Università degli Studi di Milano - Bicocca

Scuola di Dottorato in Scienze

Dottorato in Matematica Pura e Applicata - XXVI ciclo

Automorphism groups of self-dual binary linear codes

with a particular regard to the extremal case of length 72

Author:
Martino Borello
(Student ID 744878)

Supervisors:
Prof.ssa Francesca Dalla Volta
Prof. Massimiliano SALA

January 16^{th} 2014

To my masters

"*There are more things in heaven and earth, Horatio,*
Than are dreamt of in your philosophy."

(William Shakespeare)

Contents

List of Tables

Introduction

The subject of this Ph.D. thesis arises from a long-standing open problem of classical Coding Theory, that is the existence of an extremal self-dual binary linear code of length 72.

In the past, the problem was mainly approached looking at possible automorphism groups of this code. Following this kind of approach, we investigate the link between the automorphism group of a general code and its module-structure. Actually, if a linear code over a field K has a non-trivial automorphism group, then it is a module over the group algebra KG, where G is any subgroup of automorphisms. In this context, we use some properties of modules - as the property to be projective or free, the structure of the trivial part, the structure of possible modules with the same socle, etc. - to determine if there are extremal codes among those with a certain automorphism group.

Most of the results of the thesis appear in papers of the author [7, 8] and in joint papers with Wolfgang Willems [10] and with Francesca Dalla Volta and Gabriele Nebe [9].

In order to understand the origin and the aim of this dissertation, let us

give here a brief overview of the main objects and of the problems related. We will introduce them extensively in Chapter 1.

A *binary linear code* $\mathcal{C}$ of length n is a subspace of the vector space $\mathbb{F}_2^n$. Its elements are usually called *codewords*. The *dual* of $\mathcal{C}$, with respect to the standard inner product in $\mathbb{F}_2^n$, is the subspace of all vectors orthogonal to every codeword of $\mathcal{C}$ and it is denoted by $\mathcal{C}^\perp$. The code $\mathcal{C}$ is called *self-orthogonal* if $\mathcal{C} \leq \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

If $\mathcal{C}$ is self-dual, then the *weight* $\mathrm{wt}(c) := |\{i \mid c_i = 1\}|$ of every $c \in \mathcal{C}$ is even. In particular, if $\mathrm{wt}(\mathcal{C}) := \{\mathrm{wt}(c) \mid c \in \mathcal{C}\} \subseteq 4\mathbb{Z}$, the code is called *doubly-even*.

Let $\mathcal{C}$ be a self-dual binary linear code. Using invariant theory, it is shown in [54] that the *minimum weight* $\mathrm{d}(\mathcal{C}) := \min(\mathrm{wt}(\mathcal{C} \setminus \{0\}))$ is bounded above by

$$\mathrm{d}(\mathcal{C}) \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{if } n \equiv 22 \bmod 24 \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{otherwise.} \end{cases}$$

Self-dual binary linear codes achieving this bound are called *extremal*. Extremal self-dual binary linear codes of length a multiple of 24 (*jump lengths*) are particularly interesting for various reasons: for example they are always doubly-even [54] and all their codewords of a given nontrivial weight support a 5-design [2].

Zhang [55] proved that the largest length for an extremal self-dual doubly-even binary linear code is 3928. So, in principle, it is possible to classify all codes of this family. However, we are far away from such classification: the largest known extremal doubly-even self-dual binary linear code has length 136.

Regarding jump lengths, only two extremal self-dual binary linear codes are known: the extended binary Golay code $\mathcal{G}_{24}$ and the extended quadratic residue code $\mathcal{XQR}_{48}$, unique, up to equivalence, of length 24 and 48 respectively. Both have a fairly large automorphism group: $\mathrm{Aut}(\mathcal{G}_{24}) \cong \mathrm{M}_{24}$ and $\mathrm{Aut}(\mathcal{XQR}_{48}) \cong \mathrm{PSL}_2(47)$. The third step of the classification, that is the existence of an extremal self-dual binary linear code of length 72, is a

long-standing open problem posed explicitly by Sloane in 1973 [58].

A series of papers (the first one is by John Horton Conway and Vera Pless [18], published in 1982) investigates the automorphism group of a putative extremal self-dual code of length 72 excluding most of the subgroups of $\mathcal{S}_{72}$. In this dissertation we continue such investigation proving that, if an extremal self-dual binary linear code of length 72 does exist, then its automorphism group is very small. More precisely, we prove the following.

Theorem ([8]). *Let $\mathcal{C}$ be an extremal self-dual binary linear code of length 72. Then its automorphism group has order at most 5.*

The existence of extremal self-dual binary linear codes of length 96, 120 and any greater jump length is an open problem too, studied a bit in the literature. In this thesis we contribute also to the investigation of their possible automorphism groups.

Starting from these problems, we develop general methods which can be applied to self-dual binary linear codes of other lengths and not necessarily extremal. In particular, we give structure results for self-dual binary linear codes which have certain automorphisms: usually we point out "smaller pieces" which are easier to determine and then we show how to construct the whole code from these "smaller pieces". Such methods can be used to do exhaustive searches among codes with certain parameters and fixed automorphism group. This can be often reduced to the search of a relatively small set of representatives for a certain group action.
We see at least three possible applications of our methods. They can be used

a) to investigate possible automorphism groups of extremal self-dual binary linear codes;
b) to construct self-orthogonal binary linear codes with large minimum distance;
c) to classify self-dual binary linear codes with certain parameters.

Obviously the last one is the most ambitious.

Many previous investigations have been done on self-dual codes with an automorphism of odd prime order. A well-known decomposition as direct sum of two particular subcodes was given by Cary Huffman in [31] and it is the key point of many papers on the topic. In Section 2.2 we present his result in a language which is particularly useful for implementation.

We focus mainly on the interactions between automorphisms of odd prime order and involutions. Some results were given in previous works by Stefka Bouyuklieva, Eamonn O'Brien, Wolfgang Willems, Nikolay Yankov, Thomas Feulner and Gabriele Nebe [16, 47, 61, 45, 24]. Our contribution is principally regarding properties of self-dual binary linear codes with an automorphism group containing a subgroup of order $2p$. In particular, Section 2.3 deals with the abelian case and Section 2.4 deals with the non-abelian one. The first is a presentation of the joint paper with W. Willems [10] while the second one is a generalization of methods used in [24] and [9].

The key result of Section 2.3, which shows a nice link between module-theoretical properties and coding-theoretical ones, is the following.

Theorem ([10])**.** *Let $\mathcal{C}$ be a self-dual binary linear code and let σ_{2p} be an automorphism of $\mathcal{C}$ of order $2p$. Then $\mathcal{C}$ is a projective $\mathbb{F}_2\langle\sigma_{2p}\rangle$-module if and only if a natural projection of the subcode fixed by σ_{2p} is self-dual.*

In Section 2.3 we deal with the strong consequences of the theorem for the structure of the automorphism group of extremal self-dual binary linear codes.

The fundamental result of Section 2.4 is Theorem 2.7. Nevertheless, this theorem has a lot of technicalities, so we prefer to omit here a complete and accurate presentation of it. Let us just say that the key point of the theorem is an investigation of the action of the involutions on the decomposition of Huffman mentioned above. In particular, we prove a strong result on one of the components, which is usually the most difficult to determine.

In Section 2.5 we concentrate on the interactions between the subcodes fixed by different automorphisms. This plays a fundamental role in our search. We examine in particular two cases: let H be a subgroup of the automorphism group of a binary linear code $\mathcal{C}$ and suppose that $H = A \rtimes B$ for two subgroup A and B. If the semidirect product is non-abelian, then we can use the action of B on A to get a sum of subcodes fixed by automorphisms of A just knowing one of them. If the product is simply a direct product, then we get some restrictions on the possible subcodes fixed by automorphisms of both subgroups. We use such methods in our search to build quite large subcodes of putative extremal self-dual binary linear codes.

The mentioned three sections are the core of the dissertation. However, their power is mainly shown in Chapter 3, dealing with the automorphism group of a putative extremal self-dual binary linear code of length 72, and in Chapter 4, dealing with the automorphism group of extremal self-dual binary linear codes of other jump lengths.

Finally, in Chapter 5 we introduce a new class of codes related to self-dual binary linear codes of even length. We call them *semi self-dual codes* and we prove some upper bounds on their minimum distance. This provides a useful tool to get a nice result on the fixed codes of the involutions in some extremal self-dual binary linear codes. In this chapter, which is still a work in progress, we point out some open problems we are trying to solve.

Acknowledgements

First of all, I would like to express my deep gratitude to my two supervisors, Francesca Dalla Volta and Massimiliano Sala, for their guidance and inspiration. I am really in debt with Prof. Sala because he took seriously and welcomed my desire to do research, for the insightful suggestion of the nice

and difficult problem, for introducing me to Magma and for encouraging me to go on with the problem even during the hardest periods. Without Prof. Dalla Volta I would have surely been lost during these years: she introduced me (and she is still introducing me) to the complex and fascinating world of research. I learnt from her how to approach a problem, to ask approachable questions, how to write a paper, how to present my results, *et cetera*. We had a lot of fruitful (and sometimes not so quiet) discussions: I am really grateful for all her help and teaching.

I owe my heartfelt gratitude to Prof. Wolfgang Willems and to Prof. Gabriele Nebe for their contagious and enthusiastic passion for mathematics. They really have been like "co-supervisors" for me and I learnt a lot from them both.

The months in Magdeburg were very stimulating and I enjoyed a lot the rich atmosphere of the *Institut für Algebra und Geometrie*. In particular, I want to thank Anton, Javier, Qi and Yue for their friendship and for the help during those months.

The short period in Aachen was fruitful too and I am really grateful to Prof. Nebe for inviting me there. I would like to thank Prof. Nebe also for agreeing to review the current thesis.

I am grateful to all my collegues for the good office atmosphere, their patience and help. In particular I would like to thank Gianluca for all the coffee breaks we shared and for all the discussions we had. Tommaso and Claudio deserve thanks for their help as well. I cannot forget the loud and pleasant visit of Ilaria and Raimundo who enriched the atmosphere of our office even more. Let me thank here also Dr. Pablo Spiga and Prof. Andrea Previtali for their great suggestions and assistance.

The *CryptoLab* of Trento and the whole group of Prof. Sala deserve thanks for the support in the computational part. In particular I wish to express my gratitude to Matteo, Chiara and Emanuele for all the nice time spent together.

I am very grateful to Prof. Thomas Weigel and Prof. Andrea Caranti for

accepting to be part of the thesis committee.

Finally, and most importantly, I want to thank Raffaella, Vittoria, Giacomo, Giorgio, Davide, Federica, all my family and friends for their support and faithful company. They all remembered me that, before being a mathematician, I am first and foremost a man. They nurtured my passion for mathematics more and more.

CHAPTER 1

Preliminaries

In this chapter we introduce the objects which will appear in the dissertation, putting in evidence some useful properties and relations. Most of them are well-known in Coding Theory and we will omit the proofs, referring the reader to the original papers. In Section 1.9 we improve a result of Martínez-Pérez and Willems about modules over particular group algebras.

The principal references are [32] and [38], for the coding-theoretical part, and [34] and [19], for the module-theoretical one.

1.1 Basic notions about codes

In this dissertation we mainly consider linear codes over finite fields. Nevertheless, we give here a more general definition of a code.

Definition 1.1. *Let A be a (finite) set, called the* alphabet.

- *A* code $\mathcal{C}$ *is a subset of the cartesian product of n copies of the alphabet A, that is $\mathcal{C} \subseteq A^n$.*

- *The parameter n is called the* length *of the code.*
- *An element of $\mathcal{C}$ is called a* codeword*, or simply a word.*

So, a code is a collection of some of all possible words with n letters chosen in the alphabet A.

Definition 1.2. *Let $A = \mathbb{F}_q$ (the field with q elements). If $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$ the code is called* linear.
Three cases are studied more extensively:

- binary linear codes*, when $A = \mathbb{F}_2$;*
- ternary linear codes*, when $A = \mathbb{F}_3$;*
- quaternary linear codes*, when $A = \mathbb{F}_4$.*

An important parameter of a linear code is its *dimension* as an $\mathbb{F}_q$-vector space, usually indicated with the letter k.

Let $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$. The elements in $\{1, \ldots, n\}$ are called the *coordinates* and we say that v_i is the value of v at the coordinate i.

Definition 1.3. *Let $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$ be vectors in $\mathbb{F}_q^n$.*

- *The* Hamming distance *between v and w is defined as follows:*

$$\mathrm{d}_H(v, w) := \#\{i \mid v_i \neq w_i\},$$

  that is the number of coordinates in which the two vectors have different values.

- *The* Hamming weight *of a vector v is given by*

$$\mathrm{wt}(v) := \mathrm{d}(v, \mathbf{0})$$

  where $\mathbf{0}$ is the vector with value 0 at each coordinate.

The Hamming distance, which is trivially a metric, is the only one we consider throughout the dissertation. Thus we indicate it simply by $\mathrm{d}(\ ,\ )$ instead of $\mathrm{d}_H(\ ,\ )$.

Obviously,

$$\mathrm{d}(v,w) = \mathrm{wt}(v-w).$$

Definition 1.4. *The* minimum distance *of a code $\mathcal{C}$ is defined by*

$$d = \mathrm{d}(\mathcal{C}) := \min_{v,w\in\mathcal{C},\ v\neq w}\{\mathrm{d}(v,w)\}.$$

Notice that, dealing with linear codes, the minimum distance is also the minimum weight, that is

$$\mathrm{d}(\mathcal{C}) = \min_{c\in\mathcal{C},\ c\neq\mathbf{0}}\{\mathrm{wt}(c)\}.$$

Let us state an easy but powerful result on the weight in binary codes.

Proposition 1.1 (Chapter 1 [32])**.** *Let $v, w \in \mathbb{F}_2^n$. Then*

$$\mathrm{wt}(v+w) = \mathrm{wt}(v) + \mathrm{wt}(w) - 2\mathrm{wt}(v\cap w),$$

where $v\cap w$ is the vector of $\mathbb{F}_2^n$ which has 1 precisely in those positions where both v and w have 1.

We fix here some notations which we will use throughout the dissertation.

Notation 1.1. *A linear code over $\mathbb{F}_q$ of length n, dimension k and minimum distance d is called an $[n,k,d]_q$ code. If $q=2$ usually the subscript is omitted, so that an $[n,k,d]$ code is binary.*

The notation for non-linear codes is $(n,M,d)_q$, where n, d and q are as in the linear case and M is the size of the code.

The three parameters n, k, d introduced are clearly not independent. One fundamental relation is the Singleton inequality [56], which says that, for an $[n,k,d]_q$ code, we have

$$k \leq n - d + 1. \tag{1.1}$$

Codes for which the equality holds are called MDS (Maximum Distance Separable) codes.

Another well-known relation is the Griesmer bound [27] for linear codes, which says that, given an $[n,k,d]_q$ code, it holds

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil . \tag{1.2}$$

Let us introduce a very common tool to describe and to identify codes.

Definition 1.5. *For an $[n,k,d]_q$ code $\mathcal{C}$, a $k \times n$ matrix over $\mathbb{F}_q$ whose rows generate $\mathcal{C}$ is called* generator matrix *of the code and it is denoted by* $\mathrm{G}(\mathcal{C})$.

Obviously a generator matrix is not uniquely determined by a code (while a generator matrix determines uniquely a code). So, with $\mathrm{G}(\mathcal{C})$ we mean one of the possible generator matrices of $\mathcal{C}$. For any set of k independent columns of a generator matrix of a code $\mathcal{C}$, the corresponding set of coordinates forms an *information set* for $\mathcal{C}$. In general, we say that the *coordinates are independent* if the corresponding columns in a generator matrix are linearly independent.

Definition 1.6. *Let $\mathcal{C}$ be an $[n,k,d]$ linear code.*

- *The code obtained by deleting the same coordinate i in each codeword is called a* punctured code *(on the i^{th} coordinate) and it is denoted by $\mathcal{C}^*$.*

- *If T is a set of t coordinates and $\mathcal{C}(T)$ the set (which is a subcode of $\mathcal{C}$) of codewords which are 0 on T, we define $\mathcal{C}_T$, called a* shortened code *on T, the code obtained by puncturing $\mathcal{C}(T)$ on the T coordinates.*

We conclude with a very short explanation of the reason why it is interesting to have codes with large minimum distance, introducing the concept of *Error Correcting Code*. More details on such topic can be found in Chapter 1 of [38].

Codes are mainly used to correct errors on noisy communication channels: the transmitter fixes a code $\mathcal{C}$, which is the set of chosen messages of a given length n, among all possible ones. When he communicates a message, some errors may occur. The receiver, who knows $\mathcal{C}$, looks inside the code for the closest (in the sense of Hamming distance) messages. If the minimum distance of the code is large enough and the errors are not too many, then the receiver will get the original message. However, intuitively, the larger the minimum distance, the smaller the number of messages (a bound for example is given in (1.1)) and vice versa, so the main goal that one wants to achieve is, roughly speaking, to have a code with a large minimum distance and a relatively good number of codewords. We conclude by stating a result which formalizes the first request.

Theorem 1.1 (Theorem 2 [38]). *A code with minimum distance d can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. If d is even, the code can simultaneously correct $\frac{d-2}{2}$ errors and detect $\frac{d}{2}$ errors.*

1.2 Inner products and dual codes

A very important concept in Coding Theory is the duality with respect to an inner product. In this section we will give only some definitions and results which are essential in our dissertation.

Dealing mainly with binary codes, a central role is played by the standard inner product, however we will use also other types of inner products.

Definition 1.7. *Let $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n)$ be vectors of $\mathbb{F}_q^n$. Then*

- $\langle v, w \rangle := \sum_{i=1}^{n} v_i w_i$ *is the* standard inner product *of v and w.*

If $q = r^2$, we denote $\overline{\beta} := \beta^r$ for $\beta \in \mathbb{F}_{r^2}$. Then

- $\langle v, w \rangle_H := \sum_{i=1}^{n} v_i \overline{w_i}$ *is the* Hermitian inner product *of v and w;*

- $\langle v, w\rangle_{tr} := \sum_{i=1}^{n} v_i\overline{w_i} + \overline{v_i}w_i$ *is the* trace-Hermitian inner product *of* v *and* w.

There is a natural concept related to inner products.

Definition 1.8. *Let* $\mathcal{C}$ *be an* $[n, k, d]_q$ *code.*

- *The* dual code $\mathcal{C}^{\perp}$ *is defined as*

$$\mathcal{C}^{\perp} := \{v \in \mathbb{F}_q^n \mid \langle c, v\rangle = 0 \text{ for all } c \in \mathcal{C}\}.$$

If $q = r^2$, *then*

- *The* Hermitian dual code $\mathcal{C}^{\perp_H}$ *is defined as*

$$\mathcal{C}^{\perp_H} := \{v \in \mathbb{F}_q^n \mid \langle c, v\rangle_H = 0 \text{ for all } c \in \mathcal{C}\}.$$

- *The* trace-Hermitian dual code $\mathcal{C}^{\perp_{tr}}$ *is defined as*

$$\mathcal{C}^{\perp_{tr}} := \{v \in \mathbb{F}_q^n \mid \langle c, v\rangle_{tr} = 0 \text{ for all } c \in \mathcal{C}\}.$$

If $\mathcal{C}$ is an $[n, k, d]_q$ code, it is straightforward to prove that

$$\dim \mathcal{C}^{\perp} = n - k. \tag{1.3}$$

and the same holds for the Hermitian dual code and for the trace-Hermitian dual code (when $q = r^2$).

A generator matrix of $\mathcal{C}^{\perp}$ is called a *parity check matrix* of $\mathcal{C}$.

Definition 1.9. *Let* $\mathcal{C}$ *be an* $[n, k, d]_q$ *code.*

- *If* $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ *then* $\mathcal{C}$ *is called* self-orthogonal.
- *If* $\mathcal{C} = \mathcal{C}^{\perp}$ *we call* $\mathcal{C}$ self-dual.

Let $q = r^2$.

- *If* $\mathcal{C} = \mathcal{C}^{\perp_H}$ *then* $\mathcal{C}$ *is called* Hermitian self-dual.

- *If* $\mathcal{C} = \mathcal{C}^{\perp_{tr}}$ *we call* $\mathcal{C}$ trace-Hermitian self-dual.

By (1.3), it follows immediately that the dimension of a self-dual linear code is $\frac{n}{2}$. In particular self-dual linear codes exists if and only if n is even.

Example 1.1. *A well-known example of self-dual binary linear code is the extended Hamming code* $\hat{\mathcal{H}}_3$*: it is an* $[8, 4, 4]$ *code with*

$$\mathrm{G}(\mathcal{C}) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Let us state some results about self-orthogonal and self-dual binary linear codes.

Theorem 1.2 (Chapter 1 [32])**.** *Let* $\mathcal{C}$ *be a self-orthogonal binary linear code of length* n *and dimension* k*. Then we have the following.*

- *All codewords have even weight. Thus* $\mathbf{1} := (1, 1, \ldots, 1) \in \mathcal{C}^{\perp}$.
- *Let* $\mathcal{C}_0 = \{c \in \mathcal{C} \mid \mathrm{wt}(c) \equiv 0 \bmod 4\}$*. Then either* $\mathcal{C} = \mathcal{C}_0$ *or* $\mathcal{C}_0$ *is a subcode of* $\mathcal{C}$ *of dimension* $k - 1$.
- *If all rows of* $\mathrm{G}(\mathcal{C})$ *have a weight divisible by two (respectively by four), then every codeword of* $\mathcal{C}$ *has a weight divisible by two (respectively by four).*
- $\mathcal{C}$ *has minimum distance* d *if and only if* $\mathrm{G}(\mathcal{C}^{\perp})$ *has at least a set of* d *linearly dependent columns and every* $d - 1$ *columns are linearly independent.*

A binary linear code $\mathcal{C}$ in which every codeword has even weight is called *even*. If in particular

$$\{\mathrm{wt}(c) \mid c \in \mathcal{C}\} \subseteq 4\mathbb{Z}$$

the code is called *doubly-even*. By Theorem 1.2, every self-orthogonal binary linear code is even. On the other hand, it is straightforward to prove that every doubly-even binary linear code is self-orthogonal.

1.3 Weight enumerators

A very useful and important object associated to a code is its weight enumerator, a polynomial which describes the distribution of the weights in the code.

Definition 1.10. *For an $[n,k,d]_q$ code $\mathcal{C}$, we put*

$$A_i(\mathcal{C}) := \#\{c \in \mathcal{C} \mid \mathrm{wt}(c) = i\}.$$

The list of $[A_i(\mathcal{C})]_{i\in\{0,\ldots,n\}}$ is called the weight distribution *of $\mathcal{C}$.*

Obviously $A_0(\mathcal{C}) = 1$, since the code is linear, and

$$A_1(\mathcal{C}) = \ldots = A_{d-1}(\mathcal{C}) = 0.$$

Furthermore we have

- $\sum_{i=0}^{n} A_i(\mathcal{C}) = q^k$,
- $A_i(\mathcal{C}) = A_{n-i}(\mathcal{C})$ if $q = 2$ and $\mathbf{1} \in \mathcal{C}$.

Example 1.2. *Let $\hat{\mathcal{H}}_3$ be as in Example 1.1. The nonzero elements of the weight distribution of $\hat{\mathcal{H}}_3$ are*

$$A_0(\hat{\mathcal{H}}_3) = 1, \quad A_4(\hat{\mathcal{H}}_3) = 14, \quad A_8(\hat{\mathcal{H}}_3) = 1.$$

In order to give the information in a more compact way and to deduce new properties, we introduce the notion of the *weight enumerator* of a code, which in the literature is presented in a homogeneous and a non-homogeneous version as well.

Definition 1.11. *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with weight distribution*

$$[A_i(\mathcal{C})]_{i\in\{0,\ldots,n\}}.$$

Then the weight enumerator *of $\mathcal{C}$ is*

$$W_{\mathcal{C}}(x) := \sum_{i=0}^{n} A_i(\mathcal{C}) x^i,$$

polynomial in $\mathbb{Z}[x]$*, and the* homogeneous weight enumerator *is*

$$W_{\mathcal{C}}(x,y) := \sum_{i=0}^{n} A_i(\mathcal{C}) x^i y^{n-i},$$

homogeneous polynomial in $\mathbb{Z}[x,y]$*. Usually, with abuse of notation, the homogeneous weight enumerator is called simply weight enumerator.*

Example 1.3. *The weight enumerator of* $\hat{\mathcal{H}}_3$ *(see Example 1.1) is*

$$W_{\hat{\mathcal{H}}_3}(x) = 1 + 14x^4 + x^8 \quad \textit{or} \quad W_{\hat{\mathcal{H}}_3}(x,y) = y^8 + 14x^4y^8 + x^8$$

Both polynomials carry the information on the weight distribution of the code and they are, obviously, uniquely determined by $\mathcal{C}$. The converse is not true, as we will show in Example 1.6.

1.4 Equivalence of codes

We want to introduce now the concept of equivalence of codes. This is essential when we talk about classification of codes, since, usually, we classify codes with certain parameters only up to equivalence. We remark that the classification of codes with certain parameters and finding a good algorithm to establish if two general codes are equivalent are both very hard problem with only partial answers.

To define the concept of equivalence, let us introduce a natural action of the symmetric group $\mathcal{S}_n$ on the space $\mathbb{F}_2^n$. Clearly we have a natural *action of* $\mathcal{S}_n$ *on the coordinates* $\{1,\ldots,n\}$. This induces an action on the vectors of $\mathbb{F}_2^n$: let $\sigma,\tau \in \mathcal{S}_n$, then

$$(v_1, v_2, \ldots, v_n)^\sigma = (v_{1^{\sigma^{-1}}}, v_{2^{\sigma^{-1}}}, \ldots, v_{n^{\sigma^{-1}}})$$

so that $(v^\sigma)^\tau = v^{\sigma\tau}$.

Example 1.4. *Let*

$$v = (1,0,1,1,0,1,1,1,0) \in \mathbb{F}_2^9$$

and

$$\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9) \in \mathcal{S}_9.$$

Then we have

$$v^\sigma = (0, 1, 0, 1, 1, 0, 1, 1, 1).$$

Equivalently, we can consider the faithful representation of $\mathcal{S}_n$ in $\mathrm{GL}_n(2)$, which maps every element σ of $\mathcal{S}_n$ to the corresponding permutation matrix $\mathrm{P}(\sigma)$ so that

$$v^\sigma = v \cdot \mathrm{P}(\sigma),$$

where $v \in \mathbb{F}_2^n$, $\sigma \in \mathcal{S}_n$ and $\cdot$ is the usual product vector-matrix.

One very important properties of this action is the following

$$\mathrm{wt}(v^\sigma) = \mathrm{wt}(v),$$

which means that the weight is invariant under the action of $\mathcal{S}_n$. This implies obviously that $\mathcal{C}^\sigma := \{c^\sigma \mid c \in \mathcal{C}\}$ has the same weight distribution of $\mathcal{C}$. So, in particular, if $\mathcal{C}$ is an $[n, k, d]$ code, $\mathcal{C}^\sigma$ has the same parameters. We give now a fundamental definition.

Definition 1.12. *Let $\mathcal{C}, \mathcal{D} \leq \mathbb{F}_2^n$. We say that $\mathcal{C}$ is* equivalent *to $\mathcal{D}$, $\mathcal{C} \sim \mathcal{D}$, if there exists $\sigma \in \mathcal{S}_n$ such that*

$$\mathcal{C}^\sigma = \mathcal{D}.$$

We list here some properties invariant under equivalence.

Remark 1.1. *Let $\mathcal{C}$ and $\mathcal{D}$ be two equivalent codes. Then*

- *they have the same parameters,*
- *they have the same weight distribution,*
- *if $\mathcal{C}$ is self-orthogonal (self-dual) then $\mathcal{D}$ is self-orthogonal (self-dual).*

In our dissertation we will deal mainly with self-dual binary linear codes with certain parameters. According to the above, we can consider them up to equivalence. In particular, we will choose every time the most convenient shape for a generator matrix.

The properties in Remark 1.1 are not sufficient to get equivalence, in general, as we can see in the following example.

Example 1.5. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two (self-dual) $[10, 5, 2]$ codes with*

$$\mathrm{G}(\mathcal{C}_1) := \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix},$$

$$\mathrm{G}(\mathcal{C}_2) := \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

These codes are both self-dual and they have the same parameters, but they have different weight distributions. So they are not equivalent. It is proved [50] *that every self-dual* $[10, 5, 2]$ *code is equivalent to one of this two codes.*

Example 1.6. *To have an example of non-equivalent self-dual binary linear codes with the same weight distribution, we have to consider codes of length at least* 16*: there are* [50]*, up to equivalence, only two non-equivalent self-dual* $[16, 8, 4]$ *codes $\mathcal{D}_1, \mathcal{D}_2$ and both have weight enumerator*

$$W_{\mathcal{D}_1}(x) = W_{\mathcal{D}_2}(x) = 1 + 28x^4 + 198x^8 + 28x^{12} + x^{16}.$$

In the non-binary case we can define in the same way the concept of equivalence. It is quite common to call it *permutation equivalence* to distinguish it by the most common *monomial equivalence*.

Definition 1.13. *Let $\mathcal{C}$ and $\mathcal{D}$ be linear codes over $\mathbb{F}_q$ of length n. Then they are* monomial equivalent, *$\mathcal{C} \sim_m \mathcal{D}$, if there exists a monomial matrix M (i.e. a square matrix which has exactly one nonzero entry in each row and column) in $\mathrm{GL}_n(q)$ such that*

$$\mathcal{C}^M := \{c \cdot M \mid c \in \mathcal{C}\} = \mathcal{D}.$$

Also the multiplication by monomial matrices is weight preserving, so it makes sense to talk of the classification of codes with certain parameters up to monomial equivalence.

Finally, let us mention that there is an even more general concept of equivalence [37], involving the automorphisms of the field $\mathbb{F}_q$, still weight preserving. However, in the binary case the three definitions of equivalence coincide and we will need only the concept of monomial equivalence in the non-binary case.

1.5 Automorphisms of codes

In this section we introduce the automorphism group of a binary code which is one of the main objects of our dissertation. Recall that the symmetric group $\mathcal{S}_n$ acts on the vectors of $\mathbb{F}_2^n$.

Definition 1.14. *An* automorphism *of a binary code $\mathcal{C}$ of length n is a permutation which leaves the code invariant, that is a $\sigma \in \mathcal{S}_n$ such that*

$$\mathcal{C}^\sigma = \mathcal{C},$$

where $\mathcal{C}^\sigma := \{c^\sigma \mid c \in \mathcal{C}\}$.

It is trivial to prove that the set of all the automorphisms of a binary code $\mathcal{C}$ of length n is a subgroup of $\mathcal{S}_n$, called the *automorphism group* of the code and denoted by $\mathrm{Aut}(\mathcal{C})$. So

$$\mathrm{Aut}(\mathcal{C}) := \{\sigma \in \mathcal{S}_n \mid \mathcal{C}^\sigma = \mathcal{C}\}.$$

Since $\mathrm{Aut}(\mathcal{C})$ is the stabilizer of $\mathcal{C}$ in $\mathcal{S}_n$, the number of codes that are equivalent to $\mathcal{C}$ (that is the cardinality of the orbit of $\mathcal{C}$ under the action of $\mathcal{S}_n$) is obviously

$$\frac{n!}{\mathrm{Aut}(\mathcal{C})}.$$

So if we call T_n the total number of distinct codes of a certain family (for example self-dual or doubly-even), we have the so called *mass formula*

$$T_n = \sum_{\mathcal{C} \text{ inequiv.}} \frac{n!}{\mathrm{Aut}(\mathcal{C})}.$$

For some families an explicit formula for T_n is known. This is the case of self-dual binary linear codes. Using the fact that self-dual binary linear codes are maximal isotropic spaces for the standard inner product it is possible to prove that

$$T_n = \prod_{i=1}^{\frac{n-2}{2}} (2^i + 1)$$

for this family [53].

The mass formula is clearly a very important information when one tries to classify codes with certain parameters.

