Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 31, No. 2, 2013, pág. 107–120

On authomorphisms of extremal type II codes

Ismael Gutiérrez García[a]*, Darwin Villar Salinas[b]

[a] Universidad del Norte, Departamento de Matemátcias y Estadística, Barranquilla, Colombia.

[b] RWTH-Aachen University, Department of Mathematics, Aachen, Germany.

Abstract. In this article we present some techniques to determine the types of automorphisms of extremal doubly even binary self-dual codes, also called extremal type II codes, with parameters $[24, 12, 8]$, $[48, 24, 12]$ and $[120, 60, 24]$. We aim to obtain information about the automorphism group considering the exclusion of some prime numbers from its order.
Keywords: Binary codes, self-dual codes, doubly even codes, extremal codes and automorphisms of codes.
MSC2010: 11T71, 20B25, 94B60.

Sobre automorfismos de códigos extremales de tipo II

Resumen. En el presente artículo se muestran algunas técnicas para obtener tipos de automorfismos de los códigos binarios auto-duales, doblemente pares y extremales, también denominados extremales de tipo II, con parámetros $[24, 12, 8]$, $[48, 24, 12]$ y $[120, 60, 24]$. El objetivo central es obtener información sobre el correspondiente grupo de automorfismos a partir de la exclusión de algunos números primos de su orden.
Palabras claves: Códigos binarios, códigos auto-duales, códigos doblemente pares, códigos extremales, automorfismos de códigos.

1. Introduction

Extremal binary doubly even self-dual codes are one of the most outstanding areas of study in the classical theory of algebraic codes. To mention a few of them we have the $[8, 4, 4]$-Hamming code, the $[24, 12, 8]$-Golay code and the $[48, 24, 12]$-code, fully characterized, which correspond to a cyclic quadratic residue code (QR-code), up to equivalence. Mallows and Sloane proved in [14] that for large lengths such codes don't exist. Nevertheless an explicit upper bound was not established. Later Rains showed in [16] that any extremal binary self-dual code C, with length a multiple of 24, is also a doubly even code. It is then of special interest to study extremal binary doubly even self-dual codes with parameters $[24m, 12m, 4m+4]$, $m \in \mathbb{N}$. The best upper bound for the length of this

*Corresponding author: *E-mail*: isgutier@uninorte.edu.co.
Received: 16 April 2013, Accepted: 02 September 2013.

kind of codes, though somehow loose, was determined by Zhang [19] in 1999. He proved that extremal binary doubly even self-dual codes C of length $24m$ don't exist if $m > 153$.

If $m = 3, 4$ or m=5, then we get extremal binary doubly even self-dual codes with parameters $[72, 36, 16]$, $[96, 48, 20]$ or $[120, 60, 24]$, respectively. The existence of these codes is a longstanding open problem [17].

Another interesting problem in this context is the characterization of the automorphism group of the codes given C of length n. A permutation of degree n, let us say σ, is an automorphism of C if its action over a vector in C is also in the code. This is, C is invariant under the action of σ. The set of such permutations with the composition forms a group, that we will denote by $\mathrm{Aut}(C)$.

In general the results that provide information about the automorphism group of an extremal binary doubly even self-dual code are very restrictive. For instance, the automorphism group of the Hamming codes with dimension $n - k$ is $\mathrm{GL}(k, \mathbb{F}_q)$, the general linear group over $\mathbb{F}_q$.

The $[24, 12, 8]$-Golay-code has the sporadic simple Mathieu-group M_{24} as its automorphism group [12, Ch. 20, Corollary 5] and finally the extended quadratic residue $[48, 24, 12]$-code has the projective special linear group $\mathrm{PSL}(2, 23)$ [11, Theorem 6].

The next case is $m = 3$; this yields C the binary self-dual $[72, 36, 16]$-code. It has been proved in [6] and [15] that its automorphism group has order at most 36. In particular, the automorphism group is solvable. Furthermore Bouyuklieva, O'Brien, Willems [6] and Borello [3] proved that the only primes that can divide $|\mathrm{Aut}(C)|$ are 2, 3 and 5. Recently Borello [2] proved that $|\mathrm{Aut}(C)|$ if non-trivial, has no element of order 6. Finally the same author, Dalla Volta and Nebe proved in [4] that the automorphism group of C does not contain either the symmetric group of degree 3, the alternating group of degree 4 or the dihedral group of order 8.

