Universidad del Norte

División de Ciencias Básicas
Departamento de Matemáticas y Estadística

Códigos binarios autoduales con un automorfismo de orden primo impar

Eber Villa Navarro

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

Director: Dr. Javier A. de la Cruz Cantillo

Barranquilla, Septiembre 12 de 2014

Agradecimientos

Ante todo doy gracias a Dios por estar a mi lado siempre, fortaleciendome en los momentos dificiles e iluminandome a lo largo de este proceso.

Agradezco hoy y siempre a mi familia, por creer en mí y poder contar con ellos en cualquier momento. Especialmente a mi madre Carmen Navarro y mi esposa Indira Arroyo, quienes han tenido en cada instante una voz de aliento y han sido mi motor para llevar a feliz término este trabajo.

Agradezco de manera especial a mi asesor de tesis, Dr. Javier de la Cruz, por sus orientaciones y consejos. Su compromiso y disposición fueron de vital importancia para la realización de esta tesis.

Finalmente doy gracias a mis amigos, profesores y compañeros que a lo largo de estos años de estudio me ayudaron en más de una ocación para permimitirme hoy alcanzar este nuevo logro en mi vida académica.

Gracias a todos.

Índice general

Introducción

En la teoría de códigos, juegan un papel importante los códigos binarios autoduales doblemente pares. Estos se denominan códigos de *tipo II* y a esta clase pertenecen el código extendido de Golay y el código de resto cuadrático, los cuales tienen muchas aplicaciones prácticas en la transmisión de datos y más aún, proporcionan información valiosa para la construcción de nuevos códigos de mayor tamaño.

Mallows y Sloane demostraron en [13], que un código de tipo II de longitud n, tiene distancia mínima $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$. Donde $\lfloor x \rfloor$ representa el mayor entero menor o igual a x. E. M. Rains probó en [17], que esta cota también es válida sin la condición de doble paridad, siempre que $24 \nmid n + 2$. Un código binario autodual cuya distancia mínima alcanza la respectiva cota superior se denomina *extremal*.

Estos códigos extremales son de gran utilidad dado que al tener la maxima distancia minimal, poseen mayor capacidad en la corrección de errores. Sin embargo la construcción de este tipo de códigos en algunos casos es compleja, por lo cual es importante construir códigos con distancia mínima lo más cercana posible a la de un código extremal de la misma longitud. Estos códigos son denominados *optimales*. Un ejemplo de este tipo de códigos son los [120,60,20] construidos en el presente trabajo de tesis.

Si C es un código de longitud n sobre el cuerpo finito $\mathbb{F}_q$ y $\sigma \in Sym(n)$, entonces notamos con $\sigma(C)$ el conjunto de todos los vectores de $\mathbb{F}_q^n$ que resultan de permutar las coordenadas de los elementos de C mediante la acción de σ. En ese caso C y $\sigma(C)$ se denominan códigos equivalentes. Se dice que σ es un automorfismo de C, si $\sigma(C) = C$. Se puede verificar que el conjunto $\mathrm{Aut}(C)$ formado por todos los automorfismos de C es un grupo y se denomina el grupo de automorfismos de C.

E. M. Rains demostró en [17], que todo código binario autodual, extremal con

parámetros $[24m, 12m, 4m+4]$, $m \in N$, es de tipo II. S. Zhang [24] demostró en 1999 que códigos con estos parámetros tienen longitud $n = 24m \leq 3672$ aunque la existencia solo ha podido demostrarse para $m = 1$ y $m = 2$, que corresponden al [24,12,8]-código extendido de Golay y [48,24,12]-código resto cuadrático, respectivamente. Assmus-Mattson en 1969 demostraron que los soportes de los vectores de peso fijo de este tipo de códigos forman un 5-Diseño, lo cual hace que este tipo de códigos tengan además, una importancia significativa desde el punto de vista geométrico.

Aunque para $m \geq 3$ la existencia de este tipo de códigos es una pregunta abierta, se han hecho algunos avances en los últimos años los cuales han proporcionado información parcial sobre la estructura de sus grupos de automorfismos. Por ejemplo para $m = 3$, se tiene un [72,36,16]-código binario autodual extremal. Este código fue formulado por primera vez en 1972 por N. J. A. Sloane [18]. Recientemente M. Borello [3] y V. Yorgov-D.Yorgov [22] aplicando teoría de representaciones de grupos finitos demostraron que el grupo de automorfismos de tal código, si existe, no tiene un elemento de orden 4 y su orden es menor o igual a 5.

Para m = 4, estamos en presencia de un [96,48,20]-código binario autodual extremal. Su existencia es también una pregunta abierta. J. De la Cruz y W. Willems [8], [9] han establecido que los automorfismos de orden 3 tienen seis puntos fijos o carecen de ellos y los de orden 5 tienen exactamente seis. Mas aún, se demostró que en caso de que todo automorfismo de orden 3 carezca de puntos fijos, entonces el grupo de automorfismos es soluble o es Alt(5), el grupo alternante de grado 5.

Finalmente, si m = 5, entonces se tiene un [120,60,24]-código binario autodual extremal. Durante los últimos años J. De la Cruz, S. Bouyuklieva y W. Willems [4], [8] demostraron que los únicos números primos que pueden dividir al orden del grupo de automorfismos de este, si existe, son 2, 3, 5, 7, 19, 23 y 29. Además se demostró que si $p = 3, 5, 7, 19, 23, 29$, entonces p^2 no divide a dicho orden.

En el presente trabajo de tesis, en general, se presentaran condiciones suficientes y necesarias para que un código C con un automorfismo de orden un primo impar sea autodual y además construiremos códigos autoduales doblemente pares con parametros [40,20,8] (extremales) y [120,60,20] (optimales) utilizando técnicas de construcción vía automorfismos del código, cuyo orden es un primo impar.

Este documento está dividido en 4 capítulos. El primero trata sobre conceptos

básicos de los códigos lineales, centrando nuestra atención en las propiedades y ventajas que presentan algunas familias especiales de estos, como son los códigos cíclicos y los autoduales. Esta caracterización y conceptualización será necesaria cuando se aborden los resultados fundamentales para la posible construcción del código.

En el segundo capítulo introducimos el concepto de automorfismo de un código y exploramos las técnicas planteadas por W. C. Huffman en [5] y trascendidas por V. Y. Yorgov en [21], las cuales nos proporcionan herramientas para la posible construcción de un código C autodual, mediante la descomposición de este en los subcódigos $F_\sigma(C)$ y $E_\sigma(C)$ a partir de la información que nos brinda el automorfismo σ. La finalidad de este capítulo es recoger información sobre la estructura de los subcódigos de C y el comportamiento de los vectores que lo conforman, para luego utilizarlo en la posible construcción del código.

El tercer capítulo trata sobre la utilización de los resultados generales obtenidos en el capitulo anterior para construir códigos extremales tipo II con parametros [40,20,8] con automorfismos de orden 5 y 19. Además construimos veintiún códigos optimales tipo II con parametros [120,60,20] con un automorfismo de orden 23 y veinte con automorfismos de orden 29. Cabe resaltar que la construcción de los códigos con automorfismos de orden 29, es un aporte personal al trabajo de tesis.

Finalmente en el capítulo 4 se anotan los anexos de la tesis, los cuales son las rutinas de programación hechas en MAGMA, para cada una de las construcciones de los códigos en este trabajo y las matrices generadoras de los 9 códigos binarios autoduales de parámetros [24,12] de la tabla 1 de [7].

Capítulo 1

Preliminares

1.1 Códigos lineales

1.1.1 Definición. Sea $\mathbb{F}_q$ un cuerpo finito con q elementos y $n \in \mathbb{N}$. Un *código lineal* C sobre $\mathbb{F}_q$, es un subespacio del espacio vectorial $\mathbb{F}_q^n$.

Si $\dim_{\mathbb{F}_q} C = k$, entonces diremos que C es un $[n, k]$-código lineal sobre $\mathbb{F}_q$ de longitud n. Los códigos sobre $\mathbb{F}_2$ son llamados binarios.

1.1.2 Definición. Sea $\mathbb{F}_q$ un cuerpo finito y C un $[n, k]$-código sobre $\mathbb{F}_q$.

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

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

   Nótese que la expresión $\mathbb{F}_q^k G$ es otra forma de representar todas las combinaciones lineales de G.

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

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

Del álgebra lineal se sigue que:

$$\mathrm{Ran}(H) = n - \dim(\ker(H)) = n - \dim_{\mathbb{F}_q}(C) = n - k.$$

1.1.3 Teorema. Sea $G \in \mathbb{F}_q^{k\times n}$ 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 $\mathbb{F}_q$, si y solo si $B = (g_1, \ldots, g_k)$ es una base para C.

Demostración. Sea $B = (g_1, \ldots, g_k)$ una base para C. Entonces para todo $u \in \mathbb{F}_q^k$ se verifica que $uG \in C$. Por lo tanto

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

Reciprocamente, supongamos que G es una matriz generadora para C. Es decir, $C = \{uG \mid u \in \mathbb{F}_q^k\}$. 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

$$C = \{uG \mid u \in \mathbb{F}_q^k\} = \{u_1 g_1 + \cdots + u_k g_k \mid u_j \in \mathbb{F}_q\},$$

en consecuencia $C = \langle g_1, \ldots, g_k \rangle$ y dado que $\dim_{\mathbb{F}_q}(C) = k$, se sigue que B es una base para C. ∎

1.1.4 Definición. Sea $\mathbb{F}_q$ un cuerpo finito y C un código lineal de $\mathbb{F}_q^n$.

1. Dados dos vectores $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$. Definimos la *distancia de Hamming* d entre ellos, como el número natural:

$$d(u, v) := |\{i \in \{1, \ldots, n\} : u_i \neq v_i|.$$

2. Definimos y denotamos la *distancia mínima* de C, como

$$d(C) := \text{mín}\{d(u, v) \mid u, v \in C, u \neq v\}.$$

3. Para todo vector $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$, definimos el *soporte* de u como

$$\text{sop}(u) := \{j \mid u_j \neq 0\}$$

4. Para todo vector $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$, definimos el *peso* de u como

$$\mathrm{wt}(u) := |\mathrm{sop}(u)| = d(u, 0)$$

5. Definimos el *peso minimal* del código C como

$$\mathrm{wt}(C) := \mathrm{mín}\{\mathrm{wt}(u) \mid 0 \neq u \in C\} \text{ y para } C = \{0\},\ \mathrm{wt}(C) := 0$$

Hablaremos entonces de un $[n, k, d]$-código lineal C de $\mathbb{F}_q^n$, si C tiene dimensión k y distancia mínima d. Llamaremos a n, k y d los parametros de C.

1.1.5 Lema. Sea C un código lineal sobre $\mathbb{F}_q$. Entonces la distancia de Hamming cumple los axiomas de métrica. Es decir

1. $d(u, v) \geq 0$ y $d(u, v) = 0$ si y solo si $u = v$.
2. $d(u, v) = d(v, u)$.
3. $d(u, v) \leq\ d(u, z) + d(z, v)$.

Además, d es invariante bajo traslaciones. Es decir, para todo $u, v, w \in C$ se verifica que $d(u + w, v + w) = d(u, v)$.

Demostración. Las partes 1 y 2, se obtienen directamente de la definición de distancia de Hamming. Para probar la desigualdad triangular, sean

$$u := (u_1, \ldots, u_n),\ v := (v_1, \ldots, v_n),\ w := (w_1, \ldots, w_n) \in \mathbb{F}_q^n.$$

Entonces si $u_j \neq v_j$ se tiene que $u_j \neq w_j$ ó $v_j \neq w_j$, de lo cual se sigue la afirmación.
Por otra parte tenemos que:

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

■

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

Demostración. Por definición de distancia mínima tenemos que

$$d(C) = \mathrm{mín}\{d(u, v) \mid u, v \in C, u \neq v\}$$

Si utilizamos la propiedad de invariaza bajo traslaciones de la distancia, tenemos que

$$d(C) = \text{mín}\{d(u-v,0) \mid u,v \in C, u \neq v\}.$$

De donde

$$d(C) = \text{mín}\{\text{wt}(u-v) \mid u,v \in C, u \neq v \neq 0\}$$

y puesto que el código es lineal sobre $\mathbb{F}_q$, entonces

$$\{x : x \in C, x \neq 0\} = \{u-v : u,v \in C, u \neq v\}$$

En concecuencia

$$d(C) = \text{mín}\{\text{wt}(x) \mid x \in C, x \neq 0\} = \text{wt}(C).$$

■

El teorema 1.1.6 reduce el costo computacional para el cálculo de la distancia mínima de un código lineal, dado que se pasa de calcular $\begin{pmatrix} |C| \\ 2 \end{pmatrix}$ distancias a calcular $|C|-1$ pesos.

A continuación mostramos algunas cotas que brindan información sobre la longitud de un código en relación con su dimensión y distancia mínima y que serán de gran utilidad en lo que sigue de este trabajo.

1.1.7 Lema. Sea C un $[n,k,d]$-código binario. Entonces se cumple que

1. $n \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil$. **(Cota de Griesmer)**
2. Si $d \leq 2^{k-2}-2$, entonces $n > \sum_{i=0}^{k-1} \lceil d/2^i \rceil$. **(Cota de Logachev)**

Demostración. Las demostraciones de las cotas de Griesmer y Logachev se encuentran ampliamente detalladas en [14] y [11] respectivamente. ■

1.1.8 Lema. (Cota de Singleton) Si C es un $[n,k,d]$-código lineal sobre $\mathbb{F}_q$, entonces se cumple que $k \leq n-d+1$.

Demostración. Sea $f : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d+1}$ la aplicación que borra las últimas $d-1$ coordenadas; o sea, $f(C) = C^{*(d-1)}$. Es claro que $f(C)$ es un código en

$\mathbb{F}_q^{n-d+1}$. La función f restringida a C es inyectiva. En efecto, si $c, c' \in C$ con $f(c) = f(c')$, entonces

$$c = c_1 \dots c_{n-d+1} \dots x_{d-1},$$

$$c' = c_1 \dots c_{n-d+1} \dots y_{d-1},$$

y por lo tanto $\mathrm{d}(c, c') \leq d - 1$, lo cual es absurdo. Luego,

$$q^k = |C| = |f(C)| \leq q^{n-d+1},$$

de donde $k \leq n - d + 1$. ∎

Esta cota, conocida como la cota de Singleton, dice que los parametros principales de un código son muy rígidos. Es decir, que no es posible tener tamaño y distancia mínima simultaneamente grandes.

1.1.9 Definición. Un $[n, k, d]$-código que satisface la igualdad en la cota de Singleton se dice que es un MDS-código (*maximun distance separable*).
Es decir, dado que $d = n - k + 1$, entre todos los códigos de longitud n que son t-correctores, entonces C es uno que códifica el mayor número de palabras.

1.1.10 Corolario. Sea C un $[n, k, d]$-código sobre $\mathbb{F}_q$. Las siguientes afirmaciones son equivalentes:

1. C es un MDS-código.
2. Cada k columnas de una matriz G, generadora de C, son linealmente independientes.
3. Cada $n - k$ columnas de una matriz H, de control de C, son linealmente independientes.

Demostración. [14] pág 319.

1.2 Código dual

1.2.1 Definición. Definimos el *producto escalar* entre dos vectores

$$u = (u_1, \dots, u_n) \text{ y } v = (v_1, \dots, v_n) \in \mathbb{F}_q^n,$$

mediante la expresión:

$$u \cdot v = \sum_{i=1}^{n} u_i v_i. \tag{1.1}$$

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

1. Definimos $C^{\perp} := \{u \in \mathbb{F}_q^n \mid u \cdot v = 0, v \in C\}$ y decimos que $C^{\perp}$ es el *código dual* de C con respecto al producto escalar (1.1).
2. Si $C \subseteq C^{\perp}$, entonces C es llamado *auto-ortogonal*.
3. Si $C = C^{\perp}$, entonces C es llamado *autodual*.

1.2.3 Teorema. Sea C un $[n,k]$-código sobre el campo finito $\mathbb{F}_q$. Entonces se cumple que:

1. $C^{\perp}$ es un $[n, n-k]$-código sobre $\mathbb{F}_q$.
2. Todo código autodual es un $[n, \frac{n}{2}]$-código.

Demostración.

1. Sea $G = (g_{ij})$ una matriz generadora para C. Entonces G es de tamaño $k \times n$, donde k es la $\dim_{\mathbb{F}_q}(C)$ y n es la $\dim_{\mathbb{F}_q}({\mathbb{F}_q}^n)$. Tenemos entonces que $v \in C^{\perp}$ si y solo si $\sum_{j=1}^{n} v_j g_{ij} = 0$, para $i = 1, \ldots, k$. Este es un sistema homogeneo de k ecuaciones y n incógnitas $\{v_1, \ldots, v_n\}$ y dado que el rango de G es k, se concluye que existen $n-k$ variables libres. Por lo tanto la solución del sistema es un subespacio de dimensión $n-k$, es decir $\dim_{\mathbb{F}_q}(C^{\perp}) = n-k$.
2. Sea $\dim_{\mathbb{F}_q}(C) = k$. Si C es autodual, entonces por definición $C = C^{\perp}$, en consecuencia $\dim_{\mathbb{F}_q}(C) = \dim_{\mathbb{F}_q}(C^{\perp})$ y tenemos $k = n-k$, de donde $k = \frac{n}{2}$. ∎

1.2.4 Definición. Sea $1 < r \in \mathbb{N}$. Un código C se denomina *r-divisible*, si $r \mid \mathrm{wt}(c)$, para todo $c \in C$.

En particular, un código binario 4-divisible es denominado *doblemenete par*, si C es binario pero no doblemente par decimos que C es *simplemenete par* y si C es binario 2-divisible decimos que C es *par*. A continuación vemos que todo código binario autodual contiene solamente vectores de peso par.

1.2.5 Lema. Sea C un código binario autodual. Entonces C es par.

Demostración. Sea C un código binario autodual y $v = (v_1, \ldots, v_n) \in C$. Entonces

$$v \cdot v = v_1 v_1 + \cdots + v_n v_n = \sum_{i=1}^{n} v_i^2 = 0$$

y dado que $v_i^2 = \begin{cases} 0, & \text{para } v_i = 0 \\ 1, & \text{para } v_i \neq 0 \end{cases}$, entonces $0 = \sum_{i=1}^{n} v_i^2 = \sum_{v_{i\neq 0}} 1 = \text{wt}(v)$.

Es decir $2 \mid \text{wt}(v)$. ∎

Gleason, Pierce y Turyn demuestrán en [1] que si $1 < r \in \mathbb{N}$ divide el peso de cada vector de un código binario autodual, entonces $r = 2$ o $r = 4$.

1.2.6 Definición. Sea C un código binario autodual. Se dice que C es un código **Tipo II** si C es doblemente par y **Tipo I** si C es simplemente par.

1.2.7 Teorema. Sea C un código binario lineal. Entonces se cumple que:

1. Si C es auto-ortogonal y cada vector de una matriz generadora de C tiene peso divisible por 4, entonces el código C es doblemente par.

2. Si C es doblemente par, entonces C es auto-ortogonal.

Demostración. Ver [6] pág 10. ∎

En la teoría de códigos existen 4 códigos expeciales, $G_{24}, G_{23}, G_{12}, G_{11}$, introducidos por Marcel Golay en 1949 y a los cuales se les conoce como códigos de Golay. Los códigos G_{24} y G_{23} son binarios, mientras que los G_{12} y G_{11} son ternarios.
En este trabajo de tesis nos interesa analizar más detalladamente el código G_{24}.

1.2.8 Definición. El *código de Golay* G_{24} es el código lineal binario definido por la matriz generadora

$$G := (Id_{12}|A) \in M_{12\times 24}(\mathbb{F}_2),$$

donde $Id_{12} \in \mathbb{F}_2^{12\times 12}$ es la matriz identidad con unos en la diagonal principal y

ceros en las demás posiciones y A es una matriz que tiene la siguiente forma:

$$A := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{1.2}$$

Note la estructura ciclica que posee A. El siguiente teorema recoge las propiedades más importantes del código de Golay G_{24}.

1.2.9 Teorema. El código de Golay G_{24} tiene las siguientes propiedades

(1). G_{24} es autodual, es decir $G_{24}^{\perp} = G_{24}$.

(2). G_{24} está generado por la matriz $G = (A|Id_{12})$.

(3). G_{24} es doblemente par.

(4). G_{24} no tiene vectores de peso 4

(5). G_{24} es un $[24, 12, 8]$-código.

Demostración. Sea G la matriz generadora de G_{24} dada en 1.2.8.

1. Como las filas de G son ortogonales, entonces todo par de vectores de G_{24} son ortogonales. Luego, $G_{24} \subseteq G_{24}^{\perp}$. Pero como $\dim(G_{24}^{\perp}) = \dim(G_{24})$, entonces se tiene que $G_{24}^{\perp} = G_{24}$.

2. Se sigue del inciso (1) y del hecho que $A^T = A$.

3. El peso de las filas de G es 8 ó 12, por lo tanto divisibles por 4. Si x e y son filas de G, entonces tenemos que

$$\mathrm{wt}(x + y) = \mathrm{wt}(x) + \mathrm{wt}(y) - 2\mathrm{wt}(x \cdot y).$$

Pero $\mathrm{wt}(x \cdot y) \equiv x \cdot y = 0$ mód 2 y por lo tanto $\mathrm{wt}(x + y)$ es multiplo de 4. Por inducción, el peso de la suma de cualquier número de filas de G es multiplo de 4.

4. Usaremos las dos matrices generadoras $G_1 := (Id_{12}|A)$ y $G_2 := (A|Id_{12})$ de G_{24}. Denotemos a $v \in G_{24}$ tal que $v = v_I v_D$, donde $v_I, v_D \in \mathbb{F}_2^{12}$ son la parte izquierda y derecha de v, respectivamente.

   Supongamos que $\mathrm{wt}(v) = 4$. Note que cualquier combinación lineal de las filas de G_1 tiene parte izquierda con peso mayor que 1. Así mismo cualquier combinación lineal de las filas de G_2 tiene parte derecha con peso mayor que 1. Entonces $\mathrm{wt}(v_I) \geq 1$ y $\mathrm{wt}(v_D) \geq 1$. Ahora, si $\mathrm{wt}(v_I) = 1$, entonces v es una fila de G y por lo tanto $\mathrm{wt}(v_D) \neq 4$. Luego $\mathrm{wt}(v_I) \geq 2$ y analogamente $\mathrm{wt}(v_D) \geq 2$. Por lo tanto, la única posibilidad es $\mathrm{wt}(v_I) = w(v_D) = 2$. Luego, v es la suma de dos filas x e y de G_1. Lo cual es absurdo, pues $\mathrm{wt}(x + y) \neq 4$ para todo par de filas x, y de G_1. Luego G_{24} no tiene vectores de peso 4.

5. Por los incisos (3) y (4) tenemos que $\mathrm{wt}(G_{24}) \geq 8$, y la segunda fila de G tiene peso 8, luego $\mathrm{d}(G_{24}) = 8$. ∎

1.3 Códigos extremales

Mallows y Sloane demostraron en [13], que un código de tipo II de longitud n, tiene distancia mínima $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$. Donde $\lfloor x \rfloor$ representa el mayor entero menor o igual a x. Con distintos argumentos E. M. Rains probó en [17], que esta cota también es válida sin la condición de doble paridad, siempre que $24 \nmid n + 2$. Lo anterior se recoge en el siguiente teorema:

1.3.1 Teorema. ([13], [17])**(Mallows-Sloane, Rains)** Sea C un código binario autodual con parametros $[n, k, d]$. Entonces se cumple que

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

y

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 6, \text{ si } n \equiv 22 \text{ mód } 24.$$

Un código binario autodual cuya distancia mínima alcanza la respectiva cota superior se denomina *extremal*. En las aplicaciones de la teoría de códigos, los códigos extremales son de gran utilidad dado que al tener la maxima distancia minimal, poseen mayor capacidad en la corrección de errores. Sin embargo en muchos casos se dificulta la construcción de este tipo de códigos, por lo cual toman gran importancia los códigos con distancia mínima lo más cercana posible a la de un código extremal de la misma longitud. Estos códigos son

denominados *optimales.*

X. Ma [12] estableció en 1998, que no existen códigos extremales de tipo II con longitud $n > 3984$. Para longitudes pequeñas es bien conocida la existencia de un solo código extremal de tipo II de longitud 8, dos de longitud 16, uno de longitud 24, cinco de longitud 32 y uno de longitud 48. La mayor longitud para la cual se ha construido un código extremal doblemente par es 136 y corresponde a un código doblemente circulante. Por lo tanto existe una gran diferencia entre la cota superior para la longitud y lo construido hasta el momento.

