Belarusian State University
Faculty of Mechanics and Mathematics
Department of Differential Equations

Diploma thesis

Extremal codes

by **Anton Malevich**

Supervisor: **Prof. Dr. Wolfgang Willems**
Otto-von-Guericke University Magdeburg, Germany

June 2008, Minsk

Contents

1 Introduction

Coding theory arose in the middle of the previous century as an engineering discipline, but its development leads to more and more distinguished mathematical techniques.

An error-correcting code is a system of error control for data transmission, whereby the sender adds redundant data to its messages. This allows the receiver to detect and correct errors (within some bound) without the need to ask the sender for additional data. The advantage of error-correcting code is that a back-channel is not required, or that retransmission of data can often be avoided, at the cost of higher bandwidth requirements on average. Such codes are therefore applied in situations where retransmissions are relatively costly or impossible.

We deal mostly with self-dual doubly-even codes of length $24m$ (so called extremal codes). Such codes are of great interest by two reasons. Firstly, they possess remarkable inner geometry, namely all codewords of fixed weight form a 5-design. Secondly, as it is shown in the first chapter, such codes have the biggest minimal distance possible for a given length, i.e. more errors can be detected and corrected at a time.

In this thesis the problem of existence of larger extremal codes is investigated. The goal of the paper is to explore connection between the extremal and Quadratic Residue codes and to provide some tools to research putative self-dual codes.

In the first chapter we introduce the definitions, important for the whole thesis, i.e. a linear code, Hamming weight, weight spectrum of the code. We explain the concepts of self-dual and doubly-even codes and describe the general properties of such codes. The notion of extremality arise naturally in the end of the chapter.

The second chapter is crucial for understanding the work done. Here the we introduce the important concepts of cyclic codes and automorphism group, give the detailed description of Quadratic Residue codes. Further we give the two known examples of extremal codes. For both codes we find the full weight spectrum is found and examine thoroughly the automorphism group. It is very important for estimating the results adduced in subsequent chapters.

In the third chapter gives one can find a short review on the results concerning two first putative extremal codes. A lot of articles where studied to write down state-of-the-art. Here the possibilities for the order of automorphism group are concerned.

The main results of the thesis are collected in the fourth chapter. They concern the primes occurring in the order of the automorphism group of the code. Theorem 27 gives a general tool to explore putative self-dual codes. Theorem 34 establishes the connection between extremal and Quadratic Residue codes. This result's importance can be easily noticed if one concerns chapter 2. Theorem 34 describes the difference between the known and putative extremal codes.

In the final chapter we closely examine the low-weight vectors in Quadratic Residue codes. The algorithm of Karlin and MacWilliams is introduced and proved here. Here we show that larger Quadratic Residue codes are most likely not to be extremal. In other words Theorem 34 is backed with practical results.

§ 1. Duality in Coding

An $[n,k]$ linear code $\mathcal{C}$ over the binary field $\mathbb{F}_2$ is a k-dimensional subspace of $\mathbb{F}_2^n$. The Hamming weight wt of a vector a in $\mathbb{F}_2^n$ is defined by the number of its nonzero coordinates:

$$\mathrm{wt}(a) = |\{i|\ a_i \neq 0\}|\,.$$

We call $\mathcal{C}$ an $[n,k,d]$ code if d is the minimum among the weights of nonzero codewords in $\mathcal{C}$. If $u=(u_1,\ldots,u_n)$; $v=(v_1,\ldots,v_n)$ are the vectors with components in $\mathbb{F}_2$, then their scalar product will be

$$\langle u,v\rangle = u_1v_1 + ... + u_nv_n. \tag{1}$$

(All calculations are made in $\mathbb{F}_2$.)

If $\langle u,v\rangle = 0$, then the vectors u and v are called orthogonal. Since the characteristic of the field $\mathbb{F}_2$ is even it occur that $\langle a,a\rangle = 0$ even if $a \neq 0$.

Definition 1 *The dual (or orthogonal) code $\mathcal{C}^\perp$ is defined as the set of all vectors orthogonal to all codewords of $\mathcal{C}$, i.e.*

$$\mathcal{C}^\perp = \{u \in \mathcal{C} \mid \langle u,v\rangle = 0\ \forall v \in \mathcal{C}\}. \tag{2}$$

So, if $\mathcal{C}$ has the generator matrix G and the check matrix H then $\mathcal{C}^\perp$ has the generator matrix H and the check matrix G. Thus $\mathcal{C}^\perp$ is a $[n,n-k]$-code. $\mathcal{C}^\perp$ is a subspace, orthogonal to $\mathcal{C}$.

If $\mathcal{C} = \mathcal{C}^\perp$ than $\mathcal{C}$ is called self-dual. Thus the code $\mathcal{C}$ is self-dual if $\langle u,v\rangle = 0$ for each pair (not necessarily different) of codewords in $\mathcal{C}$ and has dimension $k = n/2$ (n must be an even number).

Let A_i be the number of codewords of weight i in the code $\mathcal{C}$.

$$A_i = |\{c \mid c \in \mathcal{C},\ \mathrm{wt}(c) = i\}|\,,\ (i = 0,...,n),$$

The set of all A_i for $i = 0,\ldots,n$ is called a weight spectrum of the code.

Let us call

$$W_{\mathcal{C}}(x,y) = \sum_{i=0}^{n} A_i x^{n-i}y^i = \sum_{u\in\mathcal{C}} x^{n-\mathrm{wt}(u)}y^{\mathrm{wt}(u)}. \tag{3}$$

the weight function. This polynomial generates the weight specter of the code. Here x and y are variables, and $W_{\mathcal{C}}(x,y)$ is the homogenous polynomial in x and y of the degree n. The property of homogenity of $W_{\mathcal{C}}(x,y)$ is often useful. We can always eliminate x, putting $x=1$ and nevertheless having the suitable weight function

$$W_{\mathcal{C}}(1,y) = W_{\mathcal{C}}(y) = \sum_{i=0}^{n} A_i y^i. \tag{4}$$

In the same way let A_i' be the number of the codewords of length i in the code $\mathcal{C}^\perp$. The weight function of the code $\mathcal{C}^\perp$ is then equal:

$$W_{\mathcal{C}^\perp}(x,y) = \sum_{i=0}^{n} A_i' x^{n-i}y^i = \sum_{u\in\mathcal{C}^\perp} x^{n-\mathrm{wt}(u)}y^{\mathrm{wt}(u)}. \tag{5}$$

The main result concerning dual codes is the fact that the polynomial $W_{\mathcal{C}^\perp}(x,y)$ can be defined through linear transformation of the polynomial $W_{\mathcal{C}}(x,y)$.

Theorem 1 (MacWilliams theorem for binary linear codes) *Let $\mathcal{C}$ be a linear binary $[n,k]$-code, and $\mathcal{C}^\perp$ its dual code. Then*

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x+y, x-y), \tag{6}$$

where $|\mathcal{C}| = 2^k$ is the number of the codewords in the code $\mathcal{C}$.

Proof. For a proof see [17, Chapter 5, Section 2]. □

In addition, the following identities, equivalent to (6) hold:

$$\sum_{j=0}^{n} A_i' x^{n-j} y^i = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} A_i (x+y)^{n-i} (x-y)^i \tag{7}$$

or

$$\sum_{u \in \mathcal{C}^\perp} x^{n-\mathrm{wt}(u)} y^{\mathrm{wt}(u)} = \frac{1}{|\mathcal{C}|} \sum_{u \in \mathcal{C}} (x+y)^{n-\mathrm{wt}(u)} (x-y)^{\mathrm{wt}(u)}. \tag{8}$$

The above equations are often called MacWilliams identities.

§ 2. Self-dual doubly-even codes

Assume now that $\mathcal{C}$ is a binary self-dual code such that the weights of all codewords are multiples of 4 (self-dual doubly-even code) and let $W(x,y)$ be its weight function. Since $\mathcal{C}$ is self-dual, Theorem 1 yields

$$W(x,y) = \frac{1}{2^{n/2}} W(x+y, x-y) = W(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) \tag{9}$$

(because $W(x,y)$ is a homogenous polynomial of the degree n). Since the weights of all codewords are multiples of 4, $W(x,y)$ contains only powers of y^4. Hence

$$W(x,y) = W(x, iy), \tag{10}$$

where $i = \sqrt{-1}$.

The following theorem of Gleason helps to find all polynomials $W(x,y)$ for which the equations (9) and (10) hold.

Theorem 2 (Gleason [11]) *Each polynomial for which* (9) *and* (10) *holds true is a polynomial in*

$$W_1(x,y) = x^8 + 14x^4y^4 + y^8$$

and

$$W_2(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24},$$

Corollary 3 *Instead of $W_2(x,y)$ one may prefer to take the polynomial*

$$W_2^{'}(x,y) = \frac{W_1(x,y)^3 - W_2(x,y)}{48} = x^4y^4(x^4-y^4)^4.$$

The following reformulation of Theorem 2 describes the properties of the weight function of self-dual doubly-even code.

Theorem 4 (Gleason [11]) *The weight function of a self-dual doubly-even code is a polynomial in W_1 and $W_2^{'}$.*

Corollary 5 *The length of binary self-dual doubly-even code is a multiple of 8.*

Theorem 4 was used to find an upper bound for the minimal distance of self-dual doubly-even codes.

Let $\mathcal{C}$ denote an $[n, n/2, d]$ self-dual doubly-even code with the weight function

$$W(x,y) = x^n + A_d x^{n-d}y^d + \ldots = \sum_{j=0}^{n/4} A_{4j}x^{n-4j}y^{4j}, \tag{11}$$

which is a polynomial in $W_1(x,y)$ and $W_2^{'}(x,y)$ (Theorem 4). Since $\deg W(x,y) = n$, it may be written as follows:

$$W(x,y) = \sum_{j=0}^{D} a_j W_1(x,y)^{n-24j} W_2^{'}(x,y)^j, \tag{12}$$

where $D = \left\lfloor \frac{n}{24} \right\rfloor$.

From (11) and (12) we get:

$$\sum_{j=0}^{D} a_j W_1(x,y)^{n-24j} W_2^{'}(x,y)^j = \sum_{j=0}^{n/4} A_{4j}x^{n-4j}y^{4j}. \tag{13}$$

We choose now $a_0, a_1, \ldots, a_D \in \mathbb{Z}$ so that the greatest possible number of the leading terms in $W(x,y)$ equal zero. The corresponding polynomial $W^*(x,y)$ will be the weight function of the self-dual doubly-even code with the greatest minimum weight possible, that we hope to reach. It is called the extremal weight function.

If the code with the weight function $W^*(x,y)$ exists then it has the minimum distance $d^* = 4(D+1)$. This result is stated in the following

Theorem 6 (Mallows and Sloane [18]) *The number A^*_{4D+4} of codewords of the minimum weight in the extremal weight function is given by the following expressions:*

$$\binom{n}{5}\binom{5D-2}{D-1}\Big/\binom{4D+4}{5}, \ if\ n = 24D; \tag{14}$$

$$\frac{1}{4}n(n-1)(n-2)(n-4)\frac{(5D)!}{D!(4D+4)!}, \ if\ n = 24D+8; \tag{15}$$

$$\frac{3}{2}n(n-2)\frac{(5D+2)!}{D!(4D+4)!}, \ if\ n = 24D+16. \tag{16}$$

and this number is never equal to zero. Thus, the minimum distance of the self-dual doubly-even code of length n equals at most $4\lfloor n/24 \rfloor + 4$.

