C un $[n, k]$-código sobre K.

1. Si $k \geq 1$, entonces una matriz $G \in K^{k \times n}$ se denomina una **matriz generadora** de C, si

   $$K^k G = \{(u_1, \ldots, u_k)G \mid u_j \in K\} = C.$$

   En particular, se verifica que $\operatorname{Rang}(G) = \dim(C)$.

2. Si $k < n$, entonces una matriz $H \in K^{(n-k) \times n}$ se denomina una **matriz de control** para C, si

   $$C = \{u \mid u \in K^n, \ Hu^T = 0\}.$$

   Del álgebra lineal se sigue que

   $$\operatorname{Rang}(H) = n - \dim(\ker(H)) = n - \dim(C) = n - k.$$

1.1.9 Definición. Se dice que G una matriz generadora de un $[n,k]$-código C está en su **forma estándar** si es de la forma

$$G = (I_k \mid B) = \begin{pmatrix} 1 & 0 & \cdots & 0 & * & \cdots & * \\ 0 & 1 & \cdots & 0 & * & \cdots & * \\ \vdots & & \ddots & \vdots & * & \cdots & * \\ 0 & 0 & \cdots & 1 & * & \cdots & * \end{pmatrix}.$$

Por ejemplo para el código binario auto-dual doblemente par extremal con parámetros $[24, 12, 8]$ se tiene que la matriz generadora en su forma estándar que está dada por:

$$G = (I_{12} \mid A) \in \mathbb{F}_2^{12\times 24},$$

donde $I_{12} \in \mathbb{F}_2^{12\times 12}$ es la matriz identidad con unos en la diagonal principal y ceros en las demás posiciones y A es la matriz dada por:

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

1.1.10 Teorema. Sea $G \in K^{k\times n}$ con filas $g_1 = (g_{11}, \ldots, g_{1n})$, $\ldots$, $g_k = (g_{k1}, \ldots, g_{kn})$. Entonces G es una matriz generadora de un $[n,k]$-código C sobre K, si y sólo si $B = (g_1, \ldots, g_k)$ es una base para C.

Demostración. Supongamos que $B = (g_1, \ldots, g_k)$ es una base para

C. Entonces para todo $u \in K^k$ se verifica que

$$\begin{aligned} uG &= (u_1, \ldots, u_k) \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} \\ &= (u_1 g_{11} + \cdots + u_k g_{k1}, \ldots, u_1 g_{1n} + \cdots + u_k g_{kn}) \\ &= u_1 g_1 + \cdots + u_k g_k \in C. \end{aligned}$$

Es decir,

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

y se tiene que G es una matriz generadora para C.

Recíprocamente, supongamos que G es una matriz generadora para C. Es decir, $C = \{uG \mid u \in K^k\}$. Entonces

$$(1, 0, \ldots, 0)G = g_1, \ldots, (0, \ldots, 0, 1)G = g_k$$

y se tiene que las filas de G pertenecen a C. Por lo tanto

$$C = \{uG \mid u \in K^k\} = \{u_1 g_1 + \cdots + u_k g_k \mid u_j \in K\}$$

y consecuentemente $C = \langle g_1, \ldots, g_k \rangle$. Dado que $\dim(C) = k$, se sigue que B es una base para C. □

1.2. Códigos cíclicos y QR-Códigos

En esta sección se tratarán algunos aspectos básicos sobre los códigos cíclicos y se definirán un tipo especial de ellos, los códigos de residuo cuadráticos o *QR-Codes*, por sus siglas en inglés.

1.2.1 Definición. Decimos que $C \leq \mathbb{F}_q^n$ es un **código cíclico** si $(c_0, c_1, \ldots, c_{n-1}) \in C$ implica que $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$.

1.2.2 Lema. Sea C un $[n, k]$-código sobre $\mathbb{F}_q$. Entonces, C es cíclico si, y sólo si,

$$C(x) := \left\{ \sum_{i=0}^{n-1} c_i x^i + \langle x^n - 1 \rangle \mid (c_0, \ldots, c_{n-1}) \in C \right\}$$

es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$, notado con $C(x) \trianglelefteq \mathbb{F}_q[x]/\langle x^n - 1 \rangle$.

DEMOSTRACIÓN. $\Rightarrow]$: Sea C un código cíclico, veamos que

$$C(x) \trianglelefteq \mathbb{F}_q[x]/\langle x^n - 1\rangle,$$

esto es, $C(x) \leq \mathbb{F}_q[x]/\langle x^n - 1\rangle$ y para todo $h \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$ se debe verificar que $hC(x) = C(x)$. La primera condición es clara por ser $C(x)$ cerrado con la suma de vectores y multiplicación por escalares, comprobemos entonces la segunda. En efecto, sea $\sum_{i=0}^{n-1} c_i x^i + \langle x^n - 1\rangle \in C(x)$, consideremos un caso base:

$$\begin{aligned} x\sum_{i=0}^{n-1} c_i x^i &= \sum_{i=0}^{n-1} c_i x^{i+1} \\ &= c_0 x + \ldots + c_{n-1}x^n \\ &\equiv c_0 x + \ldots + c_{n-2}x^{n-1} + c_{n-1} \text{ mód } \langle x^n - 1\rangle \\ &= c_{n-1} + c_0 x + \ldots + c_{n-2}x^{n-1} \in C(x), \end{aligned}$$

dado que C es cíclico. Con lo que se muestra la afirmación.
$\Leftarrow]$:Supongamos que $C(x) \trianglelefteq \mathbb{F}_q[x]/\langle x^n - 1\rangle$, si $\alpha = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in C(x)$, entonces $x\alpha = c_{n-1} + c_0 x + \ldots + c_{n-2}x^{n-1} \in C(x)$, luego $(c_0, c_1, \ldots, c_{n-1}) \in C$ implica que $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. Con lo que se tiene que C es cíclico. □

1.2.3 Teorema. Sean C un $[n, k]$-código sobre $\mathbb{F}_q$ y $C(x)$ su correspondiente ideal en $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Entonces:

(*a*) Existe un único polinomio mónico g con grado mínimo $n - k$, tal que $g + \langle x^n - 1\rangle \in C(x)$, $g \mid x^n - 1$ y

$$C(x) = \langle g\rangle := \{f \cdot g + \langle x^n - 1\rangle \mid f \in \mathbb{F}_q[x], \text{grad}(f) < k\}$$

(*b*) $B := (g, xg, \ldots, x^{k-1}g)$es una base para $C(x)$, además$\dim_{\mathbb{F}_q} C = n - \text{grad}(g)$.

(*c*) Si $g = \sum_{i=0}^{n-k} a_i x^i$, entonces:

$$G = \begin{pmatrix} a_0 & a_1 & \cdots & a_k & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_k & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_k \end{pmatrix} \in \mathbb{F}_q^{k\times n},$$

es una matriz generadora para C.

Demostración.

(a) Mostremos inicialmente la unicidad de g. Sean $g,\ h$ polinomios de grado mínimo $n-k$ con la propiedad enunciada, luego como ambos son mónicos $\text{grad}(g-h) < n-k$, entonces $g-h=0$ por la minimalidad de estos polinomios, y así $g=h$. Mostremos ahora su existencia, dado que $\mathbb{F}_q[x]/\langle x^n-1\rangle$ es un anillo de ideales principales y $C(x)$ es un ideal de éste, se sigue que existe g con grado mínimo tal que $C(x)=\langle g\rangle$.

Finalmente veamos que $g \mid x^n-1$. En efecto, de la división con resto se tiene que existen $h, r \in \mathbb{F}_q[x]$ tales que $x^n-1 = gh+r$, con $\text{grad}(r) < grad(g)$. De esta manera, $r = (x^n-1) - gh$, así $r \equiv -gh \in C(x)$, ya que $C(x)$ es un ideal y $g \in C(x)$. Con lo que se concluye que $r=0$ por minimalidad de g, es decir, $g \mid x^n-1$.

(b) De (a) se tiene que $C(x)=\langle g\rangle$, esto es, $(g,\ xg, \ldots,\ x^{k-1}g)$ genera a $C(x)$ y claramente es linealmente independiente, en consecuencia una base para $C(x)$ y también $\dim_{\mathbb{F}_q} C(x) = k-1+1 = k$

(c) Si $g = \sum_{i=0}^{n-k} a_i x^i$ y $a_0 \neq 0$ por minimalidad de g, entonces como nuevamente de (a), $(g,\ xg, \ldots,\ x^{k-1}g)$ es una base para $C(x) \cong C$, entonces $((a_0, a_1, \ldots, a_{n-k}, 0, \ldots, 0), \ldots, (0, \ldots, 0, a_0, a_1, \ldots, a_{n-k}))$ un sistema de $\mathbb{F}_q^n$ es una base para C sobre $\mathbb{F}_q$.

□

1.2.4 Definición. Sean p un primo impar y $a \in \mathbb{Z}^\times$ con $p \nmid a$. Entonces

a. Decimos que a es un **residuo cuadrático módulo** p si existe $b \in \mathbb{Z}$, tal que $a \equiv b^2$ mód p.

b. Definimos el **símbolo de Legendre** como la función

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z}^\times \longrightarrow \{-1,\ 0,\ 1\},$$

dada por

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{Si } a \text{ es un residuo cuadrático mód } p \\ 0, & \text{Si } p \mid a \\ -1, & \text{Si } a \text{ no es un residuo cuadrático mód } p. \end{cases}$$

Por ejemplo, en $\mathbb{Z}_7$ 1, 2 y 4 son residuos cuadráticos módulo 7, ya que $4 \equiv 2^2$ mód 7, $2 \equiv 4^2$ mód 7 y $1 \equiv 6^2$ mód $7 \equiv 1^2$ mód 7. De hecho si definimos:

$$Q_p := \left\{ a \in \mathbb{N} \mid 1 \leqslant a < p \wedge \left(\frac{a}{p}\right) = 1 \right\}$$
$$N_p := \left\{ a \in \mathbb{N} \mid 1 \leqslant a < p \wedge \left(\frac{a}{p}\right) = -1 \right\}.$$

Se puede probar que $|Q_p| = |N_p| = \frac{p-1}{2}$. En efecto, definamos

$$\alpha : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$$
$$x \longmapsto \alpha(x) := x^2,$$

Veamos que $\alpha \in \mathrm{End}(\mathbb{F}_p^\times)$. Sean $a, b \in \mathbb{F}_p^\times$, entonces

$$\alpha(ab) = (ab)^2 = a^2b^2 = \alpha(a)\alpha(b).$$

Ahora $\mathrm{Kern}(\alpha) = \{a \in \mathbb{F}_p \mid a^2 = 1\} = \{1, -1\}$. Entonces

$$|Q_p| = |\mathrm{Im}(\alpha)| = \frac{|\mathbb{F}_p^\times|}{|\mathrm{Kern}(\alpha)|} = \frac{p-1}{2}.$$

De esta forma, si $\mathbb{F}_p^\times$ tiene $\frac{p-1}{2}$ residuos cuadráticos módulo p, entonces tiene la misma cantidad de no residuos cuadráticos módulo p, estos es, $|Q_p| = |N_p| = \frac{p-1}{2}$.

1.2.5 Definición. Sean $p \neq 2$ un primo, $r \neq p$ otro primo con $(\frac{r}{p}) = 1$, E una extensión del cuerpo $\mathbb{F}_r = K$ que contiene una p-ésima raíz de la unidad $\alpha \neq 1$, i.e., $K \leq E$, $\alpha^p = 1 \neq \alpha$ y definamos

$$q(x) := \prod_{i \in Q_p} (x - \alpha^i) \in \mathbb{F}_r[x]$$
$$n(x) := \prod_{i \in N_p} (x - \alpha^i) \in \mathbb{F}_r[x],$$

entonces los códigos cíclicos de longitud p sobre $\mathbb{F}_r$ generados por $q(x)$, $n(x)$, $q(x)(x-1)$, $n(x)(x-1)$ son llamados **códigos de residuo cuadrático** y se denotan por $Q, N, \overline{Q}$ y $\overline{N}$.

1.3. Dualidad

Similar como en los espacios vectoriales euclidianos se describe el código dual con base en una forma bilineal no degenerada, la cual se construye exactamente igual al producto escalar euclidiano. Para ello definimos

$$(\mid) : K^n \times K^n \longrightarrow K$$

mediante

$$(u|v) := \sum_{j=1}^{n} u_j v_j,$$

donde K es un cuerpo, $u = (u_1, \ldots, u_n)$ y $v = (v_1, \ldots, v_n)$.

1.3.1 Lema. Sean $u, v, w \in K^n$ y $a, b \in K$. Entonces

(a) $(u + v|w) = (u|w) + (v|w)$

(b) $(au|v) = a(u|v)$

(c) $(u|v) = (v|u)$.
Es decir, $(\mid)$ es una forma bilineal simétrica.

(d) $(0|v) = (v|0) = 0$

(e) Si $(u|v) = 0$, para todo $v \in K^n$, entonces $u = 0$.
Es decir, $(\mid)$ es una forma bilineal simétrica no degenerada.

Demostración. Las primeras cuatro afirmaciones son inmediatas. Para demostrar la última, sea v el j-ésimo vector de la base canónica de K^n, esto es, $v = e_j$, entonces $0 = (u|e_j) = u_j$. Por lo tanto $u = 0$. □

1.3.2 Definición. Sea C un $[n, k]$-código sobre un cuerpo 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 $C = C^\perp$.

Puede verificarse sin dificultades que $M^{\perp}$ es siempre un subespacio vectorial de K^n, aún cuando M se simplemente un subconjunto de K^n. En particular, un código auto-dual es siempre lineal.

1.3.3 Teorema. Sea C un $[n,k]$-código sobre un cuerpo K con $|K| = q$. 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 sólo si, G es una matriz de control de $C^{\perp}$.

(c) H es una matriz de control de C si, y sólo si, H es una matriz generadora de $C^{\perp}$.

(d) 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.

(e) Si C es auto-dual, entonces $k = \frac{n}{2}$. En particular, todo código auto-dual tiene longitud par.

Demostración.

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

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

Entonces $x = (x_1, \ldots, x_n)$ es un elemento de $C^{\perp}$ si, y sólo si, $(x|f_j) = 0$, para todo $j = 1, \ldots, k$. Esto es equivalente a afirmar que x es solución del sistema homogéneo de k ecuaciones lineales en las variables $x_1, \ldots, x_n$ dado por

$$\begin{aligned} g_{11}x_1 + g_{12}x_2 + \cdots + g_{1n}x_n &= 0 \\ g_{21}x_1 + g_{22}x_2 + \cdots + g_{2n}x_n &= 0 \\ &\vdots \\ g_{k1}x_1 + g_{k2}x_2 + \cdots + g_{kn}x_n &= 0. \end{aligned}$$

En conclusión

$$x \in C^{\perp} \Leftrightarrow Gx^T = 0.$$

Del álgebra lineal sabemos que

$$n = \text{Rang}(G) + \dim_K\{x \in K^n \mid Gx^T = 0\}.$$

Es decir,

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

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

(b) Si $x \in C$ y $v \in C^\perp$, entonces $(x|v) = 0$. Por lo tanto $x \in (C^\perp)^\perp$. Esto demuestra que $C \subseteq (C^\perp)^\perp$. Además

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

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 para todo $j = 1, \ldots, k$. Es decir, cada f_j pertenece a $(C^\perp)^\perp = C$. Dado que las filas de G son linealmente independientes y además el número de filas de G, que es k, coincide con

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

Por lo tanto 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

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

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 $n-k=k$ y se tiene la afirmación.

□

1.3.4 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 $r=2$ se dice que el código es **par** y si $4 \mid \mathrm{wt}(c)$, para todo $c \in C$, entonces C se denomina **doblemente par**.

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

(a) C es 2-divisible.

(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 $K=\mathbb{F}_2$ (característica 2) tenemos

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

Por lo tanto C es 2-divisible.

(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

$$\mathrm{wt}(c+c')=\mathrm{wt}(c)+\mathrm{wt}(c')-2\,|\mathrm{sop}(c)\cap \mathrm{sop}(c')|. \tag{1.1}$$

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 (1.1) se sigue que $4 \mid \mathrm{wt}(c+c')$.

□

Entre los códigos auto-duales existe una clasificación especial dependiendo del cuerpo sobre el cual están definidos y su r-divisibilidad, de la siguiente manera.

1.3.6 Definición. Sea C un código auto-dual r-divisible, con $r > 1$. Entonces, se dice que C es un código:

(a) **Tipo I** si es binario y no es doblemente par, i.e., $r \neq 4$.

(b) **Tipo II** si es binario y doblemente par.

(c) **Tipo III** si es ternario, que a su vez por ser auto-dual implica ser 3-divisible.

(d) **Tipo IV** si es un código sobre $\mathbb{F}_4$, en consecuencia es par.

Capítulo 2

Tipos de automorfismos de códigos tipo II

Un teorema de Gleason, Pierce y Turyn [3] garantiza que, si $s > 1$ divide el peso de cada *codeword* en un código binario auto-dual no trivial, entonces $s = 2$ o $s = 4$. Los códigos binarios auto-duales satisfacen automáticamente esta condición, cuando $s = 2$. Los códigos binarios auto-duales doblemente par existen, si n es un múltiplo de ocho [4].