For $m = 4$, C is a binary self-dual $[96, 48, 20]$-code; it is known that only the primes 2, 3 and 5 can divide $|\mathrm{Aut}(C)|$, see [8], [7].

And if $m = 5$ we have a binary self-dual $[120, 60, 24]$-code. De la Cruz, et al. [5] showed that in a putative binary self-dual $[120, 60, 24]$ code C an automorphism of order 3 has not fixed points, $|\mathrm{Aut}(C)| \leq 920$ and $\mathrm{Aut}(C)$ is solvable if it contains an element of prime order $p \geq 7$. Moreover, the alternating group of degree 5 is the only non-abelian composition factor which may occur in $\mathrm{Aut}(C)$.

In this paper we give a general idea of some of the techniques used to analyze extremal binary self-dual codes with small parameters, which we then apply to the codes for $m = 1, 2$ and 5. So we obtain a characterization of the automorphism groups for the first two cases and reducing the list of primes that can divide the order of $\mathrm{Aut}(C)$ for the later case.

2. Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements and $n \in \mathbb{N}$. A k-dimensional subspace C of $\mathbb{F}_q^n$ is called a $[n, k]$-**lineal code** over $\mathbb{F}_q$. The elements of C are **codewords**, and if $q = 2$ or $q = 3$ we say that C is a **binary code** or **ternary**, respectively. The parameter n is called the length of C.

For $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ we define

$$\mathrm{d}(x, y) := |\{j \mid 1 \leq j \leq n,\ x_j \neq y_j\}|;$$

d is called the **Hamming** distance between x and y. It can be easily verified that d is a metric and that it is invariant under translations. This is, for every $x, y, z \in \mathbb{F}_q^n$ it is true that

$$\mathrm{d}(x + z, y + z) = \mathrm{d}(x, y).$$

Another important parameter of a code C is its **minimum distance** $\mathrm{d}(C)$, defined as

$$d(C) := \min\{\mathrm{d}(x, y) \mid x, y \in C,\ x \neq y\},\ \text{if } |C| > 1, \tag{1}$$

$$d(C) := 0,\ \text{if } |C| = 1. \tag{2}$$

If C is a $[n, k]$- linear code over $\mathbb{F}_q$ with minimum distance $\mathrm{d}(C) = d$, then we say that C is a $[n, k, d]$-code over $\mathbb{F}_q$, or simply we write $[n, k, d]_q$-code. The parameters $[n, k, d]$ are called the **fundamental** parameters of C.

The **weight** $\mathrm{wt}(x)$ of $x \in \mathbb{F}_q^n$ is defined as the number of non-zero components in x. We define the **minimum weight** $\mathrm{wt}(C)$ of C as

$$wt(C) := \min\{\mathrm{wt}(x) \mid 0 \neq x \in C\},\ \text{if } C \neq \{0\}, \tag{3}$$

$$wt(C) := 0,\ \text{if } C = \{0\}. \tag{4}$$

From the invariance under translation of d we get that

$$\mathrm{wt}(C) = \mathrm{d}(C).$$

Let C be a $[n, k]$-code over $\mathbb{F}_q$. If $k \geq 1$, then a $k \times n$-matrix G over $\mathbb{F}_q$ is called a **generator** matrix of C, if

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

In particular, it is possible to show that the $\mathrm{Rang}(G) = \dim_{\mathbb{F}_q}(C)$. If $k < n$, then a $(n - k) \times n$-matrix H over $\mathbb{F}_q$ is called a **parity check matrix** of C if

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

It is clear that the rank of H is $n - \dim_{\mathbb{F}_q}(C)$, which is, $n - k$. We say that G, a generator matrix of a code C, is in its **standard form** if it can be written as

$$G = (I_k \mid B),$$

where I_k represents the identity matrix of size k over $\mathbb{F}_q$; then a matrix in its standard form is also in its reduced row echelon form.

The canonical inner product on $\mathbb{F}_q^n$ is defined by

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

for $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$ in $\mathbb{F}_q^n$. Obviously this is a non-degenerate symmetric bi-linear form in $\mathbb{F}_q^n$.