For large n the weight function contains a negative coefficient and thus the described bound cannot be reached and there is no extremal doubly-even code.

Mallows and Sloane have not given an explicit bound for n. The best of what we know today is a result of Zhang ([26]), by which there is no extremal code for $n > 3928$.

From now on we shall concentrate on the case $n = 24m$. If 24 divides length of $\mathcal{C}$ then the codewords of a fixed weight form a 5-design (Assmus and Mattson [1]). $[24m, 12m, 4m + 4]$ extremal codes are also of great interest because of the bound from Theorem 6. But there are only two known examples of such extremal codes: the $[24, 12, 8]$ Golay code and the $[48, 24, 12]$ code — which are both Quadratic Residue codes.

2 Examples of extremal codes

§ 1. Definitions

Here we shall introduce some definitions crucial for coding theory and necessary for this and subsequent chapters.

Definition 2 *Matrix G is called a generator matrix of the binary $[n,k]$-code $\mathcal{C}$ if all codewords of $\mathcal{C}$ can be obtained as linear combinations of the rows of G*

Remark 1 *If $\mathbb{F}_2$ is the binary field then the operation of acting on all vectors from $\mathbb{F}_2$ is equivalent to writing out all linear combinations of rows of matrix G.*

Let R denote the ring $\mathbb{F}_2[x]/(x^n-1)$.

Definition 3 *The code $\mathcal{C} \subseteq R$ is called a cyclic code if it is an ideal of the ring R. The cyclic code contains all shifts of any of its codewords.*

Remark 2 *An ideal of the ring R (and thus a cyclic code) can be generated by a single polynomial.*

Let $\mathcal{C}$ be a cyclic code, $g(x)$ being a generating polynomial.

Definition 4 *A polynomial*

$$h(x) = (x^n-1)/g(x) = \sum_{i=0}^{k} h_i x^i,\ h_k \neq 0$$

is called check polynomial.

The reason of this name is given by the following fact. If

$$c(x) = \sum_{i=0}^{n-1} c_i x^i \equiv f(x)g(x) \mod x^n - 1$$

is an arbitrary codeword from $\mathcal{C}$ then

$$c(x)h(x) = \sum_{i=0}^{n-1} c_i x^i \sum_{j=0}^{k} h_j x^j = f(x)g(x)h(x) = 0.$$

The coefficient at x^j in this product is equal

$$\sum_{i=0}^{n-1} c_i h_{j-i}, \quad j = 0, 1, \ldots, n-1, \tag{17}$$

where the indices are taken modulo n. The equations (17) define check equations, which the code must satisfy. Let

$$H = \begin{bmatrix} & & h_k & \dots & h_2 & h_1 & h_0 \\ & h_k & \dots & h_2 & h_1 & h_0 & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_k & \dots & h_2 & h_1 & h_0 & & \end{bmatrix}, \tag{18}$$

Then (17) means that, if $c \in \mathcal{C}$ then $Hc^T = 0$. Since $k = \deg h(x) = n - \deg g(x)$ is the dimension of $\mathcal{C}$ and since the rows of H are lineary independent, the condition $Hc^T = 0$ is also sufficient for a vector c to belong to the code. Thus H is a check matrix of the code $\mathcal{C}$.

Lemma 7 *The dual code $\mathcal{C}^\perp$ is the cyclic code with the generating polynomial*

$$g^\perp(x) = x^{\deg h(x)} h(x^{-1}).$$

Proof. The statement results from (18). □

According to this theorem the code with generating polynomial $h(x)$ is equivalent to the code $\mathcal{C}^\perp$. In fact it consists of the codewords of $\mathcal{C}^\perp$, written in the inverse order.

Definition 5 *The automorphism group* $\mathrm{Aut}(\mathcal{C})$ *of a linear code $\mathcal{C}$ in $\mathbb{F}_2^n$ is defined as the group of monomial matrices $M \in \mathrm{GL}(n, K)$ that leave $\mathcal{C}$ invariant, i.e. $\mathcal{C}M = \mathcal{C}$. A matrix M is called monomial if M has only one element nonequal 0 from $\mathbb{F}_2$ in every row and every column.*

Remark 3 *For $\mathbb{F}_2$ a monomial matrix is a permutation matrix. So if $\mathcal{C}$ is a linear code over a binary field then:*

$$\mathrm{Aut}(\mathcal{C}) = \{\sigma |\ \sigma(c) \in \mathcal{C}\ \forall c \in \mathcal{C}\}.$$

Definition 6 *A polynomial $E(x)$ in R is called an idempotent if $E(x) = E^2(x) = E(x^2)$.*

Definition 7 *A cyclotomic class modulo n over $GF(q)$ is defined as:*

$$C_s = \{s, sq, sq^2, \dots, sq^{m_s - 1}\},$$

where $sq^{m_s} \equiv s \pmod{n}$. (Choosing the smallest integer as s in C_s is convenient but not essential.) The set of integers modulo n breaks up into cyclotomic classes:

$$\{0, 1, \dots, n-1\} = \bigcup_s C_s,$$

where s runs over the set of representatives of classes modulo n.

Definition 8 *Let the group G act on the set X. The group action $G \times X \to X$ is called transitive if for any two $x, y \in X$ there exists a $g \in G$ such that $g \cdot x = y$. The group action is called n-transitive if for any pairwise distinct $x_1, \dots, x_n$ and pairwise distinct $y_1, \dots, y_n$ there is a $g \in G$ such that $g \cdot x_k = y_k$ for $1 \le k \le n$.*

§ 2. Quadratic Residue codes

Since the both known examples of extremal self-dual doubly-even codes belong to the class of Quadratic Residue codes we will need to know what these codes are. The information introduced here will be used in following chapters. Also the main result of the thesis is inseparably linked with Quadratic Residue codes.

Binary Quadratic Residue codes are cyclic codes (i.e. all shifts of a codeword still belong to the code) over the field $\mathbb{F}_2$ with length p, where p is a prime number, 2 being a quadratic residue modulo p. It means that $p \equiv \pm 1 \pmod 8$.

Let Q denote the set of quadratic residues modulo p, N denoting the set of non-residues. If ρ is a primitive element of GF(p) then $\rho^e \in Q$ if and only if e is even, and $\rho^e \in N$ iff e is odd. Thus Q is a cyclic group, generated by the element ρ^2. Since $2 \in Q$, the set Q is closed under multiplication by 2. Hence Q is a union of disjoint cyclotomic classes modulo p. Thereby if α is a primitive p-th root of unity in the field extension of $\mathbb{F}_2$ then the coefficient of polynomials

$$q(x) = \prod_{r \in Q}(x - \alpha^r) \text{ and } n(x) = \prod_{n \in N}(x - \alpha^n) \tag{19}$$

lie in the field $\mathbb{F}_2$. And

$$x^p - 1 = (x - 1)q(x)n(x). \tag{20}$$

Once again we put $R = \mathbb{F}_2[x]/(x^p - 1)$.

Definition 9 *Quadratic Residue codes $\mathcal{L}$, $\overline{\mathcal{L}}$, $\mathcal{N}$, $\overline{\mathcal{N}}$ are the cyclic codes (ideals) of ring R, generated correspondingly by polynomials*

$$q(x),\ (x-1)q(x),\ n(x),\ (x-1)n(x). \tag{21}$$

Sometimes $\mathcal{L}$ and $\mathcal{N}$ are called extended QR-codes.

Since the permutation $x \to x^n$ (n is a fixed nonresidue) of the set of coordinates of R translates $\mathcal{L}$ into $\mathcal{N}$ and vice versa, these two codes are equivalent.

For the minimal distance of a QR-code holds

Theorem 8 (Square root bound for minimal distance) *If d is the minimal distance of the code $\mathcal{L}$ or $\mathcal{N}$ then $d^2 \geq p$. If $p = 4k-1$ then this bound may be strengthened as follows:*

$$d^2 - d + 1 \geq p. \tag{22}$$

Proof. Let $a(x)$ be a codeword of minimal nonzero weight d in the code $\mathcal{L}$. If n is a nonresidue then $\bar{a}(x) = a(x^n)$ is a word of minimal weight in $\mathcal{N}$. Hence $a(x)\bar{a}(x)$ must belong to intersection $\mathcal{L} \cap \mathcal{N}$, i.e. be a multiple of a polynomial

$$\prod_{r \in Q}(x - \alpha^r) \prod_{n \in N}(x - \alpha^n) = \prod_{j=1}^{p-1}(x - \alpha^j) = \sum_{j=0}^{p-1} x^j. \tag{23}$$

Hence, the weight of product $a(x)\bar{a}(x)$ equals p. Since the weight of polynomial $a(x)$ equals d, the maximal number of nonzero coefficients in $a(x)\bar{a}(x)$ is at most d^2. So $d^2 \geq p$.

If $p = 4k - 1$ we can choose $n = -1$. Then in the considered product there are d factors, that are equal 1, so that maximal weight is at most $d^2 - d + 1$. $\square$

If $p = 4k-1$ then one can choose α so that the generating idempotents of the codes $\mathcal{L}$, $\overline{\mathcal{L}}$, $\mathcal{N}$, $\overline{\mathcal{N}}$ would correspondingly be:

$$E_q(x) = \sum_{r \in Q} x^r;\ \overline{E_q}(x) = 1 + \sum_{n \in N} x^n;\ E_n(x) = \sum_{n \in N} x^n;\ \overline{E_n}(x) = 1 + \sum_{r \in Q} x^r. \qquad (24)$$

Theorem 9

$$\mathcal{L}^\perp = \overline{\mathcal{L}};\ \mathcal{N}^\perp = \overline{\mathcal{N}},\ \textit{if } p = 4k - 1; \qquad (25)$$

$$\mathcal{L}^\perp = \overline{\mathcal{N}};\ \mathcal{N}^\perp = \overline{\mathcal{L}},\ \textit{if } p = 4k + 1. \qquad (26)$$

In both cases $\mathcal{L}$ is generated by $\overline{\mathcal{L}}$ and the all-ones vector, $\mathcal{N}$ is generated by $\overline{\mathcal{N}}$ and the all-ones vector.