For our dissertation the concept of *type* of an automorphism plays a crucial role. It is the cycle-structure of the permutation. Often we briefly say *structure* of an automorphism meaning its type. We give the definition of type only for automorphisms of prime order or of order a product of two primes.

Definition 1.15. *Let p and r be two primes and σ_p and σ_{pr} be elements of $\mathcal{S}_n$ of order p and $p \cdot r$ respectively.*

- *The automorphism σ_p is of type p-(c, f) if it has c cycles of length p (p-cycles) and f fixed points.*
- *The automorphism $\sigma_{p \cdot r}$ is of type $p \cdot r$-$(a, b, c; f)$ if it has a cycles of length p, b cycles of length r, c cycles of length $p \cdot r$ and f fixed points.*

We say that an automorphism is fixed point free *if it has no fixed points.*

We introduce now a fundamental object which we will play a crucial role in the following.

Definition 1.16. *Let $\mathcal{C}$ be a binary linear code of length n and $\sigma \in \mathrm{Aut}(\mathcal{C})$. Then we define the* fixed code of σ *as*

$$\mathcal{C}(\sigma) := \{c \in \mathcal{C} \mid c^\sigma = c\}.$$

The set $\mathcal{C}(\sigma)$ is trivially a subcode of $\mathcal{C}$.

For $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ and $\Omega = \{j_1, \ldots, j_m\} \subseteq \{1, \ldots, n\}$ we put

$$v_{|\Omega} = (v_{j_1}, \ldots, v_{j_m}).$$

If $\sigma \in \mathcal{S}_n$ and $\Omega_1, \ldots, \Omega_{n_\sigma}$ are the orbits of the action of σ on the coordinates, we say that v is *constant on the orbits of* σ if, for all i, $v_{|\Omega_i}$ is either the zero or the all one vector.

Lemma 1.1. *Let $\mathcal{C}$ be a binary linear code of length n and $\sigma \in \mathrm{Aut}(\mathcal{C})$. Let $c \in \mathcal{C}$. Then c belongs to $\mathcal{C}(\sigma)$ if and only if c is constant on the orbits of σ.*

Proof. Notice that if we prove the result for an automorphism with one orbit, then we have the result for a general automorphism just repeating the argument to each orbit. So, suppose σ has one orbit and take $c = (c_1, \ldots, c_n) \in \mathcal{C}$. Then

$$c \in \mathcal{C}(\sigma) \;\Leftrightarrow\; c^\sigma = c \;\Leftrightarrow\; c_{i^{\sigma^{-1}}} = c_i \text{ for all } i \in \{1, \ldots, n\}$$

Since σ has one orbit we have $c \in \mathcal{C}(\sigma)$ if and only if $c_1 = c_2 = \ldots = c_n$. □

Then we can define a *natural projection associated to* σ which will appear a lot throughout the dissertation.

Definition 1.17. *Let $\mathcal{C} \leq \mathbb{F}_2^n$ and $\sigma \in \mathrm{Aut}(\mathcal{C})$ with orbits $\Omega_1, \ldots, \Omega_{n_\sigma}$. Then we define the map*

$$\pi_\sigma : \mathcal{C}(\sigma) \to \mathbb{F}_2^{n_\sigma}$$

so that, for $c \in \mathcal{C}(\sigma)$, the value of $\pi_\sigma(c)$ on the i^{th} coordinate is the value of c on Ω_i.

Lemma 1.1 shows that π_σ is well-defined (and injective).

1.6 MacWilliams identities and invariant theory

MacWilliams proved that the weight distribution of the dual of a linear code is determined by the weight distribution of the code. More precisely she proved the following theorem.

Theorem 1.3 (MacWilliams [36]). *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ and $\mathcal{C}^\perp$ its dual with respect to the standard inner product. Then*

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x+(q-1)y, x-y) \tag{1.4}$$

Equation (1.4) is usually called *MacWilliams identity*.

The situation is particularly interesting in the case of self-dual linear codes.

Corollary 1.1. *Let $\mathcal{C}$ be a self-dual linear code over $\mathbb{F}_q$ with respect to the standard inner product. Then its weight enumerator is invariant under the MacWilliams relation* (1.4).

Corollary 1.1 has important consequences on the shape of the weight enumerator and so on the parameters of self-dual linear codes. In the following we will give a brief idea of the methods of Invariant Theory applied to the case of self-dual binary linear codes which are doubly-even. These results are well-known but we explain them here because we will use similar methods in the Chapter 5 to obtain some new results.

Let $\mathbb{C}[x,y]$ the polynomial ring in two variables over the complex field $\mathbb{C}$. We have an action of $\mathrm{GL}_2(\mathbb{C})$ on it: if

$$M := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C}) \qquad \text{and} \qquad p(x,y) \in \mathbb{C}[x,y].$$

then

$$p(x,y)^M := p(ax+by, cx+dy).$$

Let $\mathcal{C}$ be a self-dual binary linear code. Then its weight enumerator, by (1.4), is invariant under the action of

$$G_1 := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C}),$$

that is $W_{\mathcal{C}}(x,y)^{G_1} = W_{\mathcal{C}}(x,y)$.

Furthermore, if $\mathcal{C}$ is doubly-even, $W_{\mathcal{C}}(x,y)$ is also invariant under

$$G_2 := \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

and hence under the group generated by G_1 and G_2, say $G \leq \mathrm{GL}_2(\mathbb{C})$. By direct calculations we see that $|G| = 192$.

The set of all polynomials invariant under a group $H \leq \mathrm{GL}_m(\mathbb{C})$ is a subalgebra of $\mathbb{C}[x,y]$ denoted by $\mathbb{C}[x,y]^H$.

Let $\mathbb{C}[x,y]_d^H$ the subset of all polynomials of degree d in $\mathbb{C}[x,y]^H$. This is a vector space over $\mathbb{C}$. Call $a_d(H)$ its dimension. Then we can define a series as

$$\Phi_H(\lambda) := \sum_{i=0}^{+\infty} a_i(H)\lambda^i.$$

Next we have a classical theorem of Molien.

Theorem 1.4 (Molien's Theorem [43])**.** *For any finite group $H \leq \mathrm{GL}_m(\mathbb{C})$ we have*

$$\Phi(\lambda) = \frac{1}{|H|} \sum_{A \in H} \frac{1}{\det(I - \lambda A)}$$

where I is the identity of $\mathrm{GL}_m(\mathbb{C})$.

For the group $G = \langle G_1, G_2 \rangle$ we get, by calculations,

$$\Phi_G(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} = \sum_{i=0}^{+\infty} \left(\left\lfloor \frac{i}{3} \right\rfloor + 1 \right) \lambda^{8i} \tag{1.5}$$

Gleason then proved a fundamental result.

Theorem 1.5 (Gleason's Theorem [25]). *Let $\mathcal{C}$ be a doubly-even self-dual binary linear code. Then*

$$W_{\mathcal{C}}(x,y) \in \mathbb{C}[p_1(x,y), p_2(x,y)] = \mathbb{C}[x,y]^G,$$

where

$$p_1(x,y) = x^8 + 14x^4y^4 + y^8,$$

that is the weight enumerator of $\hat{\mathcal{H}}_3$, and

$$p_2(x,y) = x^4y^4(x^4 - y^4)^4.$$

An easy but important consequence of Gleason's Theorem is the following.

Corollary 1.2. *Let $\mathcal{C}$ be a doubly-even self-dual binary linear code. Then its length is divisible by 8.*

There are analogous considerations that one can do for self-dual binary linear codes which are not doubly-even or for non-binary codes. For more details on Invariant Theory applied to self-dual codes see for example [46] and [53].

1.7 Extremal self-dual binary linear codes

As we pointed out in Section 1.1, codes with large minimum distance are good for applications. So it is interesting to have upper bounds on the minimum distance. We have already stated the Singleton inequality and the Griesmer bound; however there is a tighter bound for self-dual binary linear codes. It can be obtained by the results of the previous section.

The basic observation in order to get bounds on the minimum distance of self-dual binary linear codes is the following.

Remark 1.2. *If there exists a self-dual binary linear code of length n and minimum distance d, then there exists a homogeneous polynomial $W(x,y)$ with nonnegative (integer) coefficients such that*

$$2^{\frac{n}{2}} W(x+y, x-y) = W(x,y) \qquad (\textit{MacWilliams identity})$$

and

$$W(1,y) = 1 + O(y^d) \qquad (\textit{condition on the minimum distance}).$$

If the code is doubly-even then we have the extra condition

$$W(x,iy) = W(x,y).$$

Let $\mathcal{C}$ be a self-dual doubly-even $[n, \frac{n}{2}, d]$ binary linear code (n is a multiple of 8).

Recall that, by Theorem 1.5, we have $W_{\mathcal{C}}(x,y) \in \mathbb{C}[p_1(x,y), p_2(x,y)]_n$. Furthermore, by (1.5),

$$\dim \mathbb{C}[p_1(x,y), p_2(x,y)]_n = \left\lfloor \frac{n}{24} \right\rfloor + 1.$$

So we can arbitrarily fix $\left\lfloor \frac{n}{24} \right\rfloor + 1$ coefficients of an homogeneous polynomial $W(x,y)$ of $\mathbb{C}[p_1(x,y), p_2(x,y)]_n$.
In particular, there exists a unique element $\bar{W}(x,y) \in \mathbb{C}[p_1(x,y), p_2(x,y)]_n$ such that

$$\bar{W}(1,y) = 1 + O(y^{4\left\lfloor \frac{n}{24} \right\rfloor + 4}).$$

This is known as the *extremal* weight enumerator and it is, obviously, the polynomial of $\mathbb{C}[p_1(x,y), p_2(x,y)]_n$ with constant term 1 and first non-constant term with highest degree. By these considerations Mallows and Sloane proved the following fundamental theorem.

Theorem 1.6 ([40])**.** *The minimum distance of a self-dual doubly-even binary linear code of length n is at most $4\left\lfloor \frac{n}{24} \right\rfloor + 4$.*

Rains generalized this bound to self-dual binary linear codes (not necessarily doubly-even and so of general even length).

Theorem 1.7 ([54])**.** *Let $\mathcal{C}$ be a self-dual $[n, \frac{n}{2}, d]$ binary linear code. Then*

$$d \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \textit{if } n \equiv 22 \bmod 24 \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \textit{otherwise.} \end{cases}$$

Definition 1.18. *Self-dual binary linear codes with minimum distance reaching the bound in Theorem* 1.7 *are called* extremal.
Lengths which are multiple of 24 *are usually called* jump lengths.

Clearly, jump lengths are the ones for which the ratio between n and d is the best, among the self-dual binary linear codes. Another reason for which jump lengths are interesting is the fact, proved also by Rains in [54], that extremal self-dual binary linear codes of length a multiple of 24 are always doubly-even. Furthermore, they have unique weight enumerators.

Let us list the weight distributions of the self-dual $[24m, 12m, 4m+4]$ codes, if they exist,

for $m = 1$,

i	0-24	8-16	12
A_i	1	759	2576

for $m = 2$,

i	0-48	12-36	16-32	20-28	24
A_i	1	17296	535095	3995376	7681680

and for $m = 3$,

i	0-72	16-56	20-52	24-48	28-44	32-40	36
A_i	1	249849	$\sim 2 \cdot 10^7$	$\sim 4 \cdot 10^8$	$\sim 4 \cdot 10^9$	$\sim 10^{10}$	$\sim 2,5 \cdot 10^{10}$

Finally, we will see in the next section a nice combinatorial property of codes with jump length.

Let us conclude the section by giving a brief overview of the state of art of the classification of extremal self-dual binary linear codes.

In 1999, Zhang [55] proved , using linear programming on coefficients of weight enumerators, that extremal self-dual doubly-even binary linear codes can exist only for lengths less than or equal to 3928. However, the largest length for the known extremal doubly-even self-dual binary linear code is

$n = 136$. In particular [53] there exist extremal self-dual doubly-even binary linear codes for the following lengths:

$$8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 136$$

but their existence at lengths 72 and 96 and all greater lengths is open.
For jump lengths only two extremal doubly-even self-dual binary linear codes are known: $\mathcal{G}_{24}$, the famous extended binary Golay code, unique (up to equivalence) with parameters $[24, 12, 8]$ (as Pless proved in [51]) and $\mathcal{XQR}_{48}$, the extended quadratic residue code of length 48, unique (up to equivalence) with parameters $[48, 24, 12]$ (as Houghten and others proved in [30]). The third step of the classification, that is length 72, is still an open problem and it is one of the main reasons for this dissertation.

Question 1.1. *Is there a self-dual* $[72, 36, 16]$ *code?*

1.8 Codes and Designs

Let us introduce briefly a concept which explains another reason that makes the extremal self-dual binary linear codes of jump lengths so interesting.

Definition 1.19. *A* t-(n, k, λ) design *is a pair* $(\mathcal{P}, \mathcal{B})$ *where* $\mathcal{P}$ *is a set of* n points *and* $\mathcal{B}$ *is a collection of distinct subsets of* $\mathcal{P}$ *of size* k*, called* blocks*, such that every subset of points of size* t *is contained in precisely* λ *blocks.*

There is often a correspondence between codes and designs, in the sense that codes can give rise to designs and vice versa.

Given a binary linear code, the usual way to obtain a design from a code is the following: let the coordinates be the points and the supports of the codewords (i.e. the coordinates in which the codewords are not zero) of a given length be the blocks. Then these blocks may form a t-design for some t. In that case we say that the code *holds a design.*

Example 1.7. *Let us consider* $\hat{\mathcal{H}}_3$ (*see Example 1.1*)*. If we set the points to be the* 8 *coordinates and the blocks to be the* 14 *codewords of weight* 4 *of* $\hat{\mathcal{H}}_3$

it is easy to check that every set of three coordinates is contained in precisely one block. Thus $\hat{\mathcal{H}}_3$ *holds a* 3-$(8, 4, 1)$ *design.*

The parameters of designs are not independent and t-designs give naturally rise to i-designs for every $0 \leq i \leq t$, as it states the following Proposition.

Proposition 1.2 (Chapter 8 [32]). *Let* $(\mathcal{P}, \mathcal{B})$ *be a* t-(n, k, λ) *design and* $0 \leq i \leq t$. *Then the number of blocks is*

$$\lambda \frac{\binom{n}{t}}{\binom{k}{t}}.$$

and $(\mathcal{P}, \mathcal{B})$ *is an* i-(n, k, λ_i) *design, where*

$$\lambda_i = \lambda \frac{\binom{n-i}{t-i}}{\binom{k-i}{t-i}}.$$

The main result which links codes to designs is the fundamental theorem proved by Assmus and Mattson in 1969.

Theorem 1.8 (Assmus and Mattson [2]). *Let* $\mathcal{C}$ *be an* $[n, k, d]$ *code. Suppose that* $\mathcal{C}^\perp$ *has minimum distance* d'. *Fix a positive integer* t *with* $t < d$ *and let*

$$s := \#\{i \mid 0 < i \leq n - t \text{ and there exists a } v \in \mathcal{C}^\perp \text{ with } \mathrm{wt}(v) = i\}.$$

Suppose $s \leq d - t$. *Then*

a) *the codewords of weight* i *(if they exist) in* $\mathcal{C}$ *hold a* t*-design provided* $d \leq i \leq n$;

b) *the codewords of weight* i *(if they exist) in* $\mathcal{C}^\perp$ *hold a* t*-design for* $d' \leq i \leq n - t$.

This theorem has a nice and important application to extremal self-dual binary linear codes of length a multiple of 24: let $\mathcal{C}$ be a self-dual $[24m, 12m, 4m+4]$ code and $t = 5$ (so that $5 \leq 4m + 4$). Thus $s = 4m - 1 = 4m + 4 - 5$. Then the nonzero codewords of a fixed weight hold a 5-design.

So for example the codewords of weight 8 of the extended binary Golay code give rise to a 5-$(24, 8, 1)$ design, the codewords of weight 12 of the extended quadratic residue code of length 48 hold a 5-$(48, 12, 8)$ design. If a self-dual $[72, 36, 16]$ code exists, then its codewords of weight 16 will give rise to a 5-$(72, 16, 78)$ design.

1.9 Some preliminaries on KG-modules

If a binary linear code has a non-trivial automorphism group, then we can deduce many properties via a module-theoretical approach. We explain in this section some preliminaries on the main objects which will appear in the dissertation. For very basic facts and definitions about modules, the reader is referred to Chapter VII of [34] or to the introduction of [19].

Throughout the section, let G be a group and $K := \mathbb{F}_2$. Recall that the *group algebra* KG is defined as

$$KG := \left\{ \sum_{g \in G} k_g g \;\middle|\; k_g \in K \right\},$$

that is the set of formal linear combination of the elements of G, with sum and product defined in the most natural way.

In the following the action of G on a module will always be from the right (so that all KG-modules are right modules). In particular, if $v \in K^n$ and $G \leq \mathcal{S}_n$,

$$v \cdot \left(\sum_{g \in G} k_g g \right) = \sum_{g \in G} k_g v^g.$$

With this product, a binary linear code is a KG-module for any subgroup G of its automorphism group.

Next we define an object, not so elementary, which plays a fundamental role in our methods.

Definition 1.20. *A* projective (*or principal*) indecomposable module (*PIM*)

of KG is a submodule of KG that is a direct summand of KG and is an indecomposable module.

A projective indecomposable module W has a unique irreducible submodule, say V, and a unique irreducible factor module which is isomorphic to V.

Notation 1.2. *The module W, which is (up to isomorphism) uniquely determined by V, is the* projective cover *of V and we denote it by $\mathrm{P}(V)$. For a module $\mathcal{M}$ we denote by $\mathrm{soc}(\mathcal{M})$ its socle, i.e. the largest completely reducible submodule of $\mathcal{M}$ (as V in W).*

Projective covers for irreducible KG-modules always exist (actually they exist for any finite dimensional KG-module).

Let fix two important notations.

Notation 1.3.

- *If p is an odd prime, $\mathrm{s}(p)$ is the* multiplicative order *of 2 in $\mathbb{F}_p$, i.e. the smallest r such that $p|2^r - 1$.*
- *C_m is the cyclic group of order m.*

Since the number $\mathrm{s}(p)$ plays a very important role in the following, we collect in a table the values of $\mathrm{s}(p)$ for all odd primes p less than 100.

Table 1.1: Values of $\mathrm{s}(p)$, $p < 100$

p	$\mathrm{s}(p)$	p	$\mathrm{s}(p)$	p	$\mathrm{s}(p)$
3	2	29	28	61	60
5	4	31	5	67	66
7	3	37	36	71	35
11	10	41	20	73	9
13	12	43	14	79	39
17	8	47	23	83	82
19	18	53	52	89	11
23	11	59	58	97	48

In next chapters we deal mainly with automorphisms of order p or $2p$, where p is an odd prime. For this reason we put in evidence the following facts about the structure of the group algebra for $G = C_p$ and $G = C_{2p}$.

Remark 1.3. *Let p be an odd prime and*

$$t := \frac{p-1}{\mathrm{s}(p)}.$$

Then we have the following.

a) *There are $1+t$ irreducible KC_p-modules $V_0, V_1, \ldots, V_t$, where $V_0 = K$ (the trivial module) and $\dim V_i = \mathrm{s}(p)$ for $i \in \{1, \ldots, t\}$, so that*

$$KC_p = V_0 \oplus V_1 \oplus \ldots \oplus V_t.$$

b) *There are $1+t$ irreducible KC_{2p}-modules V_0, $V_1, \ldots, V_t$, as before. Setting $W_i := \mathrm{P}(V_i)$, we have $W_i = \begin{matrix} V_i \\ V_i \end{matrix}$, a non-split extension of V_i by V_i, so that*

$$KC_{2p} = W_0 \oplus W_1 \oplus \ldots \oplus W_t.$$

An important concept in the theory of modules is the duality (do not confuse with the duality of codes).

Definition 1.21. *Given a KG-module W we define the* dual *module $V^\star$ as follows:*

$$V^\star = \mathrm{Hom}_K(V, K).$$

This is a KG-module by

$$(\phi \cdot g)(v) = \phi(vg^{-1}),$$

where $\phi \in V^\star, g \in G$ and $v \in V$.

A module V is self-dual *if $V \cong V^\star$ (as KG-modules).*

The following result on self-dual modules improves Proposition 3.1 of [41].

Proposition 1.3. *Consider $G = C_p$, the cyclic group of odd prime order p.*

a) *If $s(p)$ is even, then all irreducible KC_p-modules are self-dual.*

b) *If $s(p)$ is odd, then the trivial module is the only self-dual irreducible KC_p-module.*

Proof. a) Let $\mathrm{s}(p) = 2m$ and let $E := \mathbb{F}_{2^{2m}}$ be the extension of K of degree $2m$. Furthermore, let W be an irreducible non-trivial KG-module. In particular, W has dimension $2m$. We have

$$W \otimes_K E = \oplus_{\alpha \in \mathrm{Gal}(E/K)} V^\alpha \tag{1.6}$$

where V is an irreducible EG-module and V^α is the α-conjugate module of V. The action of $g \in G$ on V^α is given by the matrix $(a_{i,j}(g)^\alpha)$ if g acts via the matrix $(a_{i,j}(g))$ on V. Since $p \mid (2^m+1)(2^m-1)$ we get $p \mid 2^m+1$. Clearly, the Galois group Gal(E/K) of E over K consists of all automorphisms of the form $x \mapsto x^{2^k}$ where $0 \leq k \leq 2m-1$.

If $V = \langle v \rangle$ then $v \cdot g = \epsilon v$ where ϵ is a non-trivial p-th root of unity in E. Since $p \mid 2^m + 1$ we obtain $\epsilon^{2^m+1} = 1$, hence $\epsilon^{2^m} = \epsilon^{-1}$. Thus there is an $\alpha \in \mathrm{Gal}(E/K)$ such that

$$V^\star \cong V^\alpha$$

and Equation (1.6) implies $W \cong W^\star$.

b) Now let $\mathrm{s}(p) = m$ be odd. As above the irreducible module W is self-dual if and only if $V^\star \cong V^\alpha$ for some $\alpha \in \mathrm{Gal}(\mathbb{F}_{2^m}/K)$, or equivalently if and only if $\epsilon^\alpha = \epsilon^{-1}$. Suppose that such an α exists. Then we may write $\epsilon^\alpha = \epsilon^{2^k}$ where $0 \leq k \leq m-1$. Hence $\epsilon^{2^k} = \epsilon^{-1}$ for some $0 \leq k \leq m-1$ and therefore $2^k \equiv -1 \bmod p$. Now $2^{2k} \equiv 1 \bmod p$ forces $m \mid 2k$. Since m is odd we get $m \mid k \leq m-1$, a contradiction. □

Remark 1.4. *According to Lemma 3.5 in* [41] *we have* $\mathrm{s}(p)$ *even if* $p \equiv \pm 3 \bmod 8$ *and* $\mathrm{s}(p)$ *odd if* $p \equiv -1 \bmod 8$.

Let us summarize the results in the following remark.

Remark 1.5. *Since* $KC_p \cong KC_p^\star$ (*see* [34], *Chap. VII, Lemma 8.23*), *Remark 1.3 and Proposition 1.3 imply the following.*

a) *If* $\mathrm{s}(p)$ *is even, then*

$$KC_p = W_0 \oplus W_1 \oplus \ldots \oplus W_t$$

with $W_i \cong W_i^\star$ *for all* $i \in \{0, \ldots, t\}$.

b) *If* $\mathrm{s}(p)$ *is odd, then* t *is even* (*put* $t = 2m$) *and*

$$KC_p = W_0 \oplus W_1 \oplus \ldots \oplus W_{2m}$$

with $W_0 \cong W_0^\star$ *and* $W_i \cong W_{2i}^\star$ *for all* $i \in \{1, \ldots, m\}$.

CHAPTER 2

Automorphisms of self-dual binary linear codes: general methods

In this chapter we will present some results about the automorphism group of self-dual binary linear codes. The main idea is to give structure results for self-dual binary linear codes which have particular automorphisms. Usually, as we have already said in the introduction, we want to find out "smaller pieces" which are easier to study and then try to construct the whole code from these "smaller pieces".

The results of the first two sections are mainly known, while the presentation of the last sections is new. Chapter 3 and Chapter 4 will prove the power of the results presented in this chapter.

2.1 Structure theorems

In this section we make some considerations on the cycle structure (i.e. the decomposition into disjoint cycles) of automorphisms which can occur in

codes with certain parameters. They mainly follow from the structure of the fixed codes.

Let $\mathcal{C}$ be a binary linear code of length n and $\sigma \in \mathrm{Aut}(\mathcal{C})$. Recall that, as mentioned in Chapter 1, the fixed code of σ is defined as $\mathcal{C}(\sigma) := \{c \in \mathcal{C} \mid c^\sigma = c\}$. Finally, let π_σ be the natural projection associated to σ in Definition 1.17.

In case σ has odd order, we have a very important and classical theorem proved by Conway and Pless.

Theorem 2.1 ([18])**.** *Let $\mathcal{C}$ be a binary linear code and $\sigma \in \mathrm{Aut}(\mathcal{C})$ of odd order.*

- *If $\mathcal{C}$ is self-orthogonal (self-dual) then $\pi_\sigma(\mathcal{C}(\sigma))$ is self-orthogonal (self-dual).*
- *If $\mathcal{C}$ is doubly-even and all cycles of σ have length $\equiv 1 \bmod 4$, then $\pi_\sigma(\mathcal{C}(\sigma))$ is doubly-even.*

The assertion of the above theorem does not hold for automorphisms of even order, in general.

For example, if σ is an automorphism of order 2 and $n \equiv 2 \bmod 4$, then

$$\pi_\sigma(\mathcal{C}(\sigma)) \leq \mathbb{F}_2^{\frac{n}{2}}$$

cannot be self-dual, since $\frac{n}{2}$ is odd.

In $\mathcal{G}_{24}$ and $\mathcal{XQR}_{48}$ the fixed codes by fixed point free involutions have self-dual projections. Thus we wonder if the same holds for all extremal self-dual binary linear codes of jump lengths.

Question 2.1. *Let $\mathcal{C}$ be a self-dual $[24m, 12m, 4m+4]$ code and $\sigma \in \mathrm{Aut}(\mathcal{C})$ a fixed point free involution. Is $\pi_\sigma(\mathcal{C}(\sigma))$ always self-dual?*

In the next theorem we collect some conditions on the cycle structure of automorphisms of odd prime order of self-dual binary linear codes. Conditions a),b),c) and d) are a generalization of the results in [18], e) and f) are proved in [62], g) is obvious by Theorem 2.1 and Corollary 1.2, and h) is proved in [15].

Theorem 2.2. *Let $\mathcal{C}$ be a self-dual $[n, \frac{n}{2}, d]$ code and suppose $\sigma \in \mathrm{Aut}(\mathcal{C})$ of type p-(c, f), p odd prime. Then the following conditions hold:*

a) $2^{\frac{n}{2}} \equiv 2^{\frac{c+f}{2}} \bmod p$;

b) $\frac{c+f}{2} \geq \min\{d-1, f\}$;

c) *if $p < d$ and m is the largest integer ($\leq c$) such that $mp < d$, then* $(c-m)(p-1) \geq d-2$;

d) *if $p < 2d-3$ then $c > 1$;*

e)
$$pc \geq \sum_{i=0}^{\frac{(p-1)c}{2}-1} \left\lceil \frac{d}{2^i} \right\rceil$$
where the equality does not occur if $d \leq 2^{\frac{(p-1)c}{2}-2} - 2$;

f) *if $f > c$ then*
$$f \geq \sum_{i=0}^{\frac{f-c}{2}-1} \left\lceil \frac{d}{2^i} \right\rceil$$
where the equality does not occur if $d \leq 2^{\frac{f-c}{2}-2} - 2$;

g) *if $\mathcal{C}$ is doubly-even and $p \equiv 1 \bmod 4$, then 8 divides $c+f$;*

h) *if $\mathcal{C}$ is extremal of length $n \geq 48$ and $p > 5$, then $c \geq f$.*

Proof. We give the proof only of a), b), c) and d) referring the reader to the original papers for the other statements.

a) Let us consider the action of the group $\langle\sigma\rangle$ on the codewords of $\mathcal{C}$. The orbits have cardinality 1, if the codeword is fixed, and p, otherwise. Thus $|\mathcal{C}| \equiv |\mathcal{C}(\sigma)| \bmod p$. The conclusion follows from Theorem 2.1 which states that $\pi_\sigma(\mathcal{C}(\sigma))$ is self-dual.

b) Since $\mathcal{C}$ has minimum distance d, any $d-1$ columns of every generator matrix $\mathrm{G}(\mathcal{C})$ of $\mathcal{C}$ are independent. Look at the f coordinates fixed by σ: a generator matrix $\mathrm{G}(\pi_\sigma(\mathcal{C}(\sigma)))$ (whose f columns are exactly the same of $\mathrm{G}(\mathcal{C})$) has at least $\min\{d-1, f\}$ columns linearly independent. The rank of $\mathrm{G}(\pi_\sigma(\mathcal{C}(\sigma)))$ is $\frac{c+f}{2}$ and this has to be greater than or equal to $\min\{d-1, f\}$.

c) Suppose $(c-m)(p-1) < d-2$. Consider m cycles. The corresponding coordinates are independent (see Section 1.1). Hence there is $v \in \mathcal{C}$ with only one value equal to 1 on the coordinates of these m cycles. On a general cycle Ω we have that $\mathrm{wt}(v_{|\Omega} + v^\sigma_{|\Omega})$ is obviously even and so it less than p. Thus

$$\mathrm{wt}(v + v^\sigma) \leq 2 + (c-m)(p-1) < d,$$

a contradiction.

d) Suppose $c = 1$. As in c), there exists $v \in \mathcal{C}$ such that $\min\{d-1, p\}$ values on the coordinates of the single cycle are all 0 except for only one 1. Then

$$\mathrm{wt}(v + v^\sigma) \leq 2 + (p - (d-1)) < d,$$

a contradiction again.

□

Other restrictions on the cycle structure of the automorphisms can be obtained by the following observations, contained again in [18].

Let $\mathcal{C}$ be a binary linear code of length n and let σ be an automorphism of type p-(c, f), p an odd prime.

As we have underlined in Remark 1.1, we may suppose, up to a permutation of the coordinates, that the f fixed coordinates are the last ones. We choose a generator matrix

$$\mathrm{G}(\pi_\sigma(\mathcal{C}(\sigma))) = \begin{bmatrix} A & 0 \\ 0 & B \\ D & E \end{bmatrix}$$

where

- A is a generator matrix of $\mathcal{A} := \pi_\sigma(\mathcal{C}(\sigma))_{T_f}$, the shortened code on the set T_f of fixed coordinates;
- B is a generator matrix of $\mathcal{B} := \pi_\sigma(\mathcal{C}(\sigma))_{T_c}$, the shortened code on T_c which is the set of remaining coordinates.

Obviously, $\mathcal{B}$ is also the $\mathcal{C}_T$, where T are the first pc coordinates. In particular, the minimum distance of $\mathcal{B}$ is greater than or equal to d.

Let $\mathcal{D}$ and $\mathcal{E}$ be the subspace generated by D and E respectively and let k_A, k_B, k_D and k_E the rank of the matrices A, B, D and E respectively.

We have a nice theorem which relates these ranks to the cycle structure and gives further properties.

Theorem 2.3 ([52]). *If $\mathcal{C}$ is self-dual, then*

a) $k_D = k_E$;

b) $c = 2k_A + k_D$;

c) $f = 2k_B + k_E$;

d) $A^\perp = A + D$, $B^\perp = B + E$.

Notice that $\mathcal{B}$ is an $[f, k_B, d]$ code. By the well-known Hamming Bound, that is

$$A(f,d)\sum_{i=0}^{d}\binom{n}{i} \leq 2^f,$$

where $A(f,d)$ is the maximum size of a binary code of length f and minimum distance d, one obtains further restrictions on the possible type of automorphisms.

Many examples of this last method are contained in [18], in which Conway and Pless excluded many types of automorphisms of the putative extremal self-dual binary linear code of length 72.