Por otra parte, E. M. Rains demostró en [17], que todo código binario autodual, extremal con parámetros $[24m, 12m, 4m + 4],\ m \in\ N$, es de tipo II. S. Zhang [24] demostró en 1999 que códigos con estos parámetros tienen longitud $n = 24m \leq 3672$ y como notamos anteriormente, la existencia solo ha podido demostrarse para valores muy pequeños de m. Assmus-Mattson en 1969 demostraron que los soportes de los vectores de peso fijo de este tipo de códigos forman un 5-Diseño, lo cual hace que este tipo de códigos sean de gran importancia para la geometría, especialmente la teoría de diseños..

Solo se conocen dos códigos autoduales extremales con estos parámetros, para $m = 1$ y $m = 2$, los cuales corresponden respectivamente al [24,12,8]-código extendido de Golay y [48,24,12]-código resto cuadrático.

Aunque para $m > 2$ no se han costruido códigos con estos parametros, sí se han hecho diferntes estudios en los que se ha obtenido información parcial sobre su grupo de automorfismos.

1.4 Enumerador de peso y polinomios de Gleason

1.4.1 Definición. Definimos el *enumerador de pesos* de un código C como la suma formal

$$W_C(y) := \sum_{i=0}^{n} A_i y^i,$$

donde A_i es el número de vectores de peso i en C. Es decir,

$$A_i = |\{v \in C : \mathrm{wt}(v) = i\}|.$$

Los números $A_0, \ldots, A_n$ se conocen como la *distribución de pesos* de C y si C es un $[n, k]$-código lineal, su *enumeardor de peso homogeneo* es el polinomio

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

Los códigos autoduales sobre $\mathbb{F}_2$ tienen enumeradores de peso que pueden ser expresados como combinaciones de polinomios especiales, que son los enumeradores de peso de códigos específicos de longitudes pequeñas. Estos polinomios, denotados como $g_1(x,y), g_2(x,y)$ y $g_3(x,y)$, se conocen como *Polinomios de Gleason* y proporcionan una herramienta poderosa en el estudio de todos los códigos autoduales sobre $\mathbb{F}_2$.

1.4.2 Teorema. (Gleason) Sea C un $[n, n/2]$-código sobre $\mathbb{F}_2$ y sean además

$$\begin{aligned} g_1(x,y) &= y^2 + x^2, \\ g_2(x,y) &= y^8 + 14x^4y^4 + x^8, \\ g_3(x,y) &= y^{24} + 759x^8y^{16} + 2576x^{12}y^{12} + 759x^{16}y^8 + x^{24}. \end{aligned}$$

Entonces:

1. Si C es autodual,
$$W_C(x,y) = \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} a_i g_1(x,y)^{\frac{n}{2}-4i} g_2(x,y)^i.$$
2. Si C es autodual y doblemente par,
$$W_C(x,y) = \sum_{i=0}^{\lfloor \frac{n}{24} \rfloor} a_i g_2(x,y)^{\frac{n}{8}-3i} g_3(x,y)^i.$$

Los a_i son racionales con $\sum_{i=0}^{k} a_i = 1$, donde $k = \lfloor \frac{n}{8} \rfloor$ o $k = \lfloor \frac{n}{24} \rfloor$ y en ambos casos si C es extremal, entonces su polinomio enumerador de peso es único.

Demostración. Ver [6], pág 341-344. ∎

Del teorema 1.4.2 se deriva un resultado importante en el estudio de los códigos autoduales doblemente pares, el cual expresamos en el siguiente corolario.

1.4.3 Corolario. Si C es un código binario autodual doblemente par de longitud n, entonces $8 \mid n$.

1.5 Códigos cíclicos

En esta sección supondremos que n y q son coprimos. En particular, si $q = 2$ entonces n es impar.

1.5.1 Definición. Un código lineal C es *cíclico* si para cada vector $c = (c_0c_1....c_{n-1}) \in C$, se cumple que el vector $c' = (c_{n-1}c_0...c_{n-2})$, también está en C.

Podemos comprobar que c' se obtiene a partir de c mediante la *traslación cíclica* de coordenadas $i \mapsto i+1$ mód n. El código lineal C es cíclico si es cerrado bajo la traslación cíclica $(c_0c_1....c_{n-1}) \mapsto (c_{n-1}c_0...c_{n-2})$, lo que implica que C sea cerrado bajo todas las traslaciones cíclicas

$$(c_0c_1....c_{n-1}) \mapsto (c_k...c_{n-1}c_0...c_{k-1}).$$

1.5.2 Definición. Si C es un código lineal q-ario y $c = (c_0c_1 \dots c_{n-1})$ es un vector de C. Entonces podemos asignarle a c un polinomio mediante la función:

$$\phi : C \longrightarrow \mathbb{F}_q[x], \text{ donde } \phi(c) = c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

De ahora en adelante, ignoraremos la función ϕ y pensaremos en los vectores del código como polinomios y viceversa. Note que si

$$c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \phi(C),$$

entonces el polinomio $xc(x) = c_{n-1}x^n + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}$ representará la traslación cíclica del vector c en $\phi(C)$ si $x^n = 1$. Dicho formalmente, el hecho de que C sea cíclico implica que si $c(x) \in \phi(C)$, entonces $xc(x)$ también está en $\phi(C)$, multiplicando mód $\langle x^n - 1\rangle$. Esto sugiere que el contexto más adecuado para estudiar los códigos cíclicos son el anillo de clases residuales:

$$R_n := \mathbb{F}_q[x]/\langle x^n - 1\rangle.$$

Este es el álgebra de polinomios de grado menor que n, con la suma usual de polinomios y el producto de polinomios mód $\langle x^n - 1\rangle$.

1.5.3 Definición. Un *ideal* I de un anillo conmutativo R, es un subconjunto de R que satisface las siguientes condiciones

1. I es un subgrupo aditivo de R, $(I \leq R)$.
2. Si $a \in I$, entonces $ab \in I$ para todo $b \in R$.

La primera condición significa que I es un subgrupo del grupo aditivo de R.

1.5.4 Lema. Un código C es cíclico si y solo si

$$\phi(C) \text{ es un ideal en } \mathbb{F}_q[x]/\langle x^n - 1\rangle.$$

Demostración. Para probar que $\phi(C)$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, se debe cumplir que $\phi(C) \leq \mathbb{F}_q[x]/\langle x^n - 1\rangle$ y que para $f \in \phi(C)$ se verifica que $gf \in \phi(C)$, para todo $g \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Dado que C es cíclico y por ende lineal, es claro que $\phi(C)$ es cerrado con la suma. Por lo tanto $\phi(C) \leq \mathbb{F}_q[x]/\langle x^n - 1\rangle$.
La segunda condición la probamos para el caso base, es decir para

$$g = x \in \mathbb{F}_q[x]/\langle x^n - 1\rangle \text{ y } f = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in \phi(C).$$

Tenemos que

$$\begin{aligned} gf &= x(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) \\ &= c_0x + c_1x^2 + \cdots + c_{n-1}x^n \\ &\equiv c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1} \text{ mód}(x^n - 1) \in \phi(C) \\ &= c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} \in \phi(C). \end{aligned}$$

Reciprocamente, si $\phi(C)$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ y se cumple que $f \in \phi(C)$, entonces $xf = c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1} \in \phi(C)$, con lo que se prueba que si $(c_0c_1....c_{n-1}) \in C$, entonces $(c_{n-1}c_0...c_{n-2}) \in C$, es decir C es cíclico. ∎

El siguiente resultado reune algunos hechos básicos de los códigos cíclicos

1.5.5 Teorema. Sea $\{0\} \neq C$ un ideal de R_n, es decir un código cíclico de longitud n. Entonces:

1. Existe un único polinomio mónico $g(x)$ de grado mínimo en C. Además, este polinomio genera C, es decir $C = \langle g(x)\rangle$.
2. $g(x)|(x^n - 1)$.
3. Si $\text{grad}(g(x)) = r$, entonces C tiene dimensión $n - r$. Más aún,
$$C = \langle g(x)\rangle = \{r(x)g(x) : \text{grad}(r(x)) < n - r\}.$$
4. Si $g(x) = g_0 + g_1x + \cdots + g_rx^r$, entonces $g_0 \neq 0$ y C tiene matriz generadora

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_r \end{pmatrix},$$

donde cada fila de G es una traslación cíclica de la fila previa.

Demostración.

1. Sea $g(x)$ y $f(x)$ dos polinomios mónicos de grado mínimo r en C. Entonces el grado del polinomio $f(x) - g(x)$, es menor que r y dado que r es el grado mínimo en C, tenemos que $f(x) - g(x) \equiv 0$, de donde se concluye que $f(x) = g(x)$. Ahora, sea $g(x)$ el polinomio mónico de grado mínimo en C. Dado que C es un ideal, tenemos que $\langle g(x) \rangle \subseteq C$. Por otra parte, sea $a(x)$ cualquier otro polinomio en C. Por el algoritmo de la división en $\mathbb{F}_q[x]$, tenemos que $a(x) = g(x)b(x) + r(x)$, donde el grado de $r(x)$ es menor que el grado de $g(x)$. Por definición de ideal, $r(x) \in C$. Pero esto contradice que $g(x)$ sea de grado mínimo en C. Por lo tanto $r(x) \equiv 0$ y $a(x) = g(x)b(x)$, es decir $C \subseteq \langle g(x) \rangle$.

2. Sea $g(x)$ el polinomio mónico de grado mínimo en C. Por el algoritmo de la división en $\mathbb{F}_q(x)$, tenemos que $x^n - 1 = a(x)g(x) + r(x)$, donde el grado de $r(x)$ es menor que el grado de $g(x)$. Ahora como $r(x) = -a(x)g(x) \mod \langle x^n - 1 \rangle$, entonces $r(x) \in C$. Esto contradice el hecho de que $g(x)$ sea de grado mínimo en C. Por lo tanto $r(x) \equiv 0$. Probando así que $g(x)$ divide a $x^n - 1$.

3. El ideal generado por $g(x)$ es $\langle g(x) \rangle = \{f(x)g(x) \mid f(x) \in R_n\}$.

   Queremos ver que basta restringir $f(x)$ a polinomios de grado menor que $n - r$. Sabemos que $x^n - 1 = h(x)g(x)$ para algún polinomio $h(x)$ de grado $n - r$. Dividiendo, tenemos que

   $$f(x) = q(x)h(x) + r(x), \text{ con } \operatorname{grad}(r(x)) < n - r.$$

   Entonces,

   $$f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n - 1) + r(x)g(x);$$

y así $f(x)g(x) = r(x)g(x)$ en R_n, que es lo que queríamos establecer. Esto también muestra que el conjunto $g(x), xg(x), \cdots, x^{n-r+1}g(x)$ genera C, y como es linealmente independiente, forma una base de C. Luego, $\dim(C) = n - r$.

4. Si $g_0 = 0$, entonces $g(x) = xg_1(x)$, con $\text{grad}(g_1(x)) < r$. Pero entonces tenemos que

$$g_1(x) = 1 \cdot g_1(x) \equiv x^n g_1(x) \equiv x^{n-1} x g_1(x) = x^{n-1} g(x) \in C,$$

lo cual es absurdo puesto que $g_1 \neq 0$ tiene grado menor que el grado de $g(x)$. Por lo tanto $g_0 = 0$. Por último, G es una matriz generadora de C, puesto que $g(x), xg(x), \cdots, x^{n-r+1}g(x)$ es una base de C. ∎

1.5.6 Lema. Un polinomio mónico $p(x)$ en R_n es el polinomio generador de un código cíclico de longitud n si y solo si $p(x)|(x^n - 1)$.

Demostración. Supongamos que $p(x)|(x^n - 1)$ y que $g(x)$ es el polinomio generador de $C = \langle p(x) \rangle$, con $p(x) \neq g(x)$. Como $p(x)$ y $g(x)$ son mónicos, entonces $\text{grad}(g(x)) < \text{grad}(p(x))$. Por hipótesis, $x^n - 1 = p(x)f(x)$ para algún polinomio $f(x) \neq 0$. Más aún, como $g(x) \in \langle p(x) \rangle$, entonces $g(x) \equiv a(x)p(x)$, para algún $a(x) \in R_n$. Luego, tenemos que

$$g(x)f(x) \equiv a(x)p(x)f(x) \equiv a(x)(x^n - 1) \equiv 0.$$

Pero, $\text{grad}(g(x)f(x)) < \text{grad}(p(x)f(x)) = n$, y así $g(x)f(x) = 0$, lo cual es imposible. Por lo tanto, $p(x) = g(x)$. ∎

Dado que el polinomio generador $g(x)$ de un $[n, n-r]$-código cíclico en R_n divide a $x^n - 1$, tenemos que

$$x^n - 1 = g(x)h(x),$$

donde $h(x)$ es un polinomio de grado $n - r$, llamado *polinomio de chequeo o de control de* C. El siguiente resultado resume las propiedades de $h(x)$.

1.5.7 Teorema. Sea $h(x)$ el polinomio de chequeo de un código cíclico C en R_n. Entonces se cumple que:

1. El código C puede describirse como

$$C = \{p(x) \in R_n \mid p(x)h(x) \equiv 0\}.$$

2. Si $h(x) = h_0 + h_1x + \cdots + h_{n-r}x^{n-r}$, entonces la matriz de control de C está dada por

$$H = \begin{pmatrix} h_{n-r} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & \cdots & h_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & \cdots & h_0 \end{pmatrix}.$$

Demostración.

1. Sea $g(x)$ el polinomio generador de C. Si $p(x) \in C$, entonces $p(x) = f(x)g(x)$, para algún $f(x) \in R_n$. Luego,

$$p(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) \equiv 0.$$

   Por otra parte, si $p(x) \in R_n$ y $p(x)h(x) \equiv 0$, tenemos que

$$p(x) = q(x)g(x) + r(x), \ \text{congr}(r(x)) < r.$$

   Entonces,

$$p(x)h(x) = q(x)g(x)h(x) + r(x)h(x),$$

   de donde $r(x)h(x) \equiv 0$. Sin embargo, $\text{gr}(r(x)h(x)) < r + (n - r) = n$, por lo que $r(x)h(x) = 0$. Luego, $r(x) = 0$ y $p(x) = q(x)g(x) \in C$.

2. Si $c(x) \in C$, entonces $c(x)h(x) \equiv 0$. Dado que $\text{gr}(c(x)h(x)) < 2n - r$, deducimos que los coeficientes de $x^{n-r}, x^{n-r+1}, \ldots, x^{n-1}$, en el producto $c(x)h(x)$ son 0, es decir,

$$\begin{aligned} c_0h_{n-r} + c_1h_{n-r+1} + \cdots + c_{n-r}h_0 &= 0 \\ c_1h_{n-r} + c_2h_{n-r+1} + \cdots + c_{n-r+1}h_0 &= 0 \\ &\vdots \\ c_{r-1}h_{n-r} + c_rh_{n-r+1} + \cdots + c_{n-1}h_0 &= 0. \end{aligned}$$

   Pero esto es equivalente a $(c_0c_1 \ldots c_{n-1})H^T = 0$, y así H genera un código C' que es ortogonal a C, o sea, $C' \subset C^\perp$. Como $h_{n-r} \neq 0$, se sigue que $\dim(C) = r$, y por lo tanto $C' = C^\perp$. ∎

El polinomio generador de un código cíclico tiene la propiedad de que su grado nos da información acerca de la dimensión del código. Pero para encontrar los polinomios generadores debemos encontrar los factores de $x^n - 1$ y esto puede ser muy complicado. Hay otros generadores que se pueden encontrar sin factorizar $x^n - 1$. Estos son llamados generadores idempotentes.

1.5.8 Definición. Un polinomio generador $e(x)$ de un ideal I en R_n es llamado *generador idempotente*, si este polinomio es un idempotente, es decir, si $e^2(x) = e(x)$.

Este generador actua como la unidad para el ideal, puesto que si $a(x) \in \langle e(x) \rangle$, entonces $a(x) = b(x)e(x)$ y $a(x)e(x) = b(x)e^2(x) = b(x)e(x) = a(x)$. Reciprocamente, un idempotente que actúa como unidad para un ideal I, genera a I.

1.5.9 Corolario. Sean C_1 y C_2 códigos cíclicos con polinomios generadores $g_1(x)$ y $g_2(x)$ respectivamente. Entonces $C_1 \subseteq C_2$ si y solo si $g_2(x)$ divide a $g_1(x)$.

Demostración. $C_1 \subseteq C_2$ si y solo si $\langle g_1(x) \rangle \subseteq \langle g_2(x) \rangle$ y esto ocurre si y solo si $g_2(x)$ divide a $g_1(x)$. ∎

1.5.10 Teorema. Sean C_1 y C_2 códigos cíclicos con polinomios generadores $g_1(x)$ y $g_2(x)$ y generadores idempotentes $e_1(x)$ y $e_2(x)$ respectivamente. Entonces $C_1 \cap C_2$ tiene como polinomio generador $\text{mcm}(g_1(x), g_2(x))$ y generador idempotente $e_1(x)e_2(x)$, y $C_1 + C_2$ tiene como polinomio generador $\text{mcd}(g_1(x), g_2(x))$ y generador idempotente $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Demostración. Ver [16], pág 80.

1.5.11 Teorema. Sea $h_0(x)h_1(x)\cdots h_s(x)$ la factorización del polinomio $x^n - 1$ sobre $\mathbb{F}_q$, donde $h_0(x) = x - 1$ y $h_j(x)$ es irreducible. Sean además $g_j(x) = \frac{x^n-1}{h_j(x)}$ y $I_j = \langle g_j(x) \rangle$ el ideal de R_n generado por $g_j(x)$, $j = 0, 1, \ldots, s$. Si $e_j(x)$ es el generador idempotente de I_j, $j = 0, 1, \ldots, s$, entonces se cumple que:

1. El ideal I_j, para $j = 0, 1, \ldots, s$, es un ideal minimal de R_n;
2. $R_n = I_0 \oplus I_1 \oplus \cdots \oplus I_s$;
3. I_j es un campo isomorfo a $\mathbb{F}_q^{gr(h_j(x))}$, $j = 0, 1, \ldots, s$;
4. $e_i(x)e_j(x) = 0$, $i \neq j$;

5. $\sum_{j=0}^{s} e_j(x) = 1$.

Demostración.

1. Supongamos que I_j, para $j = 0, 1, \cdots, s$ no es un ideal minimal de R_n. Entonces existe un ideal $I \neq 0$, tal que $I \subset I_j$. Luego I es también un ideal de R_n y por teorema 1.5.5, existe un polinomio $g(x)$ mónico y de grado mínimo tal que $\langle g(x)\rangle = I$ y $g(x)|(x^n - 1)$. Además como $I \subset I_j$, por el corolario 1.5.9, tenemos que $g_j(x)|g(x)$, siendo $g_j(x) = \frac{x^n-1}{h_j(x)}$, el generador de I_j y $g_j(x) \neq g(x)$. Ahora, como $h_j(x) = \frac{x^n-1}{g_j(x)}$, entonces $x^n - 1 = h_j(x)g_j(x)$ y como $g_j(x)|g(x)$, existe $p(x)$ tal que $g_j(x) = \frac{g(x)}{p(x)}$ y tenemos que $x^n - 1 = h_j(x)\frac{g(x)}{p(x)}$, de donde $h_j(x) = \frac{(x^n-1)(p(x))}{g(x)}$, pero como $g(x)|(x^n - 1)$, entonces existe $q(x)$ tal que $\frac{(x^n-1)}{g(x)} = q(x)$, teniendo así que $h_j(x) = q(x)p(x)$, lo cual es absurdo ya que $h_j(x)$ es irreducible. Luego nuestro supuesto de que I_j no es un ideal minimal es falso.

2. Como $\{g_i(x) \mid 1 \leq i \leq s\}$ no tienen ningún factor común y cada polinomio $g_i(x)$ divide a $x^n - 1$, entonces $\text{mcd}(g_1(x), ..., g_s(x)) = 1$. Aplicando el algoritmo de Euclides inductivamente tenemos que existen $a_i(x) \in \mathbb{F}_q[x]$ tal que $\sum_{i=1}^{s} a_i(x)g_i(x) = 1$, es decir

$$1 \in \sum_{i=1}^{s} \langle g_i(x)\rangle = I_1 + \cdots + I_s.$$

Por teoría del algebra, sabemos que el único ideal que contiene el elemento identidad del anillo es el anillo mismo y dado que $1 \in I_1 + \cdots + I_s$, que es a su vez un ideal de R_n, concluimos que $R_n = I_1 + \cdots + I_s$. Para probar que es la suma directa, mostraremos que $I_i \cap \sum_{j\neq i} I_j = 0$, para $1 \leq i \leq s$. Sea $j \neq i$. Entonces tenemos que $h_i(x)|g_j(x),\ h_j(x) \nmid g_j(x)$ y dado que los factores irreducibles de $x^n - 1$ son distintos, entonces $h_i(x) = \text{mcd}\{g_j(x) \mid 1 \leq j \leq s,\ j \neq i\}$. Utilizando el resultado del teorema 1.5.10 tenemos que

$$\sum_{j\neq i} I_j = \langle \text{mcd}\{g_j(x) \mid 1 \leq j \leq s, j \neq i\}\rangle = \langle h_i(x)\rangle.$$

Como $I_i \cap \sum_{j\neq i} I_j = I_i \cap \langle h_i(x)\rangle = \langle \text{mcm}\{g_i(x), h_i(x)\}\rangle$ y dado que $\text{mcm}\{g_i(x), h_i(x)\} = x^n - 1$, por teorema 1.5.10, $I_i \cap \sum_{j\neq i} I_j = \langle x^n - 1\rangle = 0$.

3. Si $0 \neq a(x) \in I_j,\ j = 0, 1, \ldots, s$, entonces $\langle a(x) \rangle \neq 0$, es un ideal de I_j y ya que I_j es un ideal minimal, tenemos que $\langle a(x) \rangle = I_j$. Por lo tanto si $e_j(x)$ es el idempotente de I_j, tenemos que $e_j(x) = a(x)b(x)$, con $b(x) \in R_n$. Si $b(x)$ está en I_j, entonces es el inverso de $a(x)$. En cualquiera de los casos $b(x)e_j(x) \in I_j$ y es el inverso de $a(x)$.

   Si $h_j(x)$ tiene grado m, entonces I_j tiene dimensión m y por lo tanto tiene 2^m elementos. Además como $h_j(x)$ es un polinomio irreducible de grado m, se puede utilizar para construir un $GF(2^m)$ y dado que que solo existe un campo con 2^m elementos, salvo isomorfismos, se concluye que $I_j \cong \mathbb{F}_q^m$, donde $m = \text{gr}(h_j(x)),\ j = 0, 1, \ldots, s$.

4. Sea $i \neq j$. Dado que $e_i(x) \in I_i$ y $e_j(x) \in I_j$, por propiedades de ideales tenemos que $e_i(x)e_j(x) \in I_i \cap I_j$. Pero ya se probó en la parte 2 del teorema que $I_i \cap I_j = 0$, para $i \neq j$. Por lo tanto $e_i(x)e_j(x) = 0$, para $i \neq j$.

5. Por teorema 1.5.10, tenemos que $I_0 + I_1$ tiene generador idempotente $e_0(x)+e_1(x)-e_0(x)e_1(x) = e_0(x)+e_1(x)$ y de esta misma forma podemos ver que $I_0+I_1+\cdots+I_s$ tiene generador idempotente $e_0(x)+e_1(x)+\cdots+e_s(x)$. También utilizando el resultado del teorema 1.5.10, sabemos que el polinomio generador de $I_0 + I_1 + \cdots + I_s$ es el $\text{mcd}\{g_0(x), \cdots, g_k(x)\}$, pero este mcd solamente puede ser 1, ya que los $g_i(x)$ no tienen factores comunes. Ahora, dado que $e_0(x) + e_1(x) + \cdots + e_s(x)$ es un generador de $I_0 + I_1 + \cdots + I_s$, tenemos que $\sum_{j=0}^{s} e_j(x) = 1$. ∎

1.5.12 Nota. De las partes 1 y 2 del teorema 1.5.11, se concluye que los ideales $I_j,\ j = 0, \ldots, s$, son todos los ideales minimales de R_n.

