On double circulant codes

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE

TECHNOLOGICAL UNIVERSITY EINDHOVEN
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS

On Double Circulant Codes

by

G.F.M. Beenker

T.H.-Report 80-WSK-04
July 1980

Contents page

Contents i

Preface iii

Chapter 1. Introduction

1.1. Definitions 1

1.2. Double circulant codes 3

1.3. t-Designs 4

Chapter 2. Examples of double circulant codes

2.1. Introduction 6

2.2. Quadratic residue codes 6

2.3. Symmetry codes 9

Chapter 3. Extended cyclic codes over GF(4) and their binary images

3.1. Introduction 15

3.2. General theory

3.2.1. A necessary and sufficient condition 16

3.2.2. Analysis of the equation $h^2(x) + h(x) + 1 = j(x)$ 19

3.3. Some properties of the cyclic code D over GF(4)

3.3.1. The idempotent of D 23

3.3.2. The generator polynomial of D 25

3.3.3. A square root bound on the minimum weight of D 28

3.4. Some properties of the double circulant codes C which are the binary images of extended cyclic codes D over GF(4)

3.4.1. Introduction 30

3.4.2. On the automorphism group of C 31

3.4.3. The dual code of C 33

3.5. A square root bound for the minimum weight of the binary images of extended quaternary QR-codes 36

3.6. Notes on chapter 3 38

Chapter 4. Extended cyclic codes over GF(9) and their ternary images

4.1. Introduction 40

4.2. General theory

4.2.1. A necessary and sufficient condition 41

4.2.2. Analysis of the equation $h^2(x) + h(x) + 2 = \pm j(x)$ 44

4.3. Some properties of the cyclic code D over GF(9)

4.3.1. The idempotent of D 46

4.3.2. A square root bound on the minimum weight of D 48

4.4. Some properties of the double ciculant codes C which are the ternary images of extended cyclic codes over GF(9)

4.4.1. Introduction 50

4.4.2. On the automorphism group of C 51

4.4.3. The dual code of C 52

4.5. Extended QR-codes over GF(9) and their ternary images

4.5.1. Introduction 53

4.5.2. An explicit form of the solution of (4.2.9), in case n is a prime of the form $n = 12k \pm 5$ 54

4.5.3. A double circulant representation of the ternary images of extended QR-codes over GF(9) 56

4.5.4. On the dual and the automorphisms of the ternary images of extended QR-codes over GF(9) 61

4.5.5. On the minimum weight of the ternary images of extended $[n+1, \frac{1}{2}(n+1)]$ QR-codes over GF(9); $n = 12k - 5$ 63

4.5.6. Examples and designs 67

4.6. A square root bound on the minimum weight of the ternary images of extended QR-codes over GF(9) 70

4.7. The relation between extended QR-codes over GF(9) and symmetry codes over GF(3) 80

Appendix A. The minimum weights of all $[2(n+1), n+1]$ double circulant codes which are the binary images of extended quaternary cyclic codes, up to $n = 45$ 83

Appendix B. The minimum weights of all $[2(n+1), n+1]$ double circulant codes which are the ternary images of extended cyclic codes over GF(9), up to $n = 35$ 86

Appendix C. Description of the computer programs 88

References 93

Index 95

Preface

This report deals with double circulant codes.
Roughly speaking this report can be divided into two parts. In the chapters 1 and 2 we give, for the sake of completeness, a short introduction to coding theory and a survey of known results on double circulant codes. In the next two chapters we introduce and analyse new classes of double circulant codes. Chapter 4 is the major part of this report.
In more detail this report deals with the following subjects.
Chapter 1: In this chapter a short introduction to coding theory is given, double circulant codes are defined and the basic-principles of t-designs are mentioned.
Chapter 2: A summary of known double circulant codes is given in chapter 2. For most of the results merely the references are given (cf. §2.1). Only two classes of double circulant codes are treated in more detail.
In §2.2 possible double circulant representations of extended binary QR-codes are discussed. The results of this section are taken from [10].
In §2.3 symmetry codes are treated. Besides the well-known results on these codes which can be found in [1] or [12], also an extension of the well-known theorem on the minimum weight of and a square root bound on the minimum weight of these codes are given. This extension of the theorem on the minimum weight is taken from [14] and the square root bound has been established by Robert Calderbank (private communication).
Chapter 3: In chapter 3 a new class of double circulant codes is introduced, namely those double circulant codes which are the binary images of extended cyclic codes over GF(4). Up until now only the binary images of extended quaternary QR-codes have been studied (cf. [1, Ch.16.§7], [16] and [17]).
In §3.2 a necessary and sufficient condition, in order that the binary image of an extended quaternary cyclic code is a double circulant code, is derived (cf. Theorem (3.2.9)). This condition is a polynomial equation which has to be satisfied. This polynomial equation is also analysed in §3.2.
In §3.3 some properties of these quaternary cyclic codes, such as a formula for the idempotent, a formula for their generator polynomial and a square root bound for their minimum weight, are discussed. These results have been found by generalizing some of the results on quaternary QR-codes.
In §3.4 some properties of the corresponding binary double circulant codes,

e.g. some theorems on the automorphisms and on the dual code, are treated. The results on the automorphisms have been found by generalizing [1, Ch.16. **Problem**(16)].

In §3.5 a square root bound on the minimum weight of the binary images of extended quaternary QR-codes is stated and compared with the results of [17]. The square root bound is taken from [16].

Using the computer the minimum weights of all [2(n+1), n+1] double circulant codes which are the binary images of extended cyclic codes over GF(4) have been determined up to n = 45. These results are reported in Appendix A and discussed in §3.6.

Chapter 4: Inspired by the results of chapter 3, another class of double circulant codes is defined in chapter 4, namely those double circulant codes which are the ternary images of extended cyclic codes over GF(9). As far as we know this class of codes is completely new.

The first part of chapter 4 is analogous to the corresponding part of chapter 3. In §4.2 a necessary and sufficient condition, in order that the ternary image of an extended cyclic code over GF(9) is a double circulant code, is derived (cf. Theorem (4.2.7)) and partially analysed. Unfortunately this condition is much harder to handle than the corresponding condition in §3.2. The computer had to be used to find the corresponding ternary double circulant codes.

In §4.3 some properties of these cyclic codes over GF(9), viz. a formula for the idempotent and a square root bound on their minimum weight, are discussed. Several results are proved generalizing the corresponding properties of QR-codes over GF(9).

In §4.4 some theorems on the automorphisms and on the dual code of the corresponding ternary images are treated.

In §4.5 the [2(n+1), n+1] double circulant codes which are the ternary images of extended [n+1, ½(n+1)] QR-codes over GF(9), n a prime of the form $n = 12k \pm 5$, are thoroughly analysed. It will appear that, in case n is a prime of the form $n = 12k - 5$, the properties of the [2(n+1), n+1] ternary images are comparable with those of symmetry codes. For instance those codes have a generator matrix of the form $G = [\ I \mid S\ ]$, where S is a Hadamard matrix of the Paley-type (cf. Theorem (4.5.13)). Furthermore a theorem on the minimum weight of these codes, analogous to Theorem (2.3.5), is proved (cf. Theorem (4.5.20)). As a direct result of this theory we have found self-dual ternary codes with parameters [16,8,6], [40,20,12] and [64,32,18]. These codes

meet the bound on the minimum weight of ternary self-dual codes (cf. [1, Ch.19. Th.17]). The first two codes were already known (cf. [1, Ch.19.§6]), but as far as we know the [64,32,18] code is new. Moreover this code is the largest known (with respect to the wordlength) ternary self-dual code which meets the above mentioned bound. These ternary code contains 3-designs which are in all propability also new.

In §4.6 a square root bound on the minimum weight of the ternary images of extended QR-codes over GF(9) is established. The proof of this bound is almost the same as the proof in [16].

In §4.7 the relation between [2(n+1), n+1] symmetry codes over GF(3) and the [n+1, ½(n+1)] extended QR-codes over GF(9), n a prime of the form n = 12k + 5, is discussed.

Using the computer the minimum weights of all [2(n+1), n+1] double circulant codes which are the ternary images of extended cyclic codes over GF(9) have been determined up to n = 35. These results are reported in Appendix B.

I wish to thank Prof.dr. J.H. van Lint and dr.ir. H.C.A. van Tilborg for their helpful comments and ir. R.M.A. Wieringa for his excellent advice on programming.

AMS Subject Classification: 94B05, 94B15.

1. Introduction

In this chapter we shall treat in a short way the theory which we need in this report.

1.1. Definitions

In this section we shall give a short introduction to coding theory. For an extensive treatment we refer to [1] or [2].

Let $R^{(n)}$ be the n-dimensional vectorspace over GF(q). A code C of length n over GF(q) is a subset of $R^{(n)}$. The elements of C are called codewords. The set of elements of GF(q) is called the alphabet of the code C.
A k-dimensional linear subspace of $R^{(n)}$ is called a linear code or [n, k]-code over GF(q).
The Hamming-weight $w_H(\underline{x})$ of a vector $\underline{x} \in R^{(n)}$ is the number of non-zero coordinates of $\underline{x}$. The Hamming-distance $d(\underline{x},\underline{y})$ of two vectors $\underline{x}$ and $\underline{y}$ in $R^{(n)}$ is defined by $d(\underline{x},\underline{y}) := w_H(\underline{x} - \underline{y})$. In words: $d(\underline{x},\underline{y})$ is the number of coordinate places in which $\underline{x}$ and $\underline{y}$ differ.
A code C is called e- error- correcting if

$$\forall_{\underline{x}\in C} \quad \forall_{\underline{y}\in C} \left[\underline{x} \neq \underline{y} \Rightarrow d(\underline{x},\underline{y}) \geq 2e + 1 \right] .$$

The minimum distance d of a code C is defined by

$$d := \min \{ d(\underline{x},\underline{y}) \mid \underline{x}\in C,\ \underline{y}\in C,\ \underline{x} \neq \underline{y} \}.$$

It is easy to see that in a linear code the minimum distance is equal to the minimum weight among all non-zero codewords.
An [n, k]-code with minimum distance d is also called an [n, k, d]-code.
In the vectorspace $R^{(n)}$ we define an innerproduct (,) in the usual way

$$\forall_{\underline{x}\in C} \quad \forall_{\underline{y}\in C} \left[(\underline{x},\underline{y}) := x_1y_1 + x_2y_2 + \ldots + x_ny_n \right]$$

(evaluated in GF(q)).
If C is an [n, k]-code, then the dual code $C^{\perp}$ of C is defined by

$$C^{\perp} := \{ \underline{x}\in R^{(n)} \mid \forall_{\underline{y}\in C} \left[(\underline{x},\underline{y}) = 0 \right] \} .$$

The code $C^{\perp}$ is an [n, n-k]-code. The code C is called self-dual, if $C = C^{\perp}$. We remark that, if an [n,k]-code is self-dual, then n has to be even and $k = \frac{1}{2}n$.
A generator matrix G of an [n, k]-code C is a k×n-matrix, the rows of which form a basis of C. A parity-check matrix H of a linear code C is a generator matrix of the code $C^{\perp}$. Both G and H define the code C. The matrices G and H satisfy $GH^T = 0$ (evaluated in GF(q)).
Let C be an [n, k]-code. If we add to every vector $(c_0, c_1, \ldots, c_{n-1})$ of C an extra letter c_∞ such that $c_\infty + c_0 + \ldots + c_{n-1} = 0$, then we obtain a new code $\overline{C}$ which is called the extended code of C. The extra letter c_∞ is called an overall parity-check.
The polynomial A(z) ,

$$A(z) := \sum_{i=0}^{n} A_i z^i,$$

is called the weight enumerator of a code C of length n, if A_i is equal to the number of codewords of weight i in C.
A monomial matrix is a matrix with exactly one non-zero entry in each row and column. An automorphism of a linear code C of length n is an n×n monomial matrix A over GF(q) such that $Ac \in C$ for all $c \in C$. The automorphisms of a code C form a group, the automorphism group, denoted by Aut(C). Two codes C_1 and C_2 both of length n are called equivalent, if there is a monomial matrix which maps C_1 onto C_2.
An [n, k]-code C over GF(q) is called cyclic, if

$$\forall_{(c_0,c_1,\ldots,c_{n-1}) \in C} \left[(c_{n-1}, c_0, \ldots, c_{n-2}) \in C \right].$$

Let R be the ring of all polynomials in x over GF(q), i.e. R = GF(q)[x], and let S be the ideal in R generated by $x^n - 1$. The polynomials of degree < n form a set of representatives for the residue class ring R mod S. This ring R mod S (considered as an additive group) is isomorphic to $R^{(n)}$. The isomorphism is given by $(a_0, a_1, \ldots, a_{n-1}) \leftrightarrow a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$. From now on we do not distinguish between codewords of length n and polynomials of degree < n (mod $(x^n - 1)$). Obviously the polynomial xa(x) mod $(x^n - 1)$ is associated with the vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$, so that multiplication by x in the ring R mod S corresponds to a cyclic shift. From this it follows that a linear code C is cyclic iff C is an ideal in R mod S. Every ideal in R mod S is a principal ideal, i.e. an ideal generated by a polynomial g(x) that divides $x^n - 1$. We shall call g(x) the generator(-polynomial) of the cyclic code C. Thus for all codewords

$c(x) \in C$ there is a polynomial $a(x) \in R$ of degree $\leq n - 1$ such that $c(x) = a(x)g(x)$. Naturally this multiplication is performed in the ring R mod S. The dimension of the cyclic code C is equal to n - degree(g(x)). For cyclic codes of length n over GF(q) we make the restriction gcd(n, q) = 1, so that $x^n - 1$ has no multiple zeros.

1.2. Double circulant codes

In this section we shall give the definition of double circulant codes and explain why we are interested in this class of codes.
First of all we have to introduce circulant matrices.

(1.2.1) Definition: An n×n-matrix is called a circulant matix if each row is obtained from the previous one by a cyclic shift over one position to the right.

Example

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{bmatrix} .$$

It is well known that the algebra of n×n circulant matrices over the field GF(q) is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^n - 1)$. The isomorphism is defined by

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \cdot & \cdot & & \cdot \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix} \quad \leftrightarrow \quad a(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} .$$

(cf. [1, Ch.16, problem(7)]).
From this we may conclude:

(i) The sum and product of two circulant matrices is a circulant matrix. In particular AB = C, where $c(x) = a(x)b(x) \bmod (x^n - 1)$.

(1.2.2) (ii) A is invertible iff a(x) is relatively prime to $x^n - 1$. The inverse, if it exists, is B, where $a(x)b(x) \equiv 1 \bmod (x^n - 1)$.

(iii) A^T is a circulant matrix corresponding to the polynomial $a^T(x) = a_0 + a_{n-1}x + \ldots + a_1 x^{n-1}$.

Now we are able to define double circulant codes.

(1.2.3) Definition: A [2n, n]-code over GF(q) is a double circulant code if it has a generator matrix G of one of the following forms:

$$G = [I_n \mid A]$$

or

$$G = \left[\begin{array}{c|ccc|c|ccc} a & 0 & \ldots & 0 & c & 1 & \ldots & 1 \\ \hline b & & & & d & & & \\ \vdots & & I_{n-1} & & \vdots & & H & \\ b & & & & d & & & \end{array}\right] .$$

Here I_k is the k×k identity matrix, A and H are circulant matrices and a,b,c and d are elements of GF(q).

We remark that in our definition the dimension of a double circulant code must be equal to half of the wordlength, i.e. k = ½n. Furthermore we demand that one of the two circulant submatrices of the generator matrix G is equal to the identity matrix.

There are several good reasons to study the class of double circulant codes.

(i) Several good codes of this type are known (cf. Chapter 2).

(ii) The double circulant codes are particularly simple to encode. If $G = [\, I_n \mid A \,]$ is the generator matrix of such a code and m(x) is a message, then the corresponding codeword becomes (m(x) ; m(x)a(x)). Here m(x) is a polynomial of degree < n over GF(q). Of course this multiplication is performed in the ring $GF(q)[x]/(x^n - 1)$.

1.3. t-Designs

(1.3.1) Definition: A t-design with parameters (v,k,λ) (or a t-(v,k,λ) design) is a collection B of subsets (called blocks) of a set S of v points, such that each block of B contains k points and any set of t points is contained in exactly λ members of B.

In our definition repeated blocks are not allowed.
A 2-design is called a balanced incomplete block design.
In a t-design let λ_i be the number of blocks containing a given set of i points, with $0 < i \leq t$, and let $\lambda_0 = b$ be the total number of blocks. For the parameters λ_i we have the well known relations (cf. [1, Ch.2.Th.9])

$$(1.3.2) \qquad \lambda_i \binom{k-i}{t-i} = \binom{v-i}{t-i} \lambda , \quad 0 \leq i \leq t.$$

From these relations it follows that λ_i is independent of the i points originally chosen. This implies that a t-(v,k,λ) design is also an i-(v,k,λ_i) design for $1 \leq i \leq t$.
It is not known whether there exist non-trivial t-designs with $t \geq 6$.
The reason, why we have given this introduction, is that many t-designs can be constructed from codes. The following theorem, due to E.F. Assmus, Jr. and H.F. Mattson, Jr. (cf. [3]) gives a sufficient condition for a code to contain t-designs.

(1.3.3) Theorem: Let A be an [n, k]-code over GF(q) and let $A^{\perp}$ be the [n, n-k] dual code. Let the minimum weights of these codes be d and e. Let t be an integer less than d. Let v_0 be the largest integer satisfying $v_0 - \left\lfloor \frac{v_0 + q - 2}{q - 1} \right\rfloor < d$ and w_0 the largest integer satisfying $w_0 - \left\lfloor \frac{w_0 + q - 2}{q - 1} \right\rfloor < e$, where , if $q = 2$, we take $v_0 = w_0 = n$. Suppose the number of non-zero weights of $A^{\perp}$, which are less than or equal to $n - t$, is itself less than or equal to $d - t$. Then for each weight v, with $d \leq v \leq v_0$, the subsets of $S := \{1,2, \ldots ,n\}$ which support codewords of weight v in A form a t-design. Futhermore, for each weight w, with $e \leq w \leq \min\{n - t, w_0\}$, the subsets of S which support codewords of weight w in A form a t-design. □

Here $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. A subset U of S is called a support of a codeword $\underline{c}$ if U consists of the indices i for which $c_i \neq 0$.
For the proof of this theorem we refer to [3].

2. Examples of double circulant codes

2.1. Introduction

In this chapter we shall briefly discuss some classes of well-known double circulant codes. We do not have at all the intention to give a complete survey of all known results on double circulant codes. Most of the results we shall only refer to, while other results will be treated more extensively. In §2.2 we shall deal with possible double circulant representations of QR-codes, and in §2.3 we shall discuss symmetry codes. In this section an extension of the well-known theorem on the minimum weight of symmetry codes will be given (cf. Theorem (2.3.5)).

For the results of an exhaustive computer search for the best possible double circulant codes which have a generator matrix G of the form $G = [\ I \mid A\ ]$, up to wordlength 42, we refer to [4], [5] and [6].

In [7] and [8] construction methods are discussed which make use of combinatorial objects, namely difference sets and (v,k,λ)-configurations.

In [9] Kasami has proved that there exist double circulant binary codes which meet a bound slightly weaker than the Gilbert-Varshamov bound.

For a short survey on decoding methods we refer to [1, Ch.16.§9].

2.2. Quadratic residue codes

In this section we shall introduce the class of quadratic residue codes (QR-codes) and discuss some results on double circulant representations of QR-codes. For an extensive treatment of QR-codes we refer [1] and [2]. The results on the double circulant representations of binary QR-codes are taken from [10].

The quadratic residue codes over GF(q) can be defined in the following way. Let n be an odd prime. An element r of $GF(n)\setminus\{0\}$ is called a (quadratic) residue, if there is an $x \in GF(n)$ such that $x^2 = r$. The set of all residues will be denoted by R_0 and the set of all nonresidues by R_1.

We assume that q is a quadratic residue, i.e. $q \in R_0$. Let α be a primitive n-th root of unity in an extension field of GF(q). We define polynomials $g_0(x)$ and $g_1(x)$ by

$$(2.1.1) \qquad g_0(x) := \prod_{r \in R_0} (x - \alpha^r) \quad , \quad g_1(x) := \prod_{r \in R_1} (x - \alpha^r).$$

Note that $x^n - 1 = (x - 1)g_0(x)g_1(x)$. Since $q \in R_0$, the sets R_0 and R_1 are closed under multiplication by q. From this it follows that $g_0(x)$ and $g_1(x)$ both have coefficients from GF(q).

(2.2.2) Definition: The cyclic codes of length n over GF(q) with generators $g_0(x)$, $(x - 1)g_0(x)$, $g_1(x)$ and $(x - 1)g_1(x)$ are called quadratic residue codes (QR-codes).

(2.2.3) Remark: Let $j \in R_1$. Then the transformation $x \to x^j$ interchanges the codes with generators $g_0(x)$ and $g_1(x)$. Hence these two codes are equivalent. In the same way the codes with generators $(x - 1)g_0(x)$ and $(x - 1)g_1(x)$ are equivalent.

(2.2.4) Remark: In this report we shall only consider QR-codes generated by $g_0(x)$. The dimension of these codes is equal to $(n + 1)/2$.

We number the coordinate places of the codewords in the extended QR-codes using the coordinates of the projective line of order n, i.e. $GF(n) \cup \{\infty\}$. The position of the overall parity check is ∞. We make the usual conventions about arithmetic operations: $0^{-1} = \infty$; $\infty^{-1} = 0$; $\infty + a = \infty$ for all a GF(n).
Before mentioning the Theorem of Gleason and Prange on the automorphism group of QR-codes, we have to define PSL(2,n).

(2.2.5) Definition of PSL(2,n): Let n be a prime power, $n = p^r$. The set of all permutations of the elements of the projective line of order n, $GF(n) \cup \{\infty\}$, of the form

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

where a, b, c, $d \in GF(n)$ are such that $ad - bc = 1$, forms a group called the projective special linear group PSL(2,n).

(2.2.6) Remark: A property of PSL(2,n) which we shall need several times is that PSL(2,n) is doubly transitive (cf.[1, Ch.16.Th.9]).

(2.2.7) Theorem (Gleason and Prange): The automorphism group of an extended QR-code over GF(q) of length n + 1 contains a subgroup isomorphic to PSL(2,n). □

For the proof of this theorem we refer to [2,Th.4.4.8].

In this section we shall restrict ourselves to the case q = 2. Since 2 has to be a residue mod n, we have to require that $n \equiv \pm 1 \bmod 8$ (cf. [1, Ch.16.Th.23]).

Double circulant representations of extended binary QR-codes

We shall now give the connection between double circulant codes and extended binary QR-codes. To be able to do that we need another theorem which we shall mention without proof (cf. [1, Ch.16.Lemma 14]).

(2.2.8) Theorem: For any prime $n > 3$, PSL(2,n) contains a permutation π consisting of two cycles of length $\frac{1}{2}(n + 1)$. □

In general let π consist of the cycles

$$(2.2.9) \qquad (l_1 l_2 \ldots l_{\frac{1}{2}(n+1)})(r_1 r_2 \ldots r_{\frac{1}{2}(n+1)}).$$

We take any codeword $\underline{c}$ from the extended QR-code and arrange the coordinates in the order $l_1 \ldots l_{\frac{1}{2}(n+1)} r_1 \ldots r_{\frac{1}{2}(n+1)}$ given by (2.2.9). Then the codewords $\underline{c}, \pi\underline{c}, \pi^2\underline{c}, \ldots, \pi^{\frac{1}{2}(n-1)}\underline{c}$ form a matrix

$$(2.2.10) \qquad [\ L \mid R\ ],$$

where L and R are $\frac{1}{2}(n+1) \times \frac{1}{2}(n+1)$ circulant matrices. If we can find a codeword $\underline{c}$ such that either L or R has full rank, we can obtain, by inverting it, a generator matrix G for the extended QR-code of the form $G = [\ I \mid A\ ]$, where A is a $\frac{1}{2}(n+1) \times \frac{1}{2}(n+1)$ circulant matrix.
The problem associated with such a construction can be stated as follows (cf. [1, Research problem (16.4)]).

(2.2.11) For any odd prime n of the form $n = 8m \pm 1$, is it always possible to find a codeword $\underline{c}$ in the extended binary QR-code, generated by $g_0(x)$, and a permutation π in PSL(2,n) of order $\frac{1}{2}(n + 1)$ such that at least one side (L or R) of the corresponding double circulant matrix $[\ L \mid R\ ]$ is invertible.

In [10] this problem is partially solved. Besides some theorems, in [10], also the results of a computer search are reported. From this computer search

the next theorem follows.

