**Revista Colombiana de Matemáticas**
Volumen 48(2014)2, páginas 135-163

# Códigos autoduales con un automorfismo de orden primo impar

## Self-Dual Codes with an Automorphism of Odd Prime Order

Javier de la Cruz[1], Ismael Gutierrez[1,✉], Jorge Robinson[2]

[1]Universidad del Norte, Barranquilla, Colombia

[2]Universidad del Atlántico, Barranquilla, Colombia

Resumen. En este artículo presentamos un resumen de algunos de los resultados más importantes sobre códigos lineales binarios y autoduales con un automorfismo de orden primo impar que se han establecido en los últimos años. Además por medio de un automorfismo de orden 59 construimos 24 nuevos $[120, 60]$-códigos binarios autoduales, doblemente pares optimales.

*Palabras y frases clave.* Códigos lineales, códigos binarios, códigos autoduales, códigos doblemente pares, códigos extremales, códigos optimales, automorfismos de códigos.

*2010 Mathematics Subject Classification.* 53C21, 53C42.

Abstract. In this paper we present a survey of the most important results on binary self-dual linear codes with an automorphism of odd prime order, which have been established in recent years. Additionally, through an automorphism of order 59, we show that there are at least 24 new binary, self dual doubly even optimal $[120, 60]$-codes.

*Key words and phrases.* Linear codes, Binary codes, Self dual codes, Doubly even codes, Extremal codes, Automorphisms.

### 1. Introducción

A lo largo de este trabajo usaremos la expresión *un código* sobre $\mathbb{F}_q$ para referirnos a *un código lineal* sobre el cuerpo finito $\mathbb{F}_q$.

Los códigos binarios autoduales, doblemente pares juegan un papel central en la teoría clásica de códigos. Estos se denominan códigos de *tipo* II. Los códigos autoduales que no son doblemente pares son llamados de tipo I.

C. L. Mallows y N. J. A. Sloane [16] demostraron que un código binario autodual doblemente par de longitud $n$ tiene mínima distancia $d \leq 4\lfloor n/24 \rfloor + 4$, donde $\lfloor x \rfloor$ denota la parte entera de $x$. Con distintos argumentos E. M. Rains [17] probó que la cota superior anterior también es válida sin la condición de doble paridad, excepto si $24 \nmid n+2$. Un código cuya distancia mínima alcanza la respectiva cota superior se denomina *extremal*.

En las aplicaciones los códigos extremales son de gran utilidad dado que existe una relación directa entre la capacidad de corregir errores y la distancia mínima del código. Sin embargo en muchos casos se dificulta la construcción de códigos extremales, por lo cual toman gran importancia los códigos con distancia mínima cercana a la de un código extremal de la misma longitud. Estos códigos son denominados *optimales*.

X. Ma en [15] estableció que no existen códigos extremales de tipo II con longitud $n \geq 3984$. 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 $[24m, 12m, 4m+4]$, $m \in \mathbb{N}$, es de tipo II. S. Zhang [22] demostró que códigos con estos parámetros tienen longitud $n = 24m \leq 3672$. Pese a su trascendencia y aunque esta cota para la longitud es considerablemente grande, solo se conocen dos códigos autoduales extremales con estos parámetros, para $m = 1$ y $m = 2$.

Si $C$ es un código de longitud $n$ sobre el cuerpo finito $\mathbb{F}_q$ y $\sigma \in \mathrm{Sym}(n)$, 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 $\sigma$. En ese caso $C$ y $\sigma(C)$ se denominan códigos *equivalentes*. Se dice que $\sigma$ es un *automorfismo* de $C$, si $\sigma(C) = C$. Se puede verificar fácilmente que el conjunto $\mathrm{Aut}(C)$ formado por todos los automorfismos de $C$ es un grupo y se denomina *el grupo de automorfismos* de $C$.

Retornemos a la familia de códigos extremales de tipo II con parámetros $[24m, 12m, 4m+4]$. Si $m = 1$, entonces se obtiene el ampliamente conocido $[24, 12, 8]$-código binario extendido de Golay.

Si $m = 2$, entonces la estructura corresponde a un $[48, 24, 12]$-código binario de resto cuadrático. W. C. Huffman [9] demostró que los códigos binarios autoduales con un automorfismo de orden primo impar se pueden escribir como la suma directa de dos subcódigos.

Si $m = 3$, entonces se tiene un $[72, 36, 16]$-código binario autodual extremal. Su existencia es aún un problema abierto. Este fue formulado por primera vez

en 1972 por N. J. A. Sloane [18]. Recientemente M. Borello [3] y V. Yorgov-D.Yorgov [19] 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.

Si $m = 4$, entonces 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 [12],[14] 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 dos últimos años J. De la Cruz, S. Bouyuklieva y W. Willems [5], [13] y [12] 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. Finalmente se demostró que si $p = 3, 5, 7, 19, 23, 29$, entonces $p^2$ no divide a dicho orden.

## 2. Preliminares

Sea $\mathbb{F}_q$ el cuerpo finito con $q$ elementos y $n \in \mathbb{N}$. Un *código lineal* $C$ de longitud $n$ sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$. Escribiremos para ello $C \leq \mathbb{F}_q^n$.

Para $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ se define la *distancia de Hamming* $d$ entre $u$ y $v$ como el número de posiciones en las que los vectores difieren. Esto es,

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

Se verifica que la distancia de Hamming $d$ define una métrica sobre $\mathbb{F}_q^n$. Si $|C| > 1$, entonces

$$d(C) \coloneqq \text{mín}\{d(c, c') : c, c' \in C, c \neq c'\}$$

se denomina la *distancia mínima* de Hamming de $C$ y si $|C| = 1$, entonces definimos $d(C) \coloneqq 0$.

Si $\dim_{\mathbb{F}_q}(C) = k$ y la distancia mínima de Hamming de $C$ es $d$, entonces decimos que $C$ es un $[n, k]$-*código* o, más preciso, un $[n, k, d]$-*código* sobre $\mathbb{F}_q$. Si $k \geq 1$, entonces $A \in \mathrm{M}_{k\times n}(\mathbb{F}_q)$ se denomina una matriz *generadora* de $C$, si las filas de $A$ forman una base de $C$. Es usual denotar tal matriz con $\text{gen}(C)$.

El *soporte* de $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, se denota por $\text{sop}(x)$ y se define como el conjunto de los índices en los que las componentes de $x$ son no nulas; esto es,

$$\text{sop}(x) \coloneqq \{i : x_i \neq 0\}.$$

El *peso* de $x$, notado con $\mathrm{wt}(x)$, se define como el número de elementos de $\mathrm{sop}(x)$; es decir, $\mathrm{wt}(x) = |\mathrm{sop}(x)|$. Si $C \leq \mathbb{F}_q^n$, entonces el *peso mínimo* de $C$ se nota y define

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

Sea $r \in \mathbb{N}$. Un código $C$ se denomina *$r$-divisible*, si $r \,|\, \mathrm{wt}(c)$, para todo $c \in C$. En particular, un código 2-divisible es denominado *par* y uno 4-divisible se llama *doblemente par*. Un teorema de A. M. Gleason, J. N. Pierce y R. Turyn [2, Part XI], [7], garantiza que, si $r > 1$ divide el peso de cada elemento en un código binario autodual no trivial, entonces $r = 2$ o $r = 4$. Todo código binario autodual es par.

El siguiente resultado establece un restricción a la distancia mínima de un código binario autodual.

**Teorema 2.1** (C. L. Mallows, N. J. A. Sloane, E. M. Rains)**.** *[16, Theorem 2], [17] Si $C$ es un código binario autodual de longitud $n$ y de distancia mínima $d$, entonces*

$$d \leq 4\lfloor n/24 \rfloor + 4, \quad si \quad n \not\equiv 22 \pmod{24}$$

*y*

$$d \leq 4\lfloor n/24 \rfloor + 6, \quad si \quad n \equiv 22 \pmod{24}.$$

**Definición 2.2.** Si $C \leq \mathbb{F}_q^n$, entonces para $i = 0, \ldots, n$ definimos la *distribución de pesos* de $C$

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

Además,

$$W_C(x) = \sum_{i=0}^{n} A_i x^i = \sum_{c \in C} x^{\mathrm{wt}(c)} \in \mathbb{Z}[x]$$

se denomina el polinomio *enumerador de pesos* de $C$. Llamamos a

$$W_C(x, y) = x^n W\big(\tfrac{y}{x}\big) = \sum_{i=0}^{n} A_i x^{n-i} y^i \in \mathbb{Z}[x, y]$$

el polinomio enumerador de pesos *homogéneo* de $C$ en las indeterminadas $x, y$.

Los siguientes resultados de A. M. Gleason pueden ser utilizados, por un lado para la determinación del polinomio enumerador de pesos de un código y por otro lado también se utilizan para demostrar la no existencia de códigos autoduales con ciertos parámetros.

**Teorema 2.3.** *[7, A. M. Gleason] Sea $C$ código binario.*

*(1) Si $C$ es autodual, entonces el polinomio enumerador de pesos, homogéneo de $C$ es un polinomio con coeficientes racionales en*

$$x^2 + y^2 \qquad y \ en \qquad x^8 + 14x^4y^4 + y^8,$$

*o en*

$$x^2+y^2 \qquad y\ en \qquad x^2y^2(x^2-y^2)^2.$$

*(2) Si $C$ es autodual y doblemente par, entonces el polinomio enumerador de pesos homogéneo de $C$ es un polinomio con coeficiente racionales en*

$$x^8+14x^4y^4+y^8 \qquad y\ en \qquad x^4y^4(x^4-y^4)^4,$$

*o en*

$$x^8+14x^4y^4+y^8 \qquad y\ en \qquad x^{24}+759x^{16}y^8+2576x^{12}y^{12}+759x^8y^{16}+y^{24}.$$

Se sigue del teorema anterior el siguiente resultado

**Corolario 2.4.** *Un código binario autodual y doblemente par tiene longitud divisible por 8.*

Si $C$ es un código de longitud $n$, entonces llamamos a $S \coloneqq \{1,\dots,n\}$ el conjunto de coordenadas de $C$.