Let us underline that restrictions on the type of automorphisms of prime order have implications on the possible automorphisms of non-prime order. For example, if all the possible automorphisms of order p of a code are of type p-(c, f) with c not divisible by p, then obviously the code has no automorphism of order p^2.

It holds even more, as we can see in the following result.

Proposition 2.1 ([14]). *Let $\mathcal{C}$ be a binary linear code of length n. Suppose that for every automorphism of $\mathcal{C}$ of type p-(c, f), c is not divisible by p and $f < p$. Then p^2 does not divide $|\mathrm{Aut}(\mathcal{C})|$.*

To conclude, let us mention that further information about the cardinality of the automorphism group can be obtained by Burnside Lemma, which in particular says that

$$t := \frac{1}{|\mathrm{Aut}(\mathcal{C})|} \sum_{\sigma \in \mathrm{Aut}(\mathcal{C})} \mathrm{Fix}(\sigma)$$

has to be a nonnegative integer (since it is the number of the orbits of the action on the coordinates).

We show the power of these results in the next chapters.

2.2 Decomposition of a code with an automorphism of odd prime order

In the search of codes with certain parameters, it is often useful to decompose them as a direct sum of smaller pieces which are easier to determine. In this section we will present a classical decomposition of codes with automorphisms of odd prime order. Such decomposition is just a particular reformulation of Maschke's Theorem. However, in this context we want to present it from a different point of view, i.e. with polynomials, because in this way it is easier to implement for calculations.

Let $\mathcal{V} := \mathbb{F}_2^n$ and $\sigma \in \mathcal{S}_n$ a permutation of odd prime order p. Then, it is trivial to prove that

$$\mathcal{V} = \mathcal{V}(\sigma) \oplus \mathcal{V}(\sigma)^\perp$$

where

- $\mathcal{V}(\sigma)$ is the subspace fixed by σ (that is the set of vectors constant on the orbits of σ);
- $\mathcal{V}(\sigma)^\perp$ it the dual of $\mathcal{V}(\sigma)$ (that is the set of even-weight vectors on the orbits of σ).

We underline here that, when we say direct sum, *we mean the normal direct sum between subspaces*. This will hold throughout the dissertation.

We will divide the presentation into three parts, dealing firstly with the easiest case, going then to the general case and finally dealing with a special case.

2.2.1 Case $n = p$

Let $n = p$, so that σ has only one orbit of order p. Thus

$$\mathrm{G}(\mathcal{V}(\sigma)) = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 & 1 \end{bmatrix} \in \mathrm{Mat}_{1,p}(\mathbb{F}_2)$$

and

$$\mathrm{G}(\mathcal{V}(\sigma)^\perp) = \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \end{bmatrix} \in \mathrm{Mat}_{p-1,p}(\mathbb{F}_2)$$

There is a natural identification between

$$\varphi : \mathbb{F}_2^p \to \mathbb{F}_2[x]/(x^p + 1) =: Q \tag{2.1}$$

which maps $(v_0, \dots, v_{p-1}) \mapsto v_0 + \dots + v_{p-1}x^{p-1}$.

Notice that $x^p+1=(x+1)(x^{p-1}+x^{p-2}+\ldots+x+1)$, with $(x+1)$ and $(x^{p-1}+x^{p-2}+\ldots+x+1)$ coprime (since p is odd).

As usual, $\mathrm{s}(p)$ denotes the order of 2 in $\mathbb{F}_p^\times$, so it is the minimal positive integer l such that $p|2^l-1$.

Lemma 2.1. *The polynomial $x^{p-1}+x^{p-2}+\ldots+x+1\in\mathbb{F}_2[x]$ is the product of $t:=\frac{p-1}{\mathrm{s}(p)}$ irreducible polynomials of degree $\mathrm{s}(p)$.*

Proof. Consider $\mathbb{F}_{2^{\mathrm{s}(p)}}$. Since $p|2^{\mathrm{s}(p)}-1$ we take $\alpha\in\mathbb{F}_{2^{\mathrm{s}(p)}}^\times$ such that $\langle\alpha\rangle\cong C_p$. Then $\mathbb{F}_2(\beta)=\mathbb{F}_{2^{\mathrm{s}(p)}}$ for every $\beta\in\langle\alpha\rangle\setminus\{1\}$, since $\mathrm{s}(p)$ is minimal. Now

$$x^{p-1}+x^{p-2}+\ldots+x+1=\frac{x^p-1}{x-1}=\prod_{\beta\in\langle\alpha\rangle\setminus\{1\}}(x-\beta)$$

To conclude, it is enough to remember that

$$\prod_{q(x)\ \text{irr. in}\ \mathbb{F}_2[x],\ \deg q(x)=\mathrm{s}(p)} q(x)=\prod_{\zeta\ \text{s.t.}\ \mathbb{F}_2(\zeta)=\mathbb{F}_{2^{\mathrm{s}(p)}}}(x-\zeta),$$

so that

$$\prod_{q(x)\ \text{irr. in}\ \mathbb{F}_2[x],\ \deg q(x)=\mathrm{s}(p)} q(x)=(x^{p-1}+x^{p-2}+\ldots+x+1)\cdot r(x)$$

for a certain $r(x)\in\mathbb{F}_2[x]$. □

Let $x^p+1=q_0(x)q_1(x)\ldots q_t(x)$, where $q_0(x):=x+1$ and the other terms are the t irreducible polynomials of Lemma 2.1. By the Chinese Remainder Theorem we have

$$\begin{aligned}\mathbb{F}_2[x]/(x^p+1)=Q &\cong \mathbb{F}_2[x]/(q_0(x))\oplus\mathbb{F}_2[x]/(q_1(x))\oplus\ldots\oplus\mathbb{F}_2[x]/(q_t(x))\cong\\ &\cong \mathbb{F}_2\oplus\mathbb{F}_{2^{s(p)}}\oplus\ldots\oplus\mathbb{F}_{2^{s(p)}}\end{aligned}$$

Furthermore, calling $Q_j:=\frac{x^p+1}{q_j(x)}$ we have

$$\mathbb{F}_2[x]/(q_j(x))\cong(Q_j)=:\mathcal{I}_j$$

which is a principal ideal of $\mathbb{F}_2[x]/(x^p+1)$ generated by Q_j. Notice that (the equalities are mod x^p+1)

- $Q_j^2 = Q_j$,
- $Q_i Q_j = 0$ if $i \neq j$.

Then

$$\mathbb{F}_2[x]/(x^p + 1) = \mathcal{I}_0 \perp \mathcal{I}_1 \perp \ldots \perp \mathcal{I}_t$$

is an orthogonal sum of ideals (generated by orthogonal idempotents), such that $\mathcal{I}_0 \cong \mathbb{F}_2$ and $\mathcal{I}_1 \cong \ldots \cong \mathcal{I}_t \cong \mathbb{F}_{2^{s(p)}}$.

2.2.2 General case

Let now n be general and σ of type p-(c, f). Without lost of generality we can relabel the coordinates to have

$$\sigma = (1, \ldots, p)(p+1, \ldots, 2p) \ldots, ((c-1)p+1, \ldots, pc)$$

Recall that $\mathcal{V}(\sigma)^\perp$ is the set of all even-weight vectors on the orbits of σ. Thus it holds $v_i = 0$, $i = pc+1, \ldots, n$ for every $v \in \mathcal{V}(\sigma)^\perp$. Let us call

$$(\mathcal{V}(\sigma)^\perp)^* \leq \mathbb{F}_2^{pc}$$

the space obtained puncturing $\mathcal{V}(\sigma)^\perp$ on the last f coordinates.

We defined in (2.1) the map $\varphi : \mathbb{F}_2^p \to Q$, where $Q = \mathbb{F}_2[x]/(x^p+1)$. Now, we can extend cycle-wise the map φ to a map φ_p in the following way:

$$\varphi_p := \underbrace{\varphi \times \ldots \times \varphi}_{c \text{ times}} : \mathbb{F}_2^{pc} \to Q^c,$$

via the natural identification $(\mathbb{F}_2^p)^c = \mathbb{F}_2^{pc}$.

Let φ_p' the map $\varphi_p \times \mathrm{id}_f$, where $\mathrm{id}_f := \mathbb{F}_2^f \to \mathbb{F}_2^f$ is the identity map, so that

$$\varphi_p' : \mathbb{F}_2^n \xrightarrow{\sim} Q^c \oplus \mathbb{F}_2^f.$$

This map gives us the identification

$$\mathbb{F}_2^n \cong \mathbb{F}_2^{c+f} \oplus \mathbb{F}_{2^{s(p)}}^c \oplus \ldots \oplus \mathbb{F}_{2^{s(p)}}^c$$

It is easy to observe that

$$\varphi'_p(\mathcal{V}(\sigma)) \cong \mathbb{F}_2^{c+f} \qquad \text{and} \qquad \varphi_p(\mathcal{V}(\sigma)^{\perp^*}) \cong \mathbb{F}_{2^{s(p)}}^c \oplus \ldots \oplus \mathbb{F}_{2^{s(p)}}^c.$$

Notice that $\varphi'_{p_{|\mathcal{V}(\sigma)}}$ is the projection π_σ defined in Section 1.5.

Now, we note that $\mathcal{C}(\sigma) = \mathcal{C} \cap \mathcal{V}(\sigma)$ and we define $\mathcal{E}(\sigma) := \mathcal{C} \cap \mathcal{V}(\sigma)^\perp$. Then we have the following classical theorem.

Theorem 2.4. *Let $\mathcal{C}$ be a self-dual binary linear code and suppose $\sigma \in \mathrm{Aut}(\mathcal{C})$ of odd prime order. Then*

$$\mathcal{C} = \mathcal{C}(\sigma) \oplus \mathcal{E}(\sigma), \tag{2.2}$$

where $\mathcal{C}(\sigma)$ is the fixed code of σ and $\mathcal{E}(\sigma)$ is the subcode of even-weight codewords on the cycle of σ.

As we have said in the introduction of this section, this result is just a particular case of Maschke's Theorem: let us consider the group algebra $\mathbb{F}_2\langle\sigma\rangle$. Then we have

$$\mathbb{F}_2\langle\sigma\rangle = \mathcal{J}_0 \oplus \mathcal{J}_1 \oplus \ldots \oplus \mathcal{J}_t$$

where $\mathcal{J}_i$ are two-sided ideals. If we write

$$1 = f_0 + f_1 + \ldots + f_t$$

with $f_i \in \mathcal{J}_i$ then $f_i f_j = \delta_{i,j} f_i$, where $\delta_{i,j}$ is the Kronecker's delta. This is called a *decomposition of* 1 *in (central) orthogonal idempotents*. Whenever $\mathcal{J}_i$ is isomorphic to a field we say that the idempotent is *primitive*. Decomposition (2.2) comes by taking

$$f_0 := 1 + \sigma + \ldots + \sigma^{p-1}$$

and

$$f_1 := \sigma + \ldots + \sigma^{p-1}.$$

It is straightforward to observe that $\mathcal{C}(\sigma) = \mathcal{C}f_0$ and $\mathcal{E}(\sigma) = \mathcal{C}f_1$. Thus it is clear that $\mathcal{C}(\sigma)$ and $\mathcal{E}(\sigma)$ are also $\mathbb{F}_2\langle\sigma\rangle$-submodules of $\mathcal{C}$.

2.2.3 Case n general and $\mathrm{s}(p) = p - 1$

Let us consider now the important case in which $\mathrm{s}(p) = p - 1$. Then $\varphi(\mathcal{V}(\sigma)^{\perp^*}) \cong \mathbb{F}_{2^{p-1}}^c$ and, on the other hand, the idempotents f_0 and f_1 are both primitive. So

$$\pi_\sigma(\mathcal{C}(\sigma)) \leq \mathbb{F}_2^{c+f} \qquad \text{and} \qquad \varphi_p(\mathcal{E}(\sigma)^*) \leq \mathbb{F}_{2^{p-1}}^c.$$

We state now a very important theorem, proved by Yorgov.

Theorem 2.5 ([62]). *Let $\mathcal{C}$ be a binary linear code with an automorphism σ of odd prime order p, with $\mathrm{s}(p) = p - 1$. Then the following are equivalent:*

a) *$\mathcal{C}$ is self-dual.*

b) *$\pi_\sigma(\mathcal{C}(\sigma))$ is self-dual and $\varphi_p(\mathcal{E}(\sigma)^*)$ is Hermitian self-dual.*

Thus we have the following.

Corollary 2.1. *Let $\mathcal{C}$ a self-dual binary linear code with an automorphism σ of type p-(c, f), where p is an odd prime with $\mathrm{s}(p) = p - 1$. Then c and f are even.*

Proof. Since $\varphi_p(\mathcal{E}(\sigma)^*)$ is Hermitian self-dual, its length c has to even. Also $\pi_\sigma(\mathcal{C}(\sigma))$ is self-dual, so that its length $c + f$ is even. Then f is even. □

Let us conclude this section with an example in the significant case $p = 3$.

Example 2.1. *Let $p = 3$. In this case the identification is given by table 2.1. Let now $\mathcal{C}$ be a self-dual $[8, 4, 2]$ code with generator matrix*

$$\mathrm{G}(\mathcal{C}) := \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

We have an automorphism $\sigma := (1, 2, 3)(4, 5, 6)$. Then

$$\mathrm{G}(\mathcal{C}(\sigma)) := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

Table 2.1: Identification $\mathbb{F}_2^3(\sigma)^\perp$ - $\mathbb{F}_4$

$\mathbb{F}_2^3(\sigma)^\perp$	$\mathbb{F}_4$
$(0,0,0)$	0
$(0,1,1)$	1
$(1,1,0)$	ω
$(1,0,1)$	ω^2

$$\mathrm{G}(\mathcal{E}(\sigma)) := \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

so that

$$\mathrm{G}(\pi_\sigma(\mathcal{C}(\sigma))) := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad \mathrm{G}(\varphi_3(\mathcal{E}(\sigma)^*)) := \begin{bmatrix} \omega & \omega \end{bmatrix},$$

self-dual $[4,2,2]$ *code and Hermitian self-dual* $[2,1,2]_4$ *code respectively.*

2.3 Self-dual codes with an automorphism of order $2p$, p odd prime

Throughout this section let $\mathcal{C}$ be a self-dual binary linear code of length n (remember that n has to be even) with an automorphism σ_{2p} of order $2p$, where p is an odd prime. We will study some module theoretical properties of such a code, showing a nice connection with the structure of the fixed code of the involution σ_{2p}^p.

2.3.1 Main theorem

Suppose that $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$ is of order $2p$, where p is an odd prime. Furthermore suppose that the involution $\sigma_2 := \sigma_{2p}^p$ acts fixed point freely on the n coordinates. Without loss of generality, we may assume that

$$\sigma_2 = \sigma_{2p}^p = (1,2)(3,4)\ldots(n-1,n).$$

We consider the natural projection $\pi_{\sigma_2} : \mathcal{C}(\sigma_2) \to \mathbb{F}_2^{\frac{n}{2}}$ (defined in Section 1.5) and the map

$$\phi : \mathcal{C} \to \mathbb{F}_2^{\frac{n}{2}}, \tag{2.3}$$

with $(c_1, c_2, \ldots, c_{n-1}, c_n) \overset{\phi}{\mapsto} (c_1 + c_2, \ldots, c_{n-1} + c_n)$.

Bouyuklieva proved that ([11], Theorem 1)

$$\phi(\mathcal{C}) \leq \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) = \phi(\mathcal{C})^{\perp}.$$

In particular,

$$\phi(\mathcal{C}) = \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) = \phi(\mathcal{C})^{\perp} \quad \text{(i.e. } \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \text{ is self-dual)}$$

if and only if

$$\dim \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) = \dim \mathcal{C}(\sigma_2) = \frac{n}{4}.$$

Recall that a projective $\mathbb{F}_2G$-module is a finite direct sum of projective indecomposable modules, or, in other words, it is a direct summand of a finite direct sum of copies isomorphic to the group algebra $\mathbb{F}_2G$ (as $\mathbb{F}_2G$-modules). Then we have the following result (that is the crucial theorem of our joint work with Wolfgang Willems [10]).

Theorem 2.6. *The code $\mathcal{C}$ is a projective $\mathbb{F}_2\langle\sigma_{2p}\rangle$-module if and only if $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ is self-dual.*

Proof. First note that for an arbitrary finite group G a $\mathbb{F}_2G$-module is projective if and only if its restriction to a Sylow 2-subgroup is projective.
Thus we have to consider the restriction $\mathcal{C}_{|\langle\sigma_2\rangle}$, i.e., $\mathcal{C}$ with the action of $\langle\sigma_2\rangle$. Since the only indecomposable modules in $\mathbb{F}_2\langle\sigma_2\rangle$ are the trivial one, $K \cong \mathbb{F}_2$, of dimension 1, and the regular one, R, of dimension 2, we have that $\mathcal{C}$, as a $\mathbb{F}_2\langle\sigma_2\rangle$-module, is

$$\mathcal{C} \cong \underbrace{R \oplus \ldots \oplus R}_{a \text{ times}} \oplus \underbrace{K \oplus \ldots \oplus K}_{\frac{n}{2}-2a \text{ times}}.$$

Then

$$\mathcal{C}(\sigma_2) = \operatorname{soc}(\mathcal{C}) = \underbrace{K \oplus \ldots \oplus K}_{a \text{ times}} \oplus \underbrace{K \oplus \ldots \oplus K}_{\frac{n}{2}-2a \text{ times}} \cong K^{\frac{n}{2}-a}.$$

Thus $\mathcal{C}$ is projective if and only if $\frac{n}{2} - 2a = 0$, hence if and only if $a = \frac{n}{4}$. This happens if and only if $\dim \mathcal{C}(\sigma_2) = \frac{n}{4}$. This is equivalent to the fact that $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ is self-dual. □

The main reason for which it is so interesting to determine if a code is projective, is the following remark, which helps a lot in constructing codes.

Remark 2.1. *Let G be a finite group and $\mathcal{M}$ a projective KG-submodule. Then for every decomposition*

$$\mathrm{soc}(\mathcal{M}) = V_1 \oplus \ldots \oplus V_m$$

of the socle in irreducible KG-submodules, we have

$$\mathcal{M} \cong \mathrm{P}(V_1) \oplus \ldots \oplus \mathrm{P}(V_m),$$

where $\mathrm{P}(V_i)$ is the projective cover of V_i in $\mathcal{M}$, for all $i \in \{1, \ldots, m\}$.

So, whenever we have a projective module, there are several restrictions on its structure and, in particular, the knowledge of its socle gives us a lot of information about the whole module.

2.3.2 Consequences on the structure of $\mathcal{C}$

Next we deduce some properties of $\mathcal{C}$ related to the action of the automorphism σ_{2p}. This may also help to decide whether $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ is self-dual or not.

Since σ_2 acts fixed point freely, σ_{2p} has x $2p$-cycles and w 2-cycles, with

$$n = 2px + 2w. \tag{2.4}$$

Thus, as an $\mathbb{F}_2\langle\sigma_{2p}\rangle$-module, we have the decomposition

$$\mathbb{F}_2^n = \underbrace{\mathbb{F}_2\langle\sigma_{2p}\rangle \oplus \ldots \oplus \mathbb{F}_2\langle\sigma_{2p}\rangle}_{x \text{ times}} \oplus \underbrace{\mathbb{F}_2\langle\sigma_2\rangle \oplus \ldots \oplus \mathbb{F}_2\langle\sigma_2\rangle}_{w \text{ times}}.$$

Using Remark 1.3 and setting $V_0 \cong \mathbb{F}_2$, we get

$$\mathbb{F}_2^n = \underbrace{\begin{matrix} V_0 & & V_0 \\ V_0 & \oplus\ldots\oplus & V_0 \end{matrix}}_{x+w \text{ times}} \oplus\ldots\oplus \underbrace{\begin{matrix} V_t & & V_t \\ V_t & \oplus\ldots\oplus & V_t \end{matrix}}_{x \text{ times}}.$$

The action of $\langle\sigma_{2p}\rangle$ on $\mathbb{F}_2^n$ and the self-duality of $\mathcal{C}$ restrict the possibilities for $\mathcal{C}$ as a subspace of $\mathbb{F}_2^n$: let us prove a technical lemma and then prove a more precise proposition.

Lemma 2.2. *Let $\mathcal{C}$ be a binary linear code of length n and let $G \leq \mathrm{Aut}(\mathcal{C})$ so that $\mathcal{C}$ is a $\mathbb{F}_2G$-module. Then*

$$\mathbb{F}_2^n/\mathcal{C}^\perp \cong \mathcal{C}^\star,$$

as $\mathbb{F}_2G$-modules, where $\mathcal{C}^\star$ is the dual module of $\mathcal{C}$.
In particular, if $\mathcal{C}$ is self-dual, we have

$$\mathbb{F}_2^n/\mathcal{C} \cong \mathcal{C}^\star.$$

Proof. Recall that $\mathcal{C}^\star = \mathrm{Hom}_{\mathbb{F}_2}(\mathcal{C}, \mathbb{F}_2)$. We define the map

$$\psi : \mathbb{F}_2^n \to \mathcal{C}^\star$$

by $\psi(v) = \langle v, \cdot\ \rangle$, where $\langle\cdot,\cdot\rangle$ is the standard inner product. The map ψ is obviously $\mathbb{F}_2$-linear. Since

$$\psi(v^\sigma)(w) = \langle v^\sigma, w\rangle = \langle v, w^{\sigma^{-1}}\rangle = \psi(v)(w^{\sigma^{-1}}) = (\psi(v)\cdot\sigma)(w),$$

the map ψ is also an $\mathbb{F}_2G$-module homomorphism.

Clearly, we have $\ker\psi = \mathcal{C}^\perp$. Finally, $|\mathbb{F}_2^n/\mathcal{C}^\perp| = |\mathcal{C}^\star|$. So ψ is surjective and the assertion is proved. □

Now we can state the proposition.

Proposition 2.2. *Let $\mathcal{C}$ be a self-dual binary linear code and let us suppose $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$. Then, as a $\mathbb{F}_2\langle\sigma_{2p}\rangle$-module, the code $\mathcal{C}$ has the following structure:*

$$\mathcal{C} = \underbrace{\begin{matrix} V_0 & & V_0 \\ V_0 & \oplus\ldots\oplus & V_0 \end{matrix}}_{y_0 \text{ times}} \oplus \underbrace{V_0 \oplus\ldots\oplus V_0}_{z_0 \text{ times}} \oplus\ldots$$

$$\ldots \oplus \underbrace{\begin{matrix} V_t & & V_t \\ V_t & \oplus \ldots \oplus & V_t \end{matrix}}_{y_t \text{ times}} \oplus \underbrace{V_t \ \oplus \ldots \oplus \ V_t}_{z_t},$$

where

a) $2y_0 + z_0 = x + w$,

b1) $2y_i + z_i = x$ *for all* $i \in \{1, \ldots, t\}$, *if* $\mathrm{s}(p)$ *is even,*

b2) $z_i = z_{2i}$ *and* $y_i + y_{2i} + z_i = x$ *for all* $i \in \{1, \ldots, t\}$, *if* $s(p)$ *is odd.*

Proof. Recall that $\mathbb{F}_2^n/\mathcal{C} \cong \mathcal{C}^\star$. The conditions on the multiplicities are an easy consequence of this fact. Let us prove, for example, part b2): if

$$\mathcal{C} = \ldots \oplus \underbrace{\begin{matrix} V_i & & V_i \\ V_i & \oplus \ldots \oplus & V_i \end{matrix}}_{y_i \text{ times}} \oplus \underbrace{V_i \ \oplus \ldots \oplus \ V_i}_{z_i \text{ times}} \oplus \ldots$$

$$\ldots \oplus \underbrace{\begin{matrix} V_{2i} & & V_{2i} \\ V_{2i} & \oplus \ldots \oplus & V_{2i} \end{matrix}}_{y_{2i} \text{ times}} \oplus \underbrace{V_{2i} \ \oplus \ldots \oplus \ V_{2i}}_{z_{2i}} \oplus \ldots,$$

then

$$\mathbb{F}_2^n/\mathcal{C} = \ldots \oplus \underbrace{\begin{matrix} V_i & & V_i \\ V_i & \oplus \ldots \oplus & V_i \end{matrix}}_{x - z_i - y_i \text{ times}} \oplus \underbrace{V_i \ \oplus \ldots \oplus \ V_i}_{z_i \text{ times}} \oplus \ldots$$

$$\ldots \oplus \underbrace{\begin{matrix} V_{2i} & & V_{2i} \\ V_{2i} & \oplus \ldots \oplus & V_{2i} \end{matrix}}_{x - z_{2i} - y_{2i} \text{ times}} \oplus \underbrace{V_{2i} \ \oplus \ldots \oplus \ V_{2i}}_{z_{2i}} \oplus \ldots$$

and since $V_i \cong V_{2i}^\star$,

$$\mathcal{C}^\star = \ldots \oplus \underbrace{\begin{matrix} V_{2i} & & V_{2i} \\ V_{2i} & \oplus \ldots \oplus & V_{2i} \end{matrix}}_{y_i \text{ times}} \oplus \underbrace{V_{2i} \ \oplus \ldots \oplus \ V_{2i}}_{z_i \text{ times}} \oplus \ldots$$

$$\ldots \oplus \underbrace{\begin{matrix} V_i \\ V_i \end{matrix} \oplus \ldots \oplus \begin{matrix} V_i \\ V_i \end{matrix}}_{y_{2i} \text{ times}} \oplus \underbrace{V_i \oplus \ldots \oplus V_i}_{z_{2i}} \oplus \ldots .$$

Thus $z_i = z_{2i}$ and $x - z_i - y_i = y_{2i}$. □

Proposition 2.2 implies that

$$\phi(\mathcal{C})^{\perp} = \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) = \pi_{\sigma_2}\left(\bigoplus_{i=0}^{t} \underbrace{V_i \oplus \ldots \oplus V_i}_{y_i + z_i \text{ times}}\right). \tag{2.5}$$

where ϕ is the map (2.3).

Since $\ker \phi = \mathcal{C}(\sigma_2)$, we furthermore have

$$\phi(\mathcal{C}) \cong \mathcal{C}/\ker \phi \cong \bigoplus_{i=0}^{t} \underbrace{V_i \oplus \ldots \oplus V_i}_{y_i \text{ times}},$$

which leads to

$$\phi(\mathcal{C})^{\perp}/\phi(\mathcal{C}) \cong \bigoplus_{i=0}^{t} \underbrace{V_i \oplus \ldots \oplus V_i}_{z_i \text{ times}}.$$

Taking dimensions we get

$$\dim \phi(\mathcal{C})^{\perp}/\phi(\mathcal{C}) = z_0 + s(p)\left(\sum_{i=1}^{t} z_i\right). \tag{2.6}$$

Proposition 2.3. *Let $\mathcal{C}$ be a self-dual binary linear code of length n and suppose $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$. Then we have*

a) $x \equiv w \bmod 2$, *if* $n \equiv 0 \bmod 4$,

b) $x \not\equiv w \bmod 2$, *if* $n \equiv 2 \bmod 4$.

Furthermore, if $\mathrm{s}(p)$ *is even, then*

$$x \equiv z_1 \equiv \ldots \equiv z_t \bmod 2.$$

Proof. a) and b) follow immediately from (2.4). The last fact is a consequence of $2y_i + z_i = x$, if $\mathrm{s}(p)$ is even, which is stated in Proposition 2.2. □

Corollary 2.2. *Let $\mathcal{C}$ be a self-dual binary linear code of length n. Suppose $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$ and let ϕ be as in (2.3). Then*

a) *$\phi(\mathcal{C})^\perp/\phi(\mathcal{C})$ is of even dimension, if $n \equiv 0 \bmod 4$,*

b) *$\phi(\mathcal{C})^\perp/\phi(\mathcal{C})$ is of odd dimension, if $n \equiv 2 \bmod 4$.*

Proof. First note that $\mathrm{s}(p)\sum_{i=1}^{t} z_i \equiv 0 \bmod 2$ whatever $\mathrm{s}(p)$ is odd or even. In case $\mathrm{s}(p)$ odd this follows from $z_i = z_{2i}$ for $i \in \{1, \ldots, 2r = t\}$ (see Proposition 2.2). Furthermore, $z_0 \equiv x + w \bmod 2$, hence z_0 even, if $4 \mid n$, and z_0 odd, if $n \equiv 2 \bmod 4$, according to Proposition 2.3. Thus (2.6) yields

$$\dim \phi(\mathcal{C})^\perp/\phi(\mathcal{C}) \equiv z_0 \equiv 0 \bmod 2, \text{ if } n \equiv 0 \bmod 4$$

and

$$\dim \phi(\mathcal{C})^\perp/\phi(\mathcal{C}) \equiv z_0 \equiv 1 \bmod 2, \text{ if } n \equiv 2 \bmod 4.$$

□

Corollary 2.3. *Let $\mathcal{C}$ be a self-dual binary linear code of length $n \equiv 0 \bmod 4$. Suppose $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$ and $\mathrm{s}(p)$ even. If w is odd, then*

$$\dim \mathcal{C}(\sigma_2) = \dim \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \geq \frac{n}{4} + \frac{\mathrm{s}(p)t}{2} = \frac{n}{4} + \frac{p-1}{2},$$

where $\sigma_2 = \sigma_{2p}^p$.
In particular, $\phi(\mathcal{C}) < \phi(\mathcal{C})^\perp$.

Proof. By Proposition 2.3, the condition $4 \mid n$ forces that w and x have the same parity. Thus w odd implies that x is odd and by Proposition 2.2, we get $z_i \geq 1$ for $i \in \{1, \ldots t\}$. Since

$$\phi(\mathcal{C}) \leq \phi(\mathcal{C})^\perp = \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \leq \mathbb{F}_2^{\frac{n}{2}},$$

we have

$$\dim \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \geq \frac{n}{4} + \frac{1}{2}\dim \phi(\mathcal{C})^\perp/\phi(\mathcal{C}).$$

Therefore, according to (2.6),

$$\dim \mathcal{C}(\sigma_2) = \dim \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \geq \frac{n}{4} + \frac{\mathrm{s}(p)t}{2} = \frac{n}{4} + \frac{p-1}{2}.$$

□

We may ask whether $\phi(\mathcal{C}) < \phi(\mathcal{C})^\perp$ implies that w is odd. This is not true in general. For instance, there exist self-dual $[36, 18, 8]$ codes and automorphisms of order 6 (note that s(3) is even) for which $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ is not self-dual, but w is even.

Furthermore, notice that if the answer to Question 2.1 (Section 2.1) is positive, then for extremal self-dual binary linear codes of jump lengths w has to be even. Actually, it holds the following.

Corollary 2.4. *Let $\mathcal{C}$ be a self-dual binary linear code of length $n \equiv 0 \bmod 4$. Suppose $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$ and $\mathrm{s}(p)$ even.*
If σ_{2p} has an odd number of cycles of order 2, then $\mathcal{C}$ is not projective as a $\mathbb{F}_2\langle\sigma_{2p}\rangle$-module (or equivalently, $\pi_{\sigma_{2p}^p}(\mathcal{C}(\sigma_{2p}^p))$ is not self-dual).

Proof. If the number of 2-cycles of σ_{2p} is odd, then w is odd. Thus, by Corollary 2.3 and Theorem 2.6, the assertion follows. □

Since $\mathrm{Aut}(\mathcal{C}) \leq \mathcal{S}_n$, the largest possible prime which may occur as the order of an automorphism of a self-dual binary linear code of length n is $p = n - 1$. If $n \equiv 0 \bmod 8$, then $\mathrm{s}(p)$ is odd (see Remark 1.4). Obviously, in this case we cannot have an automorphism of order $2p$.

Let $\mathcal{C}$ be an extremal self-dual binary linear code of length $n \geq 48$. According to Theorem 2.2 an automorphism of type p-(c, f) with $p > 5$ satisfies $c \geq f$. Hence the second largest possible prime p satisfies $n = 2p + 2$.