Let us find the generating matrices of these codes. Let

$$F_q(x) = \sum_{i=0}^{p-1} f_i x^i$$

be the idempotent, generating the code $\overline{\mathcal{L}}$. Then the generating matrix of the code $\overline{\mathcal{L}}$ is a $p \times p$ cyclic matrix

$$\overline{G} = (g_{ij}) = \begin{bmatrix} f_0 & f_1 & \dots & f_{p-1} \\ f_{p-1} & f_0 & \dots & f_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & \dots & f_0 \end{bmatrix}, \qquad (27)$$

where $0 \le i;\ j \le p-1;\ g_{ij} = f_{j-i}$ and indices are calculated modulo p. The generating matrix of the code $\mathcal{L}$ is

$$\left[\frac{\overline{G}}{1\,1\dots1}\right], \qquad (28)$$

Similar equalities take place for $\mathcal{N}$ and $\overline{\mathcal{N}}$. The rank of the matrix $\overline{G}$ is $(p-1)/2$.
QR-codes allow extensions by adding an even parity check, so that

$$\left.\begin{array}{rl} (\widehat{\mathcal{L}})^\perp = \widehat{\mathcal{L}};\ (\widehat{\mathcal{N}})^\perp = \widehat{\mathcal{N}}, & \text{if } p = 4k - 1, \\ (\widehat{\mathcal{L}})^\perp = \widehat{\mathcal{N}}; & \text{if } p = 4k + 1; \end{array}\right\} \qquad (29)$$

where " $\widehat{\ }$ " means the extended code. The codes $\widehat{\mathcal{L}}$ and $\widehat{\mathcal{N}}$ are $[p+1, (p+1)/2]$-codes.

Theorem 10 *If $p = 4k - 1$ then the extended QR-codes $\widehat{\mathcal{L}}$ and $\widehat{\mathcal{N}}$ are self-dual.*

Proof. We can get the generating matrix of the code $\widehat{\mathcal{L}}$ from the matrix (28) by adding a column:

$$\widehat{G} = \left[\begin{array}{c|c} & 0 \\ & 0 \\ \overline{G} & \vdots \\ & 0 \\ \hline 1\,1\ldots 1 & 1 \end{array}\right], \tag{30}$$

Since $\overline{\mathcal{L}} \subset (\overline{\mathcal{L}})^{\perp}$, each row of $\overline{G}$ is orthogonal to itself and to any other row of $\overline{G}$. Hence, each row of $\widehat{G}$ is orthogonal to itself and to any other row of $\widehat{G}$, so that $\widehat{\mathcal{L}} \subset (\widehat{\mathcal{L}})^{\perp}$. And since the rank of $\widehat{G}$ is equal $(p+1)/2$, then $\widehat{\mathcal{L}} = (\widehat{\mathcal{L}})^{\perp}$. □

Remark 4 *If $p = 4k+1$ then the extended code can be defined so that the equality $\widehat{\mathcal{L}} = (\widehat{\mathcal{N}})^{\perp}$ holds.*

Lemma 11 *Let $\mathcal{C}$ be a binary code, $\mathcal{C} \subset \mathcal{C}^{\perp}$. Each codeword of $\mathcal{C}$ has an even weight. Moreover, if the weight of each row of the generating matrix of $\mathcal{C}$ is a multiple of 4, then this property holds for each codeword of $\mathcal{C}$.*

Theorem 12 *If $p = 4k-1$ then the weight of each word of the code $\widehat{L}$ is a multiple of 4, and the weight of each word of the code $\mathcal{L}$ is congruent 0 or 3 modulo 4.*

Proof. If 2 is a quadratic residue modulo p than $p = 8m \pm 1$. Thus we can assume, that $p = 8m-1$. The number of residues and nonresidues in this case is equal $4m-1$ and thus the weight of each row of matrix $\overline{G}$ is a multiple of 4. The statement of the theorem results from Lemma 11. □

Remark 5 *If $p = 4k+1$, then the only thing one can say about the weight of words of the code $\widehat{\mathcal{L}}$ is that it is even.*

We will show now that the extended QR-code $\widehat{\mathcal{L}}$ is invariant under the permutation group $PSL_2(p)$.

Definition 10 *Let $p = 8m \pm 1$ be a prime number. The collection of all permutations on the set $\{0, 1, 2, \ldots, p-1, \infty\}$ of the form*

$$y \to \frac{ay+b}{cy+d}, \tag{31}$$

where $a, b, c, d \in GF(p)$ and $ad - bc = 1$ form a group, called the projective special liner group $PSL_2(p)$ (it is sometimes also called the linear fractional group).

Lemma 13 *(a). The group $PSL_2(p)$ is generated by three permutations:*

$$\begin{cases} S: \ y \to y+1; \\ V: \ y \to \rho^2 y; \\ T: \ y \to -(1/y), \end{cases} \tag{32}$$

where ρ is a primitive element of the field $GF(p)$.

(b). The group $PSL_2(p)$ consists of $p(p^2-1)/2$ permutations of the form

$$V^i S^j: \ y \to \rho^{2i} y + j;$$
$$V^i S^j T S^k: \ y \to k - (\rho^{2i} y + j)^{-1}.$$

Proof. A typical element of the group $PSL_2(p)$

$$y \to \frac{ay+b}{cy+d}, \qquad ad - bc = 1,$$

may be written either as $y \to ay^2 + ab$, if $c = 0$ (since in this case $d = 1/a$), or as $y \to \frac{a}{c} - \frac{1}{c^2 y + cd}$, if $c \neq 0$ (since in this case $b = \frac{ad}{c} - \frac{1}{c}$). It gives respectively $V^i S^{ab}$ (where $a = \rho^i$) and $V^i S^{cd} T S^{a/c}$ (where $c = \rho^i$). □

Proposition 14 *The group $PSL_2(p)$ acts 2-transitively on $\{0, 1, \ldots, p-1, \infty\}$.*

Lemma 15 (Perron [21]) *(i). Let $p = 4k-1$, let $r_1, \ldots, r_{2k}$ be $2k$ quadratic residues modulo p, including 0, and let a be coprime p. Then among $2k$ numbers of the form $r_i + a$ there are k residues (possibly including 0) and k nonresidues.*

(ii). Let $p = 4k-1$, let $n_1, \ldots, n_{2k-1}$ be $(2k-1)$ nonresidues modulo p and let a be coprime p. Then among $2k-1$ numbers of the form $n_i + a$ there are k residues (possibly including 0) and $k-1$ nonresidues.

(iii). Let $p = 4k+1$. Among $2k+1$ numbers of the form $r_i + a$ there are $k+1$ residues (including 0) and k nonresidues, if a is residue itself, and k residues (excluding 0) and $k+1$ nonresidues, if a is nonresidue.

(iv). Let $p = 4k+1$. Among $2k$ numbers of the form $n_i + a$ there are k residues (excluding 0) and k nonresidues, if a is residue itself, and $k+1$ residues (including 0) and $k-1$ nonresidues, if a is nonresidue.

Theorem 16 (Gleason and Prange) *If $p = 8m \pm 1$ then the extended QR-code $\widehat{L}$ is invariant under the group $PSL_2(p)$.*

Proof. Since the generating idempotent of the code $\mathcal{L}$ is invariant under permutation V, permutation S being a cyclic shift, then the code $\mathcal{L}$, and thus the code $\widehat{\mathcal{L}}$ are invariant under S and V. According to Lemma 13 we now shall prove the invariance

of $\widehat{\mathcal{L}}$ under permutation T. We shall consider only the case $p = 8m-1$ and show, that each row of the matrix (30), i.e. the matrix

$$\widehat{G} = \left[\begin{array}{c|c} & 1 \\ & 1 \\ \overline{G} & \vdots \\ & 1 \\ \hline 1\,1\ldots 1 & 1 \end{array}\right], \tag{33}$$

is transformed under the action of permutation T into another word of the code $\widehat{\mathcal{L}}$.

1) The first row of matrix $\widehat{G}$, say, R_0 is equal

$$\left| 1 + \sum_{n\in N} x^n \right| 0 \Big|.$$

Then

$$T(R_0) = \left| \sum_{r\in Q} x^r \right| 1 \Big| = R_0 + 1 \in \widehat{\mathcal{L}}.$$

2) Let $s \in Q$; $(s+1)$ row of the matrix $\widehat{G}$ is equal:

$$R_s = \left| x^s + \sum_{n\in N} x^{n+s} \right| 0 \Big|.$$

We shall show, that $T(R_s) = R_{-1/s} + R_0 \in \widehat{\mathcal{L}}$. For that we shall separately for each member of the equality analyze the coordinates containing symbol 1. Vector $T(R_s)$ contains symbol 1 at the coordinates $-1/s$ and $-1/(n+s)$ for $n \in N$, what includes ∞ (if $n = -s$), $2m-1$ residues and $2m$ nonresidues (according to Lemma 15). Vector

$$R_{-1/s} = \left| x^{-1/s} + \sum_{n\in N} x^{n-1/s} \right| 0 \Big|$$

contains symbol 1 at the coordinates $-1/s$ and $n-1/s$, including $2m$ residues and $2m$ nonresidues. Hence, $T(R_s)+R_{-1/s}$ contains symbol 1 at the coordinate ∞ and symbol 0 at the coordinate $-1/s$ (nonresidue). If $-1/(n+s) \in N$ then $-1/(n+s) = n' - 1/s$ for some $n' \in N$, and symbols 1 cancel out. Thus, coordinates, corresponding to nonresidues always contain symbol 0. On the other hand, if $-1/(n+s) \in Q$, then $-1/(n+s) \neq n'-1/s$, for all $n' \in N$ and coordinates, corresponding to residues contain symbol 1. Thus,

$$T(R_s) + R_{-1/s} = \left| \sum_{r\in Q} x^r \right| 1 \Big| = R_0 + 1.$$

Similarly, if $t \in N$, then $T(R_t) = R_{-1/t} + R_0$. □

From Theorem 16 it results that the group $\mathrm{Aut}\,(\mathcal{C})$ contains $PSL_2(p)$. There are cases, when $\mathrm{Aut}\,(\mathcal{C})$ is indeed larger than $PSL_2(p)$. If $p = 7$ the code $\widehat{\mathcal{L}}$ is a $[8, 4, 4]$ Hamming code and $\left|\mathrm{Aut}\,(\widehat{\mathcal{L}})\right| = 1344$ ([17, Chapter 13, Theorem 24]). And if $p = 23$ the code $\widehat{\mathcal{L}}$ is an extended Golay code and its automorphism group $\mathrm{Aut}\,(\widehat{\mathcal{L}})$ is equal to the Mathieu group.

It seems plausible that for other values of p the group $\mathrm{Aut}\,(\widehat{\mathcal{L}})$ is isomorphic to the group $PSL_2(p)$. This conjecture holds in many cases.

Theorem 17 (Assmus and Mattson) *If $(p-1)/2$ is a prime and $5 < p \leq 4079$ then, excluding the two cases, the group $\mathrm{Aut}\,(\widehat{\mathcal{L}})$ is equal (isomorphic) to the group $PSL_2(p)$.*

§ 3. The Golay code

The Golay code is perhaps one of the most important of all codes. It is a $[24, 12, 8]$ Quadratic Residue code, but for closer familiarity we shall use the following

Definition 11 *The extended Golay code $\mathcal{G}_{24}$ is the code with generator matrix G:*

l_∞	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8	l_9	l_{10}	r_∞	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	*row*
1	1												1	1		1	1	1				1		0
1		1												1	1		1	1	1				1	1
1			1										1		1	1		1	1	1				2
1				1										1		1	1		1	1	1			3
1					1										1		1	1		1	1	1		4
1						1										1		1	1		1	1	1	5
1							1						1				1		1	1		1	1	6
1								1					1	1				1		1	1		1	7
1									1				1	1	1				1		1	1		8
1										1				1	1	1				1		1	1	9
1											1		1		1	1	1				1		1	10
1												1	1	1	1	1	1	1	1	1	1	1	1	11

the columns are numbered as follows: $l_\infty, l_0, \ldots, l_{10}, r_\infty, r_0, \ldots, r_{10}$.

