Extremal self-dual codes

Dissertation

zur Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von Dipl.-Math. Anton Malevich

geb. am 07.02.1986 in Minsk

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg.

Gutachter: Prof. Dr. Wolfgang Willems
Prof. Dr. Patric R.J. Östergård

eingereicht am: 04.06.2012

Verteidigung am: 22.10.2012

Abstract

In the present thesis we consider extremal self-dual codes. We mainly concentrate on Type II codes (binary doubly-even codes), which may theoretically exist for lengths $n = 8k \leq 3928$. It is noteworthy that extremal Type II codes have been actually constructed only for 13 lengths, 136 being the largest. Over the last decades the study of extremal codes became inseparable from the study of their automorphisms. For example, one of the few methods to construct a new "good" code C is to assume that C is invariant under a certain automorphism and to use the restrictions imposed by this fact.

Making use of the non-trivial automorphism groups we classify extremal extended quadratic residue codes and quadratic double circulant codes. The two families provide examples of extremal codes for 9 of the 13 lengths, for which extremal codes are constructed.

Another of our main results is the classification of extremal Type II codes C with 2-transitive automorphism groups. We show that C is either a quadratic residue code, a Reed-Muller code, or a putative code of length 1024. Similar classification results are also obtained in case of ternary and quaternary extremal codes.

In the thesis we also provide a new easy-to-handle criterion to determine possible cycle structures of the automorphisms of binary extremal codes. Using this result we show that a binary extremal code of length n with an automorphism of prime order $p > \frac{n}{2}$ is equivalent to an extended cyclic code. We classify extremal extended cyclic codes of length $n \leq 1000$. Moreover, we prove that for all but 11 values of $n > 1000$ no extremal extended cyclic code can exist.

In the final part of the thesis we consider singly-even and doubly-even binary extremal codes in terms of their decoding performance. We are able to determine the best singly-even codes and prove that these always perform better than doubly-even codes with the same parameters.

Zusammenfassung

In der vorliegenden Arbeit untersuchen wir extremale selbstduale Codes. Hauptsächlich konzentrieren wir uns auf Typ II Codes (d.h., binäre doppeltgerade Codes), welche theoretisch für Längen $n = 8k \leq 3928$ für ganzzalige k existieren können. Es ist bemerkenswert, dass extremale Typ II Codes eigentlich nur für 13 Längen konstruiert sind, wobei 136 die größte ist. Über die letzten Jahrzehnte ist die Untesuchung der extremalen Codes fast unzertrennlich von der Untersuchung zugehöriger Automorphismen geworden. So besteht zum Beispiel eine der wenigen Methoden zur Konstruktion eines neuen Codes C darin, die Invarianz von C unter einem konkreten Automorphismus anzunehmen und die daraus folgenden Beschränkungen auszunutzen.

Unter Verwendung der nicht trivialen Automorphismengruppen klassifizieren wir sowohl die extremalen erweiterten quadratischen Restklassen-Codes, als auch die extremalen quadratischen doppelt zirkulanten Codes. Diese beiden Familien liefern Beispiele der extremalen Codes für 9 von den 13 Längen.

Zu den zentralen Ergebnissen der Arbeit gehört weiterhin die Klassifikation der extremalen Typ II Codes C mit 2-fach transitiven Automorphismengruppen. Wir beweisen, dass C entweder ein quadratischer Restklassen-Code, ein Reed-Muller-Code, oder ein möglicher Code der Länge 1024 ist. Ähnliche Klassifikationssätze erhalten wir auch für die ternären und quaternären extremalen Codes.

In der Dissertation stellen wir ein neues Kriterium bereit, mit dem man leicht die möglichen Zyklen-Strukturen der Automorphismen der binären extremalen Codes bestimmen kann. Mithilfe dieses Kriteriums zeigen wir, dass ein binärer extremaler Code der Länge n mit einem Automorphismus der Ordnung $p > \frac{n}{2}$, wobei p eine Primzahl ist, äquivalent zu einem erweiterten zyklischen Code ist. Wir klassifizieren die erweiterten zyklischen Codes der Länge $n \leq 1000$. Außerdem beweisen wir, dass für alle bis auf 11 Werte von $n > 1000$ kein extremaler erweiterter zyklischer Code existiert.

Im letzten Teil der Arbeit betrachten wir einfach- und doppeltgerade binäre extremale Codes bezüglich deren Dekodierenleistung. Wir bestimmen die besten einfachgeraden Codes und beweisen, dass diese immer leistungfähiger als die doppeltgeraden Codes mit denselben Parametern sind.

Contents

Introduction **9**

1 Preliminaries **13**
1.1 Extremal self-dual codes 13
1.2 Automorphism groups, group algebras 18
1.3 Cyclic and duadic codes 21
1.4 Weight enumerators of self-dual codes 25

2 Automorphisms of extremal codes **31**
2.1 Known extremal Type II codes and their automorphisms 31
2.2 Types of automorphisms of binary extremal codes 35
2.3 Extremal Type II codes arising from quadratic residues 37
2.4 Extremal Type II extended cyclic codes 42
2.5 Automorphism groups of binary extended duadic codes 49
2.6 Extremal binary affine-invariant codes 50
2.7 Extremal Type II codes and elementary abelian groups 54
2.8 Extremal Type II codes with 2-transitive automorphism groups . . 57
2.9 Extremal Type III codes with 2-transitive automorphism groups . . 60
2.10 Extremal Type IV codes with 2-transitive automorphism groups . . 62

3 Performance of self-dual codes **65**
3.1 A way to measure performance of codes 65
3.2 Performance of known extremal binary codes 67
3.3 Best performing extremal Type I codes 68
3.4 Performance comparison of extemal Type I and Type II codes . . . 71

A Code of Magma programs **73**

Bibliography **79**

Index **87**

List of Tables

2.1 Primes that can occur as a factor of the automorphism group order for some extremal Type II code 33
2.2 Simple groups that can occur as a socle of a 2-transitive group . . . 59

3.1 Number of minimum weight codewords in binary extremal codes 68

List of Listings

A.1 Program for Example 2.3.9 73
A.2 Program for Example 2.3.10 73
A.3 Program for Example 2.3.16 74
A.4 Program for Example 2.4.16 74
A.5 Program for Remark 2.6.9. Case $n = 512$ 75
A.6 Program for Example 2.7.4 76
A.7 Program for Example 2.8.4 76
A.8 Program for Example 2.9.2 77
A.9 Program for Example 2.10.2 78

Introduction

The theory of linear codes is a relatively new subject in mathematics. The first two papers by Golay [31] and Hamming [34] were published in 1949 and 1950, respectively. In these papers it was described how k-tuples, which represent digital messages, may be embedded in an n-dimensional space, where $k \leq n$, such that the highest possible number of errors can be corrected.

An $[n, k, d]$ *linear code* C is a k-dimensional subspace of a vector space $\mathbb{F}^n$ over a finite field $\mathbb{F}$. The dimension n of the ambient space is called the *length* of C. The parameter d stands for the smallest positive weight among the codewords and is called the *minimum distance* of the code. Here the *weight* of a codeword is the number of its nonzero coordinates. It was shown in [34] that the minimum distance d is a measurement of how many errors in the information may be corrected, if the code is used for data transmission. Thus, of particular interest are codes that attain the highest possible minimum distance for given k and n.

In the present work we concentrate on *self-dual codes*, i.e., codes that are equal to their duals with respect to a given scalar product on $\mathbb{F}^n$. For these codes the dimension k equals $\frac{n}{2}$. Self-dual codes are important mainly due to connections to invariant theory and the theory of block designs. Self-dual codes, for which the weight of every codeword is divisible by some integer greater than one, are called *divisible*. There are four types of divisible codes. Codes of Type II are binary self-dual codes with all weights divisible by 4. Type I codes are binary self-dual codes with at least one codeword of weight 2 modulo 4. Codes of Type III are ternary codes with all weights divisible by 3. Finally, a Type IV code is a code over $\mathbb{F}_4$, which is self-dual with respect to the Hermitian scalar product, such that all weights are divisible by 2.

A self-dual divisible code is called *extremal* if its minimum distance attains the highest possible value. For instance, for Type II codes we have $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$, and the code is extremal if the equality holds. Notable examples of extremal Type II codes are the $[8, 4, 4]$ and $[24, 12, 8]$ codes defined in the aforementioned papers by Hamming and Golay, respectively. Examples of extremal Type II codes were constructed for a total of 13 lengths, the highest being 136. However, it was proven that extremal codes can not exist for arbitrarily large lengths. In particular, for codes of Types II, III, and IV the explicit upper bounds of the length of an extremal code were given. The best known bound for Type II codes is especially large with $n \leq 3928$. Thus, we see that there is a huge gap between what is actually constructed and what can theoretically exist. Unfortunately, the problem of closing or reducing the gap appears to be extremely difficult, as the known methods (see [85] and [27]) produce the same upper bound, and no extremal code of length greater than 136 has been constructed.

In the thesis we do not try to attack the gap in general. Instead we classify extremal codes with some additional properties. On the one hand, we consider codes that arise from some special constructions, e.g., quadratic residue and quadratic double circulant codes. Our main results in this area include the following two theorems.

Theorem 2.3.8. *Let C be an extremal extended quadratic residue code of length n. Then* $n = 8, 24, 32, 48, 80,$ *or* 104.

Theorem 2.3.15. *Let C be an extremal quadratic double circulant code of length n. Then* $n = 8, 24, 40, 88,$ *or* 136.

On the other hand, we study codes with prescribed *automorphisms*, i.e., permutations of the n coordinate positions that leave a code invariant. One of our main results is the following classification of extremal codes with 2-transitive automorphism groups.

Theorem 2.8.1. *Let C be an extremal Type II code of length n. If* $\mathrm{Aut}(C)$ *is 2-transitive, then one of the following holds.*

(i) $n = 8, 24, 32, 48, 80,$ *or* 104, *and C is equivalent to an extended quadratic residue code,*

(ii) $n = 32$ *and up to equivalence C is the second order Reed-Muller code,*

(iii) possibly $n = 1024$ *and C is invariant under the group* $T \rtimes \mathrm{SL}(2, 2^5)$, *where T is the group of translations of the vector space* $\mathbb{F}_2^{10}$.

Another question that we touch upon in the present work is the following: Which type of binary extremal codes does perform better, if codes are used for information transmission? Both Type I and Type II codes of length $n \equiv 8$ or $16 \bmod 24$ share the same parameters. We compare their *performance* using a result of Faldum et al. [28]. We are able to determine the best performing extremal Type I codes (these are so-called *s-extremal* codes) and prove the following result.

Theorem 3.4.1.

(i) Extremal Type I codes with minimal shadow perform better than extremal Type II codes for lengths $n = 24m + 8$. *In particular, s-extremal codes perform better than extremal Type II codes.*

(ii) s-extremal Type I codes perform better than extremal Type II codes for lengths $n = 24m + 16$.

Below we give an overview of the thesis.

In **Chapter 1** we introduce the notation and definitions used throughout the work. In the first section we define the setting. The next two sections list the facts that are later used in Chapter 2. Finally, in Section 1.4 we gather the definitions and results that are important for Chapter 3.

The main part of the thesis consists of two independent chapters.

In **Chapter 2** we consider automorphism of extremal codes. More precisely, we study if extremal codes may exist under certain assumptions about the automorphism group. We mainly focus on Type II codes in this chapter, though in the last two sections we apply the methods developed for Type II codes to codes of Types III and IV.

In Section 2.1 we give an overview of the known extremal Type II codes. We also give a historical survey of how the study of putative extremal codes of lengths 72, 96, and 120 progressed over the last 30 years. In this section we also pay particular attention to the families of codes that provide several examples of extremal codes.

In Section 2.2 we study the possible cycle structures of the automorphisms of extremal Type II codes. We provide a new easy-to-handle result, which, in particular, allows us to show that a putative extremal code with an automorphism of prime order greater than $\frac{n}{2}$ is equivalent to an extended cyclic code.

We completely classify extremal Type II codes that arise from quadratic residues in Section 2.3. These codes generalize the $[8,4,4]$ Hamming and the $[24,12,8]$ Golay codes in two possible ways and provide examples of extremal Type II codes for 9 of 13 lengths, for which extremal codes have been constructed. We also describe an algorithm that we use to effectively search for small weight codewords, which is applied in the proof of some of our results.

In the next section we generalize our approach to extended quadratic residue codes from Section 2.3 to the general case of extended cyclic codes. We decribe a method to construct all cyclic codes of prime length $p \equiv -1 \bmod 8$ with self-dual extensions and provide a tool to determine the inequivalent ones. In Section 2.4 we also start a classification of extremal extended cyclic codes, where we list all extremal extended cyclic codes of length less than 1000. Moreover, we prove that for all but 11 lengths greater than 1000 no extremal extended cyclic code can exist.

In Section 2.5 we discuss when the automorphism group of an extended cyclic code can be 2-transitive. We notice that in order to classify extremal extended cyclic codes with 2-transitive groups it only remains to consider so-called *affine-invariant* codes. We classify these in Section 2.6 using a method by Charpin and Levy-dit-Vehel [17].

Sections 2.5 and 2.6 serve as a preparation for the classification of extremal Type II codes with 2-transitive groups. We generalize the approach of Section 2.6

to a more general case of codes invariant under extensions of elementary abelian groups in Section 2.7. The central point of our method is to consider a code as a module for the automorphism group. In Section 2.8 we consider extremal codes with 2-transitive simple groups, thus completing the classification of extremal Type II codes with 2-transitive automorphism groups. The method is then used in Sections 2.9 and 2.10 to classify extremal Type III and Type IV codes with 2-transitive permutation automorphism group.

The classification results in Chapter 2 rely in part on computer calculations. These are carried out with MAGMA [5] and explained in numerous examples throughout the chapter. The source code of MAGMA programs for the examples is listed in Appendix A.

In **Chapter 3** we compare extremal codes of Types I and II with respect to their performance. We use a result of [28] to define performance in terms of *weight distribution* in Section 3.1. In Section 3.2 we consider known extremal codes and discuss, which type of codes might be expected to perform better. Extremal Type II codes all have the same weight distribution, and therefore they all share the same quality of performance. However, this is not the case for extremal Type I codes. In Section 3.3 we prove that so-called *s-extremal* codes are the best performing among them. We then proceed to compare *s*-extremal (and some other Type I codes) to Type II codes in Section 3.4. We prove that certain Type I codes always perform better than any Type II codes, provided they are of the same length.

Acknowledgments

First of all, I would like to express my deep gratitude to my supervisor, Wolfgang Willems, for his guidance and inspiration, which made this thesis possible in the first place. I wish to thank Stefka Bouyuklieva and Iliya Bouyukliev for the numerous fruitful conversations, which improved my understanding of coding theory and had direct influence on my work. Additionally, I would like to thank Patric Östergård for agreeing to review the current thesis.

I am further grateful to my colleges for the good office atmosphere and their help on many occasions. In particular, I would like to thank Ralph August for all his advises, which made adapting to life in Germany much easier.

For the most welcome weekly distractions I wish to thank our "Fußballtruppe".

I am deeply grateful to my parents: to my father, for nurturing my love for mathematics, and to my mother, for her confidence in me.

Finally, and most importantly, I want to thank my best friend and my wife, Nadja, for everything, especially for helping me cope with even the most stressful moments.

Chapter 1

Preliminaries

The aim of this chapter is to introduce the notation and notions used throughout the thesis. In Section 1.1 the setting is defined and the basic concept of an extremal self-dual code is introduced. It will be the main object of interest in the work. In Section 1.2 we describe the connections between codes and group algebras. There we give a description of a code as a module for the automorphism group. Cyclic codes are described in detail in Section 1.3. The final section of the chapter is devoted to weight enumerators and some techniques to handle them.

For a more thorough discussion of these topics we refer the reader to one of the books [41], [57], or [69].

1.1 Extremal self-dual codes

Let $\mathbb{F}_q^n$ denote the n-dimensional linear space over a field $\mathbb{F}_q$ with q elements. A *linear code* C is a subspace of $\mathbb{F}_q^n$. The dimension n of the ambient space $\mathbb{F}_q^n$ is called the *length* of C. A vector $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is called a *codeword* and the number

$$\mathrm{wt}(c) = |\{i \,|\, 0 \leq i \leq n-1,\ c_i \neq 0\}|$$

is called the *weight* of c. The smallest positive weight in the code C is called the *minimum distance*. The use of the word *distance* is explained by the following fact. The function $\mathrm{dist} : \mathbb{F}_q^n \to \mathbb{N}_0$ defined by $\mathrm{dist}(x,y) = \mathrm{wt}(x-y)$ for $x, y \in \mathbb{F}_q^n$ is a metric on $\mathbb{F}_q^n$. For a linear code C we have

$$\min_{x,y \in C} \mathrm{dist}(x,y) = \min_{x \in C} \mathrm{dist}(x,0) = \min_{x \in C} \mathrm{wt}(x),$$

since by linearity $x - y \in C$ as long as $x, y \in C$.

A k-dimensional code of length n over $\mathbb{F}_q$ with minimum distance d will be referred to as an $[n,k,d]_q$ code. We omit the subscript q if the underlying field is clear from the context.

Let C be an $[n,k,d]_q$ code and let $v_1,\dots,v_k$, where $v_i = (v_{i,0}, v_{i,1} \dots, v_{i,n-1}) \in \mathbb{F}_q^n$ for all $1 \le i \le k$, be its $\mathbb{F}_q$-basis. A $(k \times n)$-matrix

$$G = \begin{pmatrix} v_{1,0} & v_{1,1} & \cdots & v_{1,n-1} \\ v_{2,0} & v_{2,1} & \cdots & v_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k,0} & v_{k,1} & \cdots & v_{k,n-1} \end{pmatrix},$$

which contains the basis vectors $v_1,\dots,v_k$ as rows, is called the generator matrix of the code C. One can *extend* the code C by adding a coordinate. The *extended* code, denoted by $\widehat{C}$, is an $[n+1,k,d']$ code, where $d' = d$ or $d' = d+1$, and has a generator matrix

$$\widehat{G} = \begin{pmatrix} v_{1,0} & v_{1,1} & \cdots & v_{1,n-1} & v_{1,\infty} \\ v_{2,0} & v_{2,1} & \cdots & v_{2,n-1} & v_{2,\infty} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_{k,0} & v_{k,1} & \cdots & v_{k,n-1} & v_{k,\infty} \end{pmatrix},$$

where $v_{i,\infty}$ are chosen so that

$$v_{i,0} + v_{i,1} + \ldots + v_{i,n-1} + v_{i,\infty} = 0$$

for all $1 \le i \le k$. In general, a vector $x = (x_0,\dots,x_{n-1}) \in \mathbb{F}_q^n$ with the sum of its components equal to zero is called *even-like*. A code is called *even-like* if it has only even-like vectors; a code is *odd-like* if it is not even-like.

In case when the all-one vector $\mathbf{1} = (1,\dots,1) \in \mathbb{F}_q^n$ does not lie in the code C, the process of extending is often preceded by *augmenting* the code, i.e., adding $\mathbf{1}$ as the last row of the generator matrix. Augmenting the code, supplemented by extending, is referred to as *lengthening*. The inverse operation to the lengthening process is called *shortening*. Let T be a set of t coordinates and let $C(T)$ denote the set of all codewords of C which are zero on T. *Puncturing* $C(T)$ on T, i.e. removing the coordinates T from all vectors of $C(T)$, gives the *shortened* code C_T of length $n-t$.

Note that in the present work we denote the $k \times k$ identity matrix by I_k.

The ambient space $\mathbb{F}_q^n$ is endowed with a standard (Euclidean) scalar product $(.,.)$ given by

$$(x,y) = \sum_{i=0}^{n-1} x_i y_i \quad \text{for all } x,y \in \mathbb{F}_q^n.$$

If q is a square (say, $q = r^2$), instead of the standard we will consider the Hermitian scalar product

$$(u,w) = \sum_{i=0}^{n-1} u_i w_i^r \quad \text{for all } u,w \in \mathbb{F}_{r^2}^n.$$

(The map $x \mapsto x^r$, $x \in \mathbb{F}_{r^2}$, is called *global conjugation*. In the case, when r is a prime, e.g., $r = 2$, this map is usually referred to as *Frobenius automorphism*.)

For a linear code C of length n over $\mathbb{F}_q$ we define the *dual code* $C^\perp$ by

$$C^\perp = \left\{ v \in \mathbb{F}_q^n \,\middle|\, (v, c) = 0 \text{ for all } c \in C \right\}.$$

If $C \leq C^\perp$ we call C *self-orthogonal*. If $C = C^\perp$ we say that the code C is *self-dual*.

From linear algebra we know that $\dim C^\perp = n - \dim C$ for every linear code C. In particular, the length of a self-dual code is always even, and its dimension equals half of the length.

For small fields self-duality also imposes restrictions on possible weights of the codewords.

Example 1.1.1. Let C be a self-dual $\left[n, \frac{n}{2}, d\right]_q$ code, where $q = 2$, 3, or 4. For all $c \in C$ we have $(c, c) = 0$. In particular, for $q = 2, 3$ we get

$$0 = (c, c) = \sum_{i=0}^{n-1} c_i^2 = 1 \cdot |\{i \,|\, 0 \leq i \leq n-1,\, c_i \neq 0\}| \bmod q = \mathrm{wt}(c) \bmod q.$$

For $\mathbb{F}_4$ and the Hermitian scalar product we get

$$0 = (c, c) = \sum_{i=0}^{n-1} c_i^3 = 1 \cdot |\{i \,|\, 0 \leq i \leq n-1,\, c_i \neq 0\}| \bmod 2 = \mathrm{wt}(c) \bmod 2.$$

Thus, for self-dual codes over $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_4$ all weights are divisible by 2, 3, and 2, respectively.

In general, if for a code C there exists an integer $\Delta > 1$, such that $\Delta | \,\mathrm{wt}(c)$ for all $c \in C$, then C is said to be *divisible*. The largest integer Δ, for which the code C is divisible, is called the *divisor* of C.

All self-dual divisible codes over F_q are classified by the famous Gleason–Pierce Theorem.

Theorem 1.1.2 (Gleason–Pierce, see [77]). *Let C be a self-dual divisible code of length n over $\mathbb{F}_q$ with divisor Δ. Then one of the following holds true*

(i) $(q, \Delta) = (2, 2)$,

(ii) $(q, \Delta) = (2, 4)$,

(iii) $(q, \Delta) = (3, 3)$,

(iv) $(q, \Delta) = (4, 2)$,

(v) $\Delta = 2$ *and C is equivalent to the code over $\mathbb{F}_q$ with generator matrix* $[I_{n/2}\ I_{n/2}]$.

Remark 1.1.3. The codes appearing in case (v) of Theorem 1.1.2 are trivial and will be of no interest in this work.

In agreement with Theorem 1.1.2 and Example 1.1.1 we distinguish four *types* of codes over $\mathbb{F}_q$ with $q \leq 4$. E.g., a code C is said to be of Type II if it is self-dual, the underlying field is $\mathbb{F}_2$ and weights of all codewords are divisible by 4. For convenience, we set Type II $\not\subseteq$ Type I[1]. This means, we say that a code is of Type I if it is self-dual, binary, all its weights are divisible by 2 and it has at least one codeword of weight 2 mod 4. A ternary code is called a Type III code if it is self-dual and weights of all its codewords are divisible by 3. Finally, a Type IV code is a Hermitian self-dual code over $\mathbb{F}_4$ with all weights divisible by 2.

Traditionally binary divisible codes with $\Delta = 4$ are called doubly-even. Codes with $\Delta = 2$ and at least one codeword of weight 2 mod 4 are called singly-even.

For codes of Types II, III, and IV the generalization of Theorem 1.1.2, the so-called Gleason–Pierce–Ward Theorem, holds true.

Theorem 1.1.4 (Gleason–Pierce–Ward, see [41]). *Let C be a divisible $\left[n, \frac{n}{2}, d\right]_q$ code with divisor Δ and let $(q, \Delta) = (2,4)$, $(3,3)$, or $(4,2)$. Then C is self-dual.*

Below we give a combination of results by Mallows and Sloane [59], MacWilliams et al. [56] and Rains [70], which provides an upper bound on the minimum distance of divisible self-dual codes.

Theorem 1.1.5 ([59], [56], [70]). *Let C be a self-dual divisible $\left[n, \frac{n}{2}, d\right]_q$ code. Then*

$$\begin{aligned} d &\leq 4\left\lfloor \tfrac{n}{24} \right\rfloor + 4, && \text{if } C \text{ is of Type II or } C \text{ is Type I and } n \not\equiv 22 \bmod 24,\\ d &\leq 4\left\lfloor \tfrac{n}{24} \right\rfloor + 6, && \text{if } C \text{ is Type I and } n \equiv 22 \bmod 24,\\ d &\leq 3\left\lfloor \tfrac{n}{12} \right\rfloor + 3, && \text{if } C \text{ is of Type III},\\ d &\leq 2\left\lfloor \tfrac{n}{6} \right\rfloor + 2, && \text{if } C \text{ is of Type IV}. \end{aligned}$$

Remark 1.1.6. The bound for Type I codes of length $n \equiv 22 \bmod 24$ may be explained by the fact that they can be obtained by shortening Type II codes of length $n + 2$.