Then, with this inner product defined, it makes sense to introduce the notion of the **dual** of a code. We define the dual $C^\perp$ of C, as usual:

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

If $C \subseteq C^\perp$, then it is said that C is **self-orthogonal**, and if $C = C^\perp$, it is called **self-dual**. From linear algebra we know that

$$\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^\perp) = n.$$

Due to this, if C is a $[n, k]$-code over $\mathbb{F}_q$, then $C^\perp$ is a $[n, n-k]_q$-code. In particular, if C is self-dual, then $n = 2k$.

Let $r \in \mathbb{N}$. A code C is called r**-divisible**, if for every $c \in C$ it is true that $r \mid \mathrm{wt}(c)$. In particular, a 2-divisible code is named **even** and a 4-divisible a **doubly even**.

Among the self-dual codes there exists a special classification depending on the field over which they are defined and their r-divisibility, as it follows: If C is a self-dual code over $\mathbb{F}_q$ and r-divisible, with $r > 1$, then we say that C is a code of

(a) **type I** if $q = 2$ and C is not doubly even, that is, $r \neq 4$.

(b) **type II** if $q = 2$ and C is doubly even.

(c) **type III** if $q = 3$ and is also 3-divisible, by being self-dual.

(d) **type IV** if $q = 4$ and therefore even as well.

A theorem from Gleason, Pierce and Turyn [1, Part XI], [9] guarantees that, if $s > 1$ divides the weight of each *codeword* in a non-trivial binary self-dual code, then either $s = 2$ or $s = 4$. The binary self-dual codes satisfy naturally this condition, when $s = 2$. Type II codes only exist if n is a multiple of eight.

A theorem proved by Mallows and Sloane [14, Theorem 2] shows that the minimum distance d of a binary self-dual $[n, k, d]$-code satisfies the inequality:

$$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4, \text{ if } \ n \not\equiv 22 \bmod 24,$$

$$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 6, \text{ if } \ n \equiv 22 \bmod 24,$$

where $\lfloor x \rfloor$ denotes the integer part of x. The codes that reach this bound are called **extremals**.

We write $\mathrm{Sym}(n)$ to represent the symmetric group of order n, $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ and $\sigma \in \mathrm{Sym}(n)$. Let's define the action of σ on $\mathbb{F}_q^n$ by

$$\sigma(x) := (x_{\sigma(1)}, \dots, x_{\sigma(n)}),\ x \in \mathbb{F}_q^n.$$

If C is a binary code and $\sigma(x) \in C$, for every $x \in C$, then σ is called an **automorphism** of C. The set of all the automorphisms of C is the **automorphism group** of C and it is denoted by $\mathrm{Aut}(C)$.

Finally, if C is a $[n, k]$-code over $\mathbb{F}_q$ and $\sigma \in \mathrm{Aut}(C)$ is of order p, with p a prime number, then we say that $\sigma \in \mathrm{Sym}(n)$ has the type $p-(c, f)$ if σ has c p-cycles and f fixed points.

3. Cited results

Let C be a linear code of length n and $\sigma \in \mathrm{Aut}(C)$ of type $p-(c,f)$, say

$$\sigma = \Omega_1 \cdots \Omega_c \Omega_{c+1} \cdots \Omega_{c+f}, \tag{5}$$

where $\Omega_1, \ldots, \Omega_c$ are the p-cycles and $\Omega_{c+1}, \ldots, \Omega_{c+f}$ the fixed points. Then, we define:

$$F_\sigma(C) := \{u \in C \mid \sigma(u) = u\}, \tag{6}$$

$$E_\sigma(C) := \{v \in C \mid \mathrm{wt}(v|_{\Omega_i}) \equiv 0 \bmod 2, i \in \{1, \ldots, c+f\}\}. \tag{7}$$

Let π be the function $\pi : F_\sigma(C) \longrightarrow \mathbb{F}_2^{c+f}$ defined by

$$u \longmapsto (\pi(u))_i := u_j,$$

where $j \in \Omega_i$. In the forthcoming $\overline{F_\sigma(C)}$ will stand for $\pi(F_\sigma(C))$.