One can easily notice that the sum of any two rows of G has the weight 8.

Lemma 18 *The code $\mathcal{G}_{24}$ is self-dual: $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.*

Proof. If u and v are two (not necessarily different) rows of G then $\mathrm{wt}(\langle u, v\rangle) \equiv 0 \pmod 2$. Hence each row of G is orthogonal to all other rows and thus $\mathcal{G}_{24} \subset \mathcal{G}_{24}^{\perp}$. But the rank of G is 12, that is why the code $\mathcal{G}_{24}$ has dimension 12, and hence $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$. □

Remark 6 *Since $\mathcal{G}_{24}$ is self-dual and the weight of any row of its generator matrix G is a multiple of 4, the code $\mathcal{G}_{24}$ is doubly-even.*

Lemma 19 *If the code $\mathcal{G}_{24}$ contains the codeword $|L|R|$, where $L = a_\infty a_0 a_1 a_2 \dots a_{10}$, $R = b_\infty b_0 b_1 b_2 \dots b_{10}$, then it contains a codeword $|L'|R'|$, where $L' = b_\infty b_0 b_{10} b_9 \dots b_1$ and $R' = a_\infty a_0 a_{10} a_9 \dots a_1$.*

Remark 7 *It follows directly from Lemma that if the code $\mathcal{G}_{24}$ contains a codeword $|L|R|$ with weights $\mathrm{wt}(L) = i$ and $wt(R) = j$ then it contains a codeword $|L'|R'|$ with weights $\mathrm{wt}(L') = j$; $\mathrm{wt}(R') = i$.*

By Remark 6 for weights of the codewords in $\mathcal{G}_{24}$ we have the following possibilities: 0, 4, 8, 12, 16, 20, 24.

If for some u we have $\mathrm{wt}(u) = 20$ then $\mathrm{wt}(u+1) = 4$. We show now, that there are no codewords of weight 4 in the code, and thus there are no words of weight 20.

Lemma 20 *The code $\mathcal{G}_{24}$ does not contain the codewords of weight 4.*

Proof. For each codeword $|L|R|$ from $\mathcal{G}_{24}$ we have that $\mathrm{wt}(L) \equiv \mathrm{wt}(R) \equiv 0 \pmod 2$. By previous Lemma we can assume that the codeword of weight 4 belongs to one of the following types.

(1) $\mathrm{wt}(L) = 0,\ \mathrm{wt}(R) = 4$;

(2) $\mathrm{wt}(L) = 2,\ \mathrm{wt}(R) = 2$.

Condition (1) is not possible: $\mathrm{wt}(L) = 0$ if we take either no rows at all or only the last row of G. In these cases $\mathrm{wt}(R) = 0$ or 12. Condition (2) is not possible either, because if $\mathrm{wt}(L) = 2$ then L equals sum of one or two rows of G, possibly with addition of the last row. In each of these cases $\mathrm{wt}(R) = 6$. □

So in the code $\mathcal{G}_{24}$ there are only weights 0, 8, 12, 16, 24. As earlier we denote by A_i the number of the codewords of weight i. Then $A_0 = A_{24} = 1$; $A_8 = A_{16}$. For each left part of the codeword L there are two corresponding right parts R and $\overline{R}$ (due to last row of G). If $\mathrm{wt}(L) = 0$, then $\mathrm{wt}(R) \neq 4$ (by Lemma 20) and $\mathrm{wt}(R) \neq 8$ (else $\mathrm{wt}(\overline{R}) = 4$ which contradicts Lemma 20 once again), thus $\mathrm{wt}(R) = 0$ or 12. If $\mathrm{wt}(L) = 2$, then by the same reasoning we have that $\mathrm{wt}(R) = 6$. Continuing like this we get the following possibilities for weight distribution in the code $\mathcal{G}_{24}$:

Number	$\mathrm{wt}(L)$	$\mathrm{wt}(R)$	$\mathrm{wt}(\overline{R})$	Full	weight
1	0	0	12	0	12
$11 + \binom{11}{2}$	2	6	6	8	8
$\binom{11}{3} + \binom{11}{4}$	4	4	8	8	12
$\alpha = ?$	6	2	10	8	16

By Lemma 19 α is equal the number of codewords of the type $(2,6)$ that is $2\left(11+\binom{11}{2}\right)$.

Hence $A_8=\left(11+\binom{11}{2}\right)+\binom{11}{3}+\binom{11}{4}=759$, and thus $A_{12}=2576$. Thus we have shown that the weight spectrum of the code $\mathcal{G}_{24}$ is

$$\begin{array}{lccccc} i: & 0 & 8 & 12 & 16 & 24 \\ A_i: & 1 & 759 & 2576 & 759 & 1 \end{array}$$

Since now all the presented properties of the Golay-code $\mathcal{G}_{24}$ were achieved directly from the definition of the code through the generator matrix.

Since the Golay code $\mathcal{G}_{24}$ is the extended quadratic residue code, it is invariant under the group $PSL_2(23)$. But we will show, that its automorphism group is a larger Mathieu group.

The coordinates of the code $\mathcal{G}_{24}$ will be enumerated by the elements of the set $\Omega=\{0,1,\ldots,22,\infty\}$, where the last coordinate corresponds to the general even parity check. Let the sets:

$$\begin{array}{l} Q=\{1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 13,\ 16,\ 18\}; \\ N=\{5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 22\} \end{array} \tag{34}$$

denote quadratic residues and nonresidues modulo 23.

We will define the code $\mathcal{G}_{23}$ as the cyclic code with generating idempotent

$$\theta(x)=\sum_{i\in N}x^i \tag{35}$$

and generating polynomial

$$(1+x+x^{20})\theta(x)=1+x^2+x^4+x^5+x^6+x^{10}+x^{11}. \tag{36}$$

The the code $\mathcal{G}_{24}$ is obtained by adding the general even parity check to the code $\mathcal{G}_{23}$, and its generating matrix is

$$\left[\begin{array}{c|c} & 1 \\ & 1 \\ \Pi & \vdots \\ & 1 \\ \hline 1\,1\ldots 1 & 1 \end{array}\right], \tag{37}$$

where Π is a 23×23-circulant matrix, $\theta(x)$ being its first row. The $(i+1)$-st row of the matrix (37) is equal $|x^i\theta(x)|1|$, where $0\le i\le 22$.

According to Theorem 16 the code $\mathcal{G}_{24}$ is invariant under the group $PSL_2(23)$ of order $\frac{1}{2}\cdot 23\cdot(23^2-1)=6072$. It is generated by the permutations of element of the set Ω ((38)):

$$\begin{array}{l} S:\ i\to i+1; \\ V:\ i\to 2i; \\ T:\ i\to -\frac{1}{i}, \end{array} \tag{38}$$

In other words,

$$S = (\infty)(0\ 1\ 2\ 3\ \ldots\ 22);$$
$$V = (\infty)(0)(1\ 2\ 4\ 8\ 16\ 9\ 18\ 13\ 6\ 12)(5\ 10\ 20\ 17\ 11\ 22\ 21\ 19\ 15\ 7\ 14);$$
$$T = (\infty\ 0)(1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18).$$

Definition 12 ([7]) *The Mathieu group M_{24} is a group generated by permutations S, V, T and W, where*

$$W : \begin{cases} \infty \to 0, \quad 0 \to \infty \\ i \to -(\frac{1}{2}i)^2, \text{ if } i \in Q, \\ i \to (2i)^2, \text{ if } i \in N, \end{cases} \tag{39}$$

or equivalently

$$W = (\infty\ 0)(3\ 15)(1\ 17\ 6\ 14\ 2\ 22\ 4\ 19\ 18\ 11)(5\ 8\ 7\ 12\ 10\ 9\ 20\ 13\ 21\ 16).$$

Theorem 21 *The code $\mathcal{G}_{24}$ is invariant under the group M_{24}.*

Proof. We only have to check, that the code $\mathcal{G}_{24}$ is invariant under the permutation W. Clearly

$$W(|\theta(x)|1|) = |\theta(x)|1| + 1 \in \mathcal{G}_{24};$$
$$W(|x\theta(x)|1|) = |x^2\theta(x) + x^{11}\theta(x) + x^{20}\theta(x)|1| \in \mathcal{G}_{24};$$
$$W(|x^{22}\theta(x)|1|) = |\theta(x) + x\theta(x) + x^{20}\theta(x) + x^{22}\theta(x)|0| \in \mathcal{G}_{24}.$$

Now we use the identity

$$VW = W^2V = (\infty\ 0)(18\ 21)(1\ 22\ 16\ 20\ 6\ 10\ 13\ 15\ 12\ 17)(2\ 19\ 3\ 14\ 8\ 5\ 9\ 11\ 4\ 7). \tag{40}$$

Since $V(|x^i\theta(x)|1|) = |x^{2i}\theta(x)|1|$, we obtain that

$$W(|x^{2i}\theta(x)|1|) = (VW)(|x^i\theta(x)|1|) = (WV^2)(|x^i\theta(x)|1|),$$

and thus W convert each row of (37) into the codeword of $\mathcal{G}_{24}$. □

Proposition 22 ([7]) *(a). The group M_{24} is 5-transitive.*

(b). $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 244823040$.

In general for QR-codes there is no better result concerning the automorphisms group then Theorem 16. Notice that it claims only, that if $\mathcal{C}$ is a $[p+1, (p+1)/2]$ extended QR-code then $PSL_2(p) \subset \operatorname{Aut}\mathcal{C}$. For the Golay code $\mathcal{G}_{24}$ we can not only extend the automorphisms group ($PSL_2(23) \subset M_{24} \subset \operatorname{Aut}\mathcal{C}$). Also holds

Theorem 23 *M_{24} is the full automorphisms group of the code $\mathcal{G}_{24}$, i.e. $M_{24} = \operatorname{Aut}\mathcal{G}_{24}$.*

§ 4. A quadratic residue $[48, 24, 12]$ code

According to Theorems 10 and 12 a $[48, 24]$ QR-code is a self-dual doubly-even code.

Theorem 24 (Sphere-packing bound, or Hamming bound) *If there is a binary code of length n, correcting t errors and containing M codewords, then the following inequality holds*

$$M\left(1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{t}\right)\leq 2^n. \tag{41}$$

Theorem 25 (van Tilborg [25]) *If $\mathcal{L}$ is a binary QR-code of the length $p=8m-1$ and $d^2-d+1=p$, then:*

(i) $p=64i^2+40i+7\geq 2551$ *and* $d=8i+3$ *for some* i*;*

(ii) there exists a projective plane of order $d-1$*.*

If $d^2-d+1>p$ *then* $d^2-d-11\geq p$*.*

Proposition 26 *Let the code $\mathcal{C}$ be invariant under a transitive permutation group. Then:*

(i). Removal of any coordinate leads to equivalent codes $\mathcal{C}^*$.

(ii). If the weights of all words of the code $\mathcal{C}$ are even then the minimal weight in the code $\mathcal{C}^*$ is odd.