(2.2.12) Theorem: For any suitable prime $n < 200$, except for $n = 89$ and $n = 167$, the extended binary QR-code, generated by $g_0(x)$, has a generator matrix G of the form $G = [\ I \mid A\ ]$, where A is a $\frac{1}{2}(n+1) \times \frac{1}{2}(n+1)$ circulant matrix.

(2.2.13) Remark: The counterexamples $n = 89$ and $n = 167$ show that not every extended QR-code has such a generator matrix.

For a second method to construct a possible double circulant representation for the extended binary QR-code, but now with a generator matrix of the form

$$G = \left[\begin{array}{c|c} I_{\frac{1}{2}(n+1)} & \begin{array}{c|c} a & b \ldots b \\ \hline c & \\ \vdots & A \\ c & \end{array} \end{array}\right] ,$$

where A is a $\frac{1}{2}(n-1) \times \frac{1}{2}(n-1)$ circulant matrix and $a, b, c \in GF(2)$, we refer to [11] and [1, p.498-500].

2.3. Symmetry codes

The symmetry codes form another important class of double circulant codes. These codes were originally defined by V.Pless and therefore they are also called Pless-codes (cf. [12]). In this section we shall discuss some well-known properties of the symmetry codes and we shall treat an extension of a well-known theorem on minimum weights of symmetry codes (cf. Theorem(2.3.5)).

(2.3.1) Definition: Let q be a power of an odd prime, $q \equiv -1 \bmod 6$, and let C_{q+1} be the $(q+1) \times (q+1)$-matrix defined in the following way: The rows and columns of this matrix are labelled using the coordinates of the projective line of order q, $GF(q) \cup \{\infty\}$

(2.3.2)
$$C_{q+1} = \begin{array}{c|c|c} & \infty & GF(q) \\ \hline \infty & 0 & 1 \ldots 1 \\ \hline GF(q) & \varepsilon & \\ & \vdots & Q \\ & \varepsilon & \end{array} ,$$

where $\varepsilon = 1$ if $q = 4k + 1$, $\varepsilon = -1$ if $q = 4k - 1$; Q is a circulant matrix with the following properties

$$Q_{a,a} = 0 ,$$
$$Q_{a,b} = \begin{cases} 1 & \text{if } a - b \text{ is a square in } GF(q), \\ -1 & \text{if } a - b \text{ is not a square in } GF(q), \end{cases}$$

for all $a, b \in GF(q)$, $a \neq b$.
Then the Pless symmetry code Sym_{2q+2} is the $[2q+2, q+1]$- code over $GF(3)$ with generator matrix $G_{2q+2} = [\ I_{q+1} \mid C_{q+1}\ ]$.

(2.3.3) Remark: The matrix Q is often called a Paley-matrix. This matrix satisfies the equation (cf. [13, Lemma 14.1.2]) $QQ^T = qI - J$ (over $\mathbb{R}$). Here J is as usual the matrix consisting entirely of ones. Hence C_{q+1} satisfies

$$C_{q+1}C_{q+1}^T = qI \qquad (\text{over } \mathbb{R}).$$

(2.3.4) Theorem: A Sym_{2q+2} is self-dual and hence all weights are divisible by 3.

Proof: From Remark (2.3.3) if follows $C_{q+1}C_{q+1}^T = -I$ over $GF(3)$, so that $G_{2q+2}G_{2q+2}^T = 0$ over $GF(3)$. Since the dimension of Sym_{2q+2} is equal to half of the wordlength, Sym_{2q+2} is self-dual.

Let $\underline{c} \in Sym_{2q+2}$. Then $w_H(\underline{c}) \equiv (\underline{c},\underline{c}) \equiv 0 \bmod 3$. This proves the second statement of the theorem. □

In describing the weight of a codeword $\underline{x}$ in a symmetry code we shall denote by $w_l(\underline{x})$, $w_r(\underline{x})$ respectively, the contribution to the weight of $\underline{x}$ due to the first $q + 1$ coordinates respectively the last $q + 1$ coordinates.
We shall now give the extension of the theorem on the minimum weight of Sym_{2q+2}.

(2.3.5) Theorem: Let $\underline{x}$ be a codeword in the symmetry code Sym_{2q+2}. Then

(i) if $w_l(\underline{x}) = 1$ then $w_r(\underline{x}) = q$,
(ii) if $w_l(\underline{x}) = 2$ then $w_r(\underline{x}) = (q + 3)/2$,
(iii) if $w_l(\underline{x}) = 3$ then $w_r(\underline{x}) \geq \lceil 3(q - 3)/4 \rceil$,
(iv) if $w_l(\underline{x}) = 5$ then $w_r(\underline{x}) \geq \lceil (q - 9)/2 \rceil$,
(v) if $w_l(\underline{x}) = 7$ then $w_r(\underline{x}) \geq \lceil (q - 27)/4 \rceil$.

Here $\lceil y \rceil$ is the smallest integer $\geq y$.

Proof

(i) By definition.

(ii) Since multiplication of a column by -1 does not alter weights, we may assume that $\underline{x}$ in (ii) is the sum of the following two rows of the generator matrix

$$\begin{array}{l} 1\ 0\ 0\ \ldots\ 0\ \ 0\ 1\ 1\ \ldots\ 1\ \ 1\ \ldots\ \ 1 \\ 0\ 1\ 0\ \ldots\ 0\ \ x_1\ 0\ \underbrace{1\ \ldots\ 1}_{a}\ \underbrace{-1\ \ldots\ -1}_{b} \end{array} .$$

Here $x_1 = 1$ or -1. Since $G_{2q+2}G_{2q+2}^T = (q+1)I$ over $\mathbb{R}$, we have

$$a - b = 0 ,$$
$$a + b = q - 1.$$

Hence $w_1(\underline{x}) = 2$ implies $w_r(\underline{x}) = (q+3)/2$.

(iii), (iv), (v). In order to prove (iii), (iv) and (v) we need some new notations.

Let $\underline{g}_1, \ldots, \underline{g}_{q+1}$ be the $q+1$ rowvectors of the generator matrix. Thus every codeword $\underline{x}$ can be written as

$$\underline{x} = \sum_{i=1}^{q+1} \lambda_i \underline{g}_i \qquad \text{over GF(3)}.$$

Here $\lambda_i \in \{-1, 0, 1\}$. Let $\overline{\underline{x}}$ be the same linear combination of the rowvectors $\underline{g}_1, \ldots, \underline{g}_{q+1}$, but now evaluated over $\mathbb{R}$, i.e.

$$\overline{\underline{x}} = \sum_{i=1}^{q+1} \lambda_i \underline{g}_i \qquad \text{over } \mathbb{R}.$$

The vector $\overline{\underline{x}}$ can be written as $\overline{\underline{x}} = (\lambda_1, \lambda_2, \ldots, \lambda_{q+1}, \mu_1, \mu_2, \ldots, \mu_{q+1})$. Note that for all $1 \leq i \leq q+1$, $|\mu_i| \leq w_1(\underline{x})$. We define the vector $\mu(\overline{\underline{x}})$ by

$$\mu(\overline{\underline{x}}) := (\mu_1, \mu_2, \ldots, \mu_{q+1}).$$

From Remark (2.3.3) it follows that for all $1 \leq i, j \leq q+1$

$$(\underline{g}_i, \underline{g}_j) = \delta_{ij}(q+1), \text{ evaluated over } \mathbb{R},$$

where

$$\delta_{ij} = \begin{cases} 1 \text{ if } i = j, \\ 0 \text{ otherwise.} \end{cases}$$

Hence

$$(2.3.6) \qquad (\underline{\bar{x}},\underline{\bar{x}}) = \sum_{i=1}^{q+1} \lambda_i^2 (\underline{g}_i,\underline{g}_i) = (q+1) w_1(\underline{x}), \text{ over } \mathbb{R},$$

and for the corresponding $\mu(\underline{\bar{x}})$ we have

$$(2.3.7) \qquad (\mu(\underline{\bar{x}}),\mu(\underline{\bar{x}})) = \sum_{i=1}^{q+1} \mu_i^2 = q\, w_1(\underline{x}).$$

To indicate how many components of $\mu(\underline{\bar{x}})$ are equal to $\pm j$, we introduce $\text{Type}(\mu(\underline{\bar{x}}))$ in the following way. If α_j components of $\mu(\underline{\bar{x}})$ are equal to $\pm j$, $0 \le j \le q+1$, then we write

$$\text{Type}(\mu(\underline{\bar{x}})) = (\pm(q+1))^{\alpha_{q+1}} (\pm q)^{\alpha_q} \ldots (\pm 1)^{\alpha_1} (0)^{\alpha_0}.$$

Let $\underline{x}$ be a codeword in Sym_{2q+2} with $w_1(\underline{x}) = p_1$ and $w_r(\underline{x}) = p_2$. We assume that p_1 is odd. Then obviously the number of even components of the vector $\mu(\underline{\bar{x}})$ is equal to p_1. Let $\text{Type}(\mu(\underline{\bar{x}}))$ be given by

$$(2.3.8) \qquad \text{Type}(\mu(\underline{\bar{x}})) = (\pm(p_1-1))^{\alpha_{p_1}-1} \ldots (\pm 2)^{\alpha_2} (0)^{p_1-\alpha_2-\alpha_4 \ldots -\alpha_{p_1}-1}$$
$$(\pm p_1)^{\alpha_{p_1}} \ldots (\pm 1)^{q+1-p_1-\alpha_3-\alpha_5- \ldots -\alpha_{p_1}}.$$

Since $w_r(\underline{\bar{x}}) = p_2$, the following equality holds

$$\alpha_2 + \alpha_4 + \alpha_8 + \ldots + (q + 1 - p_1 - \alpha_3 - \alpha_5 - \ldots - \alpha_{p_1}) +$$
$$\alpha_5 + \alpha_7 + \alpha_{11} + \ldots = p_2.$$

Hence

$$(2.3.9) \qquad \alpha_3 + \alpha_9 + \alpha_{15} + \ldots \ge q + 1 - p_1 - p_2.$$

By (2.3.7) we have

$$p_1 q = (\mu(\underline{x}), \mu(\underline{x})) = 4\alpha_2 + 16\alpha_4 + \ldots + (q + 1 - p_1 - \alpha_3 - \ldots - \alpha_{p_1})$$
$$+ 9\alpha_3 + 25\alpha_5 + \ldots \quad .$$

Hence

(2.3.10) $\quad \alpha_3 + \alpha_9 + \alpha_{15} + \ldots \leq (p_1 - 1)(q + 1)/8.$

By combination of (2.3.9) and (2.3.10) we obtain

(2.3.11) $\quad q + 1 - p_1 - p_2 \leq (p_1 - 1)(q + 1)/8.$

This inequality is trivially satisfied when $p_1 \geq 9$. From (2.3.11) it now follows that:

if $w_1(\underline{x}) = 3$ then $w_r(\underline{x}) \geq \lceil 3(q - 3)/4 \rceil$,
if $w_1(\underline{x}) = 5$ then $w_r(\underline{x}) \geq \lfloor (q - 9)/2 \rfloor$,
if $w_1(\underline{x}) = 7$ then $w_r(\underline{x}) \geq \lceil (q - 27)/4 \rceil$.

This proves (iii), (iv) and (v). □

Remark: The proof of this theorem was originally given in [14].

Without proof we mention the following theorem on the automorphism group of Sym_{2q+2} (cf. [1, Ch.16.Th.18]).

(2.3.12) Theorem: The automorphism group of Sym_{2q+2} contains the following monomial transformations:
If a codeword (L ; R) is in Sym_{2q+2}, so are

(i) (R ; $-\varepsilon$L),

where $\varepsilon = 1$ if $p = 4k + 1$ and $\varepsilon = -1$ if $p = 4k - 1$,
and

(ii) (T(L) ; T(R)),

where T is any element of PSL(2,q).
Hence $Aut(Sym_{2q+2})$ contains a subgroup isomorphic to PSL(2,q). □

(2.3.13) Corollary: Let w_1 and w_2 be integers. Then in a symmetry code:

(i) There is a codeword $\underline{x}$ with $w_1(\underline{x}) = w_1$, $w_r(\underline{x}) = w_2$ iff there is a codeword $\underline{y}$ with $w_1(\underline{y}) = w_2$ and $w_r(\underline{y}) = w_1$.

(ii) For all codewords $\underline{x}$ we have $w_r(\underline{x}) > 0$.

Proof: (i) This follows from Theorem (2.3.12),

(ii) C_{q+1} is non-singular . □

Using Theorem (2.3.12), Robert Calderbank (private communication) has established a square root bound on the minimum weight of symmetry codes.

(2.3.15) Theorem: Let d be the minimum weight of Sym_{2q+2}. Then

(i) $(d-1)^2 - (d-1) + 1 \geq 2q + 1$ if $q \equiv -1 \bmod 12$,

and

(ii) $(d-1)^2 \geq 2q - 1$ if $q \equiv 5 \bmod 12$. □

We shall not prove this theorem. The proof of this theorem is completely analogous to the proof of Theorem (4.6.11).

(2.3.14) Examples of symmetry codes

The first five symmetry codes have parameters [12,6,6], [24,12,9], [36,18,12], [48,24,15], [60,30,18] (cf. [1, Ch.16.§8]).

The weight enumerators of these codes can be found in [15]. Applying the Assmus-Mattson Theorem (cf. Theorem (1.3.3)) yields the following 5-designs (cf. [1, Ch.16.§8]):

[n, k, d]	designs from min.wt.words	other weights giving 5-designs
[12, 6, 6]	5-(12, 6, 1)	9
[24,12, 9]	5-(24, 9, 6)	12, 15
[36,18,12]	5-(36,12,45)	15, 18, 21
[48,24,15]	5-(48,15,364)	18, 21, 24, 27
[60,30,18]	5-(60,18,1530)	21, 24, 27, 30, 33

3. Extended cyclic codes over GF(4) and their binary images

3.1. Introduction

In [1, Ch.16.§7] the authors have defined a class of double circulant codes which can be considered as the binary images of extended QR-codes over GF(4) of length n + 1, where n is a prime of the form n = 8k + 3. In [16] a square root bound on the minimum weight of these codes was established. In [17] the class of double circulant codes which are the binary images of extended QR-codes over GF(4) of length n + 1, where n is a prime of the form n = 8k - 3, is also introduced. However all authors have restricted themselves to the binary images of extended quaternary QR-codes (i.e. QR-codes over GF(4)).
In order to place this class of codes within a bigger framework, we shall introduce in this chapter a much larger class of double circulant codes, namely those double circulant codes which are the binary images of extended cyclic codes over GF(4).
In §3.2 a necessary and sufficient condition in order that the binary image of an extended cyclic code over GF(4) is a double circulant code will be derived (cf. Theorem (3.2.9)). Furthermore it will appear that the double circulant codes which have a generator matrix of the form G = [I | A], A a circulant matrix, can not be the binary images of cyclic codes over GF(4) (cf. Theorem (3.2.3)).
In §3.3 we shall develop some theory on the quaternary cyclic codes over GF(4), the extended codes of which have double circulant images, e.g. the idempotent will be given and a square root bound on the minimum weight will be established.
In §3.4 some theory on the binary images will be discussed, e.g. some theory on the automorphisms and the dual code.
In §3.5 we shall discuss the known results on the binary images of the extended quaternary QR-codes. The square root bound on their minimum weight, derived in [16], will be mentioned and compared with the results of [17].
We have also determined, using the computer, the minimum weights of all [2(n+1), n+1] double circulant codes which are the binary images of extended cyclic codes over GF(4), up to n = 45. These results and also the weight enumerators of these double circulant codes, up to n = 19, are reported in Appendix A. These results will also be briefly discussed in §3.6

3.2. General theory

3.2.1. A necessary and sufficient condition

In this subsection we shall derive a necessary and sufficient condition for a double circulant code to be the binary image of an extended cyclic code over GF(4).

Let ω be a primitive element of GF(4), i.e. GF(4) consists of the elements 0, 1, ω, $\omega^2 = \omega + 1$.
The mapping which sends vectors of the n-dimensional vectorspace over GF(4) into vectors of the 2n-dimensional vectorspace over GF(2) is defined in the following way.

(3.2.1) Definition: Let $(a_1+\omega b_1, a_2+\omega b_2, \ldots, a_n+\omega b_n)$ be a vector of length n over GF(4), where $a_i, b_i \in$ GF(2). Then the binary image of this vector is defined to be

$$(a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n).$$

(3.2.2) Remark: The mapping, defined in this way, sends [n, k]-codes over GF(4), in a one-to-one way, onto [2n, 2k] binary codes.

Double circulant codes which have a generator matrix of the form $G = [\ I \mid A\ ]$ can not be the binary images of cyclic codes over GF(4), as stated in the following theorem.

(3.2.3) Theorem: Let C be a [2n, n] double circulant code with generator matrix $G = [\ I \mid H\ ]$, where H is an n×n circulant matrix with toprow h(x). Then the code C can not be the binary image of a cyclic code D over GF(4).

Proof: Let C be the binary image of a cyclic code D of lenght n over GF(4). Then $1 + \omega h(x)$ has to be a codeword of D. Hence also $(a(x) + \omega b(x))(1 + \omega h(x)) \in D$, where a(x) and b(x) are polynomials of degree < n over GF(2). Since

$$\begin{aligned}(a(x) + \omega b(x))(1 + \omega h(x)) &= a(x) + b(x)h(x) + \\ &\quad + \omega(a(x)h(x) + b(x) + b(x)h(x)),\end{aligned}$$

the binary image of this codeword is

$$(a(x) + b(x)h(x) \; ; \; a(x)h(x) + b(x) + b(x)h(x)).$$

This is an element of C. Hence the following equation must be satisfied

$$(a(x) + b(x)h(x))h(x) = a(x)h(x) + b(x) + b(x)h(x),$$

i.e.

$$b(x)(h^2(x) + h(x) + 1) = 0.$$

Since b(x) can be arbitrarily chosen, we may take b(x) = 1. This yields

$$h^2(x) + h(x) + 1 = 0.$$

Substituting x = 1 in this equation yields $h^2(1) + h(1) + 1 = 0$. This is impossible, since $h(1) \in GF(2)$. Hence we have proved the theorem. □

(3.2.4) Remark: In fact all the polynomial equations are congruence relations mod $(x^n - 1)$. Thus substituting values of x in these equations must be done carefully.

Since we want to consider cyclic codes over GF(4), the binary images of which are double circulant codes, the only quaternary codes we have to study are the codes generated by a polynomial g(x) of the form $g(x) = 1 + \omega h(x)$. We repeat that a cyclic code D over GF(4), generated by $g(x) = 1 + \omega h(x)$, is the principal ideal in $GF(4)[x]/(x^n - 1)$ generated by g(x). In this case we do not require g(x) to be a factor of $x^n - 1$.
In this report we use the following notation.

(3.2.5) Notation: $j(x) = 1 + x + x^2 + \ldots + x^{n-1}$.

(3.2.6) Lemma: Let C be the [2n, n+1] code over GF(2) with generator matrix

$$G_0 = \left[\begin{array}{c|c} \underline{0 \; . \; . \; . \; 0} & \underline{1 \; . \; . \; . \; 1} \\ I & H \end{array}\right],$$

where H is an n×n circulant matrix with toprow h(x). If the polynomial h(x)

satisfies the equation

$$h^2(x) + h(x) + 1 = j(x),$$

then the code C is the binary image of the quaternary cyclic code D generated by $g(x) = 1 + \omega h(x)$.

Proof: First of all we have to show that $\omega j(x) \in D$. This is true since $(h(x) + \omega)(1 + \omega h(x)) = \omega(h^2(x) + h(x) + 1) = \omega j(x)$. Let $(a(x) + \omega b(x))(1 + \omega h(x))$ be any codeword of D. It suffices to show that the binary image of this codeword is an element of C. The binary image is given by

$$(a(x) + b(x)h(x) \; ; \; a(x)h(x) + b(x) + b(x)h(x)).$$

This is a codeword in C iff the following relation holds

$$(a(x) + b(x)h(x))h(x) + \varepsilon j(x) = a(x)h(x) + b(x) + b(x)h(x),$$

where ε is 0 or 1.
This is equivalent with

$$\varepsilon j(x) = b(x)(h^2(x) + h(x) + 1) = b(x)j(x).$$

Since $b(x)j(x) = b(1)j(x)$, this equation is trivially satisfied by taking $\varepsilon = b(1)$.

□

(3.2.7) Remark: We have already remarked that all equations are in fact congruence relations mod $(x^n - 1)$. Since $xj(x) \equiv j(x) \bmod (x^n - 1)$, it is easily seen that $b(x)j(x) \equiv b(1)j(x) \bmod (x^n - 1)$, i.e. $b(x)j(x) = b(1)j(x)$.

(3.2.8) Corollary: A sufficient condition for a cyclic code D of length n over GF(4), generated by $g(x) = 1 + \omega h(x)$, to have dimension $\frac{1}{2}(n + 1)$ is

$$h^2(x) + h(x) + 1 = j(x).$$

Proof: By substituting $x = 1$ we obtain $j(1) = 1$. Hence n must be odd. From Lemma (3.2.6) it follows that the binary image of D has dimension $n + 1$, so D has dimension $\frac{1}{2}(n + 1)$.

□

The code C,defined in Lemma (3.2.6),is not really a double circulant code, since the dimension is n + 1 and the wordlength 2n. In our definition of double circulant codes the dimension must be equal to half of the wordlength (cf. Definition (1.2.3)). This problem can be met by looking at the binary image C of the extended code $\overline{D}$. We extend the code D in the usual way. To every codeword $(c_0,c_1, \ldots ,c_{n-1}) \in D$ we add an overall parity check c_∞ such that $c_\infty + c_0 + \ldots + c_{n-1} = 0$. Hence the codeword $1 + \omega h(x) \in D$ will be extended to $(1 + \omega h(1),\ 1 + \omega h(x))$. The binary image of this codeword is $(1,1,0 \ldots 0; h(1), h(x))$.

(3.2.9) Theorem: A necessary and sufficient condition for the binary image of the extended code $\overline{D}$ over GF(4) of wordlength n + 1 generated by $g(x) = 1 + \omega h(x)$ to be a $[2(n+1),\ n+1]$ double circulant code C is

$$h^2(x) + h(x) + 1 = j(x).$$

The generator matrix G of the code C is given by

$$G = \left[\begin{array}{c|c|c|c} 0 & 0 \ldots 0 & 1 & 1 \ldots 1 \\ \hline 1 & & h(1) & \\ \vdots & I_n & \vdots & H \\ 1 & & h(1) & \end{array}\right].$$

Here H is the n×n circulant matrix with toprow h(x).

Proof: Analogous to the proofs of Theorem (3.2.3) and Lemma (3.2.6). □

Hence for given $n \in \mathbb{N}$ we can determine all $[2(n+1),\ n+1]$ double circulant codes C which are the binary images of extended cyclic quaternary codes D of length n + 1, generated by $g(x) = 1 + \omega h(x)$, provided that we know all solutions h(x) of the equation $h^2(x) + h(x) + 1 = j(x)$.

3.2.2. Analysis of the equation $h^2(x) + h(x) + 1 = j(x)$

In this subsection we shall analyse the equation

(3.2.10) $$h^2(x) + h(x) + 1 = j(x).$$

Obviouslythis equation depends on n.

(3.2.11) Definition: We call an odd integer n feasible if the set $S = \{1,2,\ldots,n-1\}$ can be divided in two disjoint subsets S_1 and S_2 such that

(3.2.12) $\quad \forall_{a\in S} \; [\; a \in S_1 \;\Leftrightarrow\; 2a \bmod n \in S_2 \;]$.

The meaning of this definition will be clarified by the following lemma.

(3.2.13) Lemma: For given $n\in \mathbb{N}$, n odd, there exists a solution h(x) of (3.2.10) iff n is feasible.

Proof: Let $h(x) = x^{i_1} + x^{i_2} + \ldots + x^{i_\ell}$ be any solution of (3.2.10). Then

$$j(x) = h^2(x) + h(x) + 1 =$$
$$= (x^{2i_1} + x^{2i_2} + \ldots + x^{2i_\ell} + x^{i_1} + \ldots + x^{i_\ell} + 1) \bmod (x^n - 1).$$

Obviously it follows that $\ell \geq \frac{1}{2}(n-1)$ if $h(0) = 0$ and $\ell \geq \frac{1}{2}(n+1)$ if $h(0) = 1$. Furthermore h(x) + j(x) is also a solution of (3.2.10), since

$$(h(x) + j(x))^2 + h(x) + j(x) + 1 = h^2(x) + h(x) + 1 = j(x).$$

Hence it follows that $\ell \leq \frac{1}{2}(n-1)$ if $h(0) = 0$ and $\ell \leq \frac{1}{2}(n+1)$ if $h(0) = 1$. Now we may conclude that the polynomials $h^2(x)$ and h(x) have no coefficients in common, unless $h(0) = 1$. In this case $h^2(x)$ and h(x) have only the coefficient of x^0 in common. So we have proved the first part of the lemma.
Let n be feasible. Then obviously the polynomials h(x), defined by $h(x) = \sum_{r\in S_i} x^r$, respectively $h(x) = 1 + \sum_{r\in S_i} x^r$, $i = 1, 2$, satisfy equation (3.2.10). □

Because of this lemma, the only thing we have to do, in order to determine all solutions h(x) of (3.2.10), is to calculate all feasible values of n.
We shall prove some lemmas on the feasibility of n.