Now we give some facts about $F_\sigma(C)$, $E_\sigma(C)$ and $\sigma \in \mathrm{Aut}(C)$. Let σ be as in (5); then for $u = (u_1, \ldots, u_n)$ we define

$$u|_{\Omega_j} := (u_{\Omega_{j1}}, \ldots, u_{\Omega_{jl}}),$$

with $\Omega_j = (\Omega_{j1} \ldots \Omega_{jl})$, being $l \in \{1, p\}$. Therefore, if $\sigma = (123)(456)(789)$. for example, and

$$u = 000111111000000000011000,$$

then $u|_{(123)} = (000)$ and $u|_{(456)} = (111)$. Besides, note that by definition if $u \in E_\sigma(C)$ and $f \neq 0$, then $u|_{\Omega_s} = 0$ for each $s \in \{c+1, \ldots, c+f\}$. If $\sigma = (123)(456)(789)(101112)$ and

$$u = 101000000101011011000000,$$

then

$$\sigma(u) = (110000000110011011000000).$$

In this case note that $u \notin F_\sigma(C)$, since $u \neq \sigma(u)$. Moreover, we notice from the example that if $u \in C \cap F_\sigma(C)$, then $u_{\Omega_{jl}} \equiv u_{\Omega_{jk}} \bmod 2$, for every $\Omega_{jl}, \Omega_{jk} \in \Omega_j$, $j \in \{1, \ldots, c+f\}$.

Finally, $F_\sigma(C) \cup E_\sigma(C) \subseteq C$; then, if C is doubly even, both $F_\sigma(C)$ and $E_\sigma(C)$ are doubly even as well. And if C is self-orthogonal then both subcodes are also self-orthogonal.

Lemma 3.1 ([10, Lemma 1])**.** *Let C be a self-dual code of length n. Then $\overline{F_\sigma(C)}$ is self-dual of length $n - c(p-1)$. Moreover, if C is doubly even and $p \equiv 1 \bmod 4$ or $f = 0$, then $\overline{F_\sigma(C)}$ is a 4-divisible code.*

Corollary 3.2. *Let C be a binary self-dual doubly even code and $\sigma \in \mathrm{Aut}(C)$ of type $p-(c,f)$, with p odd. If $p \equiv 1 \bmod 4$ and $p - 1 \not\equiv 0 \bmod 8$, then c is even.*

Proof. Since C is self-dual and doubly even, by lemma 3.1 it is true that $\overline{F_\sigma(C)}$ is a type II code. Thus, by [9] its length is divisible by eight. Then $n - c(p-1) \equiv 0 \bmod 8$. If we also have that $p - 1 \equiv 0 \bmod 4$ and $p - 1 \not\equiv 0 \bmod 8$, since $n \equiv 0 \bmod 8$, it follows that $c \equiv 0 \bmod 2$, that is, c is even. ☑

Lemma 3.3. *Let C be a binary code of length n and $\sigma \in \mathrm{Aut}(C)$ of type $p-(c,f)$. Then*

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

If C is in addition self-dual, then

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

Moreover, the multiplicative order of $2 \in \mathbb{Z}_p$ divides $\dim_{\mathbb{F}_2} E_\sigma(C)$. In particular, if C is self-dual and 2 is a primitive root modulo p, then c is even.

Proof. Let $v \in C$ and define $w := v + \sum_{i=0}^{p-1} \sigma^i(v)$. We know that

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

for every $i \in \{0, \ldots, p-1\}$, $j \in \{1, \ldots, c+f\}$, because two distinct cycles are disjoint, this is, $\Omega_l \cap \Omega_s = \emptyset$ for $l \neq s$ so that Ω_j only reorganizes the coordinates of v, and this does not alter its weight.

For $\sigma = \Omega_1 \ldots \Omega_{c+f} \in Aut(C)$ we get that

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

C is binary, then it is even. In consequence,

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

but the order of σ is p and $k(v, \Omega_j)$(k depends on v and Ω_j). This is,

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

and since p is an odd prime it follows that

$$\mathrm{wt}(w|_{\Omega_j}) \equiv 0 \bmod 2$$

for each $j \in \{1, \ldots, c+f\}$, that is $w \in E_\sigma(C)$.

Note here that

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

This shows that $\sum_{i=0}^{p-1} \sigma^i(v) \in F_\sigma(C)$. Hence, for every $v \in C$ it is true that

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

(note that C is a vector space over a field of characteristic two, then $v = -v$ for every $v \in C$).