It results from this theorem that the minimal distance d of the $[47, 24]$ QR-code satisfies the condition $d\geq 11$. Inequality $d\geq 13$ is not possible by the sphere-packing bound (Theorem 24). Hence, according to Theorem 12, d equals 11 or 12. But by Proposition 26, d must be odd, which results that $d=11$. And hence the minimal distance of $[48, 24]$ QR-code is actually 12.

The weight function of the code is a homogenous polynomial of degree 48:

$$W(x,y)=x^{48}+A_{12}x^{36}y^{12}+\ldots\ . \tag{42}$$

The coefficients by $x^{47}y, x^{46}y^2, \ldots, x^{37}y^{11}$ are equal to zero. Here A_{12} is an unknown number of codewords of weight 12. Remarkably that because of the expression (42) the weight function of the code is fully defined by Theorem 4. It states that $W(x,y)$ must be a polynomial of $W_1(x,y)$ and $W_2'(x,y)$. And since $W(x,y)$ is a homogenous polynomial of degree 48, W_1 is homogenous of degree 8 and W_2' homogenous of degree 24, $W(x,y)$ must be a linear combination of W_1^6, $W_1^3W_2'$ and $(W_2')^2$.

Thus, Theorem 4 states that

$$W(x,y)=a_0W_1^6+a_1W_1^3W_2'+a_2(W_2')^2 \tag{43}$$

for some real a_0, a_1, a_2. Expanding (43) we have

$$\begin{aligned} W(x,y)=a_0(x^{48}+84x^{44}y^4+2946x^{40}y^8+\ldots)+\\ +a_1(x^{44}y^4+38x^{40}y^8+\ldots)+a_2(x^{40}y^8-\ldots), \end{aligned} \tag{44}$$

and, equating coefficients in (43) and (44) we obtain that

$$a_0 = 1; \qquad a_1 = -84; \qquad a_2 = 246.$$

Hence, $W(x, y)$ is defined uniquely. Substituting a_0, a_1, a_2 into (44) we find that

$$\begin{aligned} W(x,y) = x^{48} + 17\,296\, x^{36}y^{12} + 535\,095\, x^{32}y^{16} + 3\,995\,376\, x^{28}y^{20} + \\ +7\,681\,680\, x^{24}y^{24} + 3\,995\,376\, x^{20}y^{28} + 535\,095\, x^{16}y^{32} + 17\,296\, x^{12}y^{36} + y^{48}. \end{aligned} \tag{45}$$

Direct computation of this weight function would have required finding the weights of every of $2^{24} \approx 1,7 \cdot 10^7$ codewords, i.e. considerable timeconsuming for any computer.

3 Results on putative self-dual doubly-even $[72, 36, 16]$ and $[96, 48, 20]$ codes

In 1973 Sloane [24] posed a question which remained unresolved until now: is there a self-dual doubly-even $[72, 36, 16]$ code?

The automorphism group of the extended Golay code is the 5-transitive Mathieu group M_{24} of order $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. The automorphism group of the extended quadratic residue $[48, 24, 12]$-code is only 2-transitive. It is isomorphic to the projective special linear group $PSL_2(47)$ and has order $2^4 \cdot 3 \cdot 23 \cdot 47$. Both M_{24} and $PSL_2(47)$ are nonabelian simple groups, and so in particular are not solvable.

Definition 13 *A normal series of a group G is a finite sequence $(A_0, \ldots, A_r)$ of subgroups such that*

$$I = A_0 \lhd A_1 \lhd \ldots \lhd A_r = G.$$

A section of G is a quotient group A_{k+1}/A_k for some index $k < r$. G is a solvable group iff all sections are Abelian.

Every finite group of order < 60, every Abelian group, and every subgroup of a solvable group is solvable.

Here we shall collect known facts about the automorphism group of a putative self-dual doubly-even $[72, 36, 16]$ code $\mathcal{C}$. Primes larger than 7 cannot divide its order (see [8], [13], [22], [23]). Permutations of odd composite orders except 9 cannot be automorphisms of such a code (see [10]). If $\sigma \in \mathrm{Aut}\,(\mathcal{C})$ has order 5 or 7, then σ fixes two coordinates ([10]); if σ has order 2 or 3, then it is a fixed-point-free permutation (see [4] and [5]).

Finally, from [6] we got to know, that the automorphism group of a $[72, 36, 16]$ code is a solvable group of order $5, 7, 10, 14, 56$, or a divisor of 72.

And if we talk about primes, that may occur in the order of the automorphism group of the code, only 2, 3, 5 and 7 survived for the $[72, 36, 16]$ code. For the binary self-dual doubly-even $[96, 48, 20]$ code only 2, 3, and 5 are possible ([9]).

4 Primes dividing the order of the automorphism group of self-dual codes

Applying representation theoretical methods we show how to exclude special primes in the automorphism group of an arbitrary self-dual not necessarily extremal code. This may be applied attacking the existence of larger extremal codes.

Definition 14 *For an odd number $n \in \mathbb{N}$ let $s(n)$ denote the smallest non-negative integer such that $2^{s(n)} \equiv 1 \pmod{n}$. Thus $s(n)$ is the order of $2 \mod n$.*

In the following let $\mathcal{C}$ be a binary self-dual code of length $n \geq 4$ with automorphism group $\mathrm{Aut}(\mathcal{C})$. Let $\sigma \in G$ be of order p where p is an odd prime. The action of σ on the positions produces c cycles of length p and f fixed points. We say that σ is of type $p-(c,f)$.We shall prove

Theorem 27 *If $s(p)$ is even then c is even.*

As a special result of Theorem 27 we get an early result of Huffman.

Corollary 28 (Huffman, [12])

a) If 2 is a primitive root $\mod p$ then c is even.

b) If $p \equiv 1 \mod 4$ and $p \neq 1 \mod 8$ then c is even.

Proof. In both cases we have $s(p) = p-1$. □

In order to prove Theorem 27 we repeat some well-known fact in representation theory. Let G be a finite group and let k be any field.

Definition 15 *The group algebra kG, where k is a field and G is a group with operation $\circ$, is the set of all linear combinations of finitely many elements of G with coefficients in k, hence of all elements of the form*

$$a_1 g_1 + a_2 g_2 + \cdots + a_n g_n,$$

where $a_i \in k$ and $g_i \in G$ for all $i = 1, \ldots, n$. This element can be denoted in general by

$$\sum_{g \in G} a_g g,$$

where it is assumed that $a_g = 0$ for all but finitely many elements of G. kG is an algebra over k with respect to the addition defined by the rule

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,$$

the product by a scalar given by

$$a \sum_{g \in G} a_g g = \sum_{g \in G} (a\ a_g) g,$$

and the multiplication

$$(\sum_{g \in G} a_g g)(\sum_{g \in G} b_g g) = \sum_{g \in G, h \in G} (a_g b_h) g \circ h.$$

From this definition, it follows that the identity element of G is the unit of kG, and that kG is commutative iff G is an Abelian group.

If the field k is replaced by a unit ring R, the addition and the multiplication defined above yield the group ring RG.

Definition 16 *The concept of a module over a ring is a generalization of the notion of vector space, where instead of requiring the scalars to lie in a field, the "scalars" may lie in an arbitrary ring.*

A right R-module over the ring R consists of an abelian group $(M, +)$ and an operation $M \times R \to M$ (called scalar multiplication) such that for all $r, s \in R$, $x, y \in M$, we have

1. $(x + y)r = xr + yr$
2. $x(r + s) = xr + xs$
3. $x(rs) = (xr)s$
4. $x1 = x$

Usually we write "a right R-module M" or M_R. Left modules can be defined similarly.

If R is commutative, then right R-modules are simply called R-modules.

Definition 17 *Suppose M is a left R-module and N is a subgroup of M. Then N is a submodule (or R-submodule, to be more explicit) if, for any $n \in N$ and any $r \in R$, the product rn is in N (or nr for a right module).*

A module S is called simple if $S \neq \{0\}$ and whose only submodules are $\{0\}$ and S. Simple modules are sometimes called irreducible.

kG-modules are always assumed to be finite dimensional.

Definition 18 *Let W be a right kG-module. We put*

$$W^* = \mathrm{Hom}_k(W, k)$$

and call W^* the dual module of W. W^* becomes a right kG-module if we put

$$(fg)(w) = f(wg^{-1}) \quad \text{for } f \in \mathrm{Hom}_k(W, k),\ g \in G \quad \text{and } w \in W.$$

If $W \cong W^*$ then W carries a non-degenerate G-invariant k-bilinear form, say b (see [14, Chapter VII, Lemma 8.10]). Here G-invariance means that $b(w_1g, w_2g) = b(w_1, w_2)$ for all $w_1, w_2 \in W$ and all $g \in G$.

With this notation we have the following fact.

Lemma 29 *If $W \cong W^*$ and if V is a kG-submodule of W then*

$$W/V^\perp \cong V^* \tag{46}$$

where $V^\perp$ is the orthogonal of V in W w.r.t. the form b. If in addition $V = V^\perp$, then the multiplicity of any simple self-dual kG-module as composition factor of W is even.

Proof. We define a map $\alpha : W \to V^*$ by

$$\alpha(w)(v) = b(w, v) \quad \text{for } w \in W,\ v \in V.$$

α is kG-linear since G-invariance of the form b implies

$$\alpha(ag)(v) = b(ag, v) = b(a, vg^{-1}) = \alpha(a)(vg^{-1}) = (\alpha(a)g)(v).$$

Furthermore, $\ker(\alpha) = V^\perp$. Thus α induces a monomorphism

$$\bar{\alpha} : W/V^\perp \to V^*.$$

Since b is non-degenerate we have

$$\dim W = \dim V + \dim V^\perp = \dim V^* + \dim V^\perp.$$

Thus the map $\bar{\alpha}$ is a kG-isomorphism.

Let $X \cong X^*$ be a simple composition factor of W. Then X has multiplicity m as composition factor of $V^\perp = V$ iff $X \cong X^*$ has multiplicity m as composition factor of V^*. Thus the multiplicity of X as composition factor of W is even. □

Lemma 30 ([20]) *Let $k = \mathbb{F}_2$. If G is a finite group of odd order then the following conditions are equivalent.*

a) There exists a non-trivial irreducible self-dual kG-module V.

b) $s(p)$ is even for some prime $p \neq 2$ with $p \mid |G|$.

Proof of Theorem 27. Let $G = \langle \sigma \rangle$ and let k be the binary field. Suppose that σ is of type $p - (c, f)$, i.e. has exactly c p-cycles on the set of positions, $f = n - cp$ being the number of fixed points on the set of positions. In particular,

$$k^n = kG \oplus \ldots \oplus kG \oplus k \ldots \oplus k \tag{47}$$

as a kG-module where the number of kG's is c and the number of k's is f. Clearly, $\mathcal{C} \cong \mathcal{C}^*$ since $kG \cong kG^*$ (see [14, Chapter VII, Lemma 8.23]) and obviously $k \cong k^*$. Furthermore, by ([19, Proposition 3.4]), any non-trivial simple kG-module has

dimension $s(p)$. On the other hand, by Lemma 30, since $s(p)$ is even the group algebra kG contains at least one simple non-trivial self-dual module. Moreover, since G is Abelian, any simple non-trivial module has multiplicity 1 as a composition factor of kG. In particular, a simple non-trivial self-dual module has multiplicity c in k^n. Thus Lemma 29 implies that c must be even which proves Theorem 27.