Un teorema de C.L. Mallows y N.J.A. Sloane [6] demuestra que la distancia mínima d de un $[n, k, d]$-código binario auto-dual satisface la desigualdad:

$$d \leq 4\left\lfloor \tfrac{n}{24} \right\rfloor + 4, \text{ si } \ n \not\equiv 22 \text{ mód } 24$$

$$d \leq 4\left\lfloor \tfrac{n}{24} \right\rfloor + 6, \text{ si } \ n \equiv 22 \text{ mód } 24,$$

donde $\lfloor x \rfloor$ denota la parte entera de x. Los códigos que alcanzan esta cota son denominados **extremales**. Si n es un múltiplo de 24, entonces un código binario auto-dual que alcance la cota forzosamente debe ser doblemente par [7]. Por lo tanto, los códigos binarios auto-duales y extremales con longitud un múltiplo de 24 resultan de especial interés.

En resumen los códigos binarios auto-duales y extremales tienen parámetros $[24m, 12m, 4m+4]$, para algún m natural. Shengyuan Zhang [8] demostró que para $m > 153$ tales códigos no existen y hasta el momento sólo se encuentran caracterizados los casos $m = 1$ y $m = 2$, los cuales corresponden respectivamente al $[24, 12, 8]$-código extendido de

Golay y al $[48, 24, 12]$-código de resto cuadrático. Como puede notarse, tales códigos tienen una longitud acotada n. La cota conocida hasta el momento es de 3672 y como notamos anteriormente, la existencia sólo ha podido demostrarse para valores muy pequeños de m.

Otro problema interesante es la caracterización del grupo de automorfismos asociado a tales códigos. Para una permutación $\sigma \in \mathrm{Sym}(n)$ y $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ se define

$$\sigma(v) := (v_{\sigma(1)}, \ldots, v_{\sigma(n)}).$$

El código binario C y su imagen son llamados **equivalentes**. Si $C = \sigma(C)$, entonces la permutación σ se denomina un **automorfismo** de C. El conjunto de todos los automorfismos del código C forman el **grupo de automorfismos** de C y se notará con $\mathrm{Aut}(C)$.

Finalmente, si C es un $[n, k]-$código sobre $\mathbb{F}_q$ y $\sigma \in \mathrm{Aut}(C)$. Entonces, decimos que σ es del tipo $p-(c, f)$ si $\sigma \in \mathrm{Sym}(n)$ está compuesto por c p cíclos y f puntos fijos.

2.1. Fundamentos algebráicos

Siendo C un código lineal de longitud n y $\sigma \in \mathrm{Aut}(C)$ del tipo $p-(c, f)$, a lo largo de esta sección se hará uso de una notación estándar para algunos conjuntos especiales tales como:

$$F_\sigma(C) := \{c \in C \mid \sigma(c) = c\}, \text{ donde } \sigma \in \mathrm{Aut}(C).$$

$$E_\sigma(C) := \{v \in C \mid \mathrm{wt}(v|_{\Omega_i}) \equiv 0 \text{ mód } 2, i \in \{1, \ldots, c+f\}\}.$$

Sea además π la función

$$\pi : F_\sigma(C) \longrightarrow \mathbb{F}_2^{c+f}$$

$$x \longmapsto (\pi(x))_i := x_j,$$

donde $j \in \Omega_i$, $\sigma = \Omega_1 \ldots \Omega_{c+f}$. En adelante notaremos su imagen $\pi(F_\sigma(C))$ con $\overline{F_\sigma(C)}$.

Veamos algunas nociones de $F_\sigma(C)$, $E_\sigma(C)$ y $\sigma \in \mathrm{Aut}(C)$. Sea $\sigma = \Omega_1 \ldots \Omega_{c+f}$, donde $\Omega_{c+1} \ldots \Omega_{c+f}$ son puntos fijos. Así, se entenderá para $C = (c_1, \ldots, c_n)$, $C|_{\Omega_j} := (c_{\Omega_{j1}}, \ldots, c_{\Omega_{jl}})$, con $\Omega_j = (\Omega_{j1} \ldots \Omega_{jl})$, siendo l la longitud del ciclo. Luego, por ejemplo si

$$C = 000111111000000000011000 \text{ y } \sigma = (123)(456)(789),$$

entonces $C|_{(123)} = (000)$ y $C|_{(456)} = (111)$. Note además que por definición si $c \in E_\sigma(C)$ y $f \neq 0$, entonces $c|_{\Omega_s} = 0$ para todo $s \in \{c+1, \ldots, c+f\}$. Por otro lado si

$$\sigma = (1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11\,12) \text{ y } C = 101\,000\,000\,101\,011\,011\,000\,000,$$

entonces $\sigma(c) = (110\,000\,000\,110\,011\,011\,000\,000)$. En este caso note incluso que $c \neq \sigma(c)$, por lo que $c \notin F_\sigma(C)$, por definición. Además, se nota del ejemplo que para que un $c \in C$ esté en $F_\sigma(C)$ se debe cumplir que $c_{\Omega_{jl}} \equiv c_{\Omega_{jk}} \text{mód } 2$, para todo $\Omega_{jl}, \Omega_{jk} \in \Omega_j$, con $j \in \{1, \ldots, c+f\}$.

Finalmente, como claramente $F_\sigma(C) \cup E_\sigma(C) \subseteq C$, si C es doblemente par, entonces ambos, tanto $F_\sigma(C)$, como $E_\sigma(C)$, también lo son. Y si C es auto-ortogonal, mucho más si es auto-dual, entonces ambos subcódigos también lo son.

2.1.1 Lema. Sea C un código auto-dual. Entonces $\overline{F_\sigma(C)}$ es auto-dual de longitud $n - c(p-1)$. Además, si C es doblemente par y $p \equiv 1$ mód 4 ó $f = 0$, entonces $\overline{F_\sigma(C)}$ también lo es.

Demostración. Veamos inicialmente que $F_\sigma(C) \cong \overline{F_\sigma(C)}$. Claramente π es una aplicación lineal, como consecuencia de que $\sigma \in \text{Aut}(C)$, además sobreyectiva. Luego, sólo falta comprobar que π es inyectiva. En efecto, si $x \in F_\sigma(C)$ tal que $\pi(x) = 0$, entonces $x_i = 0$ para $i \in \{1, \ldots, n\}$, por definición de π. Es decir, $\pi(x) = 0$ con lo que se tiene que $x = 0$. De esta manera Kern(π)=$\{0\}$ y π es inyectiva. Por lo tanto se tiene la afirmación inicial.

Mostremos a continuación que $\overline{F_\sigma(C)}$ es auto-ortogonal. Dado que C es auto-dual, para $v, w \in F_\sigma(C) \subseteq C$ se verifica que:

$$0 \equiv (v|w) \equiv p\sum\nolimits_{i=1}^{c} v_i w_i + \sum\nolimits_{i=c+1}^{c+f} v_i w_i,$$

donde $(v_1, \ldots, v_{c+f}) = \pi(v)$ y $(w_1, \ldots, w_{c+f}) = \pi(w)$, lo cual siempre es posible por ser π biyectiva.

Como p es primo y $p \neq 2$, al ser C un código binario, se tiene que:

$$0 \equiv \sum\nolimits_{i=1}^{c+f} v_i w_i = (\pi(v), \pi(w)),$$

dado que

$$p\sum\nolimits_{i=1}^{c} v_i w_i \equiv \sum\nolimits_{i=1}^{c} v_i w_i \text{ mód } 2.$$

Además, como $\pi(v), \pi(w)$ son cualesquiera en $\overline{F_\sigma(C)}$, al serlo $v, w \in F_\sigma(C)$, se tiene como consecuencia que $\overline{F_\sigma(C)} \subseteq \overline{F_\sigma(C)}^\perp$, así por definición $\overline{F_\sigma(C)}$ es auto-ortogonal.

Es ampliamente conocido que si K es un cuerpo y $C \leq K^n$, con $n \in \mathbb{N}$, entonces

$$\dim_K(C) + \dim_K(C^\perp) = n.$$

De esta manera, como ya se sabe que $\overline{F_\sigma(C)}$ es auto-ortogonal, basta con mostrar que tiene la misma dimensión que $\overline{F_\sigma(C)}^\perp$ para tener que es auto-dual. Prosiguiendo en este sentido, se tiene del teorema 3.2 de [12] y del hecho que $F_\sigma(C) \cong \overline{F_\sigma(C)}$ que

$$\dim_{\mathbb{F}_2} \{v \in \mathbb{F}_2^n \mid \sigma(v) = v\} = 2 \dim_{\mathbb{F}_2} F_\sigma(C) = 2 \dim_{\mathbb{F}_2} \overline{F_\sigma(C)}.$$

Ahora, como

$$(e_j)_l := \begin{cases} 1, & l \in \Omega_j \\ 0, & \text{otro caso,} \end{cases}$$

es una base para $V_0 := \{v \in \mathbb{F}_2^n \mid \sigma(v) = v\}$, se sigue que:

$$\dim_{\mathbb{F}_2} \overline{F_\sigma(C)} = \frac{1}{2}(c + f),$$

siendo $(c+f)$ la longitud de $\overline{F_\sigma(C)}$, con lo que se tiene el resultado. Note que como $n = pc + f$, se verifica que $c + f = n - c(p-1)$.. Para terminar veamos la última afirmación. Sea $v \in F_\sigma(C)$, entonces $\mathrm{wt}(v) \equiv 0 \mod 4$ y $\mathrm{wt}(v) = p\sum_{i=1}^{c} \pi(v)_i + \sum_{i=c+1}^{c} + f\pi(v)_i$. Luego, si $p \equiv 1 \mod 4$, entonces:

$$\begin{aligned} \mathrm{wt}(v) =& p \sum\nolimits_{i=1}^{c} \pi(v)_i + \sum\nolimits_{i=c+1}^{c+f} \pi(v)_i \\ \equiv& \sum\nolimits_{i=1}^{c} \pi(v)_i + \sum\nolimits_{i=c+1}^{c+f} \pi(v)_i \mod 4 \\ =& \sum\nolimits_{i=1}^{c+f} \pi(v)_i = \mathrm{wt}(\pi(v)). \end{aligned}$$

Como $v \in F_\sigma(C)$ es cualquiera entonces $F_\sigma(C)$ es doblemente par. Igualmente, si $f = 0$, entonces:

$$\begin{aligned} \mathrm{wt}(v) =& p \sum\nolimits_{i=1}^{c} \pi(v)_i \\ \equiv& 0 \mod 4, \end{aligned}$$

y como p no es múltiplo de 4, entonces necesariamente lo debe ser $\sum_{i=1}^{c} \pi(v)_i = \mathrm{wt}(\pi(v))$. □

2.1.2 Corolario. Sea C un código auto-dual y doblemente par. Si $p \equiv 1$ mód 4 y $p \not\equiv 1$ mód 8, entonces c es par.

DEMOSTRACIÓN. Dado que C es auto-dual y doblemente par, por el lema 2.1.1, se tiene que $\overline{F_\sigma(C)}$ también lo es. Por ende su longitud es divisible por ocho. (Ver [4]) Entonces $n - c(p-1) \equiv 0$ mód 8, por otro lado $p - 1 \equiv 0$ mód 4 y $p - 1 \not\equiv 0$ mód 8, por hipótesis. Luego cómo además $n \equiv 0$ mód 8, se sigue que $c \equiv 0$ mód 2, es decir, c es par. □

2.1.3 Lema. Dado $C \leq \mathbb{F}_2^n$, entonces $C = F_\sigma(C) \oplus E_\sigma(C)$. Si además C es auto-dual, entonces $\dim_{\mathbb{F}_2} E_\sigma(C) = (p-1)c/2$. Más aún, el orden multiplicativo de $[2]_{\equiv \text{ mód } p}$ en $\mathbb{Z}_p$ divide a $\dim_{\mathbb{F}_2} E_\sigma(C)$. En particular si C es auto-dual y 2 es una raíz primitiva módulo p, entonces c es par.

DEMOSTRACIÓN. Sea $v \in C$ y definamos $w := v + \sum_{i=0}^{p-1} \sigma^i(v)$. Como

$$\mathrm{wt}(\sigma^i(v)|_{\Omega_j}) = \mathrm{wt}(\Omega_j^i(v)|_{\Omega_j}) = \mathrm{wt}(v|_{\Omega_j}),$$

para todo $i \in \{0, \ldots, p-1\}$, para todo $j \in \{1, \ldots, c+f\}$, dado que cada par de ciclos son disjuntos dos a dos, esto es, $\Omega_l \cap \Omega_s = \emptyset$, si $l \neq s$ y que Ω_j sólo reorganiza las coordenadas de v, por lo que no altera su peso.

Ahora, como $\sigma \in Aut(C)$ y $\sigma = \Omega_1 \ldots \Omega_{c+f}$, se sigue que

$$w|_{\Omega_j} = v|_{\Omega_j} + \sum_{i=0}^{p-1} \sigma^i(v)|_{\Omega_j}, \text{para todo } j \in \{1, \ldots, c+f\}.$$

Como C es binario, es entonces par o 2-divisible. Esto a su vez implica que

$$\mathrm{wt}(w|_{\Omega_j}) = \mathrm{wt}\left(\sum_{i=0}^{p} \sigma^i(v)|_{\Omega_j}\right) - 2k,$$

dado que el orden de σ es p y $k(v, \Omega_j)$. Es decir,

$$\mathrm{wt}(w|_{\Omega_j}) = (p+1)\mathrm{wt}(v|_{\Omega_j}) - 2k$$

y como p es un primo impar se sigue que

$$\mathrm{wt}(w|_{\Omega_j}) \equiv 0 \text{ mód } 2,$$

para cada $j \in \{1, \ldots, c+f\}$, es decir, $w \in E_\sigma(C)$.

Note que

$$\begin{aligned}\sigma\left(\sum_{i=0}^{p-1}\sigma^i(v)\right) &= \sum_{i=0}^{p-1}\sigma^{i+1}(v), \text{ dado que } \sigma \in Aut(C)\\ &= \sum_{i=0}^{p-1}\sigma^i(v), \text{ ya que } \sigma \text{ es de orden } p.\end{aligned}$$

Esto muestra que $\sum_{i=0}^{p-1}\sigma^i(v) \in F_\sigma(C)$. Por consiguiente para cualquier $v \in C$ se verifica que

$$v = \sum_{i=0}^{p-1}\sigma^i(v) + w \in F_\sigma(C) + E_\sigma(C)$$

(note que por ser C un espacio vectorial sobre un cuerpo de característica dos, para todo $v \in C$, se verifica que $v = -v$).

Mostremos a continuación que $F_\sigma(C) \cap E_\sigma(C) = \emptyset$. En efecto, sea $v \in F_\sigma(C) \cap E_\sigma(C)$, entonces por estar en ambos conjuntos, $\sigma(v) = v$, aún más, $\Omega_j(v)|_{\Omega_j} = \Omega_j(v)$ y v tiene peso par. Como cada Ω_j es un ciclo de longitud impar se tiene que para todo $l \in \Omega_j,\ v_l = 0,$ para cada $j \in \{1, \ldots, c+f\}$, esto es, $v = 0$. En consecuencia

$$C = F_\sigma(C) \oplus E_\sigma(C).$$

Además, si C es auto-dual, entonces por el lema 2.1.1 se tiene que $F_\sigma(C)$ también lo es. Luego, como

$$\dim_{\mathbb{F}_2} C = \dim_{\mathbb{F}_2} F_\sigma(C) + \dim_{\mathbb{F}_2} E_\sigma(C),$$

se tiene que

$$\dim_{\mathbb{F}_2} E_\sigma(C) = \frac{1}{2}n - \frac{1}{2}(n - c(p-1)) = \frac{1}{2}c(p-1).$$

Finalmente como el único vector de E fijado por σ es 0_C, se verifica que $p \mid 2^{\dim_{\mathbb{F}_2} E_\sigma(C)} - 1$ lo que indica que

$$2^{\dim_{\mathbb{F}_2} E_{\sigma(C)}} \equiv 1 \text{ mód } p.$$

En efecto, sea $c \in C,\ \sigma \in \mathrm{Aut}(C)$, entonces definamos:

$$O(c) := \{\ \sigma^i(c)\ \mid\ i\ \in\ \mathbb{Z}\ \},$$

dado que σ es de orden p, se sigue que $|O(c)|$ es uno o p, de hecho

$$|O(c)| := \begin{cases} 1, & c \in F_\sigma(C) \\ p, & c \notin F_\sigma(C), \end{cases}$$

para $c \in C$, más aún podemos definir una relación de equivalencia sobre C de la siguiente forma: para $c, c' \in C$

$$\begin{aligned} c \sim c' : &\Leftrightarrow c' \in O(c) \\ &\Leftrightarrow \exists i \in [0, p-1] \cap \mathbb{Z} \text{ tal que } c' = \sigma^i(c) \end{aligned}$$

y claramente las clases de equivalencia de C inducidas por esta relación corresponden a $O(c)$, con $c \in C$. Luego se verifica que

$$\dot{\bigcup}_{c \in C} O(c) = \left(\dot{\bigcup}_{c \in F_\sigma(C)} O(c)\right) \cup \left(\dot{\bigcup}_{c \notin F_\sigma(C)} O(c)\right).$$

De esta manera $|C| = |F_\sigma(C)| + s \cdot p$, donde $s \in \mathbb{Z}$, así como además se ha mostrado que $C = E_\sigma(C) \oplus F_\sigma(C)$ se tiene que:

$$2^{\dim_{\mathbb{F}_2} E_\sigma(C) + \dim_{\mathbb{F}_2} F_\sigma(C)} = 2^{\dim_{\mathbb{F}_2} F_\sigma(C)} + sp$$

o equivalentemente

$$2^{\dim_{\mathbb{F}_2} E_\sigma(C) + \dim_{\mathbb{F}_2} F_\sigma(C)} \equiv 2^{\dim_{\mathbb{F}_2} F_\sigma(C)} \text{ mód } p,$$

dado que $p \neq 2$ esto es equivalente a decir que:

$$2^{\dim_{\mathbb{F}_2} E_\sigma(C)} \equiv 1 \text{ mód } p.$$

Por otro lado, como $2^{(p-1)} \equiv 1 \,\text{mód}\, p$, por el pequeño teorema de Fermat, se sigue que $c/2 \in \mathbb{N}$, por consiguiente

$$c \equiv 0 \text{ mód } 2.$$

□

El lema anterior muestra que se puede obtener una matriz generadora para C, G, de la forma:

$$G = \begin{array}{c} \begin{array}{cc} \text{cíclos} & \text{puntos fijos} \end{array} \\ \left(\begin{array}{c|c} X & Y \\ \hline A & 0 \end{array}\right) \end{array} \begin{array}{l} \}\text{gen}(F_\sigma(C)) \\ \}\text{gen}(E_\sigma(C)). \end{array}$$

2.1.4 Lema. Sea C un $[n, k, d]$-código auto-dual binario con $\sigma \in \text{Aut}(C)$ de tipo $p - (c, f)$. Entonces se verifica que:

(a) Si $f \geq 2d$, entonces $2d - 2 - \log_2(d) \leq \frac{1}{2}(f + c)$.