Let's prove next that $F_\sigma(C)\cap E_\sigma(C)=\{0\}$. Let $v\in F_\sigma(C)\cap E_\sigma(C)$; then $\sigma(v)=v$ and $\Omega_j(v)|_{\Omega_j}=\Omega_j(v)$, v of even weight. As each Ω_j is a cycle of odd length, we have $v_l=0$ for every $l\in\Omega_j,\ j\in\{1,\dots,c+f\}$, this is, $v=0$. Thus,

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

Besides, if C is self-dual, then by Lemma 3.1 we get that $F_\sigma(C)$ is also self-dual. Hence, since

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

it follows that

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

And as the only vector of $E_\sigma(C)$ fixed by σ is 0, it is true that

$$p\mid(2^{\dim_{\mathbb{F}_2} E_\sigma(C)}-1),$$

thus

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

Let $c\in C,\ \sigma\in \mathrm{Aut}(C)$; then we define:

$$O(c):=\{\sigma^i(c)\mid i\in\mathbb{Z}\}\ \Rightarrow\ |O(c)|:=\begin{cases}1, & c\in F_\sigma(C),\\ p, & c\notin F_\sigma(C).\end{cases}$$

Moreover, we could define an equivalence relation over C as it follows:

For $c,c'\in C$ let

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

Clearly the cosets of C induced by this relation are $O(c)$, with $c\in C$. Then we get that

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

In this way $|C|=|F_\sigma(C)|+s\cdot p$, where $s\in\mathbb{Z}$; since we proved that $C=E_\sigma(C)\oplus F_\sigma(C)$, it follows that

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

or equivalently,

$$2^{\dim_{\mathbb{F}_2} E_\sigma(C)+\dim_{\mathbb{F}_2} F_\sigma(C)}\equiv 2^{\dim_{\mathbb{F}_2} F_\sigma(C)} \bmod p;$$

but we know p is odd, then it is equivalent to say that

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

Finally, since $2^{(p-1)}\equiv 1 \bmod p$, by Fermat's little theorem, we get $c/2\in\mathbb{N}$, that is c is even. ☑

Remark 3.4. If p is an odd prime number and we write $s(p)$ to name the smallest natural number such that

$$p\mid(2^{s(p)}-1),$$

then, as a consequence from the previous lemma, we obtain the next result:

Corollary 3.5. *Let C be a binary self-dual doubly even code and $\sigma \in \mathrm{Aut}(C)$ of type $p-(c,f)$, with p odd. If $s(p)$ is even, then c is even, too.*

Using the last lemma it is possible to obtain a generator matrix G for C in the form

$$G = \begin{array}{c} \\ \\ \end{array} \overset{\begin{array}{cc}\text{cycles} & \text{fixed points}\end{array}}{\left(\begin{array}{c|c} X & Y \\ \hline A & 0 \end{array}\right)} \begin{array}{l} \}\mathrm{span}(F_\sigma(C)) \\ \}\mathrm{span}(E_\sigma(C)). \end{array}$$

Lemma 3.6 ([10, Lemma 3]). *Let C be a binary self-dual $[n,k,d]$-code with $\sigma \in \mathrm{Aut}(C)$ of type $p-(c,f)$. Then:*

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

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

(c) *If $pc \leq 2d$, then or*

i. $d = 4, p = 3, c = 2$ *or*

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

Theorem 3.7 (V. Yorgov [18]). *Let C be a binary self-dual extremal doubly even $[n,k]$-code and $\sigma \in \mathrm{Aut}(C)$ of type $p-(c,f)$, with p odd. Then $c \geq f$.*

Lemma 3.8 ([10, Lemma 4]). *Let p be an odd prime such that $1 + x + \ldots + x^{p-1}$ is irreducible over $\mathbb{F}_2$. Let $\mathcal{P}$ be the set of all polynomials of even weight in $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. Then $\mathcal{P}$ is a field with module $x + x^2 + \ldots + x^{p-1}$. Moreover, multiplying by $1 + x^2 + x^3 + \ldots + x^{p-1} \in \mathcal{P}$ it corresponds to a right shift modulo the ideal $\langle x^p - 1\rangle$.*

We introduce another notation. For C self-dual with $C = F_\sigma(C) \oplus E_\sigma(C)$, as in Lemma 3.3, $v \in E_\sigma(C)$ with

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

we also define

$$f(v|_{\Omega_i}) := a_1 + a_2 x + \ldots + a_p x^{p-1} \text{for } i \in \{1, \ldots, c\}.$$

Here f induces componentwise a function from $E_\sigma(C)^*$ onto the ring $(\mathbb{F}_2[x]/\langle x^p - 1\rangle)^c$, where $E_\sigma(C)^*$ corresponds to $E_\sigma(C)$ by erasing the fixed points. Thus, if the conditions of the previous lemma hold, then $\mathcal{P} = \mathbb{F}_{2^{p-1}}$. In fact, we have the following lemma.