1.5.13 Lema. Sea

$$1 + x + \cdots + x^{p-1} = h_1(x)h_2(x)\cdots h_s(x), \tag{1.3}$$

una factorización del polinomio $1 + x + \cdots + x^{p-1}$ en $\mathbb{F}_2[x]$, con los factores $h_j(x)$, $j = 1, \ldots, s$ irreducibles. Entonces

$$P = I_1 \oplus I_2 \oplus \cdots \oplus I_s.$$

Donde I_j es el ideal de R_n generado por $g_j(x) = \frac{x^n-1}{h_j(x)}$ y con polinomio de control $h_j(x)$.

Demostración. Por el teorema 1.5.11 (3), sabemos que $\dim_{\mathbb{F}_2} I_j = \mathrm{gr}(h_j(x))$. Por lo tanto $\dim_{\mathbb{F}_2}(I_1 \oplus I_2 \oplus \cdots \oplus I_s) = p - 1$. De lo que se concluye que $\dim_{\mathbb{F}_2} P = \dim_{\mathbb{F}_2}(I_1 \oplus I_2 \oplus \cdots \oplus I_s)$. Para completar la demostración probemos que $P \subseteq (I_1 \oplus I_2 \oplus \cdots \oplus I_s)$.

Sea $v \in P$. Entonces por la nota 1.5.12, tenemos que $v = v_0 + v_1 + \cdots + v_s$ con $v_j \in I_j$. Dado que $(x-1)|g_j(x)$ para $j = 1, 2, \ldots, s$, entonces $\mathrm{wt}(v_1 + \cdots v_s)$ es par y como $\mathrm{wt}(v)$ también es par, tenemos que $\mathrm{wt}(v_0)$ es par. Pero como $(x-1) \nmid g_0(x)$, entonces se concluye que $v_0 = 0$. En concecuencia obtenemos que $v \in (I_1 \oplus I_2 \oplus \cdots \oplus I_s)$ y por lo tanto $P \subseteq (I_1 \oplus I_2 \oplus \cdots \oplus I_s)$. Lo que concluye la prueba. ∎

Capítulo 2

Estructura de códigos binarios autoduales con un automorfismo de orden primo impar

El estudio de la estructura de un código binario autodual con un automorismo de orden un primo impar es de fundamental importancia para la construcción de nuevos códigos autoduales. En este capítulo presentamos un resumen de algunos de los resultados más importantes sobre códigos binarios autoduales con un automorismo de orden primo impar que se han establecido en los últimos años. Estos resultados serán utilizados en el siguiente capítulo para la construcción de códigos binarios autoduales con parametros [40,20,8] y [120,60,20].

2.1 Fundamentos

2.1.1 Definición. Dado un vector $v \in \mathbb{F}_q^n$ y $\sigma \in \mathrm{Sym}(n)$, donde $\mathrm{Sym}(n)$ es el grupo simétrico de grado n, definimos el vector $v\sigma$ como:

$$v\sigma := (v_{\sigma^{-1}(1)}, \cdots, v_{\sigma^{-1}(n)}).$$

Dados dos códigos C y C', decimos que son *equivalentes*, lo cual denotamos $C \sim C'$, si y solo si existe $\sigma \in \mathrm{Sym}(n)$, tal que $C\sigma = C'$. Diremos que $\sigma \in \mathrm{Sym}(n)$ es un *automorfismo* de un código $C \leqslant \mathbb{F}_q^n$ si y solo si $C\sigma = C$. El conjunto formado por todos los automorfismos de C, forma un grupo bajo la operación de $\mathrm{Sym}(n)$, denominado *grupo de automorfismos* de C y denotado $\mathrm{Aut}(C)$. Si C y C' son equivalentes, entonces los grupos $\mathrm{Aut}(C)$ y $\mathrm{Aut}(C')$

son *conjugados* en $\mathrm{Sym}(n)$, esto es: $\mathrm{Aut}(C) = \sigma^{-1}\mathrm{Aut}(C)\sigma$, para algún $\sigma \in \mathrm{Sym}(n)$.

2.1.2 Definición. Sea p un primo impar, decimos que σ es un automorfismo de tipo p-$(c; f)$ si en la expresión de σ en ciclos independientes, estos son c ciclos de longitud p y f puntos fijos. En este caso denotamos los ciclos por $\Omega_1, \Omega_2, ..., \Omega_c$ y los puntos fijos por $\Omega_{c+1}, \Omega_{c+2}, ..., \Omega_{c+f}$. El vector obtenido por la eliminación de todas las coordenadas excepto por las coordenadas Ω_i se denota por $v|_{\Omega_i}$, $i = 1, ..., c + f$.

En lo que sigue del documento C representará un código binario $[n, k, d]$ y σ un automorfismo de C de tipo p-$(c; f)$, donde p es un primo impar. Sin perdida de generalidad supondremos siempre que:

$$\sigma = (1, 2, 3, ..., p)(p+1, p+2, ..., 2p)\cdots((c-1)p+1, (c-1)p+2, ..., cp). \quad (2.1)$$

2.1.3 Definición. Definimos el *subcódigo fijo* $F_\sigma(C)$ de C, como:

$$F_\sigma(C) := \{v \in C \mid v\sigma = v\}.$$

Facilmente podemos ver que $v \in F_\sigma(C)$ si y solo si $v \in C$ y $v|_{\Omega_i}$, para $i = 1, ..., c + f$ es constante.

2.1.4 Definición. Definimos el *subcódigo par* $E_\sigma(C)$ de C, como:

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

2.1.5 Lema. Sea $\pi : F_\sigma(C) \longrightarrow \mathbb{F}_2^{c+f}$ la función definida como

$$(\pi(v))_i := v_j, \text{ para algún } j \in \Omega_i,\ i = 1, 2, ...c + f.$$

Si C es un código binario autodual, entonces $\pi(F_\sigma(C))$ es un $[c + f, (c + f)/2]$-código binario autodual. Además si C es doblemente par y $p \equiv 1$ mód 4 o $f = 0$, entonces $\pi(F_\sigma(C))$ también lo es.

Demostración. Demostremos primero que $F_\sigma(C) \cong \pi(F_\sigma(C))$.

Es claro que π es una aplicación lineal, puesto que si $x, y \in F_\sigma(C)$, entonces $(\pi(x + y)i) = (x + y)_j = x_j + y_j = \pi(x)_i + \pi(y)_i$. Para probar la inyectividad, sea $x \in F_\sigma(C)$ tal que $(\pi(x)_i) = 0,\ \forall i$. Entonces $x = 0$, luego $\ker(\pi) = \{0\}$.

Por otra parte sean $v, w \in F_\sigma(C)$. Entonces dado que $F_\sigma(C) \subseteq C$ y C es autodual, tenemos que $v \cdot w = 0$ y $v \cdot w \equiv p\sum_{i=1}^{c} v_i w_i + \sum_{i=c+1}^{c+f} v_i w_i$. Ahora como

$p \neq 2$, se tiene que $p \equiv 1$ mód 2. Por lo tanto $v \cdot w \equiv \sum_{i=1}^{c+f} v_i w_i = \pi(v) \cdot \pi(w)$ mód 2, luego $\pi(v) \cdot \pi(w) \equiv 0$ y como v y w eran cualquier vector en $F_\sigma(C)$, así mismo lo son $\pi(v)$ y $\pi(w)$ en $\pi(F_\sigma(C))$. En consecuencia $\pi(F_\sigma(C))$ es auto-ortogonal.
Para mostrar que π es autodual, demostramos que $\pi(F_\sigma(C))$ y $(\pi(F_\sigma(C)))^\perp$ tienen la misma dimensión. Para ello usaremos el siguiente resultado probado en [2].

$$\dim_{\mathbb{F}_2}\{v \in \mathbb{F}_2^n | v\sigma = v\} = 2\dim_{\mathbb{F}_2} F_\sigma(C) = 2\dim_{\mathbb{F}_2} \pi(F_\sigma(C)) \tag{2.2}$$

Por otro lado, observemos que los vectores

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

son una base para $\{v \in \mathbb{F}_2^n \mid v\sigma = v\}$. De lo que podemos concluir que $\dim\{v \in \mathbb{F}^n \mid v\sigma = v\} = c + f$. Si utilizamos la ecuación (2.2) tenemos que $\dim \pi(F_\sigma(C)) = \frac{1}{2}(c+f)$, y dado que $c+f$ es la longitud de $\pi(F_\sigma(C))$ se concluye que su complemento debe tener también dimensión $\frac{1}{2}(c+f)$. ∎

2.1.6 Lema. Sea $C \leq \mathbb{F}_2^n$ un código con un automorfismo de tipo $p-(c;f)$. Entonces se cumple que $C = F_\sigma(C) \oplus E_\sigma(C)$, donde $\oplus$ es la suma directa de subespacios lineales. Además si C es autodual, entonces $\dim_{\mathbb{F}_2} E_\sigma(C) = \frac{(p-1)c}{2}$.

Demostración. Sean v y w, tal que $v \in C$ y $w := v + \sum_{i=0}^{p-1} v\sigma^i$. Entonces es claro que también $w \in C$ y que $v = w + \sum_{i=0}^{p-1} v\sigma^i$. Además podemos ver que $\mathrm{wt}(v\sigma^i|_{\Omega_i}) = \mathrm{wt}(v\sigma^i_j) = \mathrm{wt}(v|_{\Omega_j})$, $j = 1, ..., c+f$. Concluyendo así que $\mathrm{wt}(w|_{\Omega_j}) = \mathrm{wt}((v + \sum_{i=0}^{p-1} v\sigma^i)|_{\Omega_j})\ \mathrm{wt}(v|_{\Omega_j}) = (p+1)\mathrm{wt}(v|_{\Omega_j})$ y como $p \neq 2$, entonces $p+1$ es par, por lo tanto $\mathrm{wt}(w|_{\Omega_j}) \equiv 0$ mód 2 y en consecuencia $w \in E_\sigma(C)$.
Por otro lado tenemos que:

$$\left(\sum_{i=0}^{p-1} v\sigma^i\right)\sigma = v\sigma^1 + v\sigma^2 + ... + v\sigma^{p-1} + v\sigma^p = \sum_{i=0}^{p-1} v\sigma^i,$$

es decir $\sum_{i=0}^{p-1} v\sigma^i \in F_\sigma(C)$. En conclusión $v \in F_\sigma(C) + E_\sigma(C)$.
Verifiquemos ahora $F_\sigma(C) \cap E_\sigma(C) = 0$. Supongamos que $v \in F_\sigma(C) \cap E_\sigma(C)$. Entonces $v \in F_\sigma(C)$ y $v \in E_\sigma(C)$, por lo tanto las coordenadas de $v|_{\sigma_i} = 0$ son todas iguales para $i = 1, \ldots, c + f$ y además el peso de $v|_{\sigma_i} = 0$ es par. Ahora, como C es un código binario y p es impar, concluimos que $v|_{\sigma_i} = 0$ para $i = 1, \ldots, c + f$. Luego $v = 0$ y dado que v es cualquier vector en C, se concluye que $C = F_\sigma(C) \oplus E_\sigma(C)$. ∎

El lema 2.1.6 muestra que para el código C, existe una matriz generadora de la forma

$$\mathrm{gen}(C) = \left(\begin{array}{c|c} X & Y \\ \hline Z & O \end{array}\right) \begin{array}{l} \} \ \mathrm{gen}(F_\sigma(C)) \\ \} \ \mathrm{gen}(E_\sigma(C)) \end{array},$$

donde la parte izquierda de la matriz corresponde a todas las coordenadas movidas por σ y la derecha a los puntos fijos.

2.1.7 Lema. Sea $P := \{v(x) \in R_p \mid \mathrm{wt}(v(x)) \equiv 0 \text{ mód } 2\}$. Entonces

1. P es un código cíclico con $|P| = 2^{p-1}$ y polinomio generador $x - 1$.
2. P es un subanillo de $\mathbb{F}_2[x]/\langle x^p - 1\rangle$ con elemento identidad $e(x)$, donde $e(x) = x + x^2 + \cdots + x^{p-1}$.
3. Si $p \in \mathbb{P}$ y $1 + x + \cdots + x^{p-1}$ es irreducible en $\mathbb{F}_2[x]$, entonces P es un campo. Además

   $$\beta(x)p(x) \equiv xp(x) \text{ mód } \langle x^p - 1\rangle,$$

   para $p(x) \in P$, donde $\beta(x) := 1 + x^2 + x^3 + \cdots + x^{p-1}$; es decir la multiplicación por $\beta(x)$ corresponde a una traslación cíclica en P.

Demostración.

1. Sea $p(x) \in P$. Entonces $p(1) = 0$, luego $(x-1)|p(x)$. Por lo tanto existe $g(x) \in \mathbb{F}_2[x]$, tal que $p(x) = (x-1)g(x)$. Entonces $p(x) \in \langle x - 1\rangle$ y se concluye que $P = \langle x - 1\rangle$. Por otra parte, dado que P es el conjunto de todos los polinomios de peso par de R_p, entonces

   $$|P| = \frac{|R_p|}{2} = \frac{|\mathbb{F}_2|^p}{2} = \frac{2^p}{2} = 2^{p-1}.$$

2. Es claro que P es cerrado bajo la suma usual de polinomios y el producto de polinomios mód x^p-1. Para probar que $e(x) := x+x^2+\ldots+x^{p-1}$ es el elemento identidad de P, sea $0 \neq f(x) \in P$. Entonces $f(x) = g(x)(x-1)$, para algún $g(x)$. Luego

   $$f(x)(1+x+\cdots+x^{p-1}) = g(x)(x-1)(1+x+\cdots+x^{p-1}) = g(x)(x^p-1).$$

   Por lo tanto $f(x)(1+x+\cdots+x^{p-1}) \equiv 0$ mód $\langle x^p-1\rangle$ y dado que $p(x) \neq 0$ se concluye que $(1+x+x^2+\cdots+x^{p-1}) \equiv 0$ mód $\langle x^p-1\rangle$, luego $x+x^2\cdots+x^{p-1} \equiv 1$ mód $\langle x^p-1\rangle$. Es decir

   $$p(x)(x+x^2+\cdots+x^{p-1}) \equiv p(x) \text{ mód } \langle x^p-1\rangle.$$

3. Ya se probó que P es un anillo con elemento identidad $e(x)$ y dado que la multiplicación en $\mathbb{F}_2[x]$ es conmutativa, también lo es en P. Ahora supongamos que $p_1(x), p_2(x) \in P$ y que $p_1(x)p_2(x) \equiv 0$ mód $\langle x^p-1\rangle$. Entonces se cumple que $(x-1) \mid p_1(x)$ o $(x-1) \mid p_2(x)$. Además el polinomio $1+x+\cdots+x^{p-1}$ divide a $p_1(x)p_2(x)$, luego $1+x+\cdots+x^{p-1}$ divide a $p_1(x)$ o divide a $p_2(x)$, esto porque el polinomio $1+x+\cdots+x^{p-1}$ es irreducible en $\mathbb{F}_2[x]$. Por lo tanto se tiene que $p_1(x) \equiv 0$ mód $\langle x^p-1\rangle$ o $p_2(x) \equiv 0$ mód $\langle x^p-1\rangle$. En conclusión P es un anillo finito, conmutativo, invertible y sin divisores de cero. Por lo tanto P es un campo.

   Además, dado que $xe(x) - \beta(x) = x^p - 1$. Entonces $xe(x) \equiv \beta(x)$ mod $\langle x^p-1\rangle$. Ahora, si $p(x) \in P$, entonces $xe(x)p(x) \equiv \beta(x)p(x)$ mód $\langle x^p-1\rangle$. Por lo tanto $xp(x) \equiv \beta(x)p(x)$ mód $\langle x^p-1\rangle$. ∎

2.1.8 Lema. Sea $p \in P$, tal que el polinomio $1+x+\cdots+x^{p-1}$ es irreducible en $\mathbb{F}_2[x]$ y $\beta(x) = 1+x^2+x^3+\cdots+x^{p-1}$. Entonces:

1. $x^t e(x) \equiv \beta(x)^t$ mód(x^p-1), para todo $0 \leq t \leq p-1$ y $\text{ord}(xe(x)) = \text{ord}(\beta(x)) = p$.
2. Si $q(x) \in P$ con $\text{ord}(q(x)) = m$ y $(p,m) = 1$, entonces $\text{ord}(xq(x)) = pm$.
3. $H = \langle\beta(x)\rangle$ es el único subgrupo de orden p en $P\backslash\{0\}$.
4. $\beta(x), \beta(x)^2, \ldots, \beta(x)^{p-1}$ son todos los elementos de orden p en $P\backslash\{0\}$.

Demostración. Primero recordemos que, si G es un grupo cíclico y p divide el ord(G). Entonces:

a) Existe un único subgrupo $H = \langle a\rangle = \{1, a, \ldots, a^{p-1}\}$ de orden p.

b) $a, a^2, \ldots, a^{p-1}$ son los únicos elementos de orden p en G y $H = \langle a^i \rangle$, $i = 1, 2, \ldots, p-1$.

Demostremos entonces el lema.

1. Dado que $xe(x) - \beta(x) = x^p - 1$. Entonces $xe(x) \equiv \beta(x)$ mód$(x^p - 1)$, y por lo tanto $x^t e(x) \equiv \beta(x)^t$mód$(x^p - 1)$.

   Además puesto que $(xe(x))^p = e(x)$ y $p \in \mathbb{P}$, entonces $\text{ord}(xe(x)) = \text{ord}(\beta(x)) = p$.

2. Sea $q(x) \in P$ con $\text{ord}(q(x)) = m$, entonces $q(x)^m = e(x)$ y además

$$(xq(x))^{pm} = x^{pm} q^{pm} = x^{p^m} q(x)^{m^p} = e(x).$$

   Por lo tanto $\text{ord}(xq(x)) \mid pm$, y dado que p y m son primos relativos, entonces $\text{ord}(xq(x)) = pm$.

3. Puesto que $|P\backslash\{0\}| = 2^{p-1} - 1$, $\text{ord}(\beta(x)) = p$ y $p \mid (2^{p-1} - 1)$, entonces por la observación del inciso a), tenemos que $H = \langle \beta(x) \rangle$ es el único subgrupo de orden p en $P\backslash\{0\}$.

4. Es inmediato por la observación del inciso b). ∎

2.1.9 Lema. Sea C un $[n, n/2, d]$-código binario autodual con automorfismo de tipo p -$(c; f)$, donde p es un primo impar. Si definimos

$$g(k) := \lceil d/2^o \rceil + \lceil d/2^1 \rceil + \cdots + \lceil d/2^{k-1} \rceil,$$

entonces

1. $pc \geq g((p-1)c/2)$ y si $d \leq 2^{(p-1)c/2-2} - 2$ la igualdad no se produce.

2. Si $f > c$, entonces se cumple que $f \geq g((f-c)/2)$ y si $d \leq 2^{(f-c)/2-2} - 2$ la igualdad no ocurre.

Demostración.

1. Sea $E_\sigma(C)^*$ el código que se obtiene de $E_\sigma(C)$ eliminando las últimas f coordenadas y sea además $d = \text{d}(E_\sigma(C))$. Entonces es fácil verificar que $\text{d}(E_\sigma(C)^*) \geq d$ y que $E_\sigma(C)^*$ y $E_\sigma(C)$ tienen igual dimensión, donde

$$\dim(E_\sigma(C)) = \tfrac{1}{2}(p-1)c.$$

Aplicando la cota de Griesmer definida en el lema 1.1.7, al código $E_\sigma(C)^*$, que tiene longitud $m = pc$, se obtiene que: $pc \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil$ y dado que $k = \frac{1}{2}(p-1)c$, tenemos que

$$pc \geq \lceil d/2^o \rceil + \lceil d/2^1 \rceil + ... + \lceil d/2^{(\frac{1}{2}(p-1)c)-1} \rceil.$$

Por lo tanto $pc \geq g((p-1)c/2)$.

Ahora, utilizando la cota de Logachev definida en el lema 1.1.7. Tenemos que si $d \leq 2^{(p-1)c/2-2} - 2$, entonces la desigualdad es estricta.

2. Consideremos el código π_1, que consiste en todos los vectores del código $\pi(F_\sigma(C))$ con ceros en sus primeras c coordenadas. Entonces tenemos que:

$$\dim_{\mathbb{F}_2} \pi_1 \geq \dim_{\mathbb{F}_2} \pi(F_\sigma(C)) - c = \tfrac{c+f}{2} - c = \tfrac{f-c}{2}, \text{ con } f > c.$$

Sea $d = \mathrm{d}(\pi_1)$ y denotemos por π_1^* el código obtenido de π_1 eliminando las primeras c coordenadas. Claramente $\mathrm{d}(\pi_1^*) \geq d$, luego los parametros del código π_1^* son $[f, k, d']$, donde $k \geq (f-c)/2$ y $d' \geq d$. Usando la cota de Griesmer, tenemos

$$f \geq \sum_{i=0}^{k-1} \lceil d'/2^i \rceil \geq \sum_{i=0}^{\frac{f-c}{2}-1} \lceil d/2^i \rceil = g((f-c)/2).$$

Finalmente si $d \leq 2^{\frac{f-c}{2}-2} - 2$, entonces aplicando la cota de Logachev, tenemos que la desigualdad es estricta. ∎

2.2 Resultados generales

2.2.1 Definición. Sea nuevamente $E_\sigma(C)^*$ el código $E_\sigma(C)$ con las últimas f coordenadas eliminadas. Entonces cada vector v de $E_\sigma(C)^*$ puede ser particionado entre c vectores $v|_{\Omega_i}$ de longitud p, con $i = 1, 2, ..., c$. Definamos entonces la función

$$\varphi : E_\sigma(C)^* \longrightarrow P^c,$$

como $(\varphi(v))_i := v_0 + v_1 x + \cdots + v_{p-1} x^{p-1} \in P$, para $i = 1, 2, \ldots, c$ y $v \in \varphi(E_\sigma(C)^*)$ con $v|_{\Omega_i} = (v_0, v_1, \ldots, v_{p-1})$.

2.2.2 Lema. $\varphi(E_\sigma(C)^*)$ es un submódulo del módulo P^c.

Demostración. Obviamente $\varphi(E_\sigma(C)^*)$ es cerrado bajo la suma de polinomios y además si $\beta(x) := 1 + x^2 + x^3 + \cdots + x^{p-1}$, entonces $\beta(x) \in P$.
Por otra parte, si $g(x) \in P$, entonces

$$g(x) = (1 + x)q(x)$$

y dado que

$$\beta(x) \equiv x \text{ mód } (1 + x + x^2 + x^3 + \cdots + x^{p-1}),$$

puesto que $\beta(x) - x = 1 + x + x^2 + x^3 + \cdots + x^{p-1}$. Entonces

$$\beta(x)g(x) \equiv xg(x) \text{ mód } (1 + x + x^2 + x^3 + \cdots + x^{p-1}).$$

Por lo tanto, $\beta(x)g(x) \equiv xg(x) \text{ mod } (x+1)$, en el anillo $\mathbb{F}_2[x]/\langle x^p + 1\rangle$ y esto significa que multiplicar por $\beta(x)$ en el anillo P, es equivalente a una traslación cíclica en el anillo.
Por otra parte, para cada $v \in E_\sigma(C)^*$ tenemos que:

$$\beta(x)v(x) = \varphi(v\sigma) \in \varphi(E_\sigma(C)^*), \tag{2.3}$$

ya que $\sigma \in \text{Aut}(C)$.
Para $0 \leq k \leq p-1$ y $0 \leq s \leq p-1$, se satisface en P, la ecuación

$$\beta(x)^k + \beta(x)^s = x^k + x^s. \tag{2.4}$$

De esto se sigue que cada elemento del anillo P, se escriba como la suma de algunos de los elementos $e(x)$, $\beta(x)$, $\beta(x)^2, ..., \beta(x)^{p-1}$. Entonces,

$$\left(\sum_s \beta(x)^s\right)\varphi(v) = \sum_s \beta(x)^s\varphi(v) \in \varphi(E_\sigma(C)^*).$$

Por lo tanto, de acuerdo con (2.3), cada término de $\sum_s \beta(x)^s\varphi(v)$ está en $\varphi(E_\sigma(C)^*)$, lo cual concluye la prueba. ∎

2.2.3 Lema. Sea $1+x+x^2+\cdots+x^{p-1}$ irreducible sobre $\mathbb{F}_2[x]$ y C un código autodual. Entonces se tiene:

1. $\varphi(E_\sigma(C)^*)$ es un $[c, c/2]$-código sobre el campo P.
2. c es par.