**Definición 2.5.** Sea $C$ un $[n,k]$-código sobre $\mathbb{F}_q$, con conjunto de coordenadas $S$. Sea $T=\{T_1,\dots,T_p\}$ una partición de $S$ y para $j=1,\dots,p$ definamos $n_j \coloneqq |T_j|$. Para un vector $v\in\mathbb{F}_q^n$ denotamos con $W_T(v)$ la $p$-tupla

$$W_T(v) \coloneqq \big(|\operatorname{sop}(v)\cap T_1|,\dots,|\operatorname{sop}(v)\cap T_p|\big).$$

Llamamos a $W_T(v)$ el *$T$-peso* de $v$. Notamos con $W(T)$ el conjunto de todos los pesos con respecto a la partición $T$. Es decir,

$$W(T) \coloneqq \{\mathbf{i}\in\mathbb{N}^p : i_j\le n_j,\ \forall j\}.$$

Note que

$$N(T) \coloneqq |W(T)| = \prod_{j=1}^{p}(n_j+1).$$

Definimos además

$$A_{\mathbf{i}}(T) \coloneqq \big|\{v\in C : W_T(v)=\mathbf{i}\}\big|$$

y

$$B_{\mathbf{i}}(T) \coloneqq \big|\{v\in C^{\perp} : W_T(v)=\mathbf{i}\}\big|.$$

El vector $\big(\big(A_{\mathbf{i}}(T)\big)\big)_{\mathbf{i}\in W(T)}$ de longitud $N(T)$ se llama la *distribución de pesos* del código con respecto a la partición $T$. Si $p=2$, entonces hablamos de la *distribución dividida* de pesos.

## 3. El grupo de automorfismos de un código

Denotemos con $\mathrm{Sym}(n)$ al grupo simétrico de grado $n$.

**Definición 3.1.** Definimos una acción de $\sigma \in \mathrm{Sym}(n)$ sobre $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ de la siguiente manera:

$$\sigma(x) \coloneqq \big(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\big).$$

Si $C$ es un código de longitud $n$ y $\sigma(c) \in C$, para todo $c \in C$, entonces $\sigma$ es denominado un *automorfismo* de $C$. El grupo de automorfismos de $C$ se nota con $\mathrm{Aut}(C)$.

**Definición 3.2.** Sean $C$ un código de longitud $n$ y $\sigma \in \mathrm{Aut}(C)$ de orden $p$, con $p$ un número primo. Decimos que $\sigma$ es *de tipo* $p$-$(c; f)$ si $\sigma$ tiene exactamente $c$ ciclos de longitud $p$ y $f$ puntos fijos.

Sin pérdida de generalidad podemos suponer que $\sigma$ tiene la forma

$$\sigma = (12\cdots p)(p+1\ p+2\cdots 2p)\cdots\big((c-1)p+1\ (c-1)p+2\cdots cp\big). \qquad (1)$$

A lo largo del trabajo asumiremos que todos los automorfismos considerados son de la forma (1) y de tipo $p$-$(c; f)$, donde $p$ es un número primo impar.

**Definición 3.3.** Sean $G$ un grupo y $X$ un conjunto no vacío. Decimos que $X$ es un $G$-conjunto derecho, si existe una función $\circ : X \times G \longrightarrow X$ para la cual se satisfacen

(1) $x \circ e = x$ para todo $x \in X$, donde $e$ es el elemento neutro del grupo.

(2) $x \circ (gh) = (x \circ g) \circ h$, para todo $g, h \in G$ y todo $x \in X$.

En adelante escribimos simplemente $xg$ en lugar de $x \circ g$.

Si $X$ es un $G$-conjunto, entonces la *$G$-orbita* de $x \in X$ se denota con $O(x)$ y se define así:

$$O(x) = \{xg : g \in G\} \subseteq X.$$

El *estabilizador* de $x$ en $G$ así:

$$G_x = \{g \in G : xg = x\} \leq G.$$

Si $G$ es un grupo finito, se tiene que

$$|O(x)| = \frac{|G|}{|G_x|}.$$

Sea $\mathrm{Fix}(g)$ el número de elementos $x \in X$ que son fijados por la acción de $g \in G$, esto es,

$$\mathrm{Fix}(g) = \big|\{x \in X : xg = x\}\big|.$$

Entonces del lema de Burnside, también llamado muchas veces de Cauchy - Frobenius [11, 1A.6] se sigue que el número de órbitas $t(G)$ está dado por

$$t(G) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

Si $H \leq G$, entonces definimos el *normalizador* de $H$ en $G$ como

$$N_G(H) = \big\{\tau \in G : \tau H \tau^{-1} = H\big\}.$$

Para $\tau \in G$ escribimos simplemente $N_G(\tau)$ en lugar de $N_G\big(\langle\tau\rangle\big)$. Para un número primo fijo $p$ denotamos con $\mathrm{Syl}_p(G)$ el conjunto de todos los $p$-subgrupos de Sylow de $G$. Es conocido que si $S \in \mathrm{Syl}_p(G)$, entonces

$$\big|\,\mathrm{Syl}_p(G)\big| = \big|G : N_G(S)\big| = \frac{|G|}{\big|N_G(S)\big|}.$$

Además que $\big|\,\mathrm{Syl}_p(G)\big| \equiv 1 \pmod{p}$.

El siguiente lema será útil en la sección de aplicaciones.

**Lema 3.4.** *[11, 1E.2] Sea $G$ un grupo con $|G| = pqr$, donde $p < q < r$ son números primos. Entonces $\big|\,\mathrm{Syl}_r(G)\big| = 1$.*

***Observación* 3.5.** Si $C$ es un código de longitud $n$ y $G = \mathrm{Aut}(C)$, entonces podemos ver sin dificultades que tanto $C$ como el conjunto de coordenadas de $C$ son $G$-conjuntos.

El siguiente teorema es una generalización de [4, Theorem 1.3], el cual permite bajo ciertas condiciones obtener información sobre el orden de los $p$-subgrupos de Sylow de $\mathrm{Aut}(C)$.

**Teorema 3.6.** *[5] Sea $C$ un código binario de longitud $n$. Si $p$-$(c; f)$ es el único tipo para todo automorfismo $\sigma \in \mathrm{Aut}(C)$ de orden primo $p$ con $c \not\equiv 0 \pmod{p}$ y $f < p$, entonces $p^2 \nmid \big|\,\mathrm{Aut}(C)\big|$.*

**Lema 3.7.** *Sea $C$ un código binario de longitud $n$, tal que todo automorfismo de orden $p$ carezca de puntos fijos. Si $\big|\,\mathrm{Aut}(C)\big| = p^a m$, entonces*

$$a \leq \max\big\{r \in \mathbb{N} : p^r | n\big\}.$$

***Demostración.*** Supongamos que $a > \max\{r \in \mathbb{N} : p^r | n\}$. Dado que $p^a$ divide a $|\operatorname{Aut}(C)|$, se tiene que existe $H \leq \operatorname{Aut}(C)$ con $|H| = p^a$. El subgrupo $H$ actúa sobre el conjunto de coordenadas de $C$, digamos $X$ y dado que todo $\sigma \in H$ no tiene puntos fijos, se sigue que toda orbita $O(x)$ con $x \in X$ satisface que $|O(x)| = p^a$. Por lo tanto $|O(x)| = p^a \mid n$, lo cual es una contradicción. ☑

**Lema 3.8.** *Sean $C$ un código binario de longitud $n$, $G = \operatorname{Aut}(C)$ y $p \neq q$ dos números primos. Sea $\tau \in G$ un elemento de orden $p$. Supongamos que todo automorfismo de $C$ de orden $p$ tiene exactamente $f > 0$ puntos fijos y cada automorfismo de $C$ de orden $q$ carece de puntos fijos. Si*

$$q^s = \max\{q^l : 1 \leq l \leq f\}$$

*entonces $q^{s+1} \nmid |N_G(\tau)|$.*

***Demostración.*** Si $q \nmid |N_G(\tau)|$, entonces la afirmación es inmediata. Supongamos entonces que $q \mid |N_G(\tau)|$. Por lo tanto existe $Q \in \operatorname{Syl}_q(N_G(\tau))$ con $|Q| = q^r$ y $q^{r+1} \nmid |N_G(\tau)|$. Puesto que $\tau$ tiene $f$ puntos fijos, escribamos sin perdida de generalidad $\tau(x) = x$, para $1 \leq x \leq f$.

Si $g \in Q$, entonces existe $i \in \mathbb{Z}$ tal que $g\tau g^{-1}(y) = \tau^i(y)$, para todo $1 \leq y \leq n$. Por lo tanto $\tau(xg) = xg$ para todo $1 \leq x \leq f$. Es decir, $xg$ es un punto fijo de $\tau$ y por lo tanto $xg \in \{1, \ldots, f\}$.

Sea $Q_x$ el estabilizador de $x \in Q$, con $x \in \{1, \ldots, f\}$. Dado que todo $x \in Q$ tiene orden $q^r$, se verifica que $x$ no tiene puntos fijos. Por lo tanto $|Q_x| = 1$ y en consecuencia

$$|O(x)| = \frac{|Q|}{|Q_x|} = |Q|.$$

Además $xg \in \{1, \ldots, f\}$ para todo $g \in Q$. Por lo tanto

$$|Q| = |O(x)| \leq f$$

y con ello se tiene que $1 \leq q^r \leq f$. Entonces $q^r \leq q^s$ y en consecuencia $q^{s+1} \nmid |N_G(\tau)|$. ☑

## 4. Códigos cíclicos

**Definición 4.1.** $C \leq \mathbb{F}_q^n$ se denomina un código *cíclico* si y sólo si para todo $(c_0, c_1, \ldots, c_{n-1}) \in C$ se verifica que $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. Equivalentemente, $C$ es cíclico si y sólo si $\sigma = (12 \cdots n) \in \operatorname{Aut}(C)$.