(b) Si $f < 2d$, entonces $\frac{1}{2}(f-c) \leq 1 + \log_2(\frac{d}{2d-f})$.

(c) Si $pc \leq 2d$, entonces ó

I. $d = 4, p = 3, c = 2$ ó

II. $d = 4, p = 7, c = 1$.

DEMOSTRACIÓN. Empleando las cotas de Plotkin (ver [5])sobre un código con parámetros $[l, m, d']$, con $d' \geq d$ se tiene que:

$$2^m \leq 2\left(\frac{d}{2d-1}\right) \text{ , si } l < 2d \quad (1)$$

$$2^m \leq 4d \qquad \text{, si } l = 2d. \quad (2)$$

Para los casos (a) y (b), consideremos $T \subseteq X_c \cup X_f$, donde X_c, X_f son los conjuntos formados por una de las coordenadas de cada p ciclo y las coordenadas de los puntos fijos, respectivamente, que definen $\overline{F_\sigma(C)}$. Supongamos que $X_c \subseteq T$ y $|T| = c + t$, con $t \leq f$. Definamos así

$$C_T := \{(v_1, \ldots, v_{c+f}) \in \overline{F_\sigma(C)} \mid v_i = 0 \ \forall i \in T\}$$

y denotemos por $\dot{C}_T$ la versión de C_T agujereada en las coordenadas $i \in T$, luego la longitud de $\dot{C}_T$ es la longitud de $\overline{F_\sigma(C)}$ menos el número de elementos de T, esto es,

$$n - c(p-1) - (c+t) = f - t.$$

Dado que $\overline{F_\sigma(C)}$ es auto-dual

$$\begin{aligned}\dim_{\mathbb{F}_2} \dot{C}_T \geq & \frac{1}{2}(n - c(p-1)) - (c+t) \\ = & \frac{1}{2}(f-c) - t.\end{aligned}$$

Para el caso $f \geq 2d$ elegimos T tal que $t = f - 2d$. En consecuencia, la longitud de $\dot{C}_T$ sería $2d$, $\mathrm{d}(\dot{C}_T) \geq d$ y $\dim_{\mathbb{F}_2} \dot{C}_T \geq 2d - \frac{1}{2}(c+f)$, de (2):

$$\begin{aligned}2d - \frac{1}{2}(c+f) &\leq \log_2 4d \\ &= \log_2 2^2 + \log_2 d \\ &= 2 + \log_2 d,\end{aligned}$$

de donde se sigue (a)

Por otro lado si, $f < 2d$, tomamos T tal que $t = 0$. Entonces, $\dot{C}_T$ tiene longitud f, $\mathrm{d}(\dot{C}_T) \geq d$ y $\dim_{\mathbb{F}_2} \dot{C}_T \geq \frac{1}{2}(f-c)$, luego de (1) se sigue que:

$$\frac{1}{2}(f-c) \leq \log_2\ 2\left(\frac{d}{2d-f}\right),$$

con lo que se tiene (b).

Para (c) contemplemos dos casos. Primero, asumamos que $pc < \frac{3}{2}d$. Como $\dim_{\mathbb{F}_2} F_\sigma(C) < \dim_{\mathbb{F}_2} C$ existe $v \in C$ tal que $\sigma(v) \neq v$. Luego,

$$\sigma(v) + v \neq \mathbf{0}$$

y claramente $\sigma(v) + v \in E_\sigma(C)$. Si $\sigma(\sigma(v) + v) = \sigma(v) + v$, entonces $\sigma^2(v) = v$ y como p es impar se tiene que $v \in F_\sigma(C)$, esto es una contradicción. Así, definimos

$$w := \sigma(\sigma(v) + v) + (\sigma(v) + v) \neq \mathbf{0}.$$

Como

$$\mathrm{wt}(\sigma(\sigma(v) + v) = \mathrm{wt}(\sigma(v) + v)) \geq d$$

y estos vectores tienen soporte en las $pc < \frac{3}{2}d$ coordenadas de los p-ciclos, ambos ($\sigma(\sigma(v) + v)$ y $\sigma(v) + v$) tienen unos en más de $\frac{1}{2}d$ de sus posiciones. Así $\mathrm{wt}(w) < d$, lo que contradice que la distancia mínima sea d.

Supongamos ahora que $\frac{3}{2}d \leq pc \leq 2d$. Las cotas (1) y (2) aplicadas a $E_\sigma(C)$, definido en el lema 2.1.3, dan:

$$2^{\frac{(p-1)c}{2}} \leq\ 2\left(\frac{d}{2d-pc}\right)\ \text{, si } pc < 2d \quad (1')$$

$$2^{\frac{(p-1)c}{2}} \leq\ 4d \qquad\qquad \text{, si } pc = 2d. \quad (2')$$

Además como $\frac{3d}{2p} \leq c$, de (1') y (2'), se tiene que:

$$2^{\frac{d(p-1)}{4p}} \leq\ 4d. \qquad (3)$$

Dado que $\frac{p-1}{p}$ se minimiza para $p = 3$, se sigue que $2^{\frac{d}{2}} \leq 4d$, mas esto no se cumple para $d \geq 12$. Como además d debe ser par, se tiene entonces que $d \leq 10$. Si $d \in \{6, 8, 10\}$ y se analizan todas las posibilidades para p

y c que cumplan la suposición de que $\frac{3}{2}d \leq pc \leq 2d$, la única posibilidad que no elimina (1') y (2') son $d = 6, p = 3c = 4$.

Observemos este caso. Por hipótesis C es auto-dual con distancia mínima 6, cualesquiera cinco columnas de C son independientes. Por consiguiente, considerando primero $\Omega_1,\ \Omega_2,\ \Omega_3,\ \Omega_4$, existen vectores $v, w \in C$ de la forma:

$$v = 100\ 00* \ ***\ldots***$$

$$w = 000\ 01* \ ***\ldots***,$$

siendo los asteríscos valores indeterminados. Luego,

$$a := v + \sigma(v) = 110\ s0t \ ***\ldots 000$$

$$b := w + \sigma(w) = 000\ xyz \ ***\ldots 000,$$

con $xyz \in \{110, 011\}$ y $s = t$. Si $s = t = 1$, se puede reemplazar a por $a + \sigma^i(b)$ para algún i, llegando así a $s = t = 0$. Cada $*** \in \{000, 110, 101, 011\}$. Dado que el peso mínimo es seis, $*** \neq 000$. Rotando cíclicamente $\Omega_2,\ \Omega_3,\ \Omega_4$ de forma adecuada se puede tomar $b = 000\ 110\ 110\ 110\ 00\ldots0$. Sustituyendo a por $\sigma^i(a)$ y rotando cíclicamente Ω_1, se puede considerar $a|_{\Omega_3} = 110$, pero luego $\mathrm{wt}(a + b) = 4$, lo que contradice la distancia mínima supuesta.

De esta forma, $d \leq 4$. Si $d = 4$ se tienen los casos I. y II. de (c) Si $d = 2, p = 3$ y $c = 1$, se tendría que $\dim_{\mathbb{F}_2}(E_\sigma(C)) = 1$. Pero no hay código de dimensión uno con peso par y tres coordenadas preservadas por un 3-ciclo. □

2.1.5 Lema. Sea p un primo impar tal que $1 + x + \ldots + x^{p-1}$ es irreducible sobre $\mathbb{F}_2$. Sea $\mathcal{P}$ el conjunto de todos los polinomios de peso par en $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. Entonces $\mathcal{P}$ es un cuerpo con elemento identidad $x + x^2 + \ldots + x^{p-1}$. Además, multiplicar por $1 + x^2 + x^3 + \ldots + x^{p-1} \in \mathcal{P}$ corresponde a realizar un desplazamiento hacia la derecha módulo el ideal $\langle x^p - 1\rangle$.

Demostración. Nótese inicialmente que $\mathcal{P}$ está bien definido, ya que dos representantes de clases laterales en $\mathbb{F}_2[x]/\langle x^p - 1\rangle$ tienen ambos peso par o impar. En consecuencia $\mathcal{P}$ es cerrado bajo adición y multiplicación.

Sean $f, g \in \mathcal{P}$ con

$$fg \equiv 0 \text{ mód } \langle x^p - 1\rangle.$$

Entonces, $(1+x)$ divide a f y $(1+x)$ divide a g. Como también el polinomio $(1+x+\ldots+x^{p-1})$ divide a fg, se verifica que $1+x+\ldots+x^{p-1}$ divide a f ó divide a g, por ser $1+x+\ldots+x^{p-1}$ irreducible. Así $f \equiv 0$ mód $\langle x^p-1\rangle$ ó $g \equiv 0$ mód $\langle x^p-1\rangle$.

Supongamos que $f \in \mathcal{P}$. Entonces $f = (1+x)g$, para algún $g \in \mathbb{F}_2[x]/\langle x^p-1\rangle$ y

$$\begin{aligned} f(1+x+\ldots+x^{p-1}) &= g(x^p-1) \\ &\equiv 0 \text{ mód } \langle x^p-1\rangle. \end{aligned}$$

Entonces

$$f \cdot 1 \equiv f(x+\ldots+x^{p-1}) \text{ mód } \langle x^p-1\rangle$$

y $x+\ldots+x^{p-1}$ es el elemento identidad de $\mathcal{P}$ y es así un cuerpo. También fx es f desplazado cíclicamente a la derecha, entonces la multiplicación por el polinomio $1+x^2+x^3+\ldots+x^{p-1}$ corresponde a un desplazamiento cíclico a la derecha. □

Introduzcamos otra notación. Supongamos que C es auto-dual con $C = F_\sigma(C) \oplus E_\sigma(C)$, como en el lema 2.1.3. Sea $v \in E_\sigma(C)$ con

$$v|_{\Omega_i} = a_1 \ldots a_p$$

y definamos

$$f(v|_{\Omega_i}) := a_1 + a_2x + \ldots + a_px^{p-1} \text{ para } i \in \{1,\ldots,c\}.$$

Hagamos que f induzca por componentes una función de $E_\sigma(C)^*$ sobre $(\mathbb{F}_2[x]/\langle x^p-1\rangle)^c$, donde $E_\sigma(C)^*$ corresponde a $E_\sigma(C)$ con las coordenadas correspondientes a los puntos fijos borradas. Por ende, si las condiciones del lema anterior se tienen, entonces $\mathcal{P} = \mathbb{F}_{2^{p-1}}$. De hecho se tiene el siguiente lema.

2.1.6 Lema. Supongamos que C es código auto-dual y $1+x+\ldots+x^{p-1}$ es irreducible sobre $\mathbb{F}_2$. Entonces $f(E_\sigma(C)^*) \leq \mathbb{F}_{2^{p-1}}^c$ y su dimensión es $\frac{c}{2}$. En particular c es par.

Demostración. Claramente f preserva la suma. Sea

$$\beta := 1 + x^2 + \ldots + x^{p-1} \in \mathbb{F}_2[x]/\langle x^p-1\rangle.$$

Del lema anterior al multiplicar un polinomio de peso par por β^i corresponde a desplazarlo cíclicamente i veces a derecha. Entonces

$$1 + \beta = 1 + x,$$

es decir, $\{1+\beta, \beta+\beta^2, \ldots, \beta^{p-2}+\beta^{p-1}\}$ es una base para $\mathbb{F}_{2^{p-1}}$ sobre $\mathbb{F}_2$.

Por consiguiente, como

$$\beta^i f(v) = f(\sigma^i(v)) \in f(E_\sigma(C)^*) \text{ para todo } v \in E_\sigma(C)^*,$$

se tiene que $f(E_\sigma(C)^*)$ es cerrado bajo la multiplicación por escalares inducida desde $\mathbb{F}_{2^{p-1}}$. Ahora del lema 2.1.3 se tiene que

$$\begin{aligned}\dim_{\mathbb{F}_2} E_\sigma(C)^* &= \dim_{\mathbb{F}_2} E_\sigma(C) \\ &= \frac{1}{2}c(p-1).\end{aligned}$$

Luego, si $\dim_{\mathbb{F}_{2^{p-1}}} f(E_\sigma(C)^*) = k$, entonces $(2^{p-1})^k = 2^{\frac{1}{2}c(p-1)}$ de donde se sigue que $k = \frac{1}{2}c$. □

2.1.7 Lema. Si $p = 3$ y C es un código auto-dual doblemente par, entonces $f(E_\sigma(C)^*)$ es auto-dual sobre $\mathbb{F}_4$ bajo el producto interior definido por

$$(u|v) := \sum_{i=1}^{c} u_i v_i^2$$

para todo $u, v \in \mathbb{F}_{2^{p-1}}^c$. Se verifica además que C tiene distancia mínima por lo menos $\frac{d}{2}$.

Demostración. Como C es doblemente par, si $v \in E_\sigma(C)^*$, entonces

$$\begin{aligned}&\mathrm{wt}(f(v)) = \frac{1}{2}\mathrm{wt}(v), \text{ es decir,} \\ &\mathrm{wt}(f(v)) \equiv 0 \text{ mód } 2.\end{aligned}$$

Por el lema anterior y [13] se tiene que $f(E_\sigma(C)^*)$ es auto-dual y $\mathrm{d}(f(E_\sigma(C)^*)) \geq \frac{d}{2}$. □

2.1.8 Corolario. Si C es un código auto-dual doblemente par y $p = 3$, entonces $\frac{d}{2} \leq 2\lfloor \frac{c}{6} \rfloor + 2$. Si además C es extremal, entonces $\frac{n}{24} \leq \lfloor \frac{c}{6} \rfloor$.

Demostración.De [13] un código auto-dual cuaternario con parámetros $\left(c, \frac{c}{2}\right)$ tiene distancia mínima a lo más $2\lfloor \frac{c}{6} \rfloor + 2$. □

2.1.9 Lema. Si $p = 5$ y C es un código auto-dual doblemente par, Entonces $f(E_\sigma(C)^*)$ es auto-dual sobre $\mathbb{F}_{16}$ bajo el producto interior dado por

$$(u|v) := \sum_{i=1}^{c} u_i v_i^4$$

para todo $u, v \in \mathbb{F}_{2^{p-1}}^c$.

Demostración. Consideremos inicialmente la siguiente tabla para $\mathbb{F}_{16} - \{0\}$, donde $\alpha = 1 + x \in \mathbb{F}_2[x]/\langle x^5 - 1\rangle$ es un elemento primitivo.

1	01111	α	11000	α^2	10100
α^3	11110	α^4	10001	α^5	01001
α^6	11101	α^7	00011	α^8	10010
α^9	11011	α^{10}	00110	α^{11}	00101
α^{12}	10111	α^{13}	01100	α^{14}	01010

Tabla I
$\mathbb{F}_{16} \subseteq \mathbb{F}_2[x]/\langle x^5 - 1\rangle$

Supongamos $f(u) \in f(E_\sigma(C)^*)$. Nótese que α satisface el polinomio $1 + x^3 + x^4$. También, multiplicar por α^{12} corresponde a realizar un desplazamiento cíclico hacia la derecha. Para $i \in \{0, 1, 2\}$ sea a_i el número de componentes en $f(u)$ que se pueden expresar de la forma $\alpha^i(\alpha^{12j})$ para algún $j \in \{1, 2, 3, 4, 5\}$. Como

$$(\alpha^{12j})(\alpha^{12j})^4 = (\alpha^{60j}) = 1,$$

se tiene que $(f(u)|f(u)) = a_0 + a_1\alpha^5 + a_2\alpha^{10}$. Ahora, como

$$\mathrm{wt}(u) = \ 4a_0 + 2a_1 + 2a_2 \equiv \ 0 \text{ mód } 4,$$

se sigue que

$$a_1 + a_2 \equiv \ 0 \text{ mód } 2.$$

Adicionalmente, como

$$\mathrm{wt}(u + \sigma(u)) = \ 2a_0 + 2a_1 + 4a_2 \equiv \ 0 \text{ mód } 4,$$

se tiene que

$$a_0 + a_1 \equiv \ 0 \text{ mód } 2,$$

lo que a su vez implica que $a_0 \equiv\ a_1 \equiv\ a_2$ mód 2 y así

$$(f(u)|f(u)) = a_0(1 + \alpha^5 + \alpha^{10}) = 0.$$

Entonces $(x|x) = 0$ para cada $x \in f(E_\sigma(C)^*)$. Si $y \in f(E_\sigma(C)^*)$,

$$\begin{aligned} 0 &= (x + \alpha^i y|x + \alpha^i y) \\ &= (x|x) + \alpha^i(y|x) + \alpha^{4i}(x|y) + (\alpha y|\alpha y) \\ &= \alpha^i(y|x) + \alpha^{4i}(x|y). \end{aligned}$$

Entonces,$(y|x) = \alpha^{3i}(x|y)$ debe ser cero ya que α^{3i} varía con i. De esta manera como $f(E_\sigma(C)^*)$ es un $\left(c, \frac{c}{2}\right)$-código y $(\cdot|\cdot)$ es no degenerado, se sigue que $f(E_\sigma(C)^*)$ es auto-dual. □

Así también se ha mostrado el siguiente corolario.