(3.2.14) Lemma: Let $n \in \mathbb{N}$. Then n is feasible iff n and $2^{2i+1} - 1$ are relatively prime for all $i \in \mathbb{N}$.

Proof: By definition

$$n \text{ is not feasible} \Leftrightarrow \exists_i \exists_{s<n} [\ s = 2^{2i+1}s \bmod n\ ] .$$

The later statement is equivalent with

$$\exists_i \exists_{s<n} [\ n \mid s(2^{2i+1} - 1)\ ] .$$

Since $s < n$ this is equivalent with

$$\exists_i [\ \gcd(n, 2^{2i+1} - 1) \neq 1\ ] . \qquad \square$$

(3.2.15) Corollary: Let $n_i \in \mathbb{N}$, $i = 1, 2$. Then n_1 and n_2 both are feasible iff $n_1 n_2$ is feasible. $\square$

(3.2.16) Lemma: Prime numbers p of the form $p = 8k - 1$ are not feasible. Prime numbers p of the form $p = 8k \pm 3$ are feasible.

Proof: Let e be the multiplicative order of 2 mod p, i.e. $2^e \equiv 1 \bmod p$ and for all $1 \leq i \leq e$ $2^i \not\equiv 1 \bmod p$. Let g be a primitive element of GF(p) and let t be chosen such that $2 = g^t$. Then

$$e = \frac{p - 1}{\gcd(p-1, t)} .$$

If $p = 8k - 1$, then 2 is a quadratic residue mod p, so that t is even and $e = (4k - 1)/\gcd(4k-1, t/2)$ is odd. Because of Lemma (3.2.14) $p = 8k - 1$ is not feasible.
If $p = 8k \pm 3$, then 2 is a nonresidue mod p. Hence t is odd and e is even, so that $p = 8k \pm 3$ is feasible. $\square$

(3.2.17) Remark: Prime numbers of the form $p = 8k + 1$ may or may not be feasible. This follows from the fact that $p = 17$ is feasible and $p = 73$ not.

The proof of Lemma (3.2.16) is adapted from [18, Th.37].

Using Lemma (3.2.16) and Corollary (3.2.15) the feasible values of n, $n < 100$, can easily be calculated. These values are shown in Fig.3.1.

3, 5, 9, 11, 13, 15, 17, 19, 25, 27, 29, 33, 37, 39, 41, 43, 45,
51, 53, 55, 57, 59, 61, 65, 67, 75, 81, 83, 85, 87, 91, 95, 97, 99

Fig.3.1. Feasible values of n, $n \leq 100$.

For some values of n, the sets S_1 and S_2, defined in (3.2.11), are uniquely determined, up to mutually interchanging, namely for those values of n, for which the order of 2 mod n is equal to n - 1. Obviously those values must be prime numbers, because of the Theorem of Euler. The prime numbers $n < 100$ which have 2 as a primitive element are shown in Fig.3.2.

3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83

Fig.3.2. Prime numbers < 100 which have
2 as a primitive element.

To illustrate the theory of this section we shall give two examples of double circulant codes which are the binary images of extended cyclic codes over GF(4).

(3.2.18) Examples

(i) $n = 3$.

In this case S_1 and S_2 are particularly simple to determine, namely $S_1 = \{1\}$, and $S_2 = \{2\}$. Let $h(x) = 1 + x$. Then the generator matrix of the [8, 4] double circulant code is given by

$$G = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]$$

This double circulant code is equivalent to the extended [8,4,4] Hamming code (cf. [1, p.508]).

(ii) $n = 11$.

In this case $S_1 = \{1,4,5,9,3\}$ and $S_2 = \{2,8,10,7,6\}$. Let $h(x) = 1 + \sum_{r \in S_1} x^r$, then the generator matrix of the [24, 12] double circulant code is given by

$$G = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & 0 & & & \\ \vdots & & I_{11} & & \vdots & & H & \\ 1 & & & & 0 & & & \end{array}\right],$$

where H is the circulant matrix with toprow h(x).
This code is the [24,12,8] extended binary Golay code (cf. [1, p.508]).
For a complete list of all [2(n+1), n+1] double circulant codes which are the binary images of extended cyclic codes over GF(4), up to n = 45, we refer to Appendix A.
For the rest of this chapter we shall need some special properties of the function h(x) which are mentioned in the following lemma.

(3.2.19) Lemma: Let h(x) satisfy equation (3.2.10). Then

$$h^3(x) = 1 + (1 + h(1))j(x) \ , \ h^4(x) = h(x).$$

Proof: The polynomial h(x) satisfies $h^2(x) + h(x) + 1 = j(x)$. Multiplying by h(x) yields $h^3(x) + h^2(x) + h(x) = h(1)j(x)$, so that

$$h^3(x) = 1 + (1 + h(1))j(x).$$

Once again multiplying by h(x) yields

$$h^4(x) = h(x) + h(1)(1 + h(1))j(x) = h(x).$$ □

3.3. Some properties of the cyclic code *D* over GF(4)

In this section we shall show some properties of the cyclic code *D* over GF(4) generated by $g(x) = 1 + \omega h(x)$, where h(x) satisfies the equation (3.2.10). The wordlength of the code *D* is denoted by n.

3.3.1. The idempotent of *D*

First of all we have to introduce the idempotent of a cyclic code (cf. [2, Th.(3.3.1)]).

(3.3.1) Theorem: Let C be a cyclic code of length n over GF(q). Then there is a unique polynomial $F(x) \in C$, called the idempotent, with the following properties:

(i) $F(x) = F^2(x)$,

(ii) $F(x)$ generates C,

(iii) $\forall_{c(x)\in C}\ [\ c(x)F(x) = c(x)\ ]$, i.e. $F(x)$ is a unit for C.

Proof: (i) Let $g_0(x)$ be the generator polynomial of C. Since $g_0(x)$ divides $x^n - 1$, there exists a unique polynomial $h_0(x)$ in GF(q)[x] such that $g_0(x)h_0(x) = x^n - 1$. On account of the restriction gcd(n,q) = 1, which we have made for cyclic codes over GF(q), $x^n - 1$ has no multiple zeros. Hence $\gcd(g_0(x), h_0(x)) = 1$. Therefore there are polynomials p(x) and q(x) such that in GF(q)[x]

(3.3.2) $$p(x)g_0(x) + q(x)h_0(x) = 1.$$

Set $F(x) = p(x)g_0(x)$. Then from (3.3.2)

$$p(x)g_0(x)\{p(x)g_0(x) + q(x)h_0(x)\} = p(x)g_0(x).$$

Hence in $GF(q)[x]/(x^n - 1)$ the following relations holds: $F^2(x) + 0 = F(x)$. So we have proved (i).

(ii) Obviously F(x) is an element of the code generated by $g_0(x)$. Since $\gcd(F(x), x^n - 1) = \gcd(p(x)g_0(x), g_0(x)h_0(x)) = g_0(x)$, $g_0(x)$ is an element of the code generated by F(x). This proves (ii).

(iii) By (ii) every codeword $c(x) \in C$ is a multiple of F(x). Let $c_1(x) = c(x)F(x)$. Then $c_1(x)F(x) = c(x)F^2(x) = c(x)F(x) = c_1(x)$. □

The idempotent of the cyclic code D over GF(4) can easily be expressed in terms of the function h(x).

(3.3.3) Theorem: Let h(x) satisfies $h^2(x) + h(x) + 1 = j(x)$. Then the idempotent of the cyclic quaternary code D, generated by $g(x) = 1 + \omega h(x)$, is given by

$$F_e(x) = \omega^2(h(x) + 1) + \omega(h^2(x) + 1) \qquad \text{if } h(1) = 0$$

and

$$F_0(x) = \omega^2 h^2(x) + \omega h(x) \qquad \text{if } h(1) = 1.$$

Proof: (i) Let $h(1) = 0$. Then $F_e(x) = (j(x) + \omega h(x))(1 + \omega h(x))$, so that $F_e(x) \in D$. If $h(1) = 1$, then we find $F_0(x) = \omega h(x)(1 + \omega h(x))$, so that $F_0(x) \in D$.

(ii) $F_e^2(x) = \omega(h^2(x) + 1) + \omega^2(h^4(x) + 1) =$
$= \omega(h^2(x) + 1) + \omega^2(h(x) + 1) = F_e(x)$, if $h(1) = 0$;

$F_0^2(x) = \omega^4 h^4(x) + \omega^2 h^2(x) = \omega h(x) + \omega^2 h^2(x) =$
$= F_0(x)$, if $h(1) = 1$ (by Lemma (3.2.19)) .

(iii) Let $h(1) = 0$. Then by Lemma (3.2.19) it is easy to prove that

$$F_e(x)g(x) = \{\omega^2(h(x) + 1) + \omega(h^2(x) + 1)\}(1 + \omega h(x)) =$$
$$= 1 + \omega h(x) = g(x).$$

If $h(1) = 1$, then we find also that $F_0(x)g(x) = g(x)$.

By (i), (ii) and (iii) $F_e(x)$, respectively $F_0(x)$ is the idempotent of D, when $h(1) = 0$ respectively $h(1) = 1$. □

Remark: We have found this theorem by generalizing the formula of the idempotent of the quaternary QR-code (cf. [1, Ch.16.Th.4]).

3.3.2. The generator polynomial of D

We repeat that D is the cyclic code over GF(4) generated by $g(x) = 1 + \omega h(x)$. However we have not demanded $g(x)$ to be a factor of $x^n - 1$, so that $g(x)$ is not really a generator polynomial. For a subclass of the cyclic codes over GF(4) generated by polynomials of the form $1 + \omega h(x)$, where $h(x)$ satisfies $h^2(x) + h(x) + 1 = j(x)$, we have been able to determine a generator polynomial $\gamma(x)$ (i.e. a polynomial of lowest degree in the ideal of $GF(4)[x]/(x^n - 1)$ consisting of multiples of $1 + \omega h(x)$). Unfortunately it will appear that this subclass of codes contains only quaternary QR-codes.

Let n be feasible. We assume that the set $S = \{1,2, \ldots ,n-1\}$ can be divided in two mutually disjoint subsets S_1 and S_2 satisfying (3.2.12) and

$$\forall_{a \in S_1} \forall_{b \in S_1} \quad [\ ab \bmod n \in S_1\ ] ,$$

(3.3.4) $$\forall_{a\in S_1}\ \forall_{b\in S_2}\ [\ ab \bmod n \in S_2\ ]\ ,$$
$$\forall_{a\in S_2}\ \forall_{b\in S_2}\ [\ ab \bmod n \in S_1\ ]\ .$$

(3.3.5) Theorem: Let n be a feasible prime. Let S_1 and S_2 satisfy (3.2.12) and (3.3.4). Then the polynomial $\gamma(x)$, defined by

$$\gamma(x) := \prod_{i\in S_1} (x - \alpha^i)\ ,$$

is a generator polynomial of the cyclic code D over GF(4) generated by $g(x) = 1 + \omega h(x)$. Here α is a suitable chosen n-th root of unity in an extension field of GF(4); the polynomial $h(x)$ satisfies (3.2.10).

Proof: We restrict ourselves to the case $h(1) = 0$, since the proof in case $h(1) = 1$ goes along the same lines.
Obviously 1 has to be an element of S_1. Let r be any element of S_1. Then

$$h(\alpha^r) = \sum_{j\in S_1} \alpha^{rj}.$$

Since S_1 and S_2 satisfy (3.3.4), we find $h(\alpha^r) = h(\alpha)$. Hence also $h^2(\alpha^r) = h^2(\alpha)$. Let s be any element of S_2. Then in the same way we are led to $h(\alpha^s) = h^2(\alpha)$ and $h^2(\alpha^s) = h^4(\alpha) = h(\alpha)$.
So we may conclude that for $r\in S_1$

$$F_e(\alpha^r) = \omega^2(h(\alpha^r) + 1) + \omega(h^2(\alpha^r) + 1) =$$
$$= \omega^2(h(\alpha) + 1) + \omega(h^2(\alpha) + 1) = F_e(\alpha).$$

Since $F_e^2(\alpha) = F_e(\alpha)$, $F_e(\alpha)$ is equal to 0 or 1. Let us choose α such that $F_e(\alpha) = 0$. This can be done, as n is a prime. Then we find that $F_e(\alpha^r) = 0$ for all $r \in S_1$. Let $s \in S_2$. Then

$$F_e(\alpha^s) = \omega^2(h(\alpha^s) + 1) + \omega(h^2(\alpha^s) + 1) = \omega^2(h^2(\alpha) + 1) + \omega(h(\alpha) + 1) =$$
$$= \omega^2(h(\alpha) + 1) + \omega(h^2(\alpha) + 1) + h^2(\alpha) + h(\alpha) =$$
$$= F_e(\alpha) + j(\alpha) + 1 = 1.$$

Furthermore

$$F_e(1) = \omega^2(h(1) + 1) + \omega(h^2(1) + 1) = \omega^2 + \omega = 1.$$

Hence we may conclude

$$F_e(\alpha^i) = 0 \quad \Leftrightarrow \quad \gamma(\alpha^i) = 0 \qquad \text{for all } i \in S.$$

Thus $F_e(x)$ is an element of the code generated by $\gamma(x)$. The dimension of the code D is equal to $\frac{1}{2}(n + 1)$, just as the dimension of the code generated by $\gamma(x)$. As $F_e(x)$ is the idempotent of D, we now have proved that $\gamma(x)$ is the generator polynomial of D. □

Unfortunately the set of feasible values of n which permit a partition of the set S into the sets S_1 and S_2, which satisfy (3.2.12) and (3.3.4), is limited, as we shall see in the following lemma.

(3.3.6) Lemma: Let n be feasible. Then the set $S = \{1,2, \ldots ,n-1\}$ can be divided into two disjoint subsets S_1 and S_2, satisfying (3.2.12) and (3.3.4), iff n is a prime of the form $n = 8k \pm 3$, S_1 is the set consisting of the quadratic residues mod n and S_2 is the set of all nonresidues.

Proof: Let S permit such a partition into the sets S_1 and S_2. Then

(i) Obviously n must be a prime. Otherwise let $p|n$. Then $0 = (p.n/p)$ is an element of $S_1 \cup S_2$. This is impossible.

(ii) Let $n = 8k + 1$ be a feasible prime. Then in this case 2 and 2^{-1} are residues mod n . Let $a \in GF(n)$ be such that $a^2 = 2^{-1}$. Then $a \times 2a = 1 \bmod n$. Since a and 2a may not be elements of the same set S_i, 1 has to be an element of S_2. This contradicts $1 \in S_1$.

(iii) Since prime numbers of the form $n = 8k - 1$ are not feasible, the only remaining possibility is that n is a prime number of the form $n = 8k \pm 3$. In this case let $a \in S$. Then $2a^2 = a \times 2a \in S_2$. Hence $a^2 \in S_1$. This implies that S_1 has to contain all quadratic residues mod n. Since the cardinality of S_1 is equal to the cardinality of S_2, S_2 has to contain all nonresidues mod n.

Clearly if $n = 8k \pm 3$ is a prime, then the set S_1, consisting of all residues mod n, and the set S_2, consisting of all nonresidues, satisfy (3.2.12) and (3.3.4). □

(3.3.7) Corollary: Let n be a prime of the form $n = 8k \pm 3$, S_1 the set of all residues mod n and h(x) the polynomial defined by $h(x) = \sum_{r \in S_1} x^r$. Then the quaternary cyclic code generated by $g(x) = 1 + \omega h(x)$, is a QR-code of length n and dimension $\frac{1}{2}(n + 1)$.

Proof: This is a consequence of Lemma (3.3.6), Theorem (3.3.5) and the definition of QR-codes. □

3.3.3. A square root bound on the minimum weight of D

In this subsection we shall establish a square root bound on the minimum weight of the code D. We repeat that the code D is a pricipal ideal in $GF(4)[x]/(x^n - 1)$ generated by $g(x) = 1 + \omega h(x)$. Here h(x) is a solution of (3.2.10) and n denotes the wordlength of D.
We define the cyclic code D^* over GF(4) to be the principal ideal in $GF(4)[x]/(x^n - 1)$ with generator $g^*(x) = 1 + \omega h^2(x)$. We note that $h^2(x)$ is also a solution of (3.2.10), since $h^4(x) = h(x)$. Hence the binary image of the extended code $\overline{D}^*$ is also a double circulant code.

(3.3.8) Lemma: Let D and D^* be the cyclic codes over GF(4) as defined above. Then

$$D \cap D^* = \langle j(x) \rangle,$$

where $\langle j(x) \rangle$ is the ideal in $GF(4)[x]/(x^n - 1)$ generated by j(x).

Proof: The binary images of the extended codes $\overline{D}$ and $\overline{D}^*$ are denoted by C and C^*. Let H be the n×n circulant matrix with toprow h(x). Then H^2 is the circulant matrix with toprow $h^2(x)$. The generator matrices of C and C^* are called G and G* respectively, i.e.

$$G = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & h(1) & & & \\ \vdots & & I & & \vdots & & H & \\ 1 & & & & h(1) & & & \end{array}\right], \quad G^* = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & h(1) & & & \\ \vdots & & I & & \vdots & & H^2 & \\ 1 & & & & h(1) & & & \end{array}\right].$$

It suffices to show that

$$C \cap C^* = \{(\underline{0},\underline{0}),\ (\underline{0},\underline{1}),\ (\underline{1},\underline{0}),\ (\underline{1},\underline{1})\}\ ,$$

where $\underline{0}$ and $\underline{1}$ are vectors of length n + 1. Let $(a_\infty, a(x)\ ;\ b_\infty, b(x)) \in C \cap C^*$. Then

$$b(x) = a(x)h(x) + \varepsilon_1 j(x),$$

since this codeword is an element of C. Furthermore

$$b(x) = a(x)h^2(x) + \varepsilon_2 j(x),$$

since this codeword is an element of C^*. Substituting x = 1 in these two equations yields $\varepsilon_1 = \varepsilon_2 = a(1)h(1) + b(1)$. Hence it follows

$$0 = a(x)(h^2(x) + h(x)) = a(x)(1 + j(x)).$$

Thus $a(x) = a(1)j(x)$ and $b(x) = b(1)j(x)$. □

Using this lemma we can prove a square root bound for the minimum weight of the code D.

(3.3.9) Theorem: Let c(x) be a codeword of D, $c(1) \neq 0$, and let d be the weight of c(x). Then

(i) $d^2 \geq n$,

(ii) $d^2 - d + 1 \geq n$, if h(x) satisfies the extra condition $h^2(x) = h(x^{-1})$.

Proof: (i) Since $c(x) \in D$, c(x) can be written as $c(x) = (a(x) + \omega b(x))(1 + \omega h(x))$. Thus, since $h(x^2) = h^2(x)$, $c(x^2) = (a(x^2) + \omega b(x^2))(1 + \omega h(x^2)) \in D^*$. Hence

$$c(x)c(x^2) \in D \cap D^*.$$

As we have made the restriction $c(1) \neq 0$, we may conclude, by Lemma (3.3.8), that $c(x)c(x^2) = c_0(x)j(x)$, where $c_0 \in GF(4)\backslash\{0\}$. Obviously $w_H(c(x^2)) = w_H(c(x)) = d$. Thus

$$d^2 \geq w_H(c(x)c(x^2)) = n.$$

(ii) If the polynomial h(x) satisfies the extra condition $h^2(x) = h(x^{-1})$, then in the same way as in (i) it follows that $c(x) \in D$ implies that $c(x^{-1}) \in D^*$, so that

$$c(x)c(x^{-1}) \in D \cap D^*.$$

Since $c(1) \neq 0$, there exists $c_1 \in GF(4)\backslash\{0\}$ such that $c(x)c(x^{-1}) = c_1 j(x)$. Hence

$$n = w_H(c(x)c(x^{-1})) \leq w_H(c(x))w_H(c(x^{-1})) - d + 1 = d^2 - d + 1 .$$ □

(3.3.10) Remark: The set of feasible values of n, for which there exists a polynomial h(x), which satisfies (3.2.10) and the extra condition $h^2(x) = h(x^{-1})$, consists of the values of n, which permit a partition of the set $S = \{1, 2, \ldots, n-1\}$ into S_1 and S_2, satisfying $S_2 = -S_1$ and (3.2.12). This set of feasible values contains in any case all prime numbers of the form $n = 8k + 3$. For, if $n = 8k + 3$ is a prime, then -1 and 2 are nonresidues mod n. Hence the set S_1, containing all residues mod n and the set S_2, consisting of all nonresidues mod n, satisfy $S_2 = -S_1$. The feasible values of $n \leq 100$, for which S_1 and S_2 satisfy $S_2 = -S_1$ can easily be calculated by hand. These values are shown in Fig.3.3.

3, 9, 11, 19, 27, 33, 43, 51, 57, 59, 67, 81, 83, 91, 99

Fig. 3.3. Feasible values of $n \leq 100$, for which $S_2 = -S_1$.

3.4. Some properties of the double circulant codes C which are the binary images of extended cyclic ocdes D over GF(4)

3.4.1. Introduction

In this section let D be a cyclic code over GF(4) of length n generated by $g(x) = 1 + \omega h(x)$, where h(x) satisfies $h^2(x) + h(x) + 1 = j(x)$. The $[2(n+1), n+1]$ double circulant code which is the binary image of the extended code $\overline{D}$ is denoted by C. Furthermore the n×n circulant matrix with toprow h(x) is denoted by H.

In this section we shall derive some properties of the code C, e.g. some properties of the automorphism group of C and some properties of the dual of C. Let G be the generator matrix of C, i.e.

$$(3.4.1) \qquad G = \left[\begin{array}{c|ccc|c|ccc} \ell_\infty & \ell_0 & \cdots & \ell_{n-1} & r_\infty & r_0 & \cdots & r_{n-1} \\ \hline 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & h(1) & & & \\ \vdots & & I & & \vdots & & H & \\ 1 & & & & h(1) & & & \end{array}\right] .$$

In this introduction we shall prove an easy lemma on the codewords of C which we shall need several times in this chapter.

(3.4.2) Lemma: Let $(a_\infty, a(x) ; b_\infty, b(x))$ be a codeword of C. Then

$$a_\infty = a(1),\ b_\infty = b(1) \text{ and } b(x) = a(x)h(x) + (b_\infty + a_\infty h(1))j(x).$$

Proof: Let $(a_\infty, a(x) ; b_\infty, b(x))$ be in C. Then there exists a vector $(\omega_\infty, \omega(x))$ of length $n + 1$ such that

$$(\omega_\infty, \omega(x))G = (a_\infty, a(x) ; b_\infty, b(x)),$$

i.e.

$$a_\infty = \omega(1),\ a(x) = \omega(x),\ b_\infty = \omega_\infty + \omega(1)h(1),\ b(x) = \omega(x)h(x) + \omega_\infty j(x).$$

From these relations the lemma easily follows. □

3.4.2. On the automorphism group of C

In this subsection we shall derive some properties of the automorphism group of C. We have found these properties by generalizing some theorems on the automorphism group of the binary images of extended quaternary QR-codes. (cf. [1, Ch.16.Problem(16)]).