En algunas situaciones, en lugar de considerar los códigos como subespacios vectoriales de $\mathbb{F}_q^n$, podemos verlos como subanillos del anillo cociente

$$R_n \coloneqq \mathbb{F}_q[x] \,/ \langle x^n - 1 \rangle,$$

donde $\langle x^n - 1\rangle$ denota el ideal de $\mathbb{F}_q[x]$ generado por $x^n - 1$. La función

$$f : \mathbb{F}_q^n \longrightarrow R_n$$

definida por

$$f(c_0, c_1 \ldots, c_{n-1}) \coloneqq \sum_{j=0}^{n-1} c_j x^j + \langle x^n - 1\rangle = c(x) + \langle x^n - 1\rangle$$

es un isomorfismo entre $\mathbb{F}_q$-álgebras. En consecuencia, $\mathbb{F}_q^n$ puede identificarse con el sistema de representantes canónicos de las clases laterales de $R_n$; es decir, cada $v = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ puede identificarse con el polinomio $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} \in \mathbb{F}_q[x]$.

Si $C \leq \mathbb{F}_q^n$, entonces notamos con $C(x)$ al conjunto

$$\{c(x) + \langle x^n - 1\rangle : c \in C\}.$$

Se tiene que el código $C$ es cíclico si y sólo si $C(x)$ es un ideal de $R_n$. Dado que todo ideal en $R_n$ es un ideal principal, se tiene que todo código cíclico en $R_n$ tiene un polinomio que lo genera.

El siguiente resultado establece una correspondencia entre los códigos cíclicos de $R_n$ y los polinomios divisores mónicos de $x^n - 1$.

**Teorema 4.2.** *[10, Theorem 4.2.1] Sea $C$ un código cíclico no nulo en $R_n$. Entonces existe un polinomio $g(x) \in C$ con las siguientes propiedades:*

*(1) $g(x)$ es el único polinomio mónico de grado mínimo en $C$.*

*(2) $g(x)$ es un generador de $C$; es decir, $C = \langle g(x)\rangle$.*

*(3) $g(x) \mid (x^n - 1)$.*

*(4) $\dim_{\mathbb{F}_q} C = n - \operatorname{grad}\big(g(x)\big)$.*

El polinomio $g(x)$ en el lema anterior se denomina el *polinomio generador* del código cíclico $C$. Un polinomio $e(x)$ se llama un generador *idempotente* de un código cíclico $C$ si se verifica que $e(x)$ genera a $C$ y además $e^2(x) = e(x)$.

**Teorema 4.3.** *[10, Theorem 4.3.2] Sea $C = \langle g(x)\rangle$ un código cíclico no nulo en $R_n$. Entonces:*

*(1) Existe un único idempotente $e(x) \in C$ tal que $C = \langle e(x)\rangle$, es decir, $e(x) = p(x)g(x)$, para algún polinomio $p(x)$.*

*(2) Si $e(x)$ es un idempotente no nulo en $C$, entonces $C = \langle e(x)\rangle$ si y sólo si $e(x)$ es una unidad de $C$.*

En el siguiente teorema se garantiza que la suma y la intersección de dos códigos cíclicos es también un código cíclico. Además se indica quienes son sus polinomios generadores y sus idempotentes generadores.

**Teorema 4.4.** *[10, Theorem 4.3.7] Sean $C_1$ y $C_2$ códigos cíclicos de longitud $n$ sobre $\mathbb{F}_q$ con polinomios generadores $g_1(x)$ y $g_2(x)$ y generadores idempotentes $e_1(x)$ y $e_2(x)$ respectivamente. Entonces:*

*(1) $C_1 \subseteq C_2$ si y sólo si $g_2(x) \mid g_1(x)$.*

*(2) $C_1 \cap C_2$ tiene polinomio generador* $\operatorname{mcm}\big(g_1(x), g_2(x)\big)$ *y generador idempotente $e_1(x)e_2(x)$.*

*(3) $C_1 + C_2$ tiene polinomio generador* $\operatorname{mcd}\big(g_1(x), g_2(x)\big)$ *y generador idempotente $e_1(x) + e_2(x) - e_1(x)e_2(x)$.*

En el resto de la sección consideramos solamente códigos cíclicos binarios; es decir, ideales del anillo cociente $R_n = \mathbb{F}_2[x] \big/ \langle x^n - 1 \rangle$.

En el siguiente resultado se presentan unos generadores idempotentes especiales y se muestra una caracterización de los ideales minimales de $R_n$.

**Teorema 4.5.** *Sea la descomposición de $x^n - 1$ en polinomios irreducibles sobre $\mathbb{F}_2$ dada por*

$$x^n - 1 = h_0(x)h_1(x)\cdots h_s(x), \tag{2}$$

*con $h_0(x) = x - 1$. Para $j = 0, \ldots, s$ definamos $I_j \coloneqq \big\langle q_j(x) \big\rangle$, donde*

$$q_j(x) = \frac{x^n - 1}{h_j(x)}.$$

*Sea además $e_j(x)$ el generador idempotente de $I_j$. Entonces:*

*(1) Los $I_j$ son todos los ideales minimales de $R_n$.*

*(2) $R_n = I_0 \oplus I_1 \oplus \cdots \oplus I_s$.*

*(3) Si $k_j \coloneqq \operatorname{grad}\big(h_j(x)\big)$, entonces $I_j$ es un cuerpo isomorfo a $\mathbb{F}_{2^{k_j}}$.*

*(4) $e_j(x)e_i(x) = 0$ para todo $j \neq i$.*

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

***Demostración.***

(1) Demostramos inicialmente que cada $I_j$ es un ideal minimal de $R_n$. Para ello supongamos que esta afirmación es falsa. Entonces existe un ideal no nulo de $R_n$, digamos $\big\langle g(x) \big\rangle$, con $\big\langle g(x) \big\rangle \subseteq I_j$. Del teorema 4.4(1) se sigue que $q_j(x) \mid g(x)$ con $g(x) \neq q_j(x)$, lo que no es posible ya que $h_j(x)$ es irreducible y $g(x) \mid x^n - 1$.

(2) Dado que el conjunto $\{q_j(x) : 1 \leq j \leq s\}$ no tiene factores irreducibles comunes de $x^n - 1$ y dado que cada polinomio $q_j(x)$ divide a $x^n - 1$, se sigue que $\operatorname{mcd}\big(q_1(x), \ldots, q_s(x)\big) = 1$. En consecuencia, por el algoritmo de Euclides, existen $a_i(x) \in \mathbb{F}_q[x]$ tales que

$$\sum_{i=1}^{s} a_i(x) q_i(x) = 1. \tag{3}$$

Entonces 1 pertenece a la suma de los ideales $I_j$ y se tiene que $R_n = I_0 + I_1 + \cdots + I_s$. Para probar que esta suma es directa, demostramos que para cada $1 \leq j \leq s$ se verifica

$$I_j \bigcap \sum_{i \neq j} I_i = \{0\}.$$

Como $h_j(x) \mid q_i(x)$, para $j \neq i$, $h_j \nmid q_j(x)$ y los factores irreducibles de $x^n - 1$ son distintos, entonces

$$h_j(x) = \operatorname{mcd}\{q_i(x) : 1 \leq i \leq s, \quad i \neq j\}.$$

Aplicando inducción sobre el resultado del teorema 4.4(3) tenemos que

$$\langle h_j(x) \rangle = \sum_{i \neq j} I_j.$$

Por lo tanto, del teorema 4.4(2), se sigue que

$$I_j \cap \sum_{i \neq j} I_i = I_j \cap \langle h_j(x) \rangle = \langle \operatorname{mcm}\big(q_j(x), h_j(x)\big) \rangle = \langle x^n - 1 \rangle = \{0\}.$$

Para culminar la demostración de (1), sea $M = \langle m(x) \rangle$ un ideal minimal cualquiera de $R_n$. Usando la ecuación (3) tenemos

$$0 \neq m(x) = m(x) \bullet 1 = \sum_{j=1}^{s} m(x) a_j(x) q_j(x).$$

Entonces existe $j \in \{0, 1, \ldots, s\}$ tal que $m(x) a_j(x) q_j(x) \neq 0$ y en consecuencia $M \cap I_j \neq \{0\}$, ya que $m(x) a_j(x) q_j(x) \in M \cap I_j$. Por lo tanto, por la minimalidad de $M$ y de $I_j$, se tiene que $M = I_j$.

(3) Sea $0 \neq a(x) \in I_j$ con $j \in \{0, 1, \ldots, s\}$. Entonces $\langle a(x) \rangle$ es un ideal no nulo contenido en $I_j$. Por la minimalidad de $I_j$ se tiene que $\langle a(x) \rangle = I_j$. Si $e(x)$ es la identidad de $I_j$, entonces existe $b(x) \in R_n$ tal que $e_j(x) = a(x)b(x)$. Dado que $e(x) \in I_j$, entonces $c(x) = b(x)e(x) \in I_j$. Por lo tanto, $a(x)c(x) = e(x)^2 = e(x)$; es decir todo elemento no nulo tiene un inverso multiplicativo. Si $\operatorname{grad}\big(h_j(x)\big) = k_j$, entonces $I_j$ tiene dimensión $k_j$ y por lo tanto tiene $2^{k_j}$ elementos.

(4) Si $i \neq j$, entonces de (2) se sigue que $e_j(x)e_i(x) \in I_j \cap I_i = \{0\}$.

(5) Aplicando inducción al teorema 4.4(3) y usando (4) se sigue que $\sum_{j=0}^{s} e_j(x)$ es el generador idempotente de $R_n$. Pero el generador idempotente de $R_n$ es 1, con lo cual se sigue la afirmación. ☑

En el siguiente lema se presentan condiciones para garantizar que el conjunto $P$ de los *codewords* de peso par en $R_n$ formen un cuerpo, indicando además de manera explícita su elemento identidad.