Corollary 2.5. *Let $\mathcal{C}$ be a self-dual binary linear code of length $n = 2p + 2$, where p is an odd prime, and minimum distance greater than 4. Suppose that all involutions in $\mathrm{Aut}(\mathcal{C})$ are fixed point free. If $\mathrm{s}(p)$ is even, then $\mathrm{Aut}(\mathcal{C})$ does not contain an element of order $2p$.*
In case $\mathcal{C}$ is doubly-even, the condition $\mathrm{s}(p)$ even may be replaced by the condition $p \not\equiv -1 \bmod 8$.

Proof. Suppose that σ_{2p} is an automorphism of order $2p$. Thus σ_{2p} has one cycle of length $2p$ and one of length 2. Let $\sigma_2 := \sigma_{2p}^p$. By Corollary 2.3, we get

$$\dim \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \geq \frac{n}{4} + \frac{p-1}{2} = p.$$

Since $\pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \leq \mathbb{F}_2^{\frac{n}{2}} = \mathbb{F}_2^{p+1}$, we see that $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ has minimum distance 1 or 2, a contradiction.

In case that $\mathcal{C}$ is doubly-even we only have to show that $p \equiv 1 \bmod 8$ does not occur (see Remark 1.4). If $p \equiv 1 \bmod 8$ then $n = 2p+2 \equiv 4 \bmod 8$, contradicting Theorem 1.5. □

Finally we give a result about extremal self-dual binary linear codes of jump lengths.

Corollary 2.6. *Let $\mathcal{C}$ be a self-dual $[24m, 12m, 4m+4]$ code and suppose $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$. If $\mathrm{s}(p)$ is even and w is odd, then $p \leq \frac{n}{4} - 1$.*

Proof. By Corollary 2.3, $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ has parameters

$$\left[12m, \geq 6m + \frac{p-1}{2}, \geq 2m+2\right].$$

According to the Griesmer bound (1.2), we have

$$\begin{aligned} 12m &\geq \textstyle\sum_{i=0}^{6m+\frac{p-1}{2}-1} \left\lceil \frac{2m+2}{2^i} \right\rceil \\ &\geq (2m+2) + (m+1) + (6m + \tfrac{p-1}{2}) - 2. \end{aligned}$$

This implies $p \leq 6m - 1 = \frac{n}{4} - 1$. □

Clearly, the estimation in Corollary 2.6 is very crude for m large. For instance, if $m = 5$ the statement in Corollary 2.6 leads to $p \leq 29$, but computing all terms in the sum shows that $p \leq 23$.

2.4 Self-dual codes with automorphisms which form a dihedral group

In this section we want to generalize the main idea used by Nebe and Feulner to approach the case D_{10} for the extremal self-dual binary linear code of length 72 in [24]. We will use these results to exclude $\mathcal{S}_3$ for the same code in the next chapter. The assumptions which we make may be seen too restrictive, but they make the notations easier and they are sufficient for our purposes.

Let us now suppose that

- p is an odd prime with $\mathrm{s}(p) = p - 1$;
- $\mathcal{C}$ is a self-dual binary linear code of length n (n divisible by $2p$);
- $\sigma_p \in \mathrm{Aut}(\mathcal{C})$ acts fixed point free of order p (so that the number of cycles is $c = \frac{n}{p}$);
- $\sigma_2 \in \mathrm{Aut}(\mathcal{C})$ acts fixed point free of order 2;
- $\langle \sigma_p \rangle \rtimes \langle \sigma_2 \rangle \cong D_{2p}$ is a dihedral group of order $2p$.

The main idea is that we have the decomposition explained in Section 2.2, given by σ_p, and then the involution σ_2 which acts on it and gives a restrictive structure.

Finally, note that we can fix without lost of generality

$$\sigma_p := (1, \ldots, p)(p+1, \ldots, 2p) \ldots (n-p+1, \ldots, n)$$

and

$$\sigma_2 := (1, p+1)(2, 2p) \ldots (p, p+2) \ldots (n-p, n-p+2).$$

2.4.1 Preliminaries

We need to understand better the structure of the field $\mathbb{F}_{2^{p-1}}$ in its realization as an ideal $\mathcal{I}$ of $\mathbb{F}_2[x]/(x^p + 1)$, presented in Section 2.2.

Notation 2.1. *In the following we will indicate with* $a \bmod b$ *the nonnegative integer less than* b *that is the remainder of the division of* a *by* b*. Furthermore, we will indentify the cosets of* $\mathbb{F}_2[x]/(x^p+1)$ *with their representatives (the remainders of the division by* (x^p+1)*).*

Remember that the ideal $\mathcal{I}$ is generated by $(1+x)$. It is straightforward to observe that $(x+x^2+\ldots+x^{p-1}) \in \mathcal{I}$ is the identity of the field.

Since $\mathrm{s}(p) = p-1$ we have that

$$(1+x), (1+x)^2, (1+x)^4, \ldots, (1+x)^{2^{p-2}}$$

is an $\mathbb{F}_2$-basis of $\mathbb{F}_{2^{p-1}}$. Furthermore

$$a_0(1+x) + a_1(1+x)^2 + \ldots + a_{p-2}(1+x)^{2^{p-2}} =$$

$$= (a_0 + \ldots + a_{p-2}) + a_0 x + a_1 x^2 + \ldots + a_{p-2} x^{2^{p-2}}.$$

Let $\psi : i \mapsto i + \frac{p-1}{2} \bmod p-1$ and $\varphi_{2^{\frac{p-1}{2}}}$ the Frobenius automorphism of $\mathbb{F}_{2^{p-1}}$.

$$\varphi_{2^{\frac{p-1}{2}}}((a_0 + \ldots + a_{p-1}) + a_0 x + a_1 x^2 + \ldots + a_{p-2} x^{2^{p-2}}) =$$

$$= (a_0 + \ldots + a_{p-1}) + a_{\psi^{-1}(0)} x + a_{\psi^{-1}(1)} x^2 + \ldots + a_{\psi^{-1}(p-2)} x^{2^{p-2}}.$$

If we identify every polynomial with the ordered vector of $\mathbb{F}_2^p$ of its coefficients, the Frobenius automorphism corresponds to a permutation of $\mathcal{S}_p$.

Since $[2^{\frac{p-1}{2}}]_p = [-1]_p$ we have that the permutation

$$\prod_{i=1}^{\frac{p-1}{2}} (2^i \bmod p, 2^{\psi(i)} \bmod p) = (1, p-1)(2, p-2)(3, p-3)\ldots\left(\frac{p-1}{2}, \frac{p+1}{2}\right)$$

and so the Frobenius automorphism corresponds to the following permutation on the coefficients of polynomials

$$(2, p)(3, p-1)(4, p-2)\ldots\left(\frac{p+1}{2}, \frac{p+3}{2}\right)$$

that inverts the order on the last $p-1$ coordinates of the p-cycle.

Let us consider now the cartesian product of two copies of $\mathbb{F}_{2^{p-1}}$, so that the coefficients live in $\mathbb{F}_2^{2p}$. The permutation (in $\mathcal{S}_{2p}$)

$$(1, p+1)(2, 2p)(3, 2p-1)(4, 2p-2)\dots(p, p+2)$$

corresponds to $(\alpha, \beta) \mapsto (\varphi_{2^{\frac{p-1}{2}}}(\beta), \varphi_{2^{\frac{p-1}{2}}}(\alpha))$ over $\mathbb{F}_{2^{p-1}}^2$.

Notation 2.2. *Let us denote with* $\overline{\alpha} := \varphi_{2^{\frac{p-1}{2}}}(\alpha) = \alpha^{2^{\frac{p-1}{2}}}$.

It is now clear that, if we consider the cartesian product of c copies (note that c is even) of $\mathbb{F}_{2^{p-1}}$, the permutation

$$\sigma_2 = (1, p+1)(2, 2p)\dots(p, p+2)\dots(n-p, n-p+2)$$

acts as follows

$$(\alpha_1, \alpha_2, \dots, \alpha_{c-1}, \alpha_c) \mapsto (\overline{\alpha_2}, \overline{\alpha_1}, \dots, \overline{\alpha_c}, \overline{\alpha_{c-1}})$$

2.4.2 Main theorem

We can now state the main result which describes the rigid structure of a self-dual binary linear code whose automorphism group contains a dihedral group (with appropriate restrictions). The notations are those fixed in the introduction of this section.

Theorem 2.7. *Let* $\mathcal{C}$ *be a self-dual binary linear code of length* n *such that* $\langle \sigma_p \rangle \rtimes \langle \sigma_2 \rangle \leq \mathrm{Aut}(\mathcal{C})$. *If* $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ *is self-dual, then there exist*

- $\mathcal{A} \leq \mathbb{F}_2^{\frac{n}{2}}$, *which is a self-dual binary linear code,*
- $\mathcal{B} \subseteq \mathbb{F}_{2^{p-1}}^{\frac{c}{2}}$, *which is a* $\mathbb{F}_{2^{\frac{p-1}{2}}}$*-linear trace-Hermitian self-dual code,*

such that

$$\mathcal{C} = \pi_{\sigma_p}^{-1}(\mathcal{A}) \oplus \varphi_p^{-1}\left(\langle \pi^{-1}(\mathcal{B}) \rangle_{\mathbb{F}_{2^{p-1}}}\right)$$

where π_{σ_p} *is the natural projection associated to* σ_p, φ_p *is the map defined in Section 2.2 and*

$$\pi := \mathbb{F}_{2^{p-1}}^{c} \to \mathbb{F}_{2^{p-1}}^{\frac{c}{2}}$$

maps $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{c-1}, \varepsilon_c) \mapsto (\varepsilon_1, \dots, \varepsilon_{c-1})$.

Proof. Recall that, as we proved in Section 2.2,

$$\mathcal{C} = \mathcal{C}(\sigma_p) \oplus \mathcal{E}(\sigma_p).$$

Put $\mathcal{A} := \pi_{\sigma_p}(\mathcal{C}(\sigma_p)) \leq \mathbb{F}_2^{c+f}$. This is self-dual by Theorem 2.5.

Let us consider $\varphi_p(\mathcal{E}(\sigma_p)) \leq \mathbb{F}_{2^{p-1}}^c$. This is an Hermitian self-dual linear code, again by Theorem 2.5. As we have just shown the action of σ_2 on $\varphi_p(\mathcal{E}(\sigma_p))$ is the following

$$(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{c-1}, \varepsilon_c)^{\sigma_2} = (\overline{\varepsilon_2}, \overline{\varepsilon_1}, \ldots, \overline{\varepsilon_c}, \overline{\varepsilon_{c-1}})$$

Note that this action is only $\mathbb{F}_{2^{\frac{p-1}{2}}}$-linear. Then, the fixed code is

$$\varphi_p(\mathcal{E}(\sigma_p))(\sigma_2) := \{(\varepsilon_1, \overline{\varepsilon_1}, \ldots, \varepsilon_{\frac{c}{2}}, \overline{\varepsilon_{\frac{c}{2}}}) \in \varphi_p(\mathcal{E}(\sigma_p))\}.$$

Put $\mathcal{B} := \pi(\varphi_p(\mathcal{E}(\sigma_p))(\sigma_2))$.

For $\gamma, \epsilon \in \mathcal{B}$ the Hermitian inner product of their preimages in $\varphi_p(\mathcal{E}(\sigma_p))(\sigma_2)$ is

$$\sum_{i=1}^{\frac{c}{2}} (\epsilon_i \overline{\gamma_i} + \overline{\epsilon_i} \gamma_i)$$

which is 0 since $\varphi_p(\mathcal{E}(\sigma_p))$ is Hermitian self-dual. Therefore $\mathcal{B}$ is trace-Hermitian self-orthogonal. We have

$$\dim_{\mathbb{F}_2}(\mathcal{B}) = \dim_{\mathbb{F}_2}(\varphi_p(\mathcal{E}(\sigma_p))(\sigma_2)) = \frac{1}{2} \dim_{\mathbb{F}_2}(\varphi_p(\mathcal{E}(\sigma_p)))$$

since $\varphi_p(\mathcal{E}(\sigma_p))$ is a projective $\mathbb{F}_2\langle\sigma_2\rangle$-module (since $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ is self-dual), and so $\mathcal{B}$ is self-dual.

Since $\dim_{\mathbb{F}_2}(\mathcal{B}) = \dim_{\mathbb{F}_{2^{p-1}}}(\varphi_p(\mathcal{E}(\sigma_p)))$, the $\mathbb{F}_{2^{p-1}}$-linear code $\varphi_p(\mathcal{E}(\sigma_p)) \leq \mathbb{F}_{2^{p-1}}^c$ is obtained from $\mathcal{B}$ as stated. □

2.5 Interaction between fixed subcodes

In this section we will investigate the situation in which we have an automorphism group of a binary linear code which is a semidirect product (abelian or not) of two subgroups.

2.5.1 Non-abelian semidirect products of two subgroups

In this subsection we want to give an idea of what can be said when the automorphism group of a binary linear code (not necessarily self-dual) has a subgroup H that is a non-abelian semidirect product of two subgroups, say $H = A \rtimes B$.

Actually, in this case we have an action of H on the normal subgroup A and in particular on the fixed codes by the automorphisms belonging to A. We restrict our attention on a particular case, since it will be useful in the next chapter. However, this case gives some flavor of what can be done in general.

Notation 2.3. *If $\tau, \sigma \in \mathcal{S}_n$ then we denote by*

$$\tau^\sigma := \sigma^{-1}\tau\sigma,$$

the conjugate of τ by σ.

Let us start with a basic lemma.

Lemma 2.3. *Let $\mathcal{C}$ be a binary linear code of length n and take $\tau \in \mathrm{Aut}(\mathcal{C})$. If σ is a permutation of $\mathcal{S}_n$ then*

$$\tau^\sigma \in \mathrm{Aut}(\mathcal{C}^\sigma)$$

and

$$\mathcal{C}(\tau)^\sigma = \mathcal{C}(\tau^\sigma).$$

Proof. Let $c \in \mathcal{C}$. We have

$$c \in \mathcal{C}(\tau)^\sigma \Leftrightarrow c^{\sigma^{-1}} \in \mathcal{C}(\tau) \Leftrightarrow c^{\sigma^{-1}\tau} = c^{\sigma^{-1}} \Leftrightarrow c^{\tau^\sigma} = c \Leftrightarrow c \in \mathcal{C}(\tau^\sigma)$$

which proves the assertion. □

This easy observation suggests a construction for codes with semidirect automorphism groups.

Theorem 2.8. *Let $\mathcal{C}$ be a binary linear code. Suppose that $G = E_m \rtimes H \leq \mathrm{Aut}(\mathcal{C})$, where E_m is an elementary abelian p-group and H acts transitively on $E_m^\times$. Then*

$$\sum_{\varepsilon \in E_m^\times} \mathcal{C}(\varepsilon) = \sum_{\kappa \in H} \mathcal{C}(\varepsilon_0)^\kappa$$

for any $\varepsilon_0 \in E_m^\times$.

Proof. It follows directly from Lemma 2.3. □

Corollary 2.7. *Let p be a Mersenne prime, i.e. $p = 2^r - 1$ for a certain nonnegative integer r. Let E_{2^r} be an elementary abelian group of order 2^r and let $G = E_{2^r} \rtimes \langle \sigma_p \rangle$, where σ_p is an automorphism of order p (G non abelian).*
Suppose that $\mathcal{C}$ is a binary linear code such that $G \leq \mathrm{Aut}(\mathcal{C})$. Then for any involution $\varepsilon_0 \in E_{2^r}$ it holds that

$$\sum_{\varepsilon \in E_{2^r}^\times} \mathcal{C}(\varepsilon) = \sum_{i=0}^{p-1} \mathcal{C}(\varepsilon_0)^{\sigma_p^i}.$$

Proof. $|E_{2^r}^\times| = 2^r - 1$. The cyclic group $\langle \sigma_p \rangle$ acts on it. The orbits for this action can have order p or order 1. Since $p = |E_{2^r}^\times|$ there is only one orbit of order p: supposing the contrary we have G abelian, a contradiction. So the action is transitive and the assertion follows from Theorem 2.8. □

Obviously, similar results can be deduced for other groups. Notice that $\mathcal{A}_4$ satisfies the hypothesis of Corollary 2.7 with $p = 3$.

Let us conclude this short subsection, underlining a very useful tool to continue the study of a code with such an automorphism group.
Let $\mathcal{D} := \sum_{\varepsilon \in E_m^\times} \mathcal{C}(\varepsilon)$. The group G acts on $\mathcal{Q} := \mathcal{D}^\perp / \mathcal{D}$ with kernel containing E_m. The space $\mathcal{Q}$ is hence a $\mathbb{F}_2\langle \sigma_p \rangle$-module. On this space we still have a decomposition in the fixed part by σ_p and its complement and we can repeat arguments totally analogous to the ones in Section 2.2. This gives again a very restrictive structure.

2.5.2 Direct products of cyclic groups

Let us conclude this chapter with a few considerations on the interaction between fixed subcodes by different automorphisms. We will consider codes with automorphisms which commute. The results of this subsection can be generalized to any abelian finite group, but the notation would become too complex and it is not so relevant for our purposes to deal with the general case.

We consider in particular the group $C_p \times C_q$ with p, q not necessarily distinct primes. This case gives an idea of what can be said in a general context.

Let us suppose that $\mathcal{C}$ is a binary linear code (not necessarily self-dual, nor extremal) such that $C_p \times C_q \leq \mathrm{Aut}(\mathcal{C})$ with $C_p = \langle \sigma_p \rangle$, $C_q = \langle \sigma_q \rangle$, cyclic groups of prime (not necessarily distinct) order.

Let σ_p be of type p-(c, f). Then

$$\pi_{\sigma_p}(\mathcal{C}(\sigma_p)) \leq \mathbb{F}_2^{c+f}.$$

Every element of the centralizer of σ_p in $\mathcal{S}_n$, indicated with $\mathrm{C}_{\mathcal{S}_n}(\sigma_p)$, acts on the orbits of σ_p. So we can define naturally a projection

$$\eta_{\sigma_p} : \mathrm{C}_{\mathcal{S}_n}(\sigma_p) \to \mathcal{S}_{c+f}$$

that maps $\tau \in \mathrm{C}_{\mathcal{S}_n}(\sigma_p)$ on the permutation corresponding to the action of τ on the orbits of σ_p.

If σ_q is of type q-(c', f') we can define in a completely analogous way

$$\eta_{\sigma_q} : \mathrm{C}_{\mathcal{S}_n}(\sigma_q) \to \mathcal{S}_{c'+f'}.$$

We collect in the following some of observations.

Remark 2.2. *Let $\mathcal{C}$ be a binary linear code such that $C_p \times C_q \leq \mathrm{Aut}(\mathcal{C})$ with $C_p = \langle \sigma_p \rangle$, $C_q = \langle \sigma_q \rangle$, cyclic groups of prime (not necessarily distinct) order. Then*

a) $\eta_{\sigma_p}(\sigma_q) \in \mathrm{Aut}(\pi_{\sigma_p}(\mathcal{C}(\sigma_p)))$;

b) $\eta_{\sigma_q}(\sigma_p) \in \mathrm{Aut}(\pi_{\sigma_q}(\mathcal{C}(\sigma_q)))$;

c) $\eta_{\eta_{\sigma_p}(\sigma_q)}(\pi_{\sigma_p}(\mathcal{C}(\sigma_p))(\eta_{\sigma_p}(\sigma_q))) = \eta_{\eta_{\sigma_q}(\sigma_p)}(\pi_{\sigma_q}(\mathcal{C}(\sigma_q))(\eta_{\sigma_q}(\sigma_p)))$;

d) *if* p, q *are distinct and* $\sigma_p\sigma_q$ *is of type* pq-$(\alpha, \beta, \gamma; \delta)$ *then* $\eta_{\sigma_p}(\sigma_q)$ *is of type* q-$(\gamma + \beta, \alpha + \delta)$ *and* $\eta_{\sigma_q}(\sigma_p)$ *is of type* p-$(\gamma + \alpha, \beta + \delta)$.

Notice that a) and b) are strong conditions on the fixed codes.

CHAPTER 3

On the automorphism group of an extremal self-dual code of length 72

The existence of a self-dual extremal binary linear code of length 72 is a long-standing open problem of classical Coding Theory. In this chapter we will present our results on the automorphism group of such a putative code.

Remark 3.1. *Most of the computations are done with* MAGMA [17]. *The times of the main computations can be found in Appendix* A.

We begin recalling the state of art before our contribution [45]:

(∗) *Let* $\mathcal{C}$ *be a self-dual* $[72, 36, 16]$ *code. Then* $|\mathrm{Aut}(\mathcal{C})|$ *is either* 5 *or divides* 24. *If* 8 *divides* $|\mathrm{Aut}(\mathcal{C})|$ *then its Sylow* 2*-subgroup is either* D_8 *or* $C_2 \times C_2 \times C_2$.

Our results allow us to exclude most of the left subgroups in (∗), coming to the following.

Theorem 3.1. *Let* $\mathcal{C}$ *be a self-dual* $[72, 36, 16]$ *code. Then* $|\mathrm{Aut}(\mathcal{C})|$ *is at most* 5.

Remark 3.2. *The possible automorphism groups of a putative extremal self-dual binary linear code of length* 72 *are abelian and very small. So this code is almost a rigid object* (*i.e. without symmetries*) *and it might be very difficult to find it, if it exists.*

In Section 3.1 we give a brief overview of the results which led to (∗). Notice that we do not follow the chronological order, since some older results are made obsolete by more recent ones (proved independently). In Section 3.2 we present our first result [7], about elements of order 6. In Section 3.3 and 3.4 we present our joint work with Francesca Dalla Volta and Gabriele Nebe [9], about some remaining possible groups. In Section 3.5 we present our last result [8].

3.1 Previous results

For all this section let $\mathcal{C}$ be a self-dual $[72, 36, 16]$ code.

3.1.1 Cycle-structure of the automorphisms

In order to get information on the whole group $\mathrm{Aut}(\mathcal{C})$, we begin to investigate the cycle-structure of the possible automorphisms.

John H. Conway and Vera Pless, in a paper submitted in 1979 [18], were the first who faced this problem. In particular they focused on the possible automorphisms of odd prime order. Using mainly the results introduced in Section 2.1, they proved that

- *only* 9 *types of automorphism of odd prime order may occur in* $\mathrm{Aut}(\mathcal{C})$, *namely* 23-$(3, 3)$, 17-$(4, 4)$, 11-$(6, 6)$, 7-$(10, 2)$, 5-$(14, 2)$, 3-$(18, 18)$, 3-$(20, 12)$, 3-$(22, 6)$ *and* 3-$(24, 0)$.

Between 1981 and 1987, Vera Pless, John G. Thompson, W. Cary Huffman and Vassil Y. Yorgov [49, 48, 33] proved that

- *automorphisms of orders* 23, 17 *and* 11 *cannot occur in* $\mathrm{Aut}(\mathcal{C})$.

Between 2002 and 2004, Stefka Bouyuklieva [13, 12] proved that

- *the eventual elements of order* 2 *and* 3 *in* $\mathrm{Aut}(\mathcal{C})$ *are fixed point free.*

More recentely, in 2012, Thomas Feulner and Gabriele Nebe [24] showed that also

- *automorphisms of orders* 7 *cannot occur in* $\mathrm{Aut}(\mathcal{C})$.

The techniques used are different case by case, but the main tool is the decomposition of codes with an automorphism of odd prime order discussed in Section 2.2. Let us summarized these results.

Proposition 3.1. *Let* σ *be an automorphism of prime order of a self-dual* $[72, 36, 16]$ *code. Then* σ *can be only of the following types:*

- 2-$(36, 0)$,
- 3-$(24, 0)$,
- 5-$(14, 2)$.

An immediate consequence of this result is that $\mathrm{Aut}(\mathcal{C})$ does not contain elements of order 16, 27, 25 and 15. Furthermore, the possible composite orders are 4, 6, 8, 9, 12, 18, 36, 72 (fixed point free and with all cycles of the same length) and 10 (7 10-cycles and one 2-cycle). In [28], Annika Günter and G. Nebe pointed out that automorphisms of order 8 cannot occur, a result proved implicitly by Neil J.A. Sloane and J.G. Thompson in [59]. Finally, even more recently, G. Nebe and Nikolay Yankov [45, 61], excluded orders 10 and 9. Then we have the following.

Proposition 3.2. *Let* σ *be an automorphism of non-prime non-trivial order of a self-dual* $[72, 36, 16]$ *code. Then* σ *can be only*

- *of order* 4, *with* 18 *cycles of length* 4,
- *of order* 6, *with* 12 *cycles of length* 6,

- *of order* 12*, with* 6 *cycles of length* 12*.*

A very important information for the search of extremal codes, as we have already mentioned, is the classification of the possible fixed codes by the automorphisms.

We will strongly use such information, so let us collect all the results in a proposition.

Proposition 3.3. *Let* $\sigma_i \in \mathrm{Aut}(\mathcal{C})$ *be an element of order* i*. Then we have*

a) $\pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \sim \mathcal{K}$ *, where* $\mathcal{K}$ *is one of the* 41 *self-dual* $[36, 18, 8]$ *codes classified by Mechor and Gaborit* [42]*;*

b) $\pi_{\sigma_3}(\mathcal{C}(\sigma_3)) \sim \mathcal{G}_{24}$*, the extended binary Golay code;*

c) $\pi_{\sigma_5}(\mathcal{C}(\sigma_5)) \sim \hat{\mathcal{H}}_3 \oplus \hat{\mathcal{H}}_3$ *direct sum (of codes) of two copies of the extended Hamming code* $\hat{\mathcal{H}}_3$*;*

d) $\pi_{\sigma_6}(\mathcal{C}(\sigma_6)) \sim \mathcal{F}$*, a self-dual* $[12, 6, 4]$ *code with generator matrix*

$$M = \begin{bmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&1&1&1&1&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix};$$

e) $\pi_{\sigma_{12}}(\mathcal{C}(\sigma_{12})) \sim \mathcal{L}$*, a self-dual* $[6, 3, 2]$ *code with generator matrix*

$$M = \begin{bmatrix} 1&1&0&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&0&1&1 \end{bmatrix};$$

f) $\pi_{\sigma_4}(\mathcal{C}(\sigma_4)) \sim \mathcal{H}$*, a self-dual* $[18, 9, 4]$ *code (there are only two such codes, up to equivalence* [50]*).*

Proof. a) is proved in [45]. b) and c) are proved in [18].

By b), $\pi_{\sigma_6^2}\mathcal{C}(\sigma_6^2) = \mathcal{G}_{24}$. Obviously $\pi_{\sigma_6^2}(\sigma_6)$ is a fixed point free automorphism of order 2 of the extended binary Golay code. The automorphism group of $\mathcal{G}_{24}$ has just one such automorphism up to conjugacy. Let ρ be a representative of this conjugacy class; we have $\pi_{\sigma_6}(\mathcal{C}(\sigma_6)) \sim \pi_\rho(\mathcal{G}_{24}(\rho)) \sim \mathcal{F}$. So d) is proved. The same arguments can be used to prove e).

It is a little more complicate to prove f), since here we need some representation theory. By [45] we have that $\mathcal{C}$ is a free $\mathbb{F}_2\langle\sigma_4\rangle$-module (of rank 9). This implies that $\mathcal{C}(\sigma_4)$, which is the socle of such module, has dimension 9. The other parameters are trivially determined. □

3.1.2 Structure of the whole group

Once we have all the information on the structure of the automorphisms, we can investigate the structure of the whole group.

By Proposition 3.1 we have immediately that

$$|\mathrm{Aut}(\mathcal{C})| = 2^a 3^b 5^c$$

with a, b, c nonnegative integers.

Bouyuklieva was the first, in 2004, to have studied the order of $\mathrm{Aut}(\mathcal{C})$. She proved [12] that 49 does not divide $|\mathrm{Aut}(\mathcal{C})|$. Actually, this result is an easy consequence of [24] (which is proved later independently). In the same paper Bouyuklieva said, without giving an explicit proof, that the same holds for 25. For completeness and to give an idea of the techniques involved, let us prove it.

- 25 *does not divide* $|\mathrm{Aut}(\mathcal{C})|$.

Proof. Suppose that 25 divides $|\mathrm{Aut}(\mathcal{C})|$. According to Sylow's Theorem, there exists a subgroup $H \leq \mathrm{Aut}(\mathcal{C})$ of order 25. By Proposition 3.2, H is elementary abelian. Let $H = \langle\sigma, \tau\rangle$, where σ and τ are elements of type 5-$(14, 2)$ which commutes. Let

$$\Omega_1, \ldots, \Omega_{14}$$

be the non-trivial orbits of σ. Obviously, τ acts on these orbits and it fixes at least 4 of them, say $\Omega_1, \Omega_2, \Omega_3$ and Ω_4. Since τ has only 2 fixed points, it does not fix any point in such orbits (otherwise it should fix every point). So $\sigma_{|\Omega_1}$ and $\tau_{|\Omega_1}$ are permutation of order 5 on Ω_1. Without loss of generality we

can suppose $\sigma_{|\Omega_1} = (1,2,3,4,5)$. Now, $1^\tau = j$ with $1 < j \leq 5$. Notice that $1^{\sigma^{j-1}} = j$ and so $\tau\sigma^{1-j}$ is an automorphism of order 5 with at least 3 fixed points, a contradiction by Proposition 3.2. □

This means that

$$|\mathrm{Aut}(\mathcal{C})| = 2^a 3^b 5^c$$

with a, b nonnegative integers and $c = 0, 1$.
If $c = 1$ then

- if $\sigma \in \mathrm{Aut}(\mathcal{C})$ has order 5, $|N_{\mathrm{Aut}(\mathcal{C})}(\sigma)| = 2^d 5$, with $d = 0, 1$ [63].
- $\#\{\text{aut. of order 5 in } \mathrm{Aut}(\mathcal{C})\} = 4 \cdot \frac{|\mathrm{Aut}(\mathcal{C})|}{2^\delta 5}$.

So, by Burnside Lemma,

$$\frac{1}{|\mathrm{Aut}(\mathcal{C})|}\left(72 + \gamma \cdot 2 \cdot \frac{4 \cdot |\mathrm{Aut}(\mathcal{C})|}{2^\gamma 5}\right) = \frac{72}{2^\alpha 3^\beta 5^\gamma} + \gamma \cdot \frac{8}{2^\delta 5} \in \mathbb{N}$$

$$\Downarrow$$

$$|\mathrm{Aut}(\mathcal{C})| \in \{1,2,3,4,5,6,8,9,10,12,18,24,30,36,60,72,180,360\}.$$

By Proposition 3.2,

- $|\mathrm{Aut}(\mathcal{C})|$ *is not* 30 *or* 180,

since all groups of such order have elements of order 15.

Furthermore, among all the 281 possible groups with the remaining orders (for a library of Small Groups see for example [5]) only 76 satisfy the condition of Proposition 3.2. In particular, $\mathcal{A}_5$ and $\mathcal{A}_6$ are the only possible groups of order 60 and 360 respectively. In 2006, Bouyklieva together with Eamonn O'Brien and Wolfgang Willems introduced the language and the methods of representation theory in the study of the problem and they proved [16] that $\mathcal{A}_5$ (and then $\mathcal{A}_6$) cannot occur. So they proved

- $|\mathrm{Aut}(\mathcal{C})|$ *is not* 60 *or* 360 (*so that the group is solvable*).

Lately, in 2011, the last two authors improved their results proving [47] that

- $|\mathrm{Aut}(\mathcal{C})|$ *is not* 72 *and if* $|\mathrm{Aut}(\mathcal{C})| = 36$, *then* $\mathrm{Aut}(\mathcal{C}) \cong \mathcal{A}_4 \times C_3$.

Feulner and Nebe [24], in 2012, proved that $\mathrm{Aut}(\mathcal{C}) \ncong C_3 \times C_3$ and $\mathrm{Aut}(\mathcal{C}) \ncong D_{10}$ (the case of the dihedral group of order 10 involves the methods of Section 2.4), proving then that

- $|\mathrm{Aut}(\mathcal{C})|$ *is not* 9, 10, 18 *or* 36.

Finally Nebe proved [45] that $\mathrm{Aut}(\mathcal{C})$ is not isomorphic to $C_2 \times C_4$ or Q_8.

Let us summarize all these results in a theorem.