(3.4.3) Theorem: Let $(a_\infty, a(x) ; b_\infty, b(x))$ be a codeword of C. Then also

$$(b_\infty, b(x^2) ; a_\infty, a(x^2)) \text{ is in } C.$$

Furthermore, if the extra condition $h(x^{-1}) = h(x^2)$ is satisfied, then

$$(b_\infty, b(x^{-1}) ; a_\infty, a(x^{-1})) \text{ is also in } C.$$

Proof: Let $(a_\infty, a(x) ; b_\infty, b(x)) \in C$. Then by Lemma (3.4.2)

$$(3.4.4) \qquad b(x^2) = a(x^2)h(x^2) + (b_\infty + a_\infty h(1))j(x^2) =$$
$$= a(x^2)h^2(x) + (b_\infty + a_\infty h(1))j(x).$$

From Lemma (3.4.2) it easily follows that

$$(b_\infty, b(x^2) ; a_\infty, a(x^2)) \in C \text{ iff } a(x^2) = b(x^2)h(x) + (a_\infty + b_\infty h(1))j(x).$$

This is true, since by (3.4.4)

$$\begin{aligned} b(x^2)h(x) + (a_\infty + b_\infty h(1))j(x) &= \\ &= a(x^2)h^3(x) + (b_\infty + a_\infty h(1))h(1)j(x) + (a_\infty + b_\infty h(1))j(x) = \\ &= a(x^2) + a(1)(1 + h(1))j(x) + a_\infty(h^2(1) + 1)j(x) = \\ &= a(x^2). \end{aligned}$$

The second assertion can be proved in the same way. □

(3.4.5) Corollary: Let $(a_\infty, a_0, \ldots, a_{n-1} ; b_\infty, b_0, \ldots, b_{n-1}) \in C$. Then also

$$\begin{aligned} &(b_\infty, b_0, b_{\frac{1}{2}(n+1)}, b_1, b_{\frac{1}{2}(n+3)}, b_2, \ldots, b_{n-1}, b_{\frac{1}{2}(n-1)} ; \\ &a_\infty, a_0, a_{\frac{1}{2}(n+1)}, a_1, a_{\frac{1}{2}(n+3)}, \ldots, a_{n-1}, a_{\frac{1}{2}(n-1)}) \in C. \end{aligned}$$

Furthermore if the extra condition $h(x^{-1}) = h(x^2)$ is satisfied, then also

$$(b_\infty, b_0, b_{n-1}, b_{n-2}, \ldots, b_1 ; a_\infty, a_0, a_{n-1}, \ldots, a_1) \in C.$$

Proof: Let $b(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$. Then

$$\begin{aligned} b(x^2) &= b_0 + b_1x^2 + \ldots + b_{n-1}x^{2(n-1)} \mod (x^n - 1) \\ &= b_0 + b_{\frac{1}{2}(n+1)}x + b_1x^2 + b_{\frac{1}{2}(n+3)}x^3 + b_2x^4 + \ldots + \\ &\quad + b_{n-1}x^{n-2} + b_{\frac{1}{2}(n-1)}x^{n-1}. \end{aligned}$$

and

$$b(x^{-1}) = b_0 + b_{n-1}x + b_{n-2}x^2 + \ldots + b_1x^{n-1}.$$ □

(3.4.6) Lemma: Let T be the permutation of the elements of the set $\{\infty, 0, 1, \ldots, n-1\}$ defined by: $T\infty = \infty$; $Ts = s + 1 \mod n$, $0 \le s \le n - 1$.
If $(L ; R)$ is a codeword in C then also $(T(L) ; T(R))$ is an element of C.

Proof: by observation. □

In case C is the binary image of an extended quaternary QR-code of length n + 1, where n is a prime of the form n = 8k ± 3, the code C has a large automorphism group, as stated in the following theorem (cf. [1, Ch.16.Problem(16)]).

(3.4.7) Theorem: Let n be a prime of the form n = 8k ± 3. Let C be the [2(n+1), n+1] double circulant code which is the binary image of an [n+1, ½(n+1)] extended quaternary QR-code. Then the automorphism group of C, Aut(C), contains PSL(2,n) applied simultaneously to both sides of the codewords of C, i.e. for all codewords (L ; R) in C and for any element T in PSL(2,n), (T(L) ; T(R)) is an element of C.

Proof: By the Theorem of Gleason and Prange (cf. Theorem (2.2.7)) the automorphism group of the [n+1, ½(n+1)] extended quaternary QR-code contains a subgroup isomorphic to PSL(2,n). Due to our choice of the mapping, which sends codewords of the (n + 1)-dimensional vectorspace over GF(4) into codewords of the 2(n + 1)-dimensional vectorspace over GF(2) (cf. Definition (3.2.1)), the theorem easily follows. □

3.4.3. The dual code of C

In this subsection we shall prove that the double circulant code C is equivalent with its dual $C^{\perp}$. To show this we need several lemmas.

(3.4.8) Lemma: Let ($\underline{a}$; $\underline{b}$) be a codeword in C. Here $\underline{a}$ and $\underline{b}$ are both vectors of length n + 1. Then also ($\underline{a}$ + $\underline{b}$; $\underline{a}$) and ($\underline{b}$; $\underline{a}$ + $\underline{b}$) are elements of C.

Proof: Since ($\underline{a}$; $\underline{b}$) $\in C$, it follows that $\underline{a} + \omega\underline{b} \in \overline{D}$. Thus also $\omega(\underline{a} + \omega\underline{b}) \in \overline{D}$ and $\omega^2(\underline{a} + \omega\underline{b}) \in \overline{D}$. The binary images of these two vectors are ($\underline{b}$; $\underline{a}$ + $\underline{b}$) and respectively ($\underline{a}$ + $\underline{b}$; $\underline{a}$). Hence the lemma is proved. □

(3.4.9) Corollary: The [2(n+1), n+1] binary double circulant codes C_0, C_1 and C_2 with generator matrices G_0, G_1 and G_2 respectively, defined by

$$G_0 = \left[\begin{array}{c|c|c|c} 0 & 0 \ldots 0 & 1 & 1 \ldots 1 \\ \hline 1 & & h(1) & \\ \vdots & I & \vdots & H \\ 1 & & h(1) & \end{array}\right], \quad G_1 = \left[\begin{array}{c|c|c|c} 0 & 0 \ldots 0 & 1 & 1 \ldots 1 \\ \hline 1 & & h(1)+1 & \\ \vdots & I & \vdots & H+I \\ 1 & & h(1)+1 & \end{array}\right],$$

$$G_2 = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & h(1) & & & \\ \vdots & & I & & \vdots & & H^2 & \\ 1 & & & & h(1) & & & \end{array}\right]$$

are equivalent.

Proof: (i) By Lemma (3.4.8) the codes C_0 and C_1 are equivalent.

(ii) The codes C_1 and C_2 are the same, for $H^2 = H + I + J$, so that adding up the first row of G_1 to all other rows of G_1 yields the matrix G_2. □

(3.4.10) Lemma: Let A be an n×n circulant matrix with toprow a(x), $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$. Furthermore let S be the n×n permutation matrix defined by

$$S = \begin{bmatrix} & & & 1 \\ & & \cdot & \\ & \cdot & & \\ \cdot & & & \\ 1 & & & \end{bmatrix} .$$

Then $SAS = A^T$.

Proof: This lemma can be proved by straightforward calculation. □

Now we are able to prove the following theorems.

(3.4.11) Theorem: The [2(n+1), n+1] double circulant code C is equivalent with its dual $C^\perp$.

Proof: The generator matrix of C is given by (3.4.1). It can easily be verified that the generator matrix $G^\perp$ of the dual code $C^\perp$ is given by

(3.4.12) $$G^\perp = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline 1 & & & & h(1) & & & \\ \vdots & & I & & \vdots & & (H^2)^T & \\ 1 & & & & h(1) & & & \end{array}\right] .$$

Because of Corollary (3.4.9) if suffices to prove that there exist permutation matices P and Q such that $PG^{\perp}Q = G_2$, where G_2 is the matrix as defined in Corollary (3.4.9). Let S be the n×n permutation matrix as defined in Lemma (3.4.10). Furthermorelet P and Q be permutations matrices defined by

$$P = \left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & S & \\ 0 & & & \end{array}\right], \qquad Q = \left[\begin{array}{c|c} P & O \\ \hline O & P \end{array}\right],$$

where O is the (n+1)×(n+1) zero-matrix. Then by Lemma (3.4.10) it is straightforward to check that P and Q satisfy $PG^{\perp}Q = G_2$. □

(3.4.13) Theorem: If the extra condition $h^2(x) = h(x^{-1})$ is satisfied, then the [2(n+1), n+1] double circulant code C is self-dual.

Proof: The toprow of the matrix H^T is given by

$$h^T(x) = h_0 + h_{n-1}x + h_{n-2}x^2 + \ldots + h_1x^{n-1},$$

i.e.

$$h^T(x) = h(x^{-1}).$$

Thus if the extra condition $h^2(x) = h(x^{-1})$ is satisfied, then $H^2 = H^T$, i.e. $(H^2)^T = H$. Hence the theorem follows from (3.4.12). □

For the extended cyclic code $\overline{D}$ over GF(4) we can prove an analogous theorem.

(3.4.14) Theorem: Let D be the cyclic quaternary code of length n generated by $g(x) = 1 + \omega h(x)$, where h(x) satisfies both $h^2(x) + h(x) + 1 = j(x)$ and $h^2(x) = h(x^{-1})$. Then the extended code $\overline{D}$ is self-dual.

Proof: Obviously the rows of the matrix $G_{\overline{D}}$ defined by

$$G_{\overline{D}} = \left[\begin{array}{c|c} 1 + \omega h(1) & \\ \vdots & I + \omega H \\ 1 + \omega h(1) & \end{array}\right],$$

span the extended code $\overline{D}$.

Since $h^2(x) = h(x^{-1})$, the matrix H satisfies $H^2 = H^T$. Hence

$$G_{\overline{D}}G_{\overline{D}}^T = (1 + \omega h(1))^2 J + (I + \omega H)(I + \omega H^T) =$$
$$= I + (1 + h(1))J + H^3 + \omega(H + H^2 + H^3 + h(1)J) = O$$

(cf. Lemma (3.2.19)). Since $\overline{D}$ has dimension $\frac{1}{2}(n + 1)$, the theorem is proved. □

3.5. A square root bound for the minimum weight of the binary images of extended quaternary QR-codes

Let n be a prime of the form $n = 8k \pm 3$ and let Q be the set consisting of all quadratic residues mod n. The $[n, \frac{1}{2}(n+1)]$ quaternary QR-code will be denoted by E. We have already shown that this code E is also generated by $g(x) = 1 + \omega h(x)$, where $h(x) = \sum_{i \in Q} x^i$ (cf. Corollary (3.3.7)). The polynomial h(x) defined in this way satisfies $h^2(x) + h(x) + 1 = j(x)$, so that the binary image of the extended code $\overline{E}$ is a $[2(n+1), n+1]$ double circulant code B.
In this section we shall mention without proof a square root bound on the minimum weight of the double circulant code B (cf. [16]). Furthermore we shall give a list of known examples of these double circulant codes and compare their minimum distance with the lower bound which we can find using the square root bound.

We have already shown that the code B has a large automorphism group. Using theorems analogous to Theorem (3.4.3) and Theorem (3.4.7) on the automorphism group of B, Calderbank has established a square root bound for the minimum weight of the code B in case n is a prime of the form $n = 8k + 3$ (cf. [16]). Using his paper we have proved, in the same way, a square root bound for the minimum weight of the code B in case n is a prime of the form $n = 8k - 3$.

(3.5.1) Theorem: Let B be the $[2(n+1), n+1]$ double circulant code which is the binary image of the extended $[n+1, \frac{1}{2}(n+1)]$ quaternary QR-code. Here n is a prime of the form $n = 8k \pm 3$. Then the minimum weight d of the code B satisfies

(i) $(d - 1)^2 - (d - 1) + 1 \geq 2n + 1$ if $n = 8k + 3$,

(ii) $(d - 1)^2 \geq 2n - 1$ if $n = 8k - 3$.

In (i) equality holds iff n = 3 and d = 4. □

For the proof of this theorem we refer to [16]. It is true that in [16] only the first statement of this theorem is proved, but using the theorems of [16] the second statement can analogously be proved. Further in §4.6 an analogous theorem on the minimum weight of the ternary images of extended QR-codes over GF(9) will be completely proved. The proof of that theorem is almost the same as the proof of Theorem (3.5.1). Therefore we may also refer to §4.6.

(3.5.2) Remark: Theorem (3.5.1) answers [1, Research problem (16.7)] .

A lemma which we can use very well when we want to determine the minimum weight of the [2(n+1), n+1] double circulant code B, in case n is a prime of the form n = 8k + 3, is the following.

(3.5.3) Lemma: Let n be a prime of the form n = 8k + 3. Let B_0 be the [2(n+1), n+1] double circulant code which is the binary image of the extended [n+1, ½(n+1)] quaternary QR-code $\overline{E}_0$. Then

(i) B_0 is self-dual,

(ii) all weights of B_0 are divisible by 4.

Proof: (i) The code E_0 is generated by g(x) = 1 + ωh(x), where $h(x) = \sum_{i \in Q} x^i$ and Q is the set consisting of all residues mod n. Since n is a prime of the form n = 8k + 3, both 2 and -1 are nonresidues mod n, so that $h^2(x) = h(x^{-1})$. Hence by Theorem (3.4.13) B_0 is self-dual.

(ii) All weights of the rows of the generator matrix of B_0 are divisble by 4. Hence all weights of B_0 are divisible by 4. For let $\underline{c}_1$ and $\underline{c}_2$ be two codewords in B_0 which satisfy $w_H(c_1) \equiv w_H(c_2) \equiv 0 \bmod 4$. Without loss of generality we may assume

$$\underline{c}_1 : 1 \ldots 1\ 1 \ldots 1\ 0 \ldots 0\ 0 \ldots 0$$

$$\underline{c}_2 : \underbrace{1 \ldots 1}_{p}\ \underbrace{0 \ldots 0}_{q}\ \underbrace{1 \ldots 1}_{r}\ \underbrace{0 \ldots 0}_{s}$$

Then for the parameters p, q, and r we find the following relations:

$$p + q \equiv 0 \bmod 4, \quad p + r \equiv 0 \bmod 4 \quad \text{and} \quad p = (c_1, c_2) \equiv 0 \bmod 2.$$

Hence

$$2p + q + r \equiv 0 \bmod 4.$$

Since $2p \equiv 0 \bmod 4$, we find $q + r \equiv 0 \bmod 4$. Thus $w_H(\underline{c}_1 + \underline{c}_2) \equiv 0 \bmod 4$. So we have proved that all weights of B_0 are divisible by 4 (by induction). □

(3.5.4) Examples: From [17] we have taken a list of the minimum distances of the [2(n+1), n+1] double circulant codes which are the binary images of extended quaternary QR-codes, up to n = 59. Here n has to be a prime of the form $n = 8k \pm 3$. We shall compare these examples with the lower bounds which we have found using Theorems (3.5.1) and (3.5.3).

n	minimum weight of the [2(n+1), n+1] code B	a lower bound on the minimum weight of B
3	4	4
5	4	4
11	8	8
13	8	6
19	8	8
29	12	10
37	12	10
43	16	12
53	$\leq$ 18	12
59	$\leq$ 16	16

From these examples it follows that the square root bound (3.5.1) in combination with Theorem (3.5.3) yields a good lower bound on the minimum weight of the [2(n+1), n+1] double circulant codes B, certainly in case n is a prime of the form $n = 8k + 3$.

3.6. Notes on chapter 3

Using the computer we have determined the minimum weights of all [2(n+1), n+1] double circulant codes which are the binary images of extended quaternary cyclic codes of length n + 1, up to n = 45. These results are shown in Appendix A. A description of the computer program can be found in Appendix C.

From the theory, which we have derived in this chapter, and from the computer results it follows that the binary images of the extended quaternary QR-codes are the most interesting codes. These codes have a good minimum weight and a large automorphism group. Furthermore they admit a square root bound for the minimum weight (Theorem (3.5.1)) comparable with the square root bound for the minimum weight of QR-codes. In case n is a prime of the form $n = 8k + 3$, the first four examples, which have parameters [8,4,4], [24,12,8], [40,20,8] and respectively [88,44,16], all have the greatest possible minimum distance for self-dual codes over GF(2) with weights divisible by 4 (cf. Theorem of Mallows and Sloane [1, Ch.19.Th.17]). Unfortunately the next example, the [120,60,16] - code (cf. Examples (3.5.4)) does not have this property.

In [16] Calderbank has established in fact a square root bound on the minimum weight of the binary images of extended generalized QR-codes (cf. [19]) over GF(4) of length $q + 1$, where q is a prime power, $q \equiv 3 \bmod 8$. In this way he has also found a [56,28,12] binary self-dual code with weights divisible by 4. Also this code has the greatest possible minimum distance. We did not discuss this theorem in general, since in the case where q is not a prime the corresponding matrix H is not really a circulant matrix. For the details we refer to [16].

We have also applied the Assmus-Mattson Theorem (cf. Theorem (1.3.3)) on the computer results in order to find t-designs. The only t-designs, $t \geq 2$, which we have found in this way, are the well known t-designs which are contained in the [8,4,4] extended Hamming-code and the [24,12,8] binary Golay code.

4. Extended cyclic codes over GF(9) and their ternary images

4.1. Introduction

In chapter 3 we have found double circulant codes by looking at the binary images of extended cyclic codes over GF(4). It appeared that this class of codes contains a class of good double circulant codes, namely the class consisting of the binary images of extended quaternary QR-codes.
Inspired by the results of chapter 3 we have also analysed the class of double circulant codes which are the ternary images of extended cyclic codes over GF(9), hoping to find a class of good ternary double circulant codes. As far as we know this class of double circulant codes which are the ternary images of extended cyclic codes over GF(9) is completely new. It will appear that many results of this chapter can be found by generalizing the theorems of chapter 3. The first part of this chapter is almost the same as the corresponding part of chapter 3.
In §4.2 a necessary and sufficient condition in order that the ternary images of extended cyclic codes over GF(9) are double circulant codes will be derived (cf. Theorem (4.2.7)). Furthermore also in this case it will appear that the double circulant codes which have a generator matrix of the form $G = [\ I \mid A\ ]$, A a circulant matrix, can not be the ternary images of cyclic codes over GF(9).
In §4.3 we shall develop some theory on the cyclic codes over GF(9), e.g. the idempotent will be given and a square root bound on the minimum weight will be established.
In §4.4 some theory on the corresponding ternary images will be discussed, e.g. some theorems on the automorphism group and the dual code will be proved.
In §4.5 it will be shown that the ternary images of extended QR-codes over GF(9) of length n + 1 are double circulant codes, provided that n is a prime of the form $n = 12k \pm 5$. The subclass consisting of the ternary images of QR-codes will be analysed very thoroughly. In §4.5 it will appear that these [2(n+1), n+1] ternary double circulant codes, in case n is a prime of the form $n = 12k - 5$, have a generator matrix $G = [\ I \mid S\ ]$, where S is a Hadamrd matrix of the Paley type. For these codes a theorem on the minimum weight, analogous to Theorem (2.3.5) will be proved (cf. Theorem (4.5.20)). As a direct result we have found ternary self-dual codes, with parameters [16,8,6], [40,20,12], and [64,32,18], which meet the bound on the minimum weight of self-dual codes (cf.[1,Ch.19.Th.17]). Applying the Assmus-Mattson Theorem on these codes we have found 3-designs which are also

discussed in §4.5. The codes with parameters [16,8,6] and [40,20,12] were already known (cf. [1, Ch.19.§6]). The [64,32,18] code is in all propability new. As far as we know this code is the largest known (with respect to the wordlength) ternary self-dual code which meets the above mentioned bound. The designs which are contained in this code are propably also new.
In §4.6 a square root bound on the minimum weight of the ternary images of extended QR-codes over GF(9) is established.
In §4.7 the relation between symmetry codes and the ternary images of extended QR-codes over GF(9) will be described.
Using the computer the minimum weights of all [2(n+1), n+1] double circulant codes which are the ternary images of extended cyclic codes over GF(9), have been calculated, up to n = 35. These results are reported in Appendix B.

4.2. General theory

4.2.1. A necessary and sufficient condition

In this subsection we shall derive, analogously to §3.2.1, a necessary and sufficient condition for a double circulant code to be the ternary image of an extended cyclic code over GF(9).
First of all we have to construct GF(9). It is easily seen that the polynomial p(x), defined by

$$p(x) := x^2 + x + 2, \tag{4.2.1}$$

is a primitive polynomial over GF(3). Let α be a primitive element of GF(9) which is a zero of p(x). Then every element of GF(9) can be uniquely written as a power of α. In Fig. 4.1 the elements of GF(9) are shown.
Any vector of the n-dimensional vectorspace over GF(9) can be uniquely represented as $(a_1 + \alpha b_1, a_2 + \alpha b_2, \ldots, a_n + \alpha b_n)$, where $a_i, b_i \in GF(3)$.

(4.2.2) Definition: Let $(a_1 + \alpha b_1, a_2 + \alpha b_2, \ldots, a_n + \alpha b_n)$ be a vector of length n over GF(9), where $a_i, b_i \in GF(3)$. Then the ternary image of this vector is defined to be

$$(a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n).$$

as a 2-tuple	as a polynomial	as a power of α
00	0	0
10	1	1
01	α	α
12	$1 + 2\alpha$	α^2
22	$2 + 2\alpha$	α^3
20	2	α^4
02	2α	α^5
21	$2 + \alpha$	α^6
11	$1 + \alpha$	α^7

Fig.4.1. GF(9).

(4.2.3) Remark: The mapping defined in this way sends [n, k] -codes over GF(9), in a one-to-one way, onto [2n, 2k] ternary codes.

(4.2.4) Remark: The elements of GF(3) will be taken from either {-1, 0, 1} or {0, 1, 2}, depending on which form is more convenient at that moment.

Double circulant codes which have a generator matrix of the form G = [I | A] can not be the ternary images of cyclic codes over GF(9), as we shall show in the next theorem.

(4.2.5) Theorem: Let C be a [2n, n] double circulant code over GF(3) with generator matrix G = [I | H], where H is an n×n circulant matrix with toprow h(x). Then C can not be the ternary image of a cyclic code D over GF(9).

Proof: If G is the generator of the ternary image of the code D, then $1 + \alpha h(x)$ has to be an element of D. Hence also $(a(x) + \alpha)(1 + \alpha h(x)) \in D$, where a(x) is a polynomial of degree $\leq n - 1$ in GF(3)[x]. The ternary image of this codeword is

$$(a(x) + h(x) \; ; \; a(x)h(x) + 1 + 2h(x)).$$

This word has to be an element of the code generated by G, i.e.

$$(a(x) + h(x))h(x) = a(x)h(x) + 1 + 2h(x).$$

This is equivalent with

$$h^2(x) + h(x) + 2 = 0.$$

Substituting $x = 1$ in this equation yields $h^2(1) + h(1) + 2 \equiv 0 \bmod 3$. This is impossible, since $h(1) \in GF(3)$. □

Since we want to consider cyclic codes over GF(9), the ternary images of which are double circulant codes, the only cyclic codes over GF(9), we have to study, are the codes generated by a polynomial $g(x)$ of the form $g(x) = 1 + \alpha h(x)$. Just as in chapter 3 we do not require $g(x)$ to be a factor of $x^n - 1$.

(4.2.6) Lemma: Let C be the [2n, n+1] ternary code with generator matrix

$$G_0 = \left[\begin{array}{c|c} \underline{0 \ . \ . \ . \ 0} & \underline{1 \ . \ . \ . \ 1} \\ I & H \end{array}\right],$$

where H is an n×n circulant matrix with toprow $h(x)$. If the polynomial $h(x)$ satisfies the equation

$$h^2(x) + h(x) + 2 = \varepsilon j(x),$$

where ε may be taken to be 1 or -1, then the code C is the ternary image of the cyclic code of length n over GF(9) generated by $g(x) = 1 + \alpha h(x)$.

Proof: Analogous to the proof of Lemma (3.2.6). □

Just as in the binary case the code generated by G_0, defined in Lemma (4.2.6), is not really a double circulant code, since the dimension is not equal to half of the wordlength. To meet this problem, we consider also in this case the extended cyclic code $\overline{D}$ over GF(9) generated by $g(x) = 1 + \alpha h(x)$. We extend the code D in the usual way, i.e. to every codeword $(c_0, c_1, \ldots, c_{n-1}) \in D$ we add an overall parity check c_∞, say in front, $c_\infty \in GF(9)$, such that $c_\infty + c_0 + \ldots + c_{n-1} = 0$.

(4.2.7) Theorem: A necessary and sufficient condition for the ternary image of the extended cyclic code $\overline{D}$ over GF(9) of wordlength n + 1 generated by $g(x) = 1 + \alpha h(x)$, to be a $[2(n+1), n+1]$ double circulant code C is that $h(x)$ satisfies one of the following two equations

(i) $h^2(x) + h(x) + 2 = j(x)$,

(ii) $h^2(x) + h(x) + 2 = -j(x)$.

The generator matrix G of the code C is given by

$$G = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & \varepsilon & 1 & \cdots & 1 \\ \hline 2 & & & & 2h(1) & & & \\ \vdots & & I & & \vdots & & H & \\ 2 & & & & 2h(1) & & & \end{array}\right] .$$

Here H is the n×n circulant matrix with toprow h(x) and $\varepsilon = -n \bmod 3$.