**Lema 4.6.** *[9, Lemma 4] Sea* $P \coloneqq \{v(x) \in R_n : \operatorname{wt}\big(v(x)\big) \equiv 0 \pmod 2\}$. *Entonces:*

*(1) $P$ es un código cíclico con $|P| = 2^{n-1}$ y $P = \big\langle (x-1) + \langle x^n - 1\rangle \big\rangle$.*

*(2) $P$ es un subanillo de $\mathbb{F}_2[x] \big/ \langle x^n - 1\rangle$ con identidad $e(x) = x + x^2 + \cdots + x^{n-1}$.*

*(3) Si $n$ es un número primo, digamos $p$ y $1 + x + \cdots + x^{p-1}$ es irreducible sobre $\mathbb{F}_2[x]$, entonces $P$ es un cuerpo. Además*

$$\beta(x)p(x) \equiv xp(x) \qquad \big(\text{mód } (x^p - 1)\big)$$

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

Examinamos ahora parte de la estructura interna del grupo multiplicativo de $P$. Concretamente se presenta una lista de los elementos de orden $p$ en $P \setminus \{0\}$.

**Lema 4.7.** *Sea $p$ un número primo tal que $1 + x + \cdots + x^{p-1}$ es irreducible en $\mathbb{F}_2[x]$ y sea $\beta(x)$ como en el lema 4.6. Entonces:*

*(1) $x^t e(x) \equiv \beta(x)^t \pmod{(x^p - 1)}$ para todo $0 \leq t \leq p-1$ y $\operatorname{ord}\big(xe(x)\big) = \operatorname{ord}\big(\beta(x)\big) = p$.*

*(2) Si $q(x) \in P$ con $\operatorname{ord}\big(q(x)\big) = m$ y $\operatorname{mcd}(p, m) = 1$, entonces $\operatorname{ord}\big(xq(x)\big) = pm$.*

*(3) $H = \big\langle \beta(x) \big\rangle$ es el único subgrupo de orden $p$ en $P \setminus \{0\}$.*

*(4) $\beta(x), \beta(x)^2, \ldots, \beta(x)^{p-1}$ son los únicos elementos de orden $p$ en $P \setminus \{0\}$. y $H = \big\langle \beta(x)^i \big\rangle$, $i = 1, 2, \ldots, p-1$.*

***Demostración.*** Es conocido que, si $G$ es un grupo cíclico finito y $p \mid |G|$, entonces existe un único subgrupo $H = \langle a \rangle = \{1, a, \ldots, a^{p-1}\}$, con $|H| = p$. Además los elementos $a, a^2, \ldots, a^{p-1}$ son los únicos elementos de orden $p$ en $G$ y cada potencia $a^i$, con $i = 1, 2, \ldots, p-1$ genera a $H$.

(1) Dado que $xe(x)-\beta(x) = x^p-1$, se tiene que $xe(x) \equiv \beta(x)\big(\text{mód } (x^p-1)\big)$. Por lo tanto $x^t e(x) \equiv \beta(x)^t \quad \big(\text{mód } (x^p-1)\big)$. Por otro lado, puesto que $\big(xe(x)\big)^p = e(x)$ y $p$ es un número primo, se sigue que $\text{ord}\,\big(xe(x)\big) = \text{ord}\,\big(\beta(x)\big) = p$.

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

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

Por lo tanto $\text{ord}\,\big(xq(x)\big) \mid pm$, y, dado que $\text{mcd}(p,m) = 1$, se sigue que $\text{ord}\,\big(xq(x)\big) = pm$.

(3) Es claro que $\big|P \setminus \{0\}\big| = 2^{p-1}-1$. Sabemos además que $\text{ord}\,\big(\beta(x)\big) = p$ y $p \mid (2^{p-1}-1)$. Por lo tanto, de la observación inicial, se sigue que $H = \big\langle \beta(x) \big\rangle$ es el único subgrupo de orden $p$ en $P \setminus \{0\}$.

(4) Se sigue de la observación inicial. ☑

Sea nuevamente $x^p - 1 = h_0(x)h_1(x)\cdots h_s(x)$ la descomposición de $x^p-1$ en polinomios irreducibles sobre $\mathbb{F}_2$ como en (2) del teorema 4.5. Si $p$ es un primo impar, entonces

$$\text{grad}\,\big(h_j(x)\big) = \tfrac{p-1}{s}$$

y en consecuencia tenemos el siguiente resultado

**Teorema 4.8.** *$P = I_1 \oplus I_2 \oplus \cdots \oplus I_s$ y cada $I_j$ es un cuerpo con $2^{\frac{p-1}{s}}$ elementos.*

***Demostración.*** Dado que $\dim_{\mathbb{F}_2} I_j = \text{grad}\,\big(h_j(x)\big)$, se sigue que

$$\dim_{\mathbb{F}_2}\big(I_1 \oplus I_2 \oplus \cdots \oplus I_s\big) = n-1 = \dim_{\mathbb{F}_2} P.$$

Además $P \subseteq I_1 \oplus I_2 \oplus \cdots \oplus I_s$. En efecto, si $v \in P$, entonces del teorema 4.5(2) se sigue que $v = v_0 + v_1 + \cdots + v_s$ con $v_j \in I_j = \langle q_j \rangle$. Dado que para todo $j \neq 0$ se tiene que $x-1 \mid q_j(x)$, podemos afirmar que $\text{wt}(v_j)$ es par. Por lo tanto, como $\text{wt}(v)$ es par, se tiene que $\text{wt}(v_0) = \text{wt}\,\big(v - v_1 + \cdots + v_s\big)$ es par. Puesto que $x-1 \nmid q_0(x)$, se sigue que $v_0 = 0$. En consecuencia $v \in I_1 \oplus I_2 \oplus \cdots \oplus I_s$ y se tiene la afirmación. El resto se sigue del teorema 4.5(3). ☑

## 5. Códigos autoduales con un automorfismo de orden primo impar

Estudiar la estructura de un código binario autodual con un automorfismo de orden un primo impar resulta de gran importancia para la construcción de nuevos códigos autoduales. Los resultados presentados en esta sección son utilizados en el último capítulo para construir nuevos códigos optimales con parámetros $[120, 60, 20]$.

Sean $C$ un código binario de longitud $n$ y $\sigma \in \text{Aut}(C)$. Con $\Omega_1, \ldots, \Omega_c$ denotamos los $c$ ciclos de longitud $p$ y con $\Omega_{c+1}, \ldots, \Omega_{c+f}$ los $f$ puntos fijos.

**Definición 5.1.** Sean $C$ un $[n,k]$-código binario y $\sigma \in \mathrm{Aut}(C)$. Definimos

$$F_\sigma(C) \coloneqq \big\{v \in C : \sigma(v) = v\big\}$$

y

$$E_\sigma(C) \coloneqq \big\{v \in C : \mathrm{wt}(v \mid \Omega_i) \equiv 0 \pmod 2, \quad i = 1, \ldots, c+f\},$$

donde $v \mid \Omega_i$ es la restricción de $v$ sobre $\Omega_i$.

Note que $v \in F_\sigma(C)$ si y sólo si $v \in C$ y $v$ es constante sobre los ciclos de longitud $p$.

**Teorema 5.2.** *[9, Lemma 1] Sea $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$, donde $\big(\pi(v)\big)_i = v_j$ para $j \in \Omega_i$ e $i = 1, \ldots, c+f$. Entonces*

*(1) Si $C$ es código autodual, entonces $\pi\big(F_\sigma(C)\big)$ es un código autodual de longitud $n - c(p-1)$.*

*(2) Si $C$ es un código doblemente par y $p \equiv 1 \pmod 4$ o $f = 0$, entonces $\pi\big(F_\sigma(C)\big)$ es doblemente par.*

El siguiente lema será de gran utilidad para demostrar la descomposición de un código como suma directa de dos subespacios especiales.

**Lema 5.3.** *Sea $C$ un $[n,k]$-código binario con un automorfismo $\sigma$ de orden $p$ y polinomio enumerador de pesos $W_C(y) = \sum_i A_i y^i$. Si*

$$A_i^F \coloneqq \big|\{v \in C : v \in F_\sigma(C) \quad \text{y} \quad \mathrm{wt}(v) = i\}\big|,$$

*entonces $A_i \equiv A_i^F \pmod p$.*

***Demostración.*** Sabemos que $G = \langle\sigma\rangle$ actúa sobre $C$ y el número de elementos de sus órbitas está dado por:

$$\big|O(v)\big| = \begin{cases} 1, & \text{si } v \in F_\sigma(C); \\ p, & \text{si } v \notin F_\sigma(C). \end{cases}$$

Por lo tanto $C = F_\sigma(C) \cup C'$, donde $C'$ son los elementos de $C$ que no son fijados bajo $\sigma$. Entonces $A_i = A_i^F + pt$, para algún $t \in \mathbb{N}_0$. ☑

Sean $\sigma \in \mathrm{Aut}(C)$, $\pi_1$ el subcódigo de $\pi\big(F_\sigma(C)\big)$ que consta de todos los vectores que tienen sus soportes en las primeras $c$ coordenadas y $\pi_2$ el subcódigo de $\pi\big(F_\sigma(C)\big)$ que consta de todos los vectores que tienen sus soportes en las últimas $f$ coordenadas. Entonces $\pi\big(F_\sigma(C)\big)$ tiene una matriz generadora de la forma

$$\mathrm{gen}\left(\pi\big(F_\sigma(C)\big)\right) = \begin{bmatrix} A & O \\ O & B \\ D & E \end{bmatrix}, \tag{4}$$

donde $(A\,O)$ es una matriz generadora de $\pi_1$, $(O\,B)$ es una matriz generadora de $\pi_2$ y $O$ es la matriz nula de tamaño adecuado. Con esta observación tenemos el siguiente resultado

**Teorema 5.4.** *[10, Theorem 9.41] Si $k_1 = dim(\pi_1)$ y $k_2 = dim(\pi_2)$, entonces:*

*(1) (Principio del balance) $k_1 - \frac{c}{2} = k_2 - \frac{f}{2}$.*

*(2) $rank(D) = rank(E) = \frac{c+f}{2} - k_1 - k_2$.*

*(3) Sean $\mathcal{A}$ el código de longitud $c$ generado por $A$, $\mathcal{A}_D$ el código de longitud $c$ generado por $\binom{A}{D}$, $\mathcal{B}$ el código de longitud $f$ generado por $B$ y $\mathcal{B}_E$ el código de longitud $f$ generado por $\binom{B}{E}$. Entonces $\mathcal{A}^\perp = \mathcal{A}_D$ y $\mathcal{B}^\perp = \mathcal{B}_E$.*

**Definición 5.5.** Sea $p$ un número primo. Definimos

$$s(p) \coloneqq \text{mín}\{s \in \mathbb{N} : p \mid (2^s - 1)\}.$$

En [9], Huffman establece la siguiente descomposición de códigos binarios con un automorfismo de orden primo impar, la cual tiene múltiples aplicaciones en la construcción de códigos. Parte de las afirmaciones son un caso particular del teorema de Maschke [1, Chapter 5].