Lemma 3.9. *Let's suppose C is a self-dual code and $1 + x + \ldots + x^{p-1}$ is irreducible over $\mathbb{F}_2$. Then $f(E_\sigma(C)^*) \leq \mathbb{F}_{2^{p-1}}^c$ of dimension $\frac{c}{2}$. In particular, c is even.*

Proof. Clearly f preserves the addition. Let

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

By lemma 3.8, multiplying a polynomial of even weight by β^i produces a cyclic shift i times to the right. Then,

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

that is, $\{1 + \beta, \beta + \beta^2, \ldots, \beta^{p-2} + \beta^{p-1}\}$ is a basis for $\mathbb{F}_{2^{p-1}}$ over $\mathbb{F}_2$.

Hence, as

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

we obtain that $f(E_\sigma(C)^*)$ is closed under the scalar product induced from $\mathbb{F}_{2^{p-1}}$. Now by Lemma 3.3 we have that

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

Then, if $\dim_{\mathbb{F}_{2^{p-1}}} f(E_\sigma(C)^*) = k$, then $(2^{p-1})^k = 2^{\frac{1}{2}c(p-1)}$, and it follows that $k = \frac{1}{2}c$. ☑

Lemma 3.10. *If $p = 3$ and C is a doubly even self-dual code, then $f(E_\sigma(C)^*)$ is self-dual over $\mathbb{F}_4$ with the inner product given by*

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

for every $u, v \in \mathbb{F}_{2^{p-1}}^c$. It is also true that $\mathrm{d}(E_\sigma(C)^*)$ is greater or equal to $\frac{d}{2}$.

Proof. Since C is doubly even, if $v \in E_\sigma(C)^*$ then $\mathrm{wt}(f(v)) = \frac{1}{2}\mathrm{wt}(v)$, that is, $\mathrm{wt}(f(v)) \equiv 0 \bmod 2$. Using the previous lemma and [13, Theorem 1] it follows that $f(E_\sigma(C)^*)$ is self-dual and $\mathrm{d}(f(E_\sigma(C)^*)) \geq \frac{d}{2}$. ☑

Corollary 3.11. *If C is a doubly even self-dual code and $p = 3$, then $\frac{d}{2} \leq 2\lfloor \frac{c}{6} \rfloor + 2$. Moreover, if C is extremal, then $\frac{n}{24} \leq \lfloor \frac{c}{6} \rfloor$.*

Proof. By [13] a quaternary self-dual code with parameters $[c, \frac{c}{2}]$ has minimum distance at most $2\lfloor \frac{c}{6} \rfloor + 2$. ☑

Lemma 3.12 ([10, Lemma 7])**.** *If $p = 5$ and C is a self-dual doubly even code, then $f(E_\sigma(C)^*)$ is self-dual over $\mathbb{F}_{16}$ with the inner product defined by*

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

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

In this way we also have the next corollary.

Corollary 3.13. *If $p = 5$, C is a doubly even self-dual code and Ω_i is cyclically organized, then $f(E_\sigma(C)^*)$ is self-dual too. Besides, each codeword in $f(E_\sigma(C)^*)$ with a_i components of the form $\alpha^i(\alpha^{12j})$ fulfilling that $a_0 \equiv a_1 \equiv a_2 \bmod 2$.*

4. Exclusion of some prime numbers from the order of the automorphism group

4.1. The case $[24, 12, 8]$

Let's $\sigma \in \mathrm{Aut}(C)$ be of type $p-(c, f)$. The combinations that hold on first instance that $24 = pc + f$ are

p	c	f
3	1, 2, 3, 4, 5, 6, 7, 8	21, 18, 15, 12, 9, 6, 3, 0
5	1, 2, 3, 4	19, 14, 9, 4
7	1, 2, 3	17, 10, 3
11	1, 2	13,
13	1	11
17	1	7
19	1	5
23	1	1