For the binary self-dual doubly-even $[120, 60, 24]$ code the Huffman argument (Corollary 28) rules out directly the primes $61, 67, 83, 101, 107$ and 109. Theorem 27 shows that furthermore the primes 97 and 113 do not occur in the automorphism group.

In the following let $k = \mathbb{F}_2$ always denote the binary field and let $\mathcal{C}$ be an extremal doubly-even self-dual $[24m, 12m, 4m+4]$ code. By a result of Zhang [26] we know that $m \leq 153$. From the previous chapters we know that for $m = 1$ and $m = 2$ such codes are respectively the extended $[24, 12, 8]$ Golay code with automorphism group M_{24} and the extended quadratic residue code $[48, 24, 12]$ with automorphism group $PSL_2(47)$. There are no other known examples of extremal codes of the form $[24m, 12m, 4m+4]$. To be short we put $n = 24m$.

Theorem 31 ([3]) *If $\sigma \in G = \mathrm{Aut}(\mathcal{C})$ is of type $p-(c, f)$ for an odd prime p then $f \leq c$.*

Now suppose that $p > \frac{n}{2}$. Thus, by Theorem 31, σ is of type $p-(1,1)$. Thus $n = 24m = p+1$, and in particular $p \equiv -1 \mod 8$. This yields that $\frac{p-1}{2}$ is odd.

Lemma 32 *For $p > \frac{n}{2}$ we always have $s(p)$ odd.*

Proof. Note that 2 is a square root $\mod p$ since $p \equiv -1 \mod 8$, hence

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

Since $s(p) \mid \frac{p-1}{2}$ and $\frac{p-1}{2}$ is odd we are done. □

Lemma 33 *For the group algebra $k\langle\sigma\rangle$, where σ is of odd prime order, the trivial module is the only irreducible self-dual module.*

Proof. By Lemma 32 we know that $s(p)$ is odd. The assertion follows now directly from Lemma 30. □

One can easily find all primes p of the form $24m-1$ for $m \leq 153$. It turns out that apart from 6 primes, we always have $s(p) = \frac{p-1}{2}$. The exceptions appear if $m = 18, 38, 46, 98, 112$ or 133.

Theorem 34 *Apart from the 6 exceptions $\mathcal{C}$ is an extended QR code.*

Proof. The ambient space k^n can be written as

$$k^n = k\langle\sigma\rangle \oplus k.$$

Since $s(p) = \frac{p-1}{2}$ we have a decomposition

$$k\langle\sigma\rangle = k \oplus V \oplus W \tag{48}$$

with irreducible modules V and W of dimension $s(p) = \frac{p-1}{2}$. By Lemma 33 we have $V \ncong V^*$ and $W \ncong W^*$. On the other hand, a group algebra is always self-dual. Hence $W \cong V^*$ and the decomposition in (48) is unique. If $\mathcal{C}_0$ is the subspace of $\mathcal{C}$ with 0 in the last position then $\mathcal{C}_0 = V$ or $\mathcal{C}_0 = W$. On the other hand we know that

$$k^n = k \oplus Q \oplus N$$

where Q is the code associated to the squares mod p and N to the non-squares. Since Q is equivalent to N we may suppose that $\mathcal{C}_0 = V = Q$. Finally, $\mathcal{C} = \langle \mathcal{C}_0, c\rangle$, where c is the all one word. This shows that $\mathcal{C}$ is an extended QR code. □

Remark 8 *The exceptions arise when* $s(p) \neq \frac{p-1}{2}$. *The six cases are:* $m =$ 18, 38, 46, 98, 112 *and* 133.

5 Finding codewords of small weight in QR-codes

In the end of the previous chapter we have proven the very important theorem, which connects extended QR- and extremal codes. If we assume that the prime $p = n - 1$ occurs in the automorphism group of an extremal code then we immediately have that apart from the six exceptions this code is an extended Quadratic Residue code. Inversely, if we show that these codes could not be extremal than it we will have that $n - 1$ does not divide the order of the automorphism group (of course, only if we leave the exceptions aside). Furthermore, the result of Bouyuklieva [3] yields that the primes, larger than $n/2$ does not occur either.

The significance of Theorem 34 is hard to underestimate since the both examples of extremal $[24m, 12m, 4m + 4]$ codes are extended Quadratic Residue codes and have $n - 1$ in its automorphism groups.

The further work in this chapter will concern the following

Problem 1 *Can we show that an extended QR-code of length* $p+1 = 24m$ *is extremal only for* $m = 1$ *and* $m = 2$*?*

Remark 9 *By known result [16] it is true for* $m \leq 21$. *But we have to check up to* $m = 153$.

We used the algorithm of Karlin and MacWilliams [15] to exclude some entries from the list of extended QR-codes, for which $p = n - 1$ is a prime and $s(p) = \frac{p-1}{2}$.

Below we will give the explanation of the Karlin-MacWilliams algorithm. Is is designed to find low weight vectors in Quadratic Residue codes for $p = 8m - 1$.

Consider the QR code $\mathcal{L}$, $\widehat{\mathcal{L}}$ being the extended code. The permutation $V : y \to g^2 y$, where g is a primitive element of GF(p), is an element of Aut($\mathcal{L}$). The order of this permutation is $(p-1)/2$. If this number is composite, say $(p-1)/2 = sf$ then the code $\mathcal{L}$ contains codewords, invariant under the permutation $U : y \to g^{2s} y$. Let $\mathcal{U}$ be the subcode of $\mathcal{L}$, consisting of such words. We will show, how one can find the subcode $\mathcal{U}$ for $p = 8m - 1$.

Set $e = 2s$, $p - 1 = ef$, where s and f are odd. For $i = 0, 1, \ldots, e-1$ set

$$C_i = \{g^{ej+i}, j = 0, 1, \ldots, f-1\}.$$

We note that $-1 = g^{sf}$, hence $-1 \in C_s$. In the ring $R = \mathbb{F}_2[x]/(x^p + 1)$ define the following polynomials:

$$J = \sum_{j=0}^{p-1} x^j, \quad X_i = \sum_{c \in C_i} x^c, \quad X_i^* = \sum_{c \in C_i} x^{-c} = X_{i+s},$$

$$Q = X_0 + X_2 + \ldots + X_{e-2}, \quad N = X_1 + X_3 + \ldots + X_{e-1}.$$

The weight of polynomial is the number of nonzero terms. The weight of X_i is f. Since e is even, the exponents of x which occur in Q, N are respectively the quadratic residues and nonresidues of p. Note, that since $-1 \in C_s$, it is a nonresidue.

Clearly, both Q and N are idempotents. In fact, they are the generating idempotents of QR-codes, i.e. E_q and E_n from chapter 2, §2.

A polynomial $f(x)$ is in $\langle Q \rangle$ if and only if $f(x)Q = f(x)$.

Assmus and Mattson [2] have investigated the case $p = 8m + 1$, and sometimes found polynomials X_i in $\langle Q \rangle$. This cannot happen for $p = 8m-1$ and $e > 2$. However it mae happen that $1 + X_w + X_{2w}^*$ (for suitable w) is in $\langle Q \rangle$, which then contains vectors of weight $1 + 2f$.

In order to detect this case, and others, we need the multiplication table for $X_i Q$.

$X_0 Q$ is a linear combination of the X_i, hence we may suppose that

$$X_0 Q = \sum_{j=0}^{s-1} a_j X_{2j} + \sum_{j=0}^{s-1} b_j X_{2j}^*.$$

(Note that $X_{2j}^* = X_{2j+s}$, so the second summation covers the odd subscripts.)

Let σ be the automorphism of R induced by $x \to x^g$. Then $\sigma^2 X_i = X_{i+2}$; $\sigma^2 Q = Q$. Hence,

$$X_2 Q = \sigma^2 X_0 Q = \sum_{j=0}^{s-1} a_{j-1} X_{2j} + \sum_{j=0}^{s-1} b_{j-1} X_{2j}^*.$$

Let Φ be the automorphism of R induced by $x \to x^{-1}$. $\Phi^2 X_i = X_1$; $\Phi Q = N$. Thus

$$X_0^* N = \Phi X_0 Q = \sum_{j=0}^{s-1} a_j X_{2j}^* + \sum_{j=0}^{s-1} b_j X_{2j}.$$

Clearly $N = Q + J + 1$, hence, setting $\overline{a} = a + 1$, and $\overline{A} = A + J \pmod 2$,

$$X_0^* Q = 1 + \sum_{j=0}^{s-1} \overline{b_j} X_{2j} + \sum_{j=0}^{s-1} \overline{a_j} X_{2j}^* + X_0^*.$$

The multiplication table may be condensed as follows

	1	$X_0 X_2 \cdots X_{e-2}$	$X_0^* X_2^* \cdots X_{e-2}^*$
$1 \cdot Q$	0	$1 \;\; 1 \;\; \cdots \;\; 1$	$0 \;\; 0 \;\; \cdots \;\; 0$
$X_0 Q$	0		
$\vdots$	$\vdots$	A	B
$X_{e-2} Q$	0		
$X_0^* Q$	1		
$\vdots$	$\vdots$	$\overline{B}$	$\overline{A} + I$
$X_{e-2}^* Q$	1		

Here A, B are circulant matrices of size $s \times s$, and I is the identity matrix. Set

$$M = \left[\begin{array}{c|ccc|ccc} 0 & 1 & 1 & \cdots & 1 & 0 & 0 \cdots 0 \\ \hline 0 & & & & & & \\ \vdots & & A & & & B & \\ 0 & & & & & & \\ \hline 1 & & & & & & \\ \vdots & & \overline{B} & & & \overline{A} + I & \\ 1 & & & & & & \end{array}\right]$$

and consider the rows of M as basis vectors for a code $\mathcal{U}$ of block length $e + 1$. the minimum weight vectors of $\mathcal{U}$ provide an upper bound for the minimum weight in $\langle Q \rangle$.

Let $a_0 a_1 \cdots a_{s-1}$, $b_0 b_1 \cdots b_{s-1}$ be the first rows of A, B.

Lemma 35

$$\sum_{i=0}^{s-1} a_i \equiv 1 \pmod 2, \qquad \sum_{i=0}^{s-1} b_i \equiv 0 \pmod 2.$$

Proof. $Q^2 = X_0 Q + X_2 Q + \cdots + X_{e-2} Q$, and is represented by the vector sum of the rows $0|A|B$. Since $Q^2 = Q = X_0 + X_2 + \cdots + x_{e-2}$, this vector sum must equal the first row of M. Thus the sum of each column of A (B) is 1 (0) mod 2. Since A, B are circulant matrices, the same is true for each row of A, B. □

For integer m, set

$$[m] = \begin{cases} 1 & \text{if } m \text{ is a quadratic residue of } p, \\ 0 & \text{if } m \text{ is a nonresidue or } 0. \end{cases}$$

Lemma 36 *We suppose that* $m_i \neq 0$, *and use addition* $\mod 2$.