Self-dual codes that achieve the bound from Theorem 1.1.5 are called *extremal*.

Extremal codes are of particular interest not only because they have the largest possible minimum distance among self-dual codes. As a consequence of the famous theorem of Assmus and Mattson [1], the existence of an extremal code of Type II, III, or IV implies the existence of a t-design, where t can be as large as 5.

Definition 1.1.7. A *design* is a pair (X, B), where X is a non-empty finite set of v elements, called points, and B is a non-empty finite collection of k-subsets of X, called blocks, that satisfy the following property: every subset of points of size t is contained in exactly λ blocks. The pair (X, B) is also referred to as a t-(v, k, λ) design, or simply as a t-design.

[1] Some authors define Type II codes as a subset of Type I codes, see [72].

To describe designs associated with an extremal code, we define the support $\mathrm{supp}(c)$ of a codeword $c \in C$ as follows

$$\mathrm{supp}(c) = \{i \mid c_i \neq 0\}.$$

Then, the set $X = \{0, 1, \ldots, n-1\}$ of coordinate positions and the set

$$B = \{\mathrm{supp}(c) \mid c \in C,\, \mathrm{wt}(c) = i\}$$

of supports of all codewords with a given weight i form a t-(v, k, λ) design (see Theorem 1.1.8). Here, $v = n$, $k = i$ and λ is given by the formula

$$\lambda = A_i \binom{i}{t} \Big/ \binom{n}{t},$$

where A_i is the number of codewords of weight i in the code C.

Below we state the Assmus–Mattson theorem in the case of Type II codes.

Theorem 1.1.8 ([1], see also [41, Theorem 9.3.10]). *Let C be an extremal Type II code of length $n = 24m + 8\ell$ for $\ell = 0$, 1, or 2. Then codewords of any fixed weight except* 0 *and n hold t-desings for the following parameters:*

(i) $t = 5$ *if* $\ell = 0$ *and* $m \geq 1$,
(ii) $t = 3$ *if* $\ell = 1$ *and* $m \geq 0$, *and*
(iii) $t = 1$ *if* $\ell = 2$ *and* $m \geq 0$.

Remark 1.1.9. Similar results hold for extremal codes of Types III and IV.

Despite their importance, extremal codes of any Type can not exist for arbitrarily large lengths. Moreover, for Types II, III, and IV an explicit upper bound on the length of an extremal code is known.

Theorem 1.1.10 (Zhang [85]). *Let C be an extremal self-dual code of length n and of Type II or IV. Assume that n is divisible by* 8 *or* 2*, respectively. Then*

(a) Type II: $i < 154$ if $n = 24i$, $i < 159$ if $n = 24i + 8$ and $i < 164$ if $n = 24i + 16$. In particular C cannot exist for $n > 3928$.

(b) Type IV: $i < 17$ if $n = 6i$, $i < 20$ if $n = 6i + 2$ and $i < 22$ if $n = 6i + 4$. In particular C cannot exist for $n > 130$.

Theorem 1.1.11 (Zhang [85]). *Let C be an extremal self-dual code of Type III and length n. Then $n < 144$ and, moreover, $n \neq 72, 96, 120$.*

There is no explicit bound on the length of an extremal Type I code. In this case only an asymptotic bound is known.

Theorem 1.1.12 (Rains [71]). *Let C_i be a sequence of self-dual $\left[n_i, \frac{n_i}{2}, d_i\right]$ codes of Type I with $\lim\limits_{i\to\infty} n_i \to \infty$. Then*

$$\limsup_{i\to\infty} \frac{d_i}{n_i} \leq \frac{1 - 5^{-1/4}}{2} \approx 0.16563.$$

Corollary 1.1.13. *Let $(C_i)_{i\in\mathbb{N}}$ be a sequence of Type I codes of length $n_i = 24i + 2r$, where $0 \leq r \leq 11$. Then only finitely many of the codes C_i can be extremal.*

Proof. First note that by Theorem 1.4.6 extremal codes of Type I do not exist for lengths a multiple of 24.

Suppose that there is a subsequence $\left(C_{i_k}\right)_{k\in\mathbb{N}}$, such that all codes C_{i_k} are extremal. From Theorem 1.1.5 we know that the minimum distance d_{i_k} of C_{i_k} is equal to $4i_k + \varepsilon$, where $\varepsilon = 4$ if $1 \leq r \leq 10$ and $\varepsilon = 6$ if $r = 11$. Hence, we obtain

$$\limsup_{k\to\infty} \frac{d_{i_k}}{n_{i_k}} = \frac{4i_k + \varepsilon}{24i_k + 2r} = \frac{1}{6} > \frac{1 - 5^{-1/4}}{2},$$

a contradiction to Theorem 1.1.12. □

1.2 Automorphism groups, group algebras

The symmetric group S_n acts naturally on the space $\mathbb{F}_q^n$ and, hence, on a linear code C of length n by permuting the coordinate positions. Let us remark that throughout the entire work we denote the coordinates in $\mathbb{F}_q^n$ by $0, 1, \ldots, n-1$ and assume that S_n is acting on the set $\{0, 1, \ldots, n-1\}$ rather than $\{1, \ldots, n\}$. For a vector $x \in \mathbb{F}_q^n$ and a permutation $\sigma \in S_n$ we set

$$x\sigma = \left(x_{\sigma^{-1}(0)}, x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n-1)}\right). \tag{1.1}$$

Clearly, both the weight function and the scalar product (and thus the process of forming the dual code) are invariant under this action. However, apart from the binary case, we can consider other transformations that leave both the weight and the scalar product invariant. These are the monomial transformations (that is, permutations of the coordinates, followed by multiplication of the coordinates by nonzero elements) and, if the scalar product in question is Hermitian, global conjugation. Two codes are called *equivalent* if one can be obtained from the other by one of such transformations. The group of transformations that leaves a given code C invariant is called the (full) automorphism group of C and denoted $\mathrm{Aut}(C)$. Thus, for a binary code C we obtain

$$\mathrm{Aut}(C) = \{\sigma \in S_n \,|\, C\sigma = C\}.$$

Of particular interest in the thesis are codes with 2-transitive automorphism groups. We remind the reader that a group $G \leq S_n$ is called *transtitive* if for any two points there exists a permutation in G that maps one point onto the other. For a point $x \in \{0, 1, \ldots, n-1\}$ the *orbit* xG is defined by

$$xG = \{xg \,|\, g \in G\}.$$

The *stabilizer* G_x is a subgroup that consists of all permutations in G that fix x, i.e.,

$$G_x = \{ g \in G \,|\, xg = x \} .$$

A group G is called 2-*transitive* if for some point x the stabilizer G_x is transitive on the set $\{0, 1, \dots, n-1\} \setminus \{x\}$. Recursively one can define 3-transitive groups and so on.

Several times throughout the present work we use a couple of group theoretical facts about 2-transitive groups. For ease of reference we collect them in the following lemma.

Lemma 1.2.1 ([43]).

(i) Every 2-transitive group has a unique minimal normal subgroup, which is elementary abelian or simple.

(ii) A 2*-transitive group of degree q^m with a minimal normal elementary abelian subgroup T is isomorphic to a subgroup of* $\mathrm{AGL}(m, q)$*. Moreover T is isomorphic to the group of translations of the vector space $\mathbb{F}_q^m$, i.e., mappings of the form $v \mapsto v + a$, where $v, a \in \mathbb{F}_q^m$.*

(iii) Every 2*-transitive subgroup of* $\mathrm{AGL}(m, 2)$ *is an extension of an elementary abelian group T of order* 2^m *by a subgroup of* $\mathrm{GL}(m, 2)$*, which is transitive on* $2^m - 1$ *points.*

We call a unique minimal normal subgroup of a 2-transitive group the *socle* of the group. An *elementary abelian* group is a direct product of cyclic groups of the same prime order. A group is said to be *simple* if it does not have any nontrivial normal subgroups. We would like to remark that throughout the thesis we use standard notation and group names (see [47] or [22]). E.g., AGL stands for affine general linear group.

Let C be a linear code over $\mathbb{F}_q$ of length n and let $G \leq \mathrm{Aut}(C)$. If the action of G on C is defined by (1.1) then the code C becomes an $\mathbb{F}_qG$-module. Note that the ambient space $\mathbb{F}_q^n$ is also an $\mathbb{F}_qG$-module with respect to the same action of G. We formulate the fact that C is an $\mathbb{F}_qG$-module as the following statement.

Proposition 1.2.2. *Let C be an $[n, k, d]_q$ code and let $G \leq$ $\mathrm{Aut}(C)$. Then C is a k-dimensional submodule of the ambient space $\mathbb{F}_q^n$, considered as an $\mathbb{F}_qG$-module.*

In representation theory the *dual module* C^* of an $\mathbb{F}_qG$-module C is defined as the set of all $\mathbb{F}_q$-linear maps from C to $\mathbb{F}_q$, i.e., $C^* = \mathrm{Hom}_{\mathbb{F}_q}(C, \mathbb{F}_q)$. The dual module C^* becomes an $\mathbb{F}_qG$-module if we put

$$(fg)(c) = f(cg^{-1}) \text{ for } f \in C^*,\ g \in G \text{ and } c \in C.$$

As we already noted, the scalar product remains invariant under the action of the automorphism group, i.e., the following holds true

$$(xg, yg) = (x, y) \text{ for all } x, y \in C \text{ and } g \in G.$$

From this we can easily see that the dual code $C^{\perp}$ is also an $\mathbb{F}_q G$-module. Indeed, let $c \in C$, $c' \in C^{\perp}$, and $g \in G$. We get

$$(c, c'g) = \left(cg^{-1}, c'\right) = 0,$$

since $cg^{-1} \in C$. By definition of $C^{\perp}$ it follows that $c'g \in C^{\perp}$.

Clearly, the two duals C^* and $C^{\perp}$ are not the same object. However, there is a connection between these two notions of duality.

Lemma 1.2.3. *Let C be a code of length n over $\mathbb{F}_q$ and let $G \leq \operatorname{Aut}(C)$. Then $C^* \cong \mathbb{F}_q^n / C^{\perp}$ (as $\mathbb{F}_q G$-modules, in particular, as vector spaces).*

Proof. The proof follows that of [78, Proposition 2.3].

Note that to prove the assertion we need to construct an $\mathbb{F}_q G$-linear isomorphism from $\mathbb{F}_q^n / C^{\perp}$ onto C^*.

For a vector $v \in \mathbb{F}_q^n$ define a function $f_v : C \to \mathbb{F}_q$ by $f_v(c) = (v, c)$ for $c \in C$. Since the scalar product is linear in each component, f_v is $\mathbb{F}_q$-linear, hence, $f_v \in C^*$. The map $\alpha : \mathbb{F}_q^n \to C^*$ given by $v \mapsto f_v$ is $\mathbb{F}_q$-linear as well. Moreover, α is $\mathbb{F}_q G$-linear since the G-invariance of the scalar product implies

$$\begin{aligned} \alpha(vg)(c) = f_{vg}(c) = (vg, c) &= \left(v, cg^{-1}\right) \\ &= f_v\left(cg^{-1}\right) = \left(f_v g\right)(c) = \left(\alpha(v)g\right)(c) \end{aligned}$$

for all $v \in \mathbb{F}_q^n$, $g \in G$ and $c \in C$. As $C^{\perp}$ is the kernel of α we obtain an $\mathbb{F}_q G$-linear monomorphism

$$\overline{\alpha} : \mathbb{F}_q^n / C^{\perp} \to C^* \text{ with } v + C^{\perp} \mapsto \alpha(v) = f_v$$

Observe that

$$\left|\mathbb{F}_q / C^{\perp}\right| = q^{n - \dim C^{\perp}} = q^{\dim C} = |C|.$$

Finally, with $|C^*| = |C|$ (see, for instance, [78, Proposition 2.2]) we obtain

$$\left|\mathbb{F}_q / C^{\perp}\right| = |C^*|.$$

Hence, $\overline{\alpha}$ is an $\mathbb{F}_q G$-linear isomorphism and the proof is complete. □

We want to remark that in [78] the result of Lemma 1.2.3 was proved for a special case of so-called group codes. A code C is said to be a *group code* if C is an ideal in the group algebra $\mathbb{F}_q G$ for some $G \leq \operatorname{Aut}(C)$. Cyclic codes form one of the best studied subclasses of group codes. Particularly important for the present work are binary cyclic codes of odd length. We list some of their properties it the next section.

1.3 Cyclic and duadic codes

Throughout this section we only consider binary cyclic codes of odd length n.

Definition 1.3.1. A linear code C of length n is called *cyclic* if it is invariant under a cyclic shift, i.e., a permutation $\sigma \in S_n$ of order n with $\sigma : i \mapsto i+1 \bmod n$.

We want to remark that the requirement that the length should be odd is crucial for us. It implies that the group algebra $\mathbb{F}_2 \langle \sigma \rangle$ is semi-simple, i.e., it can be written as a direct sum of irreducible subalgebras. In particular, this allows to classify all cyclic codes with self-dual extensions (see Lemma 2.4.7).

Denote by R_n the ring of univariate polynomials of degree less than n with coefficients in $\mathbb{F}_2$:

$$R_n = \mathbb{F}_2[x] / \langle x^n - 1 \rangle .$$

Note that $\mathbb{R}_n \cong \mathbb{F}_2 \langle \sigma \rangle$ as algebras, where $\langle \sigma \rangle$ denotes the cyclic group generated by σ. Then a cyclic code C can be viewed as an ideal in R_n. The action of the cyclic shift σ on a codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is equivalent to the multiplication by x of a polynomial $c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \in R_n$.

Definition 1.3.2. A polynomial $g(x) \in R_n$ of the smallest degree, such that it generates the code C, is called the *generator polynomial* of C.

When describing cyclic codes, cyclotomic cosets are very helpful.

Definition 1.3.3. Let $\mathbb{Z}_n$ be the set of integers modulo n. A cyclotomic coset modulo n containing t is a subset $\mathcal{C}_t$ of $\mathbb{Z}_n$ of the form $\left\{t, 2t, 2^2 t, \ldots\right\} \bmod n$. The singleton $\{0\}$ is called the zero coset. If $\mathcal{C}_{t_1}, \ldots, \mathcal{C}_{t_k}$ are all nonzero cyclotomic cosets then the set $\mathcal{T} = \{t_1, \ldots, t_k\}$ of representatives is called a *transversal*.

Denote by $s(n)$ the multiplicative order of 2 modulo n, i.e., the smallest positive number s, such that $2^s \equiv 1 \bmod n$. We see from Definition 1.3.3 that the coset $\mathcal{C}_1$ has exactly $s(n)$ elements. Moreover, if $n = p$ is a prime then the size of every nonzero cyclotomic coset is $s(p)$. Indeed, for any $t \in \{1, \ldots, p-1\}$ we have

$$2^s t \equiv t \bmod p \;\Leftrightarrow\; 2^s \equiv 1 \bmod p,$$

since t is coprime to p, hence $|\mathcal{C}_t| = |\mathcal{C}_1|$.

Let $\alpha \in \mathbb{F}_{2^{s(n)}}$ be a primitive n-th root of unity. Then for a generator polynomial $g(x)$ of a cyclic code C we have (see [41, Section 4.4])

$$g(x) = \prod_t \prod_{i \in \mathcal{C}_t} \left(x - \alpha^i\right), \tag{1.2}$$

where t ranges over some subset of coset representatives.

Denote by $T = \bigcup_t \mathcal{C}_t$ a subset of $\mathbb{Z}_n$, such that all roots of $g(x)$ are $\left(\alpha^i\right)_{i\in T}$. Then T is called the *defining set* of the code C; $\left(\alpha^i\right)_{i\in T}$ and $\left(\alpha^j\right)_{j\notin T}$ are called *zeros* and *nonzeros* of C, respectively. (Note that the defining set T depends on the chosen primitive root of unity.) The degree of the generator polynomial of C equals $|T|$ and the dimension of C is $n - |T|$.

Sometimes it is more convenient to use the generating *idempotent* of a code instead of the generator polynomial, i.e., a unique polynomial $e(x)$ that generates the code and satisfies $e^2(x) = e(x)$. Any idempotent $e(x) \in R_n$ generates some cyclic code and has the form (see [41, Section 4.4])

$$e(x) = \sum_{j\in J} \sum_{i\in \mathcal{C}_j} x^i, \tag{1.3}$$

where J is some subset of cyclotomic coset representatives. The converse also holds true, i.e., any element of R_n of the form (1.3) is an idempotent.

There is a particular set of permutations that maps idempotents onto idempotents.

Definition 1.3.4. Let n be an integer and let a be coprime with n. The function μ_a defined on $\{0, 1, \ldots, n-1\}$ by $\mu_a : i \mapsto ia \bmod n$ is a permutation of coordinate positions of a cyclic code of length n and is called a *multiplier*. A multiplier μ_a can be regarded as acting on R_n by

$$f(x)\mu_a = f(x^a) \pmod{x^n - 1}.$$

Multipliers are essentially what is needed to establish whether two cyclic codes are equivalent.

Lemma 1.3.5 ([64], [40])**.** *Let C_1 and C_2 be cyclic codes of length n and let φ denote the Euler φ-function. If* $\gcd(n, \varphi(n)) = 1$ *then C_1 and C_2 are equivalent if and only if there is a multiplier that maps the idempotent of C_1 onto the idempotent of C_2.*

Corollary 1.3.6. *Let C_1 and C_2 be binary cyclic codes of prime length p and let $\mathcal{T}$ be a transversal. Then C_1 and C_2 are equivalent if and only if there is a multiplier μ_t with $t \in \mathcal{T}$ that maps the idempotent of C_1 onto the idempotent of C_2.*

Proof. Note that for a prime p we always have $\gcd(p, \varphi(p)) = 1$. Thus, we can apply Lemma 1.3.5. Moreover, due to the form (1.3) of the idempotent of a binary cyclic code, it suffices to check the multipliers that have different actions on the cyclotomic cosets.

First, we show that if a and b lie in the same coset then the multipliers μ_a and μ_b have the same action on all the cyclotomic cosets modulo p. Let $\mathcal{C}_t$ and $\mathcal{C}_s$ be two cyclotomic cosets and let $a, b \in \mathcal{C}_t$, i.e., $b \equiv 2^x a \bmod p$ for some x. Suppose that $sa \equiv r \bmod p$. Then

$$sb \equiv s \cdot 2^x a \equiv 2^x \cdot r \bmod p.$$

Thus, both $s\mu_a$ and $s\mu_b$ lie in the same coset $\mathcal{C}_r$. Hence $\mathcal{C}_s\mu_a = \mathcal{C}_s\mu_b = \mathcal{C}_r$.

Now, suppose that a and b lie in different cosets. Then μ_a and μ_b have different actions on the cyclotomic cosets, in particular

$$\mathcal{C}_1\mu_a = \mathcal{C}_a \neq \mathcal{C}_b = \mathcal{C}_1\mu_b.$$

It follows from these two observations that multipliers that have different actions on the cyclotomic cosets are exactly the μ_t, where t ranges over a transversal $\mathcal{T}$. This completes the proof of the corrolary. □

Lemma 1.3.7. *Let C be a cyclic code of length n. Let σ be a cyclic shift of order n with $\sigma : i \mapsto i + 1 \bmod n$. Then the group $G = \langle\sigma\rangle \rtimes \langle\mu_2\rangle$ of order $|G| = n \cdot s(n)$ is a subgroup of the automorphism group of C.*

Proof. By definition the code C is invariant under the cyclic shift σ.

The multiplier μ_2 maps the idempotent $e(x)$ of the code C onto itself, since $e(x)\mu_2 = e(x^2) = e(x)$. Hence C is invariant under the group $G = \langle\sigma, \mu_2\rangle$, generated by σ and μ_2. From Definition 1.3.4 it follows that

$$\mu_2^j(i) = \underbrace{(\mu_2 \circ \cdots \circ \mu_2)}_{j \text{ times}}(i) = i \cdot 2^j \bmod n.$$

Thus, we see that the order of μ_2 is $s(n)$. In fact G is the semidirect product $\langle\sigma\rangle \rtimes \langle\mu_2\rangle$ (see also [41, Section 4.4]) and thus $|G| = n \cdot s(n)$. □

In the present work we will be interested in cyclic codes with self-dual extensions. By a result of Pless et al. [67] every such cyclic code is duadic.

Definition 1.3.8. Fix some primitive n-th root of unity and let S_1 and S_2 be two subsets of $\{1, 2, \ldots, n-1\}$. Two cyclic codes C_1 and C_2 with defining sets $T_1 = \{0\} \cup S_1$ and $T_2 = \{0\} \cup S_2$, respectively, are called *even-like duadic codes* if S_1 and S_2 satisfy

$$S_1 \cup S_2 = \{1, 2, \ldots, n-1\} \quad \text{and} \quad S_1 \cap S_2 = \emptyset, \tag{1.4}$$

and if there exists a multiplier μ_b such that

$$S_1\mu_b = S_2 \quad \text{and} \quad S_2\mu_b = S_1. \tag{1.5}$$

The augmented codes $D_1 = C_1 + \langle\mathbf{1}\rangle$ and $D_2 = C_2 + \langle\mathbf{1}\rangle$ are called *odd-like duadic codes.*

Note that even-like duadic codes are of dimension $\frac{n-1}{2}$ and odd-like codes — of dimesion $\frac{n+1}{2}$. It follows from the form (1.2) of the generator polynomial and the definition of the defining set that each of the two sets S_1 and S_2 is a union of nonzero cyclotomic cosets. We say that S_1 and S_2 that satisfy (1.4) and (1.5) form a *splitting of n given by μ_b*. In general the same splitting of n can be given by different multipliers.

From [53] we know that duadic codes exist for lengths $n \equiv \pm 1 \bmod 8$. More precisely, the primes p_i that occur in the factorization $n = p_1^{a_1} \cdots p_r^{a_r}$ are all of the form $p_i \equiv \pm 1 \bmod 8$. However, we are mostly interested in the case $n \equiv -1 \bmod 8$, when the extensions of (odd-like) duadic codes are doubly-even (see Lemma 1.3.11). In this case idempotents of duadic codes can be easily constructed.

Lemma 1.3.9 ([41, Theorem 6.1.5]). *Let $n \equiv -1 \bmod 8$ and let S_1 and S_2 be a splitting of n given by μ_b. Then*

$$e_i(x) = \sum_{j \in S_i} x^j$$

with $i = 1$ and 2 are the generating idempotents of a pair of odd-like duadic codes. Moreover,

$$e_1(x)\mu_b = e_2(x) \quad \textit{and} \quad e_2(x)\mu_b = e_1(x) \tag{1.6}$$

Remark 1.3.10. If $e_1(x)$ and $e_2(x)$ are the idempotents of odd-like duadic codes, then $1 + e_1(x)$ and $1 + e_2(x)$ are the idempotents of even-like codes. Thus, equation (1.6) also holds for generating idempotents of even-like codes.

If generating idempotents of a pair of duadic codes satisfy (1.6), then we say that μ_b gives a *splitting* for duadic codes. Note that it follows from (1.6) and Lemma 1.3.5 that the two odd-like codes are equivalent. Clearly, the same also holds for even-like codes.