Demostración. Probemos que $\dim_P \varphi(E_\sigma(C)^*) = \frac{c}{2}$. Sabemos que P es un campo de 2^{p-1} elementos y que $\varphi(E_\sigma(C)^*)$ es un espacio vectorial sobre P, que contiene $2^{\frac{p-1}{2}c}$ elementos. Luego si $\dim_P \varphi(E_\sigma(C)^*) = k$, entonces

$$2^{\frac{p-1}{2}c} = |\varphi(E_\sigma(C)^*)| = |P|^k = (2^{p-1})^k.$$

De lo cual se concluye que $k = \frac{c}{2}$. ∎

2.2.4 Definición. Sea $1 + x + \cdots + x^{p-1} = h_1(x)h_2(x)\cdots h_s(x)$ la factorización del polinomio $1 + x + x^2 + \cdots + x^{p-1}$ en factores irreducibles h_j, sobre $\mathbb{F}_2[x]$. Entonces el conjunto

$$M_j = \{u \in \varphi(E_\sigma(C)^*) \mid u_i \in I_j,\ i = 1, 2, ..., c\},$$

para $j = 1, 2, \ldots, s$ es llamado la j-ésima componente del módulo $\varphi(E_\sigma(C)^*)$, donde $I_j = \langle \frac{x^n-1}{h_j(x)} \rangle$ son los ideales de R_n definidos en el teorema 1.5.11.

2.2.5 Lema. Sea $1+x+\cdots+x^{p-1} = h_1(x)h_2(x)\cdots h_s(x)$ la factorización del polinomio $1 + x + x^2 + \cdots + x^{p-1}$ en polinomios irreducibles sobre $\mathbb{F}_2$ como en el lema 1.3. Entonces

1. $\varphi(E_\sigma(C)^*) = M_1 \oplus M_2 \oplus \cdots \oplus M_s$ donde $\oplus$ es la suma directa interna de submódulos.
2. Si el código C es autodual, entonces $\sum_{j=1}^{s} \dim_{I_j} M_j = cs/2$.

Demostración.

1. Del teorema 1.5.11 (5) sabemos que $1 = e_1(x) + \cdots + e_s(x)$. Por lo tanto $e(x) = e_1(x) + \cdots + e_s(x)$, donde $e(x)$ es el elemento identidad del anillo P. Entonces por teorema 1.5.11 (4), tenemos que $e_1(x) + \cdots + e_s(x)$ es un idempotente de P.

   Probemos ahora que $M = e_1M + \cdots + e_sM$, donde $M = \varphi(E_\sigma(C)^*)$. Sea $u = (v_1, \ldots, v_s) \in M$. Entonces

   $$u = e(x)u = \sum_{j=1}^{s} e_j u \in e_1M + \cdots + e_sM.$$

   Luego $M \subseteq e_1M + \cdots + e_sM$. Reciprocamente, sea $v = e_1m_1 + \cdots + e_sm_s$, con $m_j \in M$. Dado que $e_j \in P$ y M es un P-módulo, entonces $e_jm_j \in M$ y como M es cerrado bajo la suma, se cumple que $v \in M$. Para culminar

esta parte de la demostración, probemos que $e_j(x)M = M_J$. En efecto sea

$$ue_j(x) = (u_1(x)e_j(x), \ldots, u_c(x)e_j(x)) \in Me_j(x),$$

con $h_j(x) \in P$. Puesto que $I_j = \langle e_j(x) \rangle$, entonces $u_j(x)e_j(x) \in I_j$.
Por otra parte, si $u = (u_1, \ldots, u_s) \in M_j$, entonces $u_j(x) \in I_j$. Por lo tanto $u_j(x)e_j(x) = u_j(x)$. Es decir, $u \in Me_j(x)$ y podemos concluir que $M = M_1 + \cdots + M_s$. Para demostrar que M es la suma directa, probemos que $M_j \cap \sum_{r \neq j} M_r = 0$. Sea $u(x) = (u_1(x), \ldots, u_s(x)) \in M$, con $u \in M_j \cap \sum_{r \neq j} M_r$. Entonces $u(x) \in M_j$. Por lo cual tenemos que $u_i(x) \in I_j$ y $u(x) \in \sum_{r \neq j} M_r$. Es decir $u_j(x) \in \sum_{r \neq j} I_r$. Como $I_j \cap \sum_{r \neq j} I_r = 0$, entonces $u_j(x) = 0$. Por lo tanto $u = 0$ y finalmente se concluye que $\varphi(E_\sigma(C)^*) = M_1 \oplus \cdots \oplus M_s$.

2. Dado que C es autodual, sabemos que

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

Por otra parte, puesto que I_j es un campo con $2^{(p-1)\frac{c}{2}}$ elementos y también un $\mathbb{F}_2$-espacio vectorial, entonces

$$(p-1)\frac{c}{2} = \sum_{j=1}^{s} \dim_{\mathbb{F}_2} M_j = \sum_{j=1}^{s} (\dim_{I_j} M_j)(\dim_{\mathbb{F}_2} I_j) = \frac{p-1}{s} \sum_{j=1}^{s} \dim_{I_j} M_j.$$

Concluyendo así que $\sum_{j=1}^{s} \dim_{I_j} M_j = \frac{cs}{2}$. ∎

2.2.6 Definición. La matriz A de la forma:

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_{p-1} \\ a_{p-1} & a_0 & \ldots & a_{p-2} \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}, \tag{2.5}$$

es llamada una *matriz circulante*.

El algebra de las matrices circulantes $(p \times p)$ sobre el campo $\mathbb{F}_2$, es isomorfa al algebra de $\mathbb{F}_2[x]/\langle x^p + 1 \rangle$, mediante la función:

$$\phi(a(x)) := A, \tag{2.6}$$

donde $a(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1}$. (Ver [14], p. 484).
La matriz transpuesta A^t corresponde al polinomio

$$a(x^{-1}) = a_0 + a_{p-1}x + a_{p-2}x^2 + \cdots + a_1x^{p-1}.$$

Los exponentes de x son tomados módulo p. Obviamente en la matriz A, cada dos filas son ortogonales si y solo si $AA^t = 0$.

El siguiente lema no requiere prueba.

2.2.7 Lema. Sean $S = [S_1|S_2|\cdots|S_c]$ y $T = [T_1|T_2|\cdots|T_c]$ matrices celdas, con $S_j, T_j \in \mathbb{F}_2^{p\times p}$, para $j = 1, \ldots, c$. Entonces se tiene que cada fila de S es ortogonal a cada fila de T, si y solo si $S_1T_1^t + \cdots + S_cT_c^t = 0$.

2.2.8 Teorema. Sean C un código binario y $\sigma \in \mathrm{Aut}(C)$ de la forma (2.1). Entonces C es un código auto-ortogonal si y solo si

1. $\pi(F_\sigma(C))$ es auto-ortogonal,

2. Para cada dos vectores

$$(a_1(x), a_2(x), \ldots, a_r(x)) \text{ y } (b_1(x), b_2(x), \ldots, b_r(x)) \text{ de } \varphi(E_\sigma(C)^*),$$

se satisface que $a_1(x)b_1(x^{-1}) + a_2(x)b_2(x^{-1}) + \cdots + a_r(x)b_r(x^{-1}) = 0$.

Demostración. Sea el código C auto-ortogonal. Entonces la condición 1 se sigue del lema 2.1.5.
De acuerdo con (2.6), los elementos de

$$(a_1(x), a_2(x), \ldots, a_r(x)) \text{ y } (b_1(x), b_2(x), \ldots, b_r(x)) \text{ de } \varphi(E_\sigma(C)^*),$$

corresponden a las matrices $S = [S_1|S_2|\cdots|S_c]$ y $T = [T_1|T_2|\cdots|T_c]$ y como las primeras filas de S y T son vectores de $E_\sigma(C)^*$ y además $\sigma \in \mathrm{Aut}(C)$, todas las filas de S y T son elementos de $E_\sigma(C)^*$. En consecuencia cada fila de S es ortogonal a cada fila de T. Entonces la condición 2 se obtiene del lema 2.2.7.
Reciprocamente, supongamos que tenemos las condiciones 1 y 2. De acuerdo al lema 2.1.6, si $u \in F_\sigma(C)$ y $v \in E_\sigma(C)$, entonces $u \cdot v = 0$, dado que el vector $u|_{\Omega_i}$ consiste solo en ceros o unos y $\mathrm{wt}(w|_{\Omega_i}) \equiv 0$ mód 2, $i = 1, 2, ..., c + f$. Luego, de acuerdo con la condición 1, los vectores de $F_\sigma(C)$ son mutuamente ortogonales, es decir $F_\sigma(C)$ es auto-ortogonal.
Por otra parte sea $u, v \in E_\sigma(C)^*$ tal que, $\varphi(u) = (a(x), b(x), ..., r(x))$, $\varphi(v) = (g(x), h(x), ..., l(x))$. De acuerdo con la condición 2, tenemos que

$a_1(x)b_1(x^{-1}) + a_2(x)b_2(x^{-1}) + \cdots + a_r(x)b_r(x^{-1}) = 0$ y por el lema 2.2.7, cada fila de S es ortogonal a cada fila de T donde las matrices celdas $S_1, \ldots, S_c, T_1, \ldots, T_c$ son obtenidas de $a_1(x), \ldots, a_r(x), b_1(x), \ldots, b_r(x)$ respectivamente, de acuerdo con 2.6. Ahora, dado que u y v son respectivamente, las primeras filas de S y T, tenemos que $u \cdot v = 0$, y en consecuencia, $E_\sigma(C)^*$ es un código auto-ortogonal. Esto significa que $E_\sigma(C)$ también lo es y como ya probamos que $F_\sigma(C)$ es auto-ortogonal, podemos afirmar, por 2.1.6, que el código C es auto-ortogonal. ∎

2.2.9 Teorema. Sea el polinomio $1 + x + x^2 + \cdots + x^{p-1}$, irreducible en $\mathbb{F}_2[x]$. Entonces el código C es autodual si y solo si, se satisfacen las siguientes condiciones.

1. El código $\pi\left(F_\sigma(C)\right)$ es autodual.
2. El código $\varphi(E_\sigma(C)^*)$ es autodual, sobre el campo P, con respecto al producto escalar $u \cdot v = \sum_{i=1}^{c} u_i v_i^{2^{(p-1)/2}}$ donde $u = (u_1, ..., u_c)$, $v = (v_1, ..., v_c)$ son elementos de P^c.

Demostración. Si el polinomio $1 + x + x^2 + \cdots + x^{p-1}$, es irreducible en $\mathbb{F}_2[x]$, entonces P es un campo de 2^{p-1} elementos y además 2 es un elemento primitivo módulo p, de lo que se obtiene la congruencia $\rho = 2^{(p-1)/2} \equiv -1$ mód p y puesto que la característica del campo es 2, se tiene que $g(x^{-1}) = g(x^\rho) = g(x)^\rho$. Ahora, de acuerdo a la condición 2 del teorema 2.2.8, tenemos que $a(x)g(x)^\rho + b(x)h(x)^\rho + \cdots + r(x)l(x)^\rho = 0$ y por el mismo teorema se concluye que el código C es auto-ortogonal si y solo si $\pi\left(F_\sigma(C)\right)$ y $\varphi(E_\sigma(C)^*)$ son auto-ortogonales. Por último si la $\dim_{\mathbb{F}_2} C = n/2$. Obtenemos las condiciones 1 y 2, utilizando los lemas 2.1.6 y 2.2.3.
Reciprocamente, si las condiciones 1 y 2 se cumplen, entonces $\dim_{\mathbb{F}_2} \pi\left(F_\sigma(C)\right) = (c + f)/2$ y $\dim_P \varphi(E_\sigma(C)^*) = c/2$, de lo que tenemos que $\dim_P \varphi(E_\sigma(C)^*) = (c/2)\dim_{\mathbb{F}_2} P = (p-1)c/2$, de acuerdo con el lema 2.1.6. Luego $\dim_{\mathbb{F}_2} E_\sigma(C) = \dim_P \varphi(E_\sigma(C)^*) = (p-1)c/2$, por lo tanto tenemos que $\dim_{\mathbb{F}_2} C = (c + f)/2 + c(p-1)/2 = (cp + f)/2 = n/2$, lo que demuestra el teorema. ∎

El siguiente teorema demostrado por W. Yorgov en [20] es de trascendental importancia al momento de reducir el número de posibles matrices generadoras de un código con ciertos parámetros, puesto que establece condiciones necesarias y suficientes para la equivalencia de dos códigos de la misma longitud con un mismo automorfismo de orden primo impar.

2.2.10 Teorema. ([20]) **(Yorgov)** Sea σ un automorfismo de los códigos autoduales C y C'. Los códigos C y C' son equivalentes si y solo si el código C' puede obtenerse del código C por la aplicación de alguna de las siguientes transformaciones:

1. La sustitución $x \to x^t$ en $\varphi(E_\sigma(C)^*)$, donde t es un entero, $1 \leq t \leq p-1$,
2. La multiplicación de la j-esima coordenada de $\varphi(E_\sigma(C)^*)$ por x^{t_j} donde t_j es un entero, $1 \leq t \leq p-1$ y $j = 1, 2, \ldots, c$,
3. La permutación de los primeros c ciclos de C,
4. la permutación de las últimas f coordenadas de C.

2.2.11 Lema. Sea $q(x) = 1 + x + \cdots + x^{p-1}$ irreducible en $\mathbb{F}_2[x]$ y $P \subseteq \mathbb{F}_2[x]/\langle x^p - 1\rangle$. Si definimos la función

$$\varphi : \mathbb{F}_2[x]/\langle q(x)\rangle \longrightarrow P,$$

tal que

$$\varphi(u(x) + \langle q(x)\rangle) := \begin{cases} u(x) + \langle x^p - 1\rangle, & \text{wt}(u(x)) \equiv 0 \bmod 2 \\ (u(x) + q(x)) + \langle x^p - 1\rangle, & \text{wt}(u(x)) \not\equiv 0 \bmod 2 \end{cases}$$

con $\text{gr}(u(x)) < p-1$, entonces φ es un Isomorfismo de cuerpos.

Demostración. Demostremos que φ está bién definida. Sean $u(x), v(x) \in \mathbb{F}_2[x]/\langle q(x)\rangle$, tal que

$$u(x) = u_0 + u_1 x + \cdots + u_{p-2}x^{p-2} \text{ y } v(x) = v_0 + v_1 x + \cdots + v_{p-2}x^{p-2}.$$

Si $u(x) + \langle q(x)\rangle = v(x) + \langle q(x)\rangle$, entonces $u(x) - v(x) = s(x)q(x)$, para algún $s(x) \in \mathbb{F}_2[x]/\langle q(x)\rangle$ y se distinguen tres casos posibles.

1. Sean $\text{wt}(u(x))$ y $\text{wt}(v(x))$ pares. Entonces el $\text{wt}(s(x))$ es par y tenemos que

$$\begin{aligned} \varphi(u(x) + \langle q(x)\rangle) - \varphi(v(x) + \langle q(x)\rangle) &= (u(x) + \langle x^p - 1\rangle) - (v(x) + \langle x^p - 1\rangle) \\ &= (u(x) - v(x)) + \langle x^p - 1\rangle \\ &= s(x)q(x) + \langle x^p - 1\rangle \\ &= g(x)(x^p - 1) + \langle x^p - 1\rangle, \end{aligned}$$

   para algún $g(x)$. Por lo tanto $\varphi(u(x) + \langle q(x)\rangle) = \varphi(v(x) + \langle q(x)\rangle)$.

2. Sean $\mathrm{wt}(u(x))$ y $\mathrm{wt}(v(x))$ impares. Entonces el $\mathrm{wt}(s(x))$ es par y tenemos que

$$\begin{aligned}\varphi(u(x)+\langle q(x)\rangle)-\varphi(v(x)+\langle q(x)\rangle) &= ((u(x)+q(x))+\langle x^p-1\rangle)- \\ &\quad ((v(x)+q(x))+\langle x^p-1\rangle) \\ &= (u(x)-v(x))+\langle x^p-1\rangle \\ &= s(x)q(x)+\langle x^p-1\rangle \\ &= g(x)(x^p-1)+\langle x^p-1\rangle,\end{aligned}$$

   para algún $g(x)$. Por lo tanto $\varphi(u(x)+\langle q(x)\rangle)=\varphi(v(x)+\langle q(x)\rangle)$.

3. Sea $\mathrm{wt}(u(x))$ par y $\mathrm{wt}(v(x))$ impar. Entonces el $\mathrm{wt}(s(x))$ es impar y tenemos que

$$\begin{aligned}\varphi(u(x)+\langle q(x)\rangle)-\varphi(v(x)+\langle q(x)\rangle) &= (u(x)+\langle x^p-1\rangle)- \\ &\quad ((v(x)+q(x))+\langle x^p-1\rangle) \\ &= ((u(x)-v(x))-q(x))+\langle x^p-1\rangle \\ &= (s(x)q(x)-q(x))+\langle x^p-1\rangle \\ &= q(x)(s(x)-1)+\langle x^p-1\rangle \\ &= g(x)(x^p-1)+\langle x^p-1\rangle,\end{aligned}$$

   para algún $g(x)$. Por lo tanto $\varphi(u(x)+\langle q(x)\rangle)=\varphi(v(x)+\langle q(x)\rangle)$. Luego la función φ está bién definida.

Demostremos que φ es aplicación lineal.

1. Sean $\mathrm{wt}(u(x))$ y $\mathrm{wt}(v(x))$ pares. Entonces $\mathrm{wt}(u(x)+v(x))$ es par. Por lo tanto

$$\begin{aligned}\varphi((u(x)+v(x))+\langle q(x)\rangle) &= ((u(x)+v(x))+\langle x^p-1\rangle \\ &= (u(x)+\langle x^p-1\rangle)+(v(x)+\langle x^p-1\rangle) \\ &= \varphi(u(x))+\varphi(v(x)).\end{aligned}$$

2. Sean $\mathrm{wt}(u(x))$ y $\mathrm{wt}(v(x))$ impares. Entonces $\mathrm{wt}(u(x)+v(x))$ es par. En consecuencia

$$\begin{aligned}\varphi((u(x)+v(x))+\langle q(x)\rangle) &= (u(x)+v(x))+\langle x^p-1\rangle \\ &= ((u(x)+v(x))+(q(x)+q(x)))+\langle x^p-1\rangle \\ &= ((u(x)+q(x))+\langle x^p-1\rangle)+ \\ &\quad ((v(x)+q(x))+\langle x^p-1\rangle) \\ &= \varphi(u(x))+\varphi(v(x)).\end{aligned}$$

3. Sea $\mathrm{wt}(u(x))$ par y $\mathrm{wt}(v(x))$ impar. Entonces $\mathrm{wt}(u(x)+v(x))$ es impar y tenemos

$$\begin{aligned}\varphi((u(x)+v(x))+\langle q(x)\rangle) &= ((u(x)+v(x))+q(x))+\langle x^p-1\rangle \\ &= (u(x)+\langle x^p-1\rangle)+((v(x)+q(x))+\langle x^p-1\rangle) \\ &= \varphi(u(x))+\varphi(v(x)).\end{aligned}$$

Demostremos la inyectividad de φ.
Sea $\varphi(u(x)+\langle q(x)\rangle) = \varphi(v(x)+\langle q(x)\rangle)$. Entonces se tienen los siguientes casos a saber.

1. Si $\mathrm{wt}(u(x))$ y $\mathrm{wt}(v(x))$ son pares, entonces

$$u(x)+\langle x^p-1\rangle = v(x)+\langle x^p-1\rangle$$

y por lo tanto $u(x)-v(x)\in\langle x^p-1\rangle$; es decir

$$u(x)-v(x) = r(x)(x^p-1),$$

para algún $r(x)$. Luego $u(x)-v(x) = r(x)(x-1)q(x) \in \langle q(x)\rangle$. En conclusión $u(x)+\langle q(x)\rangle = v(x)+\langle q(x)\rangle$.

2. Si $\mathrm{wt}(u(x))$ y $\mathrm{wt}(v(x))$ son impares, entonces

$$(u(x)+q(x))+\langle x^p-1\rangle = (v(x)+q(x))+\langle x^p-1\rangle$$

y por lo tanto $u(x)-v(x)\in\langle x^p-1\rangle$; es decir

$$u(x)-v(x) = r(x)(x^p-1),$$

para algún $r(x)$. Luego $u(x)-v(x) = r(x)(x-1)q(x) \in \langle q(x)\rangle$. En conclusión $u(x)+\langle q(x)\rangle = v(x)+\langle q(x)\rangle$.

3. Si $\mathrm{wt}(u(x))$ es par y $\mathrm{wt}(v(x))$ es impar, entonces

$$u(x)+\langle x^p-1\rangle = (v(x)+q(x))+\langle x^p-1\rangle,$$

de donde $u(x)-v(x)-q(x)\in\langle x^p-1\rangle$; es decir

$$u(x)-v(x)-q(x) = r(x)(x^p-1),$$

para algún $r(x)$. Luego

$$\begin{aligned}u(x)-v(x) &= r(x)(x-1)q(x)+q(x) \\ &= q(x)(r(x)(x-1)+1)\in\langle q(x)\rangle.\end{aligned}$$

Por lo tanto $u(x)+\langle q(x)\rangle = v(x)+\langle q(x)\rangle$.

Demostremos la sobreyectividad de φ.
Sea $b(x) = b_0+b_1x+\cdots+b_{p-2}x^{p-2}+b_{p-1}x^{p-1} \in P$, con $\mathrm{wt}(b(x))$ par. Entonces se tienen los siguientes casos posibles.

1. Si $\mathrm{gr}(b(x)) < p-1$, entonces $b(x) \in \mathbb{F}_2[x]/\langle q(x)\rangle$. Por lo tanto tenemos que
$$\varphi(b(x) + \langle q(x)\rangle) = b(x) + \langle x^p - 1\rangle.$$

2. Si $\mathrm{gr}(b(x)) = p-1$, entonces $b(x) = (b_0 + b_1x + \cdots + b_kx^k) + x^{p-1}$, con $k < p-1$.

   Sea $u(x) := ((b_0 + b_1x + \cdots + b_kx^k) + (q(x) + x^{p-1}))$. Entonces tenemos que $\mathrm{gr}(u(x)) < p-1$ y dado que $\mathrm{wt}(b(x))$ es par, concluimos que $\mathrm{wt}(u(x))$ es impar. Luego existe $u(x) \in \mathbb{F}_2[x]/\langle q(x)\rangle$ tal que

$$\begin{aligned}\varphi(u(x) + \langle q(x)\rangle) &= (u(x) + q(x)) + \langle q(x)\rangle \\ &= (((b_0 + b_1x + \cdots + b_kx^k) + (q(x) + x^{p-1})) + q(x)) + \langle x^p - 1\rangle \\ &= b(x) + \langle x^p - 1\rangle.\end{aligned}$$

■

2.2.12 Lema. Sea $p \neq 2$ un número primo, tal que $s(p) = p-1$, $\beta(x) := 1 + x^2 + x^3 + \ldots + x^{p-1}$ y $\alpha(x)$ un elemento primitivo de P. Entonces

$$\langle\delta(x)\rangle = \bigcup_{i=0}^{\frac{2^{\frac{p-1}{2}}+1}{p}-1} \delta(x)^i\langle\beta(x)\rangle,$$

donde $\delta(x) := \alpha(x)^{2^{\frac{p-1}{2}}-1}$.