(i) *If* m_i *is a quadratic residue,* $[m_1 m_2] = [m_2]$.

(ii) $[-m_i] \equiv 1 + [m_i]$ *(*-1 *is a nonresidue).*

(iii) $[m_1] + [m_2] \equiv 1 + [m_1 m_2]$.

(iv) *If* f *is odd, then*

$$[m_1] + [m_2] + \cdots + [m_f] \equiv [m_1 m_2 \cdots m_f].$$

Let $q = g^2$ be a generator of quadratic residues of p.

Lemma 37

$$a_i = [q^i - 1] + [q^i - q^s] + \cdots + [q^i - q^{(f-1)s}],$$
$$b_i = [-q^i - 1] + [-q^i - q^s] + \cdots + [-q^i - q^{(f-1)s}].$$

Proof. Write Q as $\sum_{m=0}^{p-1}[m]X^m$. a_i is the coefficient of $X_2 i$ in the product $X_0 Q$; that is , it is the coefficient of x^{q^i} in the product

$$(x + x^q + \cdots + x^{q^{(f-1)s}})Q.$$

Similarly b_i is the coefficient of x^{-q^i} in this product. We note that for $1 \leq i \leq s-1$, the quantities $\pm q^i - q^j\,(0 \leq j \leq f-1)$ in the above expressions for a_i, b_i are all nonzero. □

Lemma 38 *For* $i > 0$,

$$a_i = [q^{if} - 1],$$
$$b_i = [-q^{if} - 1].$$

Proof. By Lemma 36,

$$a_i = [q^i - 1] + [q^i - q^s] + \cdots + [q^i - q^{(f-1)s}]$$

Let $F(w) = \prod_{j=0}^{f-1}(w - q^{sj})$. The zeros of $F(w)$ are the distinct f-th roots of unity mod p. Hence,

$$F(w) = w^f - 1 \mod p,$$

and

$$a_i = [F(q^i)], \qquad b_i = [F(-q^i)].$$

□

Corollary 39 *For* $s > i > 0$ *(addition* $\mod 2$*),*

(i) $a_i + a_{s-i} = 1$,

(ii) $b_i + b_{s-i} = 0$,

(iii) $b_i + a_{2i} + a_i = 0$.

Proof.

(i) $[q^{(s-i)f} - 1] = [q^{-if}(1 - q^{if})] = 1 + [q^{if} - 1]$ by Lemma 37.

(ii) $[-q^{(s-i)f} - 1] = [q^{-if}(-1 - q^{if})] = [-1 - q^{if}]$.

(iii) $[q^{2if} - 1] + [q^{if} - 1] = 1 + [(q^{if} - 1)^2(q^{if} + 1)] = 1 + [q^{if} + 1] = [-q^{if} - 1]$ by Lemma 36.

□

Corollary 40 *The statements of Corollary 39 imply*

$$A^T = \overline{A} + I,$$
$$B^T = B,$$
$$B^2 = A^2 + A.$$

Since A and B are circulant matrices, it is convenient to treat them as polynomials mod $y^s + 1$. In particular, the matrix A is invertible if and only if the polynomial

$$a(y) = a_0 + a_1 y + a_2 y^2 + \cdots + a_{s-1} y^{s-1}$$

has an inverse in the ring of polynomials $\mod y^s + 1$.

Let φ denote a row vector of s zeros, and j a row vector of s ones. J denotes a matrix with every entry one. Then

$$M = \begin{pmatrix} 0 & j & \varphi \\ \varphi^T & A & B \\ j^T & B + J & A + I + J \end{pmatrix}.$$

It is easy to check that

$$MM^T = J,$$

hence

$$\operatorname{rank} M \leq (e + 2)/2 = s + 1.$$

Theorem 41 ([15]) *M has rank $s + 1$.*

Proof. M has the same rank as

$$M' = \begin{pmatrix} 0 & j & \varphi \\ j^T & A + B + J & A + B + J + I \\ j^T & B + J & A + J + I \end{pmatrix}.$$

Let $f_1(y)$, $f_2(y)$ be polynomials mod y^s+1 corresponding to the matrices $A+B+J$ and $A+B+J+I$. Then

$$f_2(y) = f_1(y) + 1.$$

If the vector sum of a subset of the rows of

$$A+B+J, \qquad A+B+J+I$$

is zero, there exists a polynomial $g(y)$ of degree $\leq s-1$, such that

$$g(y)f_1(y) \equiv g(y)f_2(y) = 0 \mod y^s + 1.$$

Since $g(y)$ is of degree $\leq s-1$, clearly $g(y) = 0$.

Every row of $A+B+J$ has even weight, hence no subset of these rows can have sum j, which is of odd weight.

Hence, the first $s+1$ rows of M' are linearly independent, and the rank of M is exactly $s+1$. □

Let

$$a(y) = a_0 + a_1 y + \cdots + a_{s-1}y^{s-1},$$
$$b(y) = b_0 + b_1 y + \cdots + b_{s-1}y^{s-1}$$

be the polynomials mod y^s+1 corresponding to the matrices A, B. The polynomial corresponding to A^T is

$$a(y)^T = a_0 + a_{s-1}y + \cdots + a_1 y^{s-1}.$$

If $f(y) = f(y)^T$, we say that $f(y)$ is a symmetric polynomial. Let $j(y) = \sum_{i=0}^{s-1} y^i$. We have

$$b(y^2) = a(y^2) + a(y),$$
$$a(y) + a(y)^T = j(y) + 1.$$

The first of these equations gives a linear expression for the coefficient b_i in terms od the a_i. The matrix B is completely determined by the matrix A.

The polynomials $a(y)$ may be partitioned into equivalence classes. The polynomials equivalent to $a(y)$ are obtained from $a(y)$ by a different choice of the generator g; more explicitly, if t is an integer prime to s, the polynomial $a(y^t)$ is equivalent to $a(y)$. The corresponding matrices produce codes with the same weight structure. This is not to say that different equivalence classes produce codes with different weight structure. In fact there may be fewer weight patterns than equivalence classes. To see this fact we need the following

Theorem 42 ([15]) *If A is invertible, then*

$$A^{-1}B = R + J,$$

where R is orthogonal, i.e. $RR^T = I$.

Proof. Since circulant matrices commute,

$$(A^{-1}B)(A^{-1}B) = A^{-1}B^2(A^{-1})^T = A^{-1}(A^2+A)(A^{-1})^T = \\ (A+I)(A^T)^{-1} = (A^T+J)(A^T)^{-1} = I+J.$$

□

Since $a(y)$ is an odd weight polynomial, it certainly has an inverse whenever s is a prime for which 2 is a primitive root, e.g., 11, and 13. in these cases and others, the code generated by the rows of M is equally well generated by the rows of

$$\begin{pmatrix} 1 & \varphi & j \\ \varphi^T & I & R+J \end{pmatrix},$$

and the number of weight patterns depends on the number of inequivalent circulants R.

Theorem 43 ([15])

(i) *If $y^i a(y)$ is symmetric for some integer i, the code generated by the row of the matrix M contains a vector of weight 3, eith first coordinate 1. The quadratic residue code from M was obtained contains a vector of weight $1+2f$.*

(ii) *Such $a(y)$ form one equivalence class.*

Proof. (ii). The equation

$$\left(y^i a(y)\right)^T = y^i a(y)$$

becomes, after some manipulation and using Corollary 40,

$$a(y)(y^{2i}+1) = j(y)+1.$$

Since $a(y)j(y) = j(y)$ ($a(y)$ has odd weight), this can be written

$$a(y)\left(y^{2i}+1+j(y)\right) = 1.$$

Thus both factors are invertible mod y^s+1, and

$$a(y)^{-1} = \left(y^{2i}+1+j(y)\right).$$

Hence, $a(y)$ is uniquely determined by i. Further, it is prime to s, for if $(i, s = u > 1$, the polynomial $(y^u+1)/(y+1)$ divides both $y^{2i}+1$ and $j(y)$, and $(y^{2i}+1+j(y))$ is not invertible.

Let $c(y)$ be the polynomial with coefficients

$$c_i = \begin{cases} 0 & 1 \le i \le (s-1)/2, \\ 1 & s+\frac{1}{2} \le i \le s-1. \end{cases}$$

If $s-1 = 4w$, $c_0 = 1$; if $s-1 = 4w-2$, $c_0 = 0$. In either case, $(w, s) = 1$, and $y^w c(y)$ is symmetric.

Let $y^i a(y)$ be symmetric. Since w, i are both prime to s, the transformation $y \to y^{w/i}$ changes it to

$$y^w a(y^{w/i}),$$

hence,

$$a(y^{w/i}) = c(y).$$

Hence, all "symmetric" polynomials belong to the equivalence class of $c(y)$, and it is clear that every polynomial in this class has the required property.

(i). If suffices to look at the case $a(y) = c(y)$. It is readily checked by Corollary 39 (iii) that

$$\begin{array}{rcccccl} & 1 & \overbrace{}^{w} & \overbrace{}^{w} & \overbrace{}^{w} & \overbrace{}^{w} & \\ b(y) = 0 & | & 0 \ldots 0 & | & 1 \ldots 1 & | & 1 \ldots 1 & | & 0 \ldots 0 & |, & s-1 = 4w, \\ & & \overbrace{}^{w-1} & & \overbrace{}^{w} & & \overbrace{}^{w} & & \overbrace{}^{w-1} & & \\ b(y) = 0 & | & 0 \ldots 0 & | & 1 \ldots 1 & | & 1 \ldots 1 & | & 0 \ldots 0 & |, & s-1 = 4w-2. \end{array}$$

Then

$$\begin{gathered} a^{-1}(y) b(y) = (1 + y^{2w}) b(y) = j(y) + y^w, \\ a^{-1}(y) \left(b(y) + j(y) \right) = y^w, \\ a^{-1}(y) \left(a(y) + j(y) + 1 \right) = y^{2w}. \end{gathered}$$

Thus the code generated by the rows of M contains a vector of weight 3, and the original quadratic residue code contains the vector $1 + X_w + X_{2w}^*$. □

So it is shown that in some cases there exists a vector in $\langle Q \rangle$, or $\mathcal{L}$ of weight $1+2f$. In the general case, the connection between the words of minimal weight of the subcode $\mathcal{U}$ and the weight spectrum of $\mathcal{L}$ is as follows: if $\eta + X_{i_1} + \cdots + X_{i_r}$ ($\eta = 0$ or 1) is a codeword of minimal weight of $\mathcal{U}$ then the code $\mathcal{L}$ contains codewords of weight $\eta + rf$. Hence, minimal nonzero weight of $\mathcal{U}$ specifies the upper bound for the minimal weight in $\mathcal{L}$.

In the appendix one can find a table of the extended QR-codes to be checked (see Problem 1). The 6 exceptions are marked by bold font. The codes for which we were able to find low-weight vectors (i.e. the weight is less, than the minimal distance for the corresponding extremal code) are marked by larger italic font.

The described above Karlin-MacWilliams algorithm was implemented in Mathematica. An example is given in the appendix.