Lemma 1.3.11 ([67]). *If C is a cyclic code of length n with a self-dual extension, then C is an odd-like duadic code. Moreover, if n is a prime of the form $n \equiv -1 \bmod 8$, then the extension of every odd-like duadic code is self-dual and doubly-even.*

Example 1.3.12. Let $p \equiv -1 \bmod 8$ be a prime with $s(p) = \frac{p-1}{2}$. We want to construct all cyclic codes of length p with self-dual extensions. By Lemma 1.3.11 we are interested in odd-like duadic codes. Apart from the trivial coset $\mathcal{C}_0 = \{0\}$ we have two cyclotomic cosets modulo p

$$\mathcal{C}_1 = \left\{1, 2, 4, \ldots, 2^{\frac{p-1}{2}-1}\right\} \text{ and } \mathcal{C}_{-1} = \mathbb{Z}_n \setminus (\mathcal{C}_0 \cup \mathcal{C}_1),$$

each of which is of length $s(p)$. Thus, there is only one splitting of p, namely $S_1 = \mathcal{C}_1$ and $S_2 = \mathcal{C}_{-1}$, and it is given by μ_{-1}. Hence there is only one pair of odd-like duadic codes. It follows from Lemma 1.3.9 that their idempotents are

$$e_1(x) = \sum_{r \in S_1} x^i \quad \text{and} \quad e_2(x) = \sum_{j \in S_2} x^j.$$

Since p is a prime, it follows that $\mathbb{Z}_p$ is the field $\mathbb{F}_p$. An element $x \in \mathbb{F}_p^*$ is called a *square*, or *quadratic residue*, if there exists some element $a \in \mathbb{F}_p^*$ with $x = a^2$; otherwise x is called a nonsquare (quadratic nonresidue). If α is a p-th root of unity, then $x \in \mathbb{F}_p^*$ is a square if and only if x is an even power of α. Thus, half of the elements of $\mathbb{F}_p^*$ are squares and the other half — nonsquares. In case $p \equiv -1 \bmod 8$ the element 2 is a square, and so are all the elements of $\mathcal{C}_1$. Consequently, we can write the idempotents $e_1(x)$ and $e_2(x)$ of the two odd-like duadic codes as follows

$$e_1(x) = \sum_{r \in Q} x^i \quad \text{and} \quad e_2(x) = \sum_{j \in N} x^j, \tag{1.7}$$

where Q and N denote the sets of squares and nonsquares in $\mathbb{F}_p$, respectively.

In general, duadic codes with idempotents $e_1(x)$ or $e_2(x)$ given by (1.7) (or with idempotents $1 + e_1(x)$ or $1 + e_2(x)$) are called *quadratic residue* codes. Thus, in the case when $p \equiv -1 \bmod 8$ is a prime with $s(p) = \frac{p-1}{2}$, the two odd-like quadratic residue codes are the only cyclic codes of length p with self-dual extensions.

We finish this section with the definition and some properties of the Reed-Muller codes.

Definition 1.3.13. Let $P_1, P_2, \ldots, P_n$ be the $n = 2^m$ points of $\mathbb{F}_2^m$. For any integer r with $0 \leq r \leq m$ let $\mathbb{F}_2[x_1, \ldots, x_m]_r$ be the polynomials in $\mathbb{F}_2[x_1, \ldots, x_m]$ of degree r or less. Then the rth order binary *Reed-Muller code* $\mathcal{R}(r, m)$ of length $n = 2^m$ is defined as follows

$$\mathcal{R}(r, m) = \{\, (f(P_1), \ldots, f(P_n)) \,|\, f \in \mathbb{F}_2[x_1, \ldots, x_m]_r \} \,.$$

Lemma 1.3.14 (see [57, Chapter 13]). *Let $m \geq 3$ be odd. Then the Reed-Muller code $C = \mathcal{R}(\frac{m-1}{2}, m)$ is a $[2^m, 2^{m-1}, 2^{\frac{m+1}{2}}]$ Type II code, and* $\mathrm{Aut}(C) = \mathrm{AGL}(m, 2)$. *Moreover, C is equivalent to an extended cyclic code.*

1.4 Weight enumerators of self-dual codes

Let C be a linear $[n, k, d]$ code over $\mathbb{F}_q$. In Section 1.1 the weight of a codeword c in C is defined as the number of its nonzero components. The *weight distribution* of C is the collection $(A_i)_{0 \leq i \leq n}$, where A_i denotes the number of codewords of weight i in C. The homogeneous polynomial

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

is called the *weight enumerator* of the code C. The minimum distance d is the smallest positive i, for which the number A_i is nonzero.

The weight distribution of the dual code $C^{\perp}$ can be found via the MacWilliams transform [57, Chapter 5, Section 2]:

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C\left(x+y, x-(q-1)y\right). \tag{1.8}$$

Let C be a self-dual code of one of Types I to IV. Using invariant theory Gleason [30] (and later MacWilliams et al. [55]) deduced restrictions on the weight enumerator of C. In particular, he showed that the weight enumerator is a polynomial in suitable polynomials $f(x,y)$ and $g(x,y)$.

Theorem 1.4.1 ([30], [55]). *Let C be a self-dual code of length n over $\mathbb{F}_q$ with $q \leq 4$ and let*

$$\begin{aligned}
g_1(x,y) &= x^2 + y^2, \\
g_2(x,y) &= x^8 + 14x^4y^4 + y^8, \\
g_3(x,y) &= x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}, \\
g_4(x,y) &= y^4 + 8x^3y, \\
g_5(x,y) &= y^{12} + 264x^6y^6 + 440x^9y^3 + 24x^{12}, \\
g_6(x,y) &= y^2 + 3x^2, \\
g_7(x,y) &= y^6 + 45x^4y^2 + 18x^6.
\end{aligned}$$

(i) If C is of Type I, then

$$W_C(x,y) = \sum_{i=0}^{\lfloor n/8 \rfloor} c_i g_1(x,y)^{\frac{n}{2}-4i} g_2(x,y)^i.$$

(ii) If C is of Type II, then

$$W_C(x,y) = \sum_{i=0}^{\lfloor n/24 \rfloor} c_i g_2(x,y)^{\frac{n}{8}-3i} g_3(x,y)^i.$$

(iii) If C is of Type III, then

$$W_C(x,y) = \sum_{i=0}^{\lfloor n/12 \rfloor} c_i g_4(x,y)^{\frac{n}{4}-3i} g_5(x,y)^i.$$

(iv) If C is of Type IV, then

$$W_C(x,y) = \sum_{i=0}^{\lfloor n/6 \rfloor} c_i g_6(x,y)^{\frac{n}{2}-3i} g_7(x,y)^i.$$

In all cases c_i are rationals and $\sum_i c_i = 1$.

An immediate corollary of Theorem 1.4.1 is the restriction on the length of a self-dual code.

Corollary 1.4.2. *Let C be a self-dual code of length n over $\mathbb{F}_q$ with $q \leq 4$. Then*

(i) $2 \mid n$ *if C is of Type I or Type IV,*

(ii) $4 \mid n$ *if C is of Type III,*

(iii) $8 \mid n$ *if C is of Type II.*

Mallows and Sloane [59] and MacWilliams et al. [56] used Theorem 1.4.1 to derive upper bounds on the minimum distance of self-dual codes of Types II, III, and IV (see Theorem 1.1.5). (Recall that codes that achieve the bound of Theorem 1.1.5 are called extremal.) They also showed that the weight enumerators of extremal codes of Types II, III, and IV are unique. Moreover, for sufficiently large lengths the coefficients of the weight enumerator may become negative, thus implying the nonexistence of respective codes.

Actually, the bounds in Theorems 1.1.10 and 1.1.11 come from the fact that the weight enumerator coefficients must be non-negative in order for a code to exist.

In Chapter 3 we will use the following formulas for the number A_d of codewords of minimum weight d in an extremal Type II code.

Theorem 1.4.3 ([59])**.** *Let C be an extremal Type II code of length n and minimum distance d. Then the coefficient A_d of the weight enumerator of C may be found as follows*

$$\begin{aligned} \binom{n}{5}\binom{5m-1}{m-1}\Big/\binom{4m+4}{5} &\quad \text{if } n = 24m,\\ \frac{1}{4}n(n-1)(n-2)(n-4)\frac{(5m)!}{m!(4m+4)!} &\quad \text{if } n = 24m+8,\\ \frac{3}{2}n(n-2)\frac{(5m+2)!}{m!(4m+4)!} &\quad \text{if } n = 24m+16. \end{aligned}$$

Rains [70] obtained the bound in Theorem 1.1.5 for Type I codes using restrictions that come from the weight distribution of a special nonlinear code, called the shadow, which is associated with every Type I code.

Definition 1.4.4. Let C be a self-dual code of Type I. Furthermore, let C_0 denote the subcode of C that consists of all codewords, whose weights are multiples of 4. If $C_2 = C \setminus C_0$ then the *shadow* S of the code C consists of all vectors $u \in \mathbb{F}_2^n$ such that

$$\begin{aligned} (u,v) &= 0 \quad \text{for all } v \in C_0,\\ (u,v) &= 1 \quad \text{for all } v \in C_2. \end{aligned} \tag{1.9}$$

Note that $C_0^{\perp}$ consists of the union of four cosets of C_0, say, C_0, C_1, C_2 and C_3. Since $C = C_0 \cup C_2$ then from (1.9) and self-duality of C we get

$$S = C_0^{\perp} \setminus C = C_1 \cup C_3.$$

From (1.9) it also follows that a sum of any two vectors in S lies in C.

The concept of shadow was first introduced by Ward [76]; Conway and Sloane [20] used it to find constraints on Type I codes. They showed that the weight enumerators of a Type I code and its shadow are connected by a transformation, similar to (1.8), and were able to deduce a number of restrictions on the weight distribution of the shadow.

Theorem 1.4.5 ([20])**.** *Let C be a Type I $[n, \frac{n}{2}, d]$ code and let S be its shadow. If*

$$W_S(x, y) = \sum_{j=0}^{n} B_j x^{n-j} y^j$$

is the weight enumerator of the shadow then

$$W_S(x, y) = \frac{1}{|C|} W_C(x + y, \mathbb{i}(x - y)), \tag{1.10}$$

where $\mathbb{i} = \sqrt{-1}$. Furthermore, the coefficients B_j, $0 \leq j \leq n$, satisfy the following properties:

(i) $B_j = B_{n-j}$,

(ii) $B_j = 0$ *unless* $j \equiv \frac{n}{2} \bmod 4$,

(iii) $B_0 = 0$ *and* $B_j \leq 1$ *for* $j < d/2$.

Ever since the original paper of Conway and Sloane [20] the shadow is widely used for studying extremal Type I codes. For instance, by a result of Rains [70] extremal Type I codes do not exist for lengths a multiple of 24.

Theorem 1.4.6 ([70])**.** *Let C be an extremal self-dual code of length $n \equiv 0 \bmod 24$. Then C is of Type II.*

The ultimate goal of the research of extremal Type I codes is to derive an explicit bound on the length of codes, similar to those in Theorems 1.1.10 and 1.1.11. However, the best that is achieved so far are bounds on codes, whose shadow has prescribed minimum weight. The *minimum weight* of a shadow is defined as the smallest positive j, for which the coefficient B_j of the weight enumerator $W_S(x, y)$ of the shadow is positive.

Bachoc and Gaborit [3] found an upper bound on the minimum weight of the shadow of a given Type I code.

Lemma 1.4.7 ([3])**.** *Let C be a Type I code with minimum distance d and minimum weight s of the shadow. Then*

$$2d + s = \tfrac{n}{2} + 8, \quad \textit{if } n \equiv 22 \bmod 24 \textit{ and } d = 4\left\lfloor \tfrac{n}{24} \right\rfloor + 6,$$

$$2d + s \leq \tfrac{n}{2} + 4, \quad \textit{otherwise.}$$

An $\left[n, \frac{n}{2}, d\right]$ self-dual code C of Type I is called *s-extremal* if the bound in Lemma 1.4.7 is reached, i.e., if $2d + s = \frac{n}{2} + 4$ (or $2d + s = \frac{n}{2} + 8$ in the case when C is extremal of length $n \equiv 22 \bmod 24$).

Lemma 1.4.8 ([3]). *Let C be an $\left[n, \frac{n}{2}, d\right]$ Type I s-extremal code. Then the weight distributions $(A_i)_{0 \leq i \leq n}$ of C and $\left(B_j\right)_{0 \leq j \leq n}$ of its shadow are uniquely determined. In particular,*

$$A_d = \frac{n}{d} \sum_{\substack{j,k \in \mathbb{N} \\ j+k=\frac{d}{2}-1}} (-1)^j \binom{\frac{n}{2} - 2d + j}{j} \binom{d + k - 1}{k}.$$

Apart from s-extremal codes in Chapter 3 we will consider so-called *codes with minimal shadow*. These are self-dual codes of Type I whose shadow has the smallest possible minimum weight.

Definition 1.4.9 (see [12]). Let C be a Type I code of length $n = 24m + 8\ell + 2r$, where $\ell = 0, 1, 2$ and $r = 0, 1, 2, 3$, and let S be the shadow of C. Then C is called a code with minimal shadow if for the minimum weight s of S we have

$$\begin{aligned} s &= r, \quad \text{if } r = 1, 2, \text{ or } 3, \\ s &= 4, \quad \text{if } r = 0. \end{aligned}$$

Chapter 2

Automorphisms of extremal codes

2.1 Known extremal Type II codes and their automorphisms

As we know from Theorem 1.1.10 (a), the possible length of an extremal Type II code is of the form $n = 24m + 8\ell$, where $\ell \in \{0, 1, 2\}$ and $m < 154$ if $\ell = 0$, $m < 159$ if $\ell = 1$, and $m < 164$ if $\ell = 2$. Despite the fact that the length might be as large as 3928, only extremal codes of length up to 136 are actually known to exist.

Here is a list of all lengths, for which extremal Type II codes are constructed (see [72, Section 12] and [35])

$$8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136 \tag{2.1}$$

By examining the list one notices that the first gaps occur at lengths 72 and 96. In fact, the existence of an extremal $[72, 36, 16]$ code is a long standing question, posed by Sloane [73] in 1973. In general, extremal codes of length a multiple of 24 are of particular interest, mainly because of Theorem 1.1.8, which tells that these codes hold 5-designs. Another point of interest is that by Theorem 1.4.6 extremal self-dual codes of length $n = 24m$ are always doubly-even.

However, there are only two examples of extremal $[24m, 12m, 4m + 4]$ codes. For $m = 1$ it is the famous Golay code with the 5-transitive Mathieu group M_{24} as the automorphism group [31] (see also [57, Chapter 20]). The uniqueness (up to equivalence) of the $[24, 12, 8]$ code was proved by Pless [65]. For $m = 2$ the extended quadratic residue code is the only extremal code. Its automorphism group is the 2-transitive projective special linear group $\mathrm{PSL}(2, 47)$. There was no proof of the uniqueness of this code until a lengthy computer search by Houghten et al. [37].

Although neither is a self-dual $[72, 36, 16]$ code constructed, nor is its non-existence proven, a lot may be said about the automorphism group of a putative code. Due to results of Conway, Pless, Thompson ([19], [66], [68]), and Huffman and Yorgov [42] it was already known in 1980s that the possible prime divisors of the group order are $2, 3, 5$ or 7. After a period of more than fifteen years with no significant results the next step was taken in the beginning of 2000s. Bouyuklieva [6, 7] and Doncheva et al. [26] determined the possible cycle structures (or types, see Section 2.2) of automorphisms of these orders. They showed that automorphisms of orders 2 and 3 operate fixed point freely, and of orders 5 and 7 have exactly 2 fixed points. This was a turning point in the study of the automorphism group. It was then possible to prove statements about the group structure and find bounds on the group order. First, Bouyuklieva et al. [11] showed that the group is solvable. Then, O'Brien and Willems [63] proved that the group order is smaller than or equal to 36. Further refinements were recently made by Nebe [62], Feulner and Nebe [29], Yankov [80], and Borello [4]. In particular, Feulner and Nebe showed by a lengthy computer search that 7 does not divide the group order. To sum up, the state of the art is the following: the order of the automorphism group for a putative self-dual $[72, 36, 16]$ code is either 5 or a divisor of 24.

As far as a putative $[96, 48, 20]$ code is concerned, Doncheva [23] showed that only 2, 3, and 5 can occur as prime divisors of the automorphism group order. The possible cycle structures were determined by Bouyuklieva [6] and De la Cruz [21]: automorphisms of order 2 have no fixed points, of order 5 have exactly 6 fixed points, and of order 3 have either 6 fixed points or operate fixed point freely. Moreover, if all automorphisms of order 3 are fixed-point-free then either the group is solvable and the order is 15, 30, 240, 480, or divides $2^5 \cdot 3$ or $2^5 \cdot 5$, or the group is the alternating group A_5 of order 60 [21].

Little was known until recently about a putative $[120, 60, 24]$ code. Bouyuklieva [6] showed that automorphisms of order 2 have either 24 or no fixed points. De la Cruz [21] reduced the number of possible prime divisors of the automorphism group order and determined their cycle structures. He also proved that the order of the group is $2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 19^e \cdot 23^f \cdot 29^g$, where $b, c, d, e, f, g \in \{0, 1\}$.

As we can see, it is an extremely difficult problem to prove the existence (or nonexistence) of an extremal code of length a multiple of 24. However, there is a lot of evidence suggesting that if such codes exist, the respective automorphism groups are likely to be comparatively small.

Unfortunately, the list in (2.1) provides little information about extremal codes. For instance, the following questions may arise while considering the list.

1. For what lengths in (2.1) are there examples of codes with large (e.g., multiply-transitive) automorphism groups or automorphisms of large prime order?
2. What families of codes provide examples of extremal codes for more than one entry of the list in (2.1)?

n	d	$p \mid \lvert\mathrm{Aut}(C)\rvert$	Number of codes
8	4	2, *3*, **7**	$=1$ (Hamming)
16	4	2, 3, 5, *7*	$=2$
24	8	2, 3, 5, 7, *11*, **23**	$=1$ (Golay)
32	8	2, 3, 5, 7, **31**	$=5$
40	8	2, 3, 5, 7, *19*	≥ 1000
48	12	2, 3, *23*, **47**	$=1$ (xQR)
56	12	2, 7, 13	≥ 166
64	12	2, *31*	≥ 3270
80	16	2, 3, 5, 7, 13, 19, **79**	≥ 15
88	16	2, 3, 7, 11, *43*	≥ 470
104	20	2, 3, 13, 17, **103**	≥ 1 (xQR)
112	20	2, 7	≥ 1 ([35])
136	24	2, 3, 11, *67*	≥ 1 (QDC)

Table 2.1: Primes that can occur as a factor of the automorphism group order for some extremal $\left[n, \frac{n}{2}, d\right]$ Type II code C

Table 2.1 may be helpful in approaching these questions.

In the first column we give lengths n from (2.1); the corresponding minimum distance d (determined by Theorem 1.1.5) of extremal Type II codes is in the second column. In the third we list all possible primes p that divide the automorphism group order for some extremal code of given length. In the last column we give the number (up to equivalence) of extremal codes of given length. The number is exact if it is preceded with the equality sign ($=$). With the "greater or equal" sign ($\geq$) we give the number of extremal codes that where constructed. Note that in such cases there might actually be more codes. If there is only one known code for given length, we also give its name. Thus, a unique $[8, 4, 4]$ code is the Hamming code. We already mentioned the Golay code of length 24 and the extended quadratic residue code (abbreviated xQR in the table) of length 48. The abbreviation QDC stands for the quadratic double circulant code (see below).

Table 2.1 is based on the information from [72, Section 12.1] with additions from [83] and [14] for $n = 40$, [36] and [82] for $n = 56$, [32] and [81] for $n = 64$, [24], [33], and [84] for $n = 80$, [33] for $n = 88$, and [35] for the $[112, 56, 20]$ code.

As one can notice from the table the only prime $p > \frac{n}{2}$, which occurs in the third column, is $p = n - 1$. We distinguished it with **bold** font in the table. Also, there can only be one prime p with $\frac{n}{3} < p < \frac{n}{2}$. This prime is $p = \frac{n}{2} - 1$ and it appears in *italic* font in the table.

As we will show in Section 2.2, this does not occur by chance and is caused by a restriction on the possible types of automorphisms that are admitted by extremal codes (see Theorem 2.2.8).

Note that a code accepting an automorphism of order $n-1$ is equivalent to an extended cyclic code, as we will show in Lemma 2.2.3. Among codes that are invariant under an automorphism of order $\frac{n}{2}-1$ we distinguish so-called bordered double circulant codes. A bordered double circulant code has generator matrix of the form

$$\begin{pmatrix} & 0 & 1 \;\; \cdots \;\; 1 \;\; 1 \\ & 1 & \\ I_{n/2} & \vdots & Q \\ & 1 & \\ & 1 & \end{pmatrix}, \tag{2.2}$$

where Q is an $\left(\frac{n}{2}-1\right) \times \left(\frac{n}{2}-1\right)$ *circulant* matrix, i.e., the $(i+1)$-st row of Q is a cyclic shift of the i-th row.

Among extended cyclic codes extended quadratic residue codes are of particular interest. They are extremal for every length n from the list in (2.1), such that $n = p+1$, where p is a prime. The ones of lengths 8, 24, 48, and 104 are the only known extremal codes of those lengths. Extended quadratic residue codes are remarkable codes with 2-transitive automorphism group $\mathrm{PSL}(2,p)$ (see [38]). They were studied by a number of researches, Gleason, Assmus and Mattson [2], Karlin and MacWilliams [49] to name a few.

Closely related to quadratic residue codes are so-called quadratic double circulant codes, a subclass of bordered double circulant codes. They provide examples of extremal Type II codes for lengths 8, 24, 40, 88, and 136, the latter being the largest known extremal code. Quadratic double circulant codes exist for lengths $n = 2q+2$ for prime q and are invariant under the group $\mathrm{PSL}(2,q)$.

We provide a complete classification of both extended quadratic residue and quadratic double circulant extremal Type II codes in Section 2.3.

Well-studied Reed-Muller codes also provide examples of extremal codes. These are the first order $[8,4,4]$ code (the Hamming code) and the second order $[32,16,8]$ code. From Lemma 1.3.14 we know that these codes are invariant under 3-transitive groups $\mathrm{AGL}(3,2)$ and $\mathrm{AGL}(5,2)$, respectively. However, since the minimum distance of Reed-Muller codes is known (see Lemma 1.3.14), one can easily verify that no other code of this family is extremal. In Section 2.7 we classify affine-invariant codes, a generalization of Reed-Muller codes.

Thus, as far as extremal Type II codes with multiply-transitive groups are concerned, there are exactly 7 of them known: the $[8,4,4]$ Hamming code, the $[24,12,8]$ Golay code, the second order $[32,16,12]$ Reed-Muller code and extended quadratic residue codes of lengths 32, 48, 80, and 104. As one of the main results of the thesis, we prove in Section 2.8 that there are no other such codes, except possibly a code of length 1024.

2.2 Types of automorphisms of binary extremal codes

As we discussed in the previous section, for a given automorphism of an extremal code its cycle structure is of particular interest.

Definition 2.2.1. We say that a permutation $\sigma \in S_n$ of prime order p is of type p-(c, f) if it consists of c cycles and f fixed points, so that $n = pc + f$.

We want to remark that all elements of the same type are conjugate in S_n.

Example 2.2.2. Let p be a prime and let C be a binary self-dual code of length $n = p + 1$ that is invariant under an automorphism σ of order p. In this case there is only one possibility: σ is of type p-$(1, 1)$ and has exactly one cycle of length p and one fixed point. It follows from Lemma 2.2.3 that C is equivalent to an extended cyclic code.

Lemma 2.2.3. *Let C be a self-dual code of length $n = p + 1$, where p is a prime. Let furthermore $\sigma \in \mathrm{S}_n$ be an automorphism of C of type p-$(1, 1)$. Then C is equivalent to an extended cyclic code.*

Proof. Denote by σ_0 a permutation in S_n such that $i \mapsto i + 1 \bmod p$ for all $0 \leq i \leq p - 1$, and p is a fixed point of σ_0. Let $\tau \in \mathrm{S}_n$ be such that $\tau^{-1}\sigma\tau = \sigma_0$. Furthermore, let C' be a code that is equivalent to C, where the equivalence is given by τ, i.e., $C' = C\tau$, or $C = C'\tau^{-1}$. As σ is an automorphism of C, we may write $C = C\sigma$. Thus we have

$$C'\tau^{-1} = C = C\sigma = C'\tau^{-1}\sigma,$$

and it follows that

$$C' = C'\tau^{-1}\sigma\tau = C'\sigma_0.$$

In other words, σ_0 is an automorphism of C'. It follows from Definition 1.3.1 that C' with the last coordinate removed is a cyclic code.

Finally, we stress that there is only one way to extend a code in order to obtain a self-dual code, since each codeword of the extended code should be orthogonal to itself. Note that in the binary case a vector is orthogonal to itself if and only if it is even-like. □

Remark 2.2.4. A similar result holds when the length of the code in question is not a prime. A self-dual code C of length n, invariant under an automorphism $\sigma \in \mathrm{S}_n$, which consists of a single cycle of order $n - 1$, is equivalent to an extended cyclic code. The proof remains exactly the same as for Lemma 2.2.3.

The following theorem of Yorgov [82] has proven to be of immense importance in the research of extremal codes.

Theorem 2.2.5 ([82]). *Let C be a binary self-dual $[n,k,d]$ code and let $\sigma \in \mathrm{Aut}(C)$ be of type p-(c,f), where p is an odd prime. If $f > c$ then*

$$f \geq \sum_{i=0}^{\frac{f-c}{2}-1} \left\lceil \frac{d}{2^i} \right\rceil .$$

Theorem 2.2.5 is one of the few theoretical tools that help to establish cycle structures of automorphisms.