**Lema 5.6.** *[9, Lemma 2] Sea $C$ un $[n, k, d]$-código y $\sigma \in \text{Aut}(C)$. Entonces*

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

*(2) Si $C$ es un código autodual, entonces $\dim E_\sigma(C) = \frac{(p-1)c}{2}$. Además $s(p)$ divide la dimensión $E_\sigma(C)$.*

***Demostración.***

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

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

Dado que $\sum_{i=0}^{p-1} \sigma^i(v) \in C$, se sigue que $\sum_{i=0}^{p-1} \sigma^i(v) \in F_\sigma(C)$. Por otra parte, podemos ver que $w = \sum_{i=0}^{p} \sigma^i(v)$. Además para $i, k \in \{0, 1, \ldots, p\}$ se verifica que

$$\text{wt}\left(\sigma^i v \mid \Omega_j\right) = \text{wt}\left(\sigma^k v \mid \Omega_j\right).$$

En consecuencia

$$\text{wt}(\sigma^i v + \sigma^k v \mid \Omega_j) \equiv 0 \pmod 2.$$

Dado que la suma de vectores de peso par es par y $w$ es la suma de $\frac{p+1}{2}$ vectores de peso par, tenemos que

$$\operatorname{wt}\left(\sum_{i=0}^{p}\sigma^i(v)\mid\Omega_j\right)\equiv 0 \pmod 2$$

y se tiene que $w\in E_\sigma(C)$.

Por otra parte, si $v\in F_\sigma(C)\cap E_\sigma(C)$, entonces $v$ es constante y de peso par en cada ciclo de longitud $p$, por lo cual $v=0$.

(2) De la autodualidad de $C$ se sigue que $\dim(C)=\frac{n}{2}$. Por lo tanto

$$\begin{aligned}\dim E_\sigma(C)&=\tfrac{n}{2}-\dim F_\sigma(C)\\&=\tfrac{n}{2}-\dim\pi\big(F_\sigma(C)\big)\\&=\tfrac{n}{2}-\tfrac{c+f}{2}\\&=(p-1)\tfrac{c}{2}.\end{aligned}$$

Por otra parte, según vimos en la demostración del lema 5.3

$$|C|=\big|F_\sigma(C)\big|+pt,$$

para algún $t\in\mathbb{N}$. En consecuencia

$$2^{\dim C}-2^{\dim F_\sigma(C)}=pt,$$

para algún $t\in\mathbb{N}$. Entonces

$$2^{\dim F_\sigma(C)+\dim E_\sigma(C)}\equiv 2^{\dim F_\sigma(C)} \pmod p.$$

Finalmente se tiene que, $2^{\dim E_\sigma(C)}\equiv 1 \pmod p$. ☑

Es inmediato del teorema anterior que siempre podemos suponer que la matriz generadora de $C$ tiene la forma

$$\operatorname{gen}(C)=\begin{bmatrix}X & Y\\ Z & 0\end{bmatrix}\begin{matrix}\}\ \operatorname{gen}\big(F_\sigma(C)\big)\\ \}\ \operatorname{gen}\big(E_\sigma(C)\big)\end{matrix}.$$

En particular, si se conocen las matrices $\operatorname{gen}\big(F_\sigma(C)\big)$ y $\operatorname{gen}\big(E_\sigma(C)\big)$, entonces podemos encontrar el código $C$.

Con $E_\sigma(C)^*$ denotaremos el código que se obtiene de $E_\sigma(C)$ borrando las coordenadas correspondientes a los $f$ puntos fijos. Además definimos la función

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

mediante

$$\big(\varphi(v)\big)_i=v_0+v_1x+\cdots+v_{p-1}x^{p-1}\in P,$$

para $i=1,2,\ldots,c$ y $v\in E_\sigma(C)^*$ con

$$v\mid\Omega_i=(v_0,v_1,\ldots,v_{p-1}).$$

**Lema 5.7.** *[20]* $\varphi\big(E_\sigma(C)^*\big)$ *es un* $P$*-submódulo del* $P$*-módulo* $P^c$*.*

***Demostración.*** Claramente $\varphi\big(E_\sigma(C)^*\big)$ es cerrado bajo la suma. Probemos la cerradura para la multiplicación. Si $v \in E_\sigma(C)^*$, entonces $\sigma(v) \in E_\sigma(C)^*$. Además, del lema 4.6, se sigue que

$$\beta(x)\varphi\big(v(x)\big) = \varphi\big(\sigma(v)\big) \in \varphi\big(E_\sigma(C)^*\big).$$

Por otra parte, sabemos que $e(x)+\beta(x) = 1+x$. Entonces, si $p(x) \in P$, digamos $p(x) = (1+x)r(x)$ con $r(x) = a_0 + a_1x + \cdots + a_{p-1}x^{p-1}$, tenemos

$$\begin{aligned} p(x) &= a_0\big(e(x)+\beta(x)\big) + a_1\big(e(x)+\beta(x)\big)x + \cdots + a_{p-1}\big(e(x)+\beta(x)\big)x^{p-1} \\ &= a_0\big(e(x)+\beta(x)\big) + a_1\big(e(x)+\beta(x)\big)\beta(x) + \cdots + a_{p-1}\big(e(x)+\beta(x)\big)\beta^{p-1}(x) \\ &= a_0\big(e(x)+\beta(x)\big) + a_1\big(\beta(x)+\beta^2(x)\big) + \cdots + a_{p-1}\big(\beta^{p-1}(x)+\beta^p(x)\big). \end{aligned}$$

Es decir, todo $p(x) \in P$ es una combinación lineal de $\beta^0(x), \ldots, \beta^{p-1}(x)$. Entonces

$$p(x)\varphi(v) = \left(\sum_{i=0}^{p-1} a_i\beta^i(x)\varphi(v) \in \varphi\big(E_\sigma(C)^*\big)\right),$$

ya que $\beta(x)\varphi\big(v(x)\big) \in \varphi\big(E_\sigma(C)^*\big)$. ☑

El siguiente teorema suministra una herramienta para la construcción de un nuevo código a partir de la función $\varphi$.

**Teorema 5.8.** *[20] Sea* $1 + x + x^2 + \cdots + x^{p-1}$ *irreducible sobre* $\mathbb{F}_2[x]$ *y* $C$ *un código autodual. Entonces:*

*(1)* $\varphi\big(E_\sigma(C)^*\big)$ *es un* $\big[c, \frac{c}{2}\big]$*-código sobre el cuerpo* $P$*.*

*(2)* $c$ *es par.*

***Demostración.*** En este caso $P$ es un cuerpo con $|P| = 2^{p-1}$. Entonces del lema anterior se tiene que $\varphi\big(E_\sigma(C)^*\big)$ es un espacio vectorial sobre $P$. Dado que $C$ es un código autodual, se tiene que

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

Además, como espacio vectorial sobre $\mathbb{F}_2$,

$$E_\sigma(C)^* \cong E_\sigma(C) \cong \varphi\big(E_\sigma(C)^*\big).$$

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

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

de donde se sigue que $\dim_P \varphi\big(E_\sigma(C)^*\big) = \frac{c}{2}$. ☑

**Definición 5.9.**

(1) Una $p \times p$-matriz $A$ de la forma

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{p-1} \\ a_{p-1} & a_0 & a_1 & \dots & a_{p-2} \\ a_{p-2} & a_{p-1} & a_0 & \dots & a_{p-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}$$

se denomina *circulante*.

(2) Para $a(x) = a_0 + a_1 x + \cdots a_{p-1}x^{p-1}$ definimos

$$a(x^{-1}) \coloneqq a_0 + a_1 x^{p-1} + \cdots + a_{p-1}x.$$

En el siguiente lema se demuestra que $\mathbb{F}_2[x] \big/ \langle x^p - 1 \rangle$ es isomorfa, como álgebra, con la que tiene como conjunto subyacente las matrices circulantes de tamaño $p \times p$ sobre el cuerpo binario.

**Lema 5.10.** *El álgebra $\mathbb{F}_2[x] \big/ \langle x^p - 1 \rangle$ es isomorfa al álgebra $\mathcal{M}$ de las $p \times p$-matrices circulantes sobre el cuerpo $\mathbb{F}_2$.*

***Demostración.*** La función $\phi : \mathbb{F}_2[x] \big/ \langle x^p - 1 \rangle \longrightarrow \mathcal{M}$ definida por $\phi\big(a(x)\big) = A$, donde $a(x) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}$ y

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{p-1} \\ a_{p-1} & a_0 & \dots & a_{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix},$$

es un isomorfismo de álgebras. ☑

La demostración del siguiente lema es inmediata.

**Lema 5.11.**

*(1) Si $A = \phi\big(a(x)\big)$ es una matriz circulante, entonces $A^t$ también lo es y $\phi\big(a(x^{-1})\big) = A^t$.*

*(2) En una matriz $A$ cada dos filas son ortogonales, si y sólo si, $AA^t = 0$.*

*(3) Sean $A = \big[A_1|A_2|\cdots|A_c\big]$ y $B = \big[B_1|B_2|\cdots|B_c\big]$ matrices celdadas, con $A_j, B_j \in \mathrm{M}_p(\mathbb{F}_2)$, para cada $j = 1, \dots, c$. Entonces cada fila de $A$ es ortogonal a cada fila de $B$, si y sólo si, $A_1B_1^t + \cdots + A_cB_c^t = 0$.*

**Definición 5.12.** Sean $x, y \in \mathbb{F}_2^n$. Definimos $x \cap y$ como el vector de $\mathbb{F}_2^n$ que consiste de unos en las coordenadas $i \in \operatorname{sop}(x) \cap \operatorname{sop}(y)$.