Proof: Analogous to the proof of Theorem (3.2.9). □

(4.2.8) Remark: By "h(x) satisfies $h^2(x) + h(x) + 2 = \pm j(x)$" we shall mean that h(x) satisfies either $h^2(x) + h(x) + 2 = j(x)$ or $h^2(x) + h(x) + 2 = -j(x)$.

From Theorem (4.2.7) it follows that for given $n \in \mathbb{N}$ we can determine all $[2(n+1), n+1]$ double circulant codes C which are the ternary images of extended cyclic codes over GF(9) of length n + 1 generated by polynomials of the form $g(x) = 1 + \alpha h(x)$, if we know all solutions of the equation $h^2(x) + h(x) + 2 = \pm j(x)$.

4.2.2. Analysis of the equation $h^2(x) + h(x) + 2 = \pm j(x)$

In this subsection we shall consider the equation

(4.2.9) $\quad h^2(x) + h(x) + 2 = \varepsilon j(x)$,

where $\varepsilon = 1$ or -1, in more detail.

(4.2.10) Definition: We call $n \in \mathbb{N}$ feasible, if there exists a solution h(x) of equation (4.2.9).

(4.2.11) Lemma: Let $n \in \mathbb{N}$. Then

(i) n is not feasible, if $n \equiv 0 \bmod 2$ or $n \equiv 0 \bmod 3$,

(ii) n is feasible , if n is a prime of the form $n = 12k \pm 5$.

Proof: (i) Let n be even, then -1 is a zero of the polynomials $x^n - 1$ and $j(x)$. Therefore substituting $x = -1$ in (4.2.9) yields $h^2(-1) + h(-1) + 2 \equiv 0 \bmod 3$. This is impossible, since $h(-1) \in GF(3)$.
In case $n \equiv 0 \bmod 3$ substituting $x = 1$ leads to a contradiction.

(ii) The second assertion of this lemma will be proved in §4.5. □

In general,equation (4.2.9) is much harder to analyse than the corresponding equation (3.2.10) for the polynomial $h(x)$ in the binary case. This difficulty is caused by the fact that squaring in the ring $GF(3)[x]$ is much more difficult than squaring in the ring $GF(2)[x]$. To partially obviate this difficulty, we multiply (4.2.9) by $h(x) + 2$, yielding

$$h^3(x) + h(x) + 1 = \varepsilon(h(1) + 2)j(x). \tag{4.2.12}$$

This equation is much easier to solve than (4.2.9). First of all we remark that if $h(x)$ satisfies (4.2.12), then the polynomials $h_1(x)$ and $h_2(x)$, defined by $h_1(x) = h(x) + j(x)$, and $h_2(x) = h(x) + 2j(x)$, satisfy

$$h_1^3(x) + h_1(x) + 1 = (\varepsilon(h(1) + 2) + 2)j(x) ,$$

$$h_2^3(x) + h_2(x) + 1 = (\varepsilon(h(1) + 2) + 1)j(x) .$$

Therefore we may assume, without loss of generality, that the polynomial $h(x)$ is a solution of

$$h^3(x) + h(x) + 1 = j(x). \tag{4.2.13}$$

For the sake of convenience we introduce the following notation: $S = \{1, 2, \ldots, n-1\}$ and A and B are mutually disjoint subsets of S. Let $h(x)$, defined by

$$h(x) = \sum_{i \in A} x^i + 2 \sum_{j \in B} x^j, \tag{4.2.14}$$

be a solution of (4.2.13). Substituting $h(x)$ in this equation yields

$$\sum_{i \in A} x^{3i} + 2 \sum_{j \in B} x^{3j} + \sum_{i \in A} x^i + 2 \sum_{j \in B} x^j + 1 = \sum_{i=0}^{n-1} x^i .$$

It is easily verified, by comparing the coefficients of the same powers of x, that the following conditions on the sets A and B must hold:

$$B = 3B,$$
$$A,\ 3A \text{ and } B \text{ form a partition of the set } S\backslash\{0\}.$$

Here $3A = \{3a \bmod n \mid a \in A\}$.
If the sets A and B satisfy these conditions, then the function h(x), defined by (4.2.14), is a solution of equation (4.2.13). The only thing we have further to do is to check whether the polynomial h(x) also satisfies (4.2.9).
Using this analysis, we have made a computer program in order to determine for a given value of n all solutions of (4.2.13) and further to check whether these polynomials also satisfy (4.2.9).
The feasible values of n, $n \leq 100$, which we have found in this way, are shown in Fig.4.2. We do not know whether n = 91 is feasible or not. We have let the computer run for 300 seconds, but we did not find any solution.

5, 7, 17, 19, 25, 29, 31, 35, 37, 41, 49, 53, 61, 67,
73, 79, 85, 89, 91? 95, 97

Fig.4.2. Feasible values of n, $n \leq 100$

In §4.5 we shall return to equation (4.2.9) by giving solutions of this equation in case n is a prime of the form $n = 12k \pm 5$.

4.3. Some properties of the cyclic code *D* over GF(9)

In this section we shall establish, just as in §4.3, some properties of the cyclic code *D* over GF(9) generated by $g(x) = 1 + \alpha h(x)$, where h(x) satisfies $h^2(x) + h(x) + 2 = \pm j(x)$.

4.3.1. The idempotent of *D*

The idempotent of the cyclic code *D* over GF(9) can easily be expressed in terms of the polynomial h(x).

(4.3.1) Theorem: Let h(x) satisfy $h^2(x) + h(x) + 2 = \pm j(x)$. Then the idempotent F(x) of the cyclic code *D* over GF(9) generated by $g(x) = 1 + \alpha h(x)$, is given by

$$F(x) = \begin{cases} 1 + \alpha^5 h(x) + \alpha^7 h^3(x) & \text{if } h(1) = 0, \\ 1 + 2j(1)j(x) + \alpha^5 h(x) + \alpha^7 h^3(x) & \text{if } h(1) = 1, \\ \alpha^3 h(x) + \alpha h^3(x) & \text{if } h(1) = 2. \end{cases}$$

Proof: We shall prove this theorem only for the case $h(1) = 1$. The other two cases can be settled in the same way.
Let $h(1) = 1$. Then the funcion $h(x)$ satisfies

$$h^2(x) + h(x) + 2 = j(1)j(x).$$

Multiplying by $h(x) + 2$ yields

$$h^3(x) + h(x) + 1 = 0.$$

From these equations it easily follows

$$h^4(x) + 1 = 2j(1)j(x),$$

$$h^5(x) + h(x) = 2j(1)j(x),$$

$$h^6(x) + 2h(x) + 1 = j(1)j(x).$$

Using these properties and Fig.4.1 we find, if we define

$$F(x) := 1 + 2j(1)j(x) + \alpha^5 h(x) + \alpha^7 h^3(x) =$$

$$= 1 + 2\alpha^7 + (2\alpha^7 + \alpha^5)h(x) + 2j(1)j(x) =$$

$$= \alpha^5 + \alpha^6 h(x) + 2j(1)j(x)$$

that indeed

$$\text{(i)}\quad F^2(x) = \{\alpha^5 + \alpha^6 h(x) + 2j(1)j(x)\}^2 =$$

$$= \alpha^2 + \alpha^4\{2h(x) + 1 + j(1)j(x)\} + j(1)j(x) + \alpha^7 h(x) +$$

$$+ \alpha^5 j(1)j(x) + \alpha^6 j(1)j(x) = \alpha^5 + \alpha^6 h(x) + 2j(1)j(x) = F(x).$$

(ii) $F(x)(1 + \alpha h(x)) = \{\alpha^5 + \alpha^6 h(x) + 2j(1)j(x)\}\{1 + \alpha h(x)\} =$

$= \alpha^5 + \alpha^6 h(x) + 2j(1)j(x) + \alpha^6 h(x) + \alpha^7\{2h(x) + 1 +$

$+ j(1)j(x)\} + 2\alpha j(1)j(x) = 1 + \alpha h(x)$.

(iii) $F(x) = (\alpha^7 j(1)j(x) + \alpha^4 h(x))(1 + \alpha h(x))$, so that $F(x) \in D$.

From (i), (ii) and (iii) it follows that $F(x)$ is the idempotent of the code D.

□

(4.3.2) Remark: We have found this theorem, just as Theorem (3.3.3), by generalization of the formula for the idempotent of the QR-code over GF(9), (cf. [1, Ch.16.Th.4] and §4.5).

4.3.2. A square root bound on the minimum weight of D

In this subsection we shall establish, just as in §3.3, a square root bound for the minimum weight of the code D. For this purpose we introduce the code D^*. We repeat that the code D is the principal ideal in $GF(9)[x]/(x^n - 1)$ generated by $g(x) = 1 + \alpha h(x)$. Here $h(x)$ is a solution of (4.2.9) and n denotes the wordlength of D. We define D^* to be the principal ideal in $GF(9)[x]/(x^n - 1)$ generated by $g^*(x) = 1 + \alpha h^3(x)$. It is easy to verify that the polynomial $h^3(x)$ also satisfies (4.2.9), so that the ternary image of the extended code $\overline{D}^*$ is also a double circulant code.

(4.3.3) Lemma: Let D and D^* be the cyclic codes over GF(9) as defined above. Then

$$D \cap D^* = \langle j(x) \rangle,$$

where $\langle j(x) \rangle$ is the ideal in $GF(9)[x]/(x^n - 1)$ generated by $j(x)$.

Proof: Let C and C^* be the $[2(n+1), n+1]$ double circulant codes which are the ternary images of the extended codes $\overline{D}$ and $\overline{D}^*$ respectively. The generator matrices of these codes C and C^* are called G and G* respectively, i.e.

$$G = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & \delta & 1 & \cdots & 1 \\ \hline 2 & & & & 2h(1) & & & \\ \vdots & & I & & \vdots & & H & \\ 2 & & & & 2h(1) & & & \end{array}\right], \quad G^* = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & \delta & 1 & \cdots & 1 \\ \hline 2 & & & & 2h(1) & & & \\ \vdots & & I & & \vdots & & H^3 & \\ 2 & & & & 2h(1) & & & \end{array}\right],$$

where δ is chosen in such a way that $\delta + n \equiv 0 \bmod 3$.
It suffices to show that

$$C \cap C^* = \{[\underline{0},\underline{0}], \pm[\underline{0},(\delta,\underline{1})], \pm[(\delta,\underline{1}),\underline{0}], \pm[(\delta,\underline{1}),(\delta,\underline{1})]\}.$$

Here $\underline{0}$ is the 0-vector and $(\delta,\underline{1})$ is a vector of length $n + 1$ with first component equal to δ and all other components equal to 1.
Let $(a_\infty, a(x) ; b_\infty, b(x)) \in C \cap C^*$. Then there exists an element $\gamma \in GF(3)$ such that

$$b(x) = a(x)h(x) + \gamma j(x)$$

and

$$b(x) = a(x)h^3(x) + \gamma j(x),$$

namely $j(1)\gamma = b(1) + 2a(1)h(1)$. From these equations it follows

$$a(x)(h^3(x) + 2h(x)) = 0.$$

We restrict ourselves to the case $h(1) = 0$. The other two cases can be treated in the same way. In this case $h(x)$ satisfies $h^3(x) + h(x) + 1 = j(1)j(x)$, so that

$$a(x)\{h(x) + 2 + j(1)j(x)\} = 0,$$

i.e.

$$a(x)(h(x) + 2) = 2a(1)j(1)j(x).$$

Squaring both sides of this equation yields

$$a^2(x)\{h^2(x) + h(x) + 1\} = a^2(1)j(1)\ j(x)$$

i.e.

$$a^2(x)(2j(1)j(x) + 2) = a^2(1)j(1)j(x).$$

Hence

$$a^2(x) = a^2(1)j(1)j(x).$$

Multiplying both sides by $a(x)$ yields

$$a(x^3) = a^3(x) = a^3(1)j(1)j(x) = a(1)j(1)j(x^3),$$

so that

$$a(x) = a(1)j(1)j(x).$$

This proves the theorem. □

Now we are able to prove a square root bound for the minimum weight of the cyclic code D over GF(9).

(4.3.4) Theorem: Let $c(x)$ be a codeword of D, $c(1) \neq 0$. Let d be the weight of $c(x)$. Then

(i) $d^2 \geq n$,

(ii) $d^2 - d + 1 \geq n$, if $h(x)$ also satisfies $h^3(x) = h(x^{-1})$.

Proof: The proof of this theorem is completely analogous to the proof of Theorem (3.3.9). □

4.4. Some properties of the double circulant codes C which are the ternary images of extended cyclic codes D over GF(9)

4.4.1. Introduction

In this section we shall establish, just as in §3.4, some theorems on double circulant codes which are the ternary images of extended cyclic codes over GF(9). In this section let D be the cyclic code of length n over GF(9) generated by $g(x) = 1 + \alpha h(x)$, where $h(x)$ is a solution of $h^2(x) + h(x) + 2 = \pm j(x)$. The ternary image of $\overline{D}$ is a double circulant code which we denote by C. The generator matrix of C is called G, i.e.

$$(4.4.1) \qquad G = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & \delta & 1 & \cdots & 1 \\ \hline 2 & & & & 2h(1) & & & \\ \vdots & & I & & \vdots & & H & \\ 2 & & & & 2h(1) & & & \end{array}\right] .$$

Here H is the $n \times n$ circulant matrix with toprow $h(x)$ and δ is chosen such that $\delta + n \equiv 0 \bmod 3$.

We shall need the following lemma several times in this section.

(4.4.2) Lemma: Let $(a_\infty, a(x) ; b_\infty, b(x))$ be a codeword of C. Then

$$a_\infty = 2a(1) \ , \ b_\infty = 2b(1) \text{ and } b(x) = a(x)h(x) + \gamma j(x),$$

where $\gamma = j(1)^{-1}\{b(1) + 2a(1)h(1)\}$.

Proof: Let $(a_\infty, a(x) ; b_\infty, b(x)) \in C$. Then there exists a vector $(\omega_\infty, \omega(x))$ of length n + 1 such that

$$(\omega_\infty, \omega(x))G = (a_\infty, a(x) ; b_\infty, b(x)),$$

i.e.

$$a_\infty = 2\omega(1),\ a(x) = \omega(x),\ b_\infty = \delta\omega_\infty + 2\omega(1)h(1),\ b(x) = \omega(x) + \omega_\infty j(x).$$

From these relations the lemma easily follows. □

4.4.2. On the automorphism group of C

In this subsection we shall derive, just as in §3.4, some theorems on the automorphism group of C.

(4.4.3) Theorem: Let $(a_\infty, a(x) ; b_\infty, b(x))$ be a codeword of C. Then also

$$(b_\infty, b(x^3) ; 2a_\infty, 2a(x^3)) \in C.$$

Further if the extra condition, $h^3(x) = h(x^{-1})$, is met, then

$$(b_\infty, b(x^{-1}) ; 2a_\infty, 2a(x^{-1}))$$

is also an element of C.

Proof: Let $(a_\infty, a(x) ; b_\infty, b(x)) \in C$. Then by Lemma (4.4.2)

$$(4.4.4) \qquad b(x^3) = a(x^3)h(x^3) + \gamma j(x^3) = a(x^3)h^3(x) + \gamma j(x).$$

We restrict ourselves to the case $h(1) = 1$. In the other two cases the proof goes along the same lines. In this case $h^4(x) = 2 + 2j(1)j(x)$. Hence

$$b(x^3)h(x) = a(x^3)h^4(x) + \gamma j(x) =$$

$$= 2a(x^3) + (\gamma + 2a(1)j(1))j(x),$$

so that

$$2a(x^3) = b(x^3)h(x) + 2(\gamma + 2a(1)j(1))j(x).$$

From this relation and Lemma (4.4.2) it follows that

$$(b_\infty, b(x^3) ; 2a_\infty, 2a(x^3)) \in C.$$

The second statement can be proved in exactly the same way. □

(4.4.5) Theorem: Let T be the permutation of the elements of the set $S = \{\infty, 0, 1, \ldots, n-1\}$ defined by $T\infty := \infty$; $Ti := i + 1 \bmod n$ for all $i \in \{0, 1, \ldots, n-1\}$. Let (L ; R) be an element of C. Then (T(L) ; T(R)) is also an element of C.

Proof: By observation. □

The theorem, analogous to Theorem (3.4.7), on the automorphism group of the ternary images of extended QR-codes over GF(9) will be proved in §4.5 (cf. Theorem (4.5.18)).

4.4.3. The dual code of C

In this subsection we shall show that the double circulant code C is equivalent with its dual $C^\perp$.
The dual of the ternary double circulant code C can easily be determined. The generator matrix G of the code C is given by (4.4.1). Using the fact that $h^4(x) = 2 + (h(1) + 1)j(1)j(x)$, it is straightforward to check that the generator matrix $G^\perp$ of the dual code is given by

$$(4.4.5) \qquad G^\perp = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \ldots & 0 & 1 & 1 & \ldots & 1 \\ \hline \eta & & & & \eta h(1) & & & \\ \vdots & & I & & \vdots & & (H^3)^T & \\ \eta & & & & \eta h(1) & & & \end{array}\right],$$

where $\eta \in GF(3)$ such that $\eta \equiv n \bmod 3$.
Using this representation of the dual code $C^\perp$ we can prove the following theorem.

(4.4.6) Theorem: The $[2(n+1), n+1]$ ternary double circulant code C, the generator matrix of which is defined by (4.4.1), is equivalent with its dual $C^\perp$.

Proof: The generator matrix of $C^\perp$ is given by (4.4.5). Using Lemma (3.4.10) it is easily shown that the code $C^\perp$ is equivalent with the code C_0 generated by

$$G_0 = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \cdots & 0 & \delta & 1 & \cdots & 1 \\ \hline 2 & & & & 2h(1) & & & \\ \vdots & & I & & \vdots & & H^3 & \\ 2 & & & & 2h(1) & & & \end{array}\right],$$

where δ satisfies $\delta + n \equiv 0 \bmod 3$.
Since $\gcd(3,n) = 1$ and $h^3(x) = h(x^3)$, the following relation obviously holds

$$(a_\infty, a(x) ; b_\infty, b(x)) \in C \Leftrightarrow (a_\infty, a(x^3) ; b_\infty, b(x^3)) \in C_0.$$

Let P be the permutation of the elements of the set $\{\infty, 0, 1, \ldots, n-1\}$ defined by $P\infty := \infty$, $Pi := 3i \bmod n$, $0 \le i \le n-1$. Then $(L ; R)$ is a codeword of C implies that $(P(L) ; P(R))$ is a codeword of C_0. Therefore the permutation P applied simultaneously to both sides of the codewords of C, changes the code C into C_0. Since we already have shown that C_0 is equivalent with $C^\perp$, the proof of this theorem is finished. □

(4.4.7) Theorem: If $n \equiv 2 \bmod 3$ and the polynomial $h(x)$ satisfies the extra condition $h^3(x) = h(x^{-1})$ then the ternary code C is self-dual.

Proof: Since $h(x^{-1}) = h^T(x)$, the condition $h^3(x) = h(x^{-1})$ is equivalent with $(H^3)^T = H$. Hence the theorem follows immediately from (4.4.5). □

4.5. Extended QR-codes over GF(9) and their ternary images

4.5.1. Introduction

In the previous chapter we have seen that the binary images of extended quaternary QR-codes of length n + 1, where n is a prime of the form $n = 8k \pm 3$, are double circulant codes. It appeared that these double circulant codes are rich in structure. For instance they have a large automorphism group, they allow a square root bound for their minimum distance comparable with the square root bound for the minimum distance of QR-codes, and their minimum weights are high.
In this section we shall show that the ternary images of extended QR-codes over GF(9) of length n + 1, where n is a prime of the form $n = 12k \pm 5$, are double circulant codes which also have a nice structure.
We want to point out one number-theoretical resemblance between these two classes

of codes. In the binary case the wordlength of the corresponding quaternary QR-code has to be a prime of the form $n = 8k \pm 3$, i.e. 2 is a nonresidue mod n. In the ternary case the wordlength has to be a prime of the form $n = 12k \pm 5$. In this case 3 is a nonresidue mod n. This latest statement follows from the next theorem.

(4.5.1) Theorem: Let n be a prime. Then 3 is a quadratic residue mod n iff $n \equiv \pm 1 \bmod 12$. □

For the proof of this theorem we refer to [1, Ch.16.Problem(25)]. We shall use this theorem several times in the rest of this chapter.

4.5.2. An explicit form of the solution of (4.2.9), in case n is a prime of the form $n = 12k \pm 5$

The analysis of the equation $h^2(x) + h(x) + 2 = \pm j(x)$, as described in §4.2 is not satisfactory. The only method we have indicated in that section was completely based on a computer search. We did not succeed in finding an explicit form of the polynomial h(x). However, when n is a prime of the form $n = 12k \pm 5$, we can indeed derive such an explicit form. It will appear that the resulting double circulant codes are the ternary images of extended QR-codes over GF(9). The determination of the polynomial h(x) is based on the following theorem of Perron which we shall mention without proof (cf. [1, Ch.16.Th.24]).

(4.5.2) Theorem: (i) Suppose p is a prime, $p = 4k - 1$. Let $r_1, \ldots, r_{2k}$ be the 2k quadratic residues mod p together with 0, and let a be a number relatively prime to p. Then among the 2k numbers $r_i + a$ there are k residues (possibly including 0) and k nonresidues.

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

(iii) Suppose p is a prime, $p = 4k + 1$. Among the $2k + 1$ numbers $r_i + a$ are, if a is itself a residue, $k + 1$ residues (including 0) and k nonresidues; and, if a is a nonresidue, k residues (not including 0) and $k + 1$ nonresidues.

(iv) Suppose p is a prime, $p = 4k + 1$. Among the 2k numbers $n_i + a$ are, if a is itself a residue, k residues (not including 0) and k nonresidues; and, if a is a nonresidue, $k + 1$ residues (including 0) and $k - 1$ nonresidues. □

Using this theorem, it is easy to prove the following theorem.

(4.5.3) Theorem: Let p be a prime, Q the set of all residues mod p and N the set of all nonresidues. Then in the polynomial ring $\mathbb{Z}[x]/(x^p - 1)$ the following relations hold:

(i) if p is of the form p = 4k - 1

$$\Big(\sum_{r\in Q} x^r\Big)^2 = \tfrac{1}{4}(p-3)\sum_{r\in Q} x^r + \tfrac{1}{4}(p+1)\sum_{s\in N} x^s ,$$

$$\Big(\sum_{s\in N} x^s\Big)^2 = \tfrac{1}{4}(p+1)\sum_{r\in Q} x^r + \tfrac{1}{4}(p-3)\sum_{s\in N} x^s ,$$

$$\Big(\sum_{r\in Q} x^r\Big)\Big(\sum_{s\in N} x^s\Big) = \tfrac{1}{4}(p-3)j(x) + \tfrac{1}{4}(p+1) ,$$

(ii) if p is of the form p = 4k + 1

$$\Big(\sum_{r\in Q} x^r\Big)^2 = \tfrac{1}{4}(p-5)\sum_{r\in Q} x^r + \tfrac{1}{4}(p-1)\sum_{s\in N} x^s + \tfrac{1}{2}(p-1) ,$$

$$\Big(\sum_{s\in N} x^s\Big)^2 = \tfrac{1}{4}(p-1)\sum_{r\in Q} x^r + \tfrac{1}{4}(p-5)\sum_{s\in N} x^s + \tfrac{1}{2}(p-1) ,$$

$$\Big(\sum_{r\in Q} x^r\Big)\Big(\sum_{s\in N} x^s\Big) = \tfrac{1}{4}(p-1)j(x) - \tfrac{1}{4}(p-1).$$

Proof: (i) cf. [1, Ch.16.Lemma 5].

(ii) Let p be a prime of the form p = 4k + 1. Using Theorem (4.5.2) we find

$$\Big(\sum_{r\in Q} x^r\Big)^2 = \sum_{r_1\in Q}\sum_{r_2\in Q} x^{r_1+r_2} = (k-1)\sum_{r\in Q} x^r + k\sum_{s\in N} x^s + 2k$$

$$= \tfrac{1}{4}(p-5)\sum_{r\in Q} x^r + \tfrac{1}{4}(p-1)\sum_{s\in N} x^s + \tfrac{1}{2}(p-1).$$

The other two cases can be settled in the same way. □

(4.5.4) Corollary: Let n be a prime of the form $n = 12k \pm 5$. Let Q be the set of all quadratic residues mod n and N the set of all nonresidues. Then the functions $h_1(x)$ and $h_2(x)$, defined by

$$h_1(x) := \sum_{s\in N} x^s \quad , \quad h_2(x) := \sum_{r\in Q} x^r$$

satisfy

$$h^2(x) + h(x) + 2 = \pm j(x).$$

Proof: Let $n = 12k - 5$. Then in $GF(3)[x]/(x^n - 1)$

$$\Big(\sum_{s\in N} x^s\Big)^2 = 2\sum_{r\in Q} x^r + \sum_{s\in N} x^s \quad ,$$

so that

$$\Big(\sum_{s\in N} x^s\Big)^2 + \sum_{s\in N} x^s + 2 = 2j(x).$$

Let $n = 12k + 5$. Then in $GF(3)[x]/(x^n - 1)$

$$\Big(\sum_{s\in N} x^s\Big)^2 = \sum_{r\in Q} x^r + 2 \, ,$$

so that

$$\Big(\sum_{s\in N} x^s\Big)^2 + \sum_{s\in N} x^s + 2 = j(x).$$

The statement on $h_2(x)$ follows in the same way. □

As expressed in this corollary we have now found an explicit form of the polynomial $h(x)$ satisfying $h^2(x) + h(x) + 2 = \pm j(x)$, in case n is a prime of the form $n = 12k \pm 5$.