Corollary 2.2.6. *Let $p > 23$ be a prime and let C be an extremal Type II code of length $n = 2p + 2$. Further assume that a permutation τ of order p leaves the code C invariant. Then τ is of type p-$(2,2)$.*

Proof. Recall from Corollary 1.4.2 that the length n is a multiple of 8 and from Theorem 1.1.10 that n is bounded by 3928.

Note that there are two possibilities for the type of τ: p-$(2,2)$ and p-$\left(1, \frac{n}{2} + 1\right)$. However, with Theorem 2.2.5 and a simple computation we can rule out the second possibility for all $n \leq 3928$. □

Remark 2.2.7. Recall from Table 2.1 that all extremal Type II codes of lengths 8, 16, 24, 32 and 48 are known. The only other case, not touched upon by Corollary 2.2.6, is $n = 40$. However, it follows from [39, Theorem A.3] that there are no extremal Type II codes of length 40 with automorphisms of type 7-$(1,9)$.

Despite the fact that Theorem 2.2.5 is a powerful tool of determining the possible cycle structures of automorphisms of binary self-dual codes, it is not particularly easy to apply. Together with Bouyuklieva and Willems we have proved the following easy-to-handle result.

Theorem 2.2.8. *Let C be a binary extremal self-dual code of length $n \geq 48$, invariant under an automorphism σ of type p-(c,f), where $p \geq 5$ is a prime. Then $c \geq f$.*

Proof. The lengthy proof of Theorem 2.2.8 can be found in [9]. □

Remark 2.2.9. Notice that with Theorem 2.2.8 one does not need to do any computations at all to prove Corollary 2.2.6.

Remark 2.2.10. Let us remark that the restriction on the length of a code in Theorem 2.2.8 is essential. That is, there exist codes of length less than 48 that admit automorphisms of types p-(c,f) with $f > c$. Specifically, there are Type II codes of length 40 with automorphisms of type 3-$(6,22)$ (Bouyuklieva [8]) and 5-$(4,20)$ (Yorgov [45]). As for Type I codes, there are those of length 42 with automorphisms of types 5-$(4,22)$ or 3-$(6,24)$ (both [8]) and of length 44 with automorphisms of type 11-$(2,22)$ (Yorgov and Russeva [46]), 5-$(4,24)$, or 3-$(6,26)$ (both [8]). We also refer the reader to Tables 2 and 3 in [39] and to Table II in [9].

On the other hand, there are no known extremal codes of length $n \geq 48$ that have an automorphism of order 3 with the number of fixed points exceeding the number of cycles. However, to show that automorphisms of types, say, $3\text{-}(14,26)$ or $3\text{-}(16,20)$ can not occur for extremal Type I codes of length 68 seems to be a difficult problem (see [39] and [9]).

Corollary 2.2.11. *Let C be an extremal self-dual code of length $n \geq 48$ with an automorphism σ of type $p\text{-}(c,f)$, where $p > \frac{n}{2}$ is a prime. Then $p = n-1$, $c = f = 1$. Moreover, if C is doubly-even then $n = 24m + 8\ell$, where $\ell \in \{0,1\}$ and $m \geq 2$.*

Proof. It follows from Theorem 2.2.8 that $c \geq f$. Further, since $p > \frac{n}{2}$ and $n = pc + f$, the only possibility is $p = n-1$, $c = f = 1$.

Let C be of Type II. From Corollary 1.4.2 we known that n is a multiple of 8. Thus, we have $n = 24m + 8\ell$, where $\ell \in \{0,1,2\}$. The case $n = 24m + 16$ can not occur, since $n - 1 = 24m + 15$ is divisible by 3 and, hence, is not a prime. Finally $m \geq 2$ since $n \geq 48$. □

Corollary 2.2.11 explains why there is only one prime p greater than $\frac{n}{2}$, namely $p = n-1$, in the third column of Table 2.1. By this result and by Lemma 2.2.3, the investigation of extremal Type II codes that are invariant under automorphisms of large prime orders reduces to the case of extended cyclic codes.

However before we proceed with the classification of binary extended cyclic codes, in the next section we introduce a method of effective search for small weight codewords (see Algorithm 2.3.5). We also apply this method to classify extremal codes that arise from quadratic residues.

2.3 Extremal Type II codes arising from quadratic residues

In this section we classify extremal Type II codes that arise from quadratic residues. These include quadratic residue codes, generalized quadratic residue codes, and quadratic double circulant codes.

We already considered quadratic residue codes in Example 1.3.12. For reader's convenience below we give a formal definition.

Definition 2.3.1. A duadic code C is called a quadratic residue code if the generating idempotent of C is one of the following

$$\sum_{i\in Q} x^i, \quad 1 + \sum_{i\in Q} x^i, \quad \sum_{j\in N} x^j, \quad \text{or} \quad 1 + \sum_{j\in N} x^j,$$

where Q and N denote the sets of squares and nonsquares in $\mathbb{F}_p^*$ respectively. In other words, the sets Q and N form the corresponding splitting of p.

Quadratic residue codes exist for prime lengths p of the form $p \equiv \pm 1 \bmod 8$. In this section we will only consider the case $p \equiv -1 \bmod 8$, since in this case extended quadratic residue codes are of Type II (see [57, Chapter 16]).

It follows from Theorem 1.1.10 (a) that there exist more than a hundred of extended quadratic residue codes that might potentially be extremal. To establish the minimum distance of a code of large length (say, $n > 400$) is an impossible task even for a computer. However, if we recall Section 2.1, the only extended quadratic residue codes that are known to be extremal are of lengths $n = 8$, 24, 32, 48, 80, and 104. One can verify that extended quadratic residue codes of lengths 72 or 128 are not extremal. Thus, it is reasonable to expect that no other quadratic residue codes, apart from the aforementioned six, are extremal. The task of proving the non-extremality of a code is, in fact, much easier than finding the exact minimum distance. Indeed, one needs only to find a codeword of weight strictly less than the bound in Theorem 1.1.5.

Of course, there is a number of methods of finding low weight codewords in quadratic residue codes: deterministic algorithms of Karlin and MacWilliams [49] and Lam et al. [61] and a probabilistic approach of Leon [52], to name a few. Unfortunately, for some larger lengths all of these algorithms fail to yield results in reasonable time.

The main idea behind all of these algorithms is to search for low weight codewords in a suitable subcode instead of the whole code. The problem is then, however, to choose the subcode in such a way that a codeword of desired weight should lie in it. Below we desribe a method of choosing a suitable subcode for codes with nontrivial automorphism groups.

We want to remark here that the automorphism group of quadratic residue codes was (at least, in part) known for a long time. It is one of the main reasons of attention drawn to quadratic residue codes over the last decades.

Lemma 2.3.2 (Gleason and Prange, Huffman)**.** *Let C be an extended quadratic residue code of length $n = p + 1$ for $p \equiv -1 \bmod 8$. Then* $\mathrm{Aut}(C) = \mathrm{PSL}(2, p)$, *which is of order $\frac{1}{2}(p-1)p(p+1)$, apart from the cases $p = 7$ and 23, when* $\mathrm{Aut}(C)$ *is even bigger.*

Remark 2.3.3. The original theorem of Gleason and Prange (see [57, Section 16.5]) stated only that $\mathrm{PSL}(2, p) \leq \mathrm{Aut}(C)$. Using the classification of 2-transitive groups (see [15]) Huffman [38] proved that $\mathrm{Aut}(C)$ can not be bigger.

Remark 2.3.4. The two exceptions, namely for $p = 7$ and $p = 23$, may be explained by the equivalence of the $[8, 4, 4]$ code to the first order Reed-Muller code (the group is $\mathrm{AGL}(3, 2)$) and the $[24, 12, 8]$ code to the extended Golay code (with the group M_{24}).

The idea of our method is to choose the subgroup of the automorphism group first and then take the subcode that is fixed under the chosen subgroup.

Algorithm 2.3.5 (Effective search for a codeword of small weight).

```
 Input. A code $C$ invariant under the group $G$,
        a bound $d$ on the weight.
Output. A codeword of $C$ of weight less than $d$.
Step 1. Choose the subgroup $H$ of $G$ of small order.
Step 2. Take the subcode $C^H$ of $C$ that is fixed under $H$:
        $$C^H = \mathrm{Fix}(C, H) = \{c \in C \mid c\sigma = c \text{ for all } \sigma \in H\}. \qquad (2.3)$$
Step 3. Search for a codeword of weight less that $d$ in $C^H$.
```

Remark 2.3.6. We do not have a good recipe how to choose the subgroup H in Step 1 of the algorithm. In fact, this is somewhat tricky. On the one hand, the resulting subcode C^H should be small; on the other hand, C^H should contain codewords of small enough weight.

However, for codes of length between 1000 and 4000 subgroups H of order $5 \leq |H| \leq 30$ appear to be a good choice.

Remark 2.3.7. The size of C^H depends not only on the order of H, but also on the structure.

With Algorithm 2.3.5 at hand we are able to prove one of the main results of the thesis.

Theorem 2.3.8. *Let C be an extremal extended quadratic residue code of length n. Then $n = 8, 24, 32, 48, 80,$ or 104.*

Proof. Let n denote the length of the code C. Since C is a self-dual extended quadratic residue code, we have $n = p + 1$, where p is a prime of the form $p \equiv -1 \bmod 8$ (see [57, Chapter 16]). Moreover, it follows from Lemma 1.3.11 that C is of Type II. We may write $n = 24m + 8\ell$ for $\ell \in \{0, 1\}$, since $n - 1$ is not a prime if $\ell = 2$. By Theorem 1.1.10 (a) an extremal code of this length may exist if $m \leq 154$ for $\ell = 0$ and $m \leq 159$ for $\ell = 1$.

From Section 2.1 we known that extended quadratic residue codes of lengths $n = 8, 24, 32, 48, 80$, and 104 are extremal.

Let C be an extended quadratic residue code of length $n = 24m$, where $5 \leq m \leq 11$, or of length $n = 24m + 8$, where $3 \leq m \leq 16$. For every such C we can find a codeword of weight smaller than $d = 4m + 4$ via direct enumeration. It follows, that all codes of these lengths are not extremal.

For codes of larger lengths we apply Algorithm 2.3.5. The subgroup H that we choose depends on the length of the code in question. If $n = 24m$ with $11 < m \leq 78$, we take $H = \mathbb{Z}_4$, the cyclic group of order 4. If $n = 24m + 8$, where $16 < m \leq 78$, we take $H = \mathbb{Z}_6$, the cyclic group of order 6. For codes with $m > 78$ we take the Sylow-2 subgroup of $\mathrm{PSL}(2, p)$ as H. In all cases we have

$\dim C^H \leq 235$. In every one of the subcodes C^H we find a codeword of weight smaller than $d = 4m + 4$. Thus, none of the corresponding extended quadratic residue codes C is extremal.

All computations are carried out with MAGMA [5]. □

We want to illustrate the work of Algorithm 2.3.5, vital for proving Theorem 2.3.8, on some examples.

Example 2.3.9. Let C be an extended quadratic residue code of length $n = 1872$ $= 24 \cdot 78$. Note that we construct the code C by forming the idempotent and the generator matrix explicitly. This approach proves to be faster than using the built-in MAGMA function `QRCode`. We apply Algorithm 2.3.5 to find a codeword in C of weight strictly smaller than $d = 316$.

In the first step we choose a subgroup $H = \mathbb{Z}_6$ (the cyclic group of order 6) of $G = \mathrm{PSL}(2, 1871)$. To generate the group we find an element of order 6 in G via direct enumeration. The next step is to generate the subcode $C^H = \mathrm{Fix}(C, H)$. This is done in MAGMA with the built-in function `Fix`. The resulting code C^H is of dimension $234 = n/8$. In C^H with the built-in MAGMA function `WordsOfBoundedWeight`, which does the enumeration, we find a codeword of weight $312 < d$. Thus C is not extremal.

Example 2.3.10. Let C be an extended quadratic residue code of length $n = 3824$ $= 24 \cdot 159 + 8$. We are searching for a codeword of weight less than $d = 640$.

To generate a subgroup H of $G = \mathrm{PSL}(2, 3823)$, which in this case is a Sylow 2-subgroup of G of order $2^4 = 16$, we use the built-in MAGMA function `SylowSubgroup`. The subcode C^H is of dimension 120, which is slightly greater than $n/32$. We prove the non-extremality of C by finding a codeword of weight $608 < d$ in C^H.

The MAGMA source code for the examples is given in Listings A.1 and A.2 in Appendix A.

At the end of this section we classify other extremal Type II codes that are related to quadratic residues codes.

Generalized quadratic residue codes were introduced by Ward [75] and Camion [16] as group codes for abelian groups. For an elementary description we refer the reader to van Lint and MacWilliams [74]. Here we will just define binary generalized quadratic residue codes by giving their generator matrix.

Definition 2.3.11 ([74]). Let $q = p^m$ for a prime p, such that 2 is a square modulo p, and let α be a primitive element of $\mathbb{F}_q$. Further, let U and V denote the sets of nonzero squares and nonsquares of $\mathbb{F}_q$ and let $e \in \mathbb{F}_2^q$ be a vector with components

$$e_i = \begin{cases} \frac{q+1}{2}, & \text{if } i = 0, \\ c_0, & \text{if } i \in U, \\ c_1, & \text{if } i \in V \end{cases} \tag{2.4}$$

for $c_0 \neq c_1 \in \mathbb{F}_2$. A code is called a *generalized quadratic residue* code if its generator matrix M has the following form. Label the rows and columns of M by the elements $0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$ of $\mathbb{F}_q$. Then the first row of M contains the coordinates of e from (2.4) and the entry in the position (α^i, α^j) equals that in the position $(0, \alpha^j - \alpha^i)$.

For each $q = p^m$ there are two generalized quadratic residue codes: one corresponding to the squares (with the idempotent e given by (2.4) with $c_0 = 1, c_1 = 0$) and one — to the nonsquares (with $c_0 = 0$, $c_1 = 1$). The two codes are equivalent.

Lemma 2.3.12 ([74]). *Let $q = p^m$ and let C be an extended generalized quadratic residue code of length $q + 1$. If m is odd and $p \equiv -1 \bmod 4$ then the code C is self-dual of Type II. Moreover, C is invariant under the group* $\mathrm{PSL}(2, q)$.

Notice that a generalized quadratic residue code of prime length $q = p^1 = p$, where $p \equiv \pm 1 \bmod 8$, is just a usual quadratic residue code (see Definition 2.3.1).

There is only one prime power $q = p^m$ with $p \equiv -1 \bmod 4$ and odd $m > 1$, such that $q + 1$ satisfies the bound of Theorem 1.1.10 (a), namely, $q = 343 = 7^3$. Thus, the classification of extremal extended generalized quadratic residue codes is reduced to determining whether the code of length 344 is extremal.

Theorem 2.3.13. *The* $[344, 172]$ *extended generalized quadratic residue code has minimum distance $d \leq 44$ and is not extremal.*

Proof. Let C be the $[344, 172]$ extended generalized quadratic residue code. Via direct enumeration with Magma we find that C contains a codeword of weight 44. From Theorem 1.1.5 we known that an extremal code of length 344 should have minimum distance 60. Thus, C is not extremal. □

We already mentioned in Section 2.1 that a great number of known extremal Type II codes are bordered double circulant (see also [36], [32], and [33]). Among these codes of particular interest are so-called quadratic double circulant codes, which provide the largest known example of an extremal code.

We classify extremal quadratic double circulant codes in a similar way as we did for quadratic residue codes.

Definition 2.3.14. A code of length $n = 2p + 2$, where $p \equiv 3 \bmod 8$ is a prime, is called a *quadratic double circulant* code if its generator matrix is of the form

$$\left(\begin{array}{c|cccc} & 0 & 1 & \cdots & 1 \; 1 \\ & 1 & & & \\ I_{n/2} & \vdots & & Q & \\ & 1 & & & \\ & 1 & & & \end{array} \right),$$

where Q is a $p \times p$ circulant matrix, corresponding to quadratic residues. This means that the first row of Q has 1 in the position i, $0 \leq i \leq q - 1$, if and only if $i = 0$ or i is a square in $\mathbb{F}_p^*$.

It can be seen from the form of the generator matrix that quadratic double circulant codes are always self-dual and doubly-even. As we know from Section 2.1, for $p = 3, 11, 19, 43$, and 67 quadratic double circulant codes are extremal.

A quadratic double circulant code of length $n = 2p + 2$ is invariant under the group $\mathrm{PSL}(2, p) \times \mathbb{Z}_2$ (see [57, Chapter 16]). Note that $\mathrm{PSL}(2, p)$ acts simultaneously on the first $p + 1$ positions and the second $p + 1$ positions of a codeword. The $\mathbb{Z}_2$ part means that the code remains invariant under the interchanging of the left and right parts of the generator matrix.

We may now apply Algorithm 2.3.5 to find codewords of small weight in codes of length up to $n \leq 3928$. Thus, we prove the following result.

Theorem 2.3.15. *Let C be an extremal quadratic double circulant code of length n. Then* $n = 8, 24, 40, 88,$ *or* 136.

Proof. The proof essentially repeats that of Theorem 2.3.8. We construct all quadratic double circulant codes of length up to 3928 (see Theorem 1.1.10 (a)). Then, with Algorithm 2.3.5 in every code of length $n \neq 8, 24, 40, 88$, or 136 we find with MAGMA a codeword of weight smaller than $d = 4\left\lfloor \frac{n}{24} \right\rfloor + 4$, thus showing that the code is not extremal.

Note that for codes of smaller lengths we use direct enumeration. For larger codes we take the Sylow 2-subgroup of $\mathrm{PSL}(2, p) \times \mathbb{Z}_2$ as H. □

Below we give an example how a computation runs.

Example 2.3.16. Let C be a quadratic double circulant code of length $n = 3736 = 2 \cdot 1867 + 2$. We are searching for a codeword of weight smaller than $d = 624$.

As a subgroup H of $G = \mathrm{PSL}(2, 1867) \times \mathbb{Z}_2$ we take a Sylow 2-subgroup of G of order $2^3 = 8$. The subcode C^H is of dimension 234.

With the built-in MAGMA function `WordsOfBoundedWeight` we find in C^H a codeword of weight $616 < d$. This proves that C is not extremal.

The MAGMA code for this example may be found in Listing A.3 in Appendix A.

2.4 Extremal Type II extended cyclic codes

The goal of this section is to classify extremal Type II codes with automorphisms of large prime order. As we already mentioned in Section 2.2, an extremal code invariant under an automorphism of prime order larger than half of code's length is equivalent to an extended cyclic code.

Lemma 2.4.1. *Let C be an extremal Type II code of length* $n > 48$ *and let* σ *be its automorphism of prime order* $p > \frac{n}{2}$. *Then* $p = n - 1 = 24m + 8\ell - 1$, *where* $\ell \in \{0, 1\}$, *and C is equivalent to an extended odd-like duadic code.*

Proof. From Corollary 2.2.11 we know that $p = n - 1 = 24m + 8\ell - 1$, where $\ell \in \{0, 1\}$, and that σ is of type p-$(1, 1)$. Then it follows from Lemma 2.2.3 and Lemma 1.3.11 that C is equivalent to an extended odd-like duadic code. □

Remark 2.4.2. Note that we are only interested in extremal codes of length $n > 48$. As a matter of fact, all extremal Type II codes of lengths $n \leq 48$, $n \neq 40$, are classified (see Table 2.1), and those of length 40 do not admit automorphisms of prime order $p > \frac{n}{2}$ (see Huffman [39]).

What we are actually going to do in this section is to classify extremal extended odd-like duadic codes. More precisely, we are going to construct all odd-like duadic codes of prime lengths $p \equiv -1 \bmod 8$ with $p \leq 3927$ (see Theorem 1.1.10 (a)) and check, which of them have extremal extensions.

Throughout this section let C be an odd-like duadic code of prime length $p \equiv -1 \bmod 8$. It follows from Lemma 1.3.9 and Remark 1.3.10 that the idempotent of C is of the form

$$e(x) = \sum_{j \in S} x^j,$$

where S is one of the sets S_1 or S_2 that form a splitting of p. Recall from Section 1.3 that S is a disjoint union of nonzero cyclotomic cosets modulo p, and that nontrivial cyclotomic cosets modulo a prime p all have the same size $s(p)$, where $s(p)$ is the multiplicative order of 2 modulo p. Denote by $k = \frac{p-1}{s(p)}$ the number of nonzero cosets. We want to stress that k is even, since in our case $s(p)$ is odd, as we now prove.

Lemma 2.4.3. *For a prime p of the form $p \equiv -1 \bmod 8$ we have $s(p) \mid \frac{p-1}{2}$. In particular $s(p)$ is odd, since $\frac{p-1}{2}$ is odd.*

Proof. If $p \equiv -1 \bmod 8$ then the element $2 \in \mathbb{F}_p^*$ is a square modulo p (see [57, Chapter 16]). Let $a \in \mathbb{F}_p^*$ be such that $a^2 = 2$. By Fermat's little theorem we have $a^{p-1} \equiv 2^{\frac{p-1}{2}} \equiv 1 \bmod p$, which shows that $s(p)$ divides $\frac{p-1}{2}$. □

Let us consider the extreme case $s(p) = \frac{p-1}{2}$, when the number k of nonzero cyclotomic cosets is 2. We already pointed out in Example 1.3.12 that in the case of two nonzero cosets, the cosets form the only splitting of p. Hence, there are two (equivalent) odd-like duadic codes. These are actually the two quadratic residue codes. For future reference we formulate this as the following.

Lemma 2.4.4. *If p is a prime of the form $p \equiv -1 \bmod 8$ with $s(p) = \frac{p-1}{2}$ then up to equivalence there is only one self-dual extended cyclic code of length $p + 1$, namely, the extended quadratic residue code.*

Remark 2.4.5. Note that if $p = 24m - 1$ then $s(p) = \frac{p-1}{2}$ for all $m \leq 154$ except $m = 18$, 38, 46, 98, 112, and 133. If $p = 24m + 7$ with $m \leq 159$ then $s(p) = \frac{p-1}{2}$

in approximately half of the cases. Thus, many of the codes in question are extended quadratic residue codes, which have been classified in Theorem 2.3.8.

From now on we consider the general case, i.e., $s(p)$ is not necessarily equal to $\frac{p-1}{2}$. In order to construct all odd-like duadic codes we need to know all possible splittings of p. By a result of Pless et al. [67] we can assume that μ_{-1} is a multiplier that gives every splitting.

Lemma 2.4.6 ([67], see also [41, Section 6.4]). *If p is a prime with $p \equiv -1 \bmod 8$ then every splitting of p is given by the multiplier μ_{-1}.*

Note that the image of a cyclotomic coset $\mathcal{C}_t$, where $t \in \mathbb{F}_p^*$ is a coset representative, under μ_{-1} contains the element $-t$. Thus, without loss of generality, we can denote the k nonzero 2-cyclotomic cosets modulo p by

$$\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_{k/2}}, \mathcal{C}_{-i_1}, \ldots, \mathcal{C}_{-i_{k/2}},$$

where $\{\pm i_1, \ldots, \pm i_{k/2}\}$ is a transversal.

Let S_1 and S_2 be two sets that form a splitting of p given by μ_{-1}. If for some t a coset $\mathcal{C}_t$ lies in S_1, then the coset $\mathcal{C}_{-t}$ lies in S_2. Hence, each of the two sets S_1 and S_2 contains exactly one coset of every pair $\left\{\mathcal{C}_{i_j}, \mathcal{C}_{-i_j}\right\}$, $1 \leq j \leq \frac{k}{2}$, and it follows that the total number of odd-like duadic codes is $2^{k/2}$.

Combining the discussion above with Lemma 1.3.9 and Remark 1.3.10 we get the following.

Lemma 2.4.7. *Let C be an odd-like duadic code of prime length p with $p \equiv -1 \bmod 8$. Let furthermore*

$$\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_{k/2}}, \mathcal{C}_{-i_1}, \ldots, \mathcal{C}_{-i_{k/2}}$$

denote the k nonzero cyclotomic cosets modulo p (here $i_1, \ldots, i_{k/2}$ are distinct elements in $\mathbb{F}_p^*$). Then the generating idempotent of C is given by the formula

$$e(x) = \sum_{j \in S} x^j, \tag{2.5}$$

where S is a union of exactly $\frac{k}{2}$ cosets. Moreover, S satisfies the following condition:

$$\text{if for some } t \in \{\pm i_1, \ldots, \pm i_{k/2}\} \text{ the coset } \mathcal{C}_t \text{ is contained in } S\text{, then } \mathcal{C}_{-t} \not\subset S. \tag{2.6}$$

In particular, in total there are exactly $2^{k/2}$ odd-like duadic codes.