As a consequence from Yorgov's Lemma (Lemma 3.7) we get $c \geq f$, so the previous table is reduced to

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

Using Corollary 3.5, since $s(3) = 2$ from the last table we exclude $3-(7, 3)$, because c must be even. At the end we get

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

Now we show a generator matrix for the binary self-dual doubly even $[24, 12, 8]$-code, obtained by considering an automorphism of type $3-(6,6)$. In this particular case, $\dim_{\mathbb{F}_2} E_\sigma(C) = (p-1)c/2 = 6$ and $\dim_{\mathbb{F}_2} F_\sigma(C) = (c+f)/2 = 6$.

A generator matrix for $F_\sigma(C)$ is given by

$$X = \begin{pmatrix} 111111000000000000110000 \\ 000111111000000000011000 \\ 000000111111000000001100 \\ 000000000111111000000110 \\ 000000000000111111000011 \\ 111000000000000000011111 \end{pmatrix},$$

while a generator matrix for the subcode $E_\sigma(C)$ is

$$A = \begin{pmatrix} 011000000011110110000000 \\ 000011000110011110000000 \\ 000000011110110011000000 \\ 101000000101011011000000 \\ 000101000011101011000000 \\ 000000101011011101000000 \end{pmatrix}.$$

Using Lemma 3.3, we get a generator matrix for C:

$$G = \left(\begin{array}{c|c} 111111000000000000 & 110000 \\ 000111111000000000 & 011000 \\ 000000111111000000 & 001100 \\ 000000000111111000 & 000110 \\ 000000000000111111 & 000011 \\ 111000000000000000 & 011111 \\ \hline 011000000011110110 & 000000 \\ 000011000110011110 & 000000 \\ 000000011110110011 & 000000 \\ 101000000101011011 & 000000 \\ 000101000011101011 & 000000 \\ 000000101011011101 & 000000 \end{array}\right).$$

4.2. The case $[48, 24, 12]$

Analogously as in the later case, if $\sigma \in \mathrm{Aut}(C)$ is of type $p-(c,f)$, then for this code C there are the following options:

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

A generator matrix for the self-dual doubly even binary $[48, 24, 12]$-code, obtained from an automorphism of type $23 - (2, 2)$, is given by

$$G = \left(\begin{array}{c|c}
1111111111111111111111100000000000000000000000 & 10 \\
0000000000000000000000011111111111111111111111 & 01 \\
\hline
1000000000000000000000100110010101110101111011 & 00 \\
0100000000000000000000110101011111001111000110 & 00 \\
0010000000000000000000101100111010010010011000 & 00 \\
0001000000000000000000100000001000111100110111 & 00 \\
0000100000000000000000110110010001101011100000 & 00 \\
0000010000000000000000101101011101000000001011 & 00 \\
0000001000000000000000110000111011010101111110 & 00 \\
0000000100000000000000101110001000011111000100 & 00 \\
0000000010000000000000100001010001111010011001 & 00 \\
0000000001000000000000110110111101001000110111 & 00 \\
0000000000100000000000111101001011010001100000 & 00 \\
0000000000010000000000101000110000011101001011 & 00 \\
0000000000001000000000110010001101111011011110 & 00 \\
0000000000000100000000101111010011001000010100 & 00 \\
0000000000000010000000100001111100010001110001 & 00 \\
0000000000000001000000110110101011111101000011 & 00 \\
0000000000000000100000111101000000001011011010 & 00 \\
0000000000000000010000101000110101110000010110 & 00 \\
0000000000000000001000100010001111001101110000 & 00 \\
0000000000000000000100100111010010010011000011 & 00 \\
0000000000000000000010110101111100111100011010 & 00 \\
0000000000000000000001101100101011101011110110 & 00
\end{array} \right).$$

4.3. *The case* $[120, 60, 24]$

The existence of an extremal binary self-dual doubly even code with such parameters is currently an open problem.

Under the assumption that such code exists, let $\sigma \in \mathrm{Aut}(C)$ be of type $p - (c, f)$. Then, for this code C we have the following possible types:

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

This problem is part of a research project and there is little information available about the prime numbers that divide the order of $\mathrm{Aut}(C)$. However, a remark is that $11-(10,10)$, $17-(7,1)$ and $59-(2,2)$ are not possible types, as are not either some of order 3, 5 and 7.