4.5.3. A double circulant representation of the ternary images of extended QR-codes over GF(9)

In this subsection let n be a prime of the form $n = 12k \pm 5$. The set of all residues mod n will be denoted by Q and the set of all nonresidues by N. We shall show that the $[n, \frac{1}{2}(n+1)]$ QR-code over GF(9) also is generated by $g(x) = 1 + \alpha h(x)$, where $h(x) = \sum_{s\in N} x^s$. Then because of Corollary (4.5.4) we have proved that the ternary image of the extended QR-code is a double circulant code. For this purpose we need the following theorem (cf. [1, Ch.16.Th.4]).

(4.5.5) Theorem: Let D be the QR-code over GF(9) of length n with generator

polynomial $\gamma(x) = \prod_{r\in Q} (x - \beta^r)$, where β is a suitably chosen primitive n-th root of unity in some extension field of GF(9). Then the idempotent of D is given by

$$F(x) = \begin{cases} 1 + \alpha^7 \sum_{r\in Q} x^r + \alpha^5 \sum_{s\in N} x^s & , \text{ if } n = 12k - 5, \\ \alpha \sum_{r\in Q} x^r + \alpha^3 \sum_{s\in N} x^s & , \text{ if } n = 12k + 5. \end{cases}$$

Proof: We restrict ourselves to the case $n = 12k - 5$. The other case can be treated in the same way.

(i) $F^2(x) = F(x)$ (by Theorem (4.5.3)).

(ii) Let $r\in Q$. Since the sets Q and N are closed under multiplication by r, we find $F(\beta^r) = F(\beta)$. Since $F^2(\beta) = F(\beta)$, $F(\beta)$ can only take the values 0 or 1. Let us choose β such that $F(\beta) = 0$. Then

$$\forall_{r\in Q} [\, F(\beta^r) = 0 \,] .$$

Let $s\in N$. Then

$$F(\beta^s) = 1 + \alpha^7 \sum_{s\in N} \beta^s + \alpha^5 \sum_{r\in Q} \beta^r = 1 + \alpha^7 (j(\beta) + 2 + 2 \sum_{r\in Q} \beta^r) +$$
$$+ \alpha^5 \sum_{r\in Q} \beta^r = \alpha^5 + \alpha^6 \sum_{r\in Q} \beta^r = 2(\alpha + \alpha^2 \sum_{r\in Q} \beta^r) = 1 ,$$

since we have chosen β such that

$$0 = F(\beta) = 1 + \alpha^7 \sum_{r\in Q} \beta^r + \alpha^5 \sum_{s\in N} \beta^s = 1 + \alpha^7 \sum_{r\in Q} \beta^r +$$
$$+ \alpha^5 (j(\beta) + 2 + 2 \sum_{r\in Q} \beta^r) = 1 + \alpha + \alpha^2 \sum_{r\in Q} \beta^r ,$$

i.e.

$$\alpha + \alpha^2 \sum_{r\in Q} \beta^r = 2 .$$

(iii) $F(1) = 1$.

Because of (ii) and (iii) we have shown that $F(\beta^i) = 0$ iff $\gamma(\beta^i) = 0$ for all $i \in \{0, 1, \ldots, n-1\}$. Hence we have proved that $F(x)$ is the idempotent of D.

□

(4.5.6) Corollary: Let D be the QR-code as defined in Theorem (4.5.5). Then D is also generated by

$$g(x) = 1 + \alpha \sum_{s \in N} x^s \quad ,$$

where N is the set of nonresidues mod n.

Proof: This follows immediately form Theorem (4.3.1) and Theorem (4.5.5). □

Because of Corollary (4.5.4) and Corollary (4.5.6) we may conclude that the ternary images of extended QR-codes over GF(9) of length n + 1, where n is a prime of the form $n = 12k \pm 5$, are double circulant codes.

The extension of QR-codes

The QR-codes over GF(9) will not be extended in the usual way, but in the way described below.

Let n be a prime of the form $n = 12k \pm 5$, Q the set of all residues mod n and N the set of all nonresidues mod n. Let D_0 be the QR-code of length n over GF(9) generated by $\gamma_0(x) = \prod_{r \in Q} (x - \beta^r)$ and let D_1 be the QR-code of length n over GF(9) generated by $\gamma_1(x) = \prod_{s \in N} (x - \beta^s)$, where β is a primitive n-th root of unity in an extension field of GF(9). It is well-known (cf. [1, Ch.16.§4]) that these QR-codes can be extended, by adding an overall parity check, in such a way that

(4.5.7)

$$\text{(i)} \quad (\overline{D}_0)^\perp = \overline{D}_0 \quad , \ (\overline{D}_1)^\perp = \overline{D}_1 \quad , \qquad \text{if } n = 12k - 5,$$

$$\text{(ii)} \quad (\overline{D}_0)^\perp = \overline{D}_1 \quad , \qquad \text{if } n = 12k + 5.$$

Let h(x) be the polynomial defined by

$$h(x) := \sum_{s \in N} x^s \quad , \tag{4.5.8}$$

and let H be the n×n circulant matrix with toprow h(x). Since -1 is a residue mod n, if $n = 12k + 5$, and a nonresidue, if $n = 12k - 5$, the polynomial h(x) satisfies the following relations:

$$h^T(x) = h(x^{-1}) = \sum_{r\in Q} x^r \qquad \text{if } n = 12k - 5,$$

(4.5.9) $$h^T(x) = h(x^{-1}) = h(x) \qquad \text{if } n = 12k + 5,$$

$$h^3(x) = \sum_{r\in Q} x^r \qquad \text{if } n = 12k \pm 5.$$

Using these relations it is easily checked that the rows of the following two matrices $G_{\overline{D}_0}$ and $G_{\overline{D}_0^\perp}$ generate the extended codes $\overline{D}_0$ and $\overline{D}_0^\perp$ respectively

(4.5.10) $$G_{\overline{D}_0} = \left[\begin{array}{c|ccc} \eta & \alpha & \ldots & \alpha \\ \hline \zeta & & & \\ \vdots & & I + \alpha H & \\ \zeta & & & \end{array}\right], \quad G_{\overline{D}_0^\perp} = \left[\begin{array}{c|ccc} \eta & \alpha & \ldots & \alpha \\ \hline \zeta & & & \\ \vdots & & I + \alpha (H^3)^T & \\ \zeta & & & \end{array}\right],$$

where $\eta = \alpha^3$, $\zeta = \alpha^2$ if $n = 12k - 5$,

$\eta = \alpha^5$, $\zeta = \alpha^2$ if $n = 12k + 5$.

(4.5.11) Remark: Since $n \equiv \pm 5 \bmod 12$, 3 is a nonresidue mod n. Therefore the transformation $x \to x^3$ maps the code D_0 onto D_1. This implies that the code D_1 also is generated by $g_1(x) = 1 + \alpha \sum_{r\in Q} x^r$. Hence by Corollary (4.5.4) the ternary image of $\overline{D}_1$ is a double circulant code. However since $\overline{D}_0$ and $\overline{D}_1$ are equivalent just as their ternary images, we may restrict ourselves to D_0.

Now we have proved the following theorem.

(4.5.12) Theorem: Let n be a prime of the form $n = 12k \pm 5$. Let D be the $[n, \frac{1}{2}(n+1)]$ QR-code over GF(9) and let C be the ternary image of the extended code $\overline{D}$. Then the generator matrix of the $[2(n+1), n+1]$ ternary code C is given by

$$G = \left[\begin{array}{c|ccc|c|ccc} \varepsilon & 0 & \ldots & 0 & 2 & 1 & \ldots & 1 \\ \hline 1 & & & & 2 & & & \\ \vdots & & I & & \vdots & & H & \\ 1 & & & & 2 & & & \end{array}\right],$$

where $\varepsilon = 0$ if $n = 12k + 5$ and $\varepsilon = 2$ if $n = 12k - 5$. H is the $n\times n$ circulant matrix with toprow $h(x) = \sum_{s\in N} x^s$.

Proof: This follows immediately from (4.5.10). □

If n is a prime of the form n = 12k - 5, then the code C has also another generator matrix which has also an interesting form, as stated in the following theorem.

(4.5.13) Theorem: Let n be a prime of the form n = 12k - 5 and let C be the $[2(n+1), n+1]$ double circulant code which is the ternary image of the $[n+1, \frac{1}{2}(n+1)]$ extended QR-code over GF(9). Then C has a generator matrix G_0 of the following form

$$G_0 = [\, I \mid S \,] \quad ,$$

where S is an $(n+1)\times(n+1)$ matrix which satisfies $SS^T = (n+1)I$ (over $\mathbb{R}$).

Proof: A generator matrix of C is given by Theorem(4.5.12). It is easily seen that the following matrix G_0 is also a generator matrix of C

$$G_0 = \left[\begin{array}{c|ccc|c|ccc} 1 & 0 & \cdots & 0 & 1 & -1 & \cdots & -1 \\ \hline 0 & & & & 1 & & & \\ \vdots & & I & & \vdots & & H_1 & \\ 0 & & & & 1 & & & \end{array}\right] \quad ,$$

where $H_1 = H + J$, i.e. H_1 is the $n\times n$ circulant matrix with toprow

$$h_1(x) = 1 + \sum_{r\in Q} x^r - \sum_{s\in N} x^s \, .$$

Let S be the matrix defined by

$$S = \left[\begin{array}{c|ccc} 1 & -1 & \cdots & -1 \\ \hline 1 & & & \\ \vdots & & H_1 & \\ 1 & & & \end{array}\right] \quad .$$

Then

$$SS^T = \left[\begin{array}{c|ccc} n+1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & J + H_1H_1^T & \\ 0 & & & \end{array}\right] = (n+1)I,$$

since $H_1H_1^T$ is a circulant matrix with toprow

$$h_1(x)h_1^T(x) = h_1(x)h_1(x^{-1}) =$$

$$\overset{(i)}{=} (1 + \sum_{r\in Q} x^r - \sum_{s\in N} x^s)(1 - \sum_{r\in Q} x^r + \sum_{s\in N} x^s)$$

$$= 1 - (\sum_{r\in Q} x^r)^2 - (\sum_{s\in N} x^s)^2 + 2\sum_{r\in Q} x^r \sum_{s\in N} x^s$$

$$\overset{(ii)}{=} 1 - \tfrac{1}{4}(12k-8)\sum_{r\in Q} x^r - \tfrac{1}{4}(12k-4)\sum_{s\in N} x^s$$

$$- \tfrac{1}{4}(12k-4)\sum_{r\in Q} x^r - \tfrac{1}{4}(12k-8)\sum_{s\in N} x^s + 12k - 6$$

$$+ \tfrac{1}{2}(12k-8)(\sum_{r\in Q} x^r + \sum_{s\in N} x^s) = 12k - 4 - j(x).$$

Hence $H_1H_1^T = (12k-4)I - J$.
At the indexed places we have made use of

(i) -1 is a nonresidue mod n,

(ii) Theorem (4.5.3)

□

(4.5.14) Definition: An m×m matrix S of +1's and -1's such that $SS^T = mI$ is called a Hadamard matrix of order m.

The reader who is interested in Hadamard matrices is referred to [13, Ch.14]. The properties of Hadamard matrices which we shall use can be found there. We want to point out the resemblance between the generator matrix G_0 and the generator matrix of the symmetry code (cf. (2.3.1)). In §4.7 we shall return to this resemblance.

4.5.4. On the dual and the automorphisms of the ternary images of extended QR-codes over GF(9)

In this subsection we shall prove some theorems on the dual code of and the automorphisms of the ternary images of extended QR-codes over GF(9).
Let n be a prime, $n = 12k \pm 5$, and let C the $[2(n+1), n+1]$ double circulant code which is the ternary image of the $[n+1, \frac{1}{2}(n+1)]$ extended QR-code over GF(9).

(4.5.15) Lemma: The generator matrix of the dual code of C is given by

$$G = \left[\begin{array}{c|c|c|c} \varepsilon & 0 \ . \ . \ . \ 0 & 2 & 1 \ . \ . \ . \ 1 \\ \hline 1 & & 2 & \\ \vdots & I & \vdots & (H^3)^T \\ 1 & & 2 & \end{array}\right],$$

where $\varepsilon = 0$ if $n = 12k + 5$ and $\varepsilon = 2$ if $n = 12k - 5$.

Proof: The generator matrix of C is given in Theorem (4.5.12). It is easy to verify that

$$G(G^{\perp})^T = 0. \qquad \square$$

(4.5.16) Theorem : Let n be a prime of the form $n = 12k - 5$. Then the $[2(n+1), n+1]$ ternary code C is self-dual.

Proof: The matrix H is an $n \times n$ circulant matrix with toprow $h(x)$, where $h(x) = \sum_{s \in N} x^s$.

Since n is a prime of the form $n = 12k - 5$, both -1 and 3 are nonresidues mod n. Hence

$$h^T(x) = h(x^{-1}) = h(x^3) = h^3(x).$$

Thus

$$(H^3)^T = H.$$

The theorem now follows from Theorem (4.5.12) and Lemma (4.5.15). $\square$

An easy lemma, which we shall use several times, is the following.

(4.5.17) Lemma: Let $(a_\infty, a(x) ; b_\infty, b(x))$ be a codeword of the ternary code C. Then

(i) $a_\infty = 2b(1) + a(1)$, $b_\infty = 2b(1) + 2a(1)$ if $n = 12k - 5$,

(ii) $a_\infty = a(1)$, $b_\infty = b(1)$ if $n = 12k + 5$.

Proof: Analogous to the proof of Lemma (4.4.2) $\square$

Using this lemma we can prove the following theorem on the automorphisms of C.

(4.5.18) Theorem: Let C be the $[2(n+1), n+1]$ ternary image of the $[n+1, \frac{1}{2}(n+1)]$ extended QR-code over GF(9), where n is a prime of the form $n = 12k \pm 5$.
Let $(a_\infty, a(x) ; b_\infty, b(x))$ be an element of C . Then

(i) $(2b_\infty, b(x^3)\ ;\ a_\infty, 2a(x^3))$ and $(2b_\infty, b(x^{-1})\ ;\ a_\infty, 2a(x^{-1}))$ are also codewords in C if $n = 12k - 5$.

(ii) $(b_\infty, b(x^3)\ ;\ 2a_\infty, 2a(x^3))$ is also in C if $n = 12k + 5$.

Proof: Analogous to the proof of Theorem (4.4.3). □

By the Theorem of Gleason and Prange (cf. Theorem (2.2.7)) we know that the automorphism group of the extended QR-code of length n + 1 over GF(9) contains a subgroup isomorphic to PSL(2,n). Due to our choice of the mapping from the extended QR-code over GF(9) onto the ternary code C, the following theorem holds (cf. Theorem (3.4.7)).

(4.5.19) Theorem: The automorphism group of the double circulant code C contains PSL(2,n) applied simultaneously to both sides of the codewords of C, i.e. for all codewords (L ; R) in C and any element $T \in PSL(2,n)$, (T(L) ; T(R)) is in C.

4.5.5. On the minimum weight of the ternary images of extended QR-codes over GF(9) of length n + 1; n = 12k - 5

In this subsection let n be a prime of the form $n = 12k - 5$ and C the $[2(n+1), n+1]$ code which is the ternary image of the $[n+1, \frac{1}{2}(n+1)]$ extended QR-code over GF(9). We shall establish a theorem on the minimum weight of the code C. This theorem is analogous to Theorem (2.3.5). Let $\underline{x}$ be a codeword of C then we shall denote by $w_l(\underline{x})$, $w_r(\underline{x})$ respectively, the contribution to the weight of $\underline{x}$ due to the first n + 1 coordinates respectively the last n + 1 coordinates.

(4.5.20) Theorem: Let $\underline{x}$ be a codeword of the $[2(n+1), n+1]$ double circulant code C . Then

(i) $w_r(\underline{x}) > 0$

(ii) if $w_l(\underline{x}) = 1$, then $w_r(\underline{x}) = n+1$,

(iii) if $w_l(\underline{x}) = 2$, then $w_r(\underline{x}) = \frac{1}{2}(n + 1)$,

(iv) if $w_l(\underline{x}) = 3$, then $w_r(\underline{x}) = \frac{3}{4}(n + 1)$,

(v) if $w_l(\underline{x}) = 4$, then $w_r(\underline{x}) \geq \frac{1}{4}(n + 1)$, equality is only possible if $n + 1 \equiv 0 \bmod 8$.

(vi) if $w_l(\underline{x}) = 5$, then $w_r(\underline{x}) \geq \frac{1}{2}(n + 1)$,

(vii) if $w_l(\underline{x}) = 7$, then $w_r(\underline{x}) \geq \frac{1}{4}(n + 1)$.

Proof: Because of Theorem (4.5.13), C has a generator matrix of the form

$$G_0 = [\ I \mid S\ ],$$

where S is an $(n+1)\times(n+1)$ Hadamard matrix.

(i), (ii) and (iii) follow directly from the properties of Hadamard matrices (cf. [13, Ch.14]).

(iv) Consider three rows r_1, r_2 and r_3 of the matrix S. Since multiplying a column of S by -1 does not alter weights, we may assume that these three rows have the following form

$$r_1: + \ldots + + \ldots + + \ldots + + \ldots +$$
$$r_2: + \ldots + + \ldots + - \ldots - - \ldots -$$
$$r_3: \underbrace{+ \ldots +}_{a}\ \underbrace{- \ldots -}_{b}\ \underbrace{+ \ldots +}_{c}\ \underbrace{- \ldots -}_{d}$$

Here + and - stand for respectively +1 and -1.
Since S is a Hadamard matrix, we find

$$a = b = c = d = \tfrac{1}{4}(n + 1).$$

From these relations (iv) easily follows.

(v) Let r_4 be any row of S different from r_1, r_2 and r_3. Then by (iv) every linear combination $\sum_{i=1}^{4} \alpha_i r_i$, $\alpha_i \in \{-1, 1\}$ has weight $\geq \tfrac{1}{4}(n + 1)$, with equality iff this linear combination over $\mathbb{R}$ has the following form

$$(4.5.21) \qquad \underbrace{4\varepsilon \ldots 4\varepsilon}_{a}\ \underbrace{0 \ldots 0}_{a}\ \underbrace{0 \ldots 0}_{a}\ \underbrace{0 \ldots 0}_{a}$$

or one of the other 3 possibilities, which can be obtained by a cyclic shift over a positions. Here ε can take the values +1 or -1.
As S is a Hadamard matrix, every row of S different from $r_1, \ldots, r_4$ must be orthogonal, over $\mathbb{R}$, to (4.5.21). This is only possible if a is even, i.e. $n + 1 \equiv \bmod 8$. So we have proved (v).

(vi) and (vii). In order to prove (vi) and (vii) we shall make use of the method described in the proof of Theorem (2.3.5).

Let $\underline{g}_1, \ldots, \underline{g}_{n+1}$ be the n + 1 rowvectors of the generator matrix G_0. Thus every codeword $\underline{x}$ in C can be written as

$$\underline{x} = \sum_{i=1}^{n+1} \lambda_i \underline{g}_i \quad \text{over GF(3)}, \quad \lambda_i \in \{-1, 0, 1\} .$$

Let $\overline{\underline{x}}$ be the same linear combination of the n + 1 rowvectors but now evaluated over $\mathbb{R}$, i.e.

$$\overline{\underline{x}} = \sum_{i=1}^{n+1} \lambda_i \underline{g}_i \quad \text{over } \mathbb{R} .$$

The vector $\overline{\underline{x}}$ can be written as $\overline{\underline{x}} = (\lambda_1, \ldots, \lambda_{n+1}; \mu_1, \ldots, \mu_{n+1})$.

We remark that for all $1 \le i \le n + 1$, $|\mu_i| \le w_1(\underline{x})$. For given $\overline{\underline{x}}$ we define again $\mu(\overline{\underline{x}})$ by

$$\mu(\overline{\underline{x}}) = (\mu_1, \mu_2, \ldots, \mu_{n+1}).$$

Since S is a Hadamard matrix it is easily seen that

$$(\underline{g}_i, \underline{g}_j) = \delta_{ij}(n + 2), \quad \text{over } \mathbb{R}, \quad 1 \le i \le n + 1, \quad 1 \le j \le n + 1.$$

Hence

$$(4.5.22) \qquad (\overline{\underline{x}}, \overline{\underline{x}}) = \sum_{i=1}^{n+1} \lambda_i^2 (\underline{g}_i, \underline{g}_i) = (n + 2) \sum_{i=1}^{n+1} \lambda_i^2 = w_1(\underline{x})(n + 2).$$

For the corresponding $\mu(\overline{\underline{x}})$ we have

$$(4.5.23) \qquad (\mu(\overline{\underline{x}}), \mu(\overline{\underline{x}})) = (\overline{\underline{x}}, \overline{\underline{x}}) - w_1(\underline{x}) = w_1(\underline{x})(n + 1).$$

In order to indicate how many components of $\mu(\overline{\underline{x}})$ are equal to $\pm j$, we introduce again Type$(\mu(\overline{\underline{x}}))$. If α_j components of $\mu(\overline{\underline{x}})$ are equal to $\pm j$, then we write

$$\text{Type}(\mu(\overline{\underline{x}})) = (\pm(n+1))^{\alpha_{n+1}} (\pm n)^{\alpha_n} \ldots (\pm 1)^{\alpha_1} (0)^{\alpha_0}.$$

Let $\underline{x}$ be a codeword of C, with $w_1(\underline{x}) = p_1$ and $w_r(\underline{x}) = p_2$. Let p_1 be odd. Then obviously all components of $\mu(\overline{\underline{x}})$ are odd. Let

$$\text{Type}(\mu(\overline{\underline{x}})) = (\pm p_1)^{\alpha_{p_1}} (\pm(p_1-2))^{\alpha_{p_1-2}} \ldots (\pm 3)^{\alpha_3} (\pm 1)^{n+1-\Sigma\alpha_i}.$$

Then the following relation holds.

$$(4.5.24) \qquad (n + 1 - \Sigma\alpha_i) + \alpha_5 + \alpha_7 + \alpha_{11} + \ldots = w_r(\underline{x}) = p_2.$$

Furthermore (4.5.23) provides us with

$$(4.5.25) \qquad p_1^2\alpha_{p_1} + (p_1 - 2)^2\alpha_{p_1-2} + \ldots + 9\alpha_3 + (n + 1 - \Sigma\alpha_i) = p_1(n + 1).$$

From (4.5.24) it follows that

$$\alpha_3 + \alpha_9 + \alpha_{15} + \ldots = n + 1 - p_2$$

and from (4.5.25) we obtain

$$\alpha_3 + \alpha_9 + \alpha_{15} + \ldots \leq (n + 1)(p_1 - 1)/8.$$

Combination of these two results yields

$$p_2 \geq (n + 1)(9 - p_1)/8.$$

This inequality is trivially satisfied if $p_1 \geq 9$. But

if $p_1 = 3$ then $p_2 \geq \frac{3}{4}(n + 1)$, which agrees with (iv),

if $p_1 = 5$ then $p_2 \geq \frac{1}{2}(n + 1)$,

if $p_1 = 7$ then $p_2 \geq \frac{1}{4}(n + 1)$.

This proves (vi) and (vii). □

A simple but useful lemma is the following.

(4.5.26) Lemma: Let w_1 and w_2 be integers. Then there is a codeword $\underline{x}$ in C with $w_1(\underline{x}) = w_1$, $w_r(\underline{x}) = w_2$ iff there is a codeword $\underline{y}$ in C with $w_1(\underline{y}) = w_2$, $w_r(\underline{y}) = w_1$.

Proof: This is a consequence of Theorem (4.5.18). □

(4.5.27) Remark: Lemma (4.5.26) holds for all double circulant codes which are the ternary images of extended cyclic codes over GF(9), because of Theorem (4.4.3).