Corollary 2.4.8. *There are at least $\left\lceil \frac{2^{k/2}}{k} \right\rceil$ inequivalent odd-like duadic codes of length p, where $k = \frac{p-1}{s(p)}$ is the number of nonzero cyclotomic cosets.*

Proof. From Corollary 1.3.6 we know that two odd-like duadic codes of prime length are equivalent if and only if there is a multiplier μ_t with t in a transversal $\mathcal{T}$, such that it maps the idempotent of one code onto the idempotent of the other. Thus, there are at most k codes in an equivalence class. It follows that there are at least $\left\lceil \frac{2^{k/2}}{k} \right\rceil$ inequivalent codes. □

As we know from Lemma 2.4.4, the two quadratic residue codes are the only odd-like duadic codes if $s(p) = \frac{p-1}{2}$. As a matter of fact, quadratic residue codes always appear among duadic codes of prime lengths. It is readily seen that there are no other codes in their equivalence class.

Proposition 2.4.9. *The equivalence class of the two quadratic residue codes of length p contains no other cyclic codes.*

Proof. Let Q and N denote the sets of squares and nonsquares in $\mathbb{F}_p^*$. For every $r \in Q$ the multiplier μ_r leaves the two sets invariant; for every $n \in N$, μ_n interchages Q and N. The statement follows from Lemma 1.3.5 and the form of the generating idempotents of quadratic residue codes (see Definition 2.3.1). □

Below we describe how to compute the number of inequivalent odd-like duadic codes, using only elementary group theory.

Proposition 2.4.10. *The $k = \frac{p-1}{s(p)}$ nonzero cyclotomic cosets modulo a prime p form the cyclic group $\mathcal{G} = \mathbb{F}_p^*/\mathcal{C}_1$, where $\mathcal{C}_1$ is the cyclotomic coset containing the unity $1 \in \mathbb{F}_p^*$.*

Proof. It follows from Definition 1.3.3 that $\mathcal{C}_1$ is a cyclic group of order $s(p)$ and the other cyclotomic cosets are the left cosets of $\mathcal{C}_1$ in the group $\mathbb{F}_p^*$. Indeed, for any t in a transversal we can write $\mathcal{C}_t = t\mathcal{C}_1$. Hence, the k nonzero cyclotomic cosets form the quotient group $\mathcal{G} = \mathbb{F}_p^*/\mathcal{C}_1$. Finally $\mathcal{G}$ is cyclic, since both $\mathbb{F}_p^*$ and C_1 are cyclic. □

Lemma 2.4.11. *Let p be a prime of the form $p \equiv -1 \bmod 8$. Further, let $\mathcal{G}$ denote the group of k nonzero cyclotomic cosets modulo p. Then the equivalence classes of odd-like duadic codes of length p correspond to the orbits in the action of $\mathcal{G}$ on subsets $S \subset \mathcal{G}$ of cardinality $\frac{k}{2}$ that satisfy condition* (2.6). *In particular, the number of inequivalent codes depends only on the number k of nonzero cyclotomic cosets.*

Proof. Let $\mathcal{T}$ denote a transversal. Without loss of generality we may assume that $1 \in \mathcal{T}$. From Lemma 2.4.6 it follows that $-1 \in \mathcal{T}$.

Note that we can write

$$\mathcal{G} = \{\mathcal{C}_t \,|\, t \in \mathcal{T}\},$$

and that the multiplication in $\mathcal{G}$ may be considered as the action of a multiplier, since

$$\mathcal{C}_t \cdot \mathcal{C}_s = (t\mathcal{C}_1) \cdot (s\mathcal{C}_1) = (ts)\mathcal{C}_1 = \mathcal{C}_{ts} = \mathcal{C}_{t\mu_s} = \mathcal{C}_t\mu_s$$

for $t, s \in \mathcal{T}$.

Recall from Lemma 2.4.7 that the idempotents of odd-like duadic codes are given by the formula

$$e(x) = \sum_{j \in S} x^j,$$

where S is a union of exactly $\frac{k}{2}$ cosets that satisfies condition (2.6). Note that $\mathcal{G}$ acts on the idempotents via

$$e(x)\mathcal{C}_t := e(x)\mu_t = \sum_{j\in S} x^{jt} \pmod{x^p - 1} = \sum_{j\in S\mu_t} x^j \tag{2.7}$$

for $t \in \mathcal{T}$ (see Definition 1.3.4).

From (2.7) and Corollary 1.3.6 it follows that the equivalence classes of odd-like duadic codes of length p correspond to the orbits in the action of $\mathcal{G}$ on subsets $S \subset \mathcal{G}$ of cardinality $\frac{k}{2}$ that satisfy condition (2.6). □

Remark 2.4.12. Instead of the group $\mathcal{G}$ of nonzero cyclotomic cosets modulo p in Lemma 2.4.11 we can use any cyclic group G of order $k = \frac{p-1}{s(p)}$. In this case condition (2.6) has to be replaced by the following condition:

$$\text{if some } g \in \mathcal{G} \text{ lies in } S \text{ then } gh \notin S, \tag{2.8}$$

where h is a unique element of order 2 in G. This is justified, because

$$\mathcal{C}_{-t} = \mathcal{C}_t \cdot \mathcal{C}_{-1}$$

in the group $\mathcal{G}$, and $\mathcal{C}_{-1}$ is a unique element of order 2 in $\mathcal{G}$.

Notice that Lemma 2.4.4 can be obtained as a corollary of Lemma 2.4.11. Below we apply Lemma 2.4.11 and Remark 2.4.12 in case of $k = 6$ cosets.

Corollary 2.4.13. *If $s(p) = \frac{p-1}{6}$ for a prime $p \equiv -1 \bmod 8$, then there are two equivalence classes of odd-like duadic codes of length p.*

Proof. If $s(p) = \frac{p-1}{6}$ then there are $k = 6$ nonzero cyclotomic cosets modulo p and the group $\mathcal{G}$ is of order 6. By Remark 2.4.12 we can consider any cyclic group of order 6, e.g.,

$$G = \left\{1, g, g^2, g^3, g^4, g^5\right\}.$$

Here g^3 is a unique element of order 2. Then the 8 subsets of G of cardinality $\frac{k}{2}$ that satisfy condition (2.8) are as follows:

$$\begin{aligned}
S_1 &= \{1, g, g^2\},\\
S_2 &= \{1, g, g^5\},\\
S_3 &= \{1, g^2, g^4\},\\
S_4 &= \{1, g^4, g^5\},\\
S_5 &= \{g, g^2, g^3\},\\
S_6 &= \{g, g^3, g^5\},\\
S_7 &= \{g^2, g^3, g^4\},\\
S_8 &= \{g^3, g^4, g^5\}.
\end{aligned}$$

It is an easy verification that there are indeed two orbits in the action of G on these subsets, namely,

$$\begin{aligned} S_1G &= \{S_1, S_5, S_7, S_8, S_4, S_2\} \text{ and} \\ S_3G &= \{S_3, S_6\}. \end{aligned}$$

The statement follows now from Lemma 2.4.11 and Remark 2.4.12. □

We have everything we need to start the classification of extremal Type II extended cyclic codes. First recall that if $s(p) = \frac{p-1}{2}$ then it follows from Lemma 2.4.4 that the only codes are extended quadratic residue codes and they are already classified by Theorem 2.3.8.

Let $s(p) < \frac{p-1}{2}$ and thus $k > 2$. By Corollary 2.4.8 we have to consider at least $\left\lceil \frac{2^{k/2}}{k} \right\rceil$ inequivalent odd-like duadic codes. As in Section 2.3 we search for small weight codewords in each of the codes to show their non-extremality. From Lemma 1.3.7 we know that a duadic code of length p is invariant under a group $G < \mathrm{S}_p$ of order $p \cdot s(p)$. Clearly, the same group G acts on the extended code and leaves it invariant. We only have to embed G in S_{p+1} in such a way that the added coordinate is a fixed point for all permutations in G. With this information at hand we can apply Algorithm 2.3.5. We want to remark that in Section 2.5 we discuss when the automorphism group of an extended odd-like duadic code can be bigger than G.

Note that there is much less information about the automorphism group, compared to the case of quadratic residue codes. Because of that we are not able to classify extremal extended cyclic codes completely. However we do classify all codes of lengths up to one thousand, and there are only two open cases for lengths between 1000 and 2000. More precisely, we have the following result.

Theorem 2.4.14. *Extremal Type II extended cyclic codes of length $n = p + 1$, where p is a prime, can exist only in one of the following cases:*

(i) for $p = 7, 23, 47, 79$ and 103 there is exactly one such code up to equivalence;

(ii) for $p = 31$ there are exactly two inequivalent codes;

(iii) for $p = 1399, 2383, 2767, 3343, 3463,$ or 3607 there might exist only one code up to equivalence;

(iv) for $p = 1103, 2351, 2687, 3191,$ or 3391 there might exist several inequivalent extremal codes.

Proof. For the five lengths in (i) we have $s(p) = \frac{p-1}{2}$, and it follows from Lemma 2.4.4 that there are no other duadic codes apart from quadratic residue codes. Extended quadratic residue codes of length $p + 1$ for p in (i) are extremal by Theorem 2.3.8.

It is known (see Section 2.1) that there are five extremal codes of length 32. Two of them, namely, the quadratic residue code and the second order Reed-Muller code, are extended cyclic. Thus (ii) follows.

For all lengths in (iii) we have $s(p) = \frac{p-1}{6}$. Therefore, by Corollary 2.4.13 there are two inequivalent odd-like duadic codes. By Proposition 2.4.9 one of them is the quadratic residue code, and the extended code is not extremal by Theorem 2.3.8. Hence, only one possible code remains.

For all of the cases in (iv) we have $k = \frac{p-1}{s(p)} \geq 30$ and it follows from Corollary 2.4.8 that the number of inequivalent codes is greater than one.

Let p be one of the primes of the form $p = 24m + 8\ell - 1 \leq 3827$, where $\ell \in \{0, 1\}$ and $s(p) > \frac{p-1}{2}$, that are not listed in cases (i)–(iv). (Recall from Theorem 1.1.10 (a) that extremal Type II codes do not exist for lengths greater than 3928.) Using Lemma 2.4.7 we construct all self-dual extended cyclic codes of length $n = p + 1$. In each of the codes we find a word of weight less than $4m + 4$ (either by a direct search or using Algorithm 2.3.5), thus showing that none of them is extremal.

All computations are carried out with Magma. □

Remark 2.4.15. For all primes p in Theorem 2.4.14 (iii) $s(p)$ is also a prime. Hence, the group G of order $p \cdot s(p)$ has only two nontrivial subgroups, namely, H_1 of order p and H_2 of order $s(p)$. Algorithm 2.3.5 fails to find codewords of small weight when using either one of the subgroups H_1 or H_2, since the dimensions of the subcodes C^{H_1} and C^{H_2} are too small.

For the primes $p = 1103$, 2687, and 3391 in Theorem 2.4.14 (iv) we have $s(p) = 29$, 79, and 113, respectively, which are all primes. We applied Algorithm 2.3.5 to all extended cyclic codes of length $p + 1$ with a subgroup H of order $s(p)$. However, for some of the codes of this lengths the algorithm failed to return a codeword of small weight.

If $p = 2351$, we have $s(p) = 47$, also a prime. From Corollary 2.4.8 it follows that there are at least 671 089 inequivalent duadic codes of this length. The estimated running time of Algorithm 2.3.5 for this number of codes on our computer (2.80 GHz) is approximately one and a half years. We suppose that, similar to the cases in the previous paragraph, the algorithm is likely not to find small-weight codewords for all codes in question.

Finally, for $p = 3191$ there at least 9 256 396 inequivalent codes by Corollary 2.4.8. We are not able to find a way to construct all of them in a reasonable amount of time.

Example 2.4.16. We want to construct all extended cyclic codes of length $n = 912$, and show that all of them are not extremal.

For $p = 911$ we have $s(p) = 91 = 7 \cdot 13$. As a subgroup H in Algorithm 2.3.5 we use the cyclic group of order 13.

We begin by computing the $k = \frac{p-1}{s(p)} = 10$ nonzero cyclotomic cosets modulo p and choosing a transversal. After that, we construct all sets S of cardinality $\frac{k}{2} = 5$ that satisfy condition (2.6) (see Lemma 2.4.7). For each of such sets S we do the following.

First, we construct an idempotent, which is given by (2.5). Then, with a built-in MAGMA function `CyclicCode` from the idempotent we construct a code C. Finally, we find a codeword of weight smaller than $d = 156$ in the subcode C^H, thus showing that C is not extremal.

The MAGMA code for this example may be found in Listing A.4 in Appendix A.

Recall from Lemma 2.4.1 that an extremal Type II code, which is invariant under an automorphism of large prime order (that is, p is bigger than half of code's length), is equivalent to an extended cyclic code. Thus, Theorem 2.4.14 provides some strong evidence that the following conjecture might hold true.

Conjecture 2.4.17. *Let C be an extremal Type II code of length n with an automorphism of prime order $p > \frac{n}{2}$. Then $n = 8, 24, 32, 48, 80,$ or 104.*

2.5 Automorphism groups of binary extended duadic codes

In this section we consider when the automorphism group of an extended odd-like duadic code can be bigger than the group of the original, nonextended code. We only consider binary codes in this section.

Proposition 2.5.1. *Let C be a cyclic code with extension $\widehat{C}$. If $\widehat{C}$ has an automorphism that does not fix the new coordinate, then $\mathrm{Aut}(\widehat{C})$ is 2-transitive.*

Proof. First, observe that by definition, a cyclic code C of length n is invariant under a cyclic shift σ of order n, hence $\mathrm{Aut}(C)$ is transitive. Now, denote the coordinates of $\widehat{C}$ by $0, 1, \ldots, n-1, \infty$ and let $\tau \in \mathrm{Aut}(\widehat{C})$ be such that $\tau(\infty) \neq \infty$. Note that we consider σ acting on the coordinates of $\widehat{C}$ in such a way that ∞ is a fixed point of σ. It follows that the group $G \leq \mathrm{Aut}(\widehat{C})$, generated by σ and τ, is transitive on the set of coordinates $\{0, 1, \ldots, n-1, \infty\}$. Moreover, the stabilizer G_∞ of the new coordinate contains $\langle\sigma\rangle$. Consequently, the group G, and hence $\mathrm{Aut}(\widehat{C})$, is 2-transitive. □

Some families of extended cyclic codes with 2-transitive groups were known for a very long time, e.g., Reed-Muller codes or quadratic residue codes. Recall from Section 2.1 that both of these families provide examples of extremal Type II codes.

Among extended cyclic codes of particular interest are self-dual codes. From Lemma 1.3.11 we know that a cyclic code with a self-dual extension is necessarily a duadic code. An attempt to classify extended duadic codes with 2-transitive groups was already made in [53] in a special case. However, due to an error in the proof, this classification was not complete. Later Ito [48] extended the classification to the general case, still without addressing the error in [53].

We state what was proved as the following result.

Lemma 2.5.2 ([48] and [53]). *Let C be an extended duadic code of length n. If* $\mathrm{Aut}(C)$ *is* 2*-transitive then one of the following holds*

(i) $n = 2^m$ *for some m and* $\mathrm{Aut}(C) \leq \mathrm{AGL}(m, 2)$ *or*

(ii) $n = p + 1$, *where p is a prime, and* $\mathrm{PSL}(2, p) \leq \mathrm{Aut}(C)$.

In [53] the authors claimed that part (ii) of Lemma 2.5.2 leads to a unique code, namely, the extended quadratic residue code. Although their proof of this fact was incorrect, the claim is actually true by an older result of Knapp and Schmid [51].

Lemma 2.5.3 ([51]). *Let C be a binary code of length $p + 1$, where p is an odd prime. Moreover, let C be invariant under the group* $\mathrm{PSL}(2, p)$. *Then* $p \equiv \pm 1 \bmod 8$ *and C is an extended quadratic residue code.*

Combining Lemma 2.5.2 and Lemma 2.5.3 we get the following.

Corollary 2.5.4. *Let C be an extended duadic code of length n. If* $\mathrm{Aut}(C)$ *is* 2*-transitive then one of the following holds*

(i) $n = 2^m$ *for some m and* $\mathrm{Aut}(C) \leq \mathrm{AGL}(m, 2)$ *or*

(ii) C is an extended quadratic residue code.

Recall that extremal extended quadratic residue codes are classified in Theorem 2.3.8. In the next section we finish the classification of extremal extended cyclic codes with 2-transitive groups. We will consider the case when the automorphism group is a subgroup of $\mathrm{AGL}(m, 2)$.

2.6 Extremal binary affine-invariant codes

From Corollary 2.5.4 we know that there are two classes of binary extended duadic codes with 2-transitive automorphism groups. In this section we consider case (i) of Corollary 2.5.4, namely, codes of length a power of 2 that are invariant under a 2-transitive subgroup of $\mathrm{AGL}(m, 2)$. Below we show that these are exactly the so-called *affine-invariant* codes.

Definition 2.6.1. A self-dual extended cyclic code of length 2^m, where $m \geq 3$, that is invariant under the group $\mathrm{AGL}(1, 2^m) = \{v \mapsto av + b \mid v, a, b \in \mathbb{F}_{2^m}, a \neq 0\}$ is called *affine-invariant*.

Remark 2.6.2. Denote by T a group of translations $v \mapsto v + a$, where $v, a \in \mathbb{F}_2^m$. Then the group $\mathrm{AGL}(1, 2^m)$ is isomorhic to $T \rtimes \langle \sigma \rangle$, where σ is a cyclic shift of order $2^m - 1$ with $\sigma : i \mapsto i + 1 \bmod 2^m - 1$.

Lemma 2.6.3. *Let C be a self-dual extended duadic code of length $n = 2^m$ for $m \geq 3$ and let $\mathrm{Aut}(C) \leq \mathrm{AGL}(m, 2)$ be 2-transitive. Then C is equivalent to an affine-invariant code.*

Proof. Let $T \leq \mathrm{AGL}(m, 2)$ denote the group of translations of order 2^m. From Lemma 1.2.1 (iii) we know that $\mathrm{Aut}(C)$ is an extension $T \rtimes H$ of T by a subgroup $H \leq \mathrm{GL}(m, 2)$, where H acts transitively on $2^m - 1$ points. Let $\sigma \in \mathrm{S}_n$ denote a cyclic shift of order $n - 1$ with $\sigma : i \mapsto i + 1 \bmod n - 1$. Since C is an extended cyclic code we have $\sigma \in \mathrm{Aut}(C)$. As $\mathrm{Aut}(C) = T \rtimes H$ and all elements of T have order 2, we obtain that σ lies in a conjugate of H. In particular, a conjugate of $T \rtimes \langle \sigma \rangle$ is a subgroup of $\mathrm{Aut}(C)$. By Remark 2.6.2, $T \rtimes \langle \sigma \rangle = \mathrm{AGL}(1, 2^m)$, and hence C is equivalent to an affine-invariant code. □

The aim of this section is to classify all extremal affine-invariant codes. Since affine-invariant codes exist for lengths $n = 2^m$, it follows from Lemma 1.3.11 that they are always of Type II. Note that we only have to consider the cases, where $m \leq 11$, since by Theorem 1.1.10 (a) extremal Type II codes do not exist for lengths greater than 3928. Moreover, for even m affine-invariant codes do not exist by the following well-known fact.

Lemma 2.6.4. *Self-dual extended cyclic codes do not exist for lengths 2^{2k} with $k > 1$.*

Proof. Note that the lemma is folklore. We provide one of the possible elementary proofs.

Let C be a cyclic code of length n with a self-dual extension. It follows from Lemma 1.3.11 that C is a duadic code. From Section 1.3 we know that all primes p_i in the factorization $n = p_1^{a_1} \cdots p_r^{a_r}$ are of the form $p_i \equiv \pm 1 \bmod 8$.

Suppose that $n = 2^{2k} - 1$. Then $n \equiv (-1)^{2k} - 1 \equiv 0 \bmod 3$. Hence n is divisible by 3, a contradiction. □

Therefore, in order to classify extremal affine-invariant codes we need to construct all such codes of lengths 8, 32, 128, 512, and 2048 and check, which of them have minimum distance 4, 8, 24, 88, and 388, respectively.

A way to construct all affine-invariant codes was suggested by Charpin and Levy-dit-Vehel [17]. More precisely, they give a combinatorial method to construct defining sets of all cyclic codes with affine-invariant extensions. For reader's convenience and since it is essential in our classification we repeat their construction here.

Let $n = 2^m - 1$ for odd $m \geq 3$ and let α be an n-th root of unity. For an element $s \in \mathbb{Z}_n$ we define the 2-*weight* of s as a number of nonzero coefficients in the binary expansion of s. This means that if we write

$$s = \sum_{i=0}^{m-1} s_i 2^i, \tag{2.9}$$

where each of the s_i is either 0 or 1, then

$$\mathrm{wt}_2(s) = |\{ i \,|\, 0 \leq i \leq m-1 \text{ and } s_i \neq 0 \}| .$$

Notice that the 2-weight is constant on cyclotomic cosets modulo n, hence we may speak of the 2-weight of a coset.

We know from Lemma 1.3.14 that for an odd $m \geq 3$ the Reed-Muller code $\mathcal{R}(\frac{m-1}{2}, m)$ is equivalent to an extended cyclic code. The defining set of this cyclic code can be found using the 2-weight.

Lemma 2.6.5 (see [57, Chapter 13]). *Let $m \geq 3$ be odd and let C be a cyclic code of length $n = 2^m - 1$ such that the extended code $\widehat{C}$ is equivalent to the Reed-Muller code $\mathcal{R}(\frac{m-1}{2}, m)$. Then the defining set T of the code C is given by the formula*

$$T = \left\{ s \in \mathbb{Z}_n \,\middle|\, \mathrm{wt}_2(s) \leq \frac{m-1}{2} \right\}.$$

Let $\lessdot$ denote the partial order, which we define on $\mathbb{Z}_n$ in the following way: $s \lessdot t$ if and only if $s_i \leq t_i$ for all $0 \leq i \leq m-1$, where s_i and t_i are the coefficients of the binary expansions of s and t, respectively. Denote the set of predecessors of an element $t \in \mathbb{Z}_n$ with respect to the partial order $\lessdot$ by $\Delta(t)$, i.e.,

$$\Delta(t) = \{ s \in \mathbb{Z}_n \,|\, s \lessdot t \} .$$

For a subset $I \subseteq \mathbb{Z}_n$ we set

$$\Delta(I) = \bigcup_{t \in I} \Delta(t).$$

The following description of the defining sets of affine-invariant codes is due to Kasami et al. [50].

Lemma 2.6.6 ([50]). *Let C be an extended cyclic code with defining set T. Then C is affine-invariant if and only if $\Delta(T) = T$.*

Unfortunately, it is a difficult task to find all sets that satisfy the condition in Lemma 2.6.6. Below we present a more computer-friendly method to construct all defining sets. The method is due to Charpin and Levy-dit-Vehel [17].

Lemma 2.6.7 ([17]). *Let m be odd and let R be the number of cyclotomic cosets $\mathcal{C}$ modulo $2^m - 1$ of 2-weight $\frac{m-1}{2}$ that satisfy the following condition:*

$$\text{if } s, s' \in \mathcal{C} \text{ then } s' \notin \Delta(-s). \tag{2.10}$$

Furthermore, let S_k denote a union of all cyclotomic cosets of 2-weight k. Then an extended cyclic code of length 2^m is affine-invariant if and only if its defining set T is of the form

$$T = S_1 \cup \cdots \cup S_{\frac{m-3}{2}} \cup S_{\frac{m-1}{2}} \setminus \left(\bigcup\nolimits_{i=1}^{r} \mathcal{C}_{s_i} \right) \cup \left(\bigcup\nolimits_{i=1}^{r} \mathcal{C}_{-s_i} \right), \qquad (2.11)$$

where $0 \le r \le R$, $\mathrm{wt}_2(\mathcal{C}_{s_i}) = \frac{m-1}{2}$ and the union $\bigcup_{i \le r} \mathcal{C}_{s_i}$ satisfies condition (2.10).

Remark 2.6.8. Note that the defining set T of the Reed-Muller code $\mathcal{R}(\frac{m-1}{2}, m)$ (see Lemma 2.6.5) is also given by (2.11), where $r = 0$, i.e.,

$$T = \bigcup_{k \le \frac{m-1}{2}} S_k.$$

Remark 2.6.9. As a matter of fact, in order to construct all defining sets of the form (2.11) one does not need to verify condition (2.10) for all possible unions of cyclotomic cosets of 2-weight $\frac{m-1}{2}$. Instead, this can be done recursively along the following lines (see [17]).