Theorem 3.2 (Pless, Conway, Thompson, Huffman, Yorgov, Bouyuklieva, O'Brien, Willems, Yankov, Feulner, Nebe)**.**

Let $\mathcal{C}$ *be self-dual* $[72, 36, 16]$ *code. Then* $\mathrm{Aut}(\mathcal{C})$ *is trivial or is isomorphic to one of the following:*

- *Order 2:* C_2*;*
- *Order 3:* C_3*;*
- *Order 4:* C_4 *or* $C_2 \times C_2$*;*
- *Order 5:* C_5*;*
- *Order 6:* $\mathcal{S}_3$ *or* C_6*;*
- *Order 8:* $C_2 \times C_2 \times C_2$ *or* D_8*;*
- *Order 12:* $\mathcal{A}_4$, C_{12}, $C_6 \times C_2$, D_{12} *or* $C_3 \rtimes C_4$*;*
- *Order 24:* $\mathcal{S}_4$, D_{24}, $(C_6 \times C_2) : C_2$, $D_8 \times C_3$, $\mathcal{A}_4 \times C_2$, $D_{12} \times C_2$ *or* $C_6 \times C_2 \times C_2$.

3.2 Case Aut($\mathcal{C}$) containing elements of order 6

In this section we will present our original result about automorphism of order 6 in extremal self-dual binary linear codes of length 72 [7].

Following and deepening the methods of O'Brien and Willems and doing extensive calculations with MAGMA we proved that the automorphism group of a putative extremal self-dual binary linear code of length 72 does not contain element of order 6, halving the number of the possible automorphism groups.

Let us explain our method. For all this section we set

- $K := \mathbb{F}_2$;
- $\mathcal{V} := K^{72}$;
- $\mathcal{C}$ a self-dual $[72, 36, 16]$ code

and suppose

- $\sigma_6 \in \mathrm{Aut}(\mathcal{C})$ of order 6.

By Proposition 3.2, σ_6 has no fixed point. Thus we can suppose, without lost of generality, that

$$\sigma_6 = (1, 2, 3, 4, 5, 6) \dots (67, 68, 69, 70, 71, 72). \tag{3.1}$$

The subcode $\mathcal{C}(\sigma_6^2)$ plays an important role in our method; actually σ_6^2 has order 3 and so, by Theorem 2.4,

$$\mathcal{C} = \mathcal{C}(\sigma_6^2) \oplus \mathcal{E}(\sigma_6^2),$$

where $\mathcal{E}(\sigma_6^2)$ is the subcode of even-weight codewords on the cycles of σ_6^2. Furthermore, by Proposition 3.3 we have $\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2)) \sim \mathcal{G}_{24}$, so that $\mathcal{C}(\sigma_6^2)$ is a $[72, 12, 24]$ code and

$$\dim \mathcal{E}(\sigma_6^2) = \dim \mathcal{C} - \dim \mathcal{C}(\sigma_6^2) = 36 \ - \ 12 = 24.$$

The decomposition above follows, as observed in Section 2.2, by representation theory arguments: let us take $G = \langle \sigma_6 \rangle$ and observe that

$$1 = \underbrace{(1 + \sigma_6^2 + \sigma_6^4)}_{f_0} + \underbrace{(\sigma_6^2 + \sigma_6^4)}_{f_1}$$

is a decomposition of 1 into (central) orthogonal idempotents of $K\langle \sigma_6 \rangle$.

Remark 3.3. *We point out that*

- $\mathcal{C}(\sigma_6^2) = \mathcal{C}f_0$ *and* $\mathcal{E}(\sigma_6^2) = \mathcal{C}f_1$*;*
- $\mathcal{V}(\sigma_6^2) = \mathcal{V}f_0$*, the subspace of all vectors fixed by* σ_6^2*;*
- $\mathcal{V}(\sigma_6^2)^\perp = \mathcal{V}f_1$ *is the set of vectors of even weight on the orbits of* σ_6^2*.*

All spaces $\mathcal{C}(\sigma_6^2)$, $\mathcal{E}(\sigma_6^2)$, $\mathcal{V}(\sigma_6^2)$, $\mathcal{V}(\sigma_6^2)^\perp$ *are* $K\langle \sigma_6 \rangle$*-modules.*

By Table 1.1 we have $\mathrm{s}(3) = 2$, so that the group algebra $K\langle \sigma_6 \rangle$ has exactly two irreducible submodules: the trivial one, say K and a 2-dimensional one, say V. Since $K\langle \sigma_6 \rangle$ is the tensor product of $K\langle \sigma_6^2 \rangle$ and $K\langle \sigma_6^3 \rangle$,

$$K\langle \sigma_6 \rangle = \mathrm{P}(K) \oplus \mathrm{P}(V)$$

where $\mathrm{P}(K) = \begin{matrix} K \\ K \end{matrix}$ is a non-split extension of K by K and $\mathrm{P}(V) = \begin{matrix} V \\ V \end{matrix}$ is a non-split extension of V by V. $\mathrm{P}(K)$ and $\mathrm{P}(V)$ are the two projective indecomposable modules for $K\langle \sigma_6 \rangle$.

Since σ_6 has no fixed points, $\mathcal{V} \cong K\langle \sigma_6 \rangle^{12}$. Then

$$\mathcal{V} \cong \underbrace{\begin{matrix} K \\ K \end{matrix} \oplus \ldots \oplus \begin{matrix} K \\ K \end{matrix}}_{12 \text{ times}} \oplus \underbrace{\begin{matrix} V \\ V \end{matrix} \oplus \ldots \oplus \begin{matrix} V \\ V \end{matrix}}_{12 \text{ times}}$$

Obviously

$$\mathcal{V}(\sigma_6^2) \cong \underbrace{\begin{matrix} K \\ K \end{matrix} \oplus \ldots \oplus \begin{matrix} K \\ K \end{matrix}}_{12 \text{ times}}$$

and

$$\mathcal{V}(\sigma_6^2)^\perp \cong \underbrace{\begin{matrix} V & & V \\ V & \oplus \ldots \oplus & V \end{matrix}}_{12 \text{ times}}.$$

In particular, V is the only composition factor of $\mathcal{V}(\sigma_6^2)^\perp$.

Note that $\mathrm{soc}(\mathcal{V}) = \mathcal{V}(\sigma_6^3)$ and $\mathrm{soc}(\mathcal{V}(\sigma_6^2)) = \mathcal{V}(\sigma_6)$.

Remark 3.4. *By Proposition* 3.3, $\pi_{\sigma_6^3}(\mathcal{C}(\sigma_6^3))$ *is self-dual. So, Theorem* 2.6 *tells us that* $\mathcal{C}$ *is projective.*

Furthermore, by Proposition 3.3 again,

$$\mathcal{C}(\sigma_6^2) \cap \mathcal{C}(\sigma_6^3) = \mathcal{C}(\sigma_6)$$

with $\dim \mathcal{C}(\sigma_6^2) = 12$, $\dim \mathcal{C}(\sigma_6^3) = 18$ *and* $\dim \mathcal{C}(\sigma_6) = 6$, *so that* $\mathcal{C}$ *has the following structure*

$$\mathcal{C} \cong \underbrace{\begin{matrix} K & & K \\ K & \oplus \ldots \oplus & K \end{matrix}}_{6 \text{ times}} \oplus \begin{matrix} V_1 \\ V_1 \end{matrix} \oplus \begin{matrix} V_2 \\ V_2 \end{matrix} \oplus \begin{matrix} V_3 \\ V_3 \end{matrix} \oplus \begin{matrix} V_4 \\ V_4 \end{matrix} \oplus \begin{matrix} V_5 \\ V_5 \end{matrix} \oplus \begin{matrix} V_6 \\ V_6 \end{matrix}.$$

where $V_i \cong V$ *for every* $i \in \{1, \ldots, 6\}$. *In particular,* $\mathcal{C}$ *is a free* $K\langle\sigma_6\rangle$*-module of rank* 6.

Finally, note that $\dim(\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3)) = 24$.

We know that $\mathrm{soc}(\mathcal{E}(\sigma_6^2)) = (\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3)) \cap \mathcal{V}(\sigma_6^2)^\perp$. Then, in order to get $\mathrm{soc}(\mathcal{E}(\sigma_6^2))$, we determine the possible spaces $\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3)$.

In particular, we will prove in Subsection 3.2.1 the following theorem.

Theorem 3.3. $\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3)$ *belongs, up to equivalence, to a set* $\mathbb{L}$ *of cardinality* 38. *Every element of* $\mathbb{L}$ *is a binary self-orthogonal doubly-even* $[72, 24, 16]$ *code.*

We need to modify a little the set $\mathbb{L}$.

Remark 3.5. *Theorem 3.3 implies that, if* $\mathcal{C}$ *does exist, there are* $\mathcal{L} \in \mathbb{L}$ *and* $\rho \in \mathcal{S}_{72}$ *such that*

$$(\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3))^\rho = \mathcal{L}.$$

We remark that, a priori, σ_6^ρ can be different from σ_6.

However, σ_6^ρ is an automorphism of $\mathcal{L}$ of order 6 and it has the same cycle structure as σ_6. Furthermore $\mathcal{L} = \mathcal{L}((\sigma_6^2)^\rho) + \mathcal{L}((\sigma_6^3)^\rho)$. There are few elements with these features in $\mathrm{Aut}(\mathcal{L})$, $\mathcal{L} \in \mathbb{L}$.
For every $\mathcal{L} \in \mathbb{L}$, let us call $\mathbb{B}_\mathcal{L} = \{\beta_1, \ldots, \beta_{n_L}\}$ the set of representatives of conjugacy classes of such elements and choose $\rho_1, \ldots, \rho_{n_\mathcal{L}}$ such that $\beta_i^{\rho_i} = \sigma_6$. We define a new set, say $\mathbb{L}'$, substituting each $\mathcal{L}$ with the set $\{\mathcal{L}^{\rho_1}, \ldots, \mathcal{L}^{\rho_{n_\mathcal{L}}}\}$. So there exist $\mathcal{L}' \in \mathbb{L}'$ and $\psi \in \mathcal{S}_{72}$ with

$$(\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3))^\psi = \mathcal{L}' \qquad \text{and} \qquad \sigma_6^\psi = \sigma_6.$$

We conclude the construction following the track carried out in Remark 2.1: we know the possible socles of $\mathcal{E}(\sigma_6^2)$. So we look at all the possible projective covers, doing an exhaustive search with Magma. We will explain all the details in Subsection 3.2.2.

With exhaustive search we did not find any extremal self-dual binary linear code. Thus we prove the following.

Theorem 3.4. *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain elements of order 6.*

Corollary 3.1. *The automorphism group of a self-dual $[72, 36, 16]$ code is not isomorphic to C_6, C_{12}, $C_6 \times C_2$, D_{12}, $C_3 \rtimes C_4$, D_{24}, $(C_6 \times C_2) : C_2$, $D_8 \times C_3$, $\mathcal{A}_4 \times C_2$, $D_{12} \times C_2$ or $C_6 \times C_2 \times C_2$.*

3.2.1 Proof of Theorem 3.3

By (3.1), Proposition 3.3 and Section 2.5 we have

- $\sigma_6^2 = (1,3,5)(2,4,6)\ldots(67,69,71)(68,70,72)$;
- $\sigma_6^3 = (1,4)(2,5)(3,6)\ldots(67,70)(68,71)(69,72)$;
- $\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2)) \sim \mathcal{G}_{24}$;

- $\pi_{\sigma_6^3}(\mathcal{C}(\sigma_6^3)) \sim \mathcal{K}$, where $\mathcal{K}$ is one of the 41 self-dual $[36, 18, 8]$ codes classified by Mechor and Gaborit;
- $\pi_{\sigma_6}(\mathcal{C}(\sigma_6)) \sim \mathcal{F}$, with $\mathcal{F}$ self-dual $[12, 6, 4]$ code with generator matrix M;
- $\eta_{\sigma_6^3}(\sigma_6) \in \mathrm{Aut}(\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2)))$ of type 2-$(12, 0)$;
- $\eta_{\sigma_6^2}(\sigma_6) \in \mathrm{Aut}(\pi_{\sigma_6^3}(\mathcal{C}(\sigma_6^3)))$ of type 3-$(12, 0)$;

Let us denote

$$\overline{\sigma_2} := \eta_{\sigma_6^3}(\sigma_6) = (1, 2)(3, 4)\dots(23, 24),$$

$$\overline{\sigma_3} := \eta_{\sigma_6^2}(\sigma_6) = (1, 2, 3)(4, 5, 6)\dots(34, 35, 36).$$

We have only one conjugacy class of such an element in the automorphism group of the extended binary Golay code, so the action of σ_6 on $\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2))$ is completely determined. Furthermore, the natural projection of the fixed code by this element is equivalent to $\mathcal{F}$.
Only 13 out of the 41 codes classified by Mechor and Gaborit have automorphisms of type 3-$(12, 0)$ (for a total of 19 conjugacy classes). We collect them in a set called $\mathbb{D}$. Moreover, we have that the natural projections of the fixed codes by such elements are equivalent to $\mathcal{F}$.

Now we describe the step of the proof, which is mainly algorithmic.
Step 1. Choose a particular extended binary Golay code, say $\mathcal{G}$, and find a representant, say μ, of the only conjugacy class of element of type 2-$(12, 0)$. Call $\mathcal{M} = \mathcal{G}(\mu)$. Denote by τ an element of $\mathcal{S}_{24}$ such that

$$\pi_{\overline{\sigma_2}}(\mathcal{M}^\tau) = \mathcal{F}.$$

The element μ^τ is of type 2-$(12, 0)$ and it fixes $\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F})$. The only element with these features in $\mathrm{Aut}(\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F}))$ is $\overline{\sigma_2}$, by calculations. So $\mu^\tau = \overline{\sigma_2}$.
Set $\mathcal{G}' = \mathcal{G}^\tau$. Denote $A = \mathrm{Aut}(\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F}))$ and $\mathbb{G} = \mathcal{G}'^A$, i.e. $\mathbb{G}$ is the orbit of $\mathcal{G}'$ under the action of A. We remark that $|\mathbb{G}| = \frac{|A|}{|A \cap \mathrm{Aut}(\mathcal{G}')|} = 12,288$.

Lemma 3.1. *$\mathbb{G}$ is the set of all extended binary Golay codes which have $\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F})$ as fixed code of $\overline{\sigma_2}$.*

Proof. Take an extended binary Golay code $\mathcal{J}$ with $\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F})$ as subcode fixed by $\overline{\sigma_2}$. Then, there exists $\eta \in \mathcal{S}_{24}$ such that $\mathcal{J}^\eta = \mathcal{G}$. Since there is only one conjugacy class of elements of type 2-$(12,0)$ there exists $\eta' \in \mathrm{Aut}(\mathcal{M})$ such that $\overline{\sigma_2}^{\eta\eta'} = \mu$, so that $(\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F}))^{\eta\eta'} = \mathcal{G}(\mu) = \mathcal{M}$. Then $(\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F}))^{\eta\eta'\tau} = \mathcal{M}^\tau = \pi_{\overline{\sigma_2}}^{-1}(\mathcal{F})$, so that $\eta\eta'\tau \in A$. But $\mathcal{J}^{\eta\eta'\tau} = \mathcal{G}'$ and then $\mathcal{J} \in \mathcal{G}'^A = \mathbb{G}$. □

Step 2. Take the codes in $\mathbb{D}$, say $\mathcal{D}_1, \ldots, \mathcal{D}_{13}$.
Denote

$$\begin{aligned} \{\epsilon_{1,1}, \ldots, \epsilon_{1,n_1}\} &\subset \mathrm{Aut}(\mathcal{D}_1), \\ &\vdots \\ \{\epsilon_{13,1}, \ldots, \epsilon_{13,n_{13}}\} &\subset \mathrm{Aut}(\mathcal{D}_{13}) \end{aligned}$$

the sets of representatives of conjugacy classes of automorphisms of order 3 and degree 36 of $\mathrm{Aut}(\mathcal{D}_1), \ldots, \mathrm{Aut}(\mathcal{D}_{13})$ respectively.
Find $\mu_{i,j} \in \mathcal{S}_{36}$ such that $\epsilon_{i,j}^{\mu_{i,j}} = \overline{\sigma_3}$ and $(\mathcal{D}_i(\epsilon_{i,j}))^{\mu_{i,j}} = \pi_{\overline{\sigma_3}}^{-1}(\mathcal{F})$. Set $\mathcal{D}_{i,j} = \mathcal{D}_i^{\mu_{i,j}}$.
Put $\mathbb{H} = \{\mathcal{D}_{i,j}\}$.
$\mathbb{H}$ is a proper subset of all the codes equivalent to $\mathcal{D}_1, \ldots, \mathcal{D}_{13}$ which contain $\pi_{\overline{\sigma_3}}^{-1}(\mathcal{F})$. The following lemma shows that $\mathbb{H}$ is large enough to allow us to determine all the possible $\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3)$.

Lemma 3.2. *There exist $\mathcal{G} \in \mathbb{G}$ and $\mathcal{H} \in \mathbb{H}$ such that $\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3)$ is equivalent to*

$$\pi_{\sigma_6^3}{}^{-1}(\mathcal{G}) + \pi_{\sigma_6^2}{}^{-1}(\mathcal{H}).$$

Proof. Up to equivalence, we can suppose

$$\mathcal{C}(\sigma_6^2) \cap \mathcal{C}(\sigma_6^3) = \pi_{\sigma_6}^{-1}(\mathcal{F}).$$

There exist $i \in \{1, \ldots, 13\}$ and $\mu \in \mathcal{S}_{36}$ such that $\pi_{\overline{\sigma_3}}(\mathcal{C}(\sigma_6^3))^\mu = \mathcal{D}_i$. There exist $j \in \{i, \ldots, n_i\}$ and $\mu' \in \mathrm{Aut}(\mathcal{D}_i)$ such that

$$\overline{\sigma_3}^{\mu\mu'} = \epsilon_{i,j}.$$

Set $\overline{\tau} = \mu\mu'\mu_{i,j}$. We have

a) $\pi_{\sigma_6^3}(\mathcal{C}(\sigma_6^3))^{\overline{\tau}} = \mathcal{D}_{i,j}$;

b) $\overline{\tau} \in \mathrm{C}_{\mathcal{S}_{36}}(\overline{\sigma_3})$;

c) $\overline{\tau} \in \mathrm{Aut}(\pi_{\overline{\sigma_3}}^{-1}(\mathcal{F}))$.

It is now possible to construct an element $\tau \in \mathcal{S}_{72}$ with the following properties:

a) $\pi_{\sigma_6^3}(c^\tau) = (\pi_{\sigma_6^3}(c))^{\overline{\tau}}$ for all $c \in \mathcal{C}(\sigma_6^3)$;

b) $\tau \in \mathrm{C}_{\mathcal{S}_{72}}(\sigma_6)$;

c) $\tau \in \mathrm{Aut}(\pi_{\sigma_6}^{-1}(\mathcal{F}))$.

This element is of course in $\eta_{\sigma_6^3}^{-1}(\overline{\tau})$, but here we want to give an explicit construction, which we will do in Remark 3.6.
a) implies that $\pi_{\sigma_6^3}(\mathcal{C}(\sigma_6^3)^\tau) \in \mathbb{H}$.
b) implies that $\mathcal{C}(\sigma_6^2)^\tau = \mathcal{C}^\tau(\sigma_6^2)$. Actually, if $c \in \mathcal{C}(\sigma_6^2)$, then $(c^\tau)^{\sigma_6^2} = (c^\tau)^{\tau^{-1}\sigma_6^2\tau} = c^\tau$; it follows that every word of $\mathcal{C}(\sigma_6^2)^\tau$ is fixed by σ_6^2. So $\mathcal{C}(\sigma_6^2)^\tau$, whose dimension is obviously 12, is contained in $\mathcal{C}^\tau(\sigma_6^2)$. As $\mathcal{C}^\tau$ is a self-dual $[72, 36, 16]$ code with σ_6 as automorphism, $\mathcal{C}^\tau(\sigma_6^2)$ has dimension 12 too, and thus $\mathcal{C}(\sigma_6^2)^\tau = \mathcal{C}^\tau(\sigma_6^2)$. This implies that $\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2)^\tau)$ is an extended binary Golay code.
c) implies that $\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F})$ is a subcode of $\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2)^\tau)$. Indeed,

$$\begin{aligned}\pi_{\overline{\sigma_2}}^{-1}(\mathcal{F}) &= \pi_{\sigma_6^2}(\pi_{\sigma_6}^{-1}(\mathcal{F})) = \\ &= \pi_{\sigma_6^2}((\pi_{\sigma_6}^{-1}(\mathcal{F}))^t)).\end{aligned}$$

Thus $\pi_{\sigma_6^2}(\mathcal{C}(\sigma_6^2)^\tau) \in \mathbb{G}$. □

Remark 3.6. *For reader's convenience we give an explicit construction of τ through wreath product.*
Let $\Delta = \{1, 2\}$ and $\Gamma = \{1, 2, 3\}$. We have $\mathcal{S}_\Delta \simeq \mathcal{S}_2$ and $\mathcal{S}_\Gamma \simeq \mathcal{S}_3$. We describe the action of the wreath product $\mathcal{S}_\Delta \wr \mathcal{S}_\Gamma$ on the coordinates of $\mathbb{F}_2^6$. Firstly, we can see

$$\Delta \times \Gamma = \Delta_1 \cup \Delta_2 \cup \Delta_3$$

with $\Delta_1 = \{1,4\}$, $\Delta_2 = \{2,5\}$ *and* $\Delta_3 = \{3,6\}$. *This can be send in the ordered set* $\Omega = \{1,2,3,4,5,6\}$ *in a natural way, that is sending the first element of* Δ_1 *in the first element of* Ω, *the second element of* Δ_1 *in the fourth element of* Ω, *the first element of* Δ_2 *in the second element of* Ω *and so on, i.e. by sending* i *in* i, *in the ordered set* Ω. *We denote this map*

$$\varphi : \Delta_1 \cup \Delta_2 \cup \Delta_3 \to \Omega.$$

An element μ *of* $\mathcal{S}_\Delta \wr \mathcal{S}_\Gamma$ *has the shape*

$$\mu = (\delta_1, \delta_2, \delta_3, \gamma) \in \mathcal{S}_\Delta \times \mathcal{S}_\Delta \times \mathcal{S}_\Delta \times \mathcal{S}_\Gamma.$$

The action of μ *on* $\Delta_1 \cup \Delta_2 \cup \Delta_3$ *is the following:*

$$(\Delta_1 \cup \Delta_2 \cup \Delta_3)^\mu =$$
$$= (\Delta_{\gamma^{-1}1})^{\delta_{\gamma^{-1}1}} \cup (\Delta_{\gamma^{-1}2})^{\delta_{\gamma^{-1}2}} \cup (\Delta_{\gamma^{-1}3})^{\delta_{\gamma^{-1}3}}.$$

With this notation it is possible to check that, for example,

$$(1,2,3,4,5,6) = \varphi^{-1}(Id, Id, (1,2), (1,2,3))\varphi.$$

In a similar way, we have that

$$\mathcal{S}_2 \wr \mathcal{S}_{36} = \mathcal{S}_\Delta \wr \mathcal{S}_{\Gamma_{36}},$$

where $\Gamma_{36} = \{1, \ldots, 36\}$, *acts on the coordinates of* $\mathbb{F}_2^{72}$, *thanks to a suitable*

$$\varphi_{36} : \underbrace{\{1,4\}}_{\Delta_1} \cup \underbrace{\{2,5\}}_{\Delta_2} \cup \underbrace{\{3,6\}}_{\Delta_3} \cup \ldots \cup \underbrace{\{69,72\}}_{\Delta_{36}} \to \Omega_{72},$$

where $\Omega_{72} = \{1, \ldots, 72\}$. *With this notation we have that*

$$\sigma_6 = \varphi_{36}^{-1}(Id, Id, (1,2), \ldots, Id, Id, (1,2), \overline{\sigma_3})\varphi_{36}.$$

Now, the $\tau \in \mathcal{S}_{72}$ *that we were looking for is*

$$\tau = \varphi_{36}^{-1}(Id, Id, (1,2), \ldots, Id, Id, (1,2), \overline{\tau})\varphi_{36}.$$

This τ *has all the required properties (it is checkable by hand).*

Step 3. Construct the set of all ${\pi_{\overline{\sigma_2}}}^{-1}(\mathcal{G}) + {\pi_{\overline{\sigma_3}}}^{-1}(\mathcal{H})$, with $\mathcal{G} \in \mathbb{G}$ and $\mathcal{H} \in \mathbb{H}$ and take one representant for each equivalence class of this set. Collect them in the set $\mathbb{L}$.

3.2.2 Description of the exhaustive search

We know that $(\mathcal{C}(\sigma_6^2) + \mathcal{C}(\sigma_6^3))^\psi = \mathcal{L}$ and $\sigma_6^\psi = \sigma_6$ for some $\mathcal{L} \in \mathbb{L}'$ and $\psi \in \mathcal{S}_{72}$. Put $\mathcal{C}' = \mathcal{C}^\psi$. Then $\mathcal{C}'$ is a self-dual $[72, 36, 16]$ code which admits σ_6 as automorphism. We have $\mathcal{C}' = \mathcal{C}'(\sigma_6^2) \oplus \mathcal{E}'(\sigma_6^2)$. From Remark 3.4 we have $\mathrm{soc}(\mathcal{E}'(\sigma_6)) = (\mathcal{C}'(\sigma_6^2) + \mathcal{C}'(\sigma_6^3)) \cap \mathcal{V}(\sigma_6^2)^\perp = \mathcal{L} \cap \mathcal{V}(\sigma_6^2)^\perp$. Let us fix

$$\mathcal{L} \cap \mathcal{V}(\sigma_6^2)^\perp = V_1 \oplus V_2 \oplus V_3 \oplus V_4 \oplus V_5 \oplus V_6,$$

a decomposition of $\mathcal{L} \cap \mathcal{V}(\sigma_6^2)^\perp$ in irreducible $K\langle\sigma_6\rangle$-modules.
By Remark 2.1 and Remark 3.4 we have that

$$\mathcal{E}'(\sigma_6^2) = \begin{matrix} V_1 \\ V_1 \end{matrix} \oplus \begin{matrix} V_2 \\ V_2 \end{matrix} \oplus \begin{matrix} V_3 \\ V_3 \end{matrix} \oplus \begin{matrix} V_4 \\ V_4 \end{matrix} \oplus \begin{matrix} V_5 \\ V_5 \end{matrix} \oplus \begin{matrix} V_6 \\ V_6 \end{matrix},$$

where $\mathrm{P}(V_i) = \begin{matrix} V_i \\ V_i \end{matrix}$ is a projective indecomposable module with socle V_i, for $i \in \{1, \ldots, 6\}$.

Remark 3.7. *Since $1 + \sigma_6^3$ is in the Jacobson radical of $K\langle\sigma_6\rangle$, we get*

$$V_i = \mathrm{P}(V_i)(1 + \sigma_6^3).$$

Remark 3.8. *We have $\mathcal{L} \subset \mathcal{C}' = \mathcal{C}'^\perp \subset \mathcal{L}^\perp$. In particular*

$$\mathcal{L} \cap \mathcal{V}(\sigma_6^2)^\perp \subset \mathcal{E}'(\sigma_6^2) \subset \mathcal{L}^\perp \cap \mathcal{V}(\sigma_6^2)^\perp.$$

Let us call $\mathcal{U}$ a subspace of $\mathcal{L}^\perp \cap \mathcal{V}(\sigma_6^2)^\perp$ such that

$$(\mathcal{L} \cap \mathcal{V}(\sigma_6^2)^\perp) \oplus \mathcal{U} = \mathcal{L}^\perp \cap \mathcal{V}(\sigma_6^2)^\perp$$

(by simple calculations $\dim(\mathcal{U}) = 24$). Obviously there exist $W_1, \ldots, W_6$, 2-dimensional subspaces of $\mathcal{U}$, such that

$$\mathrm{P}(V_i) = V_i \oplus W_i,$$

for $i \in \{1, \ldots, 6\}$. Let us underline that every W_i is a subspace but not a $K\langle\sigma_6\rangle$-module. Furthermore, by Remark 3.7, $W_i(1 + \sigma_6^3)$ is contained in V_i.

Finally, it is easy to prove that, for every nonzero $v_i \in V_i$, there exists a $w_i \in W_i$ such that

$$w_i \cdot K\langle\sigma_6\rangle = \mathrm{P}(V_i) \qquad \textit{and} \qquad w_i(1+\sigma_6^3) = v_i.$$

These remarks give us all the tools to do an exhaustive search. Let us explain our algorithm.

Take the set $\mathbb{L}'$ defined in Remark 3.5 and, for every $\mathcal{L} \in \mathbb{L}'$, do:

Step 1. Find 6 irreducible $K\langle\sigma_6\rangle$-modules, say $V_1, \ldots, V_6$, such that

$$\mathcal{L} \cap \mathcal{V}(\sigma_6^2)^\perp = V_1 \oplus \ldots \oplus V_6.$$

Choose one nonzero element $v_i \in V_i$ for every $i \in \{1, \ldots, 6\}$.

Step 2. Set $\mathcal{U} := \mathcal{L}^\perp \cap \mathcal{V}(\sigma_6^2)^\perp$ and, for every $i \in \{1, \ldots, 6\}$, find the sets

$$(\mathbb{H}_\mathcal{L})_i := \{u \in \mathcal{U} \mid u(1+\sigma_6^3) = v_i\}.$$

By linear algebra arguments, $(\mathbb{H}_\mathcal{L})_i$ is the coset $\ker(m) + w_i$, where

$$m : \mathcal{U} \to \mathrm{soc}(\mathcal{V}(\sigma_6^2)^\perp)$$

is the map $u \mapsto u(1+\sigma_6^3)$ and $m(w_i) = v_i$.
Moreover $|\ker(m)| = 2^{12} = 4096$.
For every $i \in \{1, \ldots, 6\}$, find the sets

$$(\mathbb{H}_\mathcal{L}{}')_i := \{w \in (\mathbb{H}_\mathcal{L})_i \mid \mathcal{L} + K\langle\sigma_6\rangle \text{ is doubly-even}\}$$

and then

$$(\mathbb{H}_\mathcal{L}{}'')_i := \{w \in (\mathbb{H}_\mathcal{L}{}')_i \mid \mathrm{d}(\mathcal{L} + w \cdot K\langle\sigma_6\rangle) \geq 16\}.$$

We can remark that $|(\mathbb{H}_\mathcal{L}{}'')_i| < 2^{11} = 2048$, by calculations.

Step 3. Find the subset $\mathbb{P}_\mathcal{L}$ of $(\mathbb{H}_\mathcal{L}{}'')_1 \times (\mathbb{H}_\mathcal{L}{}'')_2$ so defined

$$\mathbb{P}_\mathcal{L} := \{(w_1, w_2) \mid \mathrm{d}(\mathcal{L} + w_1 \cdot K\langle\sigma_6\rangle + w_2 \cdot K\langle g\rangle) \geq 16\}.$$

Find the subset $\mathbb{T}_\mathcal{L}$ of $\mathbb{P}_\mathcal{L} \times (\mathbb{H}_\mathcal{L}{}'')_3$ so defined

$$\mathbb{T}_\mathcal{L} := \{(w_1, \ldots, w_3) \mid \mathrm{d}(\mathcal{L} + w_1 \cdot K\langle\sigma_6\rangle + \ldots + w_3 \cdot K\langle\sigma_6\rangle) \geq 16\}.$$

Find the subset $\mathbb{Q}_{\mathcal{L}}$ of $\mathbb{T}_{\mathcal{L}} \times (\mathbb{H}_{\mathcal{L}}'')_4$ so defined

$$\mathbb{Q}_{\mathcal{L}} := \{(w_1, \ldots, w_4) \mid \mathrm{d}(\mathcal{L} + w_1 \cdot K\langle\sigma_6\rangle + \ldots + w_4 \cdot K\langle\sigma_6\rangle) \geq 16\}.$$

Find the subset $\mathbb{F}_{\mathcal{L}}$ of $\mathbb{Q}_{\mathcal{L}} \times (\mathbb{H}_{\mathcal{L}}'')_5$ so defined

$$\mathbb{F}_{\mathcal{L}} := \{(w_1, \ldots, w_5) \mid \mathrm{d}(\mathcal{L} + w_1 \cdot K\langle\sigma_6\rangle + \ldots + w_5 \cdot K\langle\sigma_6\rangle) \geq 16\}.$$

Find the subset $\mathbb{S}_{\mathcal{L}}$ of $\mathbb{F}_{\mathcal{L}} \times (\mathbb{H}_{\mathcal{L}}'')_6$ so defined

$$\mathbb{S}_{\mathcal{L}} := \{(w_1, \ldots, w_6) \mid \mathrm{d}(\mathcal{L} + w_1 \cdot K\langle\sigma_6\rangle + \ldots + w_6 \cdot K\langle\sigma_6\rangle) \geq 16\}.$$

Theorem 3.3 tells us that, if a self-dual $[72, 36, 16]$ code with automorphism of order 6 exists, then it has a subcode equivalent to one of the 38 codes in $\mathbb{L}$.
Remarks 3.5 and 3.8 imply that the eventual code can be found in the sets

$$\{\mathcal{L} + w_1 \cdot K\langle\sigma_6\rangle + \ldots + w_6 \cdot K\langle\sigma_6\rangle \mid (w_1, \ldots, w_6) \in \mathbb{S}_{\mathcal{L}}\}_{\mathcal{L} \in \mathbb{L}'}.$$

MAGMA calculations find $\mathbb{S}_{\mathcal{L}}$ empty, for every $\mathcal{L} \in \mathbb{L}'$. So a self-dual $[72, 36, 16]$ code with automorphism of order 6 does not exist.