4.5.6. Examples and designs

In this subsection we shall discuss as an application of Theorem (4.5.20) the first three examples of the ternary images of the $[n+1, \frac{1}{2}(n+1)]$ QR-codes over GF(9), where n is a prime of the form $n = 12k - 5$.
We repeat that these codes are self-dual and have weights divisible by 3 (cf. Theorem (4.5.16)). It will appear that each of these three codes has a minimum weight that meets the bound on the minimum weight of self-dual codes over GF(3). This bound is given by the following lemma (cf. [1, Ch.19.Th.17]).

(4.5.28) Lemma (Mallows&Sloane): The minimum distance of a self-dual code over GF(3) of length n satisfies

$$d \leq 3\lfloor n/12 \rfloor + 3.$$

□

In order to investigate whether these codes contain t-designs we have applied the Assmus-Mattson Theorem (cf. Theorem (1.3.3)).
As usual the parameters of a t-design are denoted by v (= the number of points), b (= the number of blocks), k (= the blocksize) and λ_t (= the number of blocks containing any fixed t-subset).

(i) n = 7

Let C_7 be the [16,8] ternary image of the [8,4] extended QR-code over GF(9). Using Theorem (4.5.20) and Lemma (4.5.26) it is easy to see that the minimum weight of C_7 is equal to 6. Hence C_7 is a [16,8,6] self-dual code over GF(3). By Lemma (4.5.28) C_7 has a minimum weight that meets the bound on the minimum weight of self-dual codes over GF(3).
Application of the Assmus-Mattson Theorem reveals that the supports of codewords of weight 6 or 9 form 3-designs. In order to calculate the parameters of these designs we have determined the weight enumerator of C_7.
Let A_i be the number of codewords of weight i. Then the non-zero coefficients of the weight enumerator of C_7 are given by

$$A_0 = 1,$$
$$A_6 = 224,$$
$$A_9 = 2720,$$
$$A_{12} = 3360,$$
$$A_{15} = 256.$$

Since obviously

$$\lambda_3 = \frac{b\binom{k}{3}}{\binom{v}{3}} ,$$

we find that the supports of codewords of weight respectively 6 or 9 form a 3-design with parameters

$$v = 16, \quad b = 224, \quad k = 6, \quad \lambda_3 = 8$$

respectively

$$v = 16, \quad b = 2720, \quad k = 6, \quad \lambda_3 = 408.$$

In order to investigate whether these 3-designs are possibly 4-designs, we have calculated

$$\lambda_4 = \frac{b\binom{k}{4}}{\binom{v}{4}} .$$

The result was that in both cases λ_4 is not integral, so that these 3-designs can not be 4-designs.

(ii) n = 19

Let C_{19} be the [40,20] ternary image of the [20,10] extended QR-code over GF(9). By Theorem (4.5.20) and Lemma (4.5.26) the minimum weight of C_{19} is equal to 12. Hence C_{19} is a [40,20,12] self-dual code over GF(3). It is easily verified that this code also meets the bound of Lemma (4.5.28).
By the Assmus-Mattson Theorem we find that the supports of the codewords of weight respectively 12, 15, 18 or 21 form 3-designs. In this case we have not been able to determine the complete weight enumerator of C_{19}, but using the computer and Theorem (4.5.20) we have calculated for $1 \leq j \leq 10$ the weights of all linear combinations consisting of j rows of the generator matrix of C_{19}. Because of Lemma (4.5.26) we could calculate with these results A_{12}, A_{15}, A_{18} and A_{21},

$$A_{12} = 19760 ,$$
$$A_{15} = 1138176 ,$$
$$A_{18} = 25549680 ,$$
$$A_{21} = 236945280 .$$

From these results we find that the supports of the codewords of weight respectively 12, 15, 18 and 21 form 3-designs with parameters

$$v = 40,\ b = 19760,\ k = 12 \text{ and } \lambda_3 = 440,$$

$$v = 40,\ b = 1138176,\ k = 15 \text{ and } \lambda_3 = 52416,$$

$$v = 40,\ b = 25549680,\ k = 18 \text{ and } \lambda_3 = 2109960,$$

respectivley

$$v = 40,\ b = 236945280,\ k = 21 \text{ and } \lambda_3 = 31896480.$$

Also in these four cases λ_4 is not integral. Hence these 3-designs can not be 4-designs.

(iii) n = 31

Let C_{31} be the [64,32] ternary image of the [32,16] extended QR-code over GF(9). Let $\underline{x}$ be any codeword of C_{31}, $\underline{x} \neq \underline{0}$. Then by Theorem (4.5.20)

$$\text{if } w_1(\underline{x}) = 1 \text{ then } w_r(\underline{x}) = 32,$$

$$\text{if } w_1(\underline{x}) = 2 \text{ then } w_r(\underline{x}) = 16,$$

$$\text{if } w_1(\underline{x}) = 3 \text{ then } w_r(\underline{x}) = 24,$$

$$\text{if } w_1(\underline{x}) = 4 \text{ then } w_r(\underline{x}) \geq 8,$$

$$\text{if } w_1(\underline{x}) = 5 \text{ then } w_r(\underline{x}) \geq 16,$$

$$\text{if } w_1(\underline{x}) = 7 \text{ then } w_r(\underline{x}) \geq 8.$$

Using the computer we have calculated the weights of all linear combinations consisting of respectively 4, 6 and 7 rows of the generator matrix of C_{31}. This resulted in

$$\text{if } w_1(\underline{x}) = 4 \text{ then } w_r(\underline{x}) \geq 17,$$

$$\text{if } w_1(\underline{x}) = 6 \text{ then } w_r(\underline{x}) \geq 12,$$

$$\text{if } w_1(\underline{x}) = 7 \text{ then } w_r(\underline{x}) \geq 11.$$

By Lemma (4.5.26) we find that the minimum weight of this code is equal to 18. Hence C_{31} is a [64,32,18] self-dual code over GF(3) which meets the bound of Lemma (4.5.28).

The Assmus-Mattson Theorem reveals that the supports of codewords of weight respectively 18, 21, 24, 27, 30 and 33 form a 3-design. In this case we have not been able even to calculate the number of codewords of minimum weight. Therefore

we can not calculate the parameters of these 3-designs.

(4.5.29) Remark: The codes with parameters [16,8,6] and [40,20,12] were already known (cf. [1, Ch.19.§5]). The code with parameters [64,32,18] is propably new. As far as we know this is the largest known (with respect to the wordlength) self-dual code over GF(3) which meets the bound on the minimum weight of self-dual codes over GF(3) (cf. Lemma (4.5.28)). Hence also the 3-designs in this code are in all propability new.

4.6. A square root bound on the minimum weight of the ternary images of extended QR-codes over GF(9)

In this section we shall establish a square root bound on the minimum weight of the ternary images of extended QR-codes over GF(9). The proof of the square root bound is based on the theory of [16]. In this paper a square root bound on the minimum weight of the $[2(n+1), n+1]$ double circulant codes which are the binary images of extended quaternary QR-codes of length $n + 1$, n a prime of the form $n = 8k + 3$, has been proved.(cf. Theorem (3.5.1)). The proof of the square root bound in the ternary case is, except for the beginning, completely analogous to the proof in [16].

In this section let n_0 and n_1 be prime numbers of the form $n_0 = 12k - 5$ and $n_1 = 12k + 5$. Let C_i, $i = 0, 1$, be the $[2(n_i + 1), n_i + 1]$ ternary image of the extended QR-code D_i over GF(9) of length $n_i + 1$ and dimension $\frac{1}{2}(n_i + 1)$. The generator matrices of the ternary codes C_1 and C_2 are denoted by G_0 and respectively G_1, i.e. (cf. Theorem (4.5.12))

$$(4.6.1)\quad G_0 = \left[\begin{array}{c|ccc|c|ccc} 2 & 0 & \dots & 0 & 2 & 1 & \dots & 1 \\ \hline 1 & & & & 2 & & & \\ \vdots & & I & & \vdots & & H_0 & \\ 1 & & & & 2 & & & \end{array}\right], \quad G_1 = \left[\begin{array}{c|ccc|c|ccc} 0 & 0 & \dots & 0 & 2 & 1 & \dots & 1 \\ \hline 1 & & & & 2 & & & \\ \vdots & & I & & \vdots & & H_1 & \\ 1 & & & & 2 & & & \end{array}\right].$$

Here H_i is an $n_i \times n_i$ circulant matrix with toprow $h_i(x) = \sum_{s \in N_i} x^s$, where N_i is the set of nonresidues mod n_i, $i = 0, 1$.

Let $(a_{0\infty}, a_0(x) ; b_{0\infty}, b_0(x)) \in C_0$ and $(a_{1\infty}, a_1(x) ; b_{1\infty}, b_1(x)) \in C_1$.

The automorphism which changes $(a_{0\infty}, a_0(x) ; b_{0\infty}, b_0(x))$ into

$(2b_{0\infty}, b_0(x^{-1}) ; a_{0\infty}, 2a_0(x^{-1}))$ is called τ_0. (Thus τ_0 is an automorphism of C_0). The automorphism of C_1 which changes $(a_{1\infty}, a_1(x) ; b_{1\infty}, b_1(x))$ into $(b_{1\infty}, b_1(x^3) ; 2a_{1\infty}, 2a_1(x^3))$ is denoted by τ_1. (cf. Theorem (4.5.18)). Furthermore we repeat that $\mathrm{Aut}(C_i)$ contains $\mathrm{PSL}(2,n_i)$ applied simultaneously to both sides of the codewords of C_i, i = 0, 1. (cf. Theorem (4.5.19)).
Let $\underline{v} = (\underline{a} ; \underline{b}) = (a_\infty, a_0, \ldots, a_{n-1} ; b_\infty, b_0, \ldots, b_{n-1})$ be any vector of length 2(n + 1) over GF(3). Then we define

$$
\begin{aligned}
d_1(\underline{v}) &:= \left| \{ i \in GF(n) \mid a_i \neq 0 \} \right|, \\
d_2(\underline{v}) &:= \left| \{ i \in GF(n) \mid b_i \neq 0 \} \right|.
\end{aligned}
\tag{4.6.2}
$$

Let d_i be the minimum weight of the code C_i. Then for i = 0, 1, we define sets $\Omega_i^{\#}$ and Ω_i to be

$$
\begin{aligned}
\Omega_i^{\#} &:= \{ \underline{v} = (\underline{a} ; \underline{b}) \in C_i \mid a_\infty \neq 0, b_\infty \neq 0 \text{ and } w_H(\underline{v}) = d_i \} , \\
\Omega_i &:= \{ \underline{v} = (\underline{a} ; \underline{b}) \in C_i \mid a_\infty \neq 0, b_\infty = 0 \text{ and } w_H(\underline{v}) = d_i \} .
\end{aligned}
\tag{4.6.3}
$$

We have not been able to prove that $\Omega_i^{\#}$ is non-empty, but we do have

(4.6.4) Lemma: a) The set Ω_i is non-empty

b) If $\underline{v} \in \Omega_i$ and $d_2(\underline{v}) > d_1(\underline{v})$ then there exists an element $\underline{x} \in \Omega_i$ with $d_1(\underline{x}) = d_2(\underline{v}) - 1$ and $d_2(\underline{x}) = d_1(\underline{v}) + 1$.

c) If $\Omega_i^{\#}$ is empty , then the following holds. If $\underline{x} \in \Omega_i$ and $d_1(\underline{x}) \geq d_2(\underline{x})$, then there exists an element $\underline{v} \in \Omega_i$ with $d_2(\underline{v}) = d_1(\underline{x}) + 1$ and $d_1(\underline{v}) = d_2(\underline{x}) - 1$.

This lemma holds for both i = 0 and i = 1.

Proof: Let $i \in \{0, 1\}$.

a) Let $\underline{v} = (\underline{a} ; \underline{b})$ be a codeword in C_i of minimum weight d_i. If $a_\infty \neq 0$ and $b_\infty = 0$, then $\underline{v} \in \Omega_i$ and the proof is finished. Also if $a_\infty = 0$ and $b_\infty \neq 0$ then $\tau_0(\underline{v}) \in \Omega_i$. Therefore we may assume that either $a_\infty = b_\infty = 0$ or $a_\infty \neq 0$ and $b_\infty \neq 0$.
We can find $j \in GF(n)$ such that either $a_j \neq 0$, $b_j = 0$ or $a_j = 0$, $b_j \neq 0$, unless $\underline{a}$ and $\underline{b}$ have the same support, i.e. for all $k \in GF(n) \cup \{\infty\}$ $a_k \neq 0$ iff $b_k \neq 0$.

This last can not happen. For since $(\underline{a} ; \underline{b}) \in C_i$, we know that $\underline{a} + \alpha\underline{b} \in D_i$. Thus also $\alpha(\underline{a} + \alpha\underline{b})$ and $\alpha^7(\underline{a} + \alpha\underline{b})$ are elements of D_i. The ternary images of these two codewords are respectively $(\underline{b}; \underline{a} + 2\underline{b})$ and $(\underline{a} + \underline{b} ; \underline{a})$. As $\underline{v}$ is a codeword of minimum weight we have

$$\text{(i)} \quad w_H((\underline{b} ; \underline{a} + 2\underline{b})) \geq w_H((\underline{a} ; \underline{b})) ,$$

$$\text{(ii)} \quad w_H((\underline{a} + \underline{b} ; \underline{a})) \geq w_H((\underline{a} ; \underline{b})) .$$

It is easily seen that this is impossible if $\underline{a}$ and $\underline{b}$ have the same support. Therefore let $j \in GF(n_i)$ such that either $a_j \neq 0$, $b_j = 0$ or $a_j = 0$, $b_j \neq 0$. Let $T \in PSL(2,n_i)$ such that T interchanges the indices j and ∞, and let $\underline{v}' = (T(a) ; T(b))$. Then $\underline{v} \in C_i$ with $w_H(\underline{v}) = d_i$ and either $\underline{v}' \in \Omega_i$ or $\tau_0(\underline{v}') \in \Omega_i$. Hence we have proved a).

b) Let $\underline{v} = (\underline{a} ; \underline{b}) \in \Omega_i$ with $d_2(\underline{v}) > d_1(\underline{v})$. Then there exists an element $j \in GF(n)$ with $b_j \neq 0$ and $a_j = 0$. Let T be the automorphism which interchanges the indices j and ∞ and define $\underline{x}$ to be $\underline{x} := \tau_i((T(\underline{a}) ; T(\underline{b}))$. Then $\underline{x} \in \Omega_i$ with $d_1(\underline{x}) = d_2(\underline{v}) - 1$ and $d_2(\underline{x}) = d_1(\underline{v}) + 1$, as required.

c) We assume $\Omega_i^{\#}$ to be empty.

Let $\underline{x} = (\underline{c} ; \underline{d}) \in \Omega_i$ with $d_1(\underline{x}) \geq d_2(\underline{x})$. Since we have made the assumption that $\Omega_i^{\#}$ is empty, it is easily seen that for all $j \in GF(n) \cup \{\infty\}$ $d_j \neq 0$ implies $c_j = 0$. There are two different cases to consider, namely $\underline{d} \neq \underline{0}$ and $\underline{d} = \underline{0}$.

Let $\underline{d} \neq \underline{0}$. Since $\underline{x} \in \Omega_i$, $d_\infty = 0$. Hence there exists an element $j \in GF(n)$ such that $d_j \neq 0$ and $c_j = 0$. In the same way as in b) the proof can now be finished.

Let $\underline{d} = \underline{0}$. In this case we have to consider the two possiblities $i = 0$ and $i = 1$ separately.

Let $i = 0$. Since $\underline{v} \in C_0$ we have by Lemma (4.5.17)

$$0 = d_\infty = 2c(1) + 2d(1) = 2c(1),$$

and

$$c(x)h_0(x) + \varepsilon j(x) = d(x) = 0.$$

Substituting $x = 1$ yields $\varepsilon = 0$, so that

$$0 = c(x)(h_0^2(x) + h_0(x)) = c(x)(1 + j(x)) = c(x) + c(1)j(x) = c(x).$$

Hence $\underline{v} = \underline{0}$. This contradicts $w_H(\underline{v}) = d_0$.

Let $i = 1$. Then we find in the same way that $c(x) = 2c(1)j(x)$, but in

this case c(1) is not necessary equal to 0. Since $w_H(\underline{v}) = d_1$, this forces $d_1 = n + 1$. Let r_∞ and r_0 be respectively the first and second row of the generator matrix G_1, defined by (4.6.1). Then obviously

$$w_H(r_\infty + 2r_0) = 2 + \tfrac{1}{2}(n + 1),$$

so that we may conclude

$$n + 1 = d_1 \leq 2 + \tfrac{1}{2}(n + 1), \text{ i.e. } n \leq 3.$$

Thus also in this case we are led to a contradiction, since $n \geq 5$. Hence $\underline{d} \neq \underline{0}$. So we have proved c). □

We remark once again that the QR-code D_i over GF(9) of length n_i is also generated by $g_i(x) = 1 + \alpha h_i(x)$, where $h_i(x) = \sum_{s \in N_i} x^s$ and N_i the set of all nonresidues mod n_i. Let D_i^* be the cyclic code over GF(9) of length n_i generated by $g_i^*(x) = 1 + \alpha h_i^3(x)$, $i = 0,1$.
We have already shown that (cf. Lemma (4.3.3))

$$D_i \cap D_i^* = \langle j(x) \rangle, \quad i = 0, 1. \tag{4.6.5}$$

We remark that -1 and 3 are nonresidues mod n_0, since n_0 is a prime of the form $n_0 = 12k - 5$, so that

$$h_0^3(x) = h_0(x^{-1}). \tag{4.6.6}$$

Let $a(x), b(x) \in D_i$. Then it is easily seen that $a(x)b(x^3) \in D_i \cap D_i^*$. Furthermore from (4.6.6) it follows that, if $a(x), b(x) \in D_0$, then also $a(x)b(x^{-1}) \in D_0 \cap D_0^*$.
We define integers t_i' and t_i by

$$\begin{aligned} t_i' &:= \max_{\underline{v} \in \Omega_i} \{d_1(\underline{v}) - d_2(\underline{v})\}, \\ t_i &:= \max_{\underline{v} \in \Omega_i} \{d_2(\underline{v}) - d_1(\underline{v})\}. \end{aligned} \tag{4.6.7}$$

Let $t_{imax} := \max \{t_i, t_i'\}$. Then obviously $t_{imax} \geq 0$.

(4.6.8) Theorem: Let $s_i := \max_{v \in \Omega_i^{\#}} \{ |d_1(\underline{v}) - d_2(\underline{v})| \}$.
If $\Omega_i^{\#}$ is non-empty, then the minimum weight d_i of C_i satisfies

$$(d_i - 1)^2 - (d_i - 1) + 1 - s_i t_{imax} \geq 2n_i + 1.$$

This theorem holds for both i = 0 and i = 1.

Proof: Let $i \in \{0, 1\}$.
Without loss of generality we may assume that $t_{imax} = t_i$. Let

$$\underline{e} = (1, a_0, \ldots, a_{n-1} ; 0, b_0, \ldots, b_{n-1}) \in \Omega_i$$

with

$$d_1(\underline{e}) = \frac{(d_i - 1) - t_i}{2} , \quad d_2(\underline{e}) = \frac{(d_i - 1) + t_i}{2} .$$

Since $\tau_i \in \mathrm{Aut}(C_i)$ there exixts a vector

$$\underline{v} = (1, c_0, \ldots, c_{n-1} ; d_\infty, d_0, \ldots, d_{n-1}) \in \Omega_i^{\#}, \ d_\infty \neq 0$$

with

$$d_1(\underline{v}) = \frac{(d_i - 2) + s_i}{2} , \quad d_2(\underline{v}) = \frac{(d_i - 2) - s_i}{2} .$$

Let $$u(x) = \sum_{j=0}^{n_i-1} c_j x^j + \alpha \sum_{j=0}^{n_i-1} d_j x^j, \quad y(x) = \sum_{j=0}^{n_i-1} a_j x^{3j} + \alpha \sum_{j=0}^{n_i-1} b_j x^{3j}.$$

Then $u(x) \in D_i$ and $y(x) \in D_i^*$, so that $u(x)y(x) \in D_i \cap D_i^*$.
Hence there exist elements $k_1, k_2 \in GF(3)$ such that

$$k_1 \sum_{j=0}^{n_i-1} x^j + \alpha k_2 \sum_{j=0}^{n_i-1} x^j = u(x)y(x) =$$

$$= \sum c_j x^j \sum a_j x^{3j} + \sum d_j x^j \sum b_j x^{3j} +$$

$$+ \alpha \{ \sum c_j x^j \sum b_j x^{3j} + \sum a_j x^{3j} \sum d_j x^j + 2 \sum d_j x^j \sum b_j x^{3j} \} .$$

Substituting x = 1 yields

$$k_1 \equiv \sum c_j \sum a_j + \sum d_j \sum b_j \equiv (c(1)a(1) + d(1)b(1)) \bmod 3$$

$$k_2 \equiv \sum c_j \sum b_j + \sum a_j \sum d_j + 2 \sum d_j \sum b_j \equiv$$

$$\equiv (c(1)b(1) + a(1)d(1) + 2d(1)b(1)) \bmod 3.$$

We now consider the two cases i = 0 and i = 1 separately.
Let i = 0. Then by Lemma (4.5.17)

$$1 = a_\infty = a(1) + 2b(1) \quad \text{and} \quad 0 = b_\infty = 2b(1) + 2a(1),$$

so that b(1) = 1 and a(1) = 2.
Furthermore

$$1 = c_\infty = c(1) + 2d(1) \quad \text{and} \quad d_\infty = 2d(1) + 2c(1).$$

This leads to

$$\text{if } d_\infty = 1, \text{ then } d(1) = 1 \text{ and } c(1) = 0,$$
$$\text{if } d_\infty = 2, \text{ then } d(1) = 0 \text{ and } c(1) = 1.$$

In both cases we find $k_1 \neq 0$.
Let i = 1. Then by Lemma (4.5.17)

$$1 = a_\infty = a(1), \quad 0 = b_\infty = b(1), \quad 1 = c_\infty = c(1) \quad \text{and} \quad d_\infty = d(1).$$

Both $d_\infty = 1$ and $d_\infty = 2$ yield $k_1 \neq 0$.
So we may conclude that $k_1 \neq 0$, if both i = 0 and i = 1. Hence

$$k_1 \sum_{j=0}^{n_i-1} x^j = \sum c_j x^j \sum a_j x^{3j} + \sum d_j x^j \sum b_j x^{3j} \quad .$$

Counting non-zero coefficients gives

$$\left(\frac{(d_i - 2) + s_i}{2}\right)\left(\frac{(d_i - 1) - t_i}{2}\right) + \left(\frac{(d_i - 2) - s_i}{2}\right)\left(\frac{(d_i - 1) + t_i}{2}\right) \geq n_i$$

This formula can easily be reduced to the assertion of the theorem. □

Hence assuming that $\Omega_i^{\#}$ is non-empty we have established a square root bound on the minimum weight d_i of the code C_i. For the rest of this section we assume $\Omega_i^{\#}$ to be empty. Also in this case we shall establish a square root bound on the minimum weight d_i. From now on the proof is completely analogous to the proof in [16]. For the sake of completeness we remark that Theorem (4.6.8) is almost analogous to the corresponding theorem in [16], but the lemma analogous to Lemma (4.6.4) is in the binary case easier to prove.