Denote by $\mathcal{I}_1$ the set of representatives of the cyclotomic cosets of 2-weight $\frac{m-1}{2}$ that satisfy condition (2.10), i.e.,

$$\mathcal{I}_1 = \left\{ s \,\middle|\, \mathrm{wt}_2(s) = \tfrac{m-1}{2} \text{ and } \mathcal{C}_s \text{ satisfies (2.10)} \right\}.$$

Next, construct the set of pairs

$$\mathcal{I}_2 = \{ \{s, t\} \mid s, t \in \mathcal{I}_1 \text{ and } \mathcal{C}_s \cup \mathcal{C}_t \text{ satisfies (2.10)} \}.$$

Notice that to construct the set $\mathcal{I}_3$ of triples one only requires information from $\mathcal{I}_2$, not $\mathcal{I}_1$. More precisely, if for some triple $\{s, t, r\}$ the union $\mathcal{C}_s \cup \mathcal{C}_t \cup \mathcal{C}_r$ satisfies condition (2.10) then all three unions $\mathcal{C}_s \cup \mathcal{C}_t$, $\mathcal{C}_t \cup \mathcal{C}_r$, and $\mathcal{C}_s \cup \mathcal{C}_r$ also satisfy (2.10). In other words, we have

$$\mathcal{I}_3 = \left\{ \{s, t, r\} \,\middle|\, s, t, r \in \bigcup \mathcal{I}_2 \text{ and } \mathcal{C}_s \cup \mathcal{C}_t \cup \mathcal{C}_r \text{ satisfies (2.10)} \right\},$$

where $\bigcup \mathcal{I}_2 = \bigcup_{I \in \mathcal{I}_2} I$ is the set of distinct representatives that can occur in elements of $\mathcal{I}_2$. Furthermore, we can recursively define

$$\mathcal{I}_k = \left\{ \{s_1, \ldots, s_k\} \,\middle|\, s_1, \ldots, s_k \in \bigcup \mathcal{I}_{k-1} \text{ and } \bigcup\nolimits_{i=1}^{k} \mathcal{C}_{s_i} \text{ satisfies (2.10)} \right\}.$$

Note that we need to construct the sets $\mathcal{I}_k$ only for $k \le r \le |\mathcal{I}_1|$, such that the set $\mathcal{I}_{r+1}$ is empty. This means that the unions of more than r cyclotomic cosets of 2-weight $\frac{m-1}{2}$ do not satisfy condition (2.10).

Finally let $\mathcal{I}$ be the union of all constructed sets $\mathcal{I}_i$, $i \le r$. For uniformity we put

$$\mathcal{I} = \{\emptyset\} \cup \{ \{s\} \mid s \in \mathcal{I}_1 \} \cup \mathcal{I}_2 \cup \cdots \cup \mathcal{I}_r.$$

Observe that there is one-to-one correspondence between the elements of $\mathcal{I}$ and different defining sets of the form (2.11). (By the previous remark, the empty set corresponds to the defining set of the Reed-Muller code).

We provide our implementation of the algorithm described in Remark 2.6.9 in Listing A.5 in Appendix A for the case $n = 512$. Note that for $n = 512$ the set $\mathcal{I}_4$ from Remark 2.6.9 will be empty (see also [17]). Therefore, we only need to construct the sets $\mathcal{I}_1$, $\mathcal{I}_2$, and $\mathcal{I}_3$.

With Lemma 2.6.7 and Remark 2.6.9 we are ready to classify extremal affine-invariant codes.

Theorem 2.6.10. *Let C be an extremal affine-invariant code. Then C is either the $[8, 4, 4]$ Hamming code or the $[32, 16, 8]$ second order Reed-Muller code.*

Proof. It follows from Theorem 1.1.10 (a) and Lemma 2.6.4 that we only need to consider codes of length 2^m with $m = 3$, 5, 7, 9, and 11. From Section 2.1 we know all extremal codes of lengths 8 and 32. Only two codes among them, namely, the Hamming code of length 8 and the second order Reed-Muller code of length 32, are affine-invariant. In the case $m = 7$ we can use Theorem 2.4.14, since $2^m - 1 = 127$ is a prime and affine-invariant codes are extended cyclic. Therefore, there are no extremal affine-invariant codes of length 128.

As 511 and 2043 are not primes, we can not use Theorem 2.4.14 for the cases $m = 9$ and 11. Nevertheless, we can construct all affine-invariant codes of lengths 512 and 2048 with Lemma 2.6.7 and Remark 2.6.9. We find that there are 70 codes of length 512, which agrees with [17], and 515 617 codes of length 2048. Then to each of the constructed codes we can apply Algorithm 2.3.5 to search for codewords of small weights. It appeared that none of the affine-invariant codes of these lengths is extremal.

The computations are carried out with Magma. □

2.7 Extremal Type II codes invariant under 2-transitive extensions of elementary abelian groups

In this section we continue to study extremal Type II codes with 2-transitive automorphism groups. However, we will be no longer restricted to the case of extended cyclic codes.

Let C be an extremal Type II code invariant under a 2-transitive group G and let T denote the socle of G. From Lemma 1.2.1 (i) we know that T is either elementary abelian or simple. In this section we consider the first possibility, i.e., T is elementary abelian, and prove the following result.

Theorem 2.7.1. *Let C be an extremal Type II code of length n. Then C is invariant under a 2-transitive group with elementary abelian socle if and only if one of the following holds*

(i) $n = 8$ *and C is equivalent to the Hamming code,*

(ii) $n = 32$ *and C is equivalent to the second order Reed-Muller code,*

(iii) possibly $n = 1024$ *and* C *is invariant under the group* $T \rtimes \mathrm{SL}(2, 2^5)$*, where* T *is the group of translations of the vector space* $\mathbb{F}_2^{10}$*.*

To prove Theorem 2.7.1 we first need to gather some information about the group G.

Proposition 2.7.2. *Let* C *be an extremal Type II code of length* n *invariant under a* 2*-transitive group* G *with the elementary abelian socle* T*. Then* $n = 2^m$ *for some* $m \leq 11$ *and* $G = T \rtimes H$*, where* H *is a subgroup of* $\mathrm{GL}(2, m)$ *that acts transitively on* $2^m - 1$ *points. Moreover,* T *is a group of translations of the vector space* $\mathbb{F}_2^m$*.*

Proof. Recall from Section 1.2 that the degree of G equals the length of the code C. From Corollary 1.4.2 it follows that the degree n of G is divisible by 8. Since the socle T of G is elementary abelian, we have that n is a prime power. Hence $n = 2^m$ for some integer $m \geq 3$, and $m \leq 11$ by Theorem 1.1.10 (i). From Lemma 1.2.1 (ii) it follows that $G \leq \mathrm{AGL}(m, 2)$ and T is the group of translations of the vector space $\mathbb{F}_2^m$.

Furthermore, by Lemma 1.2.1 (iii) every 2-transitive subgroup G of $\mathrm{AGL}(m, 2)$ is an extension of T by a suitable transitive subgroup of the general linear group $\mathrm{GL}(m, 2)$. Therefore, we may write $G = T \rtimes H$, where $H \leq \mathrm{GL}(m, 2)$ acts transitively on $2^m - 1$ points. □

Information on transitive subgroups of the general linear group can be found in [44, Chapter XII, 7.5]. For reader's convenience we repeat this result here.

Lemma 2.7.3 ([44, Chapter XII, 7.5])**.** *Let* $H \leq \mathrm{GL}(m, 2)$ *act transitively on* $2^m - 1$ *points. If* m *is a prime then* H *contains a cycle of order* $(2^m - 1)$*. If* $m = kr$ *for* $k > 1$ *and* $r > 1$*, then one of the following possibilities holds for* H*:*

(i) H *contains a cycle of order* $(2^m - 1)$ *for all* m*;*

(ii) $\mathrm{SL}(k, 2^r) \leq H$ *for all* k *and* r*;*

(iii) $\mathrm{Sp}(k, 2^r) \leq H$ *for even* k*;*

(iv) $\mathrm{G}_2(2) \leq H$ *for* $m = 6$*;*

(v) $H \cong \mathrm{PSU}(3, 3^2)$ *for* $m = 6$*;*

(vi) $H \cong \mathrm{A}_6$ *for* $m = 4$*;*

(vii) $H \cong \mathrm{A}_7$ *for* $m = 4$*.*

We are now ready to prove Theorem 2.7.1.

Proof of Theorem 2.7.1. Let $G = \mathrm{Aut}(C)$ and let T denote the elementary abelian socle of G. It follows from Proposition 2.7.2 that $n = 2^m$ for some $m \leq 11$. Besides, T is a group of translations of the vector space $\mathbb{F}_2^m$ and $G = T \rtimes H$, where H is a subgroup of $\mathrm{GL}(m, 2)$ that acts transitively on $2^m - 1$ points. The possibilities for H are listed in Lemma 2.7.3.

First we consider the case when H contains a cycle of order $2^m - 1$. It follows from Lemma 2.2.3 and Remark 2.2.4 that C is equivalent to an extended cyclic code, which is affine-invariant by Definition 2.6.1. Finally, from Theorem 2.6.10 it follows that up to equivalence C is either the Hamming code of length 8 or the second order Reed-Muller code of length 32.

Now, suppose that H does not contain a cyclic shift of order $2^m - 1$, i.e., C is not an extended cyclic code. It follows from Lemma 2.7.3 that m is not a prime. Hence, we may write $m = kr$ for some integers $k, r > 1$.

Next, we check whether a group $G = T \rtimes H$, where H is given by one of the cases (ii) to (vi) of Lemma 2.7.3, may occur as an automorphism group of a Type II code C of length $n = 2^m$. In order to do this we exploit the structure of C and the ambient space $\mathbb{F}_2^n$ as $\mathbb{F}_2G$-modules. In particular, from Proposition 1.2.2 we know that C is a submodule of $\mathbb{F}_2^n$ of dimension $\frac{n}{2}$. For each H from Lemma 2.7.3, cases (ii) to (vi), we construct all G-modules of dimension $\frac{n}{2}$. Then, for every such module C we check whether it is self-dual as a code.

Recall that $n = 2^m$ with $m \leq 11$. If m is even, then the only cases, for which there exist $\frac{n}{2}$-dimensional $\mathbb{F}G$-modules, are $H \cong \mathrm{SL}(2, 2^r)$, where $r = 4$ or 5. For $r = 4$ we get more than 50 000 modules, but none of them is a self-dual code. For $r = 5$ the number of modules is even bigger, and we are unable to find a way to construct all of them in a reasonable amount of time.

Apart from the case $H \cong \mathrm{SL}(2, 2^5)$, for which we can not prove the desired result, the only group from Lemma 2.7.3, cases (ii) to (vi), that admits self-dual codes is $H \cong \mathrm{SL}(3, 2^3)$ for $m = 9 = 3 \cdot 3$. In this case there are exactly three Type II codes of length 512 invariant under $T \rtimes \mathrm{SL}(3, 2^3)$. One of them is the Reed-Muller code $\mathcal{R}(4, 9)$. By Lemma 1.3.14 the code $\mathcal{R}(4, 9)$ has minimum distance 32 and is, therefore, not extremal. Using Algorithm 2.3.5 we check that the other two codes are not extremal either.

Thus, if H does not contain a cycle of order $2^m - 1$ then C might exist only if $H \cong \mathrm{SL}(2, 2^5)$. This completes the proof of Theorem 2.7.1.

All computations are carried out with MAGMA. □

Example 2.7.4. We want to find all extremal Type II codes of length $n = 2^9 = 512$ that are invariant under a group $G = T \rtimes \mathrm{SL}(3, 2^3)$, where T is elementary abelian of order n.

First, using the built-in MAGMA function `Subgroups` we construct G as a subgroup of $\mathrm{AGL}(9, 2)$ of order $2^9 \cdot 16\,482\,816$. With a function `Submodules` we find all submodules M of the ambient space $\mathbb{F}_2^n$, which is considered as an $\mathbb{F}_2G$-module, such that $\dim M = \frac{n}{2}$. For each of these submodules M we check if it is self-dual and doubly-even as a code C. If this is the case then we search for a small weight codeword in the code C.

It appears that there are exactly three Type II codes of length 512 invariant under G, and none of these codes is extremal.

The MAGMA code for this example may be found in Listing A.6 in Appendix A.

Based on the results of this section we want to mention an interesting observation. By Lemma 2.7.3 extended cyclic self-dual codes of length $n = 2^m$ exist only for odd m. But even if we drop the requirement that the code is extended cyclic, there are still no self-dual codes invariant under a 2-transitive group with elementary abelian socle for even $m < 10$. Furthermore, for odd m, the only transitive subgroups of $\mathrm{GL}(m, 2)$ apart from the cyclic groups are $\mathrm{SL}(k, 2^r)$, where $m = kr$ with $k > 1$ and $r > 1$.

We conclude this section with an open problem.

Conjecture 2.7.5. *Let C be a Type II code of length 2^m invariant under a 2-transitive automorphism group G with elementary abelian socle T. Then m is odd and one of the following holds true*

(i) $\mathrm{AGL}(1, 2^m) \leq G$*, and C is affine-invariant, or*

(ii) $T \rtimes \mathrm{SL}(k, 2^r) \leq G$*, where $m = kr$ and $k, r > 1$.*

2.8 Extremal Type II codes with 2-transitive automorphism groups

In this section we finish the classification of extremal Type II codes with 2-transitive automorphism groups and prove one of the main results of the thesis. This result was published in [58].

Theorem 2.8.1. *Let C be an extremal Type II code of length n. If* $\mathrm{Aut}(C)$ *is 2-transitive, then one of the following holds.*

(i) $n = 8, 24, 32, 48, 80,$ *or* 104*, and C is equivalent to an extended quadratic residue code,*

(ii) $n = 32$ *and up to equivalence C is the second order Reed-Muller code,*

(iii) possibly $n = 1024$ *and C is invariant under the group* $T \rtimes \mathrm{SL}(2, 2^5)$*, where T is the group of translations of the vector space* $\mathbb{F}_2^{10}$*.*

Let C be an extremal Type II code of length n invariant under a 2-transitive automorphism group G with a socle T. Recall from Lemma 1.2.1 (i) that T is either elementary abelian or simple. We considered the case when T is elementary abelian in the previous section. So, let in the following T be simple.

First, we deal with the case that T is the alternating group A_n.

Lemma 2.8.2. *No Type II code of length $n \geq 8$ is invariant under* A_n*.*

A more general result was already proven in [51], where the authors used advanced representation theoretical methods. Here we present a short, pure coding theoretical proof.

Proof of Lemma 2.8.2. Let C be a Type II code and assume that $\mathrm{A}_n \leq \mathrm{Aut}(C)$. Since C is doubly-even, the minimum distance of C is at least 4.

Fix a codeword c of C. Let i_0 denote a coordinate position, in which c has a zero, i.e., $c_{i_0} = 0$. Let i_1 and i_2 be positions, in which c has ones. The cycle $\tau = (i_0, i_1, i_2)$ of order 3 is in A_n, hence $c\tau \in C$. Notice that the codeword $c + c\tau \in C$ has ones in positions i_0 and i_1 and zeros in all other positions. Hence $\mathrm{wt}(c + c\tau) = 2$, a contradiction. □

The following result is the classification of extremal Type II codes with 2-transitive groups in the case when the socle T is simple.

Theorem 2.8.3. *Let C be an extremal Type II code of length n. Further, let $G = \mathrm{Aut}(C)$ be 2-transitive and let the socle T of G be simple. Then $n = 8$, 24, 32, 48, 80, or 104 and C is equivalent to an extended quadratic residue code.*

Proof. First, we consider the case when $p = n - 1$ is a prime. Since the group G is 2-transitive, it contains an element of order p. It follows from Lemma 2.2.3 that C is equivalent to an extended cyclic code. Moreover C is equivalent to an extended quadratic residue code by Corollary 2.5.4. (Note that part (i) of Corollary 2.5.4 can not happen, since in that case the socle of the automorphism group is elementary abelian.) Finally, from Theorem 2.3.8 it follows that $n = 8$, 24, 32, 48, 80, or 104.

Now, let $n - 1$ be a composite number. Note that in this case C is not necessarily equivalent to an extended cyclic code.

All simple groups that can occur as a socle T of a 2-transitive group are known (see [15]). For reader's convenience we list the possibilities in Table 2.2. The first column of the table contains groups names; the degree a of 2-transitive representation is in the second column. The degree of transitivity of a given group T is the third column. Note that the number in parentheses is the highest possible degree of transitivity for any group that contains T as a socle.

It follows from Lemma 2.8.2 that the case $T = \mathrm{A}_n$ can not happen. To eliminate some other cases we use the restrictions on the length n of the code C, on which the group T acts. Recall from Corollary 1.4.2 that n is a multiple of 8. This condition, together with the bound on n from Theorem 1.1.10 (a), leaves the following possibilities for T from Table 2.2:

(1) HS with $n = 176$;

(2) $\mathrm{PSL}(2, 7^3)$ with $n = 344$;

(3) $\mathrm{PSU}(3, 7)$ with $n = 344$;

T	n	k	Remarks
A_n, $n \geq 5$	n	$n-2$ (n)	Two representations if $n=6$
$\mathrm{PSL}(2,q)$	$q+1$	2 (3)	$q \neq 2,3$ a prime power
$\mathrm{PSL}(d,q)$, $d>2$	$(q^d-1)/(q-1)$	2	Two representations
$\mathrm{PSU}(3,q)$	q^3+1	2	$q>2$
${}^2B_2(q)$ (Suzuki)	q^2+1	2	$q=2^{2a+1}>2$
${}^2G_2(q)$ (Ree)	q^3+1	2	$q=3^{2a+1}>3$
$\mathrm{PSp}(2d,2)$	$2^{2d-1}+2^{d-1}$	2	$d>2$
$\mathrm{PSp}(2d,2)$	$2^{2d-1}-2^{d-1}$	2	$d>2$
$\mathrm{PSL}(2,11)$	11	2	Two representations
$\mathrm{PSL}(2,8)$	28	1 (2)	
A_7	15	2	Two representations
M_{11} (Mathieu)	11	4	
M_{11} (Mathieu)	12	3	
M_{12} (Mathieu)	12	5	Two representations
M_{22} (Mathieu)	22	3	
M_{23} (Mathieu)	23	4	
M_{24} (Mathieu)	24	5	
HS (Higman–Sims)	176	2	Two representations
Co_3 (Conway)	276	2	

Table 2.2: Simple groups that can occur as a socle of a 2-transitive group

(4) $\mathrm{PSL}(8,3)$ with $n=3280$;

(5) $\mathrm{PSL}(4,p)$ for $p=3,7,11$, $n=40,400,1464$;

(6) $\mathrm{PSp}(2d,2)^-$ for $d=4,5,6$, $n=120,496,2016$;

(7) $\mathrm{PSp}(2d,2)^+$ for $d=4,5,6$, $n=136,528,2080$.

For each of these groups T we need to find all extremal Type II codes that are invariant under T. In order to do this we use Proposition 1.2.2.

Let T be a group in one of cases (1) to (7). We are looking for submodules C of the ambient space $\mathbb{F}_2^n$, such that $\dim C = \frac{n}{2}$. If such submodule C is found, we check if it is self-dual and doubly-even as a code. Then, for Type II codes C we use Algorithm 2.3.5 to find codewords of small weight in C.

For the Higman–Sims group HS one can take representation data from the Atlas of Finite Group Representations [79]. For the groups in cases (2), (3), (4) and (5) the default Magma representations may be used. However, obtaining representations for the groups PSp (cases (6) and (7)) is not straightforward. The Atlas only provides information about smaller groups and the representations of $\mathrm{PSp}(2 \cdot 6, 2)$ are not included. Information about maximal subgroups (the action on their cosets yield possible permutation representations) of $\mathrm{PSp}(2d,2)$ may be found, for instance, in [54, Section 3]. Considering the orders of the subgroups we find that

$$\left|\mathrm{PSp}(2d,2) : \mathrm{O}^-(2d,2)\right| = 2^{2d-1} - 2^{d-1}$$

and

$$\left|\mathrm{PSp}(2d,2) : \mathrm{O}^+(2d,2)\right| = 2^{2d-1} + 2^{d-1},$$

where O^+ and O^- are orthogonal groups Hence, the representations in case (6) are given by the action of $\mathrm{PSp}(2d,2)$ on the cosets of $\mathrm{O}^-(2d,2)$ and the ones in (7) — of $\mathrm{O}^+(2d,2)$.

A computation with Magma shows that for all cases, apart from case (2), there are no submodules of $\mathbb{F}_2^n$ of dimension $\frac{n}{2}$. In the case $T = \mathrm{PSL}(2,7^3)$ there are exactly two such submodules. It follows from Lemma 2.3.12 that these are exactly the extended generalized quadratic residue codes. By Theorem 2.3.13 these codes are not extremal.

Thus, the case $n-1$ does not lead to extremal codes and the proof is complete. □

Example 2.8.4. We want to construct all self-dual codes of length $n = 2016$ that are invariant under the group $G = \mathrm{PSp}(2 \cdot 6, 2)$ of degree n.

First we obtain the required permutation representation of G as the image of the action of G on the cosets of the maximal subgroup $\mathrm{O}^-(2 \cdot 6, 2) \leq G$. For that purpose we use the built-in Magma function `CosetImage`. Then we find all submodules of the ambient space $\mathbb{F}_2^n$, which we consider as an $\mathbb{F}_2G$-module. None of these submodules is of dimension $\frac{n}{2}$. Therefore, there are no self-dual dual codes of length n invariant under G.

The Magma code for this example may be found in Listing A.7 in Appendix A.

Proof of Theorem 2.8.1. The proof follows from Lemma 1.2.1 (i) and Theorems 2.7.1 and 2.8.3. □

2.9 Extremal Type III codes with 2-transitive automorphism groups

In this section we apply the methods from the previous sections to classify extremal Type III codes with 2-transitive permutation automorphism groups.

Theorem 2.9.1. *Let C be an extremal Type III code of length n with a 2-transitive permutation automorphism group. Then $n = 12$ and C is the ternary Golay code.*

Proof. Let G denote the permutation automorphism group of C. Since G is 2-transitive, it follows from Lemma 1.2.1 (i) that the socle T of G is either elementary abelian or simple.

Consider the case that T is elementary abelian. From Corollary 1.4.2 we know that $4 \mid n$. Hence $n = 2^m$ and $m \leq 7$ by Theorem 1.1.11. By Lemma 1.2.1 (iii) and (ii) we can write $G = T \rtimes H$, where $H \leq \mathrm{GL}(m, 2)$ acts transitively on $2^m - 1$ points. Note that the possibilities for H are given in Lemma 2.7.3. With Magma we find that for all $m \leq 7$ and all posssible groups H there are no $\frac{n}{2}$-dimensional $\mathbb{F}_3G$-modules and, therefore, no Type III codes.

Now, let T be simple. Then T is one of the groups from Table 2.2 with $4 \mid n \neq 72$, 96, 120 and $n < 144$ (by Corollary 1.4.2 and Theorem 1.1.11). The possibilities are as follows:

(1) A_n;

(2) $\mathrm{PSL}(2, p)$ with $n = p + 1$;

(3) M_{11} with $n = 12$;

(4) M_{12} with $n = 12$;

(5) M_{24} with $n = 24$;

(6) $\mathrm{PSL}(2, 8)$ with $n = 28$;

(7) $\mathrm{PSp}(2 \cdot 3, 2)^-$ with $n = 28$;

(8) $\mathrm{PSL}(4, 3)$ with $n = 40$;

(9) $\mathrm{PSp}(2d, 2)^+$ for $d = 3, 4$, $n = 36, 136$.

Note that the first two cases, namely, $T = \mathrm{A}_n$ and $T = \mathrm{PSL}(2, p)$, can be eliminated using results of Knapp and Schmid [51]. With Magma we see that the only possible group, which has an $\frac{n}{2}$-dimensional $\mathbb{F}_3T$-module is the Mathieu group M_{11} of degree 12. The module is in fact the famous $[12, 6, 6]_3$ Golay code, which is a unique Type III code of this length (see [65]). Note that the full (monomial) automorphism group of this code is a non-split extension of $\mathbb{Z}_2$ by M_{12} (see [41, Section 10.4.2]). □

Example 2.9.2. We want to prove that there are no Type III codes of length $n = 64 = 2^6$ that are invariant under a 2-transitive subgroup of $\mathrm{AGL}(6, 2)$.

We need construct all 2-transitive subgroups of $\mathrm{AGL}(6, 2)$. We know from Lemma 1.2.1 (iii) that these are the extensions of an elementary abelian group T of order 2^6 by a subgroup of $\mathrm{GL}(6, 2)$, which is transitive on $2^6 - 1$ points. So, as a first step we find all transitive subgroups H of $\mathrm{GL}(6, 2)$ with a built-in Magma function `Subgroups`. Then for every such H we find 2-transitive subgroups G of $\mathrm{AGL}(6, 2)$ of order $2^6 \cdot |H|$. Finally, for every group G, found in the previous step, we verify that the ambient space $\mathbb{F}_3^n$, considered as an $\mathbb{F}_3G$-module, does not have any $\frac{n}{2}$-dimensional submodules. In particular, there are no ternary self-dual codes of length n for every G.