5. Conclusion

Let C be a extremal binary self-dual code with parameters $[24m, 12m, 4m+4]$, with $m \in \mathbb{N}$. We present the following table as a summary, where in the last column we show the information about the automorphism group of the code C and also the prime numbers that probably divide its order. Besides, M_{24} denotes the sporadic Mathieu group that acts on a set of 24 objects.

m	Parameters	Code	Aut(C)
1	$[24, 12, 8]$	Golay	M_{24}
2	$[48, 24, 12]$	QR-code	PSL(2, 47)
3	$[72, 36, 16]$	?	2, 3, 5, solvable
4	$[96, 48, 20]$	?	2, 3, 5, solvable
5	$[120, 60, 24]$	?	2, 3, 5, 7, 11, 19, 23, 29, 59, solvable
⋮	⋮	⋮	⋮
153			

References

[1] Assmus E. Jr., Mattson H. Jr., and Turyn R., "Research to develop the algebraic theory of codes", *Air force Cambridge Res. Lab., Bedford, MA, Report AFCRL-67-0365* (1967).

[2] Borello M., "The automorphism group of a self-dual $[72, 36, 16]$ binary code does not contain elements of order 6", *IEEE Trans. Inform. Theory* 58 (2012), no. 12, 7240–7245.

[3] Borello M. and Willems W., "Automorphism of order $2p$ in binary self-dual extremal codes of length a multiple of 24", *IEEE Trans. Inform. Theory* 59 (2013), no. 6, 3378–3383.

[4] Borello M., Dalla Volta F. and Nebe G., "The automorphism group of a self-dual $[72, 36, 16]$ code does not contain S_3, A_4 or D_8", *arXiv:1303.4899*

[5] Bouyuklieva S., De la Cruz J. and Willems W., "On the automorphism group of a binary self-dual $[120, 60, 24]$ code", *Appl. Algebra Engrg. Comput.* 24 (2013), no. 3-4, 201–214.

[6] Bouyuklieva S., O'Brien E. and Willems W., "The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code is solvable", *IEEE Trans. Inform. Theory* 52 (2006), no. 2, 4244–4248.

[7] De la Cruz J. and Willems W., "On extremal self-dual codes of Length 96", *IEEE Trans. Inform. Theory* 57 (2011), no. 10, 6820–6823.

[8] Dontcheva R., "On the doubly-even self-dual codes of length 96", *IEEE Trans. Inform. Theory* 48 (2002), no. 7, 557–560.

[9] Gleason A.M., "Weight polynomials of self-dual codes and the MacWilliams identities", *1970 Actes du Congrès International des Mathématiciens*, vol 3 (1971), 211–215.

[10] Huffman W.C., "Automorphisms of codes with applications to extremal doubly even codes of length 48", *IEEE Trans. Inform. Theory* 28 (1982), 511–521.

[11] Leon J.S, Masley J.M. and Pless V., "Duadic codes", *IEEE Trans. Inform. Theory* 30 (1984), 709–714.

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

[13] MacWilliams F., Odluzko A., Sloane N. and Ward H., "Self-dual codes over $GF(4)$", *Journal of Combinatorial Theory* 25A (1978), 288–318.

[14] Mallows C., and Sloane N., "An upper bound for self-dual codes", *Information and Control* 22 (1973), 188–200.

[15] O'Brien E. and Willems W., "On the automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code", *IEEE Trans. Inform. Theory* 57 (2011), no. 7, 4445–4451.

[16] Rains E., "Shadow bounds for self-dual codes", *IEEE Trans. Inform. Theory* 44 (1998), 134–139.

[17] Sloane N., "Is there a (72; 36) $d = 16$ self-dual code?", *IEEE Trans. Inform. Theory* IT-19 (1973), no. 2, 251–251.

[18] Yorgov V.Y. and Huffman W.C., "A $[72, 36, 16]$ doubly even code does not have an automorphism of order 11", *IEEE Trans. Inform. Theory* 33 (1987), no. 5, 749–752.

[19] Zhang S., "On the nonexsitence of extremal self-dual codes", *Discrete Appl. Math.* 91 (1999), no. 1-3, 277–286.