Un resultado inmediato es que si $x, y \in \mathbb{F}_2^n$ entonces

$$\operatorname{wt}(x \cap y) \equiv xy \pmod 2. \tag{5}$$

**Teorema 5.13** (V. Y. Yorgov)**.** *[20] Sean $C$ un código binario y $\sigma \in \operatorname{Aut}(C)$ de la forma* (1)*. Entonces $C$ es un código auto-ortogonal ($C \subseteq C^{\perp}$) si y sólo si:*

*(1) $\pi\big(F_\sigma(C)\big)$ es un código binario auto-ortogonal.*

*(2) Si $\big(a_1(x), \ldots, a_c(x)\big)$, $\big(b_1(x), \ldots, b_c(x)\big) \in \varphi\big(E_\sigma(C)^*\big)$, entonces*

$$a_1(x)b_1\big(x^{-1}\big) + \cdots + a_c(x)b_c\big(x^{-1}\big) = 0.$$

***Demostración.*** Sea $C$ un código auto-ortogonal. Entonces (1), se sigue del teorema 5.2(1).

Por otra parte, del lema 5.10 se sigue que los elementos $\big(a_1(x), \ldots, a_c(x)\big)$ y $\big(b_1(x), \ldots, b_c(x)\big)$ de $\varphi\big(E_\sigma(C)^*\big)$ están en correspondencia con las matrices celdadas $A = \big[A_1|A_2|\ldots|A_c\big]$ y $B = \big[B_1|B_2|\ldots|B_c\big]$ con celdas $A_i = \phi\big(a_i(x)\big)$ y $B_i = \phi\big(b_i(x)\big)$ son matrices circulantes de tamaño $p \times p$. Las primeras filas de $A$ y $B$ son vectores de $E_\sigma(C)^*$. Puesto que las otras filas se obtienen por una traslación, es decir, por acción de $\sigma$ y $\sigma \in \operatorname{Aut}(C)$, entonces todas las filas de $A$ y $B$ son elementos de $E_\sigma(C)^*$. En consecuencia toda fila de $A$ es ortogonal a toda fila de $B$. Entonces por el lema 5.11 tenemos

$$\begin{aligned} 0 &= A_1B_1^t + \cdots + A_cB_c^t \\ &= \phi\big(a_1(x)\big)\phi\big(b_1\big(x^{-1}\big)\big) + \cdots + \phi\big(a_c(x)\big)\phi\big(b_c\big(x^{-1}\big)\big), \end{aligned}$$

de donde

$$a_1(x)b_1\big(x^{-1}\big) + a_2(x)b_2\big(x^{-1}\big) + \cdots + a_c(x)b_c\big(x^{-1}\big) = 0.$$

Recíprocamente, supongamos que se cumplen (1) y (2). Del lema 5.6 se sigue que que $C = F_\sigma(C) \oplus E_\sigma(C)$. Para probar que $C$ es un código auto-ortogonal, demostremos que $u \bullet v = 0$ para todo $u \in F_\sigma(C)$, $v \in E_\sigma(C)$ y además que $F_\sigma(C)$, y $E_\sigma(C)$ son auto-ortogonales. Sean $u \in F_\sigma(C)$ y $v \in E_\sigma(C)$. Dado que el vector $u|_{\Omega_i}$ consiste solo de ceros o unos y para $i = 1, \ldots, c + f$ se verifica que

$$\operatorname{wt}(v_{\Omega_i}) \equiv 0 \pmod 2,$$

se tiene que

$$\operatorname{wt}(u|_{\Omega_i} \cap v|_{\Omega_i}) \equiv 0 \pmod 2.$$

De la ecuación (5) en los preliminares tenemos que

$$u|_{\Omega_i} \bullet v|_{\Omega_i} \equiv \mathrm{wt}\left(u|_{\Omega_i} \cap v|_{\Omega_i}\right) \pmod 2.$$

En consecuencia $u \bullet v = 0$.

Por otra parte, la condición (1) implica que $F_\sigma(C)$ es un código auto-ortogonal. Sean ahora $u, v \in E_\sigma(C)^*$ tales que $\varphi(u) = \big(a_1(x), \ldots, a_n(x)\big)$ y $\varphi(v) = \big(b_1(x), \ldots, b_n(x)\big)$. De la condición (2) se tiene que

$$a_1(x)b_1\big(x^{-1}\big) + a_2(x)b_2\big(x^{-1}\big) + \cdots + a_c(x)b_c\big(x^{-1}\big) = 0.$$

Entonces

$$\begin{aligned} 0 &= \phi\big(a_1(x)\big)\phi\big(b_1\big(x^{-1}\big)\big) + \cdots + \phi\big(a_c(x)\big)\phi\big(b_c\big(x^{-1}\big)\big) \\ &= \phi\big(a_1(x)\big)\phi\big(b_1(x)\big)^t + \cdots + \phi\big(a_c(x)\big)\phi\big(b_c(x)\big)^t. \end{aligned}$$

Si $A = \big[A_1|A_2|\ldots|A_c\big]$ y $B = \big[B_1|B_2|\ldots|B_c\big]$ donde $A_i = \phi\big(a(x)\big)$ y $B_i = \phi\big(b(x)\big)$, entonces por el lema 5.11(3), cada fila de $A$ es ortogonal a cada fila de $B$. Ahora, dado que $u$ y $v$ son respectivamente, las primeras filas de $A$ y $B$, entonces $u \bullet v = 0$. Es decir, $E_\sigma(C)^*$ es auto-ortogonal y en consecuencia, $E_\sigma(C)$ también lo es. ☑

El siguiente teorema establece condiciones necesarias y suficientes para que un código binario con un automorfismo de orden primo impar sea autodual.

**Teorema 5.14** (W. C. Huffman & V. Y. Yorgov)**.** *[20, Theorem 3] Sea $s(p) = p - 1$. Entonces $C$ es un código binario autodual con un automorfismo $\sigma$ de orden $p$ si y sólo si se verifican las siguientes dos condiciones*

*(1) $\pi\big(F_\sigma(C)\big)$ es un código binario autodual de longitud $c + f$.*

*(2) $\varphi\big(E_\sigma(C)^*\big)$ es un código binario autodual sobre $P$, bajo el producto escalar $u \bullet v \coloneqq \sum_{i=0}^{c} u_i v_i^r$, con $r = 2^{\frac{p-1}{2}}$, $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in P^c$.*

***Demostración.*** Inicialmente note que, si $s(p) = p - 1$, entonces el polinomio $1 + x + x^2 + \cdots + x^{p-1}$ es irreducible en $\mathbb{F}_2[x]$ y por ello $P$ es un cuerpo con $|P| = 2^{p-1}$. Además dado que $s(p) = p - 1$, se tiene que el orden de 2 módulo $p$ es $p - 1$, de donde

$$2^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Por lo tanto $a\big(x^{-1}\big) = a(x^r)$, donde $r = 2^{\frac{p-1}{2}}$. Puesto que la característica del cuerpo es 2, entonces $a(x)^r = a(x^r) = a\big(x^{-1}\big)$, para toda $a(x) \in P$.

Para demostrar (1) y (2), supongamos que $C$ es autodual y demostramos (1) y (2). Del teorema 5.2(1) se tiene que $\pi\big(F_\sigma(C)\big)$ es un código autodual. Por

otra parte, del teorema 5.8 se sabe que $\varphi\big(E_\sigma(C)^*\big)$ es un $[c, \frac{c}{2}]$-código sobre $P$. Probemos entonces que $\varphi\big(E_\sigma(C)^*\big)$ es autodual bajo el producto interior definido por

$$u \bullet v \coloneqq \sum_{i=0}^{c} u_i v_i^{2^{\frac{p-1}{2}}},$$

donde $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in \varphi\big(E_\sigma(C)^*\big)$. Del teorema 5.13(2) se tiene que

$$\begin{aligned} 0 &= u_1(x)v_1\big(x^{-1}\big) + u_2(x)v_2\big(x^{-1}\big) + \cdots + u_c(x)v_c\big(x^{-1}\big) \\ &= u_1(x)v_1(x)^r + u_2(x)v_2(x)^r + \cdots + u_c(x)v_c(x)^r; \end{aligned}$$

es decir, $\varphi\big(E_\sigma(C)^*\big) \subseteq \varphi\big(E_\sigma(C)^*\big)^\perp$. Note que

$$\dim_P \varphi\big(E_\sigma(C)^*\big)^\perp = c - \dim_P \varphi\big(E_\sigma(C)^*\big) = c - \frac{c}{2} = \dim_P \varphi\big(E_\sigma(C)^*\big).$$

Por lo tanto $\varphi\big(E_\sigma(C)^*\big) = \varphi\big(E_\sigma(C)^*\big)^\perp$.

Recíprocamente, supongamos que se satisfacen (1) y (2). Entonces se tiene que $\dim_{\mathbb{F}_2} \pi\big(F_\sigma(C)\big) = \frac{c+f}{2}$ y $\dim_P \varphi\big(E_\sigma(C)^*\big) = \frac{c}{2}$, con lo cual

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

Además $\dim_{\mathbb{F}_2} E_\sigma(C) = \dim_{\mathbb{F}_2} \varphi\big(E_\sigma(C)^*\big) = (p-1)\frac{c}{2}$. Por lo tanto, dado que $C = F_\sigma(C) \oplus E_\sigma(C)$ se sigue que

$$\dim_{\mathbb{F}_2} C = \tfrac{(c+f)}{2} + \tfrac{c(p-1)}{2} = \tfrac{(cp+f)}{2} = \tfrac{n}{2}.$$

Finalmente, el hecho que $C = C^\perp$ se sigue del teorema 5.13. ☑

## 6. Aplicaciones

**Ejemplo 6.1.** La existencia de un código binario autodual $C$ con parámetros $[96, 48, 20]$ es aún un problema abierto. En [14] J. De la Cruz y W. Willems demostraron que un automorfismo $\sigma$ de $C$ con orden 3 sólo puede ser de tipo 3-$(32; 0)$ o 3-$(30; 6)$. Si los automorfismos de este orden carecieran de puntos fijos, entonces sería más fácil estudiar la estructura del grupo de automorfismos. Lamentablemente no se ha podido excluir el tipo 3-$(30; 6)$.