The Magma code for this example may be found in Listing A.8 in Appendix A.

2.10 Extremal Type IV codes with 2-transitive automorphism groups

This section is devoted to the classification of extremal Type IV codes with 2-transitive permutation automorphism groups. Once again we use the same methods as in the binary case (see Sections 2.7 and 2.8).

Theorem 2.10.1. *Let C be an extremal Type IV code of length $n > 2$ with a 2-transitive permutation automorphism group. Then one of the following holds true*

(i) $n = 6$, 8, 14, *or* 30 *and C is equivalent to an extended generalized quadratic residue code,*

(ii) $n = 22$ *and C is unique up to equivalence.*

Proof. Let G denote the permutation part of $\mathrm{Aut}(C)$. Furthermore, let T denote the socle of G, which by Lemma 1.2.1 (i) is either elementary abelian or simple.

If T is elementary abelian then $n = 2^m$. Moreover, by Theorem 1.1.10 (b) we have $m \leq 6$. We check with Magma that for even m there are no Hermitian self-dual codes for all possible groups G. If $m = 3$ or 5 then we find with Magma that the only Type IV codes that are invariant under a 2-transitive permutation group are generalized Reed-Muller codes (see [41, Section 13.2.3]). Only one generalized Reed-Muller code is extremal, namely, if $n = 8$. In this case it is also equivalent to an extended generalized quadratic residue code (see [74] for a definition over $\mathbb{F}_4$).

Now, let T be simple. Then T is one of the groups in Table 2.2, where n is even by Corollary 1.4.2 and satisfies the bounds in Theorem 1.1.10 (b). Thus, the possibilities for T are as follows:

(1) A_n;

(2) $\mathrm{PSL}(2, p)$ with $n = p + 1$;

(3) M_{11} with $n = 12$;

(4) M_{12} with $n = 12$;

(5) M_{22} with $n = 22$;

(6) M_{24} with $n = 24$;

(7) $\mathrm{PSL}(2, 8)$ with $n = 28$;

(8) $\mathrm{PSp}(2 \cdot 3, 2)^+$ with $n = 36$;

(9) $\mathrm{PSL}(4,3)$ with $n = 40$;

(10) $\mathrm{PSp}(2d,2)^-$ for $d = 3,4$, $n = 28,120$;

With MAGMA we find that the only groups that have $\frac{n}{2}$-dimensional $\mathbb{F}_4T$-modules are the Mathieu groups M_{22} and M_{24} and $\mathrm{PSL}(2,p)$, in which case p is a prime.

For $T = \mathrm{M}_{22}$ there are three Type IV codes, two of which are extremal. However, we check with MAGMA that the two extremal codes are equivalent.

For $T = \mathrm{M}_{24}$ we get only one Type IV code, namely, the $\mathbb{F}_4$ extension of the binary Golay code, which is also an extended generalized quadratic residue code. The minimum distance is 8 and, therefore, the code is not extremal.

From [51] we know that extended generalized quadratic residue codes are the only codes over $\mathbb{F}_4$ of length $n = p + 1$ that are invariant under $\mathrm{PSL}(2,p)$. Note that by a result of Martínez-Pérez and Willems [60] these codes are Hermitian self-dual if and only if -2 is a nonsquare in $\mathbb{F}_p^*$.

Among Type IV extended generalized quadratic residue codes only those of length $n = 6$, 8, 14, and 30 are extremal.

All computations are carried out with MAGMA. □

Example 2.10.2. We want to find all extremal Type IV codes of length $n = 22$ that are invariant under the group $G = \mathrm{M}_{22}$ of degree n.

We construct G using the generators taken from the ATLAS of Finite Group Representations [79]. Then we find all $\mathbb{F}_4G$-modules M of dimension $\frac{n}{2}$ as submodules of the ambient space $\mathbb{F}_4^n$, which we consider as an $\mathbb{F}_4G$-module. For every such submodule M we check, if it is Hermitian self-dual as a code C and if all its weights are even. After that we check the minimum distance of the found Type IV codes and see that exactly two codes are extremal. Finally, we verify that the two extremal codes are indeed equivalent.

The MAGMA code for this example may be found in Listing A.9 in Appendix A.

Chapter 3

Performance of self-dual codes

The previous chapter is devoted almost entirely to extremal doubly-even self-dual codes. The main reasons that make dealing with extremal Type II codes easier, as opposed to Type I codes, are the uniqueness of their weight enumerator and the bound of Theorem 1.1.10 (a) on their length.

We can not use the classification methods from the previous chapter for Type I codes. Nevertheless, we may wonder whether binary extremal self-dual codes of one type are better than the codes of the other type. Clearly, the codes that have "better" parameters (i.e., smaller length or larger minimum distance) are better. Thus, we may want to compare codes that have the same parameters. On the one hand, Type II codes exist only at lengths a multiple of 8 (see Corollary 1.4.2). On the other hand, Type I codes can not be extremal if their length divides 24 (see Theorem 1.4.6). Therefore, in this chapter we will just consider codes of length $n = 24m + 8\ell$, where $\ell = 1$ or 2.

In this chapter we investigate how good codes of different types perform if used for error correction in data transmission. This information allows to compare the codes. To measure performance we will consider the probability of erroneous decoding. That is, the code is said to perform better if the decoding error probability is smaller.

The chapter is structured as follows. First, we introduce a way to measure performance, which is based on comparing the weight enumerators of codes. Then, we consider how known extremal self-dual codes perform. After that, we find the best performing representatives (weight enumerator-wise) among Type I codes and compare those to Type II codes for lengths, for which the latter codes might exist. The chapter is mainly based on [10].

3.1 A way to measure performance of codes

The question of decoding error probabilities was studied by Faldum et. al. [28] for bounded distance decoding. For reader's convenience we repeat their result, which we shall apply below to measure the quality of performance.

Assume that a linear $[n,k,d]_q$ code C is used for error correction in data transmission over a non-reliable channel with symbol error probability p. In addition, we assume that *bounded distance decoding* is used, i.e., we decode only up to $t \le \frac{d-1}{2}$ errors. Finally, for $x \in \mathbb{F}_q^n$ and $r \in \mathbb{N}_0$ the set

$$\mathrm{B}_r(x) = \Big\{ y \mid y \in \mathbb{F}_q^n,\ \mathrm{dist}(x,y) \le r \Big\}$$

describes the ball around x of radius r. Recall from Section 1.1 that $\mathrm{dist}(x,y)$ stands for the Hamming distance between the vectors x and y. A received vector y is decoded to a codeword x if and only if $y \in \mathrm{B}_t(x)$.

Clearly, a decoding error occurs exactly when the receiver gets a vector $y \in \mathrm{B}_t(c)$ for some codeword $c \in C$ that was not transmitted. Thus, the probability of a decoding error is the conditioned probability

$$\mathrm{P}(C,t,p) = \mathrm{P}\big(X \in C \setminus \{c\} \mid Y \in \mathrm{B}_t(c)\big),$$

where the random variable X stands for the transmitted codeword and Y — for the received vector. The main result of [28] shows the correspondence between the decoding error probability and the weight distribution of the code C for small symbol error probability.

Definition 3.1.1. Let $u = (u_0, u_1, \ldots, u_n)$ and $v = (v_0, v_1, \ldots, v_n)$ be two vectors in $\mathbb{Z}^{n+1}$. We say that u is *lexicographically smaller* than v if there is an index $j \in \{0,1,\ldots,n\}$, such that $u_i = v_i$ for all $0 \le i < j$ and $u_j < v_j$.

Theorem 3.1.2 ([28])**.** *Let C and C' be two $[n,k,d]_q$ codes with weight distributions $(A_i)_{0\le i\le n}$ and $(A'_i)_{0\le i\le n}$ respectively. If the symbol error probability p is small enough then for all $t \le \frac{d-1}{2}$ the following two conditions are equivalent:*

(i) $\mathrm{P}(C,t,p) < \mathrm{P}(C',t,p)$.

(ii) $(A_0,\ldots,A_n)$ *is lexicographically smaller than* $(A'_0,\ldots,A'_n)$.

Remark 3.1.3. The function $f(p) = \mathrm{P}(C',t,p) - \mathrm{P}(C,t,p)$ is a polynomial in p with coefficients in $\mathbb{Q}$. More precisely, $f(p)$ is of the form

$$f(p) = (A'_l - A_l)\binom{l}{t}\left(\frac{1}{q-1}\right)^{l-t} p^{l-t} + \text{ terms in } p^r \text{ with } r > l-t,$$

where l is the smallest position, in which the weight distributions of C and C' differ. Hence, if p is small enough we get $f(p) > 0$ if and only if $A_l < A'_l$.

For more details see [28].

Thus, for small p the quality of performance can be read off from the weight distribution. We define performance of codes in the spirit of Theorem 3.1.2.

Definition 3.1.4. Let C and C' be two $[n,k,d]$ codes with weight distributions $(A_0,\ldots,A_n)$ and $(A'_0,\ldots,A'_n)$, respectively. We say that C *performs better* than C', if $(A_0,\ldots,A_n)$ is lexicographically smaller than $(A'_0,\ldots,A'_n)$.

Our goal is to compare two different types of binary self-dual codes in the sense of the definition given above. However, before moving to that we investigate how self-dual codes compare to non-self-dual ones as far as their performance is concerned.

3.2 Performance of known extremal binary codes

Let C be a Type II code of length n and minimum distance d with weight distribution $(A_0,\ldots,A_n)$. Suppose that C' is any non-self-dual code with the same parameters as C and that the weight distribution of C' is $(A'_0,\ldots,A'_n)$. Since C is doubly-even, we have $A_k = 0$ for all $k \not\equiv 0 \bmod 4$. Thus, the weight function takes generically less values on C than on C'; in other words, the codewords of C are concentrated in fewer weight values. Therefore, we may expect that $A'_d < A_d$ and, in particular, that C' performs better than C.

The following example shows that this is not true in general.

Example 3.2.1. Let C be any extremal Type II $[32,16,8]$ code, for instance, the extended quadratic residue code. From Theorem 1.4.3 it follows that $A_8 = 620$. In [18], Cheng and Sloane contructed a $[32,17,8]$ code. If we delete the last row in the generator matrix of the aforementioned $[32,17,8]$ code, we obtain a $[32,16,8]$ code C', which is not self-dual. With a Magma computation we find that $A'_8 = 681$. Since $A_8 < A'_8$, it follows from Definition 3.1.4 that the Type II code C performs better than the non-self-dual code C'.

Same arguments as above may be applied when comparing binary self-dual codes of different types. Indeed, for doubly-even codes only a quarter of all weight coefficients may be nonzero, whereas for singly-even codes as many as half of them may be positive. Thus, Type I codes might be expected to perform better than Type II. However, before making any assumptions based on this observation alone, we consider lengths, for which extremal self-dual codes of both types are constructed.

Let C and C' be extremal self-dual codes of length n of Types II and I, respectively. From Theorem 1.4.6 we know that an extremal self-dual code of length $n = 24m$ is always doubly-even. Thus, we assume that $n = 24m + 8$ or $n = 24m + 16$, since we want the codes C and C' to have the same parameters. Recall from Section 1.1 that the minimum distance of C and C' is $d = 4m + 4$. Let A_d and A'_d denote the number of codewords of weight d in C and C', respectively. Information that we found by checking examples of known extremal

n	d	A_d (Type II)	A'_d (Type I)
32	8	620	364
40	8	285	$125 + 16\beta$ $(0 \leq \beta \leq 26)$ (two codes are known with $A'_d = 285$, i.e. $\beta = 10$)
56	12	8 190	$\leq 4\,862$
64	12	2 976	$1\,312 + 16\beta$ $(0 \leq \beta \leq 284)$ (in all known examples $A'_d \leq 2\,336$ and $\beta \leq 64$)
80	16	97 565	$\leq 66\,845$
104	20	1 136 150	$\leq 739\,046$

Table 3.1: Number of codewords of minimum weight in binary extremal self-dual codes

codes is presented in Table 3.1. For the existence of particular codes we refer the reader to [13], [25], and [20].

From the table we see that Type I codes always perform better than Type II codes, provided $n = 24m + 8 \geq 32$. The parameter β in the last column of Table 3.1 takes care of the fact that the weight distribution of a Type I code is not unique in general. For $n = 56$, 80, and 104 we have computed a'_d for all possible weight distributions and the bounds are given in the fourth column. Finally note that for $n = 40$ the two known Type I codes that satisfy $A'_d = 285$ perform worse than any extremal Type II code since $A'_{d+2} \neq 0$, but $A_{d+2} = 0$.

3.3 Best performing extremal Type I codes

Let C be an extremal Type I code of length $n = 24m + 8\ell$ ($\ell = 1$ or 2) with the weight enumerator

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

Since $A_i = 0$ for odd i, we can set $a_{i/2} = A_i$ for even i and use the homogeneous polynomial $A(x,y)$ with coefficients a_j, $0 \leq j \leq \frac{n}{2}$, instead of $W_C(x,y)$. With Theorem 1.4.1 we obtain

$$A(x,y) = \sum_{j=0}^{n/2} a_j x^{n-2j} y^{2j} = \sum_{i=0}^{n/8} c_i (x^2 + y^2)^{\frac{n}{2}-4i} \left\{ x^2 y^2 (x^2 - y^2)^2 \right\}^i \tag{3.1}$$

with $a_j \in \mathbb{N}_0$ and $c_i \in \mathbb{Q}$.

Let S denote the shadow of the code C. Further let

$$W_S(x,y) = \sum_{j=0}^{n} B_j x^{n-j} y^j$$

be the weight enumerator of the shadow. Since n is a multiple of 8, from Theorem 1.4.5 we know that $B_j = 0$ if $j \not\equiv 0 \bmod 4$. Setting $b_j = B_{4j}$, $0 \leq j \leq \frac{n}{4}$ and using Theorem 1.4.5 we can write

$$S(x,y) = \sum_{j=0}^{n/4} b_j x^{n-4j} y^{4j} = \sum_{i=0}^{n/8} (-1)^i c_i 2^{\frac{n}{2}-6i} (xy)^{\frac{n}{2}-4i} \left(x^4 - y^4\right)^{2i}, \tag{3.2}$$

where $b_j \in \mathbb{N}_0$ and $c_i \in \mathbb{Q}$ are the same as in (3.1). In what follows we use $S(x,y)$ in place of the shadow weight enumerator $W_S(x,y)$.

In the remaining part of this section we prove that s-extremal codes are the best performing extremal Type I codes. In particular, we show that the number a_{2m+2} of codewords of minimum weight is smallest in case of s-extremal codes.

Theorem 3.3.1. *In the set of self-dual extremal codes of Type I and length $n = 24m + 8$ or $n = 24m + 16$ the s-extremal codes perform best of all.*

Proof. Here we only consider the case $n = 24m + 8$. For the other case the proof runs similarly with only some minor changes in the formulas.

Let C be an arbitrary extremal Type I code of length $n = 24m + 8$ and let S denote its shadow. Since all weights of the shadow are divisible by 4 the minimum weight of the shadow can be written as $4s$ with $s \geq 1$. We express the dependency on s in the formulas for the weight enumerators.

Setting $x = 1$ in (3.1) and (3.2) we obtain

$$A^{(s)}(y) = \sum_{j=0}^{12m+4} a_j^{(s)} y^{2j} = \sum_{i=0}^{3m+1} c_i^{(s)} \left(1+y^2\right)^{12m+4-4i} \left\{y^2\left(1-y^2\right)^2\right\}^i,$$

$$S^{(s)}(y) = \sum_{j=0}^{6m+2} b_j^{(s)} y^{4j} = \sum_{i=0}^{3m+1} (-1)^i c_i^{(s)} 2^{12m+4-6i} y^{12m+4-4i} \left(1-y^4\right)^{2i}.$$

Recall that $a_j^{(s)}, b_j^{(s)} \in \mathbb{N}_0$ and $c_j^{(s)} \in \mathbb{Q}$. As in [70] we express $c_i^{(s)}$ as a linear combination of the $a_j^{(s)}$ for $0 \leq j \leq i$ and as a linear combination of the $b_j^{(s)}$ for $0 \leq j \leq \frac{n}{8} - i$.

$$c_i^{(s)} = \sum_{j=0}^{i} \alpha_{ij} a_j^{(s)} = \sum_{j=0}^{3m+1-i} \beta_{ij} b_j^{(s)}$$

with $\alpha_{ij}, \beta_{ij} \in \mathbb{Q}$. We want to remark that α_{ij} and β_{ij} do not depend on the parameter s. From [70] for β_{ij}, $i > 0$, we have

$$\beta_{ij} = (-1)^i 2^{-12m-4+6i} \cdot \frac{3m+1-j}{i} \binom{3m+i-j}{3m+1-i-j}, \tag{3.3}$$

One can see that the α_{ij} do not depend on s using the Bürmann-Lagrange Theorem (see, for instance, [72, Theorem 32]).

Furthermore, notice that $a_0^{(s)} = 1$, $a_j^{(s)} = 0$ for $j \in \{1, \ldots, 2m+1\}$, since C is extremal, and $b_j^{(s)} = 0$ for $j \in \{1, \ldots, s-1\}$, since $4s$ is the minimum weight of S. Consequently, we have $c_i^{(s)} = \alpha_{i,0}$ for $i \in \{1, \ldots, 2m+1\}$. Thus, for the coefficient $c_{2m+2}^{(s)}$ we obtain the following equation:

$$c_{2m+2}^{(s)} = \alpha_{2m+2,0} + \alpha_{2m+2,2m+2} a_{2m+2}^{(s)} = \sum_{j=0}^{m-1} \beta_{2m+2,j} b_j^{(s)}. \tag{3.4}$$

One the other hand, (3.3) yields

$$\beta_{2m+2,j} = 2^8 \cdot \frac{3m+1-j}{2m+2} \binom{5m+2-j}{m-1-j}, \tag{3.5}$$

in particular $\beta_{2m+2,j} > 0$ for $j = 1, 2, \ldots, m-1$. Therefore, it follows from (3.4) that $c_{2m+2}^{(s)} \geq 0$, since $b_j^{(s)} \geq 0$. Moreover, $c_{2m+2}^{(s)} = 0$ if and only if $b_i^{(s)} = 0$ for all $i = 0, 1, \ldots, m-1$. By Lemma 1.4.7 we get $4s \leq 4m$ since $d = 4m+4$, and in the case $s = m$ the code C is s-extremal. This shows that $c_{2m+2}^{(s)} = 0$ if and only if C is s-extremal. In this case we have

$$a_{2m+2}^{(m)} = -\frac{\alpha_{2m+2,0}}{\alpha_{2m+2,2m+2}}. \tag{3.6}$$

We go back to the general case, i.e., we do not assume that C is s-extremal. Now, from (3.4) we obtain

$$a_{2m+2}^{(s)} = \frac{c_{2m+2}^{(s)} - \alpha_{2m+2,0}}{\alpha_{2m+2,2m+2}} = \frac{c_{2m+2}^{(s)}}{\alpha_{2m+2,2m+2}} + a_{2m+2}^{(m)}. \tag{3.7}$$

To prove the theorem, we only have to show that

$$a_{2m+2}^{(s)} > a_{2m+2}^{(m)} \quad \text{for } 1 \leq s \leq m-1.$$

This is obviously equivalent to proving that $\alpha_{2m+2,2m+2}$ is positive, since we have $c_{2m+2}^{(s)} > 0$ for $s < m$.

From [70] we know that

$$\begin{aligned} \alpha_{i,0} &= -\frac{n}{2i} \left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n/2-1+4i}(1-y)^{-2i} \right] \\ &= -\frac{12m+4}{i} \left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-12m-5+4i}(1-y)^{-2i} \right]. \end{aligned}$$

For $i = 2m+2$ we compute

$$\begin{aligned} \alpha_{2m+2,0} &= -\frac{12m+4}{2m+2} \left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^{-12m-5+8m+8}(1-y)^{-4m-4} \right] \\ &= -\frac{6m+2}{m+1} \left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^{-4m+3}(1-y)^{-4m-4} \right] \\ &= -\frac{6m+2}{m+1} \left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^{7}(1-y^2)^{-4m-4} \right] \end{aligned} \tag{3.8}$$

and it follows that $\alpha_{2m+2,0}$ is negative. Since $a^{(m)}_{2m+2}$ is positive, we obtain from (3.6) that $\alpha_{2m+2,2m+2}$ is also positive, which completes the proof. □

Remark 3.3.2. We would like to mention that we do not have $a^{(s-1)}_{2m+2} \geq a^{(s)}_{2m+2}$ in general. In particular, it may happen that $a^{(1)}_{2m+2} < a^{(s)}_{2m+2}$ for some $s > 1$. For example, if $n = 80$ then $a^{(1)}_{2m+2} = 58\,653$ while $a^{(2)}_{2m+2}$ can be as large as $66\,845$.

3.4 Performance comparison of extemal Type I and Type II codes

In this section we prove the following result.

Theorem 3.4.1.

(i) Extremal Type I codes with minimal shadow perform better than extremal Type II codes for lengths $n = 24m + 8$. In particular, s-extremal codes perform better than extremal Type II codes.

(ii) s-extremal Type I codes perform better than extremal Type II codes for lengths $n = 24m + 16$.

Proof. Keeping notation of the previous section we first consider an extremal Type I code C with minimal shadow S of length $n = 24m + 8$. It follows from Definition 1.4.9 that the minimum weight $4s$ of the shadow S equals 4. Clearly S contains at least one vector, say v, of weight 4. Suppose that S contains another vector $w \neq v$ with $\mathrm{wt}(w) = i$ for some $i \in \{4, 8, 12, \ldots, 4m - 4\}$. Recall from Setion 1.4 that a sum of any two vectors in S is a codeword in C. Hence, we have $v + w \in C$ with $0 \neq \mathrm{wt}(v + w) \leq 4m$, a contradiction to the extremality of C. This shows that

$$b^{(1)}_1 = 1,\ b^{(1)}_2 = \cdots = b^{(1)}_{m-1} = 0.$$

Rewriting equation (3.4) we get

$$c^{(1)}_{2m+2} = \alpha_{2m+2,0} + \alpha_{2m+2,2m+2} a^{(1)}_{2m+2} = \beta_{2m+2,1}.$$

Using equations (3.7) and (3.6) we see that

$$\begin{aligned} a^{(1)}_{2m+2} &= \frac{c^{(1)}_{2m+2} - \alpha_{2m+2,0}}{\alpha_{2m+2,2m+2}} = \frac{\beta_{2m+2,1}}{\alpha_{2m+2,2m+2}} + a^{(m)}_{2m+2} \\ &= -\frac{\beta_{2m+2,1}}{\alpha_{2m+2,0}} a^{(m)}_{2m+2} + a^{(m)}_{2m+2} = a^{(m)}_{2m+2}\left(1 - \frac{\beta_{2m+2,1}}{\alpha_{2m+2,0}}\right). \end{aligned} \tag{3.9}$$

Note that all terms of (3.9) are computable. The number $a^{(m)}_{2m+2}$ of minimum weight vectors of the s-extremal code is given by Lemma 1.4.8. We have

$$a^{(m)}_{2m+2} = \frac{6m+2}{m+1} \sum_{\substack{j,k \in \mathbb{N} \\ j+k=2m+1}} (-1)^j \binom{4m-4+j}{j} \binom{4m+k+3}{k}.$$

Furthermore, from (3.5) we know that

$$\beta_{2m+2,1} = 2^8 \cdot \frac{3m}{2m+2}\binom{5m+1}{m-2}.$$

Finally, from (3.8) we obtain

$$\alpha_{2m+2,0} = -\frac{6m+2}{m+1}\left[7\binom{5m+3}{m} + \binom{7}{3}\binom{5m+2}{m-1} + \binom{7}{5}\binom{5m+1}{m-2} + \binom{5m}{m-3}\right].$$

Thus we can compute $a^{(1)}_{2m+2}$ explicitely.

Let C' be an extremal Type II code of length $n = 24m+8$ with A'_{4m+4} codewords of weight $4m+4$. From Theorem 1.4.3 we know that

$$A'_{4m+4} = \frac{1}{4}(24m+8)(24m+7)(24m+6)(24m+4)\frac{(5m)!}{m!(4m+4)!}.$$

Furthermore, from Theorem 1.1.10 (a) it follows that $m < 159$. Using a computer one easily verifies that

$$a^{(1)}_{2m+2} < A'_{4m+4}$$

for $m = 1, 2, \ldots, 158$. Thus, we may conclude that in the case $n = 24m+8$ extremal Type I codes with minimal shadow always perform better than extremal Type II codes. Finally, with Theorem 3.3.1 we have

$$a^{(m)}_{2m+2} < a^{(1)}_{2m+2} < A'_{4m+4},$$

which shows that s-extremal codes perform better than extremal Type II codes. Thus, part (i) of the theorem is proven.