3.3 Case $\mathrm{Aut}(\mathcal{C})$ containing a subgroup isomorphic to $\mathcal{S}_3$

In this section we will get that the automorphism groups of extremal self-dual binary linear codes of length 72 cannot be of order 6, excluding also the non-abelian case. We apply here the methods of Section 2.4, which are, as we said, a generalization of those used by Nebe and Feulner in [24] for the non-abelian automorphism group of order 10.

Let $\mathcal{C}$ be a self-dual $[72, 36, 16]$ code and suppose that $G \leq \mathrm{Aut}(\mathcal{C})$ with $G \cong \mathcal{S}_3$.

Let σ_2 denote an element of order 2 and σ_3 an element of order 3 in G. By Proposition 3.1, σ_2 and σ_3 are fixed point free automorphisms. So we can suppose that

$$\sigma_2 = (1,4)(2,6)(3,5)\dots(67,70)(68,72)(69,71)$$

and

$$\sigma_3 = (1,2,3)(4,5,6)\dots(67,68,69)(70,71,72).$$

As we have seen in Section 2.2,

$$\mathcal{C} = \mathcal{C}(\sigma_3) \oplus \mathcal{E}(\sigma_3)$$

where $\mathcal{E}(\sigma_3)$ is the subcode of $\mathcal{C}$ of all the codewords with an even weight on the cycles of σ_3, of dimension 24.

Since σ_2 and σ_3 are fixed point free, $s(3) = 3 - 1$ and $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ is self-dual, all the requirements of Theorem 2.7 are satisfied. Then

$$\mathcal{C} = \pi_{\sigma_3}^{-1}(\mathcal{A}) \oplus \varphi_3^{-1}(\langle \pi^{-1}(\mathcal{B}) \rangle_{\mathbb{F}_4})$$

where $\mathcal{A} \leq \mathbb{F}_2^{24}$, self-dual binary linear code, $\mathcal{B} \subseteq \mathbb{F}_4^{12}$, $\mathbb{F}_2$-linear (additive) trace-Hermitian self-dual quaternary code, φ_3 is the map defined in Section 2.2 and

$$\pi := \mathbb{F}_4^{12} \to \mathbb{F}_4^6$$

maps $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{11}, \varepsilon_{12}) \mapsto (\varepsilon_1, \dots, \varepsilon_{11})$.
We have, in particular,

$$\mathcal{C}(\sigma_3) = \pi_{\sigma_3}^{-1}(\mathcal{A})$$

and

$$\mathcal{E}(\sigma_3) = \varphi_3^{-1}(\langle \pi^{-1}(\mathcal{B}) \rangle_{\mathbb{F}_4}).$$

Since every nonzero element of the field correspond to a vector of weight 2, we have that the minimum distance of $\varphi_3(\mathcal{E}(\sigma_3))$ is ≥ 8. So the code $\mathcal{B}$ is an additive trace-Hermitian self-dual $(12, 2^{12}, \geq 4)_4$ code. All additive trace-Hermitian self-dual codes in $\mathbb{F}_4^{12}$ are classified in [20]. There are $195,520$ such codes that have minimum distance ≥ 4 up to monomial equivalence.

Remark 3.9. *If $\mathcal{X}$ and $\mathcal{Y}$ are monomial equivalent, via a 12×12 monomial matrix $M := (m_{i,j})$, then $\varphi_3(\mathcal{X})$ and $\varphi_3(\mathcal{Y})$ are monomial equivalent too, via the 24×24 monomial matrix $M' := (m'_{i,j})$, where $m'_{2i-1,2j-1} = m_{i,j}$ and $m'_{2i,2j} = \overline{m_{i,j}}$, for all $i, j \in \{1, \ldots, 12\}$.*

An exhaustive search with MAGMA shows that the minimum distance of $\langle \pi^{-1}(\mathcal{B}) \rangle_{\mathbb{F}_4}$ is ≤ 6, for each of the 195,520 additive trace-Hermitian self-dual $(12, 2^{12}, \geq 4)_4$ codes. But $\mathcal{E}(g)'$ should have minimum distance ≥ 8, a contradiction. So we proved the following.

Theorem 3.1. *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain a subgroup isomorphic to $\mathcal{S}_3$.*

In particular we exclude $\mathcal{S}_3$ and $\mathcal{S}_4$.

3.4 Case $\mathrm{Aut}(\mathcal{C})$ containing a subgroup isomorphic to $\mathcal{A}_4$ or to D_8

In this section we will prove that the automorphism group of the putative extremal self-dual binary linear code of length 72 is not isomorphic to $\mathcal{A}_4$ or D_8, excluding the last possible non-abelian automorphism groups.

The methods for the two groups are very similar, so we will present them in parallel. In facts, we firstly look at the action of the Klein four group, which is a normal subgroup of both, finding the sum of the codes fixed by the involutions using the action of the full group, with methods similar to those exposed in Section 2.5. Then we build the whole code, with different methods for the two cases. Doing an exhaustive search with MAGMA, we check that no extremal code occurs.

3.4.1 The action of the Klein four group

First of all, we note, as we said above, that the Klein four group V_4 is a normal subgroup of both the alternating group $\mathcal{A}_4$ of degree 4 and the dihedral

group D_8 of order 8. In particular, we point out their structure as semidirect product:

$$\begin{aligned} \mathcal{A}_4 \cong &\ \mathcal{V}_4 \rtimes C_3 \cong &\ (C_2 \times C_2) \rtimes C_3 \\ D_8 \cong &\ \mathcal{V}_4 \rtimes C_2 \cong &\ (C_2 \times C_2) \rtimes C_2 \end{aligned}$$

Let now $\mathcal{C}$ be a self-dual $[72, 36, 16]$ code such that $H \leq \mathrm{Aut}(\mathcal{C})$ where $H \cong \mathcal{A}_4$ or $H \cong D_8$.

By Proposition 3.1 all non-trivial elements in H are fixed point free and we can suppose, without lost of generality, that $H = \langle \alpha, \beta \rangle \rtimes \langle \sigma_i \rangle$, $i = 3$ and $i = 2$ respectively, with

$$\begin{aligned} \alpha := &\ (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)\dots(71,72) \\ \beta := &\ (1,3)(2,4)(5,7)(6,8)(9,11)(10,12)\dots(70,72) \\ \sigma_3 := &\ (1,5,9)(2,7,12)(3,8,10)(4,6,11)\dots(64,66,71) \\ \sigma_2 := &\ (1,5)(2,8)(3,7)(4,6)\dots(68,70) \end{aligned}$$

Let

$$G := \mathrm{C}_{\mathcal{S}_{72}}(H) = \{\tau \in \mathcal{S}_{72} \mid \tau\alpha = \alpha\tau, \tau\beta = \beta\tau, \tau\sigma_i = \sigma_i\tau\}$$

($i = 2, 3$ respectively) denote the centralizer of H in $\mathcal{S}_{72}$.

Then G acts on the set of extremal self-dual binary linear codes with H subgroup of their automorphism group and we aim to find a system of orbit representatives for this action.

As usual we define $\pi_\alpha : \mathbb{F}_2^{72} \to \mathbb{F}_2^{36}$. Then we have

$$\begin{aligned} &\pi' : \{v \in \mathbb{F}_2^{72} \mid v^\alpha = v \text{ and } v^\beta = v\} \to \mathbb{F}_2^{18} \\ &(v_1, v_1, v_1, v_1, v_2, \dots, v_{18}) \mapsto (v_1, v_2, \dots, v_{18}) \end{aligned}$$

the bijection between the fixed space of $\langle \alpha, \beta \rangle$ and $\mathbb{F}_2^{18}$. Then β acts on the image of $\mathbb{F}_2^{18}$ as

$$(1,2)(3,4)\dots(35,36).$$

Let

$$\begin{aligned} &\pi'' : \{v \in \mathbb{F}_2^{36} \mid v^{\eta_\alpha(\beta)} = v\} \to \mathbb{F}_2^{18}, \\ &(v_1, v_1, v_2, v_2, \dots, v_{18}, v_{18}) \mapsto (v_1, v_2, \dots, v_{18}), \end{aligned}$$

so that $\pi' = \pi'' \circ \pi_\alpha$.

Remark 3.10. *As in Section 2.5 we note that* $\mathrm{C}_{\mathcal{S}_{72}}(\alpha) \cong C_2 \wr \mathcal{S}_{36}$ *acts on the set of fixed points of* α *and so we denote by* η_α *the map*

$$\eta_\alpha : \mathrm{C}_{\mathcal{S}_{72}}(\alpha) \to \mathcal{S}_{36}$$

with kernel C_2^{36}*. Similarly we obtain the epimorphism*

$$\eta'' : \mathrm{C}_{\mathcal{S}_{36}}(\eta_\alpha(\beta)) \to \mathcal{S}_{18}.$$

The normalizer $\mathrm{N}_{\mathcal{S}_{72}}(\langle \alpha, \beta \rangle)$ *acts on the set of* $\langle \alpha, \beta \rangle$*-orbits which defines a homomorphism*

$$\eta' : \mathrm{N}_{\mathcal{S}_{72}}(\langle \alpha, \beta \rangle) \to \mathcal{S}_{18}.$$

We know by Proposition 3.1 that the code $\pi_\alpha(\mathcal{C}(\alpha))$ is, up to equivalence, one among the 41 codes classified in [42]. Let

$$\mathcal{Y}_1, \ldots, \mathcal{Y}_{41}$$

be a system of representatives of these extremal self-dual binary linear codes of length 36.

Remark 3.11. *We have that* $\mathcal{C}(\alpha) \in \mathbb{D}$ *where*

$$\mathbb{D} := \left\{ \mathcal{D} \leq \mathbb{F}_2^{36} \;\middle|\; \begin{array}{c} \mathcal{D} = \mathcal{D}^\perp, \mathrm{d}(\mathcal{D}) = 8, \eta_\alpha(\beta) \in \mathrm{Aut}(\mathcal{D}) \\ \text{and } \eta''(\sigma_i) \in \mathrm{Aut}(\pi''(\mathcal{D}(\eta_\alpha(\beta)))) \end{array} \right\}.$$

For $1 \leq k \leq 41$ *let* $\mathbb{D}_k := \{\mathcal{D} \in \mathbb{D} \mid \mathcal{D} \cong \mathcal{Y}_k\}$.

Let $G_{36} := \{\tau \in \mathrm{C}_{\mathcal{S}_{36}}(\eta_\alpha(\beta)) \mid \eta''(\tau)\eta'(\sigma_i) = \eta'(\sigma_i)\eta''(\tau)\}$.

Remark 3.12. *The following facts hold, by direct calculations:*

- *for* $H \cong \mathcal{A}_4$ *the group* G_{36} *is isomorphic to* $C_2 \wr C_3 \wr \mathcal{S}_6$*. It contains* $\eta_\alpha(G) \cong \mathcal{A}_4 \wr \mathcal{S}_6$ *and of index* $[G_{36} : \eta_\alpha(G)] = 64$*;*
- *for* $H \cong D_8$ *we get* $G_{36} = \eta_\alpha(G) \cong C_2 \wr C_2 \wr \mathcal{S}_9$*.*

Now we want to compute a set of representatives of the G_{36}-orbits on $\mathbb{D}_k$. Thus we perform the following steps:

- Let $\beta_1, \ldots, \beta_s$ represent the conjugacy classes of fixed point free elements of order 2 in $\mathrm{Aut}(\mathcal{Y}_k)$.
- Compute elements $\tau_1, \ldots, \tau_s \in \mathcal{S}_{36}$ such that $\tau_i^{-1}\beta_i\tau_i = \eta_\alpha(\beta)$ and put $\mathcal{D}_i := \mathcal{Y}_k^{\tau_i}$ so that $\eta_\alpha(\beta) \in \mathrm{Aut}(\mathcal{D}_i)$.
- For all $\mathcal{D}_i$ let $\zeta_1, \ldots, \zeta_{t_i}$ a set of representives of the action by conjugation by the subgroup $\eta''(\mathrm{C}_{\mathrm{Aut}(\mathcal{D}_i)}(\eta_\alpha(\beta)))$ on fixed point free elements of order 3 (for $H \cong \mathcal{A}_4$) respectively 2 (for $H \cong D_8$) in $\mathrm{Aut}(\pi_\alpha(\mathcal{D}_i(\eta_\alpha(\beta))))$.
- Compute elements $\rho_1, \ldots \rho_{t_i} \in \mathcal{S}_{18}$ such that $\rho_j^{-1}\zeta_j\rho_j = \eta''(\sigma_\iota)$ ($\iota = 3, 2$ respectively), lift ρ_j naturally to a permutation $\tilde{\rho}_j \in \mathcal{S}_{36}$ commuting with $\eta_\alpha(\beta)$ (defined by $\tilde{\rho}_j(2a-1) = 2\rho_j(a) - 1$, $\tilde{\rho}_j(2a) = 2\rho_j(a)$) and put
$$\mathcal{D}_{i,j} := (\mathcal{D}_i)^{\tilde{\rho}_j} = \mathcal{Y}_k^{\tau_i\tilde{\rho}_j}$$
so that $\eta_\alpha(\sigma_\iota) \in \mathrm{Aut}(\pi'(\mathcal{D}_{i,j}(\eta_\alpha(\beta))))$.

Lemma 3.3. *The set $\{\mathcal{D}_{i,j} \mid 1 \le i \le s, 1 \le j \le t_i\}$ defined above represents the G_{36}-orbits on $\mathbb{D}_k$.*

Proof. Clearly these codes lie in $\mathbb{D}_k$.
Now assume that there is some $\tau \in G_{36}$ such that
$$\mathcal{Y}_k^{\tau_{i'}\tilde{\rho}_{j'}\tau} = \mathcal{D}_{i',j'}^{\tau} = \mathcal{D}_{i,j} = \mathcal{Y}_k^{\tau_i\tilde{\rho}_j}.$$
Then
$$\epsilon := \tau_{i'}\tilde{\rho}_{j'}\tau\tilde{\rho}_j^{-1}\tau_i^{-1} \in \mathrm{Aut}(\mathcal{Y}_k)$$
satisfies $\epsilon\beta_i\epsilon^{-1} = \beta_{i'}$, so β_i and $\beta_{i'}$ are conjugate in $\mathrm{Aut}(\mathcal{Y}_k)$, which implies $i = i'$ (and so $\tau_i = \tau_{i'}$). Now,
$$\mathcal{Y}_k^{\tau_i\tilde{\rho}_{j'}\tau} = \mathcal{D}_i^{\tilde{\rho}_{j'}\tau} = \mathcal{D}_i^{\tilde{\rho}_j} = \mathcal{Y}_k^{\tau_i\tilde{\rho}_j}.$$
Then
$$\epsilon' := \tilde{\rho}_{j'}\tau\tilde{\rho}_j^{-1} \in \mathrm{Aut}(\mathcal{D}_i)$$

commutes with $\eta_\alpha(\beta)$. We compute that $\eta''(\epsilon')\zeta_j\eta''(\epsilon'^{-1}) = \zeta_{j'}$ and hence $j = j'$.

Now let $\mathcal{D} \in \mathbb{D}_k$ and choose some $\xi \in \mathcal{S}_{36}$ such that $\mathcal{D}^\xi = \mathcal{Y}_k$. Then $\eta_\alpha(\beta)^\xi$ is conjugate to some of the chosen representatives $\beta_i \in \mathrm{Aut}(\mathcal{Y}_k)$ $(i \in 1, \ldots, s)$ and we may multiply ξ by some automorphism of $\mathcal{Y}_k$ so that $\eta_\alpha(\beta)^\xi = \beta_i = \eta_\alpha(\beta)^{\tau_i^{-1}}$. So $\xi\tau_i \in \mathrm{C}_{\mathcal{S}_{36}}(\eta_\alpha(\beta))$ and $\mathcal{D}^{\xi\tau_i} = \mathcal{Y}_k^{\tau_i} = \mathcal{D}_i$. Since $\eta''(\sigma_\iota) \in \mathrm{Aut}(\pi''(\mathcal{D}(\eta_\alpha(\beta))))$ we get

$$\eta''(\xi\tau_i)^{-1}\eta''(\sigma_\iota)\eta''(\xi\tau_i) \in \mathrm{Aut}(\pi''(\mathcal{D}_i(\eta_\alpha(\beta))))$$

and so there is some automorphism $\mu \in \eta''(\mathrm{C}_{\mathrm{Aut}(\mathcal{D}_i)}(\eta_\alpha(\beta)))$ and some $j \in \{1, \ldots, t_i\}$ such that $\mu^{-1}\eta''(\xi\tau_i)^{-1}\eta''(\sigma_\iota)\eta''(\xi\tau_i)\mu = \zeta_j$. Then

$$\mathcal{D}^{\xi\tau_i\tilde{\mu}\tilde{\rho}_j} = \mathcal{D}_{i,j}$$

where $\xi\tau_i\tilde{\mu}\tilde{\rho}_j \in G_{36}$. □

Next we will deal separately the two cases.

3.4.2 Case $H \cong \mathcal{A}_4$

We now deal with the case $H \cong \mathcal{A}_4$.

Remark 3.13. *We use the algorithm given in Lemma 3.3 to compute, with* Magma, *that there are exactly* $25,299$ G_{36}*-orbits on* $\mathbb{D}$*, represented by, say,* $\mathcal{X}_1, \ldots, \mathcal{X}_{25,299}$.

By Remark 3.12 we have $[G_{36} : \pi_\alpha(G)] = 64$. Let $\alpha_1, \ldots, \alpha_{64} \in G_{36}$ be a left transversal of $\pi_\alpha(G)$ in G_{36} .

Then the set

$$\{\mathcal{X}_i^{\alpha_j} \mid 1 \leq i \leq 25,299, 1 \leq j \leq 64\}$$

contains a set of representatives of the $\eta_\alpha(G)$-orbits on $\mathbb{D}$.

Remark 3.14. *For all* $1 \leq i \leq 25,299, 1 \leq j \leq 64$ *we compute, with* MAGMA, *the code*

$$\mathcal{E} := \mathcal{E}(\mathcal{X}_i^{\alpha_j}, \sigma_3) := \tilde{\mathcal{D}} + \tilde{\mathcal{D}}^{\sigma_3} + \tilde{\mathcal{D}}^{\sigma_3^2}, \text{ where } \tilde{\mathcal{D}} = \pi_\alpha^{-1}(\mathcal{X}_i^{\alpha_j}).$$

For three $\mathcal{X}_i$ *there are two codes* $\tilde{\mathcal{D}}_{i,1} = \pi_\alpha^{-1}(\mathcal{X}_i^{\alpha_{j_1}})$ *and* $\tilde{\mathcal{D}}_{i,2} = \pi_\alpha^{-1}(\mathcal{X}_i^{\alpha_{j_2}})$ *such that* $\mathcal{E}(\mathcal{X}_i^{\alpha_{j_1}}, \sigma_3)$ *and* $\mathcal{E}(\mathcal{X}_i^{\alpha_{j_2}}, \sigma_3)$ *are doubly even and of minimum distance* 16. *In all three cases, the two codes are equivalent. Let us call the inequivalent codes* $\mathcal{E}_1, \mathcal{E}_2$ *and* $\mathcal{E}_3$, *respectively. They have dimension* 26, 26, *and* 25, *respectively, minimum distance* 16 *and their automorphism groups are*

$$\mathrm{Aut}(\mathcal{E}_1) \cong \mathcal{S}_4, \mathrm{Aut}(\mathcal{E}_2) \text{ of order } 432, \mathrm{Aut}(\mathcal{E}_3) \cong (\mathcal{A}_4 \times \mathcal{A}_5) : 2.$$

All three groups contain a unique conjugacy class of subgroups conjugate in $\mathcal{S}_{72}$ *to* $\mathcal{A}_4$ (*which is normal for* $\mathcal{E}_1$ *and* $\mathcal{E}_3$).

Thus we have the following result, which is a direct consequence of Remark 3.14 and of Theorem 2.8.

Theorem 3.5. *The code* $\mathcal{C}(\alpha) + \mathcal{C}(\beta) + \mathcal{C}(\alpha\beta)$ *is equivalent under the action of* G *to one of the three codes* $\mathcal{E}_1, \mathcal{E}_2$ *or* $\mathcal{E}_3$ *of Remark* 3.14.

Now, we know, up to equivalence, a quite large subcode of our putative extremal self-dual binary linear code. Next, we try to construct the whole code.

Let $\mathcal{E}$ be one of these three codes. The group $\mathcal{A}_4$ acts on $\mathcal{V} := \mathcal{E}^\perp/\mathcal{E}$ with kernel $\langle \alpha, \beta \rangle$. The space $\mathcal{V}$ is hence an $\mathbb{F}_2\langle \sigma_3 \rangle$-module supporting a σ_3-invariant form such that $\mathcal{C}$ is a self-dual submodule of $\mathcal{V}$. We obtain as usual a canonical decomposition, as in Section 2.2,

$$\mathcal{V} = \mathcal{V}(\sigma_3) \oplus \mathcal{W}$$

where $\mathcal{V}(\sigma_3)$ is the fixed space of σ_3 and σ_3 acts as a primitive third root of unity on $\mathcal{W}$.

For $\mathcal{E} = \mathcal{E}_1$ or $\mathcal{E} = \mathcal{E}_2$ we compute that $\mathcal{V}(\sigma_3) \cong \mathbb{F}_2^4$ and $\mathcal{W} \cong \mathbb{F}_4^8$. For both codes the full preimage of every self-dual submodule of $\mathcal{V}(\sigma_3)$ is a code of minimum distance < 16.

For $\mathcal{E} = \mathcal{E}_3$ the dimension of $\mathcal{V}(\sigma)$ is 2 and there is a unique self-dual submodule of $\mathcal{V}(\sigma_3)$ so that the full preimage $\mathcal{E}_3$ is doubly-even and of minimum distance ≥ 16. The element σ_3 acts on $\mathcal{E}_3^\perp/\mathcal{E}_3 \cong \mathcal{W}$ with irreducible minimal polynomial, so $\mathcal{E}_3^\perp/\mathcal{E}_3 \cong \mathbb{F}_4^{10}$. The code $\mathcal{C}$ is a preimage of one of the $58,963,707$ maximal isotropic $\mathbb{F}_4$-subspaces of the Hermitian $\mathbb{F}_4$-space $\mathcal{E}_3^\perp/\mathcal{E}_3$.

The unitary group $\mathrm{GU}(10,2)$ of $\mathcal{E}_3^\perp/\mathcal{E}_3 \cong \mathbb{F}_4^{10}$ acts transitively on the maximal isotropic subspaces. So a quite convenient way to enumerate all these spaces is to compute an isometry of $\mathcal{E}_3^\perp/\mathcal{E}_3$ with the standard model used in Magma and then compute the $\mathrm{GU}(10,2)$-orbit of one maximal isotropic space (e.g. the one spanned by the first 5 basis vectors in the standard model). For computational reasons, we first compute all $142,855$ one dimensional isotropic subspaces $\overline{\mathcal{E}}_3/\mathcal{E}_3 \leq_{\mathbb{F}_4} \mathcal{E}_3^\perp/\mathcal{E}_3$ for which the code $\overline{\mathcal{E}}_3$ has minimum distance ≥ 16. The automorphism group $\mathrm{Aut}(\mathcal{E}_3) = \mathrm{Aut}(\mathcal{E}_3)$ acts on these codes with $1,264$ orbits. For all these $1,264$ orbit representatives $\overline{\mathcal{E}}_3$ we compute the $114,939$ maximal isotropic subspaces of $\overline{\mathcal{E}}_3^\perp/\overline{\mathcal{E}}_3$ (as the orbits of one given subspace under the unitary group $\mathrm{GU}(8,2)$ in Magma) and check whether the corresponding self-dual doubly-even binary linear code has minimum distance 16. No such code is found.

This computation concludes the proof of the following theorem.

Theorem 3.2. *The automorphism group of a self-dual* $[72,36,16]$ *code does not contain a subgroup isomorphic to* $\mathcal{A}_4$.

3.4.3 Case $H \cong D_8$

For this subsection we assume that $H \cong D_8$.

Then, by Remark 3.12, $\pi_\alpha(G) = G_{36}$ and we may use Lemma 3.3 to compute, with Magma a system of representatives of the $\eta_\alpha(G)$-orbits on the set $\mathbb{D}$.

Remark 3.15. *The group $\eta_\alpha(G)$ acts on $\mathbb{D}$ with exactly $9,590$ orbits represented by, say, $\mathcal{X}_1, \ldots, \mathcal{X}_{9,590}$. For all $1 \le i \le 9,590$ we compute the code*

$$\mathcal{E} := \mathcal{E}(\mathcal{X}_i, \sigma_2) := \tilde{\mathcal{D}} + \tilde{\mathcal{D}}^{\sigma_2}, \text{ where } \tilde{\mathcal{D}} = \pi_\alpha^{-1}(\mathcal{X}_i).$$

For four $\mathcal{X}_i$ the code $\mathcal{E}(\mathcal{X}_i, \sigma_2)$ is doubly even and of minimum distance 16. Let us call the inequivalent codes $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ and $\mathcal{E}_4$, respectively. All have dimension 26 and minimum distance 16.

Thus we have the following result, which is a direct consequence of Remark 3.15 and of direct calculations.

Lemma 3.4. *The code $\mathcal{C}(\alpha) + \mathcal{C}(\beta) + \mathcal{C}(\alpha\beta)$ is equivalent under the action of G to one of the four codes $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ or $\mathcal{E}_4$ of Remark 3.15.*

As it seems to be quite hard to compute all D_8-invariant self-dual overcodes of $\mathcal{E}_i$ for these four codes $\mathcal{E}_i$ we apply a different strategy which is based on the fact that $\beta = (\alpha\sigma_2)^2$ is the square of an element of order 4. So let

$$\kappa := \alpha\sigma_2 = (1,8,3,6)(2,5,4,7)\ldots(66,69,68,71) \in D_8.$$

By [45], $\mathcal{C}$ is a free $\mathbb{F}_2\langle\kappa\rangle$-module (of rank 9). Since $\langle\kappa\rangle$ is abelian, the module is both left and right; here we use the right notation. The regular module $\mathbb{F}_2\langle\kappa\rangle$ has a unique irreducible module, 1-dimensional, called the socle, that is $\langle(1+\kappa+\kappa^2+\kappa^3)\rangle$. So $\mathcal{C}$, as a free $\mathbb{F}_2\langle\kappa\rangle$-module, has socle $\mathcal{C}(\kappa) = \mathcal{C}\cdot(1+\kappa+\kappa^2+\kappa^3)$. This implies that, for every basis $b_1, \ldots, b_9$ of $\mathcal{C}(\kappa)$, there exist $w_1, \ldots, w_9$ such that $w_i \cdot (1+\kappa+\kappa^2+\kappa^3) = b_i$ and

$$\mathcal{C} = w_1 \cdot \mathbb{F}_2\langle\kappa\rangle \oplus \ldots \oplus w_9 \cdot \mathbb{F}_2\langle\kappa\rangle.$$

To get all the possible overcodes of $\mathcal{E}_i$, we choose a basis of the socle $\mathcal{E}_i(\kappa)$, say $b_1, \ldots, b_9$, and look at the sets

$$\mathbb{W}_{i,j} := \{w + \mathcal{E}_i \in \mathcal{E}_i^\perp/\mathcal{E}_i \mid w\cdot(1+\kappa+\kappa^2+\kappa^3) = b_j \text{ and } \mathrm{d}(\mathcal{E}_i + w\cdot\mathbb{F}_2\langle\kappa\rangle) \ge 16\}$$

For every i we have at least one j for which the set $\mathbb{W}_{i,j}$ is empty. This computation then shows the following result.

Theorem 3.3. *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain a subgroup isomorphic to D_8.*

3.5 Case $\mathrm{Aut}(\mathcal{C})$ containing a subgroup isomorphic to $C_2 \times C_2 \times C_2$

In this section we will present our last result [8] on the automorphism group of the putative extremal self-dual binary linear code of length 72, excluding the elementary abelian group of order 8.

Partially inspired by the methods of the previous section, here the situation it is quite different, because of the abelianity of the group: the point is that we do not have a non-trivial action of a group on a normal subgroup, since the group is abelian. However, after the classification of the sum of two fixed codes, a simple dimension argument gives the contradiction.

3.5.1 Preliminary observations and main theorem

Let us start with some preliminary observations.

Suppose $\mathcal{C}$ is a self-dual $[72, 36, 16]$ code such that

$$\mathrm{Aut}(\mathcal{C}) \cong C_2 \times C_2 \times C_2.$$

By Proposition 3.1 all non-trivial elements of $\mathrm{Aut}(\mathcal{C})$ are fixed point free and so, without lost of generality, we may suppose that $\mathrm{Aut}(\mathcal{C}) = \langle \alpha, \beta, \gamma \rangle$ with

$$\begin{aligned} \alpha &:= (1,2)(3,4)(5,6)(7,8)\dots(71,72), \\ \beta &:= (1,3)(2,4)(5,7)(6,8)\dots(70,72), \\ \gamma &:= (1,5)(2,6)(3,7)(4,8)\dots(68,72). \end{aligned}$$

Let $\mathcal{V} := \mathbb{F}_2^{72}$.

We define the projections

$$\pi_\alpha : \mathcal{V}(\alpha) \to \mathbb{F}_2^{36},\ \pi_\beta : \mathcal{V}(\beta) \to \mathbb{F}_2^{36} \text{ and } \pi_\gamma : \mathcal{V}(\gamma) \to \mathbb{F}_2^{36}$$

as in Definition 1.17. As usual we get epimorphisms

$$\eta_\alpha : \mathrm{C}_{S_{72}}(\alpha) \to S_{36},\ \eta_\beta : \mathrm{C}_{S_{72}}(\beta) \to S_{36} \text{ and } \eta_\gamma : \mathrm{C}_{S_{72}}(\gamma) \to S_{36}$$

all with kernel C_2^{36}.

By Proposition 3.3 we have that $\pi_\alpha(\mathcal{C}(\alpha))$, $\pi_\beta(\mathcal{C}(\beta))$ and $\pi_\gamma(\mathcal{C}(\gamma))$ are self-dual $[36, 18, 8]$ codes. As we have said many times there 41 such codes, up to equivalence.