En este ejemplo vemos cómo, usando algunos de los resultados establecidos en las secciones anteriores, podemos determinar el polinomio enumerador de pesos del subcódigo fijo $F_\sigma(C)$ si $\sigma \in \mathrm{Aut}(C)$ es de tipo 3-$(30; 6)$. En este caso $\pi\big(F_\sigma(C)\big)$ es un $[36, 18, d]$-código autodual.

Del teorema 2.1 se sigue que $d \leq 8$. Si escribimos $d = x + y$, donde $x$ es el número de unos en las primeras $c$ coordenadas de los vectores con peso

mínimo y $y$ el número de unos en las últimas coordenadas, entonces $x+y \leq 8$ y $3x+y \geq 20$. Esto lleva a que $x \geq 6$, $y = 0$ y $d = 8$. Por lo tanto $\pi\big(F_\sigma(C)\big)$ es un $[36, 18, 8]$-código binario autodual. Usando [6] se tiene que existen dos posibles polinomios enumeradores de pesos para $\pi\big(F_\sigma(C)\big)$:

$$W_1(y) = 1 + 225y^8 + 2016y^{10} + \cdots$$

y

$$W_2(y) = 1 + 289y^8 + 1632y^{10} + \cdots$$

Consideremos una matriz generadora de $\pi\big(F_\sigma(C)\big)$ de la forma (4). Puesto $f = 6 < 20$, entonces $k_2 = 0$. Del teorema 5.4, usando el principio del balance, tenemos que $k_1 = 12$. Entonces

$$\operatorname{gen}\big(\pi\big(F_\sigma(C)\big)\big) = \begin{bmatrix} A & 0 \\ D & E \end{bmatrix}.$$

Note que el código $\mathcal{A}$ generado por la matriz $A$ es un código binario doblemente par con parámetros $[30, 12, d_1]$, donde $d_1 = 8$ o $d_1 = 12$.

Si la distancia mínima $d_1^\perp$ del correspondiente código dual satisface $d_1^\perp \leq 4$, entonces se tiene que

$$\operatorname{wt}\big(\pi^{-1}(a|b)\big) \leq 12 + \operatorname{wt}(b) \leq 12 + 6 < 20,$$

para un vector $(a|b) \in \pi\big(F_\sigma(C)\big)$, lo cual es una contradicción. Por lo tanto $d_1^\perp \geq 5$. Por otra parte las tablas de [8] muestran que la distancia mínima de cualquier $[30, 18]$-código binario es a lo mas 6. En consecuencia $d_1^\perp = 5$ o $d_1^\perp = 6$. Se puede demostrar que $d_1^\perp = 5$ y que

$$W_{\mathcal{A}}(y) = 1 + 75y^8 + 1360y^{12} + 2175y^{16} + 480y^{20} + 5y^{24}$$

y

$$W_{\mathcal{A}^\perp}(y) = 1 + 36y^5 + 155y^6 + 600y^7 + 1425y^8 + 2580y^9 + \cdots$$

Sean $W_{F_\sigma(C)}(y) = \sum_i A_i^F y^i$ y $W_{\pi(F_\sigma(C))}(y) = \sum_i A_i^\pi y^i$. Sea además $\{T_1, T_2\}$ una partición de $\{1, \ldots, 36\}$, donde $T_1 = \{1, \ldots, 30\}$ y $T_2 = \{31, \ldots, 36\}$.

Sea $\big(\big(A_{\mathbf{i}}(T)\big)\big)_{\mathbf{i} \in W(T)}$ la distribución dividida de pesos del código $\pi\big(F_\sigma(C)\big)$, donde (ver definición 2.5),

$$A_{\mathbf{i}} = A_{(x,y)} = \big|\{(v|u) \in \pi\big(F_\sigma(C)\big) : \operatorname{wt}(v) = x \quad \text{y} \quad \operatorname{wt}(u) = y\}\big|.$$

Entonces $A_{20}^F = A_{(5,5)} + A_{(6,2)}$ y $A_8^\pi = A_{(6,2)} + A_{(8,0)}$. Por lo tanto

$$A_{20}^F = A_{(5,5)} + \big(A_8^\pi - A_{(8,0)}\big) = \begin{cases} 36 + (225 - 75) = 186 \equiv 0 \pmod 3 \\ 36 + (289 - 75) = 250 \equiv 1 \pmod 3. \end{cases}$$

Del lema 5.3 se sigue que

$$A_{20} \equiv A_{20}^{F} \pmod 3$$

y en [16] se demostró que

$$A_{20} = 3217056 \equiv 0 \pmod 3.$$

Por lo tanto

$$W_{\pi(F_\sigma(C))}(y) = W_1(y).$$

En consecuencia $A_{20}^{F} = 186$ y se tiene que

$$W_{F_\sigma(C)}(y) = 186y^{20} + 680y^{24} + 2730y^{28} + 8040y^{32} + 18640y^{36} + 30600y^{40} + 11160y^{44} + 49295y^{48} + \cdots$$

**Ejemplo 6.2.** Un problema interesante es el estudio de la estructura del grupo de automorfismos de un código extremal $C$ de longitud 96. En [9], [4] y [5] fue demostrado que para las longitudes $n = 48, 72, 120$ un elemento de orden 3 carece de puntos fijos. Como se mencionó en el ejemplo anterior para $n = 96$ no ha podido establecerse aun esa afirmación.

En [14] se demostró que si $C$ es un $[96, 48, 20]$-código binario autodual y $G$ su grupo de automorfismos, entonces los únicos primos que pueden dividir a $|G|$ son 2, 3 y 5. Si suponemos que los elementos de orden 3 carecen de puntos fijos, entonces todo elemento $\sigma \in G$ de orden primo es de tipo 2-$(48; 0)$, 3-$(32; 0)$ o 5-$(18; 6)$. Por lo tanto $|G| = 2^a 3^b 5^c$, con $a, b, c \in \mathbb{N}_0$.

Del teorema 3.6 se sigue que $3^2 \nmid |G|$ y por lo tanto $b \in \{0, 1\}$. Además por el lema 3.7 se tiene que $a \in \{0, \ldots, 5\}$. Por otra parte, si $|G| = 2^a 3^b 5$, con $a \in \{0, \ldots, 5\}$ y $b \in \{0, 1\}$, entonces

$$\big|O(x)\big| = \begin{cases} 2^a 3^b 5; \\ 2^a 3^b, \end{cases} \tag{6}$$

para todo $x \in \{1, \ldots, 96\}$, ya que $\big|O(x)\big| = |G : G_x|$ y los automorfismos no triviales con puntos fijos tienen orden 5, lo cual implica que $|G_x| = 1$ o $|G_x| = 5$.

En [14] se probó el siguiente lema del cual nosotros presentaremos ahora una demostración diferente usando ciertos resultados de la sección 2.

**Lema 6.3.** *Sea $\tau \in G$ de orden 5. Si $15 \mid |G|$ y $3 \nmid |N_G(\tau)|$, entonces $|G| = 60$. En particular* Alt(5) *es el único grupo de automorfismos que puede ocurrir.*

***Demostración.*** Del lema 3.8 se sigue que $2^3 \nmid |N_G(\tau)|$. Además en [14] se probó que $|N_G(\tau)| = 2^x \bullet 5$, donde $0 \leq x \leq 2$. Puesto que $\langle \tau \rangle \in \mathrm{Syl}_5(G)$, se tiene que

$$|\,\mathrm{Syl}_5(G)| = |G : N_G(\tau)| = \frac{2^a \bullet 3 \bullet 5}{2^x \bullet 5} = 2^{a-x} \bullet 3 \equiv 1 \pmod 5.$$

Las únicas posibilidades para $(a, x)$ son

$$(1,0),(2,1),(3,2),(5,0).$$

Además el número de órbitas es

$$t = \frac{1}{|G|}\big(96 + \big|\operatorname{Syl}_5(G)\big|\bullet 4\bullet 6\big).$$

En el último caso ($a = 5$ y $x = 0$) tenemos $|G| = 32\bullet 15 = 480$ y $G$ tiene exactamente 96 5-subgrupos de Sylow. Entonces el número de órbitas es

$$t = \frac{1}{480}(96 + 96\bullet 4\bullet 6) = 5.$$

De (6) tenemos que las órbitas de $G$ tienen longitud $2^a\bullet 3 = 96$. Esto contradice el hecho de que $t = 5$.

En los otros casos $\big|\operatorname{Syl}_5(G)\big| = 6$. Por lo tanto el número de órbitas es

$$t = \frac{1}{2^a\bullet 3\bullet 5}(96 + 6\bullet 4\bullet 6) = \frac{2^4}{2^a}.$$

En el caso $a = 3$ se tiene que $t = 2$, lo cual tampoco es posible ya que las órbitas de $G$, con base en (6) tienen longitud $2^a \cdot 3 = 24$.

Si $a = 2$, entonces se tiene que $|G| = 60$. Se sabe que Alt(5) es el único grupo $U$ de orden 60 con $\big|\operatorname{Syl}_5(U)\big| = 6$.

Si $a = 1$, entonces $|G| = 30 = 2\bullet 3\bullet 5$ y $\big|\operatorname{Syl}_5(G)\big| = 6$, lo cual contradice el lema 3.4. ☑

**Ejemplo 6.4.** Aunque la existencia de un código binario extremal $C$ con parámetros $[120, 60, 24]$ es desconocida, en este ejemplo utilizamos algunos resultados de A. M. Gleason para determinar su polinomio enumerador de pesos.