Demostración. De acuerdo con el lema 2.1.8, $H = \langle\beta(x)\rangle$ es el único subgrupo de orden p en $P\backslash\{0\}$ y $\beta(x), \beta(x)^2, \ldots, \beta(x)^{p-1}$ son los únicos elementos de orden p. Puesto que $s(p) = p-1$, entonces $p \mid 2^{p-1} - 1$. Por lo tanto $p \mid 2^{\frac{p-1}{2}} + 1$. Puesto que

$$\mathrm{ord}(\delta(x)^{\frac{2^{\frac{p-1}{2}}+1}{p}}) = \frac{2^{\frac{p-1}{2}} + 1}{(\frac{2^{\frac{p-1}{2}}+1}{p}, 2^{\frac{p-1}{2}} + 1)} = p$$

tenemos que $\langle\delta(x)^{\frac{2^{\frac{p-1}{2}}+1}{p}}\rangle = \langle\beta(x)\rangle$. Por lo tanto $\langle\beta(x)\rangle \leq \langle\delta(x)\rangle$. Sabemos que $\langle\delta(x)\rangle/\langle\beta(x)\rangle = \langle\delta(x)\langle\beta(x)\rangle\rangle$. Puesto que $|\langle\delta(x)\rangle/\langle\beta(x)\rangle| = \frac{|\langle\delta(x)\rangle|}{|\langle\beta(x)\rangle|} =$

$\frac{2^{\frac{p-1}{2}}+1}{p}$ obtenemos

$$\langle\delta(x)\rangle/\langle\beta(x)\rangle = \{e(x)\langle\beta(x)\rangle, \delta(x)\langle\beta(x)\rangle, \delta(x)^2\langle\beta(x)\rangle, \ldots, \delta(x)^{\frac{2^{\frac{p-1}{2}}+1}{p}-1}\langle\beta(x)\rangle\}.$$

Esto es,

$$\langle\delta(x)\rangle = \bigcup_{i=0}^{\frac{2^{\frac{p-1}{2}}+1}{p}-1} \delta(x)^i\langle\beta(x)\rangle.$$

■

Capítulo 3

Aplicaciones

En este capítulo utilizaremos los resultados obtenidos sobre códigos binarios autoduales con un automorismo de orden primo impar que se presentaron en el capítulo anterior. Principalmente utilizaremos los teoremas 2.2.8 y 2.2.9 que nos brindan las condiciones suficientes y necesarias para la construcción de códigos binarios auto-ortogonales o autoduales respectivamente, con un automorfismo de orden primo impar.

Iniciaremos construyendo tres [40,20,8]-códigos binarios autoduales doblemente pares y extremales con un automorfismo de orden 19 y un [40,20,8]-código binario autodual doblemente par y extremal con un automorfismo de orden 5. También construiremos 21 códigos autoduales doblemente pares con parámetros [120,60,20] con un automorfismo de orden 23 y finalmente 20 códigos autoduales doblemente pares con parámetros [120,60,20] con un automorfismo de orden 29.

3.1 Códigos binarios autoduales doblemente pares y extremales con parametros [40,20,8]

3.1.1 Lema. Sea C un [40,20,8]-código binario autodual doblemente par. Entonces el enumerador de peso de C está dado por el polinomio

$$W_C(x) = x^{40} + 285x^{32} + 21280x^{28} + 239970x^{24} + 525504x^{20} + 239970x^{16} + 21280x^{12} + 285x^8 + 1.$$

Demostración. Según el teorema 1.4.2, tenemos que

$$W_C(x,y) = \sum_{i=0}^{1} a_i g_2(x,y)^{5-3i} g_3(x,y)^i, \tag{3.1}$$

donde $g_2(x,y) = y^8 + 14x^4y^4 + x^8$ y $g_3(x,y) = y^{24} + 759x^8y^{16} + 2576x^{12}y^{12} + 759x^{16}y^8 + x^{24}$. También sabemos por definición que

$$W_C(x,y) = \sum_{i=0}^{40} A_i x^{n-i} y^i. \tag{3.2}$$

Por otra parte, por lema 1.2.5 sabemos que C solo contiene vectores de peso par, luego $A_i = 0$ para i impar. Teniendo en cuenta que C es doblemente par y que $\mathrm{d}(C) = 8$, podemos afirmar que

$$A_2 = A_4 = A_6 = A_{10} = A_{14} = A_{18} = A_{22} = A_{26} = A_{30} = A_{34} = A_{38} = 0.$$

Además, como solo existe un vector con entradas todas 1 y un vector con entradas todas 0, sabemos que $A_0 = A_{40} = 1$. Ahora, si hacemos $y := 1$ e igualamos las expresiones (3.1) y (3.2) obtenemos que:
$a_0(1+14x4+x8)^5 + a_1(1+14x^4+x^8)^2(1+759x^8+2576x^{12}+759x^{16}+x^{24}) = x^{40}+A_{36}x^{36}+A_{32}x^{32}+A_{28}x^{28}+A_{24}x^{24}+A_{20}x^{20}+A_{16}x^{16}+A_{12}x^{12}+A_8x^8+1$.
Si desarrollamos los productos indicados e igualamos término a término obtenemos las siguientes relaciones

$$a_0 + a_1 = A_{40} = A_0,$$
$$70a_0 + 28a_1 = A_{36},$$
$$1965a_0 + 957a_1 = A_{32} = A_8,$$
$$27720a_0 + 23856a_1 = A_{28} = A_{12},$$
$$197970a_0 + 223170a_1 = A_{24} = A_{16},$$
$$593124a_0 + 552552a_0 = A_{20}.$$

Teniendo en cuenta que $A_i = A_{n-i}$, sabemos que $A_{36} = A_4 = 0$ y dado que $A_{40} = A_0 = 1$. Con las dos primeras ecuaciones obtenemos el siguiente sistema de ecuaciones:

$$a_0 + a_1 = 1$$
$$70a_0 + 28a_1 = 0,$$

Del cual se deduce que $a_1 = \frac{35}{21}$ y $a_0 = -\frac{14}{21}$ y realizando los cálculos correspondientes, obtenemos que

$$A_0 = A_{40} = 1,$$
$$A_{32} = A_8 = 285,$$
$$A_{28} = A_{12} = 21280,$$
$$A_{24} = A_{16} = 239970,$$
$$A_{20} = 525504.$$

■

3.1.2 Lema. Sea C un [40,20,8]-código binario autodual doblemente par y σ un automorfismo de C de tipo p-$(c; f)$, donde p es un primo impar. Entonces los posibles tipos de σ son los siguientes:

p	c	f
3	12, 10, 8, 6	4, 10, 16, 22
5	8, 4	0, 20
7	5	5
19	2	2

Demostración. Dado que $\sigma \in \mathrm{Sym}(40)$, tenemos que $p \leq 37$ y se verifica que todos los posibles tipos de automorfismos son los siguientes:

p	c	f
3	13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1	1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34,37
5	8, 7, 6, 5, 4, 3, 2, 1	0, 5, 10, 15, 20, 25, 30, 35
7	5, 4, 3, 2, 1	5, 12, 19, 26, 33
11	3, 2, 1	7, 18, 29
13	3, 2, 1	1, 14, 27
17	2, 1	6, 23
19	2, 1	2, 21
23	1	17
29	1	11
31	1	9
37	1	3

(3.3)

De los posibles tipos registrados en (3.3) se verifica que los casos 37-(1;3), 31-(1; 9), 29-(1;11), 23-(1;17), 19-(1;21), 17-(2;6), 13-(2;14), 11-(3;7), 11-(2;18),

7-(4;12), 7-(3;19), 5-(6;10) no satisfacen la condición 2 del lema 2.1.9. Los casos 17-(1;23), 13-(1;27), 11-(1;29), 7-(2;26), 7-(1;33), 5-(2;30), 3-(4;28), 3-(2; 34) no satisfacen la condición 1 del lema 2.1.9. Finalmente los casos 13-(3;1), 5-(7; 5), 5-(5;15), 5-(3,25), 5-(1;35), 3-(13;1), 3-(11;7), 3-(9;13), 3-(7;19), 3-(5; 25), 3-(3; 31), 3-(1;37), no satisfacen el lema 2.2.3. ∎

De los posibles tipos de automorfismos que se anotan en el lema 3.1.2, tenemos que los casos 5-(8;0) y 3-(12;4) ya han sido trabajados en [15] y los casos 3-(6;22), 3-(8;16) y 3-(10;10) aún son desconocidos.
De los casos restantes, seran trabajados en esta sección los automorfismos de tipos 19-(2;2) y 5-(4;20).

3.1.1 Automorfismos de orden 19

3.1.3 Teorema. Existen, salvo equivalencia, únicamente tres [40,20,8]-códigos autoduales doblemente pares con un automorfismo de tipo 19-(2;2).

Demostración. Sea C un código autodual con un automorfismo de orden 19. Entonces por el lema 3.1.2, $p = 19$ y $c = f = 2$. Del lema 2.1.5 tenemos que $\pi(F_\sigma(C))$ es un [4,2]-código autodual y de [15] sabemos que

$$\pi(F_\sigma(C)) \sim C_2 \oplus C_2.$$

Es conocido que

$$\mathrm{gen}(C_2 \oplus C_2) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

Por lo tanto

$$\mathrm{gen}(\pi(F_\sigma(C))) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

puesto que otra elección llevaría a un vector $v \in F_\sigma(C)$ de peso menor que 8 o no divisible por 4, lo cual es un absurdo. En consecuencia

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \end{array}\right),$$

donde $\mathbf{1}$ es el vector de todos 1 de longitud 19 y $\mathbf{0}$ es el vector de todos 0 de longitud 19.
Dado que el orden multiplicativo de 2 módulo 19 es 18, tenemos que el polinomio $1+x+x^2+\cdots+x^{18}$ es irreducible en $\mathbb{F}_2[x]$ y por el lema 2.2.9, sabemos que el código $\varphi(E_\sigma(C)^*)$ es autodual con parámetros [2,1] sobre el campo P de 2^{18} elementos, con respecto al producto escalar $u \cdot v = u_1 {v_1}^{2^9} + u_2 {v_2}^{2^9}$.

Luego, la matriz generadora del código $\varphi(E_\sigma(C)^*)$ se puede tomar de la forma $[e(x), a(x)]$, donde $e(x) = x + x^2 + \cdots + x^{18}$ es el elemento identidad de P y $0 \neq a(x) \in P$ (Si $a(x) = 0$ el vector resultante no es auto-ortogonal).
Si $\mu(x)$ es un elemento primitivo de P, entonces $a(x) = \mu(x)^t$, para algún t tal que, $0 \leq t < 2^{18} - 1$. Tenemos entonces $2^{18} - 1$ posibilidades para el código $\varphi(E_\sigma(C)^*)$ y la matriz $\text{gen}(\varphi(E_\sigma(C)^*))$ será de la forma $[e(x), \mu(x)^t]$, para $0 \leq t < 2^{18} - 1$.
De la condición de auto-ortogonalidad tenemos que si $v = [e(x), a(x)]$, entonces

$$0 = v \cdot v = (e(x), \mu(x)^t) \cdot (e(x), \mu(x)^t), \text{ para } 0 \leq t < 2^{18} - 1.$$

De donde concluimos que $\mu(x)^{513t} = e(x)$ y por lo tanto $\text{ord}(\mu(x))|513t$, es decir $513t \equiv 0$ mód $2^{18} - 1$ y $t \equiv 0$ mód 511. Consecuentemente $a(x) = \psi(x)^k$, donde $\psi(x) = \mu(x)^{511}$ y $0 \leq k \leq 512$. Entonces el orden del elemento $\psi(x)$ es 513, obteniendoce así 513 posibles códigos y por lo tanto

$$\text{gen}(\varphi(E_\sigma(C)^*)) = [e(x), \psi(x)^t],$$

donde $0 \leq t < 512$.
Por otra parte, ya vimos en el numeral 3. del lema 2.1.7, que multiplicar en P por el elemento $\beta(x) = 1 + x^2 + x^3 + \cdots + x^{18}$ es equivalente a una traslación cíclica. Ahora, por el lema 2.1.8, tenemos que el orden multiplicativo de $\beta(x)$ es 19 y que $\beta(x), \beta(x)^2, \ldots, \beta(x)^{18}$ son todos los elementos de orden 19 en P. Pero, dado que $\text{ord}(\psi(x)^{27})$ es 19, concluimos que el grupo cíclico $\langle\beta(x)\rangle$ es un subgrupo de $\langle\psi(x)\rangle$, ya que como el $\text{ord}(\psi(x)^{27}) = 19$, entonces $\psi(x)^{27} \in \{\beta^j(x), j = 1, \ldots, 18\}$. Por lo tanto $\langle\beta(x)\rangle = \langle\psi(x)^{27}\rangle \leq \langle\psi(x)\rangle$.

Por el lema 2.2.12 podemos tomar como un transversal de $\langle\beta(x)\rangle$ en $\langle\delta(x)\rangle$ el conjunto

$$\langle\psi(x)\rangle/\langle\beta(x)\rangle = \langle\psi(x)\langle\beta(x)\rangle\rangle = \{e(x)\langle\beta(x)\rangle, \psi(x)\langle\beta(x)\rangle, \ldots, \psi^{26}(x)\langle\beta(x)\rangle\}.$$

Además si $g(x)$ y $c(x)$ de $\langle\psi(x)\rangle$ pertenecen a la misma clase lateral de $\langle\psi(x)\rangle$ con respecto a $\langle\beta(x)\rangle$, entonces los códigos correspondientes a $g(x)$ y $c(x)$ son equivalentes, debido al hecho de que $g(x) = \beta^j(x)c(x)$. Esto porque si $g(x), c(x) \in p(x)\langle\beta(x)\rangle$, con $p(x) = \psi^i(x), i = 0, \ldots, 26$, entonces $g(x) = p(x)\beta^k(x)$ y $c(x) = p(x)\beta^h(x)$. Obteniendose que $p(x) = g(x)\beta^{-k} = c(x)\beta^{-h}$ y por lo tanto $g(x) = \beta^j(x)c(x)$, $j = k - h$. Ahora si C' y C son los códigos generados por las matrices que generan los vectores $(e(x), g(x))$ y $(e(x), c(x))$ en $\text{gen}(\varphi(E_\sigma(C)^*)$ respectivamente, entonces C' tiene una matriz generada por el vector $(e(x), c(x)\beta^j(x))$, es decir C' se obtiene de C por la multiplicación de la segunda componente por el elemento $\beta^j(x), j = 1, \ldots, 18$. Por la operación 2 del lema 2.2.10, los códigos C y C' son equivalentes. Por lo tanto para la

construción del código no hay necesidad de tomar todos los $\psi(x)^t$ de $\langle\psi(x)\rangle$, sino solamente los elementos del transversal

$$T = \{e(x), \psi(x), \ldots, \psi(x)^{26}\}. \tag{3.4}$$

Entonces la matriz generadora del código C tiene la forma:

$$\text{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\psi^t(x)] & \mathbf{0} & \mathbf{0} \end{array}\right), \; 0 \leq t \leq 26.$$

donde $\mathbf{1}$ y $\mathbf{0}$ son respectivamente las matrices de unos y ceros. En conclusión hay 27 posibles códigos.

Por la operación 1 del teorema 2.2.10, los códigos $(e(x), \psi(x)^i)$ y $(e(x), \psi(x)^{2i})$ son equivalentes, lo cual particiona el transversal (3.4) en cuatro orbitas, que son:

$$\begin{aligned}
[\psi(x)] &= \{\psi(x), \psi^2(x), \psi^4(x), \psi^8(x), \psi^{16}(x), \psi^5(x), \psi^{10}(x), \psi^{20}(x), \psi^{13}(x), \psi^{26}(x), \\
&\qquad \psi^{25}(x), \psi^{23}(x), \psi^{19}(x), \psi^{11}(x), \psi^{22}(x), \psi^{17}(x), \psi^7(x), \psi^{14}(x)\}, \\
[\psi^3(x)] &= \{\psi^3(x), \psi^6(x), \psi^{12}(x), \psi^{24}(x), \psi^{21}(x), \psi^{15}(x)\}, \\
[\psi^9(x)] &= \{\psi^9(x), \psi^{18}(x)\} \text{ y} \\
[e(x)] &= \{e(x)\}.
\end{aligned}$$

Por lo tanto se reduce la cantidad de posibles codigos no equivalentes a 4. Pero teniendo en cuenta que el código para el cual $\text{gen}(\varphi(E_\sigma(C)^*) = (e(x), e(x))$ no es extremal, ya que $E_\sigma(C)$ contiene el vector $0111\cdots10111\cdots100$ cuya suma con el vector de todos los unos es igual a 4, solo se consideran los representantes $\psi(x), \psi(x)^3, \psi(x)^9$ para la formación de los códigos. Entonces la matriz generadora del código C tiene la forma:

$$\text{gen}(C) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\psi^t(x)] & \mathbf{0} & \mathbf{0} \end{array}\right), \; t = 1, 3, 9.$$

Tomando el elemento primitivo $\mu(x) = 1 + x + x^3 + x^6 \in P$ y sabiendo que $\psi(x) = \mu(x)^{511}$, calculamos:

$$\begin{aligned}
\psi(x) &= x^2 + x^3 + x^5 + x^9 + x^{10} + x^{12} + x^{13} + x^{14} + x^{15} + x^{17}. \\
\psi(x)^3 &= x + x^3 + x^5 + x^6 + x^8 + x^{11}. \\
\psi(x)^9 &= 1 + x + x^6 + x^8 + x^{10} + x^{11} + x^{12} + x^{13} + x^{16} + x^{17}.
\end{aligned}$$

Sean B_1, B_2 y B_3 los códigos sobre $\mathbb{F}_2$ generados por las siguientes matrices, respectivamente:

$$\text{gen } (B_1) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\psi(x)] & 0 & 0 \end{array}\right),$$

$$\text{gen } (B_1) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\psi(x)^3] & 0 & 0 \end{array}\right) \text{ y}$$

$$\text{gen } (B_1) = \left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\psi(x)^9] & 0 & 0 \end{array}\right),$$

donde **1** y **0** son las matrices de todos de unos y todos ceros respectivamente; $[e(x)]$, $[\psi(x)]$, $[\psi(x)^3]$ y $[\psi(x)^9]$ son matrices de dimensiones (18×19), circulantes, cuyas primeras filas son: 0111111111111111111, 0011010001101111010, 0101011010010000000 y 110000101011110011, respectivamente.
Puesto que los vectores de la matriz generadora del código B_i, $i = 1, 2, 3$ son ortogonales, entonces el código B_i es auto-ortogonal. Ademaás dado que el peso de cada vector de la matriz generadora es doblemente par, por el teorema 1.2.7, el código B_i es doblemente par. Hecho que también comprobamos utilizando el programa Magma (ver anexos 4.0.3).
Luego, hemos demostrado que cada [40,20,8]-código autodual doblemente par con automorfismo de orden 19 es equivalente a uno de los códigos B_1, B_2, B_3 definidos anteriormente. ∎

3.1.2 Automorfismos de orden 5

3.1.4 Teorema. Existe, salvo equivalencia, únicamente un $[40, 20, 8]$-código autodual doblemente par con un automorfismo de tipo 5-(4;20).

Demostración. Probemos primero que el código $\pi(F_\sigma(C))$ es equivalente al Golay code G_{24}.
Puesto que el orden de 2 mod 5 es 4, tenemos que el polinomio $1+x+x^2+x^3+x^4$ es irreducible en $\mathbb{F}_2[x]$ y por lo tanto P es un campo de 2^4 elementos. Dado que el código C es autodual, entonces por el lema 2.1.5, tenemos que $\pi(F_\sigma(C))$ es un $[24, 12, d']$-código binario autodual. Además como C es doblemente par y $5 \equiv 1 \bmod 4$, tenemos que el código $\pi(F_\sigma(C))$ también es doblemente par. Por lo tanto d' es un multiplo de 4.

Teniendo en cuenta que $d' \leq 4\lfloor \frac{n}{24} \rfloor + 4$, concluimos que los posibles valores de d' son 4 y 8. Todos estos $[24, 12, d']$-códigos autoduales y doblemente pares, se encuentran caracterizados en la tabla 1 de [7] y las siguientes son las componentes de sus matrices generadoras (ver más detalles en anexos 4.0.4):

Código	Componentes	Generadores de cola
A_{24}	d_{12}^2	ab/ba
B_{24}	d_{10}/e_7^2	$bcc/a0c$
C_{24}	d_8^3	$abb/bab/bba$
D_{24}	d_6^4	$baa0/0baa/a0ba/aa0b$
E_{24}	d_{24}	a
F_{24}	d_4^6	$b0a^30/0ba^3/a0b0a^2/a^20b0a/a^30b0/0a^30b$
G_{24}	Golay code	
H_{24}	$d_{16}e_8$	a
I_{24}	e_8^3	

(3.5)

Donde

$$d_n := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & & \\ & & & & & & \cdots & & & & & \\ & & & & & & 1 & 1 & 1 & 1 & & \\ & & & & & & & & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$e_n := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & & \\ & & & & & & \cdots & & & & & \\ & & & & & & 1 & 1 & 1 & 1 & & \\ & & & & & & & & 1 & 1 & 1 & 1 \\ 1 & & 1 & & 1 & & 1 & & 1 & & 1 & \end{pmatrix}$$

$$a := \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 & 1 \end{pmatrix}$$

$$b := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$$

$$c := \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & \cdots & 1 & 0 \end{pmatrix}$$

Probemos ahora que de los 9 códigos en la tabala 3.5, unicamente el Golay code es equivalente al código $\pi(F_\sigma(C))$.
Los códigos de la tabla 3.5, con componentes e_n^i ó d_n^i tienen 6 o más vectores de peso 4. Notese que realizando todas las posibles permutaciones a las columnas de estos códigos, siempre se forma al menos un vector de peso 4, cuyas primeras 4 coordenadas son ceros. Dicho vector genera en C un vector de peso 4 , lo cual es un absurdo ya que $\mathrm{d}(C) = 8$. De lo anterior podemos concluir que el código $\pi(F_\sigma(C))$ es equivalente al Golay code G_{24}.

Encontremos ahora la forma de la matriz $\mathrm{gen}(\varphi(E_\sigma(C)^*))$.
Dado que el polinomio $1 + x + x^2 + x^3 + x^4$ es irreducible en $\mathbb{F}_2[x]$ y C es un código autodual, entonces por los teoremas 2.2.3 y 2.2.9 tenemos que $\varphi(E_\sigma(C)^*)$ es un $[4, 2, \hat{d}]$-código autodual sobre el campo P con 2^4 elementos, respecto al producto escalar

$$u \cdot v = u_1v_1^4 + u_2v_2^4 + u_3v_3^4 + u_4v_4^4. \tag{3.6}$$

Demostremos que $\varphi(E_\sigma(C)^*)$ un [4,2,3]-código sobre P, es decir, que $\hat{d} = 3$.
Si $\hat{d} = 1$, entonces existe un vector $v \in \varphi(E_\sigma(C)^*)$ compuesto por un único polinomio $0 \neq v_1 \in P$. Vemos que v no es auto-ortogonal respecto al producto escalar 3.6, ya que $v \cdot v = v_1v_1^4 = v_1^5 \neq 0$. Por lo tanto $\hat{d} \neq 1$.
Si $\hat{d} = 2$, entonces existe un vector $u \in \varphi(E_\sigma(C)^*)$ de peso 2. Supongamos que $u = (u_1, u_2, 0, 0)$ con $u_1, u_2 \in P/\{0\}$.
Sea $M = \langle u \rangle$, sobre P. Entonces $M = \{(pu_1, pu_2, 0, 0) \mid p \in P\}$, luego $\dim_{\mathbb{F}_2}(M) = 4$. Entonces $W := \varphi(M) \subseteq E_\sigma(C)^*$ es un código sobre $\mathbb{F}_2$ de $\dim_{\mathbb{F}_2}(W) = 4$, dado que $8 = \mathrm{d}(C) \leq \mathrm{d}(E_\sigma(C)) = \mathrm{d}(E_\sigma(C)^*) \leq \mathrm{d}(W)$, entonces W es un $[20, 4, \widetilde{d}]$-código sobre $\mathbb{F}_2$ con $\widetilde{d} \geq 8$.
Ahora, sea $W^* \subseteq \mathbb{F}_2^{10}$, obtenido de W borrandole las últimas 10 coordenadas. Entonces W^* es un [10,4,d''], donde $d'' = \widetilde{d} \geq 8$. Vemos que el código W^* contradice la cota de Griesmer, (ver lema 1.1.7) ya que

$$\sum_{i=0}^{3} \lceil d''/2^i \rceil \geq \sum_{i=0}^{3} \lceil 8/2^i \rceil = 15 > 10.$$

Por lo tanto $\hat{d} \neq 2$ y puesto que $\hat{d} \leq n - k + 1 = 3$, por Singleton (lema 1.1.8), tenemos que $\hat{d} \leq 3$. Habiendo descartado $\hat{d} = 1$ y $\hat{d} = 2$, concluimos que $\hat{d} = 3$. En conclusión hemos probado que $\varphi(E_\sigma(C)^*)$ un [4,2,3]-código sobre P.