Now, let C be an s-extremal code of length $24m+16$ and let C' be an extremal Type II code of the same length. In this case the minimum weight of the shadow S of C is $4m+4$ (see Lemma 1.4.7). The number $a^{(m+1)}_{2m+2}$ of codewords of minimum weight of an s-extremal code is given by Lemma 1.4.8

$$a^{(m+1)}_{2m+2} = \frac{6m+4}{m+1}\sum_{\substack{j,k\in\mathbb{N}\\ j+k=2m+1}} (-1)^j \binom{4m+j}{j}\binom{4m+k-3}{k}.$$

From Theorem 1.4.3 we have

$$A'_{4m+4} = \frac{3}{2}(24m+16)(24m+14)\frac{(5m+2)!}{m!(4m+4)!}$$

for the number of codewords of minimum weight in C'. According to Theorem 1.1.10 (a) we need to compare $a^{(m)}_{2m+2}$ and A'_{4m+4} only for $m < 164$. This can be easily done with a computer. We get

$$a^{(m+1)}_{2m+2} < A'_{4m+4}$$

for all codes of length $n = 24m+16$ with $m = 1, 2, \ldots, 163$. This completes the proof of the theorem. □

Appendix A

Code of Magma programs

In the appendix we list the source code of Magma programs for the examples in Chapters 2 and 3. We refer the reader to [5] for the introduction to Magma.

We distinguish the built-in Magma functions and keywords with **bold** font in the listings. Note that we do not provide the code for all user-defined functions. Instead, we briefly explain what each of them does. We will be happy to send the full source code by e-mail at reader's first request.

In the two following programs (Listings A.1 and A.2) we use the user-defined functions `ExtendedBinaryQRCode(p)` and `PSL2p(p)`. The first one returns an extended quadratic residue code of length $p+1$. The second generates the representation of the group $\mathrm{PSL}(2,p)$ that acts on an extended quadratic residue code of length $p+1$.

Listing A.1: Program for Example 2.3.9

```
p := 1871;
C := ExtendedBinaryQRCode(p);
G := PSL2p(p);
_ := exists(g){p : p in G | Order(p) eq 6};
H := sub< G | g >;
S := Fix(C, H);
d := 4*Floor( (p+1)/24 ) + 4;
WordsOfBoundedWeight( S, d-60, d-4: NumWords := 1 );
```

Listing A.2: Program for Example 2.3.10

```
p := 3823;
C := ExtendedBinaryQRCode(p);
G := PSL2p(p);
H := SylowSubgroup(G, 2);
S := Fix(C, H);
d := 4*Floor( (p+1)/24 ) + 4;
WordsOfBoundedWeight( S, d-60, d-4: NumWords := 1 );
```

In the following program the user-defined function `QDCCode(p)` generates the quadratic double circulant code of length $2p+2$. The function `PSLxC(p)` generates the representation of the group $\mathrm{PSL}(2,p) \times \mathbb{Z}_2$ that acts on a quadratic double circulant code of length $2p+2$ and leaves it invariant.

Listing A.3: Program for Example 2.3.16

```
p := 1867;
C := QDCCode(p);
G := PSLxC(p);
H := SylowSubgroup(G,2);
S := Fix(C, H);
d := 4*Floor( (2*p+2)/24 ) + 4;
WordsOfBoundedWeight( S, d-60, d-4: NumWords := 1 );
```

In the next program the following user-defined functions are used. The function `Cycls(p)` generates the $k = \frac{p-1}{s(p)}$ nonzero cyclotomic cosets modulo p. For a prime p and a transversal T the function `CosetCollections(p, T)` returns a collection of all sets S of cardinality $\frac{k}{2}$ that satisfy condition (2.6) of Lemma 2.4.7. The function `KnownCyclicAut(p)` is used to generate the representation of the group $G = \langle\sigma\rangle \rtimes \langle\mu_2\rangle$ (see Lemma 1.3.7) that acts on an extended cyclic code of length $p+1$. Finally, `GeneratingIdempotent(p, S)` returns the idempotent of length p that corresponds to a set S (see equation (2.5) of Lemma 2.4.7).

Listing A.4: Program for Example 2.4.16

```
p := 911;
d := 4*Floor( (p+1)/24 ) + 4;
T := [ Min(c) : c in Cycls(p) ];
db := CosetCollections(p, T);
G := KnownCyclicAut(p);
_ := exists(g){p: p in G | Order(p) eq 13};
H := sub< G | g >;
for S in db do
  Idem := GeneratingIdempotent(p, S);
  C := LengthenCode( CyclicCode( Idem ) );
  D := Fix(C, H);
  WordsOfBoundedWeight( D, d-60, d-4: NumWords := 1 );
end for;
```

The function Cycls, which is decribed above, is also used in the following program. The other user-defined function that we use is ConditionAI. It takes a set S (which is a union of cyclotomic cosets) as an argument and returns **true** if condition (2.10) of Lemma 2.6.7 holds for S.

Listing A.5: Program for Remark 2.6.9. Case $n = 512$

```
m := 9; n := 2^m;
Cosets := [ PowerSequence(Integers())!c :
        c in Cycls(n-1) ];
ts := [ Min(c) : c in Cosets ];
seq := [ PadRight(Intseq(t,2), m) : t in ts ];
db := [ <ts[i], seq[i], &+ seq[i]> : i in [1..#ts] ];
WtHalf := [ e : e in db | e[3] eq (m-1) div 2 ];

I1 := [ e[1] : e in WtHalf |
        ConditionAI( Cosets[ Index(ts,e[1]) ] ) ];

I2 := [];
for i in [1..#I1] do
  s := I1[i];
  for j in [i+1..#I1] do
    t := I1[j];
    temp := &cat Cosets[ [Index(ts, s), Index(ts,t)] ];
    if ConditionAI(temp) then
      Append( ~I2, [s,t]);
    end if;
  end for;
end for;

I3 := [];
for pair in I2 do
  s,t := Explode(pair);
  cur := {e[2] : e in I2 | e[1] eq s}
        meet {e[2] : e in I2 | e[1] eq t};
  for r in cur do
    temp := &cat Cosets[
        [Index(ts, s), Index(ts,t), Index(ts,r)] ];
    if ConditionAI(temp) then
      Append( ~I3, [s,t,r]);
    end if;
  end for;
end for;
```

The built-in function **`AGL`**`(m, 2)` that we use in the next program returns $\mathrm{AGL}(m,2)$ as a permutation group of degree 2^m. The group $G = T \rtimes \mathrm{SL}(3,2^3)$ is constructed as a subgroup of $\mathrm{AGL}(9,2)$. To obtain the vector space $V = \mathbb{F}_2^n$ as an $\mathbb{F}_2G$-module W we use the command `W =` **`PermutationModule`**`(G, V)`. We convert a module M to a subspace $U \leq \mathbb{F}_2^n$ using the built-in function **`Morphism`**`(M, W)`, which returns the embedding of M into W, and the constructor **`sub`** of subspaces. A subspace U is converted to a code C using the function **`LinearCode`**.

Listing A.6: Program for Example 2.7.4

```
m := 9; n := 2^m;
d := 4*Floor( n/24 ) + 4;
G0 := AGL(m, 2);
Subs := Subgroups( G0 : IsTransitive := true,
        OrderEqual := (2^m)*16482816 );
G := Subs[1]`subgroup;
V := VectorSpace(GF(2), n);
W := PermutationModule(G, V);
VS := Submodules(W);
VSK := [ m : m in VS | Dimension(m) eq n div 2];
for M in VSK do
  phi := Morphism(M, W);
  U := sub< V | [ V!phi(x) : x in Basis(M) ] >;
  C := LinearCode(U);
  if IsSelfDual(C) then
    if IsDoublyEven(C) then
      WordsOfBoundedWeight( C, d-30, d-4: NumWords := 1 );
    end if;
  end if;
end for;
```

The built-in function **`PSp`**`(2*d, 2)` that is uses in the following program returns the permutation representation of $\mathrm{PSp}(2*d,2)$ of degree 4095.

Listing A.7: Program for Example 2.8.4

```
G0 := PSp(2*6,2);
Hm := PSOMinus(2*6,2);
n := Index(G0,Hm);
G := CosetImage(G0, Hm);
V := VectorSpace(GF(2), n);
PV := PermutationModule(G, V);
[Dimension( m ) : m in Submodules(PV)];
```

In the following program we use a built-in function **PGL**(m, 2) to generate the group $\mathrm{GL}(m,2) = \mathrm{PGL}(m,2)$ as a permutation group of degree $2^m - 1$.

Listing A.8: Program for Example 2.9.2

```
m := 6; n := 2^m;
K := GF(3);
Subs := Subgroups( PGL(m,2) : IsTransitive := true);

TTGroups := [];
for H in Subs do
  ord := H`order;
  ASubs := Subgroups( AGL(m,2) : IsTransitive := true,
        OrderEqual := (2^m)*ord);
  for i in [1..#ASubs] do
    A := ASubs[i];
    if IsTransitive(A`subgroup, 2) then
      Append(~TTGroups, A`subgroup);
    end if;
  end for;
end for;

for G in TTGroups do
  V := VectorSpace(K,n);
  PV := PermutationModule(G, V);
  VS := Submodules(PV);
  [ m : m in VS | Dimension(m) eq n div 2];
end for;
```

In the next program we construct the permutation representation of the group $G = \mathrm{M}_{22}$ of degree 22 using the constructor **PermutationGroup**. The generators for the representation are taken from the Atlas of Finite Group Representations [79].

Listing A.9: Program for Example 2.10.2

```
G := PermutationGroup< 22 |
[13,8,16,12,5,22,17,2,10,9,14,4,1,11,15,3,7,18,19,20,21,6],
[22,18,21,13,12,11,15,14,9,8,7,5,2,20,6,16,19,4,17,10,1,3]
>;

n := 22;
K := GF(4);
V := VectorSpace(K,n);
PV := PermutationModule(G, V);
VS := Submodules(PV);
Mods := [ M : M in VS | Dimension(M) eq (n div 2) ];

Codes := [];
for M in Mods do;
  phi := Morphism(M, PV);
  U := sub< V | [ V!phi(x) : x in Basis(M)] >;
  C := LinearCode(U);
  if IsHermitianOrthogonal(C) then
    if IsEven(C) then
      Append(~Codes, C);
    end if;
  end if;
end for;

Extremal := [];
for C in Codes do
  d := MinimumDistance(C);
  if d eq (2*Floor(n div 6)+2) then
    Append(~Extremal, C);
  end if;
end for;

IsEquivalent(Extremal[1], Extremal[2]);
```

Bibliography

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr. New 5-designs. *J. Combinatorial Theory*, 6:122–151, 1969.

[2] E. F. Assmus, Jr. and H. F. Mattson, Jr. On weights in quadratic-residue codes. *Discrete Math.*, 3:1–20, 1972.

[3] C. Bachoc and P. Gaborit. Designs and self-dual codes with long shadows. *J. Combin. Theory Ser. A*, 105(1):15–34, 2004.

[4] M. Borello. The automorphism group of an extremal $[72, 36, 16]$ code does not contain elements of order 6.
Preprint available at `http://arxiv.org/abs/1203.3321v1`.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] S. Bouyuklieva. On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length $24m$. *Des. Codes Cryptogr.*, 25(1):5–13, 2002.

[7] S. Bouyuklieva. On the automorphism group of a doubly-even $(72, 36, 16)$ code. *IEEE Trans. Inform. Theory*, 50(3):544–547, 2004.

[8] S. Bouyuklieva. Some optimal self-orthogonal and self-dual codes. *Discrete Math.*, 287(1-3):1–10, 2004.

[9] S. Bouyuklieva, A. Malevich, and W. Willems. Automorphisms of extremal self-dual codes. *IEEE Trans. Inform. Theory*, 56(5):2091–2096, 2010.

[10] S. Bouyuklieva, A. Malevich, and W. Willems. On the performance of binary extremal self-dual codes. *Adv. Math. Commun.*, 5(2):267–274, 2011.

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

[12] S. Bouyuklieva and W. Willems. Singly-even self-dual codes with minimal shadow.
Preprint available at `http://arxiv.org/abs/1106.5936v2`.

[13] S. Bouyuklieva and V. Yorgov. Singly-even self-dual codes of length 40. *Des. Codes Cryptogr.*, 9(2):131–141, 1996.

[14] F. C. Bussemaker and V. D. Tonchev. Extremal doubly-even codes of length 40 derived from Hadamard matrices of order 20. *Discrete Math.*, 82(3):317–321, 1990.

[15] P. J. Cameron. Finite permutation groups and finite simple groups. *Bull. London Math. Soc.*, 13(1):1–22, 1981.

[16] P. Camion. Codes quadratiques abéliens et plans inversifs miquéliens. *C. R. Acad. Sci. Paris Sér. A-B*, 284(21):A1401–A1404, 1977.

[17] P. Charpin and F. Levy-dit-Vehel. On self-dual affine-invariant codes. *J. Combin. Theory Ser. A*, 67(2):223–244, 1994.

[18] Y. Cheng and N. J. A. Sloane. Codes from symmetry groups, and a $[32, 17, 8]$ code. *SIAM J. Discrete Math.*, 2(1):28–37, 1989.

[19] 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 Math.*, 38(2-3):143–156, 1982.

[20] J. H. Conway and N. J. A. Sloane. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory*, 36(6):1319–1333, 1990.

[21] J. de la Cruz. *Über die Automorphismengruppe extremaler Codes der Längen* 96 *und* 120. PhD thesis, Otto-von-Guericke University Magdeburg.

[22] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[23] R. Dontcheva. On the doubly-even self-dual codes of length 96. *IEEE Trans. Inform. Theory*, 48(2):557–561, 2002.

[24] R. Dontcheva and M. Harada. Extremal doubly-even [80,40,16] codes with an automorphism of order 19. *Finite Fields Appl.*, 9(2):157–167, 2003.

[25] R. Dontcheva and M. Harada. Some extremal self-dual codes with an automorphism of order 7. *Appl. Algebra Engrg. Comm. Comput.*, 14(2):75–79, 2003.

[26] R. A. Dontcheva, A. J. van Zanten, and S. M. Dodunekov. Binary self-dual codes with automorphisms of composite order. *IEEE Trans. Inform. Theory*, 50(2):311–318, 2004.

[27] I. Duursma. Extremal weight enumerators and ultraspherical polynomials. *Discrete Math.*, 268(1-3):103–127, 2003.

[28] A. Faldum, J. Lafuente, G. Ochoa, and W. Willems. Error probabilities for bounded distance decoding. *Des. Codes Cryptogr.*, 40(2):237–252, 2006.

[29] T. Feulner and G. Nebe. The automorphism group of a self-dual binary $[72, 36, 16]$ code does not contain Z_7, $Z_3 \times Z_3$, or D_{10}.
Preprint available at `http://arxiv.org/abs/1110.6012`.

[30] A. M. Gleason. Weight polynomials of self-dual codes and the MacWilliams identities. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3*, pages 211–215. Gauthier-Villars, Paris, 1971.

[31] M. J. E. Golay. Notes on digital coding. In *Proceedings of the I.R.E., volume 37*, page 657. 1949.

[32] T. A. Gulliver and M. Harada. Classification of extremal double circulant self-dual codes of lengths 64 to 72. *Des. Codes Cryptogr.*, 13(3):257–269, 1998.

[33] T. A. Gulliver and M. Harada. Classification of extremal double circulant self-dual codes of lengths 74–88. *Discrete Math.*, 306(17):2064–2072, 2006.

[34] R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech. J.*, 29:147–160, 1950.

[35] M. Harada. An extremal doubly even self-dual code of length 112. *Electron. J. Combin.*, 15(1):Note 33, 5, 2008.

[36] M. Harada, T. A. Gulliver, and H. Kaneta. Classification of extremal double-circulant self-dual codes of length up to 62. *Discrete Math.*, 188(1-3):127–136, 1998.

[37] 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 Trans. Inform. Theory*, 49(1):53–59, 2003.

[38] W. C. Huffman. The automorphism groups of the generalized quadratic residue codes. *IEEE Trans. Inform. Theory*, 41(2):378–386, 1995.

[39] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11(3):451–490, 2005.

[40] W. C. Huffman, V. Job, and V. Pless. Multipliers and generalized multipliers of cyclic objects and cyclic codes. *J. Combin. Theory Ser. A*, 62(2):183–215, 1993.

[41] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[42] W. C. Huffman and V. Y. Yorgov. A $[72, 36, 16]$ doubly even code does not have an automorphism of order 11. *IEEE Trans. Inform. Theory*, 33(5):749–752, 1987.

[43] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[44] B. Huppert and N. Blackburn. *Finite groups. III*, volume 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1982.

[45] V. Ĭ. Ĭorgov. Binary self-dual codes with automorphisms of odd order. *Problemy Peredachi Informatsii*, 19(4):11–24, 1983.

[46] V. Ĭ. Ĭorgov and R. Ruseva. Two extremal codes of length 42 and 44. *Problemy Peredachi Informatsii*, 29(4):99–103, 1993.

[47] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[48] N. Ito. A characterization of quadratic residue codes. *Math. J. Okayama Univ.*, 28:1–5 (1987), 1986.

[49] M. Karlin and F. J. MacWilliams. On finding low weight vectors in quadratic residue codes for $p = 8m - 1$. *SIAM J. Appl. Math.*, 25:95–104, 1973.

[50] T. Kasami, S. Lin, and W. W. Peterson. Some results on cyclic codes which are invariant under the affine group and their applications. *Information and Control*, 11:475–496, 1967.

[51] W. Knapp and P. Schmid. Codes with prescribed permutation group. *J. Algebra*, 67(2):415–435, 1980.

[52] J. S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Trans. Inform. Theory*, 34(5, part 2):1354–1359, 1988. Coding techniques and coding theory.

[53] J. S. Leon, J. M. Masley, and V. Pless. Duadic codes. *IEEE Trans. Inform. Theory*, 30(5):709–714, 1984.

[54] M. W. Liebeck. On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc. (3)*, 50(3):426–446, 1985.

[55] F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane. Generalizations of Gleason's theorem on weight enumerators of self-dual codes. *IEEE Trans. Information Theory*, IT-18:794–805, 1972.

[56] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward. Self-dual codes over GF(4). *J. Combin. Theory Ser. A*, 25(3):288–318, 1978.

[57] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[58] A. Malevich and W. Willems. On the classification of the extremal self-dual codes over small fields with 2-transitive automorphism groups. *Designs, Codes and Cryptography*. Available online at `http://dx.doi.org/10.1007/s10623-012-9655-9`.

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

[60] C. Martínez-Pérez and W. Willems. Self-dual extended cyclic codes. *Appl. Algebra Engrg. Comm. Comput.*, 17(1):1–16, 2006.

[61] J. Mykkeltveit, C. Lam, and R. J. McEliece. On the weight enumerators of quadratic residue codes. *JPL Technical Report 32-1526*, XII:161–166, 1972.

[62] G. Nebe. An extremal $[72, 36, 16]$ binary code has no automorphism group containing $Z_2 \times Z_4$, Q_8, or Z_{10}.
Preprint available at `http://arxiv.org/abs/1109.1680`.

[63] E. A. O'Brien and W. Willems. On the automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code. *IEEE Trans. Inform. Theory*, 57(7):4445–4451, 2011.

[64] P. P. Pálfy. Isomorphism problem for relational structures with a cyclic automorphism. *European J. Combin.*, 8(1):35–43, 1987.

[65] V. Pless. On the uniqueness of the Golay codes. *J. Combinatorial Theory*, 5:215–228, 1968.

[66] V. Pless. 23 does not divide the order of the group of a (72, 36, 16) doubly even code. *IEEE Trans. Inform. Theory*, 28(1):113–117, 1982.

[67] V. Pless, J. M. Masley, and J. S. Leon. On weights in duadic codes. *J. Combin. Theory Ser. A*, 44(1):6–21, 1987.

[68] V. Pless and J. G. Thompson. 17 does not divide the order of the group of a $(72, 36, 16)$ doubly even code. *IEEE Trans. Inform. Theory*, 28(3):537–541, 1982.

[69] V. S. Pless, W. C. Huffman, and R. A. Brualdi, editors. *Handbook of coding theory. Vol. I, II.* North-Holland, Amsterdam, 1998.

[70] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44(1):134–139, 1998.

[71] E. M. Rains. New asymptotic bounds for self-dual codes and lattices. *IEEE Trans. Inform. Theory*, 49(5):1261–1274, 2003.

[72] E. M. Rains and N. J. A. Sloane. Self-dual codes. In *Handbook of coding theory, Vol. I, II*, pages 177–294. North-Holland, Amsterdam, 1998.

[73] N. J. A. Sloane. Is there a $(72,36)$ $d = 16$ self-dual code? *IEEE Trans. Information Theory*, IT-19(2):251, 1973.

[74] J. H. van Lint and F. J. MacWilliams. Generalized quadratic residue codes. *IEEE Trans. Inform. Theory*, 24(6):730–737, 1978.

[75] H. N. Ward. Quadratic residue codes and symplectic groups. *J. Algebra*, 29:150–171, 1974.

[76] H. N. Ward. A restriction on the weight enumerator of a self-dual code. *J. Combinatorial Theory Ser. A*, 21(2):253–255, 1976.

[77] H. N. Ward. Quadratic residue codes and divisibility. In *Handbook of coding theory, Vol. I, II*, pages 827–870. North-Holland, Amsterdam, 1998.

[78] W. Willems. A note on self-dual group codes. *IEEE Trans. Inform. Theory*, 48(12):3107–3109, 2002.

[79] R. Wilson, P. Walsh, J. Tripp, and I. Suleiman. Atlas of finite group representations.
Available at `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

[80] N. Yankov. A putative doubly even [72,36,16] code does not have an automorphism of order 9. *IEEE Trans. Inform. Theory*, 58(1):159 –163, jan. 2012.

[81] V. Y. Yorgov. Doubly-even extremal codes of length 64. *Problemy Peredachi Informatsii*, 22(4):35–42, 1986.

[82] V. Y. Yorgov. A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Trans. Inform. Theory*, 33(1):77–82, 1987.

[83] V. Y. Yorgov. On the minimal weight of some singly-even codes. *IEEE Trans. Inform. Theory*, 45(7):2539–2541, 1999.

[84] R. A. Yorgova. On binary self-dual codes with automorphisms. *IEEE Trans. Inform. Theory*, 54(7):3345–3351, 2008.

[85] S. Zhang. On the nonexistence of extremal self-dual codes. *Discrete Appl. Math.*, 91(1-3):277–286, 1999.

Index

affine-invariant code, 51
all-one vector $\mathbf{1} \in \mathbb{F}^n$, 14
automorphism, 18
  group, 18
  type of, 35
    Yorgov's theorem, 36

bounded distance decoding, 66

ciculant matrix, 34
code, 13
  augmented, 14
  dual, 15
  equivalent, 18
  even-like, 14
  extended, 14
  lengthened, 14
  odd-like, 14
  punctured, 14
  self-orthogonal, 15
  shortened, 14
codeword, 13
  even-like, 14
cyclic code, 21
  generator polynomial, 21
  automorphism group, 23
  defining set, 22
  idempotent, 22
  nonzeros, 22
  with self-dual extension, 24, 35
  zeros, 22
cyclotomic coset, 21

t-design, 16
divisible code, 15
  divisor, 15
  Gleason–Pierce theorem, 15
  Gleason–Pierce–Ward theorem, 16
double circulant code
  bordered, 34
  quadratic, 34, 41
duadic code, 23
  defining set of, 23
  even-like, 23
  idempotent of, 24
  odd-like, 23
  splitting for, 24
  with self-dual extension, 24

elementary abelian group, 19

Frobenius automorphism, 15

global conjugation, 15

lexicographical ordering, 66

monomial transformation, 18
multiplier μ_a, 22

orbit, 18

performance of codes, 67

quadratic residue, 25
quadratic residue code, 25, 38
  generalized, 40–41

scalar product
  Hermitian, 14
  standard (Euclidean), 14
self-dual code, 15
  extremal, 16
    bounds on length, 17–18
  of Type I-IV, 16
shadow, 27–28

code with minimal shadow, 29
minimum weight of, 28
s-extremal code, 28
weight enumerator of, 28
simple group, 19
socle, 19
splitting of n given by μ_b, 24
stabilizer, 19

transitive group, 18
2-transitive group, 19
transversal, 21

weight, 13
distibution, 25
weight enumerator, 25
Gleason's theorem, 26
MacWilliams transform, 26
2-weight, 52