Sea

$$A(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i \in \mathbb{Z}[x,y]$$

el polinomio enumerador de pesos homogéneo de $C$. Dado que $d = 24$, se tiene que $A_1, \ldots, A_{23} = 0$. Además, si $4 \nmid A_i$, entonces $A_i = 0$. Por otra parte, puesto que $C$ es autodual, se tiene que $A_i = A_{120-i}$, para todo $i = 0, \ldots, 120$.

Sean ahora $r \coloneqq x^8 + 14x^4y^4 + y^8$ y $s \coloneqq x^4y^4\big(x^4 - y^4\big)^4$. Del teorema 2.3 se tiene que

$$A(x,y) = ar^{15} + br^{12}s + cr^9s^2 + dr^6s^3 + er^3s^4 + fs^5,$$

de donde se sigue que

$$\begin{aligned} A(y) &= A_0 + A_{24}y^{24} + A_{28}y^{28} + \cdots \\ &= a + (210a + b)y^4 + (20595a + 164b + c)y^8 + \cdots + \\ &(38263749615a + 358399128b + 3228646c + 25272d + 39e - 20f)y^{24} + \cdots \end{aligned}$$

Igualando los coeficientes tenemos el siguiente sistema de ecuaciones

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 210 & 1 & 0 & 0 & 0 & 0 \\ 20595 & 164 & 1 & 0 & 0 & 0 \\ 1251460 & 12282 & 118 & 1 & 0 & 0 \\ 52705485 & 554740 & 6085 & 72 & 1 & 0 \\ 1630086822 & 16800251 & 178456 & 2004 & 26 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

el cual tiene como solución el vector

$$(a, b, c, d, e, f) = (1, -210, 13845, -305950, 1571490, -492372).$$

Un cálculo sencillo lleva a que

$$\begin{aligned} A_0 = A_{120} &= 1 \\ A_{24} = A_{96} &= 39703755 \\ A_{28} = A_{92} &= 6101289120 \\ A_{32} = A_{88} &= 475644139425 \\ A_{36} = A_{84} &= 18824510698240 \\ A_{40} = A_{80} &= 397450513031544 \\ A_{44} = A_{76} &= 4630512364732800 \\ A_{48} = A_{72} &= 30531599026535880 \\ A_{52} = A_{68} &= 116023977311397120 \\ A_{56} = A_{64} &= 257257766776517715 \\ A_{60} &= 335200280030755776. \end{aligned}$$

**Ejemplo 6.5.** Si $C$ es un código binario autodual de longitud 120, entonces su distancia mínima $d$ es menor o igual que 24. En [21] fueron construidos 26 códigos autoduales no equivalentes con parámetros $[120, 60, 20]$ y con un automorfismo de orden 23.

Nosotros construimos 24 nuevos códigos no equivalentes con parámetros $[120, 60, 20]$ y con un automorfismo de orden 59. Utilizando nuevamente el teorema 2.3 encontramos que el polinomio enumerador de pesos de un $[120, 60, 20]$-código binario autodual doblemente par está dado por

$$W_C(1, y) = 1 + (492372 + \beta)y^{20} + (29856315 - 20\beta)y^{24} + \cdots$$

con $\beta \in \mathbb{Z}$.

**Teorema 6.6.** *Existen por lo menos* 24 *códigos autoduales doblemente pares con parámetros* $[120, 60, 20]$ *y con un automorfismo* $\sigma$ *de orden* 59.

***Demostración.*** Sea $C$ un código autodual de longitud 120 con distancia mínima 24 y con un automorfismo $\sigma$ de orden 59. Del teorema 5.14 se sigue que el código $\pi\big(F_\sigma(C)\big)$ es auto dual con parámetros $[4, 2, 2]$. Por lo tanto

$$\operatorname{gen}\big(\pi\big(F_\sigma(C)\big)\big) = \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right].$$

Consecuentemente

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

donde $\mathbf{1}$ es el vector de solo unos, $\mathbf{0}$ el vector de solo ceros de longitud 59. Del teorema 5.8 se sigue que $\varphi\big(E_\sigma(C)^*\big)$ es un $[2, 1]$-código sobre el cuerpo $P$. En [13] se demostró que su matriz generadora está dada por

$$\operatorname{gen}\big(\varphi\big(E_\sigma(C)^*\big)\big) = \Big(e(x)\alpha(x)^{t\left(2^{29}-1\right)}\Big),$$

donde $e(x) = x + x^2 + \cdots + x^{58}$ es el elemento identidad del cuerpo $P$, $\alpha(x)$ es un elemento primitivo del cuerpo $P$ y $t$ recorre un conjunto de representantes de 156889 órbitas ciclotómicas. Usando el lema 5.6, se tiene que la matriz generadora del código $C$ es de la forma

$$\operatorname{gen}(C) = \left[\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 0 & 1 \\ \hline [e(x)] & [\alpha(x)^{t(2^{29}-1)}] & 0 & 0 \end{array}\right].$$

Los cálculos fueron realizados con el software *Magma computational algebra system* tomando como elemento primitivo

$$\alpha(x) = x^{55}+x^{51}+x^{50}+x^{48}+x^{42}+x^{39}+x^{35}+x^{29}+x^{23}+x^{20}+x^{10}+x^9+x^3+x$$

y, aunque no es posible encontrar un código extremal, se tiene 24 nuevos códigos con distancia mínima 20, para algunos parámetros $t$ como se muestra en la siguiente tabla. ☑

| $t$ | $A_{20}$ | $\beta$ | $t$ | $A_{20}$ | $\beta$ |
|---|---|---|---|---|---|
| 51 | 103368 | -389004 | 8317 | 97704 | -394668 |
| 63 | 107616 | -384756 | 8811 | 96996 | -395376 |
| 103 | 96642 | -395730 | 203425 | 104784 | -387588 |
| 181 | 99828 | -392544 | 203731 | 102306 | -390066 |
| 287 | 107262 | -385110 | 203801 | 103014 | -389358 |
| 361 | 106908 | -385464 | 203805 | 91686 | -400686 |
| 665 | 101244 | -391128 | 396325 | 103722 | -388650 |
| 681 | 98058 | -394314 | 397141 | 105138 | -387234 |
| 779 | 100536 | -391836 | 397397 | 101952 | -390420 |
| 7503 | 100890 | -391482 | 400309 | 102660 | -389712 |
| 7521 | 101598 | -390774 | 789641 | 98412 | -393960 |
| 7607 | 99474 | -392898 | 8357499 | 105020 | -387352 |

TABLA 1. $[120, 60, 20]$-códigos de tipo II con un automorfismo de orden 59.

## Referencias


[1] J. L. Alperin and R. B. Bell, *Groups and Representations*, 2 ed., Springer-Verlag, New York, USA, 1995.

[2] E. F. Assmus, H. F. Mattson, and R. Turyn, *Research to Develop the Algebraic Theory of Codes*, Air force Cambridge Res. Lab., Bedford, MA, Report **AFCRL-67-0365** (1967), I1–XI4.

[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, *On the Automorphism Group of a Doubly-Even* $(72, 32, 16)$ *Code*, IEEE Transactions on Information Theory **50** (2004), 544–547.

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

[6] J. H. Conway and N. J. A. Sloane, *A New Upper Bound on the Minimal Distance of Self-Dual Codes*, IEEE Transactions on Information Theory **36** (1990), no. 6.

[7] A. M. Gleason, *Weight Polynomials of Codes and the MacWilliams Identities*, Actes Congrès Intern. de Math. Gauthier-Villars, Paris **3** (1971), 211–215.

[8] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*, http://www.codetables.de.

[9] W. C. Huffman, *Automorphisms of Codes with Applications to Extremal Doubly Even Codes of Length* 48, IEEE Transactions on Information Theory **28** (1982), 511–521.

[10] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, UK, 2003.

[11] I. M. Isaacs, *Finite Group Theory*, vol. 92, AMS, Providence, Graduate Studies in Math, 2008.

[12] J. De la Cruz, *Über die Automorphismengruppe der Extremaler Codes der Längen 96 Und 120*, Ph.d. dissertation, Otto-von-Guericke Universität, Magdeburg - Germany, 2012.

[13] ———, *On Extremal Self-Dual Codes of Length 120*, Design, Codes and Cryptography (2013), (to appear).

[14] 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.

[15] X. Ma, *Nonexistence of Extremal Doubly Even Self-Dual Codes With Large Length*, Discrete Math. **185** (1998), 265–274.

[16] C. L. Mallows and N. J. A. Sloane, *An Upper Bound for Self-Dual Codes*, Information and Control **22** (1973), 188–200.

[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] V. Yorgov and D. Yorgov, *The Automorphism Group of a Self Dual Binary* $[72, 36, 16]$ *Code does not Contain* $\mathrm{Z}_4$, preprint, arXiv:1310.2570v2, Nov 2013.

[20] V. Y. Yorgov, *Binary Self-Dual Codes with Automorphisms of Odd Order*, Probl. Pered. Inform. **19** (1983), 11–24.

[21] R. Yorgova and A. Wassermann, *Binary Self-Dual Codes with Automorphisms of Order* 23, Des. Codes and Cryptography **48** (2008), 155–164.

[22] S. Zhang, *On the Nonexistence of Extremal Self-Dual Codes*, Discrete Appl. Math. **91** (1999), 277–286.

(Recibido en octubre de 2013. Aceptado en junio de 2014)

Departamento de Matemáticas y Estadística
División de Ciencias Básicas
Universidad del Norte
Km 5 vía a Puerto Colombia
Barranquilla, Colombia
*e-mail:* jdelacruz@uninorte.edu.co
*e-mail:* isgutier@uninorte.edu.co

Departamento de Matemáticas
Facultad de Ciencias
Universidad del Atlántico
Km 7 vía a Puerto Colombia
Barranquilla, Colombia
*e-mail:* jorgerobinson@mail.uniatlantico.edu.co

Esta página aparece intencionalmente en blanco