2.1.10 Corolario. Si $p = 5$, C es un código auto-dual doblemente par y Ω_i es reordenado de forma cíclica, entonces $f(E_\sigma(C)^*)$ también es auto-dual. Además, cada palabra de código en $f(E_\sigma(C)^*)$ con a_i componentes de la forma $\alpha^i(\alpha^{12j})$ cumple que $a_0 \equiv a_1 \equiv a_2$ mód 2.

2.2. Exclusión de algunos primos del orden del grupo de automorfismos

A continuación se hace uso de las condiciones establecidas en la sección anterior, para caracterizar el grupo de automorfismos de los siguientes códigos tipo II, haciendo uso de la contrarrecíproca del:

I. Lema 2.1.4 (a)

II. Lema 2.1.4 (b)

III. Lema 2.1.4 (c)

IV. Corolario 2.1.2.

V. Lema 2.1.6.

VI. Corolario 2.1.8.

Además, las posibilidades cuando $p = 2$ quedan excluidas dado que las técnicas empleadas consideran que p sea un primo impar.

2.2.1. Caso [24,12,8]

Dado que éste código C es de longitud 24, si p es el orden de $\sigma \in \mathrm{Aut}(C)$, entonces $p \leq 23$. De esta manera los tipos posibles para σ son:

p	c	f
2	12	0
	11	2
	10	4
	9	6
	8	8
	7	10
	6	12
	5	14
	4	16
	3	18
	2	20

p	c	f
2	1	22
3	8	0
	7	3
	6	6
	5	9
	4	12
	3	15
	2	18
	1	21
5	4	4
	3	9

p	c	f
5	2	14
	1	19
7	3	3
	2	10
	1	17
11	2	2
	1	13
13	1	11
17	1	7
19	1	5
23	1	1

De estos tipos a continuación se relacionarán aquellos excluidos por las razones enunciadas al inicio de la sección:

p	c	f	Razón
3	7	3	IV.
3	5	9	II., III., V.
3	4	12	II., III., VI.
3	3	15	II., III., V.
3	2	18	I., III., VI.

p	c	f	Razón
3	1	21	III. V.
5	3	9	II., III., V.
5	2	14	II., III.
5	1	19	I., III. IV. V.
7	2	10	II., III.

p	c	f	Razón
7	1	17	III.
11	1	13	II., III., V.
13	1	11	II., III., IV., V.
17	1	7	II.
19	1	5	II., V.

Así las únicas posibilidades restantes son:

p	3	3	5	7	11	23
c	8	6	4	3	2	1
f	0	6	4	3	2	1

2.2.2. Caso [48,24,12]

Dado que éste código C es de longitud 48, si p es el orden de $\sigma \in \mathrm{Aut}(C)$, entonces $p \leq 47$. De esta manera los tipos posibles para σ son:

p	c	f
2	24	0
	23	2
	22	4
	21	6
	20	8
	19	10
	18	12
	17	14
	16	16
	15	18
	14	20
	13	22
	12	24
	11	26
	10	28

p	c	f
2	9	30
	8	32
	7	34
	6	36
	5	38
	4	40
	3	42
	2	44
	1	46
3	16	0
	15	3
	14	6
	13	9
	12	12
	11	15

p	c	f
3	10	18
	9	21
	8	24
	7	27
	6	30
	5	33
	4	36
	3	39
	2	42
	1	45
5	9	3
	8	8
	7	13
	6	18
	5	23

p	c	f
5	4	28
	3	33
	2	38
	1	43
7	6	6
	5	13
	4	20
	3	27
	2	34
	1	41
11	4	4
	3	15
	2	26
	1	37
13	3	9

p	c	f
13	2	22
	1	35
17	2	14
	1	31
19	2	10
	1	29
23	2	2
	1	25
29	1	19
31	1	17
37	1	11
41	1	7
43	1	5
47	1	1

De estos tipos a continuación se relacionarán aquellos excluidos por las razones enunciadas al inicio de la sección:

p	c	f	Razón
3	15	3	V.
	13	9	V.
	11	15	II., V.
	10	18	II., VI.
	9	21	II., V.
	8	24	I., III., VI.
	7	27	I., III., V.
	6	30	I., III., VI.
	5	33	III., V.
	4	36	III., VI.
	3	39	III., V.
	2	42	III., VI.
	1	45	III., V.
5	9	3	IV., V.

p	c	f	Razón
5	7	13	II., IV., V.
	6	18	II.
	5	23	II., IV., V.
	4	28	I., III.
	3	33	I., III., IV., V.
	2	38	III.
	1	43	III., IV., V.
7	5	13	II.
	4	20	II.
	3	27	I., III.
	2	34	I., III.
	1	41	III.
11	3	15	II., V.
	2	26	I., III.

p	c	f	Razón
11	1	37	III., V.
13	3	9	II., IV., V.
	2	22	II.
	1	35	I., III., IV., V.
17	2	14	II.
	1	31	I., III.
19	2	10	II.
	1	29	I., III., V.
23	1	25	I., III.
29	1	19	II., IV., V.
31	1	17	II.
37	1	11	II., IV., V.
41	1	7	II.
43	1	5	II.

De esta manera las posibilidades restantes son:

p	3	3	3	5	7	11	23	47
c	16	14	12	8	6	4	2	1
f	0	6	12	8	6	4	2	1

2.2.3. Caso [120,60,24]

Dado que éste código C es de longitud 120, si p es el orden de $\sigma \in \mathrm{Aut}(C)$, entonces $p \leq 113$. De esta manera los tipos posibles para σ son:

p	c	f
2	60	0
	59	2
	58	4
	57	6
	56	8
	55	10
	54	12
	53	14
	52	16
	51	18
	50	20
	49	22
	48	24
	47	26
	46	28
	45	30
	44	32
	43	34
	42	36
	41	38
	40	40
	39	42
	38	44
	37	46
	36	48
	35	50
	34	52
	33	54
	32	56
	31	58
	30	60
	29	62
	28	64
	27	66
	26	68
	25	70
	24	72
	23	74
	22	76
	21	78
	20	80
	19	82
	18	84

p	c	f
2	17	86
	16	88
	15	90
	14	92
	13	94
	12	96
	11	98
	10	100
	9	102
	8	104
	7	106
	6	108
	5	110
	4	112
	3	114
	2	116
	1	118
3	40	0
	39	3
	38	6
	37	9
	36	12
	35	15
	34	18
	33	21
	32	24
	31	27
	30	30
	29	33
	28	36
	27	39
	26	42
	25	45
	24	48
	23	51
	22	54
	21	57
	20	60
	19	63
	18	66
	17	69
	16	72
	15	75

p	c	f
3	14	78
	13	81
	12	84
	11	87
	10	90
	9	93
	8	96
	7	99
	6	102
	5	105
	4	108
	3	111
	2	114
	1	117
5	24	0
	23	5
	22	10
	21	15
	20	20
	19	25
	18	30
	17	35
	16	40
	15	45
	14	50
	13	55
	12	60
	11	65
	10	70
	9	75
	8	80
	7	85
	6	90
	5	95
	4	100
	3	105
	2	110
	1	115
7	17	1
	16	8
	15	15
	14	22
	13	29

p	c	f
7	12	36
	11	43
	10	50
	9	57
	8	64
	7	71
	6	78
	5	85
	4	92
	3	99
	2	106
	1	113
11	10	10
	9	21
	8	32
	7	43
	6	54
	5	65
	4	76
	3	87
	2	98
	1	109
13	9	3
	8	16
	7	29
	6	42
	5	55
	4	68
	3	81
	2	94
	1	107
17	7	1
	6	18
	5	35
	4	52
	3	69
	2	86
	1	103
19	6	6
	5	25
	4	44
	3	63
	2	82

p	c	f
19	1	101
23	5	5
	4	28
	3	51
	2	74
	1	97
29	4	4
	3	33
	2	62
	1	91
31	3	27
	2	58
	1	89
37	3	9
	2	46
	1	83
41	2	38
	1	79
43	2	34
	1	
47	2	26
	1	
53	2	14
	1	
59	2	2
	1	
61	2	59
	1	
67	1	53
71	1	49
73	1	47
79	1	41
83	1	37
89	1	31
97	1	23
101	1	19
103	1	17
107	1	13
109	1	11
113	1	7

De estos tipos a continuación se relacionarán aquellos excluidos por las razones enunciadas al inicio de la sección:

p	c	f	Razón
3	39	3	V.
	37	9	V.
	35	15	V.
	33	21	V.
	31	27	V.
	29	33	II., V.
	28	36	II., VI.
	27	39	II., V.
	26	42	II., VI.
	25	45	II., V.
	24	48	I., VI.
	23	51	I., V.
	22	54	I., VI.
	21	57	I., V.
	20	60	I., VI.
	19	63	I., V.
	18	66	VI.
	17	69	V.
	16	72	III., VI.
	15	75	III., V.
	14	78	III., VI.
	13	81	III., V.
	12	84	III., VI.
	11	87	III., V.
	10	90	III., VI.
	9	93	III., V.
	8	96	III., VI.
	7	99	III., V.
	6	102	III., VI.
	5	105	III., V.
	4	108	III., VI.
	3	111	III., V.
	2	114	III., VI.
	1	117	III., V.
5	23	5	IV., V.
	21	15	IV., V.
	19	25	II., IV., V.
	18	30	II.
	17	35	II., IV., V.
	16	40	II.
	15	45	II., IV., V.
	14	50	I.
	13	55	I., IV.,V.
	12	60	I.

p	c	f	Razón
5	11	65	I., IV.,V.
	10	70	I.
	9	75	III., IV., V.
	8	80	III.
	7	85	III., IV., V.
	6	90	III.
	5	95	III., IV., V.
	4	100	III.
	3	105	III., IV., V.
	2	110	III.
	1	115	III., IV., V.
7	14	22	II.
	13	29	II.
	12	36	II.
	11	43	II.
	10	50	I.
	9	57	I.
	8	64	I.
	7	71	I.
	6	78	III.
	5	85	III.
	4	92	III.
	3	99	III.
	2	106	III.
	1	113	III.
11	9	21	II., V.
	8	32	II.
	7	43	II., V.
	6	54	I.
	5	65	I., V.
	4	76	I.,III.
	3	87	III., V.
	2	98	III.
	1	109	III., V.
13	9	3	IV., V.
	8	16	II.
	7	29	II., IV., V.
	6	42	II.
	5	55	I., IV.,V.
	4	68	I.
	3	81	III., IV., V.
	2	94	III.
	1	107	III., IV., V.
17	6	18	II.

p	c	f	Razón
17	5	35	II.
	4	52	I.
	3	69	I.
	2	86	III.
	1	103	III.
19	5	25	II., V.
	4	44	II.
	3	63	I., V.
	2	82	III.
	1	101	III., V.
23	4	28	II.
	3	51	I.
	2	74	I.,III.
	1	97	III.
29	3	33	II., IV., V.
	2	62	I.
	1	91	III., IV., V.
31	3	27	II.
	2	58	I.
	1	89	III.
37	3	9	II., IV., V.
	2	46	II.
	1	83	III., IV., V.
41	2	38	II.
	1	79	I.,III.
43	2	34	II.
	1	77	I.,III.
47	2	26	II.
	1	73	I.,III.
53	2	14	II.
	1	67	I., IV., V.
59	1	61	I., V.
61	1	59	I., IV.,V.
67	1	53	I.,V.
71	1	49	I.
73	1	47	II.
79	1	41	II.
83	1	37	II., V.
89	1	31	II.
97	1	23	II.
101	1	19	II., IV.,V.
103	1	17	II.
107	1	13	II.,V.
109	1	11	II., IV.
113	1	7	II.

Luego las posibilidades restantes corresponden a:

p	3	3	3	3	3	3	5	5	5	7	7	7	11	17	19	23	29	59
c	40	38	36	34	32	30	24	22	20	17	16	15	10	7	6	5	4	2
f	0	6	12	18	24	30	0	10	20	1	8	15	10	1	6	5	4	2

Capítulo 3

Análisis de algunos tipos restantes

En el presente capítulo cuando se escriba $\bar{0}$, $\bar{1}$ se entenderán como los vectores con todas las coordenadas 0 ó 1, respectivamente, de tamaño apropiado y por $\bar{I}_n$ se entenderá como la matriz obtenida de la identidad de tamaño $n \times n$ reemplazando 1 por $\bar{1}$ y 0 por $\bar{0}$, es decir, si $\bar{0}$ y $\bar{1}$ son de longitud p, entonces $\bar{I}_n$ es una matriz de tamaño $n \times np$. A continuación se dan unas definiciones necesarias para el estudio de algunos de los tipos analizados a continuación.

3.1. Caso [24,12,8]

Denotemos por $C = G_{24}$ el código de Golay de longitud 24. Para este caso un resultado trascendental de la teoría de automorfismos de códigos tipo II es que el $\mathrm{Aut}(C) \cong M_{24}$, donde M_{24} es el grupo esporádico simple de Mathieu, que tiene elementos del tipo 3-(6,6) y 3-(8,0). Se analizaran estos casos; considerando técnicas que se explorarán con más detalle en el código [48,24,12].

3.1.1 Definición. Sea C un código de longitud n. Entonces:

(a) Decimos que $\{i, j \mid 1 \leq i, j \leq n, i \neq j\}$, una pareja de coordenadas del código, es un **duo**.

(b) Decimos que un **clúster** es un conjunto de duos disjuntos tal que un par de duos distintos forman el soporte de un vector de peso 4.

(*c*) Un *d*-**conjunto** para un cluster dado es un subconjunto de coordenadas tales que hay exactamente un elemento de cada duo del cluster en él.

(*d*) Un **conjunto definitivo** para un código es un cluster y un *d*-conjunto con la condición de que el código es generado por los vectores de peso cuatro resultantes del cluster y por el vector cuyo soporte es el *d*- conjunto.

3.1.1. Tipo $3-(6,6)$

Supongamos que $\sigma \in \mathrm{Aut}(C)$ es del tipo 3-(6,6). Debido a que $\overline{F_\sigma(C)}$ no puede tener vector alguno de peso 2 se tiene que $\overline{F_\sigma(C)} = B_{12}$. (Ver [14]) Sean X_c, X_f las coordenadas de los 3-ciclos y de los puntos fijos, respectivamente. Veamos que B_{12} tiene un conjunto definitivo. Si d es un duo con $d \subset X_c$ o $d \subset X_f$, entonces se llega a una contradicción como se muestra para el código [48,24,12]. Por lo tanto cada duo contiene exactamente un elemento de X_c y X_f, pudiéndose considerar los duos de la forma $\{\Omega_i, i\}$, siendo $\Omega_1, \ldots, \Omega_6$ los 3-ciclos de σ. Así el $d-$ conjunto es $\{\Omega_i, 2, 3, 4, 5, 6\}$ ó $\{1, 2, 3, 4, 5, 6\}$; pero este último genera una palabra de código de peso 6 en $F_\sigma(C)$.

La acción natural del Sym(6) sobre X_c, y análogamente sobre X_f, preserva los duos y envía el $d-$ conjunto en otro que define al mismo código. Por consiguiente al adjuntar $f(E_\sigma(C)^*)$ no importa la manera como se organizan las coordenadas.