Puesto que $\varphi(E_\sigma(C)^*)$ satisface la igualdad en la cota de Singleton, tenemos que $\varphi(E_\sigma(C)^*)$ es un MDS-código sobre P. Por lo tanto, por corolario 1.1.10,

cada dos columnas de $\varphi(E_\sigma(C)^*)$ son linealmente independientes y por lo cual podemos suponer que

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \alpha^{t_1} & 0 & \alpha^{t_3} & \alpha^{t_5} \\ 0 & \alpha^{t_2} & \alpha^{t_4} & \alpha^{t_6} \end{pmatrix},$$

donde α es un elemento primitivo de $P/\{0\}$ y $1 \leq t_i \leq 2^4 - 2 = 14$.
Sabemos que el orden multiplicativo de P es $2^4 - 1 = 5 \times 3$. Luego sean $\phi = \alpha^5$ y $\delta = \alpha^3$. Entonces $\mathrm{ord}(\phi) = 3$ y $\mathrm{ord}(\delta) = 5$, por lo tanto

$$\mathrm{ord}(\phi\delta) = \mathrm{ord}(\phi)\mathrm{ord}(\delta) = 15 = \mathrm{ord}(\alpha).$$

Entonces $\phi\delta$ es también un elemento primitivo de $P/\{0\}$ y podemos suponer que

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} (\phi\delta)^{i_1} & 0 & (\phi\delta)^{i_3} & (\phi\delta)^{i_5} \\ 0 & (\phi\delta)^{i_2} & (\phi\delta)^{i_4} & (\phi\delta)^{i_6} \end{pmatrix},$$

donde $0 \leq i_j \leq 14$. Si multiplicamos la primera fila por $\delta^{-i_3}\phi^{-i_1}$ y la segunda por $\delta^{-i_4}\phi^{-i_2}$ tenemos que

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \delta^{s_1} & 0 & \phi^{t_1} & \phi^{t_2}\delta^{s_2} \\ 0 & \delta^{s_3} & \phi^{t_3} & \phi^{t_4}\delta^{s_4} \end{pmatrix},$$

donde $0 \leq s_i \leq 4$ y $0 \leq t_i \leq 2$.

Por el lema 2.2.12 podemos tomar como un transversal de $\langle\beta(x)\rangle$ en $\langle\delta(x)\rangle$ el conjunto $\{e(x)\}$. Entonces podemos suponer que

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} e & 0 & \phi^{t_1} & \phi^{t_2} \\ 0 & e & \phi^{t_3} & \phi^{t_4}\delta^{s_5} \end{pmatrix},$$

donde $0 \leq s_i \leq 4$ y $0 \leq t_i \leq 2$.
Ahora, dado que $\varphi(E_\sigma(C)^*)$ es autodual, utilizando el producto escalar (3.6) tenemos que

$$(0, e, \phi^{t_3}, \phi^{t_4}\delta^{s_4}) \cdot (e, 0, \phi^{t_1}, \phi^{t_2}) = \phi^{t_3}\phi^{4t_1} + \phi^{t_4}\delta^{s_5}\phi^{4t_2} = 0.$$

Pero como $\mathrm{ord}(\phi) = 3$, entonces $\phi^4 = \phi$. Por lo tanto tenemos que

$$\phi^{t_3}\phi^{t_1} + \phi^{t_4}\delta^{s_5}\phi^{t_2} = 0.$$

En consecuencia $\phi^{t_3+t_1-t_4-t_2} = \delta^{s_5}$ y entonces $\mathrm{ord}(\phi^{t_3+t_1-t_4-t_2}) \mid \mathrm{ord}(\delta^{s_5})$. Además $\mathrm{ord}(\phi^{t_3+t_1-t_4-t_2}) \mid \mathrm{ord}(\phi) = 5$ y $\mathrm{ord}(\delta^{s_5}) \mid \mathrm{ord}(\delta) = 5$. Por lo tanto podemos afirmar que

$$\mathrm{ord}(\phi^{t_3+t_1-t_4-t_2}) = \mathrm{ord}(\delta^{s_5}) = 1.$$

Por consiguiente $\phi^{t_3+t_1-t_4-t_2} = \delta^{s_5} = e$, y $\phi^{t_3+t_1} = \phi^{t_4+t_2}$. Entonces tenemos que

$$\text{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} e & 0 & \phi^{t_1} & \phi^{t_2} \\ 0 & e & \phi^{t_3} & \phi^{t_4} \end{pmatrix},$$

con

$$t_4 - t_3 \equiv t_1 - t_2 \text{ mód } 3. \tag{3.7}$$

Por otra parte, de la auto-ortogonalidad de $\varphi(E_\sigma(C)^*)$ tenemos que $(e, 0, \phi^{t_1}, \phi^{t_2}) \cdot (e, 0, \phi^{t_1}, \phi^{t_2}) = e + \phi^{t_1}\phi^{4t_1} + \phi^{t_2}\phi^{4t_2} = 0$. Dado que $(\phi^4)^{t_i} = \phi^{t_i}$, tenemos que $\phi^{2t_1} + \phi^{2t_2} = e$. Puesto que la caracteristica del campo es 2, entonces $\phi^{2t_1} + \phi^{2t_2} = (\phi^{t_1} + \phi^{t_2})^2$, por lo tanto tenemos que $\phi^{t_1} + \phi^{t_2} = e$. De forma similar obtenemos que $\phi^{t_3} + \phi^{t_4} = e$. En conclusión, se debe cumplir que

$$\begin{aligned} \phi^{t_1} + \phi^{t_2} &= e, \\ \phi^{t_3} + \phi^{t_4} &= e. \end{aligned} \tag{3.8}$$

Dado que $\text{ord}(\phi) = 3$, los valores de t_i pueden ser $0, 1, 2$, pero como $\phi^0 = e$ y además ϕ^i es un elemento de $P/\{0\}$, entonces los únicos valores posibles para t_i son 1 y 2.
Sea $\alpha = 1 + x$ de $P/\{0\}$. Entonces realizando los cálculos con MAGMA, tenemos que $\text{ord}(\alpha) = |P/\{0\}| = 15$, luego α es un elemento primitivo de $P/\{0\}$ y dado que $\phi = \alpha^5$, tenemos que $\phi = x + x^4$ y $\phi^2 = x^2 + x^3$. Por lo tanto $\phi + \phi^2 = x + x^2 + x^3 + x^4 = e$. Además como $1 - 2 \equiv 1 - 2$ mód 3 y $2 - 1 \equiv 2 - 1$ mód 3, entonces los únicos pares $(t_1, t_2), (t_3, t_4)$ que satisfacen las condiciones (3.7) y (3.8) son $(1, 2), (2, 1)$ y $(2, 1)(1, 2)$, respectivamente. Por lo tanto la matriz $\text{gen}\varphi(E_\sigma(C)^*)$ tiene las siguientes formas

$$M = \text{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} e & 0 & \phi^1 & \phi^2 \\ 0 & e & \phi^2 & \phi^1 \end{pmatrix},$$

$$M' = \text{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} e & 0 & \phi^2 & \phi^1 \\ 0 & e & \phi^1 & \phi^2 \end{pmatrix},$$

Teniendo en cuenta que el grupo de automorfismos del código de Golays es 5-transitivo ([6]-pag 616), entonces cada permutación de coordenadas del código $\varphi(E_\sigma(C)^*)$ conduce a un código equivalente a C. Por lo tanto M Y M' conducen a dos códigos C y C' equivalentes. Luego podemos afirmar que

$$\text{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} e & 0 & \phi^1 & \phi^2 \\ 0 & e & \phi^2 & \phi^1 \end{pmatrix}.$$

Por lo tanto la matriz $\mathrm{gen}(C)$ es de la forma:

$$\mathrm{gen}(C) = \left(\begin{array}{c|c|c|c|c} \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & [\mathbf{N}] \\ \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \\ \hline [e(x)] & [\mathbf{0}] & [x+x^4] & [x^2+x^3] & [\mathbf{0}] \\ \hline [\mathbf{0}] & [e(x)] & [x^2+x^3] & [x+x^4] & [\mathbf{0}] \end{array}\right),$$

donde $\mathbf{0}$ es el vector de longitud 5 con entradas todas ceros, $\mathbf{1}$ es el vector de longitud 5 con entradas todas unos, $\mathbf{J}$ es la matriz de tamaño 8×5 con entradas todas unos, $\mathbf{O}$ es la matriz de tamaño 8×5 con entradas todas ceros, $[p(x)]$ es la matriz circulante de tamaño 4×5 generada por el polinomio $p(x)$ y $[\mathbf{N}]$ es la matriz de tamaño 12×20 formada por las últimas 20 columnas del código de Golays.

En conclusión solo existe está matriz como posible matriz generadora del código C y se ha verificado con MAGMA que esta conduce a un autodual doblemente par con $\mathrm{d}(C) = 8$. ∎

3.2 Códigos binarios autoduales doblemente pares con parámetros [120,60,20]

En la sección de códigos extremales se habló sobre la familia de códigos con parámetros $[24m, 12m, 4m+4], m \in \mathbb{N}$ y su importancia para la detección y corrección de errores y su conección con los diseños. Se dijo que solamente se han construido dos códigos autoduales extremales con estos parámetros y corresponden a $m = 1$ y $m = 2$. Para los casos $m = 3, 4$ y 5, se han hecho algunos avances en los últimos años y se tiene información parcial sobre la estructura de sus grupos de automorfismos, pero hasta la fecha la existencia de códigos con estos parametros es una pregunta abierta. Por lo tanto resulta interesante la construcción de códigos que aunque no son extremales, tienen distancia mínima lo más cercana a la de uno extremal de igual longitud, estos son los llamados códigos optimales. En esta sección abordaremos códigos optimales cuando $m = 5$, es decir códigos binarios autoduales doblemente pares con parámetros [120,60,20] y para su construcción utilizaremos automorfismos de orden 23 y 29.

3.2.1 Automorfismos de orden 23

Para la construción de este tipo de códigos con automorfismo de orden 23 nos apoyaremos en los resusltados obtenidos por Wassermann y Yorgova [23].

3.2.1 Teorema. Existen por lo menos 21 códigos autoduales doblemente pares con parámetros [120,60,20] y con un automorfismo de orden 23.

Demostración. Para la obtención de estos códigos hallaremos las posibles matrices generadoras de códigos tipo II con parámetros [120,60,24] con un automorfismo de orden 23. Luego con MAGMA realizaremos una búsqueda exhaustiva de todos los códigos optimales generados con estas matrices.

Sea C un $[120, 60, 24]$-código autodual doblemente par con un automorfismo σ de orden 23. Entonces, por teorema 1 en [21], σ solamente puede estar constituido por 5 ciclos de orden 23 y 5 puntos fijos. Es decir, σ es un automorfismo del tipo 23-$(5; 5)$. Por lo tanto del lema 2.1.5, tenemos que el código $\pi(F_\sigma(C))$ es un [10,5]-código binario autodual y según la tabla 2 en [7], para el código $\pi(F_\sigma(C))$ solamente existen dos posibilidades, estas son C_2^5 y $A_8 \oplus C_2$. Cualquier elección de 5 posiciones fijas del código $A_8 \oplus C_2$, genera un vector de peso 26 en el subcódigo $F_\sigma(C)$, lo cual es un absurdo ya que C es doblemente par. Por lo tanto $\pi(F_\sigma(C))$ es equivalente a C_2^5 y su matriz generadora tiene la siguiente forma

$$\mathrm{gen}(\pi(F_\sigma(C))) = \left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

y por lo tanto

$$\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{ccccc|ccccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 & 0 & 1 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 1 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 & 0 & 1 \end{array}\right),$$

donde $\mathbf{1}$ es el vector de longitud 23 de todos 1 y $\mathbf{0}$ es el vector de longitud 23 de todos 0.

Hallemos ahora la forma de la matriz gen$(\varphi_\sigma(C)^*)$ para esto debemos tener en cuenta la siguiente factorización

$$x^{23} - 1 = (x-1)h_1(x)h_2(x),$$

donde

$$h_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1 \text{ y}$$
$$h_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

son irreducibles en $\mathbb{F}_2$ y por lo tanto, según lema 1.5.13, $P = I_1 \oplus I_2$, donde $I_j = \langle \frac{x^{23}-1}{h_j(x)} \rangle$, $j = 1, 2$.
Recordemos que I_j es un campo con 2^{11} elementos y también es un ideal minimal con polinomio de control $h_j(x)$.

Por el numeral 1 del lema 2.2.5, tenemos que $\varphi(E_\sigma(C)^*) = M_1 \oplus M_2$, donde M_j son códigos lineales sobre el campo I_j. Por lo tanto por el numeral 2 del lema 2.2.5

$$\dim_P(\varphi_\sigma((C)^*)) = \dim_{I_1}(M_1) + \dim_{I_2}(M_2) = \tfrac{cs}{2} = 5.$$

Sea $\delta_j(x) := \dfrac{x^{23}-1}{h_j(x)}$, para $j = 1, 2$. Entonces

$$\delta_1(x) := \frac{x^{23}-1}{h_1(x)} = (x-1)h_2(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^2 + 1$$
$$\delta_2(x) := \frac{x^{23}-1}{h_2(x)} = (x-1)h_1(x) = x^{12} + x^{10} + x^7 + x^4 + x^3 + x^2 + x + 1$$

Notemos que $\delta_j(x)$ es un elemento primitivo de I_j, es decir

$$I_j = \langle \delta_j(x) \rangle = \{0, \delta_j^k(x) \mid k = 0, 1, \ldots, 2^{11} - 2\}, \text{ para } j = 1, 2.$$

Luego, el orden multiplicativo de $\delta_j(x)$ es $2^{11} - 1 = 23 \times 89$ y dado que ord(x)=23, podemos escribir $\delta_j(x) = x\alpha_j(x)$. Teniendo así que ord$(\alpha_j(x))$=89 y que $\alpha_j(x)$ también es un generador de I_j, para $j = 1, 2$.
En este caso $x \equiv \beta_j(x) = xe_j(x)$, $j = 1, 2$. Donde $e_j(x)$ es el generador idempotente del ideal I_j. Sean ahora

$$e_1(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{17} + x^{15} + x^{14} + x^{11} + x^{10} + x^7 + x^5 + 1$$
$$e_2(x) = x^{18} + x^{16} + x^{13} + x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1.$$

Con MAGMA podemos comprobar que

1. $e_1^2(x) = e_1(x)$,
2. $e_2^2(x) = e_2(x)$,
3. $e_1(x)e_2(x) = 0$ y
4. $e_1(x) + e_2(x) = e(x)$, donde $e(x)$ es el elemento identidad de P.

Por teorema 1.5.11, $e_1(x)$ y $e_2(x)$ son generadores idempotentes de I_1 e I_2 respectivamente y por propiedades de ideales, $e_j(x)$ actua como elemento identidad en I_j.
Por lo anterior tenemos que:

$$\alpha_1(x) = x^{20} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^7 + x^3 + x + 1.$$

Denotemos $k_1 = \dim_{I_1}(M_1)$ y $k_2 = \dim_{I_2}(M_2)$. Notemos que siempre podemos linealizar la matriz $\text{gen}(M_1)$ de tal forma que $\text{gen}(M_1) = [I|A]$. Si esto no es posible, entonces en M_1 existe un vector no nulo que inicia con k_1 ceros, lo cual conlleva a una contradicción con el numeral 2 del teorema 2.2.8.

La sustitución $x \to x^2$ intercambia los idempotentes $e_1(x)$ y $e_2(x)$ y por lo tanto, también a M_1 y M_2. Por lo cual podemos asumir que $k_1 \geq k_2$ y dado que $k_1 + k_2 = 5$, entonces dos casos son posibles.

Caso 1: $k_1 = 4$ y $k_2 = 1$

$$\text{gen}(M_1) = \begin{pmatrix} e_1(x) & & & & \alpha_1^{t_1}(x) \\ & e_1(x) & & & \alpha_1^{t_2}(x) \\ & & e_1(x) & & \alpha_1^{t_3}(x) \\ & & & e_1(x) & \alpha_1^{t_4}(x) \end{pmatrix},$$

donde $t_i \in \{1, \ldots, 89\}$, para $i = 1, \ldots, 4$.

Por otra parte, si $\text{wt}(\alpha_1^{t_1}(x)) < 12$, entonces

$$\text{wt}((e_1, 0, 0, 0, \alpha_1^{t_1}(x), 0, 0, 0, 0, 0) < 24$$

y si $\text{wt}(\alpha_1^{t_1}(x)) > 12$, entonces

$$\text{wt}((e_1, 0, 0, 0, \alpha_1^{t_1}(x), 0, 0, 0, 0, 0) + (0, 0, 0, 0, 1, 0, 0, 0, 0, 1) < 24.$$

Por lo anterior podemos concluir que $\text{wt}(\alpha_1^{t_1}(x)) = 12$. De igual forma comprobamos que $\text{wt}(\alpha_1^{t_i}(x)) = 12$, para $i = 1, \ldots, 4$.

Calculamos los valores de t_i tal que $\mathrm{wt}(\alpha_1^{t_i}(x)) = 12$ y hallamos que

$$\begin{aligned} t_i \in T = \{&1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 16, 17, 18, 19, 20, 21, 23, 24, 27, \\ &28, 29, 32, 34, 36, 37, 38, 39, 40, 42, 45, 46, 47, 48, 49, 53, 54, 55, \\ &56, 58, 59, 63, 64, 67, 68, 69, 71, 72, 74, 76, 78, 79, 80, 84, 89\}, \end{aligned}$$

para $i = 1, \ldots, 4$.

Aplicando la sustitución $x \to x^2$ particionamos el conjunto T en cinco clases que son:

$\{1, 2, 4, 8, 16, 32, 64, 39, 78, 67, 45\}$, $\{3, 6, 12, 24, 48, 7, 14, 28, 56, 23, 46\}$,
$\{5, 10, 20, 40, 80, 71, 53, 17, 34, 68, 47\}$, $\{9, 18, 36, 72, 55, 21, 42, 84, 79, 69, 49\}$,
$\{19, 38, 76, 63, 37, 74, 53, 29, 58, 27, 54\}$ y $\{89\}$.

Si $t_1 = 89$, entonces $\alpha_1^{t_1}(x) = e(x)$ y por consiguiente se formará en M_1 un vector que no es auto-ortogonal.

Por la operación 1 del teorema 2.2.10 los valores de una misma clase, generan códigos equivalentes. Por esta razón solamente tomaremos un representante de cada clase para los posibles valores de t_1. Luego $t_1 = 1, 3, 5, 9, 19$ y $t_2, t_3, t_4 \in T$. Teniendo entonces que

$$\mathrm{gen}(M_1) = \begin{pmatrix} e_1(x) & & & & \alpha_1^{t_1}(x) \\ & e_1(x) & & & \alpha_1^{t_2}(x) \\ & & e_1(x) & & \alpha_1^{t_3}(x) \\ & & & e_1(x) & \alpha_1^{t_4}(x) \end{pmatrix},$$

donde $t_1 = \{1, 3, 5, 9, 19\}, t_2, t_3, t_4 \in T$.

Puesto que $\dim(M_2) = 1$ y dado que $\alpha_1(x^{-1})$ es un generador de M_2. Entonces es posible llevar $\mathrm{gen}(M_2)$ a la forma

$$\mathrm{gen}(M_2) = \begin{bmatrix} \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_2}(x^{-1}) & \alpha_1^{t_3}(x^{-1}) & \alpha_1^{t_4}(x^{-1}) & e_2(x) \end{bmatrix}.$$

En consecuencia

$$\mathrm{gen}(\varphi(E_\sigma(C))) = \begin{pmatrix} e_1(x) & & & & \alpha_1^{t_1}(x) \\ & e_1(x) & & & \alpha_1^{t_2}(x) \\ & & e_1(x) & & \alpha_1^{t_3}(x) \\ & & & e_1(x) & \alpha_1^{t_4}(x) \\ \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_2}(x^{-1}) & \alpha_1^{t_3}(x^{-1}) & \alpha_1^{t_4}(x^{-1}) & e_2(x) \end{pmatrix},$$

donde $t_1 = 1, 3, 5, 9, 19$ y $t_2, t_3, t_4 \in T$.

Por lo tanto gen(C) tiene la siguiente forma

$$\left(\begin{array}{ccccc|ccccc} \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 \\ \hline e_1(x) & & & & \alpha_1^{t_1}(x) & 0 & 0 & 0 & 0 & 0 \\ & e_1(x) & & & \alpha_1^{t_2}(x) & 0 & 0 & 0 & 0 & 0 \\ & & e_1(x) & & \alpha_1^{t_3}(x) & 0 & 0 & 0 & 0 & 0 \\ & & & e_1(x) & \alpha_1^{t_4}(x) & 0 & 0 & 0 & 0 & 0 \\ \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_2}(x^{-1}) & \alpha_1^{t_3}(x^{-1}) & \alpha_1^{t_4}(x^{-1}) & e_2(x) & 0 & 0 & 0 & 0 & 0 \end{array}\right),$$

donde $t_1 = 1, 3, 5, 9, 19$ y $t_2, t_3, t_4 \in T$.

Utilizando MAGMA encontramos que no existen códigos generados por la matriz gen(C) anterior con distancia mínima 20. (Ver anexos 4.0.6)

Caso 2: $k_1 = 3$ y $k_2 = 2$. Siguiendo el mismo orden de ideas que en el caso 1, tenemos que

$$\text{gen}(M_1) = \begin{pmatrix} e_1(x) & & & \alpha_1^{t_1}(x) & \alpha_1^{t_2}(x) \\ & e_1(x) & & \alpha_1^{t_3}(x) & x^{s_1}\alpha_1^{t_4}(x) \\ & & e_1(x) & \alpha_1^{t_5}(x) & x^{s_2}\alpha_1^{t_6}(x) \end{pmatrix}$$

donde $t_i \in \{1, \ldots, 89, \}i = 1, \ldots, 6$.

Aplicando la sustitución $x \to x^2$, reducimos los valores de t_2 tal que $t_2 \in \{1, 3, 5, 9, 11, 13, 19, 33\}$. Por otra parte tenemos que

$$\text{gen}(M_2) = \begin{pmatrix} \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_3}(x^{-1}) & \alpha_1^{t_5}(x^{-1}) & e_2(x) & 0 \\ \alpha_1^{t_2}(x^{-1}) & x^{23-s_1}\alpha_1^{t_4}(x^{-1}) & x^{23-s_2}\alpha_1^{t_6}(x^{-1}) & 0 & e_2(x) \end{pmatrix}$$

Por lo tanto una matriz para el código $\varphi(E_\sigma(C))$ puede ser la siguiente

$$\begin{pmatrix} e_1(x) & & & \alpha_1^{t_1}(x) & \alpha_1^{t_2}(x) \\ & e_1(x) & & \alpha_1^{t_3}(x) & x^{s_1}\alpha_1^{t_4}(x) \\ & & e_1(x) & \alpha_1^{t_5}(x) & x^{s_2}\alpha_1^{t_6}(x) \\ \alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_3}(x^{-1}) & \alpha_1^{t_5}(x^{-1}) & e_2(x) & 0 \\ \alpha_1^{t_2}(x^{-1}) & x^{23-s_1}\alpha_1^{t_4}(x^{-1}) & x^{23-s_2}\alpha_1^{t_6}(x^{-1}) & 0 & e_2(x) \end{pmatrix}$$

Consecuentemente gen(C) tiene la siguiente forma:

$$\left(\begin{array}{ccccc|ccccc}
\mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 1 \\
\hline
e_1(x) & & & \alpha_1^{t_1}(x) & \alpha_1^{t_2}(x) & 0 & 0 & 0 & 0 & 0 \\
 & e_1(x) & & \alpha_1^{t_3}(x) & x^{s_1}\alpha_1^{t_4}(x) & 0 & 0 & 0 & 0 & 0 \\
 & & e_1(x) & \alpha_1^{t_5}(x) & x^{s_2}\alpha_1^{t_6}(x) & 0 & 0 & 0 & 0 & 0 \\
\alpha_1^{t_1}(x^{-1}) & \alpha_1^{t_3}(x^{-1}) & \alpha_1^{t_5}(x^{-1}) & e_2(x) & 0 & 0 & 0 & 0 & 0 & 0 \\
\alpha_1^{t_2}(x^{-1}) & x^{23-s_1}\alpha_1^{t_4}(x^{-1}) & x^{23-s_2}\alpha_1^{t_6}(x^{-1}) & 0 & e_2(x) & 0 & 0 & 0 & 0 & 0
\end{array}\right),$$

donde $1 \leq t_1, t_3, t_4, t_5, t_6 \leq 89,\ 1 \leq s_1, s_2 \leq 23,\ t_2 \in \{1, 3, 5, 9, 11, 13, 19, 33\}$.
$e_1(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{17} + x^{15} + x^{14} + x^{11} + x^{10} + x^7 + x^5 + 1$,
$e_2(x) = x^{18} + x^{16} + x^{13} + x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1$,
$\alpha_1(x) = x^{20} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^7 + x^3 + x + 1$ y
$\alpha_1(x^{-1}) = x^{22} + x^{20} + x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^3 + 1$.