Denoted

$$\chi = (1,2)(3,4)\dots(35,36)$$

and

$$\mu = (1,3)(2,4)\dots(34,36),$$

we have

$$H := \langle \chi, \mu \rangle = \langle \eta_\alpha(\beta), \eta_\alpha(\gamma) \rangle = \langle \eta_\beta(\alpha), \eta_\beta(\gamma) \rangle = \langle \pi_\gamma(\alpha), \eta_\gamma(\beta) \rangle,$$

and in particular, $H \leq \mathrm{Aut}(\pi_\alpha(\mathcal{C}(\alpha)))$, $H \leq \mathrm{Aut}(\pi_\beta(\mathcal{C}(\beta)))$ and $H \leq \mathrm{Aut}(\pi_\gamma(\mathcal{C}(\gamma)))$ respectively.

By direct calculations we have that exactly 14 of the 41 self-dual $[36, 18, 8]$ codes, say

$$\mathbb{Y} := \{\mathcal{Y}_1, \dots, \mathcal{Y}_{14}\}, \tag{3.2}$$

have an automorphism group which contains at least one subgroup conjugated to H. Furthermore, we get the following conditions on the dimensions of intersections of fixed codes.

Lemma 3.5. *Let*

$$(\chi', \mu', \zeta') \in \{(\alpha,\beta,\gamma), (\alpha,\gamma,\beta), (\beta,\alpha,\gamma), (\beta,\gamma,\alpha), (\gamma,\alpha,\beta), (\gamma,\beta,\alpha)\}.$$

Then we have only the following possibilities:

Let $G := \mathrm{C}_{S_{72}}(\mathrm{Aut}(\mathcal{C}))$. Then G acts on the set of extremal self-dual binary linear codes with automorphism group $\langle \alpha, \beta, \gamma \rangle$. We aim to find a system of orbit representatives for this action.

As we have observed in Section 2.5, we have

$$\pi_\alpha(\mathcal{C}(\alpha))(\chi) = \pi_\beta(\mathcal{C}(\beta))(\chi) \tag{3.3}$$

Table 3.1: Intersections of fixed codes

$\dim(\mathcal{C}(\chi') \cap \mathcal{C}(\mu') \cap \mathcal{C}(\zeta'))$	$\dim(\mathcal{C}(\chi') \cap \mathcal{C}(\mu'))$	$\dim(\mathcal{C}(\chi') \cap \mathcal{C}(\zeta'))$
5	9	9
5	9	10
6	9	9
6	9	10
6	9	11
6	10	10
6	10	11

and similar relations hold for the other pairs of fixed codes.

The above property allows us to combine properly $\mathcal{C}(\alpha)$ and $\mathcal{C}(\beta)$ classifying their sum. We will get contradiction just by referring to Table 3.1.

So we will prove the following.

Theorem 3.6. *The automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain a subgroup isomorphic to* $C_2 \times C_2 \times C_2$.

3.5.2 Proof of Theorem 3.6

Let

$$\mathbb{D} := \{\mathcal{D} = \mathcal{D}^{\perp} \leq \mathbb{F}_2^{36} \mid \mathrm{d}(\mathcal{D}) = 8,\ \langle \chi, \mu \rangle \leq \mathrm{Aut}(\mathcal{D})\}.$$

The group

$$G_{36} := \mathrm{C}_{S_{36}}(H) = \eta_\alpha(G) = \eta_\beta(G) = \eta_\gamma(G)$$

acts, naturally, on this set.

A set of representatives of the G_{36}-orbits on $\mathbb{D}$ can be computed by performing the following computations on each $\mathcal{Y} \in \mathbb{Y}$ (where $\mathbb{Y}$ is as in (3.2)):

- Let $\chi_1, \ldots, \chi_s$ represent the conjugacy classes of fixed point free elements of order 2 in $\mathrm{Aut}(\mathcal{Y})$.
- Compute elements $\tau_1, \ldots, \tau_s \in S_{36}$ such that $\tau_k^{-1} \chi_k \tau_k = \chi$ and put $\mathcal{Y}_k := \mathcal{Y}^{\tau_k}$ so that $\chi \in \mathrm{Aut}(\mathcal{Y}_k)$.

- For every $\mathcal{Y}_k$, consider the set of fixed point free elements $\tilde{\mu}$ of order 2 in $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$ such that $\langle \chi, \tilde{\mu} \rangle$ is conjugate to $\langle \chi, \mu \rangle$ in S_{36}. Let $\mu_1, \ldots, \mu_{t_k}$ represent the $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$-conjugacy classes in this set.

- Compute elements $\sigma_1, \ldots, \sigma_{t_k} \in \mathrm{C}_{S_{36}}(\chi)$ such that $\sigma_l^{-1}\mu_l\sigma_l = \mu$ and put $\mathcal{Y}_{k,l} := \mathcal{Y}_k^{\sigma_l}$ so that $\langle \chi, \mu \rangle \leq \mathrm{Aut}(\mathcal{Y}_{k,l})$.

Lemma 3.6. *The set* $\mathbb{D}' := \{\mathcal{Y}_{k,l} \mid \mathcal{Y} \in \mathbb{Y}, 1 \leq k \leq s, 1 \leq l \leq t_k\}$ *represents the* G_{36}*-orbits on* $\mathbb{D}$*.*

Proof. Clearly these codes lie in $\mathbb{D}$.
Since $G_{36} \leq S_{36}$, if we consider different (and so non-equivalent) elements in $\mathcal{Y}, \mathcal{Y}' \in \mathbb{Y}$, then $\mathcal{Y}'_{k',l'}$ and $\mathcal{Y}_{k,l}$, defined as above, are not in the same orbit, for any k', l', k, l.
Now assume that there is some $\lambda \in G_{36}$ such that

$$\mathcal{Y}^{\tau_{k'}\sigma_{l'}} = \mathcal{Y}^{\lambda}_{k',l'} = \mathcal{Y}_{k,l} = \mathcal{Y}^{\tau_k\sigma_l}.$$

Then

$$\epsilon := \tau_{k'}\sigma_{l'}\lambda\sigma_l^{-1}\tau_k^{-1} \in \mathrm{Aut}(\mathcal{Y})$$

satisfies $\epsilon\chi_k\epsilon^{-1} = \chi_{k'}$, so χ_k and $\chi_{k'}$ are conjugate in $\mathrm{Aut}(\mathcal{Y})$, which implies $k = k'$ (and so $\tau_k = \tau_{k'}$). Now,

$$\mathcal{Y}^{\tau_k\sigma_{l'}\lambda} = \mathcal{Y}_k^{\sigma_{l'}\lambda} = \mathcal{Y}_k^{\sigma_l} = \mathcal{Y}^{\tau_k\sigma_l}.$$

Then

$$\epsilon' := \sigma_{l'}\lambda\sigma_l^{-1} \in \mathrm{Aut}(\mathcal{Y}_k)$$

commutes with χ. Furthermore $\epsilon'\sigma_l\epsilon'^{-1} = \sigma_{l'}$ and hence $l = l'$.

Now let $\mathcal{Z} \in \mathbb{D}$ and choose some $\xi \in S_{36}$ such that $\mathcal{Z}^{\xi} = \mathcal{Y} \in \mathbb{Y}$. Then $\xi^{-1}\chi\xi$ is conjugate to some of the chosen representatives $\chi_k \in \mathrm{Aut}(\mathcal{Y})$ $(i = 1, \ldots, s)$ and we may multiply ξ by some automorphism of $\mathcal{Y}$ so that

$$\xi^{-1}\chi\xi = \chi_k = \tau_k\chi\tau_k^{-1}.$$

So $\xi\tau_k \in \mathrm{C}_{S_{36}}(\chi)$ and $\mathcal{Z}^{\xi\tau_k} = \mathcal{Y}^{\tau_k} = \mathcal{Y}_k$.
It is straightforward to prove that the element $(\xi\tau_k)^{-1}\mu(\xi\tau_k) \in \mathrm{Aut}(\mathcal{Y}_k)$ is a fixed point free element of order 2 in $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$ such that $\langle \chi, (\xi\tau_k)^{-1}\mu(\xi\tau_k)\rangle$ is conjugate to $\langle \chi, \mu\rangle$ in S_{36}. So there is some automorphism $\omega \in \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$ and some $l \in \{1, \ldots, t_k\}$ such that $(\xi\tau_k\omega)^{-1}\mu(\xi\tau_k\omega) = \mu_l$. Then

$$\mathcal{Y}^{\xi\tau_k\omega\sigma_l} = \mathcal{Y}_{k,l}$$

where $\xi\tau_k\omega\sigma_l \in G_{36}$. □

With MAGMA we compute that $|\mathbb{D}'| = 242$. For our purposes we need to slightly modify this set: consider $\{\mathcal{Y}(\chi) \mid \mathcal{Y} \in \mathbb{D}\}$ and take a set of representatives for the action of G_{36} on this set, say $\mathbb{E} := \{\mathcal{E}_1, \ldots, \mathcal{E}_m\}$. By calculations $m = 40$. For every $i \in \{1, \ldots, m\}$ define the set

$$\tilde{\mathbb{D}}_i := \{\mathcal{Y}^\epsilon \mid \mathcal{Y} \in \mathbb{D}' \text{ such that there exists } \epsilon \in G_{36} \text{ so that } \mathcal{Y}(\chi)^\epsilon = \mathcal{E}_i\}.$$

Clearly $\bigcup_{i=1}^m \tilde{\mathbb{D}}_i$ is still a set of representatives of the G_{36}-orbits on $\mathbb{D}$. However, here we have $\mathcal{Y}_j(\chi) = \mathcal{Y}_k(\chi)$ if and only if $\mathcal{Y}_j, \mathcal{Y}_k \in \tilde{\mathbb{D}}_i$. Furthermore, if $\mathcal{Y}_j$ and $\mathcal{Y}_k$ do not belong to the same $\tilde{\mathbb{D}}_i$, we have that $\mathcal{Y}_j(\chi)$ and $\mathcal{Y}_k(\chi)$ are not equivalent via the action of G_{36} (that is they are not in the same orbit).

Let

$$\mathbb{D}_{(\alpha,\beta)_i} = \{\pi_\alpha^{-1}(\mathcal{Y}_\alpha) + (\pi_\beta^{-1}(\mathcal{Y}_\beta))^\omega \leq \mathbb{F}_2^{72} \mid \mathcal{Y}_\alpha, \mathcal{Y}_\beta \in \tilde{\mathbb{D}}_i, \omega \in \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu\rangle)\}.$$

Remark 3.16. *We observe that, in order to make the computations faster, we can consider* $(\pi_\beta^{-1}(\mathcal{Y}_\beta))^\tau$ *with* τ *varying in a right transversal of*

$$\mathrm{Aut}(\mathcal{Y}_\beta(\chi)) \cap \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu\rangle)$$

in

$$\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu\rangle),$$

instead of $(\pi_\beta^{-1}(\mathcal{Y}_\beta))^\omega$ *with* ω *varying in* $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu\rangle)$.

Then we have the following fundamental result.

Theorem 3.7. *The code $\mathcal{C}(\alpha)+\mathcal{C}(\beta)$ is equivalent, via the action of G, to an element of $\bigcup_{i=1}^{m}\mathbb{D}_{(a,b)_i}$.*

Proof. By Lemma 3.6 and by construction of $\bigcup_{i=1}^{m}\tilde{\mathbb{D}}_i$, there exist $i\in\{1,\dots,m\}$, $\mathcal{Y}_a\in\tilde{\mathbb{D}}_i$ and $\bar{\rho}\in G_{36}$ such that $\pi_\alpha(\mathcal{C}(\alpha))^{\bar{\rho}}=\mathcal{Y}_\alpha$. Choose $\rho\in\eta_\alpha^{-1}(\overline{\rho})$. Then it is easy to observe that

- $\pi_\beta(\mathcal{C}^\rho(\beta))$ is a self-dual $[36,18,8]$ code;
- $\langle\chi,\mu\rangle\leq\mathrm{Aut}(\pi_\beta(\mathcal{C}^\rho(\beta)))$ (since $\rho\in G$);
- $(\pi_\beta(\mathcal{C}^\rho(\beta)))(\chi)=(\pi_\alpha(\mathcal{C}^\rho(\alpha)))(\chi)=\mathcal{E}_i$ (as in (3.3)).

Now, $\{(\mathcal{Y}_\beta)^\tau \mid \mathcal{Y}_\beta\in\tilde{\mathbb{D}}_i,\ \tau\in \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle\chi,\mu\rangle)\}$ is the set of all possible such codes, so $(\pi_\beta(\mathcal{C}^\rho(\beta)))(\chi)$ is one of these codes. □

Remark 3.17. *There are, up to equivalence in the full symmetric group S_{72}, only 22 codes in $\bigcup_{i=1}^{m}\mathbb{D}_{(\alpha,\beta)_i}$ such that the minimum distance is at least 16, say $\mathcal{D}_1,\dots,\mathcal{D}_{22}$. They are all $[72,26,16]$ codes. In particular*

$$\dim(\mathcal{D}_i(\alpha)\cap\mathcal{D}_i(\beta))=10.$$

Corollary 3.2. *The code $\mathcal{C}(\alpha)+\mathcal{C}(\beta)$ is equivalent, via the action of the full symmetric group S_{72}, to a code $\mathcal{D}_i$, with $i\in\{1,\dots,22\}$.*

We can repeat in a completely analogous way all the procedure for the pairs (α,γ) and (β,γ), interchanging the roles of the elements α,β and γ. Then we get the following.

Corollary 3.3. *The codes $\mathcal{C}(\alpha)+\mathcal{C}(\gamma)$ and $\mathcal{C}(\beta)+\mathcal{C}(\gamma)$ are equivalent, via the action of the full symmetric group S_{72}, to some codes $\mathcal{D}_j$ and $\mathcal{D}_k$, with $j,k\in\{1,\dots,22\}$.*

This implies that

$$\dim(\mathcal{C}(\alpha)\cap\mathcal{C}(\gamma))=10\quad\text{and}\quad\dim(\mathcal{C}(\beta)\cap\mathcal{C}(\gamma))=10. \tag{3.4}$$

Furthermore, by MAGMA calculations we get that

$$\dim(\mathcal{C}(\alpha) \cap \mathcal{C}(\beta) \cap \mathcal{C}(\gamma)) = 5. \tag{3.5}$$

Both statements can be verified by taking all the elements α', β', γ' of order 2 and degree 72 in $\mathrm{Aut}(\mathcal{D}_i)$ such that $\langle \alpha', \beta', \gamma' \rangle$ is conjugate to $\langle \alpha, \beta, \gamma \rangle$ in S_{72}.

To get a contradiction it is now enough to observe that (3.4) and (3.5) are not compatible with the Table 3.1. So we have the thesis of Theorem 3.6.

3.6 Conclusion

Putting together all the results of these sections, we get the following theorem, which summarize the actual state of art on the problem of the automorphism group of a putative extremal self-dual binary linear code of length 72.

Theorem 3.8 (Pless, Conway, Thompson, Huffman, Yorgov, Bouyuklieva, O'Brien, Willems, Yankov, Feulner, Nebe, Borello, Dalla Volta)**.**

Let $\mathcal{C}$ be self-dual $[72, 36, 16]$ *code. Then* $\mathrm{Aut}(\mathcal{C})$ *is trivial or it is isomorphic to one of the following:*

- *Order 2:* C_2*;*
- *Order 3:* C_3*;*
- *Order 4:* C_4 *or* $C_2 \times C_2$*;*
- *Order 5:* C_5*.*

Remark 3.18. *When this dissertation was already under review a preprint by Vassil I. Yorgov and Daniel Yorgov* [64] *on the subject appeared. In this paper they claim that the automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain elements of order* 4*. We presented our result about the*

dihedral group of order 8*, since the methods are interesting in any case and, even if our result is weaker, the computations are much faster. In a recent preprint* [6] *we review the current state of research in the light of the result of the Yorgovs.*

As one can see, the possible groups are abelian and very small, so that the putative code has very few symmetries. We can say that it is "almost rigid". This does not prove its non-existence. However, if such code does exist, it would be very difficult to find it, at least with methods related to automorphisms.

The following question remains open.

Question 3.1. *Is a putative extremal self-dual binary linear code of length* 72 *rigid (i.e. with trivial automorphism group)?*

In case of a positive answer to Question 3.1, it would be still possible, of course, that the code exists. However, a classical module-theoretical approach would be useless in this case. The surveys [23] and [35] suggest some ideas for a different approach to the problem. In any case, the following question is still completely open.

Question 3.2. *How can we prove that an extremal self-dual binary linear code of length* 72 *does exist or not?*

CHAPTER 4

Some results on extremal self-dual binary linear codes of other jump lengths

In this short chapter we present some results on automorphism groups of extremal self-dual binary linear codes of jump lengths greater than 72, which are investigated a bit in literature. We focus in particular on the case of length 120, which is quite extensively studied. Our aim is mainly to show that the methods of Chapter 2, thought to approach the case 72, may be applied to many other codes.

It should be possible to deepen more the study of such cases, but this is beyond the aim of this dissertation. Let us just mention that, to investigate the automorphism groups of extremal self-dual binary linear codes of a certain length with our methods, we need a classification of codes of smaller lengths, as we saw for example in Proposition 3.3. The actual state of the research is often not advanced enough.

4.1 Structure of automorphisms of prime order

In Chapter 3 we pointed out the following result by Bouyuklieva: all the possible involutions in the automorphism group of a self-dual $[72, 36, 16]$ code are fixed point free. Her result however is more general. In fact she proved the following theorem.

Theorem 4.1 ([13]). *Let $\mathcal{C}$ be a self-dual $[24m, 12m, 4m + 4]$ code and $\sigma_2 \in \mathrm{Aut}(\mathcal{C})$ of type 2-(c, f). Then*

- *$(c, f) = (8, 8)$ or $(c, f) = (12, 0)$, if $m = 1$;*
- *$(c, f) = (48, 24)$ or $(c, f) = (60, 0)$, if $m = 5$;*
- *$f = 0$, otherwise.*

It is well-known that the automorphism group of the extended binary Golay code (length 24) contains involutions with fixed points. In all the other cases the involutions are fixed point free, except, maybe, for $m = 5$. It is natural to ask the following.

Question 4.1. *Are the automorphisms of order 2 of a self-dual $[120, 60, 24]$ code fixed point free?*

If we look at the automorphisms of odd prime order, no general strong result is known.

However, we get some partial results using the methods of Chapter 2.

Firstly, we reduce the possible orders and types of automorphisms, just applying Theorem 2.2. In Table 4.1 we show which odd prime orders satisfies the conditions of the theorem for some self-dual $[24m, 12m, 4m + 4]$ codes.

We observe that the table could be refined with other methods. For example, a significant classification result about extremal extended cyclic codes contained in the Ph.D thesis [39] of Anton Malevich (Theorem 2.4.14.) implies that the primes in bold of the above table can be excluded.

In the following section we focus on the case of length 120.

Table 4.1: Automorphisms of odd prime order in jump lengths

parameters	possible odd prime orders by Theorem 2.2
$[96, 48, 20]$	3, 5, 7, 11, 23, 31, 47
$[120, 60, 24]$	3, 5, 7, 11, 17, 19, 23, 29, 59
$[144, 72, 28]$	3, 5, 7, 11, 17, 23, 47, 71
$[168, 84, 32]$	3, 5, 7, 11, 13, 23, 41, 83, **167**
$[192, 96, 36]$	3, 5, 7, 11, 13, 17, 19, 23, 31, 47, **191**
$[216, 108, 40]$	3, 5, 7, 11, 13, 17, 23, 53, 71, 107
$[240, 120, 44]$	3, 5, 7, 11, 13, 17, 19, 23, 29, 47, 59, 79, **239**
...	...
$[2400, 1200, 404]$	3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 59, 79, 109, 149, 199, 239, 479, 599, **2399**
...	...

4.2 Automorphisms of order $2p$ of the putative self-dual $[120, 60, 24]$ code

In this section we show an application of the methods contained in Section 2.3 to the putative extremal self-dual binary linear code of length 120.

From now on, let $\mathcal{C}$ be a self-dual $[120, 60, 24]$ code.

Next theorem gives the most recent results about the cycle structure of the automorphisms of $\mathcal{C}$.

Theorem 4.2 ([21]). *Let $\sigma \in \mathrm{Aut}(\mathcal{C})$. Then*

a) *if σ has order 2, then it is of type 2-$(48, 24)$ or 2-$(60, 0)$;*

b) *if σ has odd prime order, then it is of type 3-$(40, 0)$, 5-$(24, 0)$, 7-$(17, 1)$, 19-$(6, 6)$, 23-$(5, 5)$ or 29-$(4, 4)$;*

c) *if σ has odd composite order, then it is of type $3 \cdot$ 5-$(0, 0, 8; 0)$, $3 \cdot$ 19-$(2, 0, 2; 0)$ or $5 \cdot$ 23-$(1, 0, 1; 0)$.*

The even composite orders are not considered in Theorem 4.2. So it is natural to ask what is the cycle structure of an element $\sigma_{2p} \in \mathrm{Aut}(C)$ of order $2p$, where p is an odd prime.

Statement a) of Theorem 4.2 affirms that the involution $\sigma_2 := \sigma_{2p}^p$ has no or exactly 24 fixed points. The following result gives the possible cycle structure of σ_{2p} in both cases.

Lemma 4.1. *If the involution σ_2 has no fixed points, then σ_{2p} is of type*

- $2 \cdot 29\text{-}(2, 0, 2; 0)$,
- $2 \cdot 19\text{-}(3, 0, 3; 0)$,
- $2 \cdot 5\text{-}(0, 0, 12; 0)$,
- *or* $2 \cdot 3\text{-}(0, 0, 20; 0)$.

If σ_2 has 24 fixed points then σ_{2p} is of type

- $2 \cdot 23\text{-}(2, 1, 2; 1)$,
- *or* $2 \cdot 3\text{-}(0, 8, 16; 0)$.

Note that $\mathrm{Aut}(\mathcal{C})$ *does not contain elements of order* $2 \cdot 7$.

Proof. The proof is straightforward by considering the possible cycle structures of σ_{2p}^p and of σ_{2p}^2 given in Theorem 4.2. □

The above Lemma shows that σ_{2p} satisfies the hypothesis of Corollary 2.3 if and only if $p = 19$. In this case we have

$$\dim \mathcal{C}(\sigma_2) \geq \frac{120}{4} + \frac{19 - 1}{2} = 39$$

so that $\pi_{\sigma_2}(C(\sigma_2))$ is a $[60, \geq 39, \geq 12]$ code. According to Grassl's list [26] a binary linear code of length 60 and dimension greater than or equal to 39 has minimum distance at most 10. This proves the following.

Theorem 4.3. *The automorphism group of a self-dual* $[120, 60, 24]$ *code does not contain elements of order* 38.

The situation is slightly more complicated for the possible automorphism σ_{58} of order 58. By Lemma 4.1, we know that σ_{58} is of type $2 \cdot 29$-$(2, 0, 2; 0)$. Therefore $\sigma_{29} := \sigma_{58}^2$ is of type 29-$(4, 4)$ and $\sigma_2 := {\sigma_{58}}^{29}$ is of type 2-$(60, 0)$. Thus, without loss of generality, we may assume that

$$\sigma_{29} = (1, \ldots, 29)(30, \ldots, 58)(59, \ldots, 87)(88, \ldots, 116)$$

and

$$\sigma_2 = (1, 30) \ldots (59, 88) \ldots (117, 118)(119, 120).$$

If $\pi_{\sigma_{29}} : \mathcal{C}(\sigma_{29}) \to \mathbb{F}_2^8$ is the usual projection, the code $\pi_{\sigma_{29}}(\mathcal{C}(\sigma_{29}))$ is a self-dual binary linear code of length 8, according to Theorem 2.1, and its minimum distance must be greater than or equal to 4, since $\mathcal{C}$ is doubly-even and of minimum distance 24. It is well-known that, up to equivalence, the only code with such parameters is the extended Hamming code $\hat{\mathcal{H}}_3$.

Let $K := \mathbb{F}_2$. According to Remark 1.3, the structure of K^{120} as a $K\langle\sigma_{58}\rangle$-module is

$$K^{120} = \begin{matrix} K & K & K & K \\ K & K & K & K \end{matrix} \oplus \begin{matrix} V & V \\ V & V \end{matrix}$$

where V is an irreducible module of dimension 28. Since $\mathcal{C}(\sigma_{29})$ has dimension 4, the code $\mathcal{C}(\sigma_{58}) = (\mathcal{C}(\sigma_{29}))(\sigma_2)$ has dimension at least 2.

Let $\hat{\mathcal{H}}_3^{\mathcal{S}_8}$ be the set of all self-dual $[8, 4, 4]$ codes. By direct calculations with MAGMA we verify that

$$\dim((\pi_{\sigma_{29}}^{-1}(\mathcal{A}))(\sigma_{58})) \leq 2$$

for every $\mathcal{A} \in \hat{\mathcal{H}}_3^{\mathcal{S}_8}$. Note that $|\hat{\mathcal{H}}_3^{\mathcal{S}_8}| = \frac{|\mathcal{S}_8|}{|\mathrm{Aut}(\hat{\mathcal{H}}_3)|} = 30$. Thus $\dim \mathcal{C}(\sigma_{58}) = 2$ and the possible structures for $\mathcal{C}$ are only

a) $\mathcal{C} = \begin{matrix} K & K \\ K & K \end{matrix} \oplus V \oplus V$ or

b) $\mathcal{C} = \begin{matrix} K & K \\ K & K \end{matrix} \oplus \begin{matrix} V \\ V \end{matrix}$.

Next we look at $\mathcal{C}(\sigma_2)$. Obviously $\mathcal{B} := \pi_{\sigma_2}(\mathcal{B})$ is a $[60, \geq 30, \geq 12]$ code. In case a) we have $\dim \mathcal{B} = 58$, a contradiction.
We are left with the case b).
According to Theorem 2.6, $\mathcal{C}$ is projective and $\mathcal{B}$ is a self-dual $[60, 30, 12]$ code. Furthermore $\mathcal{B}$ has an automorphism of type 29-$(2, 2)$. We have the following result (for the definition of bordered double-circulant see, for example, [29]).

Proposition 4.1. *Every self-dual* $[60, 30, 12]$ *code* $\mathcal{B}$ *with an automorphism of type* 29-$(2, 2)$ *is bordered double-circulant. There are* (*up to equivalence*) *three such codes.*

Proof. We can easily determine the submodule of $\mathcal{B}$ fixed by the given automorphism. Then we investigate its complement in K^{60} through an exhaustive search with MAGMA (following the methods described in Section 2.2 and considering the complement as a vector space over $\mathbb{F}_{2^{28}}$). It turns out that $\mathcal{B}$ is equivalent to one of the three bordered double-circulant even codes of length 60 classified by Harada, Gulliver and Kaneta in [29]. □

It is computationally easy to check that there are exactly 14 conjugacy classes of elements of type 29-$(2, 2)$ in $\mathrm{Aut}(\mathcal{B})$ for each of the three possiblities for $\mathcal{B}$.

Using this we are able to do an exhaustive search for $\mathcal{C}$ along the methods introduced in Section 3.2. Without repeating all the details, we just recall the two main steps of the search.

First we determine a set, say $\mathbb{L}$, such that there exists a permutation $\tau \in \mathrm{C}_{\mathcal{S}_{120}}(\sigma_{58})$ and $\mathcal{L} \in \mathbb{L}$ such that $(\mathcal{C}(\sigma_2) + \mathcal{C}(\sigma_{29}))^\tau = \mathcal{L}$. It turns out that $|\mathbb{L}| = 42$. In the second step, as in Section 3.2, we construct all possible codes with socle $\mathcal{L}(\sigma_2')$, with $\mathcal{L} \in \mathbb{L}$ and σ_2' varying in all representatives of conjugacy classes of fixed point free elements of order 2 in $\mathrm{Aut}(\mathcal{L})$. Checking the minimum distance we see no code is extremal. This proves the following.

Theorem 4.4. *The automorphism group of a self-dual* $[120, 60, 24]$ *code does not contain elements of order* 58.

Bouyuklieva, Willems and De la Cruz recentely used these results in [14], where they investigate carefully the structure of the whole automorphism group of $\mathcal{C}$.

As in the general case, also for length 120 the following question is still open.

Question 4.2. *Can we say something more on the automorphism group of a self-dual* $[120, 60, 24]$ *code using the methods of Chapter 2?*

CHAPTER 5

New bounds for semi self-dual codes

In Chapter 2 we posed Question 2.1 about the self-duality of the natural projection of fixed codes by involutions. In this chapter, which is a presentation of some results obtained with Gabriele Nebe during a visit to RTWH Aachen, we give a partial answer to the question. To do this, we introduce a new class of codes of even length - the semi self-dual codes - and we prove some bounds for the minimum distance of their dual.

Definition 5.1. *Let $n \geq 4$ even. We call $\mathcal{D} \leq \mathbb{F}_2^n$* semi self-dual code *if*

- *$\mathcal{D}$ is self-orthogonal;*
- $\dim\mathcal{D} = \frac{n}{2} - 1$*;*
- $\mathbf{1} \in \mathcal{D}$*.*

It follows directly from the definition that for $\mathcal{D}$ semi self-dual code we have

$$\langle \mathbf{1} \rangle \leq \mathcal{D} < \mathcal{D}^{\perp} \leq \langle \mathbf{1} \rangle^{\perp} < \mathbb{F}_2^n,$$

where $\langle \mathbf{1} \rangle$ is the 1-dimensional code generated by $\mathbf{1}$ and $\langle \mathbf{1} \rangle^\perp$, its dual, is the set of all even weight vectors.

We want to determine an upper bound for $\mathrm{d}(\mathcal{D}^\perp)$.

5.1 Main Result

Theorem 1.7 gives easily a bound for the minimum distance of the dual of a semi self-dual code: let $\mathcal{D}$ a semi self-dual code and set $\mathcal{D} < \mathcal{F} = \mathcal{F}^\perp < \mathcal{D}^\perp$ an intermediate self-dual code. Then

$$\mathrm{d}(\mathcal{D}^\perp) \leq \mathrm{d}(\mathcal{F}) \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{if } n \equiv 22 \bmod 24 \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{otherwise.} \end{cases} \tag{5.1}$$

We improve this bound, proving the following.

Theorem 5.1. *Let $\mathcal{D} \leq \mathbb{F}_2^n$ ($n \geq 4$ even) a semi self-dual code. Then*

$$\mathrm{d}(\mathcal{D}^\perp) \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 2 & \text{if } n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \bmod 24, \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & \text{if } n \equiv 16, 18, 20 \bmod 24, \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & \text{if } n \equiv 22 \bmod 24. \end{cases}$$

Furthermore, if $n \equiv 0 \bmod 24$ and $\mathcal{D}$ doubly-even,

$$\mathrm{d}(\mathcal{D}^\perp) \leq 4\left\lfloor \frac{n}{24} \right\rfloor.$$

By direct calculations with Magma, using a database [44] of all self-dual binary linear codes of length up to 40, we get the following.

Remark 5.1. *There exist semi self-dual codes such that their dual codes have parameters* $[4, 3, 2]$, $[6, 4, 2]$, $[8, 5, 2]$, $[10, 6, 2]$, $[12, 7, 2]$, $[14, 8, 2]$, $[16, 9, 4]$, $[18, 10, 4]$, $[20, 11, 4]$ *and* $[22, 11, 6]$.
So the bound is reached for $n \equiv 4, 6, 8, 10, 12, 14, 16, 18, 20, 22 \bmod 24$.

There exists a semi self-dual code with dual code of parameters $[24, 13, 4]$ *code with doubly-even dual code.*
So the bound is reached for $n \equiv 0 \bmod 24$ in the doubly-even case.

Question 5.1. *Semi self-dual codes with dual codes of parameters* $[24, 13, 6]$ *and* $[26, 14, 6]$ *do not exist.*
Is it possible to improve the bound for $n \equiv 0, 2 \bmod 24$*?*

The proof of this theorem is divided into two parts. For reader's convenience we will state two different propositions and we will prove them separately. Theorem 5.1 will be a direct consequence of them.

Before stating and proving the propositions, let us show some strong consequences of Theorem 5.1.