De [13], dado que $f(E_\sigma(C)^*)$ tiene distancia mínima por lo menos 4, se sigue que $f(E_\sigma(C)^*) = E_6$. La única forma como se podría obtener un vector de peso 4 a través de esta construcción, sería si vectores de peso cuatro en $\overline{F_\sigma(C)}$ y $f(E_\sigma(C)^*)$ tuviesen el mismo soporte, lo que no es posible dado que por definición vectores de peso 4 en $\overline{F_\sigma(C)}$ tienen como soporte la unión de dos duos. Para $\sigma = (1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11\,12)(13\,14\,15)(16\,17\,18)(19)(20)(21)(22)(23)(24)$ del tipo 3-(6,6) se obtiene:

$$G_{F_\sigma(C)} = \begin{pmatrix} 111111000000000000110000 \\ 000111111000000000011000 \\ 000000111111000000001100 \\ 000000000111111000000110 \\ 000000000000111111000011 \\ 111000000000000000011111 \end{pmatrix}$$

$$G_{E_\sigma(C)} = \begin{pmatrix} 011000000011110110000000 \\ 000011000110011110000000 \\ 000000011110110011000000 \\ 101000000101011011000000 \\ 000101000011101011000000 \\ 000000101011011101000000 \end{pmatrix}$$

Con lo que del lema 2.1.3 se obtiene una matriz G generadora del código, de la forma:

$$G = \begin{pmatrix} 111111000000000000110000 \\ 000111111000000000011000 \\ 000000111111000000001100 \\ 000000000111111000000110 \\ 000000000000111111000011 \\ 111000000000000000011111 \\ \hline 011000000011110110000000 \\ 000011000110011110000000 \\ 000000011110110011000000 \\ 101000000101011011000000 \\ 000101000011101011000000 \\ 000000101011011101000000 \end{pmatrix}$$

3.1.2. Tipo $3-(8,0)$

Supongamos que $\sigma \in \mathrm{Aut}(C)$ es del tipo 3-(8,0). Del lema 2.1.1, $\overline{F_\sigma(C)} \cong A_8$, donde A_8 denota el código extendido de Hamming con parámetros [8,4,4], y por [13], $f(E_\sigma(C)) \cong A_8$ también. Seleccionemos el conjunto definitivo de $f(E_\sigma(C))$ como

$$\{\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{1,3,5,7\}\}.$$

Se construyen los duos de $F_\sigma(C)$ con la condición de que vectores de peso 4 de $f(E_\sigma(C))$ y $\overline{F_\sigma(C)}$ no compartan el mismo soporte. Por el lema 3.2.14 se puede suponer que $\overline{F_\sigma(C)}$ tiene duos $\{1,2\},\{3,x\}$, con $x \neq 4$. Debido a que $\mathrm{Aut}(f(E_\sigma(C)))$ contiene a (5,6)(7,8), (5,7)(6,8) se puede suponer que $x = 5$ y se tiene el duo $\{4,y\}$, donde y es 7 u 8. Y como $\mathrm{Aut}(f(E_\sigma(C)))$ contiene a (1,2)(7,8), se puede suponer en particular $y = 7$. Entonces $\{6,8\}$ es el duo faltante. El $d-$ conjunto $\{1,5,4,8\}$ no resulta, con lo que el d- conjunto ha de ser $\{1,3,4,8\}$. Para $\sigma =$

(1 2 3)(4 5 6)(7 8 9)(10 11 12)(13 14 15)(16 17 18)(19 20 21)(22 23 24) del tipo 3-(8,0) se obtiene:

$$G_{F_\sigma(C)} = \begin{pmatrix} 111111111000111000000000 \\ 000000111111111000111000 \\ 000000000111000111111111 \\ 111000111111000000000111 \end{pmatrix}$$

$$G_{E_\sigma(C)} = \begin{pmatrix} 011011011011000000000000 \\ 000000011011011011000000 \\ 000000000000011011011011 \\ 011000011000011000011000 \\ 101101101101000000000000 \\ 000000101101101101000000 \\ 000000000000101101101101 \\ 101000101000101000101000 \end{pmatrix}$$

Con lo que del lema 2.1.3 se obtiene una matriz G generadora del código, de la forma:

$$G = \left(\begin{array}{c} 111111111000111000000000 \\ 000000111111111000111000 \\ 000000000111000111111111 \\ 111000111111000000000111 \\ \hline 011011011011000000000000 \\ 000000011011011011000000 \\ 000000000000011011011011 \\ 011000011000011000011000 \\ 101101101101000000000000 \\ 000000101101101101000000 \\ 000000000000101101101101 \\ 101000101000101000101000 \end{array}\right)$$

3.2. Caso [48,24,12]

A continuación se analizarán los casos restantes para establecer cuáles son posibles tipos para automorfismos de un código tipo II con parámetros [48,24,12].

3.2.1. Tipo $47-(1,1)$:

3.2.1 Teorema. Si C es un código tipo II de parámetros [48,24,12] con $\sigma \in \mathrm{Aut}(C)$ del tipo $47-(1,1)$, entonces $C \cong Q$.

Demostración. Sea C^* él código obtenido de C borrando la coordenada correspondiente al punto fijo de σ. Luego C se obtiene de C^* agregándole un bit de control de paridad. De esta manera C^* es cíclico y por [11], fig. 7.1, los únicos códigos cíclicos de parámetros $[47,24]$ son los códigos definidos en 1.2.5 como Q y N. Estos son equivalentes y por ende, $C \cong Q$. □

3.2.2. Tipo $23-(2,2)$:

3.2.2 Definición. Sea $M \in \mathbb{F}_q^{n\times n}$, decimos que M es una **matriz circulante** si es de la forma

$$\begin{pmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & \ddots & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & \ddots & \ddots & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{pmatrix},$$

es decir, dada su primera columna cada una de las siguientes es una permutación cíclica respecto a la anterior. También suele definirse este concepto no para permutaciones de columnas respecto a las anteriores, sino de filas.

Ordenamos $\sigma = (1,2,\ldots,23)(f_1)(1',2',\ldots,23')(f_1')$, con f_1 un punto fijo de σ y ordenamos las coordenadas de la misma forma, es decir, $1,2,\ldots,23,f_1,1',2',\ldots,23',f_1'$. Como $\overline{F_\sigma(C)}$ es un código auto-dual de parámetros $[4,2]$, reordenando los puntos fijos, de ser necesario, se puede hacer que $\overline{F_\sigma(C)}$ sea generado por

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

Entonces $F_\sigma(C)$ es generado por $v_1 = (\bar{1}\ 1\ \bar{0}\ 0),\ v_2 = (\bar{0}\ 0\ \bar{1}\ 1)$, donde $(\bar{0},\ \bar{1}$ son vectores de longitud 23. Definamos

$$E_1 := \{u \in E_\sigma(C) \mid u_j = 0,\ \text{para } j = 1,\ldots,23,f_1,f_1'.\},$$

de esta manera obtengamos E_1^* de borrar en E_1 las coordenadas $1, \ldots, 23, f_1, f_1'$. Ahora E_1^* es un código cíclico de longitud 23 con distancia mínima por lo menos 12. De la cota de Plotkin, si $k = \dim_{\mathbb{F}_2} E_1^*$, entonces

$$2^k \leq 2\left(\frac{12}{24-23}\right) = 24,$$

lo que implica $k \leq 4$. Debido a que la permutación $\tau = (1', 2', \ldots, 23')$ actúa sobre los vectores de E_1^* en órbitas de longitud 1 o 23 y como además E_1^* es un código de peso par, sólo $\{\bar{0}\}$ es una órbita de longitud 1, de donde se tendría $2^k \equiv 1$ mód 23 o $k = 0$. De esta forma $E_1^* = \{\bar{0}\}$ y la matriz generadora de E tiene la forma

$$[B\ \bar{0}^T\ D\ \bar{0}^T],$$

donde $B,\ D \in \mathbb{F}_2^{22\times 23}$. Si $\mathrm{Rang}(B) < 22$, entonces $E_1^* \neq \{\bar{0}\}$. Así, reduciendo el código $E_\sigma(C) \oplus (v_1 + E_\sigma(C))$ por filas se obtiene una matriz generadora para C de la forma:

$$\left(\begin{array}{ccc|c|ccc|c} 0 & \ldots & 0 & 0 & 1 & \ldots & 1 & 1 \\ \hline & & & 1 & & & & 0 \\ & I_{23} & & \vdots & & A & & \vdots \\ & & & 1 & & & & 0 \end{array}\right),$$

dónde las últimas 23 filas generan a $E_\sigma(C) \oplus (v_1 + E_\sigma(C))$. Si llamamos a las filas de esta matriz $v_2, w_1, \ldots, w_{23}$, entonces $w_i - \sigma^{i-1}(w_1) \in E_1$, que implica $w_i = \sigma^{i-1}(w_1)$. Con lo que A es una matriz circulante.

Supongamos que $w_1 = 1\ 0\ \ldots 0\ 1\ a_1\ \ldots\ a_{23}\ 0$, donde $a_1\ \ldots\ a_{23} =: a$ es la primera fila de A. El siguiente lema limita las posibilidades para tomar a.

3.2.3 Lema. Sea $\tau = (1, \ldots, p)$ y $v \in \mathbb{F}_2^p$, donde v tiene una cadena de s ceros y s unos, en particular si $v_1 = v_p$ se considerarán las cadenas iniciales y finales de v como una sola. Entonces $\mathrm{wt}(v + \tau(v)) = 2s$.

Demostración. El vector $v + \tau(v)$ sólo tiene un 1 en las coordenadas i donde $v_i \neq \tau(v)_i$. Luego, i debe ser una cadena que inicia una coordenada de ceros o de unos, pues son las únicas posiciones que al desplazarse una vez no coincidirán con el mismo valor. □

3.2.4 Teorema. Si C es un código doblemente par con parámetros $[48, 24, 12]$ y $\sigma \in \mathrm{Aut}(C)$ del tipo $23 - (2, 2)$, entonces $C \cong Q$.

DEMOSTRACIÓN. Claramente se pueden ordenar las coordenadas de tal forma que $a_1 = 1,\ a_{23} = 0$ y que la cadena de 1's más larga en a inicie en a_1. Si hay r cadenas de unos en a, del **lema anterior** se sigue que

$$\mathrm{wt}(w_1 + \sigma(w_1)) = 2 + 2r,$$

con lo que se tiene que $r \in \{5,\ 7,\ 9,\ 11\}$. También

$$\mathrm{wt}(w_1 + v_2 + \sigma(w_1)) = 2 + (24 - 2r),$$

de donde se sigue que $r \notin \{9,\ 11\}$. Como

$$\mathrm{wt}(w_1) = 2 + \mathrm{wt}(a) \text{ y}$$

$$\mathrm{wt}(w_1 + v_2) = 2 + (24 - \mathrm{wt}(a)),$$

se verifica que $\mathrm{wt}(a) = 10, 14$. Análogamente si $\tau = (1',\ \ldots,\ 23')$, se prueba que

$$\mathrm{wt}(w_1 + \sigma^i(w_1)) = 2 + \mathrm{wt}(a + \tau^i(a)),\ \text{y}$$

$$\mathrm{wt}(v_2 + w_1 + \sigma^i(w_1)) = 2 + (24 - \mathrm{wt}(a + \tau^i(a))),$$

y de esta forma $\mathrm{wt}(a + \tau^i(a)) = 10,\ 14$.

Entonces hay cuatro casos a considerar correspondientes a los valores de $\mathrm{wt}(a)$ y r. Primero se descompone $\mathrm{wt}(a)$ en r cantidades no negativas correspondientes a las longitudes de cada cadena de unos, apareciendo la más extensa primero. Dado que aplicar σ^{-1} es equivalente a realizar una desplazamiento en sentido contrario, se pueden omitir algunas de estas posibilidades.

Ahora, si se descompone también $23 - \mathrm{wt}(a)$ en r factores no negativos que representen por el contrario las longitudes de las cadenas de ceros y se analizan las combinaciones posibles, de forma computacional se obtiene que entre los 24566 vectores considerables, luego de verificar que $\mathrm{wt}(a + \tau^i(a))$ es 10 o 14 para cada i quedan dos, uno de peso 10 y otro de peso 14. Basta además considerar solo cuando $1 \leq i \leq 11$, pues

$$\mathrm{wt}(a + \tau^i(a)) = \mathrm{wt}(\tau^j(a) + \tau^{i+j}(a)),$$

con $i + j = 23$. En efecto, los vectores resultantes, omitiendo los equivalentes al reemplazar σ por σ^i y reordenar sus coordenadas para

que coincidieran con las de σ^i, son $a = 11011010000011010001010$ y $a = 11101110011010011010110$. Con el primero se cumple que

$$\mathrm{wt}(v_2 + w_1 + \sigma^6(w_1) + \sigma^{16}(w_1)) = 8,$$

lo que conlleva a una contradicción, mientras que con la segunda posibilidad se llega a Q. De donde se obtiene una matriz generadora de la forma:

$$G_{48} = \begin{pmatrix}
000000000000000000000000111111111111111111111111\\
100000000000000000000001111011100110100110101100\\
010000000000000000000001011101110011010011010110\\
001000000000000000000001101110111001101001101010\\
000100000000000000000001110111011100110100110100\\
000010000000000000000001011011101110011010011010\\
000001000000000000000001101101110111001101001100\\
000000100000000000000001010111011101100110100110\\
000000010000000000000001101011011101110011010010\\
000000001000000000000001110101101110111001101000\\
000000000100000000000001011010110111011100110100\\
000000000010000000000001001101011011101110011010\\
000000000001000000000001100110101101110111001100\\
000000000000100000000001010011010110111011100110\\
000000000000010000000001101001101011011101110010\\
000000000000001000000001110100110101101110111000\\
000000000000000100000001011010011010110111011100\\
000000000000000010000001001101001101011011101110\\
000000000000000001000001100110100110101101110110\\
000000000000000000100001110011010011010110111010\\
000000000000000000010001111001101001101011011100\\
000000000000000000001001011100110100110101101110\\
000000000000000000000101101110011010011010110110\\
000000000000000000000011110111001101001101011010
\end{pmatrix}$$

□

3.2.3. Tipo $11-(4,4)$:

Ordenamos el automorfismo $\sigma = (1,\ldots,11)\ldots(34,\ldots,44)(45)\ldots(48)$ y ordenamos las coordenadas correspondientemente. El código $\overline{F_\sigma(C)}$ es un [8,4] código auto-dual, todos estos códigos se encuentran listados en [14]. Si A_i es el número de palabras de código en C de peso i, estos números se conocen de [6]. En particular

$$A_{12} = 17296 \equiv 4 \text{ mód } 11.$$

Por ende $F_\sigma(C)$ contiene 4 mód 11 vectores de peso 12 cuyas imágenes tiene peso 2 en $\overline{F_\sigma(C)}$. De esta manera de la lista de [14], $\overline{F_\sigma(C)}$ es generado por $[I_4|I_4]$. Por ende,

$$\text{gen}(C)= \left(\begin{array}{c|c} \bar{I}_4 & I_4 \\ \hline A & 0 \end{array} \right) ,$$

donde 0 es la matriz nula de tamaño 20×4, y $E_\sigma(C)$ es generado por $(A \mid 0)$.

3.2.5 Lema. No existe $w \in E_\sigma(C),\ w \neq \bar{0}$, tal que w es cero en dos de los 11-cíclos.

Demostración. Supongamos que w es no nulo sobre $\Omega_i,\ \Omega_j$. Del lema 2.1.6 $w|_{\Omega_i} \in \mathbb{F}_{2^1 0}$ y se puede multiplicar por un escalar tal que

$$\text{w}|_{\Omega_i} = 11000000000.$$

Luego $\text{wt}(w|_{\Omega_j}) = 10$ y claramente $\text{wt}(w + \sigma(w)) = 4$, que es una contradicción. □

Por el lema 2.1.6, se puede suponer que:

$$gen(f(E)) = \left(\begin{array}{cccc} \alpha & 0 & \beta & \gamma \\ 0 & \alpha & \delta & \epsilon \end{array} \right),$$

donde $\alpha = 11000000000$ y $\beta,\ \gamma,\ \delta, \epsilon$ son distintos de cero por el lema anterior. Entonces se puede asumir

$$A = \left(\begin{array}{cccc} X & 0 & R & S \\ 0 & X & T & U \end{array} \right),$$

donde

$$X = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix};$$

$R,\ S,\ T,\ U \in \mathbb{F}_q^{10\times 11}$ son matrices circulantes no nulas. Sean $x_1, \ldots, x_{20}$ las filas de A.

Supongamos que las primeras filas de $R,\ S,\ T,\ U$ son $r = r_1 \ldots r_{11},\ s = s_1 \ldots s_{11}, t = t_1 \ldots t_{11}, u = u_1 \ldots u_{11}$, respectivamente, y denotemos las cuatro filas de $(\bar{I}_4 | I_4)$ por $v_1, \ldots, v_4$. Al intercambiar Ω_3, Ω_4, de ser necesario, se tiene que $\text{wt}(r) \leq \text{wt}(s)$. Si $\text{wt}(s) = 10,\ \text{wt}(r) = 4$ u 8, se sigue que

$$\text{wt}(x_1 + v_4) = 8 \text{ ó } \text{wt}(x_1 + v_3 + v_4) = 8.$$

De esta forma se tienen dos casos:

a. $\mathrm{wt}(r) = 6,\ \mathrm{wt}(s) = 8.$

b. $\mathrm{wt}(r) = 4,\ \mathrm{wt}(s) = 6.$

Sean c, d el número de cadenas de unos en r, s, respectivamente. Del lema 3.2.3,

$$\mathrm{wt}(x_1 + \sigma(x_1)) = 2 + 2(c + d).$$

Entonces $c + d = 5, 7, 9, 11$. Claramente $c, d \leq 5$. Si c o d es cinco, entonces

$$\mathrm{wt}((x_1 + \sigma(x_1))|_{\Omega_3}) = 10 \text{ ó } \mathrm{wt}((x_1 + \sigma(x_1))|_{\Omega_4}) = 10 \text{ y}$$

$$\mathrm{wt}((x_1 + \sigma(x_1))|_{\Omega_1}) = 2,$$

lo que conlleva a una contradicción como anteriormente. Si c o d es 1,

$$\mathrm{wt}((x_1 + \sigma(x_1))|_{\Omega_3}) = 2 \text{ ó } \mathrm{wt}((x_1 + \sigma(x_1))|_{\Omega_4}) = 2 \text{ y}$$

$$\mathrm{wt}((x_1 + \sigma(x_1))|_{\Omega_1}) = 2,$$

que igualmente conlleva a una contradicción. Así las posibilidades son $c = 2$ y $d = 3$, $c = 3$ y $d = 2$, $c = 3$ y $d = 4$, o $c = 4$ y $d = 3$. Para el caso a., no es posible que $c = 3$ y $d = 4$.