Utilizando MAGMA (Ver anexos 4.0.7) encontramos la existencia de 21 nuevos códigos generados por la última matriz gen(C) con distancia mínima 20. Los cuales tienen los parámetros registrados en la tabla 3.1.

Tabla 3.1: Nuevos códigos tipo II con parametros $[120, 60, 20]$ con un automorfismo de orden 23.

Código	t_1	t_2	t_3	s_1	t_4	t_5	s_2	t_6	A_{20}
C_1	1	1	2	0	1	5	19	12	102534
C_2	1	1	2	0	1	5	22	53	102258
C_3	1	1	2	0	1	5	20	73	101568
C_4	1	1	2	0	1	4	16	13	101430
C_5	1	1	2	0	1	4	9	66	101292
C_6	1	1	2	0	1	6	19	58	101154
C_7	1	1	2	0	1	4	20	5	101016
C_8	1	1	2	0	1	4	10	41	100878
C_9	1	1	2	0	1	5	19	26	100740
C_{10}	1	1	2	0	1	4	21	17	100602
C_{11}	1	1	2	0	1	7	20	35	100464
C_{12}	1	1	2	0	1	4	18	4	100326
C_{13}	1	1	2	0	1	6	20	47	100188
C_{14}	1	1	2	0	1	4	11	62	100050
C_{15}	1	1	2	0	1	4	3	33	99912
C_{16}	1	1	2	0	1	4	7	14	99774
C_{17}	1	1	2	0	1	4	2	16	99636
C_{18}	1	1	2	0	1	4	8	35	99498
C_{19}	1	1	2	0	1	4	14	43	99360
C_{20}	1	1	2	0	1	4	13	6	99084
C_{21}	1	1	2	0	1	4	3	22	98946

3.2.2 Automorfismos de orden 29

3.2.2 Teorema. Existen por lo menos 20 códigos autoduales doblemente pares con parámetros [120,60,20] y con un automorfismo de orden 29.

Demostración. Sea C un código autodual doblemente par con parámetros $[120, 60, 20]$ con un automorfismo σ de tipo 29-$(c; f)$. Puesto que $s(29) = 28$, el polinomio $1+x+x^2+\cdots+x^{p-1}$ es irreducible sobre $\mathbb{F}_2[x]$ y por el numeral 2 del lema 2.2.3 tenemos que $c = 2$ o $c = 4$. Usando el teorema 2.1.9, concluimos que los posibles tipos de σ son 29-(2; 62) y 29-(4; 4). Supongamos que σ es de tipo 29-$(4; 4)$. Entonces $\pi(F_\sigma(C))$ es un $[8, 4]$-código binario autodual.

Puesto que $29 - 1 \equiv 0$ mód 4, por lema 2.1.5 tenemos que $\pi(F_\sigma(C))$ es un $[8, 4]$-código binario autodual doblemente par sobre $\mathbb{F}_2$. Sabemos de [15] que $\pi(F_\sigma(C)) \sim A_8$ o $\pi(F_\sigma(C)) \sim C_2^4$, donde

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

$$\text{gen}(C_2^4) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Puesto que C_2^4 no es doblemente par tenemos que $\pi(F_\sigma(C)) \sim A_8$. Luego una posible matriz generadora de $\pi(F_\sigma(C))$ es

$$\text{gen}(\pi(F_\sigma(C))) = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right). \tag{3.9}$$

Por lo tanto una posible matriz generadora de $F_\sigma(C)$ es

$$\text{gen}(F_\sigma(C)) = \left(\begin{array}{cccc|cccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 1 & 1 & 1 & 0 \end{array}\right), \tag{3.10}$$

donde $\mathbf{1}$ es el vector de todos 1 y $\mathbf{0}$ el vector de todos 0 de longitud 29.

3.2.3 Lema. Sea $L := \{(i, j)(i + 4, j + 4) \in S_8 \mid 1 \leq i \leq 4 \text{ y } 1 \leq j \leq 4\}$. Entonces $L \subseteq \text{Aut}(\pi(F_\sigma(C)))$.

Demostración. Debido a la simetria de la matriz en (3.9) tenemos que si v es una fila de (3.9) y si $\rho \in L$, entonces $\rho(v)$ es también una fila de (3.9). ∎

Por lo tanto tenemos los siguiente

3.2.4 Corolario. Sea $\text{gen}(C) = \left(\begin{array}{c|c} X & Y \\ \hline Z & O \end{array}\right)$ y $\text{gen}(C') = \left(\begin{array}{c|c} X & Y \\ \hline \xi(Z) & O \end{array}\right)$, donde $(X \mid Y)$ es la matriz en (3.10), O es la matriz cero de tamaño apropiado, $(Z \mid O) = \text{gen}(E_\sigma(C))$ y $\xi \in S_4$ una permutación de los 29-ciclos. Entonces $C \sim C'$.

Puesto que $s(29) = 28$ sabemos por teorema 2.2.9 que $\varphi(E_\sigma(C)^*)$ es un $[4, 2]$-código autodual sobre el campo $P = \langle x+1\rangle \subseteq \mathbb{F}_2[x]/\langle x^{29}-1\rangle$ con el producto escalar

$$u \cdot v = u_1 v_1^{2^{14}} + u_2 v_2^{2^{14}} + u_3 v_3^{2^{14}} + u_4 v_4^{2^{14}}. \tag{3.11}$$

3.2.5 Lema. Si la matriz generadora de $F_\sigma(C)$ es como en (3.10), entonces $\varphi(E_\sigma(C)^*)$ es un $[4, 2, 3]$-código autodual sobre $P \cong \mathbb{F}_{2^{28}}$.

Demostración. $\varphi(E_\sigma(C)^*)$ puede tener distancia minimal 1, 2 o 3 en P.

(1) $\varphi(E_\sigma(C)^*)$ no puede tener un vector de peso 1.

Sea $v \in \varphi(E_\sigma(C)^*)$ con $\text{wt}(v) = 1$. Según el corolario 3.2.4 podemos asumir que $v = (v_1, 0, 0, 0)$ con $v_1 \in P\backslash\{0\}$. Si multiplicamos v por $(x+1)v_1^{-1}$ entonces $v = (x+1, 0, 0, 0)$. Lo cual es una contradicción puesto que $\text{wt}(\varphi^{-1}(v)) = 2 < 20$.

(2) $\varphi(E_\sigma(C)^*)$ no puede tener un vector de peso 2.

Sea $v \in \varphi(E_\sigma(C)^*)$ con $\text{wt}(v) = 2$. Por el corolario 3.2.4 podemos asumir que $v = (v_1, v_2, 0, 0)$ con $v_1, v_2 \in P\backslash\{0\}$.

Sea M el espacio vectorial sobre P generado por v, es decir $M := \{(uv_1, uv_2, 0, 0) \mid u \in P\}$ y $\dim_{\mathbb{F}_2} M = 28$.

$W := \varphi^{-1}(M) \subseteq E_\sigma(C)^*$ es un código sobre el campo $\mathbb{F}_2$ con $\dim_{\mathbb{F}_2}(W) = 28$. Puesto que

$$20 = d(C) \leq d(E_\sigma(C)) = d(E_\sigma(C)^*) \leq d(W),$$

W es un $[116, 28, d']$-código sobre $\mathbb{F}_2$ con $d' \geq 20$.

Sea $W^* \subseteq \mathbb{F}_2^{58}$ el código obtenido de W eliminando las últimas 58 coordenadas. Entonces W^* es un código $[58, 28, d'']$ con $d'' = d' \geq 20$. Por consiguiente

$$\left\lceil (\frac{d''}{2^0}) \right\rceil + \left\lceil (\frac{d''}{2^1}) \right\rceil + \cdots + \left\lceil (\frac{d''}{2^{27}}) \right\rceil \geq$$

$$\left\lceil \frac{20}{1} \right\rceil + \left\lceil \frac{20}{2} \right\rceil + \left\lceil \frac{20}{4} \right\rceil + \left\lceil \frac{20}{8} \right\rceil + \left\lceil \frac{20}{16} \right\rceil + \left\lceil \frac{20}{32} \right\rceil + \cdots + \left\lceil \frac{20}{2^{27}} \right\rceil =$$
$$20 + 10 + 5 + 3 + 2 + (22 + 1)1 = 63 > 58,$$

lo cual contradice la cota de Griesmer (lema 1.1.7).

Por lo tanto $\varphi(E_\sigma(C)^*)$ es un $[4, 2, 3]$-código autodual sobre P con el producto escalar

$$v \cdot u = v_1 u_1^{2^{14}} + \ldots + v_4 u_4^{2^{14}},\ \forall v, u \in \varphi(E_\sigma(C)^*).$$

Note que $\varphi(E_\sigma(C)^*)$ es un MDS-código. Así que en la matriz generadora de $\varphi(E_\sigma(C)^*)$ cualquier dos columnas son linealmente independiente. Claramente, podemos elegir

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \alpha^{t_1} & 0 & \alpha^{t_3} & \alpha^{t_5} \\ 0 & \alpha^{t_2} & \alpha^{t_4} & \alpha^{t_6} \end{pmatrix},$$

donde α es un elemento primitivo de P y $0 \leq t_i \leq 2^{28} - 2$.

Por lo tanto sabemos que $2^{28} - 1 = (2^{14} + 1)(2^{14} - 1)$. Sea $\phi = \alpha^{2^{14}+1}$ y $\delta = \alpha^{2^{14}-1}$. Entonces $\mathrm{ord}(\phi) = 2^{14} - 1 = 3 \times 43 \times 127$ y $\mathrm{ord}(\delta) = 2^{14} + 1 = 5 \times 29 \times 113$. Puesto que $\gcd(\mathrm{ord}(\phi), \mathrm{ord}(\delta)) = 1$, tenemos que

$$\mathrm{ord}(\phi\delta) = \mathrm{ord}(\phi) \cdot \mathrm{ord}(\delta) = 2^{28} - 1 = \mathrm{ord}(\alpha).$$

por lo tanto $\phi\delta$ es también un elemento primitivo de P. Así pues

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} (\phi\delta)^{i_1} & 0 & (\phi\delta)^{i_3} & (\phi\delta)^{i_5} \\ 0 & (\phi\delta)^{i_2} & (\phi\delta)^{i_4} & (\phi\delta)^{i_6} \end{pmatrix},$$

donde $0 \leq i_1, i_2, i_3, i_4, i_5, i_6 \leq 2^{28} - 2$. Si multiplicamos la primera fila por $\delta^{-i_3}\phi^{-i_1}$ y la segunda por $\delta^{-i_4}\phi^{-i_2}$ obtenemos

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \delta^{s_1} & 0 & \phi^{t_1} & \phi^{t_2}\delta^{s_2} \\ 0 & \delta^{s_3} & \phi^{t_3} & \phi^{t_4}\delta^{s_4} \end{pmatrix}, \tag{3.12}$$

donde $0 \leq s_1, s_2, s_3, s_4 \leq 2^{14},\ 0 \leq t_1, t_2, t_3, t_4 \leq 2^{14} - 2$.

Por el lema 2.2.12 podemos tomar como un transversal de $\langle\beta(x)\rangle$ en $\langle\delta(x)\rangle$ el conjunto $\{e(x), \delta(x), \ldots, \delta(x)^{(5\times13)-1}\}$. Por Lema 2.1.8 tenemos que $x^t e(x) \equiv \beta(x)^t \mathrm{mód}(x^{29} - 1)$, para $0 \leq t \leq 28$ y puesto que la multiplicación de la segunda coordenada de $\varphi(E_\sigma(C)^*)$ por x^t conduce a códigos equivalentes entonces podemos asumir que

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \delta^{l_1} & 0 & \phi^{t_1} & \phi^{t_2}\delta^{l_2} \\ 0 & \delta^{l_3} & \phi^{t_3} & \phi^{t_4}\delta^{s_5} \end{pmatrix}, \tag{3.13}$$

donde $0 \leq l_1, l_2, l_3 \leq (5 \times 113) - 1,\ 0 \leq t_1, t_2, t_3, t_4 \leq 2^{14} - 2$ y $0 \leq s_5 \leq 2^{14}$.

De la misma manera como en [20] debido a la ortogonalidad de las filas de la matriz (3.13), con respecto al producto escalar (3.11), obtenemos

$$\mathrm{gen}(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} \delta^{l_1} & 0 & \phi^{t_1} & \phi^{t_2}\delta^{l_2} \\ 0 & \delta^{l_3} & \phi^{t_3} & \phi^{t_4}\delta^{l_2} \end{pmatrix}, \tag{3.14}$$

donde $0 \leq l_1, l_2, l_3 \leq (5 \times 113) - 1,\ 0 \leq t_1, t_2, t_3, t_4 \leq 2^{14} - 2$ con

$$t_4 - t_3 \equiv t_1 - t_2 \bmod (2^{14} - 1). \tag{3.15}$$

Por otra parte, multiplicando cada fila de (3.14) por si misma, obtenemos

$$(\delta^{l_1}, 0, \phi^{t_1}, (\phi^{t_2}\delta^{l_2})) \cdot (\delta^{l_1}, 0, \phi^{t_1}, (\phi^{t_2}\delta^{l_2})) = \delta^{(2^{14}+1)l_1} + \phi^{(2^{14}+1)t_1} + (\phi^{(2^{14}+1)t_2}\delta^{(2^{14}+1)l_2}) = 0.$$

Puesto que $\delta^{(2^{14}+1)} = e$, $\phi^{(2^{14}+1)t_1} + \phi^{(2^{14}+1)t_2} = e$, y como $\phi^{(2^{14}+1)} = \phi^2$ obtenemos

$$\phi^{2t_1} + \phi^{2t_2} = e.$$

Ahora $(\phi^{t_1} + \phi^{t_2})^2 = \phi^{2t_1} + \phi^{2t_2}$ implica

$$\phi^{t_1} + \phi^{t_2} = e. \tag{3.16}$$

De la misma manera obtenemos

$$\phi^{t_3} + \phi^{t_4} = e. \tag{3.17}$$

Calculamos con MAGMA las parejas (t_1, t_2), (t_3, t_4) que satisfacen las condiciones (3.16). y (3.17). Si M es el conjunto que contiene las parejas $(t_1, t_2), (t_3, t_4)$, Entonces $|M| = 8192$. Validando las dos condiciones anteriores encontramos que $t_1 = t_4$ y $t_2 = t_3$. Por lo tanto tenemos que

$$\varphi(E_\sigma(C)^*) = \begin{pmatrix} \delta^{l_1} & 0 & \phi^{t_1} & \phi^{t_2}\delta^{l_2} \\ 0 & \delta^{l_3} & \phi^{t_2} & \phi^{t_1}\delta^{l_2} \end{pmatrix},$$

donde $0 \leq l_1, l_2, l_3 \leq (5 \times 113) - 1$ y $\{t_1, t_2\} \in M$. Mediante la sustitución $x \to x^2$ obtenemos códigos equivalentes por la operación $(l_1, l_2, l_3, t_1, t_2) \to (2l_1, 2l_2, 2l_3, 2t_1, 2t_2)$. La operación $(t_1, t_2) \to (2t_1, 2t_2)$ divide el conjunto M en orbitas. Estas orbitas son

$$O(t_1, t_2) = \{(t_1 2^n \bmod (2^{14} - 1),\ t_2 2^n \bmod (2^{14} - 1)) \mid n \in \mathbb{Z}\}.$$

Sea M' un sistema de representantes. Encontramos que $|M'| = 595$.

Por otro lado se puede comprobar facilmente con MAGMA que $\alpha(x) = x^{13} + x^{12} + x^6 + x^5 + x^4 + x^2$ es un elemento primitivo de P.

Finalmente, una posible matriz generadora de un código binario autodual doblemente par con parametros $[120, 60, 20]$ con un automorfismo de orden 29 es:

$$\mathrm{gen}(C) = \left(\begin{array}{cccc|cccc} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 1 & 1 & 1 & 0 \\ \hline [\delta^{l_1}] & [\,0\,] & [\phi^{t_1}] & [\phi^{t_2}\delta^{l_2}] & 0 & 0 & 0 & 0 \\ [\,0\,] & [\delta^{l_3}] & [\phi^{t_2}] & [\phi^{t_1}\delta^{l_2}] & 0 & 0 & 0 & 0 \end{array}\right), \tag{3.18}$$

donde $\mathbf{1}$ es el vector de todos 1 y $\mathbf{0}$ es el vector de todos 0 de longitud 29, $\alpha = x^{13} + x^{12} + x^6 + x^5 + x^4 + x^2$ es un elemento primitivo del campo P, $\phi = \alpha^{2^{14}+1}$, $\delta = \alpha^{2^{14}-1}$, $0 \leq l_1, l_2, l_3 \leq (5 \times 113) - 1$ y $\{t_1, t_2\} \in M'$ con $|M'| = 595$.

Usando la construcción de la matriz (3.18) y haciendo una búsqueda exhaustiva con MAGMA encontramos 20 nuevos códigos no equivalentes autoduales doblemente pares con parametros $[120, 60, 20]$, todos con un automorfismo de orden 29 (ver tabla 3.2). ∎

Tabla 3.2: Nuevos códigos tipo II con parametros $[120, 60, 20]$ con un automorfismo de orden 29.

l_1	l_2	l_3	t_1	t_2	A_{20}
342	565	4	4510	13312	96744
21	120	120	9117	11766	97788
342	4	342	4510	13312	97962
200	565	342	3921	16257	98136
200	4	342	3921	16257	98310
342	200	1	4510	13312	98832
29	11	565	9117	11766	99702
23	565	1	5469	9024	100050
29	24	11	12859	13349	100224
29	21	565	12859	13349	100398
11	565	120	12859	13349	100572
200	342	565	5469	9024	100920
55	33	2	4457	7488	101094
120	24	565	1379	6536	101268
323	16	123	9306	13071	101442
120	29	565	1105	12212	101616
1	23	565	4503	11151	102834
565	4	23	4503	11151	103530
342	1	23	5469	9024	103878
1	200	5	4510	13312	102138

Capítulo 4

Anexos

4.0.3 Rutina en MAGMA para códigos [40,20,8] con automorfismos de orden 19

Mediante esta rutina se forman las matrices generadoras de los tres códigos C autoduales, doblemente pares y extremales, no equivalentes salvo isomorfías, con un automorfismo de orden 19.

```
R<x>:=PolynomialRing(GF(2));
z:=R ! x^(19)-1;
I:=ideal<R | z>;
U<x>:=quo<R | I>; b:=U ! 1+x+x^(3)+x^(6);
V19:=VectorSpace(GF(2),19);

function potvec(p)
    v:=Zero(V19);
    while p ne 0 do v[Degree(p)+1]:=1;
                    p:=p-x^Degree(p);
    end while;
    return v;
end function;

e:= x;
for i:=2 to 18 do
    e:=e+x^i;
end for;
```

```
function Ct(t)
G:=Matrix( GF(2),20,40,[]);
for i:=1 to 19 do
    G[1,i]:=1;  G[1,19+i]:=0;
    G[2,i]:=0;  G[2,19+i]:=1;
end for;

G[1,39]:=0; G[1,40]:=1;
G[2,39]:=1; G[2,40]:=0;
vbt:=b^t; ve:=e;

for i:=3 to 20 do
    for j:=1 to 19 do
        vece:=potvec(ve);
        vecbt:=potvec(vbt);
        G[i,j]:= vece[j]; G[i,19+j]:=vecbt[j];
    end for;
    ve:=x*ve;
    vbt:=x*vbt;
end for;

C:=LinearCode(G);
return C;
end function;

C0:=Ct(2^((18)-1)); C1:=Ct(1); C3:=Ct(3); C9:=Ct(9);

w0:=MinimumWeight(C0);
w1:=MinimumWeight(C1);
w3:=MinimumWeight(C3);
w9:=MinimumWeight(C9);
w0; w1; w3; w9;

IsSelfDual(C1); IsDoublyEven(C1); WeightDistribution(C1);

IsEquivalent(C1,C2);
IsEquivalent(C1,C3);
IsEquivalent(C2,C3);
```

4.0.4 Matrices generadoras de los 9 [24,12]-códigos binarios autoduales doblemente pares.

Las siguientes son las matrices generadoras de los 9 [24,12]-códigos binarios autoduales doblemente pares de la tabla 3.5.

$$A_{24} := d_{12}^2/ab/ba$$

$$\left(\begin{array}{cccccccccccc|cccccccccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
\hline
0&1&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1&1\\
\hline
0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1
\end{array}\right)$$

$$B_{24} := d_{10}/e_7^2/bcc/a0c$$

$$\left(\begin{array}{cccccccccc|cccccccc|ccccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1\\
\hline
0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0\\
0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0
\end{array}\right)$$

$$C_{24} := d_8^3/abb/bab/bba$$

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

$$D_{24} := d_6^4/baa0/0baa/a0ba/aa0b$$

$$\left(\begin{array}{cccccc|cccccc|cccccc|cccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
\hline
0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0\\
\hline
0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&1\\
\hline
0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&1\\
\hline
0&1&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1&1
\end{array}\right)$$

$$E_{24} := d_{24}/a$$

$$\left(\begin{array}{cccccccccccccccccccccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1\\
\hline
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1
\end{array}\right)$$