Corollary 5.1. *Let* $\mathcal{C}$ *be a self-dual* $[24m, 12m, 4m + 4]$ *code, with* m *odd, and let* σ_2 *be fixed point free automorphism of order* 2*. Then* $\pi_{\sigma_2}(\mathcal{C}(\sigma_2))$ *is an extremal self-dual* $[12m, 6m, 2m + 2]$ *code. In particular* $\mathcal{C}$ *is a free* $\mathbb{F}_2\langle\sigma_2\rangle$*-module.*

Proof. By [11] there exists a subcode $\mathcal{E} \leq \pi_{\sigma_2}(\mathcal{C}(\sigma_2)) \leq \mathbb{F}_2^{12m}$ such that

$$\mathcal{E} \leq \mathcal{E}^\perp = \pi_{\sigma_2}(\mathcal{C}(\sigma_2)). \tag{5.2}$$

Since $\mathcal{C}$ is doubly-even, $\mathcal{E}^\perp \leq \langle \mathbf{1} \rangle^\perp$.

If the equality holds in (5.2), then the thesis is proved. Suppose, on the contrary, that $\mathcal{E} < \mathcal{E}^\perp$. Then there exists $\mathcal{D}$ of dimension $6m - 1$ such that

$$\langle \mathbf{1} \rangle \leq \mathcal{E} \leq \mathcal{D} < \mathcal{D}^\perp \leq \mathcal{E}^\perp \leq \langle \mathbf{1} \rangle^\perp.$$

Clearly $\mathrm{d}(\mathcal{E}^\perp) \geq \frac{\mathrm{d}(\mathcal{C})}{2}$. So $\mathcal{D}^\perp$ has parameters $[12m, 6m + 1, \geq 2m + 2]$.

Let $n = 12m$. If m is odd, then $m = 2\left\lfloor \frac{n}{24} \right\rfloor + 1$. Furthermore $n \equiv 12 \bmod 24$.

Then $\mathcal{D}^\perp$ has parameters $[n, \frac{n}{2} + 1, \geq 4\left\lfloor \frac{n}{24} \right\rfloor + 4]$, a contradiction with the bounds in Theorem 5.1. □

Remark 5.2. *Theorem 3.1 in* [45] *affirms that the natural projection of the fixed code by an involution in an extremal self-dual binary linear code of length* 72 *is self-dual. The proof is based on the classification of self-dual* $[36, 18, 8]$ *codes. Corollary* 5.1 *gives a direct proof of that result, without classification.*

We have an easy consequence for the cycle-structure of automorphism of order $2p$ of extremal self-dual binary linear codes of jump lengths.

Corollary 5.2. *Let $\mathcal{C}$ be a self-dual $[24m, 12m, 4m+4]$ code with m odd. Suppose that $\sigma_{2p} \in \mathrm{Aut}(\mathcal{C})$ is an automorphism of type $2 \cdot p\text{-}(w, 0, x; 0)$ with $\mathrm{s}(p)$ even. Then w is even.*

Proof. It follows directly by Corollary 2.3 and Corollary 5.1. □

Remark 5.3. *Corollary* 5.2 *gives a new direct proof of Theorem* 4.3 *of Chapter* 4.

Let us conclude this section with few considerations related to Question 2.1.

Corollary 5.1 gives a positive answer in the case of m odd. Unfortunately it is not enough to repeat the same arguments if m is even. Actually, if m is even the lower bound for $\mathrm{d}(\mathcal{D}^{\perp})$ is compatible with the upper bound given in Theorem 5.1. Anyway we could not find a counterexample and the problem is still open.

Let us underline that there exist extremal doubly-even self-dual binary linear codes of parameters $[8, 4, 4]$, $[16, 8, 4]$, $[32, 16, 8]$ and $[40, 20, 8]$ for which the natural projections of fixed codes of fixed point free involutions are not self-dual.

5.2 Proof of Theorem 5.1

From now on let $\mathcal{D}$ be a semi self-dual code of length $n \geq 4$, even. Furthermore, let $\mu = \left\lfloor \frac{n}{24} \right\rfloor$.

Proposition 5.1. *If $\mathcal{D}$ is doubly-even, then*

$$d(\mathcal{D}^{\perp}) \leq \begin{cases} 4\mu & \text{if } n \equiv 0 \bmod 24 \\ 4\mu + 2 & \text{if } n \equiv 4, 8, 12 \bmod 24 \\ 4\mu + 4 & \text{if } n \equiv 16, 20 \bmod 24 \end{cases}$$

Proof. Since every doubly-even binary linear code is self-orthogonal, $\mathcal{D}^\perp$ cannot be doubly-even and so in $\mathcal{D}^\perp$ there exists a codeword of weight $w \equiv 2 \bmod 4$. Thus we can take $\mathcal{D} < \mathcal{F} = \mathcal{F}^\perp < \mathcal{D}^\perp$ with $\mathcal{F}$ not doubly-even, so that $\mathcal{D} = \mathcal{F}_0$ (i.e. the maximal doubly-even subcode of $\mathcal{F}$ introduced in Theorem 1.2).

Let $\mathcal{S} := \mathcal{D}^\perp - \mathcal{F}$. By [4],

$$2\mathrm{d}(\mathcal{F}) + \mathrm{d}(\mathcal{S}) \leq 4 + \frac{n}{2}. \tag{5.3}$$

Note that $\mathrm{d}(\mathcal{D}^\perp) = \min\{\mathrm{d}(\mathcal{F}), \mathrm{d}(\mathcal{S})\}$, since $\mathcal{D}^\perp = \mathcal{S} \cup \mathcal{F}$. Since we have the bound (5.3), the maximum for $\min\{\mathrm{d}(\mathcal{F}), \mathrm{d}(\mathcal{S}\}$ is reached if

$$\mathrm{d}(\mathcal{D}^\perp) = \mathrm{d}(\mathcal{F}) = \mathrm{d}(\mathcal{S}) = \left\lfloor \frac{4 + \frac{n}{2}}{3} \right\rfloor$$

so that

$$\mathrm{d}(\mathcal{D}^\perp) \leq \left\lfloor \frac{8+n}{6} \right\rfloor,$$

which is the same bound in the thesis, remembering that $\mathrm{d}(\mathcal{D}^\perp)$ is even. □

Furthermore, it holds the following.

Proposition 5.2. *If $\mathcal{D}$ is not doubly even, then*

$$\mathrm{d}(\mathcal{D}^\perp) \leq \begin{cases} 4\mu + 2 & \text{if } n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \bmod 24 \\ 4\mu + 4 & \text{if } n \equiv 16, 18, 20, 22 \bmod 24 \end{cases}$$

Before proving it we need to introduce some notations, objects and to prove a lemma. Most of the proof is inspired and motivated by [54].

Let us define the following:

- $N := \frac{n}{2}$;
- $A(x, y) := \sum_{i=0}^{N} a_i x^{2N-2i} y^{2i}$ weight enumerator of $\mathcal{D}$;
- $D(x, y) := A(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) = \sum_{i=0}^{N} d_i x^{2N-2i} y^{2i}$, so that $2D$ is the weight enumerator of $\mathcal{D}^\perp$;

- $B(x,y) := A(x,y) - D(x,y) = \sum_{i=0}^{N} b_i x^{2N-2i} y^{2i}$;
- $F(x,y) := B\left(\frac{x+y}{\sqrt{2}}, i\frac{x-y}{\sqrt{2}}\right)$.

The polynomial $B(x,y)$ is anti-invariant under the MacWilliams transformation:

$$B\left(\tfrac{x+y}{\sqrt{2}}, \tfrac{x-y}{\sqrt{2}}\right) = A\left(\tfrac{x+y}{\sqrt{2}}, \tfrac{x-y}{\sqrt{2}}\right) - D(\tfrac{x+y}{\sqrt{2}}, \tfrac{x-y}{\sqrt{2}}) = D(x,y) - A(x,y) = -B(x,y).$$

The following holds for anti-invariant polynomials under the MacWilliams transformation.

Lemma 5.1. *The set of all anti-invariants polynomials under the MacWilliams transformation is*

$$\mathbb{A} := (x - (\sqrt{2}+1)y) \cdot \mathbb{C}[x + (\sqrt{2}-1)y, x^2 + 2xy - y^2].$$

Proof. It is easy to prove, with arguments similar to those of Section 1.6, that

$$\mathbb{C}[x + (\sqrt{2}-1)y, x^2 + 2xy - y^2]$$

is the set of all polynomials which are invariant under the MacWilliams transformation. Since $x - (\sqrt{2}+1)y$ is anti-invariant, all polynomials in $\mathbb{A}$ are anti-invariant.

Vice versa, let $a(x,y)$ be an anti-invariant polynomial. We have that

$$a((\sqrt{2}+1)y, y) = -a\left(\frac{(\sqrt{2}+1)y + y}{\sqrt{2}}, \frac{(\sqrt{2}+1)y - y}{\sqrt{2}}\right) = -a((\sqrt{2}+1)y, y),$$

so that $a((\sqrt{2}+1)y, y) = 0$. Thus $a(x,y)$ is divisible by $x - (\sqrt{2}+1)y$. Finally, their quotient is obviously an invariant polynomial. □

Thus $B(x,y) \in \mathbb{A}$. Furthermore, $B(x,y)$ is invariant for the transformation $I := x \mapsto -x$; i.e. it has only even powers of x (and y).

Let $\mathbb{A}^I$ the set of all polynomials in $\mathbb{A}$ invariant under I and $\mathbb{A}^I_d$ the subset of $\mathbb{A}^I$ of polynomials of degree d. Clearly $\mathbb{A}^I_0 = \mathbb{C}$ and $\mathbb{A}^I_d = \emptyset$ for all odd d. Furthermore $\mathbb{A}^I_2 = \emptyset$. Finally it is easy to prove that

$$(x^4 - 6x^2y^2 + y^4) = (x - (\sqrt{2}+1)y)(x + (\sqrt{2}-1)y)(x^2 + 2xy - y^2)$$

divides every polynomial in $\mathbb{A}^I$ and, as before, the quotient is invariant both under MacWilliams transformation and under I. Thus we get the following.

Lemma 5.2. *Let*

- $p(x,y) := (x^4 - 6x^2y^2 + y^4)$,
- $f_0(x,y) := x^2 + y^2$,
- $f_1(x,y) := x^2y^2(x^2 - y^2)^2$.

Then

$$\mathbb{A}^I = p(x,y) \cdot \mathbb{C}[f_0(x,y), f_1(x,y)].$$

Since $B(x,y) \in \mathbb{A}^I$, we can write

$$B(x,y) = (x^4 - 6x^2y^2 + y^4) \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} e_i (x^2+y^2)^{N-2-4i} (x^2y^2(x^2-y^2)^2)^i \quad (5.4)$$

and, consequently,

$$F(x,y) = 2(x^4+y^4) \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} e_i (2xy)^{N-2-4i} \left(-\frac{1}{4}x^8 + \frac{1}{2}x^4y^4 - \frac{1}{4}y^8 \right)^i. \quad (5.5)$$

Notice that (5.5) implies that the degrees of the monomials of $F(x,y)$ are congruent to $N-2$ modulo 4.

The following lemma insures us that $F(x,y)$ has nonnegative integer coefficients.

Lemma 5.3. *$F(x,y)$ is the weight enumerator of a coset in $\mathcal{D}_0^\perp/\mathcal{D}$, so that its coefficients are integers and nonnegative.*

Proof. Recall that $\langle \mathbf{1} \rangle < \mathcal{D} < \mathcal{D}^\perp < \langle \mathbf{1} \rangle^\perp < \mathbb{F}_2^{2N}$ with $\dim \mathcal{D} = N-1$. There are exactly 3 self-dual binary linear codes, say $\mathcal{C}_1, \mathcal{C}_2$ and $\mathcal{C}_3$, which contains $\mathcal{D}$ (since $\dim \mathcal{D}^\perp/\mathcal{D} = 2$). Notice that it holds

$$\mathcal{D}^\perp = \mathcal{C}_1 \sqcup (\mathcal{C}_2 \setminus \mathcal{D}) \sqcup (\mathcal{C}_3 \setminus \mathcal{D}).$$

This implies that

$$2A(x,y)+2D(x,y) = 2W_{\mathcal{D}}(x,y)+W_{\mathcal{D}^\perp}(x,y) = W_{\mathcal{C}_1}(x,y)+W_{\mathcal{C}_2}(x,y)+W_{\mathcal{C}_3}(x,y)$$

so that

$$2F(x,y) = (4A-(2A+2D))\left(\frac{x+y}{2}, i\frac{x-y}{2}\right) =$$

$$2W_{\mathcal{D}_0^\perp\setminus\mathcal{D}^\perp}(x,y) - \sum_{i=1}^{3} W_{\mathcal{C}_{i,0}^\perp\setminus\mathcal{C}_i}(x,y).$$

Consider $\mathcal{D}_0^\perp/\mathcal{D} \cong \mathbb{F}_2^3$. We choose a basis v_1, v_2, v_3 of $\mathcal{D}_0^\perp/\mathcal{D}$ such that $\mathcal{D}^\perp/\mathcal{D} = \langle v_1, v_2\rangle$, $\mathcal{C}_1/\mathcal{D} = \langle v_1\rangle$, $\mathcal{C}_2/\mathcal{D} = \langle v_2\rangle$, $\mathcal{C}_3/\mathcal{D} = \langle v_1+v_2\rangle$. So

$$\begin{aligned}
\mathcal{D}_0^\perp \setminus \mathcal{D}^\perp &= \{v_3, v_1+v_3, v_2+v_3, v_1+v_2+v_3\};\\
\mathcal{C}_{1,0}^\perp \setminus \mathcal{C}_1 &= \{v_3, v_1+v_3\};\\
\mathcal{C}_{2,0}^\perp \setminus \mathcal{C}_2 &= \{v_3, v_2+v_3\};\\
\mathcal{C}_{3,0}^\perp \setminus \mathcal{C}_3 &= \{v_1+v_3, v_2+v_3\}.
\end{aligned}$$

So

$$F(x,y) = W_{v_1+v_2+v_3}(x,y),$$

where $W_{a+\mathcal{D}}(x,y) := \sum_{c\in\mathcal{D}} x^{2N-\mathrm{wt}(a+c)}y^{\mathrm{wt}(a+c)}$.

□

Then we get the following.

Corollary 5.3. *Let* $\{e_i\}$ *be as in* (5.4) *and* (5.5). *Then* $e_i \cdot e_{i-1} \le 0$ *for every* i, $1 \le i \le \lfloor \frac{N-2}{4} \rfloor$.

Proof. We have

$$F(1,y) = (1+y^4)y^{N-2} \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_i y^{-4i}(1-y^4)^{2i}.$$

with $\epsilon_i := (-1)^i 2^{N-1-6i} e_i$. Substitute $\lfloor \frac{N-2}{4} \rfloor - i = h$.

$$F(1,y) = y^{N-2-4\lfloor \frac{N-2}{4} \rfloor}(1+y^4)(1-y^4)^{2\lfloor \frac{N-2}{4} \rfloor} \cdot \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_{\lfloor \frac{N-2}{4} \rfloor - h}(y^4(1-y^4)^{-2})^h.$$

Let $r := N - 2 - 4\lfloor \frac{N-2}{4} \rfloor$. Note that

$$r = \begin{cases} 2 & \text{if } N \equiv 0 \bmod 4 \\ 3 & \text{if } N \equiv 1 \bmod 4 \\ 0 & \text{if } N \equiv 2 \bmod 4 \\ 1 & \text{if } N \equiv 3 \bmod 4 \end{cases}$$

$$\begin{aligned} F(1,y) &= \textstyle\sum_{j=0}^{2N} f_j y^j = f_0 + \ldots + f_{r-1} y^{r-1} + y^r \sum_{j=r}^{2N} f_j y^{j-r} = \\ &= y^r (1+y^4)(1-y^4)^{2\lfloor \frac{N-2}{4} \rfloor} \cdot \textstyle\sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} (y^4 (1-y^4)^{-2})^h. \end{aligned}$$

Then $f_j = 0$ if $j \not\equiv r \bmod 4$. Set $j = 4k + r$ and $Z = y^4$. Then

$$\sum_k f_{4k+r} Z^k = (1+Z)(1-Z)^{2\lfloor \frac{N-2}{4} \rfloor} \cdot \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} (Z(1-Z)^{-2})^h.$$

Put

$$f(Z) := (1+Z)^{-1}(1-Z)^{-2\lfloor \frac{N-2}{4} \rfloor}, \quad g(Z) := Z(1-Z)^{-2}.$$

Find coefficient $\gamma_{h,k}$ such that

$$Z^k f(Z) = \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \gamma_{h,k} g(Z)^h$$

Clearly $\gamma_{h,k} = 0$ if $h < k$ ($g(Z)$ has a zero of order 1 in 0). Then

$$\epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} = \sum_{4k+r \le h} \gamma_{h,k} f_{4k+r}.$$

Since $g(0) = 0$ and $g'(0) \neq 0$, we can apply Bürmann-Lagrange theorem, in the version of Lemma 8 [54]

$$\gamma_{h,k} = [\text{coeff. of } Z^{h-k} \text{ in } (1-Z)^{-1-2\lfloor \frac{N-2}{4} \rfloor + 2h}]$$

Note that $-1 - 2\left\lfloor \frac{N-2}{4} \right\rfloor + 2h$ is negative, for every h ($h \le \left\lfloor \frac{N-2}{4} \right\rfloor$), so $(1-Z)^{-1-2\lfloor \frac{N-2}{4} \rfloor + 2h}$ is a power of the geometric series. Thus $\gamma_{h,k}$ is always nonnegative.

So

$$\epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} = \sum_{4k+r \le h} \gamma_{h,k} f_{4k+r} \ge 0.$$

Now,

$$e_i = (-1)^i 2^{6i} \epsilon_i.$$

This implies that $e_i \cdot e_{i+1} \leq 0$ for all i. □

We can finally prove the proposition.

Proof of Proposition 5.2. We have that

$$\begin{aligned} B(1,Y) &= 1/2 + \textstyle\sum_{j=d}^{N-d} b_j Y^j + 1/2 Y^N = \\ &= (1-6Y+Y^2)(1+Y)^{N-2} \textstyle\sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} e_i (Y(1-Y)^2(1+Y)^{-4})^i \end{aligned}$$

Let

$$f(Y) := (1-6Y+Y^2)^{-1}(1+Y)^{2-N}, \qquad g(Y) := Y(1-Y)^2(1+Y)^{-4}.$$

Find coefficient $\alpha_i(N)$ such that

$$f(Y) = \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} \alpha_i(N) g(Y)^i.$$

Then, for $i < d$,

$$e_i = \frac{1}{2}\alpha_i(N).$$

Since $g(0) = 0$ and $g'(0) \neq 0$, we can apply Bürmann-Lagrange theorem, in the version of Lemma 8, Rains,

$$\alpha_i(N) = [\text{coeff. of } Y^i \text{ in } (1+Y)^{1-N+4i}(1-Y)^{-2i-1}]$$

that is

$$\frac{1}{i!}\left(\frac{d^i}{dY^i}(1+Y)^{1-N+4i}(1-Y)^{-2i-1}\right)(0)$$

so that

$$\alpha_i(N) = \sum_{a=0}^{i} (-1)^a \binom{N-2-4i+a}{a} \binom{3i-a}{i-a}.$$

Let $N = 12m + q$.

Case $q = 0, 1, 2, 3, 5, 6, 7$. Let $d > 2m + 1$. Then,

$$e_{2m} \cdot e_{2m+1} = \frac{1}{4}\, \alpha_{2m}(12m + q) \cdot \alpha_{2m+1}(12m + q) > 0$$

by direct calculations (and the previous are nonpositives). A contradiction with Corollary 5.3. So $d \leq 2m + 1$.

Case $q = 8, 9, 10, 11$. Let $d > 2m + 3$. Then

$$e_{2m+2} \cdot e_{2m+3} = \frac{1}{4}\, \alpha_{2m+2}(12m + q) \cdot \alpha_{2m+3}(12m + q) > 0.$$

by direct calculations (and the previous are nonpositives). A contradiction. So $d \leq 2m + 3$. In this case the bound is weaker than (or equal to) (5.1). □

APPENDIX A

Times of computation

In this very short appendix we collect some details about the computations. In the following website all the main MAGMA programs of the dissertation are available:
`sites.google.com/a/campus.unimib.it/mborello/programs`
The machines we used are the following:

- Machine A: Intel(R) Xeon(R) CPU X5460 (3.16GHz)
- Machine B: Core i7 870 (2.93GHz)

In Tables A.1 and A.2 the CPU times of the computations for the self-dual $[72, 36, 16]$ code and for the self-dual $[120, 60, 24]$ code respectively are collected. A product $a \cdot b$ means that the computations were split into a jobs, each of about b CPU time.

Table A.1: Times of main computations (case 72)

Case	CPU time	Machine
C_6	182 hours	A
$\mathcal{S}_3$	7 minutes	A
$\mathcal{A}_4$	26 hours	A
$\mathcal{A}_4$	$10 \cdot 7,5$ hours	B
D_8	9 minutes	A
$C_2 \times C_2 \times C_2$	307 hours	A

Table A.2: Times of main computations (case 120)

Case	CPU time	Machine
C_{58}	2 minutes	A
C_{58}	$42 \cdot 65$ hours	A

Bibliography

[1] R.P. Anstee, M. Hall and J.G. Thompson. *Planes of order* 10 *do not have a collineation of order* 5. Journal of Combinatorial Theory, Series A 29 (1): 39–58, 1980.

[2] E. F. Assmuss and H.F. Mattson. *New* 5*-designs*. Journal of Combinatorial Theory 6 (2): 122–151, 1969.

[3] E.F. Assmus, H.F. Mattson and R.J. Turyn. *Research to develop the algebraic theory of codes*. Air Force Cambridge Res. Labs., Belford, MA, Report AFCRL-67-0365, 1967.

[4] C. Bachoc and P. Gaborit. *Designs and self-dual codes with long shadows*. Journal of Combinatorial Theory, Series A 105 (1): 15–34, 2004.

[5] H.U. Besche, B. Eick and E.A. O'Brien. *A millennium project: Constructing small groups*. Int. J. Algebra Comput. 12: 623–644, 2002.

[6] M. Borello. *On the automorphism groups of binary linear codes*. arXiv preprint arXiv:1311.3868, 2013.

[7] M. Borello. *The automorphism group of a self-dual* $[72, 36, 16]$ *binary code does not contain elements of order* 6. IEEE Transactions on Information Theory 58 (12): 7240–7245, 2012.

[8] 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: 1–7, 2014.

[9] M. Borello, F. Dalla Volta and G. Nebe, *The automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain* $\mathcal{S}_3$, $\mathcal{A}_4$ *or* D_8. Advances in Mathematics of Communications 7 (4): 503–510, 2013.

[10] M. Borello and W. Willems. *Automorphisms of order* $2p$ *in binary self-dual extremal codes of length a multiple of* 24. IEEE Transactions on Information Theory 59 (6): 3378–3383, 2013.

[11] S. Bouyuklieva. *A method for constructing self-dual codes with an automorphism of order* 2. IEEE Transactions on Information Theory 46 (2): 496–504, 2000.

[12] S. Bouyuklieva. *On the automorphism group of a doubly even* $(72, 36, 16)$ *code*, IEEE Transactions on Information Theory 50 (3): 544–547, 2004.

[13] S. Bouyuklieva. *On the automorphisms of order* 2 *with fixed points for the extremal self-dual codes of length* $24m$. Des. Codes Cryptogr. 25: 5–13, 2002.

[14] S. Bouyuklieva, J. De la Cruz and W. Willems. *On the automorphism group of a binary self-dual* $[120, 60, 24]$ *code*. Applicable Algebra in Engineering, Communication and Computing 24 (3-4): 201–214, 2013.

[15] S. Bouyuklieva, A. Malevich and W. Willems. *Automorphisms of extremal self-dual codes*. IEEE Transactions on Information Theory 56 (5): 2091–2096, 2010.

[16] S. Bouyuklieva, E.A. O'Brien and W. Willems. *The Automorphism Group of a Binary Self-Dual Doubly Even* $[72, 36, 16]$ *Code is Solvable.* IEEE Transactions on Information Theory 52 (9): 4244–4248, 2006.

[17] W. Bosma, J. Cannon and C. Playoust. *The* Magma *algebra system* I*: The user language.* J. Symbol. Comput. 24: 235–265, 1997.

[18] J.H. Conway and V. Pless. *On primes dividing the group order of a doubly-even* $(72; 36; 16)$ *code and the group order of a quaternary* $(24; 12; 10)$ *code.* Discrete Mathematics 38: 143–156, 1982.

[19] C.W. Curtis and I. Reiner. *Methods of representation theory with applications to finite groups and orders.* Vol. I, Wiley Classics Library, 1990.

[20] L.E. Danielsen and M.G. Parker. *On the Classification of All Self-Dual Additive Codes over* $GF(4)$ *of length up to* 12. Journal of Combinatorial Theory, Series A 112 (7): 1351–1367, 2006.

[21] J. de la Cruz. *Über die Automorphismengruppe extremaler Codes der Längen* 96 *und* 120. PhD thesis (OVGU Magdeburg), 2012.

[22] R. Dontcheva, A.J.V. Zanten, S. Dodunekov. *Binary self-dual codes with automorphism of composite order.* IEEE Transactions on Information Theory 50 (2): 311–318, 2004.

[23] S.T. Dougherty. *The Search for the* $[24k, 12k, 4k + 4]$ *Extremal Type II Code.* Online available at `http://dl.dropboxusercontent.com/u/20879623/survey.pdf`, 2011.

[24] T. Feulner and G. Nebe. *The automorphism group of an extremal* $[72, 36, 16]$ *code does not contain* Z_7*,* $Z_3 \times Z_3$*, or* D_{10}. IEEE Transactions on Information Theory 58 (11): 6916–6924, 2012.

[25] A.M. Gleason. *Weight polynomials of self-dual codes and MacWilliams identies.* 1970 Actes Congrés Internl. de Mathematique 3: 211–215, 1971.

[26] M. Grassl. *Bounds on the minimum distance of linear codes and quantum codes*. Online available at `www.codetables.de` , accessed on 2012-09-15.

[27] J.H. Griesmer. *A bound for error-correcting codes*. IBM Journal of Res. and Dev. 4 (5): 532–542, 1960.

[28] A. Günther and G. Nebe. *Automorphisms of doubly even self-dual binary codes*. Bulletin of the London Mathematical Society 41 (5): 769–778, 2009.

[29] M. Harada, T.A. Gulliver and H. Kaneta. *Classification of extremal double-circulant self-dual codes of length up to* 62, Discrete Mathematics 188: 127–136, 1998.

[30] S. K. Houghten, C. W. H. Lam, L. H. Thiel, and J. A. Parker. *The extended quadratic residue code is the only* $(48, 24, 12)$ *self-dual doubly-even code*. IEEE Transactions on Information Theory, 49 (1): 53–59, 2003.

[31] W.C. Huffman. *Automorphisms of codes with application to extremal doubly even codes of length* 48. IEEE Transactions on Information Theory 28 (3): 511–521, 1982.

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

[33] W.C. Huffman and V. Yorgov. *A* $[72, 36, 16]$ *doubly even code does not have an automorphism of order* 11. IEEE Transactions on Information Theory 33 (5): 749–752, 1987.

[34] B. Huppert and N. Blackburn. *Finite Groups II*. Springer, 1982.

[35] Jon-Lark Kim. *A Prize Problem in Coding Theory*. Online available at `www.math.louisville.edu/∼jlkim/jlkim07.pdf`

[36] J. MacWilliams. *A theorem on the distribution of weights in a systematic code*. Bell Syst. Tech. J 42 (1): 79–94, 1963.

[37] J. MacWilliams. *Combinatorial problems of elementary abelian groups*. Ph.D Thesis (Harvard University), 1962.

[38] J. MacWilliams and N. Sloane. *The Theory of Error-correcting Codes*. Vol. 16. Elsevier, 1977.

[39] A. Malevich. *Extremal self-dual codes*. Ph.D Thesis (OVGU Magdeburg), 2012.

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

[41] C. Martínez-Pérez and W. Willems. *Self-dual codes and modules of finite groups in characteristic two*. IEEE Transactions on Information Theory 50 (8): 67–78, 2004.

[42] C.A. Mechor and P. Gaborit. *On the classification of extremal* $[36, 18, 8]$ *binary self-dual codes*. IEEE Transactions on Information Theory 54 (10): 4743–4750, 2008.

[43] T. Molien. *Über die Invarianten der linearen Substitutionsgruppen*. Sitzungber. König. Preuss. Akad. Wiss. (J. Berl. Ber.) 52: 1152–1156, 1897.

[44] A. Munemasa. *Database of Binary Self-dual Codes*. Online available at `www.math.is.tohoku.ac.jp/ munemasa/research/codes/sd2.htm`

[45] G. Nebe. *An extremal* $[72, 36, 16]$ *binary code has no automorphism group containing* $\mathbb{Z}_2 \times \mathbb{Z}_4$, Q_8, *or* $\mathbb{Z}_{10}$. Finite Fields and their applications 18 (3): 563–566, 2012.

[46] G. Nebe, E.M. Rains and N.J.A. Sloane. *Self-dual codes and invariant theory*. Vol. 17, Springer, 2006.

[47] E.A. O'Brien and W. Willems. *On the automorphism group of a binary self-dual doubly-even* $[72, 36, 16]$ *code*. IEEE Transactions of Information Theory 57 (7): 4445–4451, 2011.

[48] V. Pless and J. Thompson. 17 *does not divide the order of the group of a* $(72, 36, 16)$ *doubly even code*. IEEE Transactions on Information Theory 28 (3): 537–541, 1982.

[49] V. Pless. 23 *does not divide the order of the group of a* $(72, 36, 16)$ *doubly even code*. IEEE Transactions on Information Theory 28 (1): 113–117, 1982.

[50] V. Pless. *A classification of self-orthogonal codes over* $\mathbb{F}_2$. Discrete Mathematics 3 (1): 209–246, 1972.

[51] V. Pless. *On the uniqueness of the Golay codes*. Journal of Combinatorial Theory, 5: 215–228, 1968.

[52] V. Pless, N. Sloane and H. Ward. *Ternary codes of minimum weight* 6 *and the classification of the self-dual codes of length* 20. IEEE Transactions on Information Theory 26 (3): 305–316, 1980.

[53] E.M. Rains and N.J.A. Sloane. *Self Dual Codes*. In Handbook of Coding Theory, Eds V. Pless et al., North-Holland, Amsterdam: 177–294, 1998.

[54] E.M. Rains. *Shadow bounds for self-dual codes*, IEEE Transactions on Information Theory 44 (1): 134–139, 1998.

[55] S. Zhang. *On the nonexistence of extremal self-dual codes*. Discrete applied mathematics 91 (1): 277–286, 1999.

[56] R.C. Singleton. *Maximum distance q-nary codes*. IEEE Transactions on Information Theory 10 (2): 116–118, 1964.

[57] N.J.A. Sloane. *Binary codes, lattices, and sphere-packings*, "Combinatorial Surveys" edited P.J. Cameron, Academic Press, NY: 117–164, 1977.

[58] N.J.A. Sloane. *Is there a* $(72; 36)$ $d = 16$ *self-dual code?*. IEEE Transactions on Information Theory 19 (2): 251, 1973.

[59] N.J.A. Sloane and J.G. Thompson. *Cyclic Self-Dual Codes*. IEEE Transactions on Information Theory 29 (3): 364–366, 1983.

[60] W. Willems. *A note on self-dual group codes*. IEEE Transactions on Information Theory 48 (12): 3107–3109, 2002.

[61] N. Yankov. *A putative doubly even* $[72, 36, 16]$ *code does not have an automorphism of order* 9. IEEE Transactions on Information Theory 58 (1): 159–163, 2012.

[62] V.I. Yorgov. *Binary self-dual codes with automorphisms of odd order*. Problemy Peredachi Informatsii 19 (4): 11-24, 1983.

[63] V.I. Yorgov. *On the automorphism Group of a putative code*. IEEE Transactions on Information Theory 52 (4): 1724–1726, 2006.

[64] V.I. Yorgov and D. Yorgov. *The Automorphism Group of a Self Dual Binary* $[72, 36, 16]$ *Code Does Not Contain* Z_4. arXiv preprint arXiv:1310.2570, 2013.

Index