Asumamos que la cadena de unos más extensa se da al inicio de r y s y que $r_{11} = s_{11} = 0$. Se pueden excluir posibilidades para r al descomponer $\mathrm{wt}(r)$ en c enteros positivos, para que correspondan con las longitudes de las cadenas de unos en r y haciendo lo mismo para $11 - \mathrm{wt}(r)$ con las cadenas de ceros, además de reemplazar σ por σ^{-1}. Realizando el mismo proceso para s, excepto sin reemplazar σ por σ^{-1}, se obtienen 573 combinaciones de valores de r, s.

De éstas se excluyen las que no cumplan que $x_1, \sigma(x_1), \ldots, \sigma^9(x_1)$ sean ortogonales o que alguna combinación lineal de elementos de esta base genere un vector que al ser combinado con un vector de $F_\sigma(C)$ implique alguna contradicción.

Con estas condiciones, treinta posibilidades quedan. Si se reemplaza σ por σ^i, x_1 por $\sum_{j=0}^{i-1} \sigma^j(x_1)$, y se reorganizan las coordenadas acorde a σ^i, entonces la lista se reduce a seis posibilidades. Si se encuentra un vector

$$v \in \langle x_1, \sigma(x_1), \ldots, \sigma^9(x_1) \rangle,$$

tal que $v|_{\Omega_3} = 1100\ldots0$ o $v|_{\Omega_4} = 1100\ldots0$ y reordenando $\Omega_1, \ldots, \Omega_4$ se reduce esta lista aún más a dos, que son

$$r = 1110000000010, s = 11110100010$$
y $$r = 11100000010, s = 11100110100.$$

Para determinar T, U las treinta posibilidades mencionadas con antelación para $r,\ s$ pueden ser exploradas para $t,\ u$. Para ello se toman en sentido contrario sobre $\Omega_3,\ \Omega_4$, posiblemente también u permutado cíclicamente e invirtiendo la pareja $t,\ u$.

Así, se prueba la ortogonalidad de x_{11} con $x_1, \sigma(x_1), \ldots, \sigma^{10}(x_1)$, lo que implica que $\sigma^{11}(x_1)$ es ortogonal a todo $\sigma^j(x_1)$. De esta manera sólo tres posibilidades sobreviven para t, u, dos de las cuales son equivalentes. Estas posibilidades emplean el caso b. enunciado antes y para x_{11} se tienen

$$t = 00101100111,\ u = 01000000111$$
ó $$t = 11110100010,\ u = 01110000001.$$

Para la primera combinación se verifica luego que

$$\mathrm{wt}(x_1 + \sigma(x_1) + \sigma^{10}(x_1) + x_{11} + \sigma^9(x_{11}) + \sigma^{10}(x_{11})) = 8,$$

y para la segunda

$$\mathrm{wt}(x_1 + \sigma(x_1) + \sigma^2(x_1) + \sigma^3(x_1) + \sigma^3(x_{11}) + \sigma^4(x_{11}) + \sigma^5(x_{11})) = 8.$$

Lo que conlleva a una contradicción.

De esta forma se tiene el siguiente teorema

3.2.6 Teorema. No existe un código doblemente par con parámetros $[48, 24, 12]$ y $\sigma \in \mathrm{Aut}(C)$ de orden 11.

3.2.4. Tipo $7 - (6, 6)$:

Ordenamos $\sigma = (1, \ldots, 7) \ldots (36, \ldots, 42)(43) \ldots (48)$ y las coordenadas de C también de forma correspondiente. El código $\overline{F_\sigma(C)}$ es un código auto-dual de parámetros [12,6] listado en [14]. Dado que un vector de peso dos en $\overline{F_\sigma(C)}$ se obtiene a partir de un vector de peso ocho en $F_\sigma(C)$. En consecuencia $\overline{F_\sigma(C)}$ es B_{12} de [14]. Como para el caso anterior,

$$A_{12} \equiv 6 \text{ mód } 7,$$

de donde se sigue que $F_\sigma(C)$ contiene 6 mód 7 vectores v de peso doce.

Pero entonces

$$\mathrm{wt}(\pi(v)) = 6,$$

es decir, v tiene su soporte en únicamente un 7-ciclo. Si $v_1, v_2 \in F_\sigma(C)$ tienen peso doce y $\pi(v_1), \pi(v_2)$ coinciden en posiciones correspondientes a un mismo ciclo, entonces

$$\mathrm{wt}(v_1 + v_2) \leq 2,$$

y así $v_1 = v_2$. De esta forma hay exactamente seis vectores de peso doce en $F_\sigma(C)$, que se proyectan a vectores independientes en $\overline{F_\sigma(C)}$. Entonces,

$$\mathrm{gen}(F_\sigma(C)) = (\bar{I}_6 \mid J_6 - I_6),$$

donde J_6 es la matriz de tamaño 6×6 con todas sus coordenadas 1.

Sean $v_1, \ldots, v_6$ las filas de $\mathrm{gen}(F_\sigma(C))$.

3.2.7 Lema. Sean $i \in \{1, \ldots, 6\}$ y

$$V \subseteq \{v \in \mathbb{F}_2^7 \mid v = w|_{\Omega_i}, \text{ con } w \in E_\sigma(C)\},$$

tal que V es un subespacio cerrado bajo $\sigma|_{\Omega_i}$. Entonces V es un código cíclico generado por $\bar{0}$, 1110100, 1110010 ó 1100000.

Demostración.La acción de $\sigma|_{\Omega_i}$ garantiza que V es un código cíclico par. Además, como

$$x^7 + 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$$

se tiene el resultado. □

3.2.8 Lema. Sea $v \in E_\sigma(C)$, donde v tiene coordenadas cero en al menos tres de las coordenadas de los 7-ciclos. Entonces $\mathrm{wt}(v) = 12$ y todas sus restricciones no nulas a los 7-ciclos de σ es una permutación de 1110100 ó 1110010.

Demostración. Sea

$$W := \langle \{\sigma^i(v) \mid 0 \leq i \leq 6\} \rangle.$$

Supongamos que W es no nulo sobre $\Omega_i, \Omega_j, \Omega_k$ y que existe $0 \neq w \in W$, con $w|_{\Omega_i} = 0$. Entonces

$$\mathrm{wt}(w|_{\Omega_i}) = \mathrm{wt}(w|_{\Omega_k}) = 6 \text{ y } \mathrm{wt}(w + \sigma(w)) = 4.$$

Si ahora se supone que existe $w \in W$ con $\mathrm{wt}(w|_{\Omega_j}), \mathrm{wt}(w|_{\Omega_k}) \in \{4, 6\}$ y

$$\mathrm{wt}(w + v_j + v_k) = 8,$$

que es una contradicción. Por ende si $W_l := W|_{\Omega_l}$, entonces por el lema anterior, W_i, W_j, W_k son todos códigos cíclicos generados por 1110100 ó 1110010. Si dos (o uno) son generados por el primero y uno (o dos) por el segundo (respectivamente) y si $w \neq 0$ con $w \in W$, entonces $\mathrm{wt}(w + \sigma(w) + \sigma^3(w)) \in \{4, 8\}$, que es también una contradicción. □
Sea

$$\mathrm{gen}(C) = \left(\begin{array}{c|c} \bar{I}_6 & J_6 - I_6 \\ \hline A & 0 \end{array}\right),$$

donde 0 es la matriz nula de tamaño 18×6 y $[A \mid 0]$ genera a $E_\sigma(C)$. Además debido a la simetría de $(\bar{I}_6 \mid J_6 - I_6)$ se pueden ordenar los 7-ciclos de cualquier forma conveniente y sólo organizar también de forma adecuada los puntos fijos. Haciendo uso ahora de los dos lemas anteriores, de tal forma que luego de reordenar los 7-ciclos A se reduzca a una matriz de la siguiente forma

$$\text{a.} \begin{pmatrix} X & 0 & 0 & K & L & M \\ 0 & X & 0 & N & P & R \\ 0 & 0 & X & S & T & U \end{pmatrix}$$

ó

$$\text{b.} \begin{pmatrix} X & 0 & K & L & M & N \\ 0 & X & P & R & S & T \\ 0 & 0 & Y_1 & U & V & W \\ 0 & 0 & 0 & Y_2 & B & D \end{pmatrix},$$

donde

$$X = \begin{pmatrix} 1100000 \\ 0110000 \\ \vdots \\ 0000011 \end{pmatrix},$$

con 0 la matriz nula de tamaño apropiado y Y_i siendo alguna de las siguientes matrices:

$$\begin{pmatrix} 1110100 \\ 0111010 \\ 0011101 \end{pmatrix} \text{ ó } \begin{pmatrix} 1110010 \\ 0111001 \\ 1011100 \end{pmatrix}.$$

Denotemos las 18 filas de $(A \mid 0)$ por $w_1, \ldots, w_{18}$. Se puede asumir claramente que todas las matrices en las formas a. y b., son circulantes. Consideremos la forma b. primero.

3.2.9 Lema. Si se tiene la forma b., entonces se puede reducir a la forma a. o se puede suponer

$$\begin{pmatrix} Y_1 & 0 & V & W \\ 0 & Y_2 & B & D \end{pmatrix} = \begin{pmatrix} Y & 0 & Y & Z \\ 0 & Y & Y & Y \end{pmatrix},$$

donde

$$Y = \begin{pmatrix} 1110100 \\ 0111010 \\ 0011101 \end{pmatrix}, \; Z = \begin{pmatrix} 0111010 \\ 0011101 \\ 1001110 \end{pmatrix},$$

y 0 es el módulo de $\mathbb{F}_2^{3\times 7}$.

Demostración. Al reemplazar σ por σ^{-1} se puede asumir que $Y_2 = Y$. Del lema anterior, si se reorganizan cíclicamente las coordenadas de los ciclos Ω_5, Ω_6, se puede suponer $B = D = Y$. Si la cerradura del generado de las filas de

$$\begin{pmatrix} U \\ Y \end{pmatrix}$$

bajo $\sigma|_{\Omega_4}$ genera al subcódigo de peso par , notado con $E_\sigma(C)$, al invertir Ω_3, Ω_4, la forma a. es obtenida. Por consiguiente, se puede suponer que el generado de las filas de U está contenido en el generado de las filas de Y, y en consecuencia, U es cero al llevar la matriz a su forma escalonada reducida, de ser necesario.

Si la cerradura del generado de las filas de

$$\begin{pmatrix} V \\ Y \end{pmatrix} \text{ o } \begin{pmatrix} W \\ Y \end{pmatrix}$$

bajo $\sigma|_{\Omega_5}$ o $\sigma|_{\Omega_6}$ genera el subcódigo de peso par, análogamente se puede llegar al caso a. Entonces se puede suponer, del lema anterior, que las filas superiores de Y_1, V, W son permutaciones cíclicas de 1110100. Al reemplazar w_{13} por $\sigma^i(w_{13})$ para algún i, se puede considerar $V = Y$. Reordenando cíclicamente Ω_3 se puede suponer además que $Y_1 = Y$.

Veamos ahora que la fila superior z de Z es una permutación cíclica de 1110100. Si $z = 1110100$, entonces

$$\mathrm{wt}(w_{13} + w_{16}) = 8,$$

que es una contradicción. Sea $a = 1110100$. Restringiendo los vectores a los 7-cíclos se tiene $w_{16} = \bar{0}\ \bar{0}\ \bar{0}\ a\ a\ a,\ w_{13} = \bar{0}\ \bar{0}\ a\ \bar{0}\ a\ z$. Definamos

$$w'_{13} := w_{13} + w_{16} = \bar{0}\ \bar{0}\ a\ a\ \bar{0}(a + z).$$

Reemplazando w_{13} por w'_{13} e invirtiendo Ω_4, Ω_5 se puede reemplazar z por $a + z$. Esto significa que sólo es necesario considerar

$$z \in \{0011101,\ 0011101,\ 0100111\}.$$

Si $z = 0011101$ ó $z = 0100111$, al reemplazar σ por σ^2 ó σ^4, respectivamente y reordenar las coordenadas adecuadamente, se obtiene $z = 0111010$. Este proceso fija a a pero implica hacer una reducción por filas nuevamente de $\{w_1, \ldots, w_{12}\}$. □

3.2.10 Lema. Si se tiene la forma b., las filas superiores de K, L, P y R se pueden suponer $\bar{0}$ o permutaciones cíclicas de 1100000.

Demostración. Los representantes de las clases laterales del código cíclico generado por 1110100 en el subcódigo de $\mathbb{F}_2^7$ de peso par son $\bar{0}$ y permutaciones cíclicas de 1100000. Sumándoles a w_1 y w_7, $\sigma^i(w_{13})$ y/o $\sigma^j(w_{16})$ para algunos i, j, arroja el resultado deseado. □

Supongamos que K es nula sin pérdida de generalidad. Para encontrar w_1 tal que $w_1, \sigma(w_1), \ldots, \sigma^6(w_1)$ sean ortogonales, es suficiente hallar w_1 con $4 \mid \mathrm{wt}(w_1)$ y w_1 ortogonal a $\sigma(w_1), \sigma^2(w_1), \sigma^3(w_1)$.

Haciendo uso de las cadenas de unos y ceros como en el Tipo 11-(4,4), las posibilidades para las primeras filas de M, N se pueden determinar. Si la primera fila de M es una permutación cíclica de 1110100, entonces

$$\mathrm{wt}((w_1 + \sigma^i(w_{16}))|_{\Omega_5}) = 0$$

para algún i y $w_1 + \sigma^i(w_{16})$ resultado que contradice el lema 3.2.8; análogamente sucede si la primera fila de N es una permutación cíclica de 1110100. Las únicas posibilidades para las primeras filas de M, N son permutaciones de ciclos independientes de las siguientes combinaciones: 1101100, 1101100 ó 1110010, 1110010. Al considerar la primera

$$\mathrm{wt}(w_1 + \sigma(w_1) + \sigma^2(w_1)) = 8 \text{ y con la segunda}$$

$$\mathrm{wt}(w_1 + \sigma^2(w_1) + \sigma^3(w_1)) = 8.$$

Entonces, K, L, P, R son matrices no nulas y sus filas superiores son permutaciones cíclicas de 1100000. Supongamos que la primera fila de

M (o N) es también una permutación cíclica del mismo vector, entonces la primera fila de N (o M) es una permutación cíclica de 1110100 o de 11100101 (respectivamente). En cualquier caso

$$\mathrm{wt}(w_1 + \sigma^2(w_1) + \sigma^4(w_1) + v_1 + v_3 + v_4 + v_5 + v_6) = 8.$$

Así, ninguna de las filas superiores de M, N, S, T es una permutación cíclica de 1100000. Al reemplazar w_1, w_7 por $\sigma^i(w_1), \sigma^j(w_7)$, respectivamente, y reordenando cíclicamente Ω_1, Ω_2 se puede asumir que las filas superiores de K, P son 1100000.

Haciendo uso de las técnicas empleadas para el Tipo 11-(4,4), las primeras filas de M y N (y de S y T) se escogen de la siguiente lista, con permutaciones de ciclos independientes e inversión de los dos vectores admisibles: 1111110, 1101100; 1111000, 1001000; ó 1010000, 1101010.

Cada posibilidad para w_1, y en consecuencia para w_7, es comprobada para cumplir con el criterio de ortogonalidad con respecto a $w_{13}, \ldots, w_{18}$. Treinta vectores resultan como posibles para w_1, y así para w_7 también. Todas las parejas $\{w_1, w_7\}$ probables pueden ser comprobadas para ver si $w_1, \ldots, w_{12}$ son ortogonales. Sólo tres combinaciones pasan esta verificación. Si

$$\Omega := \Omega_4 \cup \Omega_5 \cup \Omega_6,$$

entonces el conjunto $\{w_1|_\Omega, w_7|_\Omega\}$ se puede escoger de:

$$\{0011000\ 1111110\ 1100110,\ 1000001\ 0011011\ 1111101\},$$
$$\{0000110\ 0011110\ 0100010,\ 0001100\ 0101000\ 1101010\}\ \text{ó}$$
$$\{0000110\ 0100100\ 1110001,\ 0000011\ 1010110\ 0100001\}.$$

En el primer caso si w_1 representa el primer vector,

$$\mathrm{wt}(w_1 + \sigma^2(w_1) + \sigma^4(w_1) + \sigma^{-1}(w_{13}) + v_1 + v_3 + v_4 + v_5 + v_6) = 8.$$

En los dos casos siguientes si w_1 representa el primer vector de la pareja, $\mathrm{wt}(w_1 + \sigma^4(w_1) + \sigma^5(w_1) + \sigma(w_{13}) + \sigma^5(w_{16}) + v_1 + v_3 + v_4 + v_5 + v_6) = 8$.