$$F_{24} := d_4^6 b0a^3 0/0ba^3/a0b0a^2/a^2 0b0a/a^3 0b0/0a^3 0b$$

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

$G_{24} :=$ Golay code
Definición 1.2.8

$$H_{24} := d_{16}e_8/a0$$

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

$$I_{24} := e_8^3$$

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

4.0.5 Rutina en MAGMA para códigos [40,20,8] con automorfismos de orden 5

Mediante esta rutina se forman dos matrices generadoras de códigos C_1 y C_2 autoduales, doblemente pares y extremales, con un automorfismo de orden 5, comprobando que C_1 y C_2 son equivalentes.

```
G:=Matrix( GF(2),20,40,[]);
for i:=1 to 11 do
   for j:=1 to 5 do
     G[i,j]:=1;      G[1,j+5]:=1;    G[2,j+10]:=1;
     G[3,j+15]:=1; G[12,j+30]:=1; G[12,j+35]:=1;
   end for;
end for;

for i:=1 to 2 do
   for j:=1 to 3 do
      G[1,29+i]:=1;  G[1,32+j]:=1; G[1,39]:=1;
      G[2,30+i]:=1;  G[2,33+j]:=1; G[2,40]:=1;
      G[3,30]:=1;    G[3,31+i]:=1; G[3,34+j]:=1;
      G[4,21]:=1;    G[4,31]:=1;   G[4,32+i]:=1;
      G[4,35+j]:=1;  G[5,22]:=1;   G[5,32]:=1;
      G[5,33+i]:=1;  G[5,36+j]:=1; G[6,23]:=1;
      G[6,33]:=1;    G[6,34+i]:=1; G[6,37+j]:=1;
      G[7,24]:=1;    G[7,30]:=1;   G[7,34]:=1;
      G[7,35+i]:=1;  G[7,38+i]:=1; G[8,25]:=1;
      G[8,29+i]:=1;  G[8,35]:=1;   G[8,36+i]:=1;
```

```
      G[8,40]:=1;     G[9,26]:=1;     G[9,29+j]:=1;
      G[9,36]:=1;     G[9,37+i]:=1;   G[10,27]:=1;
      G[10,30+j]:=1;  G[10,37]:=1;    G[10,38+i]:=1;
      G[11,28]:=1;    G[11,30]:=1;    G[11,31+j]:=1;
      G[11,38]:=1;    G[11,40]:=1;    G[12,28+i]:=1;
   end for;
end for;

for i:=1 to 2 do
   for j:=1 to 3 do
      for k:=1 to 4 do
         G[13,1+k]:=1;   G[13,12]:=1;    G[13,15]:=1;
         G[13,17+i]:=1;  G[14,1]:=1;     G[14,2+j]:=1;
         G[14,11]:=1;    G[14,13]:=1;    G[14,18+i]:=1;
         G[15,i]:=1;     G[15,3+i]:=1;   G[15,12]:=1;
         G[15,14]:=1;    G[15,16]:=1;    G[15,20]:=1;
         G[16,j]:=1;     G[16,5]:=1;     G[16,13]:=1;
         G[16,14+j]:=1;  G[17,6+k]:=1;   G[17,12+i]:=1;
         G[17,17]:=1;    G[17,20]:=1;    G[18,6]:=1;
         G[18,7+j]:=1;   G[18,13+j]:=1;  G[18,18]:=1;
         G[19,5+i]:=1;   G[19,8+j]:=1;   G[19,15]:=1;
         G[19,17]:=1;    G[19,19]:=1;    G[20,5+j]:=1;
         G[20,9+j]:=1;   G[20,18]:=1;    G[20,20]:=1;
      end for;
   end for;
end for;

M:=Matrix( GF(2),20,40,[]);
for i:=1 to 11 do
   for j:=1 to 5 do
      M[i,j]:=1;   M[1,j+5]:=1;  M[2,j+10]:=1;
      M[3,j+15]:=1;  M[12,j+30]:=1;  M[12,j+35]:=1;
   end for;
end for;

for i:=1 to 2 do
   for j:=1 to 3 do
      M[1,29+i]:=1;   M[1,32+j]:=1;  M[1,39]:=1;
      M[2,30+i]:=1;   M[2,33+j]:=1;  M[2,40]:=1;
```

```
        M[3,30]:=1;     M[3,31+i]:=1; M[3,34+j]:=1;
        M[4,21]:=1;     M[4,31]:=1;   M[4,32+i]:=1;
        M[4,35+j]:=1;   M[5,22]:=1;   M[5,32]:=1;
        M[5,33+i]:=1;   M[5,36+j]:=1; M[6,23]:=1;
        M[6,33]:=1;     M[6,34+i]:=1; M[6,37+j]:=1;
        M[7,24]:=1;     M[7,30]:=1;   M[7,34]:=1;
        M[7,35+i]:=1;   M[7,38+i]:=1; M[8,25]:=1;
        M[8,29+i]:=1;   M[8,35]:=1;   M[8,36+i]:=1;
        M[8,40]:=1;     M[9,26]:=1;   M[9,29+j]:=1;
        M[9,36]:=1;     M[9,37+i]:=1; M[10,27]:=1;
        M[10,30+j]:=1; M[10,37]:=1;   M[10,38+i]:=1;
        M[11,28]:=1;    M[11,30]:=1;  M[11,31+j]:=1;
        M[11,38]:=1;    M[11,40]:=1;  M[12,28+i]:=1;
    end for;
end for;

for i:=1 to 2 do
    for j:=1 to 3 do
        for k:=1 to 4 do
            M[13,1+k]:=1;  M[13,12+i]:=1; M[13,17]:=1;
            M[13,20]:=1;   M[14,1]:=1;    M[14,2+j]:=1;
            M[14,13+j]:=1; M[14,18]:=1;   M[15,i]:=1;
            M[15,3+i]:=1;  M[15,11]:=1;   M[15,15]:=1;
            M[15,17]:=1;   M[15,19]:=1;   M[16,j]:=1;
            M[16,5]:=1;    M[16,10+i]:=1; M[16,18]:=1;
            M[16,20]:=1;   M[17,6+k]:=1;  M[17,12]:=1;
            M[17,15]:=1;   M[17,17+i]:=1; M[18,6]:=1;
            M[18,7+k]:=1;  M[18,13]:=1;   M[18,18+i]:=1;
            M[19,5+i]:=1;  M[19,8+i]:=1;  M[19,12]:=1;
            M[19,14]:=1;   M[19,16]:=1;   M[19,20]:=1;
            M[20,5+j]:=1;  M[20,10]:=1;   M[20,13]:=1;
            M[20,14+j]:=1;
        end for;
    end for;
end for;

C1:=LinearCode(G);
w1:=MinimumWeight(C1);
w1;
```

```
IsSelfDual(C1);
IsDoublyEven(C1);
WeightDistribution(C1);

C2:=LinearCode(M);
w2:=MinimumWeight(C2);
w2;
IsSelfDual(C2);
IsDoublyEven(C2);
WeightDistribution(C2);

IsEquivalent(C1,C2);
```

4.0.6 Rutina 1 en MAGMA para códigos [120,60,20]

Mediante esta rutina se crean las matrices generadoras de los códigos C autoduales y doblemente pares con un automorfismo del tipo 23-(5;5), para los cuales $k_1 = \dim_{I_1}(M_1) = 4$ y $k_2 = \dim_{I_2}(M_2) = 1$. Además se exploran los valores $t_i,\ i = 1,2,3,4$, tal que $\mathrm{w}(C) = 20$.

```
R<x>:=PolynomialRing(GF(2)); z:=R ! x^(23)-1;

I:=ideal<R | z>; U<x>:=quo<R | I>;

b:=U ! x^(20)+x^(17)+x^(15)+x^(14)+x^(13)+x^(12)+x^(11)+
x^(10)+ x^(7)+x^(3)+x+1;
B:= U ! x^(22)+x^(20)+x^(16)+x^(13)+x^(12)+x^(11)+x^(10)+
x^(9)+x^(8)+x^(6)+x^(3)+1;
e1:= U ! x^(22)+x^(21)+x^(20)+x^(19)+x^(17)+x^(15)+x^(14)+
x^(11)+x^(10)+x^(7)+x^(5)+1;
e2:= U ! x^(18)+x^(16)+x^(13)+x^(12)+x^(9)+x^(8)+x^(6)+
x^(4)+x^(3)+x^(2)+x+1;
V23:=VectorSpace(GF(2),23);
function potvec(p)
    v:=Zero(V23);
    while p ne 0 do v[Degree(p)+1]:=1; p:=p-x^Degree(p);
    end while;
    return v;
end function;
```

```
function Ct(t1,t2,t3,t4)
   G:=Matrix(GF(2),60,120,[]);
      for i:=1 to 23 do
         G[1,i]:=1;    G[1,116]:=1;  G[2,23+i]:=1;
         G[2,117]:=1;  G[3,46+i]:=1; G[3,118]:=1;
         G[4,69+i]:=1; G[4,119]:=1;  G[5,92+i]:=1;
         G[5,120]:=1;
      end for;
ve1:=e1; ve2:=e2; vbt1:=b^(t1); vbt2:=b^(t2); vbt3:=b^(t3);
vbt4:=b^(t4);     vBt1:=B^(t1); vBt2:=B^(t2); vBt3:=B^(t3);
vBt4:=B^(t4);

for i:=6 to 16 do
   for j:=1 to 23 do
      vece1:= potvec(ve1);  vece2:= potvec(ve2);
      vecbt1:=potvec(vbt1); vecbt2:=potvec(vbt2);
      vecbt3:=potvec(vbt3); vecbt4:=potvec(vbt4);
      vecBt1:=potvec(vBt1); vecBt2:=potvec(vBt2);
      vecBt3:=potvec(vBt3); vecBt4:=potvec(vBt4);
      G[i,j]:=vece1[j];        G[i+11,j+23]:=vece1[j];
      G[i+22,j+46]:=vece1[j];  G[i+33,j+69]:=vece1[j];
      G[i+44,j+92]:=vece2[j];  G[i,j+92]:=vecbt1[j];
      G[i+11,j+92]:=vecbt2[j]; G[i+22,j+92]:=vecbt3[j];
      G[i+33,j+92]:=vecbt4[j]; G[i+44,j]:=vecBt1[j];
      G[i+44,j+23]:=vecBt2[j]; G[i+44,j+46]:=vecBt3[j];
      G[i+44,j+69]:=vecBt4[j];
   end for;
     ve1:=x*(ve1);   ve2:=x*(ve2);   vbt1:=x*(vbt1);
     vbt2:=x*(vbt2); vbt3:=x*(vbt3); vbt4:=x*(vbt4);
     vBt1:=x*(vBt1); vBt2:=x*(vBt2); vBt3:=x*(vBt3);
     vBt4:=x*(vBt4);
end for;
C:=LinearCode(G);
return C;
end function;

L1:=[1..5]; L2:=[9..10]; L3:=[18..19]; M1:=[1..10];
M2:=[12..21]; M3:=[23..29]; M4:=[32..40]; M5:=[42..49];
M6:=[53..59]; M7:=[63..69]; M8:=[71..80]; M9:=[84..89];
```

```
A1:={<t1 , t2 , t3 , t4 >: t1 in L1, t2 in M1, t3 in M1,
t4 in M1| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A1;

A2:={<t1 , t2 , t3 , t4 >: t1 in L2, t2 in M1, t3 in M1,
t4 in M1| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A2;

A3:={<t1 , t2 , t3 , t4 >: t1 in L3, t2 in M1, t3 in M1,
t4 in M1| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A3;

A4:={<t1 , t2 , t3 , t4 >: t1 in L1, t2 in M2, t3 in M2,
t4 in M2| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A4;

A5:={<t1 , t2 , t3 , t4 >: t1 in L2, t2 in M2, t3 in M2,
t4 in M2| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A5;

A6:={<t1 , t2 , t3 , t4 >: t1 in L3, t2 in M2, t3 in M2,
t4 in M2| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A6;

A7:={<t1 , t2 , t3 , t4 >: t1 in L1, t2 in M3, t3 in M3,
t4 in M3| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A7;

A8:={<t1 , t2 , t3 , t4 >: t1 in L2, t2 in M3, t3 in M3,
t4 in M3| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A8;

A9:={<t1 , t2 , t3 , t4 >: t1 in L3, t2 in M3, t3 in M3,
t4 in M3| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
A9;

A10:={<t1 , t2 , t3 , t4 >: t1 in L1, t2 in M4, t3 in M4,
t4 in M4| MinimumWeight( Ct(t1 , t2 , t3 , t4 )) eq 20};
```

A10;

$$A11:=\{<t1,t2,t3,t4>:\ t1\ in\ L2,\ t2\ in\ M4,\ t3\ in\ M4,\ t4\ in\ M4 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A11;

$$A12:=\{<t1,t2,t3,t4>:\ t1\ in\ L3,\ t2\ in\ M4,\ t3\ in\ M4,\ t4\ in\ M4 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A12;

$$A13:=\{<t1,t2,t3,t4>:\ t1\ in\ L1,\ t2\ in\ M5,\ t3\ in\ M5,\ t4\ in\ M5 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A13;

$$A14:=\{<t1,t2,t3,t4>:\ t1\ in\ L2,\ t2\ in\ M5,\ t3\ in\ M5,\ t4\ in\ M5 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A14;

$$A15:=\{<t1,t2,t3,t4>:\ t1\ in\ L3,\ t2\ in\ M5,\ t3\ in\ M5,\ t4\ in\ M5 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A15;

$$A16:=\{<t1,t2,t3,t4>:\ t1\ in\ L1,\ t2\ in\ M6,\ t3\ in\ M6,\ t4\ in\ M6 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A16;

$$A17:=\{<t1,t2,t3,t4>:\ t1\ in\ L2,\ t2\ in\ M6,\ t3\ in\ M6,\ t4\ in\ M6 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A17;

$$A18:=\{<t1,t2,t3,t4>:\ t1\ in\ L3,\ t2\ in\ M6,\ t3\ in\ M6,\ t4\ in\ M6 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A18;

$$A19:=\{<t1,t2,t3,t4>:\ t1\ in\ L1,\ t2\ in\ M7,\ t3\ in\ M7,\ t4\ in\ M7 \mid MinimumWeight(Ct(t1,t2,t3,t4))\ eq\ 20\};$$
A19;

$$A20:=\{<t1,t2,t3,t4>:\ t1\ in\ L2,\ t2\ in\ M7,\ t3\ in\ M7,$$

```
t4 in M7| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A20;

A21:={<t1,t2,t3,t4>: t1 in L3, t2 in M7, t3 in M7,
t4 in M7| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A21;

A22:={<t1,t2,t3,t4>: t1 in L1, t2 in M8, t3 in M8,
t4 in M8| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A22;

A23:={<t1,t2,t3,t4>: t1 in L2, t2 in M8, t3 in M8,
t4 in M8| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A23;

A24:={<t1,t2,t3,t4>: t1 in L3, t2 in M8, t3 in M8,
t4 in M8| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A24;

A25:={<t1,t2,t3,t4>: t1 in L1, t2 in M9, t3 in M9,
t4 in M9| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A25;

A26:={<t1,t2,t3,t4>: t1 in L2, t2 in M9, t3 in M9,
t4 in M9| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A26;

A27:={<t1,t2,t3,t4>: t1 in L3, t2 in M9, t3 in M9,
t4 in M9| MinimumWeight(Ct(t1,t2,t3,t4)) eq 20};
A27;
```

4.0.7 Rutina 2 en MAGMA para códigos [120,60,20]

Mediante esta rutina se crean las matrices generadoras de los códigos C autoduales y doblemente pares con un automorfismo del tipo 23-(5;5), para los cuales $k_1 = \dim_{I_1}(M_1) = 3$ y $k_2 = \dim_{I_2}(M_2) = 2$. Además se registran los valores de los parametros $t_i,\ i = 1, \cdots, 6$ y $s_j,\ j = 1, 2$, para 21 códigos que poseen $\mathrm{w}(C) = 20$.

```
R<x>:=PolynomialRing(GF(2)); z:=R ! x^(23)-1;
```

```
I:=ideal<R | z>; U<x>:=quo<R | I>;
b:=U ! x^(20)+x^(17)+x^(15)+x^(14)+x^(13)+x^(12)+x^(11)+
x^(10)+ x^(7)+x^(3)+x+1;
B:= U ! x^(22)+x^(20)+x^(16)+x^(13)+x^(12)+x^(11)+x^(10)+
x^(9)+x^(8)+x^(6)+x^(3)+1;
e1:= U ! x^(22)+x^(21)+x^(20)+x^(19)+x^(17)+x^(15)+ x^(14)+
x^(11)+x^(10)+x^(7)+x^(5)+1;
e2:= U ! x^(18)+x^(16)+x^(13)+x^(12)+x^(9)+x^(8)+ x^(6)+
x^(4)+x^(3)+x^(2)+x+1;

V23:=VectorSpace(GF(2),23);
function potvec(p)
    v:=Zero(V23);
    while p ne 0 do v[Degree(p)+1]:=1; p:=p-x^Degree(p);
    end while;
    return v;
end function;

function Ct(t1,t2,t3,s1,t4,t5,s2,t6)
G:=Matrix(GF(2),60,120,[]);
for i:=1 to 23 do
  G[1,i]:=1;    G[1,116]:=1;  G[2,23+i]:=1;
  G[2,117]:=1;  G[3,46+i]:=1; G[3,118]:=1;
  G[4,69+i]:=1; G[4,119]:=1;  G[5,92+i]:=1;
  G[5,120]:=1;
end for;

ve1:=e1; ve2:=e2; vbt1:=b^(t1); vbt2:=b^(t2);
vbt3:=b^(t3); vbt4:=(x^(s1))*b^(t4);
vbt5:=b^(t5); vbt6:=(x^(s2))*b^(t6); vBt1:=B^(t1);
vBt2:=B^(t2); vBt3:=B^(t3); vBt4:=(x^(23-s1))*B^(t4);
vBt5:=B^(t5); vBt6:=(x^(23-s2))*(B^(t6));

for i:=6 to 16 do
   for j:=1 to 23 do
      vece1:= potvec(ve1);  vece2:= potvec(ve2);
      vecbt1:=potvec(vbt1); vecbt2:=potvec(vbt2);
      vecbt3:=potvec(vbt3); vecbt4:=potvec(vbt4);
      vecbt5:=potvec(vbt5); vecbt6:=potvec(vbt6);
```

```
        vecBt1:=potvec(vBt1); vecBt2:=potvec(vBt2);
        vecBt3:=potvec(vBt3); vecBt4:=potvec(vBt4);
        vecBt5:=potvec(vBt5); vecBt6:=potvec(vBt6);

        G[i,j]:=vece1[j];          G[i+11,j+23]:=vece1[j];
        G[i+22,j+46]:=vece1[j];    G[i+33,j+69]:=vece2[j];
        G[i+44,j+92]:=vece2[j];    G[i,j+69]:=vecbt1[j];
        G[i,j+92]:=vecbt2[j];      G[i+11,j+69]:=vecbt3[j];
        G[i+11,j+92]:=vecbt4[j];   G[i+22,j+69]:=vecbt5[j];
        G[i+22,j+92]:=vecbt6[j];   G[i+33,j]:=vecBt1[j];
        G[i+33,j+23]:=vecBt3[j];   G[i+33,j+46]:=vecBt5[j];
        G[i+44,j]:=vecBt2[j];      G[i+44,j+23]:=vecBt4[j];
        G[i+44,j+46]:=vecBt6[j];

    end for;
        ve1:=x*(ve1); ve2:=x*(ve2);       vbt1:=x*(vbt1);
        vbt2:=x*(vbt2); vbt3:=x*(vbt3); vbt4:=x*(vbt4);
        vbt5:=x*(vbt5); vbt6:=x*(vbt6); vBt1:=x*(vBt1);
        vBt2:=x*(vBt2); vBt3:=x*(vBt3); vBt4:=x*(vBt4);
        vBt5:=x*(vBt5); vBt6:=x*(vBt6);
end for;

C:=LinearCode(G);
return C;
end function;

C1:=Ct(1,1,2,0,1,5,19,12);   C2:=Ct(1,1,2,0,1,5,22,53);
C3:=Ct(1,1,2,0,1,6,18,37);   C4:=Ct(1,1,2,0,1,5,20,73);
C5:=Ct(1,1,2,0,1,4,16,13);   C6:=Ct(1,1,2,0,1,4,9,66);
C7:=Ct(1,1,2,0,1,6,21,84);   C8:=Ct(1,1,2,0,1,6,19,58);
C9:=Ct(1,1,2,0,1,5,20,79);   C10:=Ct(1,1,2,0,1,6,19,35);
C11:=Ct(1,1,2,0,1,4,20,5);   C12:=Ct(1,1,2,0,1,4,10,41);
C13:=Ct(1,1,2,0,1,5,19,26); C14:=Ct(1,1,2,0,1,4,21,17);
C15:=Ct(1,1,2,0,1,7,20,35); C16:=Ct(1,1,2,0,1,4,18,4);
C17:=Ct(1,1,2,0,1,6,20,47); C18:=Ct(1,1,2,0,1,4,11,62);
C19:=Ct(1,1,2,0,1,4,3,33);   C20:=Ct(1,1,2,0,1,4,7,14);
C21:=Ct(1,1,2,0,1,4,2,16);   C22:=Ct(1,1,2,0,1,4,8,35);
C23:=Ct(1,1,2,0,1,4,14,43); C24:=Ct(1,1,2,0,1,4,13,6);
C25:=Ct(1,1,2,0,1,4,3,22);
```

```
w1:=MinimumWeight(C1); IsSelfDual(C1); IsDoublyEven(C1);
w1;
w2:=MinimumWeight(C2); IsSelfDual(C2); IsDoublyEven(C2);
w2;
w3:=MinimumWeight(C3); IsSelfDual(C3); IsDoublyEven(C3);
w3;
w4:=MinimumWeight(C4); IsSelfDual(C4); IsDoublyEven(C4);
w4;
w5:=MinimumWeight(C5); IsSelfDual(C5); IsDoublyEven(C5);
w5;
w6:=MinimumWeight(C6); IsSelfDual(C6); IsDoublyEven(C6);
w6;
w7:=MinimumWeight(C7); IsSelfDual(C7); IsDoublyEven(C7);
w7;
w8:=MinimumWeight(C8); IsSelfDual(C8); IsDoublyEven(C8);
w8;
w9:=MinimumWeight(C9); IsSelfDual(C9); IsDoublyEven(C9);
w9;
w10:=MinimumWeight(C10); IsSelfDual(C10); IsDoublyEven(C10);
w10;
w11:=MinimumWeight(C11); IsSelfDual(C11); IsDoublyEven(C11);
w11;
w12:=MinimumWeight(C12); IsSelfDual(C12); IsDoublyEven(C12);
w12;
w13:=MinimumWeight(C13); IsSelfDual(C13); IsDoublyEven(C13);
w13;
w14:=MinimumWeight(C14); IsSelfDual(C14); IsDoublyEven(C14);
w14;
w15:=MinimumWeight(C15); IsSelfDual(C15); IsDoublyEven(C15);
w15;
w16:=MinimumWeight(C16); IsSelfDual(C16); IsDoublyEven(C16);
w16;
w17:=MinimumWeight(C17); IsSelfDual(C17); IsDoublyEven(C17);
w17;
w18:=MinimumWeight(C18); IsSelfDual(C18); IsDoublyEven(C18);
w18;
w19:=MinimumWeight(C19); IsSelfDual(C19); IsDoublyEven(C19);
w19;
w20:=MinimumWeight(C20); IsSelfDual(C20); IsDoublyEven(C20);
```

```
w20;
w21:=MinimumWeight(C21); IsSelfDual(C21); IsDoublyEven(C21);
w21;
w22:=MinimumWeight(C22); IsSelfDual(C22); IsDoublyEven(C22);
w22;
w23:=MinimumWeight(C23); IsSelfDual(C23); IsDoublyEven(C23);
w23;
w24:=MinimumWeight(C24); IsSelfDual(C24); IsDoublyEven(C24);
w24;
w25:=MinimumWeight(C25); IsSelfDual(C25); IsDoublyEven(C25);
w25;
```

Bibliografía & Referencias

[1] 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.

[2] 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.

[3] M. Borello, *The automorphism group of a self-dual [72,36,16] code is not an elementary abelian group of order 8*, Finite Fields and Their Applications 25 (2014), 1-7.

[4] S. Bouyuklieva, J. de la Cruz, W. Willems, *On the Automorphism Group of a Binary Self-dual* $[120, 60, 24]$ *Code*, *AAECC* (2013).

[5] 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.

[6] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes* Cambridge University Press, New York, (2003).

[7] J. H. Conway and V. Pless, *On enumeration of self-dual codes*, J Combin Theory, Ser. A, 28, 26-53 (1980).

[8] J. de la Cruz, *Über die Automorphismengruppe der extremaler Codes der Längen 96 und 120*. Ph.D., Otto-von-Guericke Universität, Magdeburg, Germany, 2012.

[9] J. De la Cruz and W. Willems, *On extremal self-dual code of length 9,* IEEE Transactions on Information Theory 6 (2011), no. 57, 6820-6828.

[10] 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.

[11] V. N. Logachev, *Refinament of the Griesmer bound in the case of small code distances, in: Methods of Optimization and Their Applications*, [in Russian], SEI SOAA SSSR, Izd. Sib. Otd. Akad. Nauk SSSR, Irkutsk (1974), pp. 108-112.

[12] X. Ma, *Nonexistence of extremal doubly even self-dual codes with large length*, Discrete Math, 185 (1998), 265-274.

[13] C.L. Mallows, N.J.A. Sloane, *An upper bound for self-dual codes*, Information and Control 22 (1973), 188-200.

[14] F.J. McWilliams and N. J. Sloane, *Theory of Error-Correcting Codes*, [Russian traslation], Svyaz Moscow (1979).

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

[16] V. Pless, *Introduction to the theory of error correcting codes, second edition*, [United States of America], (1989).

[17] E. M. Rains, *Shadow bounds for self-dual codes*, IEEE Transactions on Information Theory 44 (1998), 134-139.

[18] N. J. A. Sloane, *Is there a [72; 36], d = 16 self-dual code?*, IEEE Transactions on Information Theory 19 (1973), 251.

[19] H. Weyl, *Algebraic Theory of Numbers*, Princeton University Press (1945).

[20] V.Y. Yorgov, *A method for Constructing Inequivalent Self-Dual Codes with Applications to Length 56*, *IEEE Trans. Inform. Theory* IT-**33**, (1987) 77-82.

[21] V.Y. Yorgov, *Binary self-dual codes with automorphisms of odd order*, Russian, Probl. Pered. Inform. 19, 11-24 (1983).

[22] V. Yorgov and D. Yorgov, *The automorphism group of a self dual binary [72; 36; 16] code does not contain* Z_4, preprint,arXiv:1310.2570v2 (2013).

[23] R. YORGOVA, A. WASSERMANN, *Binary self-dual codes with automorphisms of order 23,* Des. Codes Cryptogr. (2008) 48:155-164.

[24] S. ZHANG, *On the nonexistence of extremal self-dual codes*, Discrete Appl. Math. 91 (1999), 277-286.