References

[1] E.F. Assmus and H.F. Mattson, New 5-designs, *J. Combin. Theory*, 6, pp. 122-151, 1969.

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

[3] S. Bouyuklieva, Automorphisms of extremal $[24m, 12m, 4m + 4]$ self-dual codes, preprint 2007.

[4] S. Bouyuklieva, On the automorphisms of order 2 with fixed points for the extremal self-dual code of length $24m$, *Des. Codes Cryptogr.*, 25, pp. 5-13, 2002.

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

[6] 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, pp. 498-504, 2006.

[7] J.H. Conway, Three lectures on exceptional groups, in: *Finite Simple Groups*, ed. M.B. Powell and G. Higman (Academic Press, New York, 1971) pp. 215-247.

[8] 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, pp. 143-156, 1982.

[9] R. Dontcheva, On doubly-even self-dual codes of length 96, *IEEE Trans. Inform. Theory*, 28, pp. 557-561, 2002.

[10] R. Dontcheva, A.J. van Zanten and S. Dodunekov, Binary self-dual codes with automorphism of composite order, *IEEE Trans. Inform. Theory*, 50, pp. 53-59, 2003.

[11] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, *Actes Congrès Internat. de Mathematique*, 3 1970 (Gauthier-Villars, Paris, 1971) 211-215.

[12] W.C. Huffman, Automorphisms of codes with application to extremal doubly-even codes of length 48, *IEEE Trans. Inform. Theory*, 28, pp. 511-521, 1982.

[13] W.C. Huffman and V. Yorgov, A $[72, 36, 16]$ doubly-even code does not have an automorphism of order 11, *IEEE Trans. Inform. Theory*, 33, pp. 749-752, 1987.

[14] B. Huppert and D. Blackburn, Finite groups II, Springer, Berlin, 1982.

[15] M. Karlin and F.J. MacWilliams, On finding low weight vectors in quadratic residue codes for $p = 8m - 1$, *SIAM J. Appl. Math.*, 25, pp. 95-104, 1973.

[16] J.S. Leon, A probabilistic algorithm for computing the minimum weights of large error-correcting codes, *IEEE Trans. Inform. Theory*, 34, pp. 1354-1359, 1988.

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

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

[19] Martínez-Pérez and W. Willems, Is the class of cyclic codes asymptotically good? *IEEE Trans. Inform. Theory*, 52, pp. 696-700, 2006.

[20] Martínez-Pérez and W. Willems, Self-dual extended cyclic codes. *Appl. Algebra in Eng. Comm. and Computing*, 17, pp. 1-16, 2006.

[21] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste. *Math. Zeit.*, 56 (1952) 122-130.

[22] V. Pless, 23 does not divide the order of the group of a $(72, 36, 12)$ doubly-even code, *IEEE Trans. Inform. Theory*, 28, pp. 113-117, 1982.

[23] V. Pless and J.G. Thompson, 17 does not divide the order of the group of a $(72, 36, 12)$ doubly-even code, *IEEE Trans. Inform. Theory*, 28, pp. 537-541, 1982.

[24] N.J.A. Sloane, Is there a $(72, 36)$, $d = 16$ self-dual code? *IEEE Trans. Info. Theory*, 19, p. 251, 1973.

[25] H.C.A. van Tilborg, On weight in codes, Report71-WSK-03, Department of Mathematics, Technological University of Eindhoven, Netherlands, December 1971.

[26] S. Zhang. On the nonexistence of extremal self-dual codes. *Disc. Appl. Math.* 91, 103-127, 1999.

The list of QR-codes to check ($n - 1$ is a prime)

m	$p = 24m-1$	$(p-1)/2$	s(p) == $p-1$	d	wt < d
1	23	11^1	True	8	–
2	47	23^1	True	12	–
3	71	$5^1 7^1$	True	16	–
7	167	83^1	True	32	–
8	191	$5^1 19^1$	True	36	–
10	239	$7^1 17^1$	True	44	–
11	263	131^1	True	48	–
13	311	$5^1 31^1$	True	56	–
15	359	179^1	True	64	–
16	383	191^1	True	68	–
18	**431**	$\mathbf{5^1 43^1}$	**False**	**76**	**–**
20	479	239^1	True	84	–
21	503	251^1	True	88	–
25	*599*	$13^1 23^1$	*True*	*104*	*79*
27	*647*	$17^1 19^1$	*True*	*112*	*103*
30	719	359^1	True	124	–
31	*743*	$7^1 53^1$	*True*	*128*	*107*
35	839	419^1	True	144	–
36	863	431^1	True	148	–
37	887	443^1	True	152	–
38	**911**	$\mathbf{5^1 7^1 13^1}$	**False**	**156**	**–**
41	983	491^1	True	168	–
43	1031	$5^1 103^1$	True	176	–
46	**1103**	$\mathbf{19^1 29^1}$	**False**	**188**	**–**
48	*1151*	$5^2 23^1$	*True*	*196*	*184*
51	*1223*	$13^1 47^1$	*True*	*208*	*95*
55	1319	659^1	True	224	–
57	1367	683^1	True	232	–
60	1439	719^1	True	244	–
62	1487	743^1	True	252	–
63	1511	$5^1 151^1$	True	256	–
65	*1559*	$19^1 41^1$	*True*	*264*	*228*
66	1583	$7^1 113^1$	True	268	–
67	*1607*	$11^1 73^1$	*True*	*272*	*243*
76	1823	911^1	True	308	–
77	*1847*	$13^1 71^1$	*True*	*312*	*300*

78	*1871*	$5^1 11^1 17^1$	*True*	*316*	*307*
85	2039	1019^1	True	344	–
86	2063	1031^1	True	348	–
87	*2087*	$7^1 149^1$	*True*	*352*	*299*
88	2111	$5^1 211^1$	True	356	–
92	2207	1103^1	True	372	–
98	**2351**	$\mathbf{5^2 47^1}$	**False**	**396**	**–**
100	2399	$11^1 109^1$	True	404	–
101	*2423*	$7^1 173^1$	*True*	*408*	*347*
102	2447	1223^1	True	412	–
106	*2543*	$31^1 41^1$	*True*	*428*	*411*
108	*2591*	$5^1 7^1 37^1$	*True*	*436*	*371*
111	2663	11^3	True	448	–
112	**2687**	$\mathbf{17^1 79^1}$	**False**	**452**	**–**
113	2711	$5^1 271^1$	True	456	–
120	2879	1439^1	True	484	–
121	2903	1451^1	True	488	–
122	*2927*	$7^1 11^1 19^1$	*True*	*492*	*419*
125	2999	1499^1	True	504	–
126	3023	1511^1	True	508	–
130	3119	1559^1	True	524	–
132	3167	1583^1	True	532	–
133	**3191**	$\mathbf{5^1 11^1 29^1}$	**False**	**536**	**–**
140	*3359*	$23^1 73^1$	*True*	*564*	*507*
142	3407	$13^1 131^1$	True	572	–
147	*3527*	$41^1 43^1$	*True*	*592*	*560*
151	3623	1811^1	True	608	–
153	3671	$5^1 367^1$	True	616	–

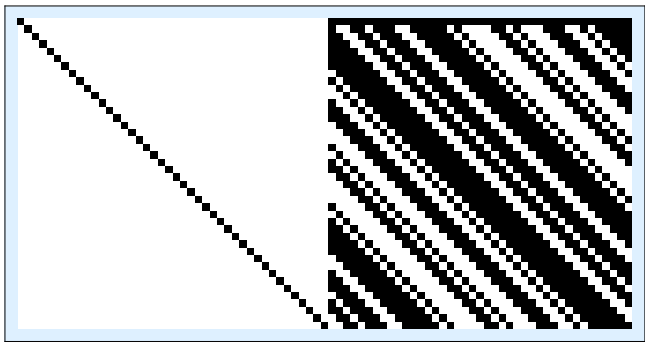
Bold — the 6 exceptions.
LARGER — the cases checked with Karlin–MacWilliams algorithm.

An example of Karlin-MacWilliams algorith implementation for $p = 3527$

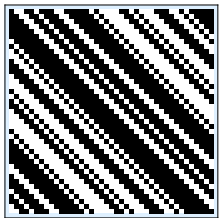
```
p = 3527; m = (p + 1)/24; d = 4 m + 4;

#[[1]]^#[[2]] & /@ FactorInteger[p - 1];

{e = 2 (s = Min@Select[%, OddQ]), f = (p - 1)/e}
```

```
{82, 43}
```

```
Primitive[p_?PrimeQ] := Do[Block[{li},
    If[(li = Union[Table[PowerMod[k, ι, p], {ι, p - 1}]]) == Range[p - 1], Return[k]]
  ], {k, PrimePi[p]}]
QuadraticResidues[p_] := Union[PowerMod[#, 2, p] & /@ Range[p - 1]];
QuadraticNonResidues[p_] := Complement[Range[p - 1], QuadraticResidues[p]];

ρ = Primitive[p];
T = Table[PowerMod[ρ, e j + i, p], {i, 0, e - 1}, {j, 0, f - 1}];
X = Plus @@@ x^T;

E = Plus @@ X[[Range[1, e, 2]]];

A = NestList[RotateRight,
    Prepend[Boole[MemberQ[QuadraticResidues[p], #] & /@
       Table[Mod[PowerMod[ρ, 2 i f, p] - 1, p], {i, 1, e/2 - 1}]],
     Mod[1/2 (e/2 + 1), 2]], s - 1];
B = NestList[RotateRight,
    Prepend[Boole[MemberQ[QuadraticResidues[p], #] & /@
       Table[Mod[-PowerMod[ρ, 2 i f, p] - 1, p], {i, 1, e/2 - 1}]], 0],
    s - 1];

ℐ = IdentityMatrix[s];
𝒥 = Array[1 &, {s, s}];
UBig = Mod[ArrayFlatten[{{0, 1, 0}, {0, A, B}, {1, B + 𝒥, A + ℐ + 𝒥}}], 2];
ArrayPlot[U = RowReduce[UBig, Modulus → 2][[ ;; s + 1]], Background → LightBlue]
```



```
ArrayPlot[SubU = U[[2 ;;, s + 2 ;;]], Background → LightBlue, ImageSize → Tiny]
```



```
Reduce[1 + x f < d, Integers][[-1]]
b = %[[-1]];
```

```
x ≤ 13
```

```
Timing[vecs = Table[Mod[Plus @@@ Subsets[SubU, {k}], 2], {k, 1, 3}];]
Timing[ans = Union /@ Apply[Plus, vecs, {2}]]
```

```
{0.61, Null}
```

```
{0.109, {{24}, {14, 18, 22, 26, 30}, {14, 18, 22, 26}}}
```

```
Grid[MapIndexed[{Item[#1 + #2[[1]], Background → LightGreen]  #1 < s/2
                 Item[s - #1 + #2[[1]], Background → LightOrange]  True} &, ans, {2}]]
```

```
18
16  20  21  17  13
17  21  22  18
```

```
StringForm[
 "Since we have a `` in the `` than there is a codeword of weight `` < d = ``",
 mw = 13, Style["red area", Background → LightOrange], 1 + mw f, d]
```

Since we have a 13 in the red *area than there is a codeword of weight* 560 < *d* = 592