Ahora supongamos que se tiene la forma a. Nuevamente, como en el Tipo 11-(4,4) se pueden determinar las posibilidades para las filas superiores de K, L, M. Al ordenar cada ciclo adecuadamente se puede asumir la mayor cadena de unos a la izquierda. Existen siete posibilidades de esta forma. Las cuales se reducen a cuatro al reemplazar σ por σ^i y w_1

por $\sum_{j=0}^{i-1} \sigma^j(w_1)$. Las once posibilidades, con permutaciones de los ciclos $\Omega_4, \Omega_5, \Omega_6$ y permutaciones cíclicas independientes conllevan a todas las opciones para w_7 y w_{13}. Cada elección para w_7 (o w_{13}) se pone a prueba con

$$\left\{ \sigma^i \left(\sum_{j=0}^{k} \sigma^j(w_1) \right) \;\middle|\; 0 \leq k \leq 3, 0 \leq i \leq 6 \right\},$$

para los pesos adecuados. Entonces para cada w_{13} y w_7 se prueba su ortogonalidad a cada conjunto

$$\{\sigma^i(w_7) \mid 0 \leq i \leq 5\}.$$

Un análisis computacional de los resultados indica que al intercambiar w_1, w_7, w_{13}, de ser necesario, se puede asumir $w_1|_\Omega$=1111000 1111110 1101010, donde

$$\Omega = \Omega_4 \cup \Omega_5 \cup \Omega_6.$$

Existen 12 posibilidades para la pareja $\{w_7|_\Omega, w_{13}|_\Omega\}$. En seis de ellos un vector de peso 8 puede ser fácilmente encontrado entre $\{w_7, \ldots, w_{18}\}$. Los otros seis se puede mostrar que son equivalentes a dos de ellos:

$$\{1111000\ 1011001\ 0100001,\ 1100000\ 0111010\ 1100101\},$$
$$\{1010011\ 1100000\ 1011100,\ 0010001\ 1111110\ 0100001\}.$$

En el primer caso $\mathrm{wt}(w_1 + \sigma(w_1) + \sigma^5(w_1) + \sigma^6(w_1) + w_7 + \sigma(w_7) + \sigma^5(w_7) + \sigma^6(w_7) + w_{13} + \sigma(w_{13})) = 8$ y en el segundo, si $x = w_1 + \sigma^3(w_1) + \sigma^5(w_1) + w_7 + w_{13} + \sigma(w_{13}) + \sigma^3(w_{13}) + \sigma^5(w_{13})$, entonces

$$\mathrm{wt}(x + \sigma(x)) = 8.$$

Para estos dos casos, haciendo uso de w_1, w_7, w_{13} se llega a una contradicción. Así se tiene el siguiente teorema.

3.2.11 Teorema. No existe un código C doblemente par de parámetros [48,24,12] con $\sigma \in \mathrm{Aut}(C)$ de orden 7.

3.2.5. Tipo $5 - (8, 8)$:

Se ordena $\sigma = (1, \ldots, 5) \ldots (36, \ldots, 40)(41) \ldots (48)$ y las coordenadas también correspondientemente. Del lema 2.1.1 el código $\overline{F_\sigma(C)}$ es par con

parámetros [16,8]. Observando la lista en [14], existen dos alternativas para $F_\sigma(C):\ A_8 \oplus A_8$ o E_{16}, donde

$$\mathrm{gen}(A_8) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathrm{gen}(E_{16}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Ambos códigos aparecen también para el caso cuando $p = 3$. Ambos códigos, A_8, E_{16}, tienen conjuntos definitivos. También cabe notar que una vez se ha elegido el cluster resultan dos d-conjuntos que generan el mismo código, esto cambiando los representantes de un número impar de duos. En efecto, fijado un cluster, si se considera cada duo como un conjunto ordenado y listándolos en algún orden, entonces se pueden escoger dos d-conjuntos al tomar el primer elemento de cada duo para un d-conjunto y para el otro todos los primeros elementos de los duos, excepto en el último que se toma el segundo. Estos dos d-conjuntos conllevan a dos códigos distintos (pero equivalentes), y todos los d-conjuntos llevan a un código equivalente a uno de ellos.

Ahora, sean X_c, X_f las coordenadas que representan los 5-ciclos y los puntos fijos de $\overline{F_\sigma(C)}$, respectivamente. Supongamos que

$$\overline{F_\sigma(C)} = \ A_8 \oplus A_8.$$

Entonces $\overline{F_\sigma(C)}$ queda determinado por dos clusters C_1, C_2 y los d-conjuntos D_1, D_2. Supongamos que cinco o más coordenadas que constituyen un cluster se dan en X_c o X_f. Entonces cinco o más coordenadas, de digamos C_1, estarán en X_f. Por ende hay un duo, digamos $d_1 \in C_1$, con $d_1 \subset X_f$. Escojamos un duo $d_2 \in C_1$ con $d_2 \cap X_f \neq \emptyset$.

Así, $d_1 \cup d_2$, conforma el soporte de un vector de peso 4 $\pi(v) \in \overline{F_\sigma(C)}$, con $v \in F_\sigma(C)$; pero $\mathrm{wt}(v) = 4$ u 8, que es una contradicción. Luego,

cada C_i está constituido por cuatro puntos de cada conjunto, X_c, X_f. Si en C_i, hay un duo $d_1 \in C_i$ con $d_1 \subset X_f$ se llega a una contradicción, como anteriormente.

Entonces cada duo tiene un punto de X_c y X_f. En consecuencia, hay un d-conjunto conformado por cuatro puntos, tres de los cuales están en X_f, de donde se sigue que es el soporte de un $\pi(v) \in \overline{F_\sigma(C)}$, con $\mathrm{wt}(v) = 4$ u 8, que no es posible. Supongamos ahora que

$$\overline{F_\sigma(C)} = E_{16}.$$

Entonces $\overline{F_\sigma(C)}$ está definido por un cluster C_1 y un d-conjunto de D_1. Si hay un duo $d \subset X_f$ o X_c, entonces se llega a una contradicción como sucedió antes. De esta forma cada duo tiene un punto de X_c y X_f. Con lo que se puede asumir que D_1 tiene siete elementos de X_f. Si el octavo punto también está en X_f, se obtiene una contradicción. Por consiguiente si las coordenadas izquierdas representan X_c y las derechas X_f, entonces los duos son $\{\Omega_x, x\}$, donde $1 \leq x \leq 8$ y

$$\mathrm{gen}(\overline{F_\sigma(C)}) =: Z$$

es

$$\left(\begin{array}{cccccccc|cccccccc}
\bar{1} & \bar{1} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\bar{0} & \bar{1} & \bar{1} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
\bar{0} & \bar{0} & \bar{1} & \bar{1} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
\bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{1} & \bar{0} & \bar{0} & \bar{0} & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
\bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{1} & \bar{0} & \bar{0} & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{1} & \bar{0} & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{1} & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\bar{1} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{0} & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right).$$

Sean $z_1, \ldots, z_8$ las filas de Z. Entonces

$$\mathrm{gen}(C) = \left(\begin{array}{c|c} Z & \\ \hline A & 0 \end{array}\right),$$

donde $[A \mid 0]$ genera a $E_\sigma(C)$ y 0 es la matriz nula de tamaño 16×8.

3.2.12 Lema. Sea $v \in E_\sigma(C), v \neq 0$. Entonces v es cero en tres o menos de los 5-ciclos.

Demostración. Sea $v \in E_\sigma(C)$ cero en más de tres 5-ciclos. Entonces:

I. v tiene 3-ciclos $\Omega_i, \Omega_j, \Omega_k$ de peso 4, 5 ciclos $\bar{0}$.

II. v tiene 4 ciclos $\Omega_i, \Omega_j, \Omega_k, \Omega_l$ de peso 4, 4 ciclos $\bar{0}$ ó

III. v tiene 2 ciclos Ω_i, Ω_j de peso 4, 2 ciclos de peso 2, 4 ciclos $\bar{0}$.

Sea w el vector con soporte $\{\Omega_i, i\} \cup \{\Omega_j, j\}$ para los casos I., II. y soporte $\{\Omega_i, i\} \cup \{\Omega_j, j\} \cup \{\Omega_k, k\} \cup \{\Omega_l, l\}$ en II. Entonces

$$\mathrm{wt}(w + v) = 8.$$

□

Por el lema 2.1.9, se puede establecer A al encontrar $f(E_\sigma(C)^*)$. Debido al lema anterior, es un [8,4] código auto-dual sobre $\mathbb{F}_{16}$ con distancia mínima de por lo menos 5; así $f(E_\sigma(C)^*)$ debe ser un código MDS con distancia mínima 5. Por consiguiente. Claramente cualquier permutación de

$$\{x \mid 1 \leq x \leq 8\}$$

cambia los duos de $\overline{F_\sigma(C)}$ y transforma los d-conjuntos en otros que conllevan al mismo código. Entonces, las permutaciones de las posiciones de los 5-ciclos se pueden efectuar de cualquier forma. Utilizando la tabla I se obtiene $f(E_\sigma(C)^*)$. El producto interno se definió de tal forma que al desplazar cíclicamente cualquier 5-ciclo (esto es, multiplicando cualquier coordenada de $f(E_\sigma(C)^*)$ por α^{12i}) hace que $f(E_\sigma(C)^*)$ sea auto-dual. Por ende, del corolario 2.1.10, se obtiene que

$$\mathrm{gen}(f(E_\sigma(C)^*)) = \begin{pmatrix} \alpha & 0 & 0 & 0 & 1 & 1 & 1 & \alpha^2 \\ 0 & \alpha & 0 & 0 & x & y & z & w \\ 0 & 0 & \alpha & 0 & * & * & * & * \\ 0 & 0 & 0 & \alpha & * & * & * & * \end{pmatrix},$$

donde $w \in \{1, \alpha, \alpha^2\}, x, y, z, * \in \mathbb{F}_{16} - \{0\}$. Se obtiene un vector de peso 4 en $f(E_\sigma(C)^*)$, si una de las siguientes afirmaciones son ciertas.

- Dos de x, y, z son iguales.
- $1 \in \{x, y, z\}$, si $w = \alpha^2$.
- $\alpha^{14} \in \{x, y, z\}$, si $w = \alpha$.
- $\alpha^{13} \in \{x, y, z\}$, si $w = 1$.

Sean $u_1, \ldots, u_4$ las filas de $\text{gen}(f(E_\sigma(C)^*))$. Usando el corolario 2.1.10 y

$$\langle u_1, u_2 \rangle = 0,$$

se pueden determinar los conjuntos $\{x, y, z\}$ para cada elección de w. Dieciséis vectores resultan posibles para u_2.

En consecuencia, hay $6 \cdot 16 = 96$ posibilidades para u_3. Las 96 opciones para u_3 se prueban por ortogonalidad respecto a las 16 alternativas para u_2, de donde se llegan a sólo 41 parejas no ordenadas para $\{u_2, u_3\}$ y en consecuencia también para $\{u_3, u_4\}$. Se pueden verificar estas parejas y ver que no existen ternas $\{u_2, u_3, u_4\}$ tales que cualesquiera dos elementos son por parejas mutuamente ortogonales.

Así, de hecho, se puede mostrar que no existe un código auto-dual con parámetros $[8, 4, 5]_{16}$. De esta forma se tiene el siguiente teorema.

3.2.13 Teorema. No existe un código auto-dual C de parámetros [48,24,12] con un automorfismo de orden 5.

3.2.6. Tipo $3 - (12, 12)$:

Si $\sigma \in \text{Aut}(C)$ es del tipo $3 - (12, 12)$, del corolario 2.1.8 se verifica que $f(E_\sigma(C)^*)$ es auto-dual y de parámetros $[12, 6, d']_4$, con $d' \geq 6$. De [13], se tiene que tal código no existe. Luego σ no puede ser del tipo $3 - (12, 12)$.

3.2.7. Tipo $3 - (14, 6)$:

Si $\sigma \in \text{Aut}(C)$ es del tipo $3 - (14, 6)$, no existen vectores de peso 2 en $\overline{F_\sigma(C)}$ con parámetros $[20, 10]$, al ser auto-dual y doblemente par.

También los vectores de peso 4 tienen soporte en las coordenadas correspondientes a los 3-ciclos y por ende todos los vectores de peso 4 en $\overline{F_\sigma(C)}$ pueden tener soporte en sólo un total de 14 coordenadas, es decir, a lo más una posición no nula en cada 3-ciclo. De [14], se sigue que no puede existir este código.

3.2.8. Tipo $3 - (16, 0)$:

Supongamos σ como $(1, 2, 3)(4, 5, 6) \ldots (46, 47, 48)$ y ordenando las coordenadas correspondientemente. El código $f(E_\sigma(C)^*)$ es un códi-

go doblemente par de parámetros [16,8], por el lema 2.1.1. Entonces $\overline{F_\sigma(C)} = A_8 \oplus A_8$ o E_{16}. Del lema 2.1.7

$$f(E_\sigma(C)) = f(E_\sigma(C)^*)$$

es un código auto-dual con parámetros $[16, 8, d']_4$ con $d' \geq 6$. Estos códigos de acuerdo a [15] tienen distancia mínima 6.

Se describe a continuación el procedimiento para construir C. Hay cuatro códigos, denotados como 52, 53, 54, y 55 en [15], los cuales son candidatos a $f(E_\sigma(C))$. Cada uno de estos es fijado con gen$(f(E_\sigma(C)))$ como es listado en [15]. Para construir C, lo único que es necesario es seleccionar el orden adecuado de las coordenadas de $\overline{F_\sigma(C)}$. Esto es posible hacerlo por medio de los clusters, como para el Tipo 5-(8,8).

El código C tendrá peso mínimo 12, dado que las siguientes dos condiciones sean satisfechas:

a. El soporte de un vector de peso 4 en $\overline{F_\sigma(C)}$ no puede estar contenido en el soporte de un vector en $f(E_\sigma(C))$ de peso 6.
b. El soporte de un vector en $\overline{F_\sigma(C)}$ de peso 8 no puede ser igual al soporte de un vector de peso 8 en $f(E_\sigma(C))$.

Fijando las coordenadas de $f(E_\sigma(C))$, se pueden generar los 56 soportes de vectores de peso 6 en $f(E_\sigma(C))$ y los 870 soportes de vectores de peso 8 en $f(E_\sigma(C))$. Consideremos

$$\overline{F_\sigma(C)} = E_{16}.$$

Se seleccionan primero los duos de las coordenadas que conforman el cluster que define el subcódigo de E_{16} generado por los vectores de peso 4.

Para formar un cluster, se eligen primero dos duos y luego se van añadiendo seis más. Luego de añadir uno se verifica que se cumpla a., observando todas las posibles uniones de un par de duos. El número de parejas de duos se puede limitar haciendo uso de Aut$(F(E_\sigma(C)))$ y del hecho que cada coordenada debe hacer parte de algún duo.

La cantidad de duos necesarios es el siguiente: 9 si $f(E_\sigma(C))$ es 52, 5 si $f(E_\sigma(C))$ es 53, 9 si $f(E_\sigma(C))$ es 54, y 18 $f(E_\sigma(C))$ es 55. En caso de ser 53, no hay cluster que satisfaga a. Usando Aut$(F(E_\sigma(C)))$ se puede reducir el número de clusters para luego comprobar si cumplen b. En caso de ser 52, 54 o 55, hay 26, 5 o 15 clusters, respectivamente, que requieren de más pruebas.

Al examinar los subconjuntos de 4 duos, que constituyen el soporte de vectores de peso 8 en $\overline{F_\sigma(C)}$ y comparándolos con los soportes de vectores de peso 8 en $f(E_\sigma(C))$, no se encuentra conjunto de clusters alguno que satisfaga b. Consideremos ahora,

$$\overline{F_\sigma(C)} = A_8 \oplus A_8.$$

Primero se seleccionan dos duos de un cluster C_1 para uno de los A_8. Dos duos más se pueden agregar. Utilizando $\mathrm{Aut}(f(E_\sigma(C)))$ se puede reducir el número de parejas de duos a comprobar. Se puede asumir que el primer duo de C_1 contiene la primera coordenada. El siguiente resultado permite disminuir aún más las posibilidades.

3.2.14 Lema. Un cluster para A_8 se puede seleccionar de tal forma que cualquier par de coordenadas de A_8 forma un duo. Una vez se ha elegido el primer duo, los otros tres se determinan de forma única.

Demostración. La primera afirmación se sigue de que $\mathrm{Aut}(A_8)$ es **doblemente transitivo**, es decir, para todo $x_1, x_2, y_1, y_2 \in A_8$ existe un $\delta \in \mathrm{Aut}(A_8)$ tal que $\delta(x_i) = y_i$, i=1,2. La segunda se sigue de que hay exactamente tres vectores de peso 4 en A_8 cuyos soportes contienen el primer duo. De la forma en que se define el cluster, los otros tres duos al unir cada uno al primero da el soporte de estos tres vectores de peso 4. □

Veamos un ejemplo, considere el caso donde $f(E_\sigma(C))$ es 55. Una base, con coordenadas $1, \ldots, 16$, aparece en la siguiente figura.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ω	1	ω	0	1	0	0	0	0	0	1	0	0	0	1	0
1	0	0	0	ω	1	ω	0	1	0	0	0	0	0	1	0
1	0	0	0	1	0	0	0	ω	1	ω	0	1	0	0	0
0	0	1	0	1	0	0	0	1	0	0	0	ω	1	ω	0
ω	0	ω	1	0	0	1	0	1	0	0	0	1	0	0	0
0	0	1	0	ω	0	ω	1	0	0	1	0	1	0	0	0
0	0	1	0	0	0	1	0	ω	0	ω	1	0	0	1	0
1	$\overline{\omega}$	0	$\overline{\omega}$	0	1	0	0	0	1	0	0	0	0	0	1

Tabla II
$\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$

Esta base se obtuvo de [15]. $\mathrm{Aut}(f(E_\sigma(C)))$ es $\langle X, Y \rangle$, donde

$$X = (1,5,9,13,3,7,11,15)(2,6,10,14,4,8,12,16)$$
y
$$Y = (1,3)(6,8)(9,13)(10,14)(11,15)(12,16).$$

Las dos órbitas de coordenadas bajo $\langle X, Y\rangle$ son precisamente las de las coordenadas pares e impares. Claramente uno de los dos clusters debe contener al menos dos coordenadas impares. Del lema anterior se puede suponer que el cluster C_1 contiene dos coordenadas impares.

Al examinar $\langle X, Y\rangle$ se puede suponer que un duo de C_1 es $\{1,3\}$ ó $\{1,5\}$. Si seleccionamos $\{1,3\}, \{a,b\}$. Utilizando el estabilizador en $\langle X, Y\rangle$ de $\{1,3\}$ se pueden reducir las opciones para $\{a,b\}$, de tal forma que $\{1,3,a,b\}$ cumpla la condición a. Supongamos que se elige $\{1,5\}, \{c,d\}$. La órbita de $\{1,3\}$ bajo $\langle X, Y\rangle$ es $\{\{1,3\},\{5,7\},\{9,11\},\{13,15\}\}$. Por consiguiente se puede llegar al caso anterior o se puede suponer que $\{c,d\}$ y los otros dos duos contienen precisamente dos coordenadas impares más, digamos $\{9,11\}$ ó $\{13,15\}$, por el lema anterior también.

Utilizando $\langle X, Y\rangle$ sólo es necesario considerar 23 casos para $\{c,d\}$ de tal forma que $\{1,5,c,d\}$ no incumpla a. A medida que se incluye algún duo a C_1 es necesario verificar a. Cuando se completa C_1, se forman los posibles d-conjuntos; los cuales no satisfacen a.

De esta manera se supone que $\{1,3\}$ es un duo de C_1. Utilizando las 11 opciones para $\{a,b\}$ se pueden completar el cluster C_1 y los $d-$conjuntos puestos a prueba con la condición a. Empleando el estabilizador de $\{1,3\}$ $\langle X, Y\rangle$ para reducir los conjuntos definitivos equivalentes, se obtienen 74 de ellos para A_8. Luego para el segundo A_8 se determinan conjuntos definitivos que cumplan a. y b.; Para ello se hace uso directo del lema anterior.

Dos posibilidades cumplen todas los requerimientos, y resultan ser equivalentes, cambiando A_8 por un elemento de $\langle X, Y\rangle$. Las otras alternativas para $f(E_\sigma(C))$ se puede verificar que no satisfacen a. y b. Estos resultados se condensan en el siguiente teorema.

3.2.15 Teorema. Si C es un código con parámetros [48,24,12] y $\sigma \in \mathrm{Aut}(C)$ de tipo 3-(6,0), entonces $C \cong Q$. $f(E_\sigma(C))$ está definido por la tabla II y $\overline{F_\sigma(C)} = A_8 \oplus A_8$ siendo los dos conjuntos definitivos de A_8 $\{\{1,3\},\{5,12\},\{7,10\},\{14,16\},\{1,5,7,14\}\}$ y $\{\{2,4\},\{6,13\},\{8,15\},\{9,11\},\{2,6,8,9\}\}$.

Cabe notar que hay otros resultados que por poco conllevan al código

buscado, por ejemplo si se considera $f(E_\sigma(C))$ como el código 52 de [15] resulta un conjunto definitivo para un A_8 que cumpliera a. y b., mas no para el segundo, esto resulta en un código auto-ortogonal de parámetros [48,23,12].

3.3. Caso [120,60,24]

Debido a que este caso es objeto de estudio actual en el trabajo doctoral del MSc. Javier de la Cruz bajo la asesoría del Prof. Dr.Wolfgang Willems, no se tiene información con certeza sobre los primos que dividen el orden de $\mathrm{Aut}(C)$. Sin embargo, en un artículo próximo a ser publicado se muestra que los únicos tipos restantes de orden 11, 17 y 59, es decir, el 11-(10,10), 17-(7,1) y el 59-(2,2) no son posibles, al mismo tiempo que se han excluido algunos tipos de orden 3, 5 y 7.

Capítulo 4

ANEXOS

A continuación se presentar algunos algoritmos empleados en el desarrollo de esta tesis y que permitieron obtener resultados importantes.

4.1. Generador del código tipo II con parámetros [24,12,8]

```
% -------Generador Código de Golay con parámetros [24,12,8]--------
% En el programa se construye la matriz generadora para el código
% con el fin de facilitar la creación del mismo, empleando el hecho
% de que las filas de la matriz generadora constituye una base para
% el espacio formado por el código, así que cada Codeword queda
% determinado de manera única por una combinación lineal de escalares
% en Z2.
I=eye(12,24); %Genera la matriz identidad de tamaño12x12 y deja el
                %espacio para la matriz A
A(2,2:12)=[1 1 0 1 1 1 0 0 0 1 0];          %Construcción de matriz
                                            % bloque A
A(1,2:12)=1; A(2:12,1)=1; for i=2:11
A(i+1,2:12)=circshift(A(i,2:12),[0,-1]);    %Parte de la generadora
                                            %del código [24,12,8]-Golay
end
I(:,13:24)=A;%Superposición de la matriz identidad y de la matriz A.
                            %Ésta es la matriz generadora completa.
for i=1:2^12
  C(1:24,i)=(double(dec2binvec(i-1,12))*I)';%Escalares que generarán
                      % a cada Codeword, dado que el campo es Z2.
```

```
end
C(:,:)=mod(C(:,:),2); %Ubica a los elementos de la matriz en
%                        el espacio adecuado.
%Polinomio enumerador del peso
B=sum(C,1); c1=0;c2=0;c3=0;c4=0;c5=0;c6=0;c7=0;c8=0;c9=0;c10=0;
c11=0;c12=0;c13=0;c14=0;c15=0;c16=0;c17=0; for i=1:2^12
  switch B(i)
          case 8
          c1=c1+1;
          case 9
          c2=c2+1;
          case 10
          c3=c3+1;
          case 11
          c4=c4+1;
          case 12
          c5=c5+1;
          case 13
          c6=c6+1;
          case 14
          c7=c7+1;
          case 15
          c8=c8+1;
          case 16
          c9=c9+1;
          case 17
          c10=c10+1;
          case 18
          c11=c11+1;
          case 19
          c12=c12+1;
          case 20
          c13=c13+1;
          case 21
          c14=c14+1;
          case 22
          c15=c15+1;
          case 23
          c16=c16+1;
          case 24
          c17=c17+1;
  end
end
```

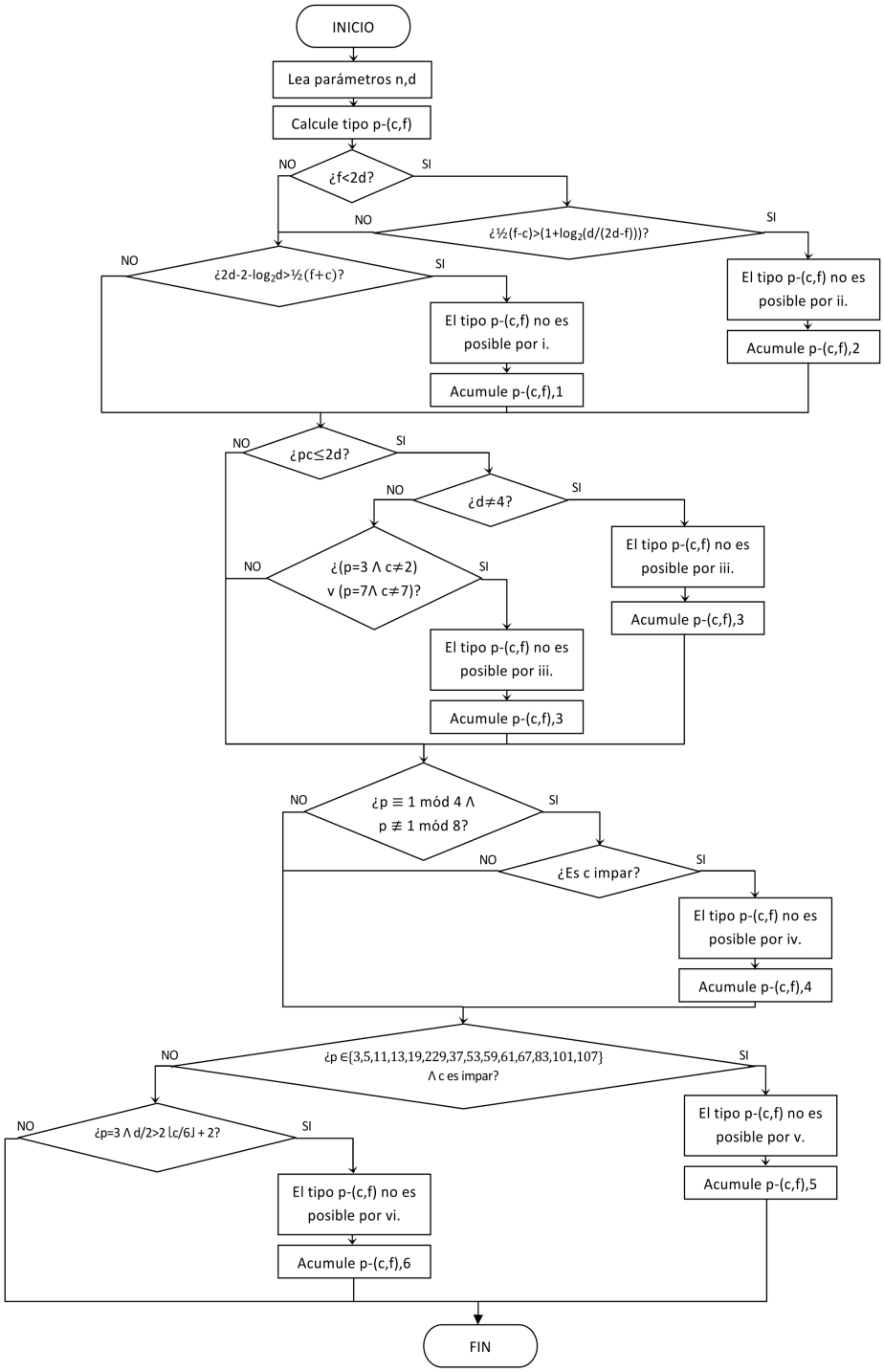
4.2. Algoritmo para excluir tipos del grupo de automorfismos de un código tipo II

```
clc; clear all; P=[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53,
 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127];
N=[24,48,120;12,24,60;8,12,24]; TI=zeros(7,320); E=zeros(7,240);
co=1; ce=1; for i=1:3
    j=1;
    n=N(1,i);
    d=N(3,i);
    while P(j)<n
        p=P(j);
        k=floor(n/p);
        for c=k:-1:1
            e=4;
            f=n-p*c;
            TI(1,co)=p;
            TI(2,co)=c;
            TI(3,co)=f;
            if f<2*d;
                if 0.5*(f-c)>(1+log2(d/(2*d-f)));
                    fprintf('El tipo %g - (%g, %g) no es posible
                     por b\n',p,c,f)
                    TI(e,co)=2;e=e+1;
                end
            elseif (2*d-2-log2(d))>0.5*(f+c);
                fprintf('El tipo %g - (%g, %g) no es posible por
                a\n',p,c,f)
                TI(e,co)=1;e=e+1;
            end
            if ~(p*c>2*d)
                if d~=4;
                    fprintf('El tipo %g - (%g, %g) no es posible
                    por c\n',p,c,f)
                    TI(e,co)=3;e=e+1;
                elseif (p==3 && c~=2)||(p==7 && c~=1)
                    fprintf('El tipo %g - (%g, %g) no es posible
                    por c\n',p,c,f)
                    TI(e,co)=3;e=e+1;
                end
            end
            if 1==mod(p,4) && 1~=mod(p,8)
                if 0~=mod(c,2)
                    fprintf('El tipo %g - (%g, %g) no es posible
                    por corolario\n',p,c,f)
                    TI(e,co)=4;e=e+1;
```

```
            end
        end
        if ((p==3)||(p==5)||(p==11)||(p==13)||(p==19)||
        (p==29)||(p==37)||(p==53)||(p==59)||(p==61)||
        (p==67)||(p==83)||(p==101)||(p==107))&&(0~=mod(c,2))
            fprintf('El tipo %g - (%g, %g) no es posible
             por d\n',p,c,f)
                TI(e,co)=5;e=e+1;
        elseif (p==3)&& ((d/2>2*floor(c/6)+2)||
        (floor(n/24)>floor(c/6)))
            fprintf('El tipo %g - (%g, %g) no es posible
             por e\n',p,c,f)
                TI(e,co)=6;e=e+1;
        end
        if e>4
            E(:,ce)=TI(:,co);
            ce=ce+1;
        end
        co=co+1;

    end
    j=j+1;
end
ce=ce+1;
end
```

Este algoritmo se puede expresar por medio del siguiente flujograma:


INICIO
Lea parámetros n,d
Calcule tipo p-(c,f)
¿f<2d?
NO
SI
¿½(f-c)>(1+log2(d/(2d-f)))?
¿2d-2-log2d>½(f+c)?
El tipo p-(c,f) no es posible por ii.
Acumule p-(c,f),2
El tipo p-(c,f) no es posible por i.
Acumule p-(c,f),1
¿pc≤2d?
¿d≠4?
El tipo p-(c,f) no es posible por iii.
Acumule p-(c,f),3
¿(p=3 Λ c≠2) v (p=7Λ c≠7)?
El tipo p-(c,f) no es posible por iii.
Acumule p-(c,f),3
¿p ≡ 1 mód 4 Λ p ≢ 1 mód 8?
¿Es c impar?
El tipo p-(c,f) no es posible por iv.
Acumule p-(c,f),4
¿p ∈{3,5,11,13,19,229,37,53,59,61,67,83,101,107} Λ c es impar?
¿p=3 Λ d/2>2 ⌊c/6⌋ + 2?
El tipo p-(c,f) no es posible por v.
Acumule p-(c,f),5
El tipo p-(c,f) no es posible por vi.
Acumule p-(c,f),6
FIN

Bibliografía

[1] W. C. Huffman, *Automorphisms of codes with applications to extremal doubly even codes of length 48,* IEEE Trans. Inform. Theory 28, pp. 511-521, 1982.

[2] V. I. Yorgov, *Binary self-dual codes with automorphism of odd order,* Translated from Problemy Peredachi Informatsii, Vol. 19, pp.11-24, October-December, 1983.

[3] E. F. Assmus, jr., H, F. Mattson, Jr., and R. J. Turyn, *Research to develop the algebraic theory of codes,* Air force Cambridge Res. Lab., Bedford, MA, Report AFCRL-67-0365, June 1967.

[4] A. M. Gleason, *Weight polynomials of self-dual codes an the MacWilliams identities*, in 1970 Actes Congres Internal de Mathematique, vol 3. Paris: Gauthier-Villars, 1971, pp. 211-215.

[5] M. Plotkin, *Binary codes with specified minimum distance,* IRE Transaction on Information Theroy, Vol. 6, 1960, pp. 445-450.

[6] C.L. Mallows, and N.J.A. Sloane, *An upper bound for self-dual codes*. Inform. and Control. v22. 188-200.

[7] E.M. Rains, *Shadow Bounds for Self-Dual Codes,* IEEE Trans. Info. Theory, 44, pp. 134 - 139, 1998.

[8] S. Zhang, *On the nonexsitence of extremal self-dual codes*, Discrete Applied Mathematics, v.91 n.1-3, pp. 277-286, 1999.

[9] S. Bouyuklieva, E.A. O'Brien and W. Willems, *The automorphism group of a binary self-dual doubly-even* $[72, 36, 16]$*-code is solvable,* IEEE Trans. Inform. Theory 52, pp. 4244-4248, 2006.

[10] W. Willems, *Codierungstheorie*. De Gruyter Lehrbuch, 1999.

[11] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes,* North Holland, Amsterdam 1977.

[12] R. P. Anstee, M. Hall, Jr., and J. G. Thompson, *Planes of order 10 do not have a collineation of order 5,* Journal of Combinatorial Theory, vol. 29A, pp. 39-58, July 1967.

[13] F. J. MacWilliams, A. M. Odluzko, N. J. A. Sloane and H. N. Ward,*Self-dual codes over $GF(4)$,* Journal of combinatorial Theory, vol. 25A, pp. 288-318, November 1978.

[14] V. Pless, *A classification of self-orthoginal codes over $GF(2)$,* Discrete Mathematics, vol. 3, pp. 209-246, September 1972.

[15] J.H. Conway, V. Pless, and N.J. A. Sloane, *Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16,* IEEE Transactions on Information Theory, vol. IT-25, pp. 312-322, May 1979.