From Lemma (4.6.4c) it follows that t_i, defined by (4.6.7) is greater than zero. Only for i = 0 we define

$$r := \min_{\substack{\underline{v}\in\Omega_0 \\ d_2(\underline{v}) > d_1(\underline{v})}} \{ d_2(\underline{v}) - d_1(\underline{v}) \} .$$

(4.6.9) Lemma: The minimum weight d_0 of the code C_0 satisfies

$$\frac{(d_0 - 1)^2}{2} + \frac{(r - 2)^2}{2} - (d_0 - 1) + 1 \geq n_0 .$$

Proof: By Lemma (4.6.4b) there exists a vector

$$\underline{v} = (1, a_0, \ldots, a_{n-1} ; 0, b_0, \ldots, b_{n-1}) \in \Omega_0$$

with

$$d_1(\underline{v}) = \frac{(d_0 - 1) + (r - 2)}{2} , \quad d_2(\underline{v}) = \frac{(d_0 - 1) - (r - 2)}{2} .$$

Let

$$u(x) = \sum_{j=0}^{n_0-1} a_j x^j + \alpha \sum_{j=0}^{n_0-1} b_j x^j .$$

Then $u(x) \in C_0$ and $u(x)u(x^{-1}) \in C_0 \cap C_0^*$. Hence there exist elements k_1, k_2 in GF(3) such that

$$u(x)u(x^{-1}) = \sum a_j x^j \sum a_j x^{-j} + \sum b_j x^j \sum b_j x^{-j} +$$

$$+ \alpha \{ \sum a_j x^j \sum b_j x^{-j} + \sum a_j x^{-j} \sum b_j x^j + 2 \sum b_j x^j \sum b_j x^{-j} \} =$$

$$= k_1 \sum x^j + \alpha k_2 \sum x^j .$$

Substituting $x = 1$ yields

$$k_1 = a^2(1) + b^2(1), \quad k_2 = 2a(1)b(1) + 2b^2(1).$$

By Lemma (4.5.17) we have

$$1 = a_\infty = a(1) + 2b(1) , \quad 0 = b_\infty = 2a(1) + 2b(1),$$

i.e.

$$a(1) = 2 \text{ and } b(1) = 1.$$

Hence $k_1 = 2$ and $k_2 = 0$. Thus we may conclude that

$$2 \sum x^j = \sum a_j x^j \sum a_j x^{-j} + \sum b_j x^j \sum b_j x^{-j} .$$

Counting non-zero coefficients gives

$$\left(\frac{(d_0 - 1) + (r - 2)}{2} \right)^2 + \left(\frac{(d_0 - 1) - (r - 2)}{2} \right)^2 - (d_0 - 1) + 1 \geq n_o .$$

This formula can easily be reduced to the statement of the theorem. □

(4.6.10) Lemma: The minimum weight d_i of the code C_i satisfies

$$\frac{(d_i - 2)^2}{2} - \frac{t_i^2}{2} + t_i \geq n_i \qquad i = 0, 1.$$

Proof: Let $i \in \{0, 1\}$.
By Lemma (4.6.4b) there exists a vector

$$\underline{v} = (1, a_0, \ldots, a_{n-1} ; 0, b_0, \ldots, b_{n-1}) \in \Omega_i$$

with

$$d_1(\underline{v}) = \frac{(d_i - 1) - t_i}{2} \quad \text{and} \quad d_2(\underline{v}) = \frac{(d_i - 1) + t_i}{2} ,$$

and by the same lemma there exists a vector

$$\underline{e} = (1, c_0, \ldots, c_{n-1} ; 0, d_0, \ldots, d_{n-1}) \in \Omega_i$$

with

$$d_1(\underline{e}) = \frac{(d_i - 1) + (t_i - 2)}{2} \quad \text{and} \quad d_2(\underline{e}) = \frac{(d_i - 1) - (t_i - 2)}{2}.$$

Let

$$u(x) = \sum a_j x^j + \alpha \sum b_j x^j \quad \text{and} \quad y(x) = \sum c_j x^{3j} + \alpha \sum d_j x^{3j} .$$

Then $u(x) \in D_i$, $y(x) \in D_i^*$, so that $u(x)y(x) \in D_i \cap D_i^* = \langle j(x) \rangle$.
Hence there exists elements k_1, $k_2 \in GF(3)$ such that

$$\begin{aligned} u(x)y(x) &= \sum a_j x^j \sum c_j x^{3j} + \sum b_j x^j \sum d_j x^{3j} + \\ &\quad + \alpha\{ \sum a_j x^j \sum d_j x^{3j} + \sum c_j x^{3j} \sum b_j x^j + 2 \sum b_j x^j \sum d_j x^{3j} \}. \\ &= k_1 \sum x^j + \alpha k_2 \sum x^j. \end{aligned}$$

Substituting $x = 1$ yields

$$k_1 = a(1)c(1) + b(1)d(1) \quad \text{and} \quad k_2 = a(1)d(1) + c(1)b(1) + 2b(1)d(1).$$

It is easy to see that for $i = 0$ as well for $i = 1$ this leads to $k_1 \neq 0$ and $k_2 = 0$. Hence we may conclude that

$$k_1 \sum x^j = \sum a_j x^j \sum c_j x^{3j} + \sum b_j x^j \sum d_j x^{3j} .$$

Counting non-zero coefficients gives

$$\left(\frac{(d_i - 1) - t_i}{2}\right)\left(\frac{(d_i - 1) + (t_i - 2)}{2}\right) + \left(\frac{(d_i - 1) + t_i}{2}\right)\left(\frac{(d_i - 1) - (t_i - 2)}{2}\right) \geq$$

$$\geq n_i.$$

This reduces to the statement of the lemma. □

Now we are able to prove the square root bound on the minimum weight of the codes C_i , i = 0, 1.

(4.6.11) Theorem: Let C be the [2(n+1), n+1] double circulant code which is the ternary image of the extended QR-code over GF(9) of length n + 1 and dimension ½(n + 1); n is a prime of the form n = 12k ± 5. Then the minimum weight d of C satisfies

$$\text{(i)} \quad (d-1)^2 - (d-1) + 1 \geq 2n+1 \qquad \text{if } n = 12k-5,$$

$$d \equiv 0 \bmod 3$$

$$\text{(ii)} \quad (d-1)^2 \geq 2n-1 \qquad \text{if } n = 12k+5.$$

Proof: (i) Let n be a prime of the form n = 12k - 5. If $\Omega_0^{\#}$ is non-empty, the statement has already been settled by Theorem (4.6.8). Therefore we may assume that $\Omega_0^{\#}$ is empty.
If $t_0 \leq \sqrt{d-1} + 1$, then $r \leq \sqrt{d-1} + 1$, so that Lemma (4.6.9) gives

$$\frac{(d-1)^2}{2} - \frac{(d-1)}{2} \geq n$$

and the statement holds. If $t_0 = \sqrt{d-1} + \delta$, $\delta > 1$, then Lemma (4.6.10) gives

$$\frac{(d-1)^2}{2} - \frac{(d-1)}{2} - \sqrt{d-1}\,(\delta-1) - (\frac{\delta}{2}-1) \geq n \quad .$$

Since $\delta > 1$ this inequality can be reduced to

$$(d-1)^2 - (d-1) + 1 \geq 2n+1.$$

(ii) Let n be a prime of the form n = 12k + 5. If $\Omega_1^{\#}$ is non-empty, even a more powerful statement has been proved (cf. Theorem (4.6.8)). Therefore we make the assumption that $\Omega_1^{\#}$ is empty. Since, in this case, $t_1 \geq 1$, the second part of the theorem follows directly from Lemma (4.6.10). □

(4.6.12) Examples: Using the computer and Theorem (4.5.20) we have calculated the minimum weight of all [2(n+1), n+1] double circulant codes which are the ternary

images of $[n+1, \frac{1}{2}(n+1)]$ extended QR-codes over GF(9), up to n = 31 (cf. §4.5.6). Here n is a prime of the form $n = 12k \pm 5$. We shall compare these values with the lower bounds which we have found by using the square root bound.

n	minimum weight of the $[2(n+1), n+1]$ code C	a lower bound on the minimum weight of C
5	4	4
7	6	6
17	10	7
19	12	9
29	16	9
31	18	12

The examples reveal that the square root bound,mentioned in Theorem (4.6.11), is not very sharp for small values of n; this in contrast with the square root bound in the binary case (cf. Theorem (3.5.11)).

4.7. The relation between extended QR-codes over GF(9) and symmetry codes over GF(3)

In §4.5 we have shown that the $[2(n+1), n+1]$ double circulant codes which are the ternary images of $[n+1, \frac{1}{2}(n+1)]$ extended QR-codes over GF(9), where n is a prime of the form $n = 12k - 5$, have a generator matrix of the form $G = [\ I \mid S\ ]$, where S is a Hadamard matrix of the Paley-type (cf. Theorem (4.5.13)). After we had noticed that, the question arose whether it is also possible to consider the symmetry codes in one way or another as the ternary images of extended QR-codes over GF(9). In this section the question will be answered in the affirmative in case n is a prime of the form $n = 12k + 5$.
Let α be a primitive element of GF(9) which satisfies

$$\alpha^2 + \alpha + 2 = 0$$

(cf. §4.2). It is easily seen that every element $\xi \in GF(9)$ can be written uniquely as $\xi = a + \alpha^2 b$, where $a, b \in GF(3)$. Therefore any vector $\underline{c}$ of an n-dimensional vectorspace over GF(9) can be written as

$$\underline{c} = (a_1 + \alpha^2 b_1, a_2 + \alpha^2 b_2, \ldots, a_n + \alpha^2 b_n),$$

where $a_i, b_i \in GF(3)$, $1 \leq i \leq n$.
The ternary image of this vector $\underline{c}$ is defined to be

$$(a_1, a_2, \ldots, a_n ; b_1, b_2, \ldots, b_n) .$$

The mapping which sends vectors of length n over GF(9) into vectors of length 2n over GF(3), in the above defined way, is called ψ.
Analogously to Theorem (4.2.7) it is easy to prove

(4.7.1) Theorem: A necessary and sufficient condition for the ternary image of an extended cyclic code over GF(9) of length n + 1, generated by $g(x) = 1 + \alpha^2 h(x)$, under the mapping ψ, to be a $[2(n+1), n+1]$ double circulant code C is that the polynomial h(x) satisfies

(4.7.2) $\quad h^2(x) + 1 = \pm j(x).$ □

Let n be a prime of the form $n = 12k + 5$. Let as usual Q be the set of all residues mod n and N the set of all nonresidues. Then the polynomial h(x), defined by

(4.7.3) $\quad h(x) = 2 + \sum_{s \in N} x^s ,$

is a solution of equation (4.7.2), as easily can be verified using Theorem (4.5.3). Hence the ternary image of the extended cyclic code over GF(9) of length n + 1 generated by $g(x) = 1 + \alpha^2(2 + \sum_{s \in N} x^s)$ is a double circulant code of length 2(n + 1) and dimension n + 1. This code D over GF(9) generated by $g(x) = 1 + \alpha^2(2 + \sum_{s \in N} x^s)$ is a QR-code. For the code D is also generated by

$$g_0(x) = \alpha^7 g(x) = \alpha^7 + 2\alpha + \alpha \sum_{s \in N} x^s = 1 + \alpha \sum_{s \in N} x^s .$$

We have already shown that the cyclic code over GF(9) of length n, n a prime of the form $n = 12k + 5$, generated by $g_0(x) = 1 + \alpha \sum_{s \in N} x^s$ is a QR-code (cf. Corollary (4.5.6)).
The generator matrix of the extended code $\overline{D}$ is given by (4.5.10). Therefore the matrix $G_{\overline{D}}$, defined by

$$(4.7.4)\quad G_{\overline{D}} = \alpha\left[\begin{array}{c|c} \alpha^5 & \alpha \ldots \alpha \\ \hline \alpha^2 & \\ \vdots & I + \alpha H_0 \\ \alpha^2 & \end{array}\right] = \left[\begin{array}{c|c} \alpha^6 & \alpha^2 \ldots \alpha^2 \\ \hline \alpha^3 & \\ \vdots & I + \alpha^2(2I + H_0) \\ \alpha^3 & \end{array}\right] ,$$

where H_0 is the circulant matrix with toprow $h_0(x) = \sum_{s\in N} x^s$, is also a generator matrix of the extended code $\overline{D}$.
Since $\alpha^6 = 2\alpha^2$ and $\alpha^3 = 1 + \alpha^2$, the ternary image C of the extended code $\overline{D}$, under the mapping ψ, has a generator matrix of the following form

$$(4.7.5)\quad G = \left[\begin{array}{c|c|c|c} 0 & 0 \ldots 0 & 2 & 1 \ldots 1 \\ \hline 1 & & 1 & \\ \vdots & I & \vdots & H \\ 1 & & 1 & \end{array}\right] ,$$

where H is a circulant matrix with toprow $h(x) = 2 + \sum_{s\in N} x^s$. Obviously the matrix G_1, defined by

$$(4.7.6)\quad G_1 = \left[\begin{array}{c|c|c|c} 0 & 0 \ldots 0 & 1 & 1 \ldots 1 \\ \hline 1 & & 0 & \\ \vdots & I & \vdots & H + J \\ 1 & & 0 & \end{array}\right] ,$$

is also a generator matrix of the double circulant code C. Since H + J is a circulant matrix with toprow

$$h_1(x) = h(x) + j(x) = \sum_{r\in Q} x^r - \sum_{s\in N} x^s ,$$

the code C is equivalent with the symmetry code (cf. Definition (2.3.1)). Hence we have proved the following theorem.

(4.7.7) Theorem: Let n be a prime of the form $n = 12k + 5$. Then the $[2(n+1), n+1]$ symmetry code Sym_{2n+2} is equivalent with the ternary image, under the mapping ψ, of the extended $[n+1, \frac{1}{2}(n+1)]$ QR-code over GF(9). □

We have not been able to prove an analogous theorem for Sym_{2n+2}, in case n is a prime of the form $n = 12k - 1$.

Appendix A. The minimum weights of all [2(n+1), n+1] double circulant codes which are the binary images of extended quaternary cyclic codes, up to n = 45

In this appendix a complete list of all [2(n+1), n+1] double circulant codes which are the binary images of extended quaternary cyclic codes will be given up to n = 45. That means that for all feasible values of $n \leq 45$ all polynomials $h(x)$ which satisfy $h^2(x) + h(x) + 1 = j(x)$ and the corresponding codes have been determined. The theory of these double circulant codes has been treated in chapter 3.

Using the computer the minimum weights of all these codes have been calculated. All polynomials $h(x)$ have been recorded, except when two polynomials $h_1(x)$ and $h_2(x)$ satisfied one of the following relations: $h_1(x) = h_2(x^{-1})$, $h_1(x) = h_2(x) + j(x)$, $h_1(x) = h_2^2(x)$ or $h_1(x) = x^k h_2(x)$ for any $k \leq n - 1$. In these cases only one of the two polynomials has been recorded. For the sake of completeness we want to emphasize the fact that it is very well possible that we have mentioned codes which are equivalent.

Up to n = 19 also the weight enumerators of the [2(n+1), n+1] double circulant codes have been calculated.

Because of Corollary (3.4.9) the polynomial $h(x)$ might be chosen such that $h(1) = 1$. In this case $h(x)$ is invertible, i.e. $\gcd(h(x), x^n - 1) = 1$, so that also the circulant matrix H, with toprow $h(x)$, is invertible. Moreover in this case H satisfies $H^3 = I$ (cf. Lemma (3.2.19)), i.e. $H^2 = H^{-1}$. In order to simplify the calculations we have made use of some of the theory developed in [11].

In this appendix the toprow of H, $h(x) = h_0 + h_1 x + \ldots + h_{n-1} x^{n-1}$, is given in octal as $|h_0 h_1 h_2|h_3 h_4 h_5|\ldots$. E.g. 2704 stands for $h(x) = x + x^3 + x^4 + x^5 + x^9$.

The wordlength of the code is denoted by N, i.e. $N = 2n + 2$, the dimension by k, i.e. $k = n + 1$, and the minimum distance by d. The codes labelled with the symbol # are self-dual and have weights divisible by 4.

	n	N	k	d	h(x)
#	3	8	4	4	2 (extended Hammingcode)
	5	12	6	4	62
	9	20	10	4	662
#	11	24	12	8	2704 (extended binary Golay code)
	13	28	14	8	66064
	15	32	16	4	23451, 22662
				8	27206, 27015
	17	36	18	8	670072, 626322
#	19	40	20	8	2365030
	25	52	26	4	634512344, 624716244
#	27	56	28	4	262662262, 226626226
	29	60	30	12	6364221362
	33	68	34	4	27055611342
				8	63411255706, 66266622262, 62622266626, 63401257706
				12	66276620262, 62632264626
	37	76	38	12	6627420436464
	39	80	40	4	2606730325415
				8	2626622226626, 2242374761051
				12	2626422236626
	41	84	42	14	66236241236232, 62421763742122
#	43	88	44	16	272142741347210, 270577342005610,
					226302455363130, 224737056021530
	45	92	46	4	672066720627206 + 19 other possiblities
				8	672466360223642 + 43 other possiblities

Since for n = 45 the corresponding codes have a low minimum weight, we have not mentioned all 64 polynomials h(x).

The weight enumerators of the [2(n+1), n+1] double circulant codes have been calculated, up to n = 19, i.e. up to wordlength N = 40. Since the all-one vector

is a codeword, it is easily seen that the number of codewords of weight i, A_i, is equal to the number of codewords of weight N - i, i.e. $A_i = A_{N-i}$. Therefore we have only recorded the values of A_i for $i \leq n + 1$.

n = 3, h(x) = 2

$A_0 = 1$
$A_4 = 14$

n = 5, h(x) = 62

$A_0 = 1$
$A_4 = 15$
$A_6 = 32$

n = 9, h(x) = 662

$A_0 = 1$
$A_4 = 9$
$A_6 = 72$
$A_8 = 246$
$A_{10} = 368$

n = 11, h(x) = 2704

$A_0 = 1$
$A_8 = 759$
$A_{12} = 2576$

n = 13, h(x) = 66064

$A_0 = 1$
$A_8 = 546$
$A_{10} = 1456$
$A_{12} = 3549$
$A_{14} = 5280$

n = 15, h(x) = 23451

$A_0 = 1$
$A_4 = 15$
$A_8 = 450$
$A_{10} = 2560$
$A_{12} = 4193$
$A_{14} = 17920$
$A_{16} = 15258$

n = 15, h(x) = 26226

$A_0 = 1$
$A_4 = 15$
$A_6 = 30$
$A_8 = 450$
$A_{10} = 1990$
$A_{12} = 6113$
$A_{14} = 14620$
$A_{16} = 19098$

n = 15, h(x) = 27206

$A_0 = 1$
$A_8 = 360$
$A_{10} = 2080$
$A_{12} = 6608$
$A_{14} = 14560$
$A_{16} = 18318$

n = 15, h(x) = 27015

$A_0 = 1$
$A_8 = 300$
$A_{10} = 2560$
$A_{12} = 4928$
$A_{14} = 17920$
$A_{16} = 14118$

n = 17, h(x) = 670072
h(x) = 626322

$A_0 = 1$
$A_8 = 170$
$A_{10} = 2346$
$A_{12} = 8840$
$A_{14} = 29240$
$A_{16} = 56525$
$A_{18} = 67900$

n = 19, h(x) = 2365030

$A_0 = 1$
$A_8 = 285$
$A_{12} = 21280$
$A_{16} = 239970$
$A_{20} = 525504$

Appendix B. The minimum weights of all [2(n+1), n+1] double circulant codes which are the ternary images of extended cyclic codes over GF(9), up to n = 35

In this appendix a complete list of all [2(n+1), n+1] double circulant codes which are the ternary images of extended cyclic codes over GF(9) will be given for $n \leq 35$. That means that for all values of $n \leq 35$ all polynomials $h(x)$ which satisfy $h^2(x) + h(x) + 2 = \pm j(x)$, and their corresponding ternary double circulant codes have been determined. The theory of these codes has been discussed in chapter 4.

Using the computer the minimum weights of all these codes have been calculated. All polynomials $h(x)$ have been recorded, except when two polynomials $h_1(x)$ and $h_2(x)$ satisfied $h_1(x) = \pm h_2^3(x)$, $h_1(x) = \pm h_2(x^{-1})$ or $h_1(x) = \pm h_2(x) \pm j(x)$. In these cases only one of the two polynomials has been given, since obviously the corresponding codes are equivalent.

The toprow of the circulant matrix H, the polynomial $h(x)$, can be written as follows

$$h(x) = \sum_{i \in A} x^i + 2 \sum_{i \in B} x^i,$$

where A and B are two mutually disjoint subsets of $S = \{1, 2, \ldots, n-1\}$. In the following table the polynomials $h(x)$ will represented by the sets A and B. Furthermore when n is a prime, the set of nonresidues mod n will be denoted by R_1. The wordlength of the codewords is denoted by N, i.e. $N = 2n + 2$, the dimension by k, i.e. $k = n + 1$ and the minimum weight by d.

n	N	k	d	h(x)
5	12	6	4	$A = R_1$, $B = \emptyset$
7	16	8	6	$A = R_1$, $B = \emptyset$
17	36	18	10	$A = R_1$, $B = \emptyset$
19	40	20	12	$A = R_1$, $B = \emptyset$
25	52	26	4	$A = \{1, 4, 5, 6, 9, 11, 14, 16, 19, 20, 21, 24\}$, $B = \emptyset$
				$A = \{1, 4, 6, 9, 10, 11, 14, 15, 16, 19, 21, 24\}$, $B = \emptyset$
29	60	30	16	$A = R_1$, $B = \emptyset$
31	64	32	18	$A = R_1$, $B = \emptyset$
35	72	36	4	$A = \{3, 5, 6, 7, 10, 12, 13, 17, 19, 20, 24, 26, 27, 28, 31, 33, 34\}$, $B = \emptyset$
			6	$A = \{2, 3, 5, 7, 8, 10, 12, 13, 17, 18, 20, 22, 23, 27, 28, 32, 33\}$, $B = \emptyset$
			8	$A = \{2, 5, 7, 8, 10, 18, 20, 22, 23, 28, 32\}$,
				$B = \{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33\}$
			12	$A = \{6, 7, 19, 24, 26, 28, 31, 34\}$,
				$B = \{1, 3, 4, 5, 9, 10, 11, 12, 13, 15, 16, 17, 20, 25, 27, 29, 30, 33\}$

Appendix C. Description of the computer programs

In this appendix we shall briefly discuss the computer programs which we have made.

The computer program, which we have made in order to determine all polynomials $h(x)$, which satisfy $h^2(x) + h(x) + 2 = \pm j(x)$, is completely based on the algorithm described in §4.2.2. Therefore any further treatment of this program is superfluous.

The other programs have been made in order to determine the weight enumerator or the minimum weight of double circulant codes over GF(2) and GF(3).

In view of the structure of the generator matrix of these codes we needed a procedure which calculated for given k and n the sums of all linear combinations, consisting of k rows of an n×n circulant matrix. Of course this procedure had to be made in such a way that only one single sum of all the shifts of the same vector was calculated. Furthermore the number of different shifts of each vector had to be calculated (of course this number is mostly equal to n, but, sometimes, when n is not a prime this number is equal to a divisor of n).

In order to describe the procedure we have to introduce circular permutations (cf. [13, §2.1]). If letters $a_1, \ldots, a_n$ are arranged in a circle with a_1 following a_n, then any one of the linear sequences $a_2,a_3, \ldots, a_n,a_1$; $a_3, \ldots, a_n, a_1,a_2$; ... ; $a_n,a_1,a_2, \ldots, a_{n-1}$ may be thought of as determining the same circular sequence, called a circular permutation. With each circular permutation of length n we may associate a unique minimum period d such that the circular sequence consists of n/d repetitions of a sequence of d letters.

The recursive procedure which we have made generates, in a lexicographical way, for given k and n, all circular permutations consisting of k 1's and n-k 0's. Furthermore this procedure calculates the period of each circular permutation.

Let n be 12 and k equal to 3. Then all circular permutations consisting of 9 0's and 3 1's are, in lexicographical order, given by

111000000000	101010000000
110100000000	101001000000
110010000000	101000100000
110001000000	101000010000
110000100000	101000001000
110000010000	101000000100
110000001000	100100100000
110000000100	100100010000
110000000010	100100001000
	100010001000

All circular permutations, except the last one, have period 12; the period of the last one is equal to 4.

In our procedure the circular permutations are recursively built up and stored in an array B[0:n-1] of length n. One moment reflection shows that B[0] has to be 1 and B[n-1] has to be 0.

Let the rows of the n×n matrix H be indexed by 0, 1, ..., n-1. Then of course a circular permutation for which $B[i_l] = 1$, $1 \leq l \leq k$, corresponds with a linear combination consisting of the k rows of H indexed by $i_1, \ldots, i_k$.

We shall now give the procedure for the binary case.

Notation:

n: length of the circular permutation, i.e. the size of the square circulant matrix H;

k: the number of ones in the circular permutations;

B[0:n-1]: integer array, in which the circular permutations will be stored;

p: the number of ones which have already been stored in the array B;

j0: the highest index for which B[j0] = 1;

per: the period in the sequence B[0], ..., B[j];

s0[0:n-1]: an integer array which contains the linear combination of the rows of the matrix H which are indexed by the elements j for which $0 \leq j \leq j0$ and B[j] = 1, i.e. s0[0:n-1] contains a linear combination consisting of p rows of the matrix H;

pd: the period of the circular permutation B[0], ..., B[n-1];

ok: boolean variable;

sum(a,b): a procedure which calculates the binary sum of two vectors a and b;

ones(s0): a procedure which counts the number of ones in the array s0;

Bpos(upindex, length): a boolean procedure which gets the value true iff there exists j, upindex - length + 1 ≤ j ≤ upindex, such that B[j] = 1;

H(j): the j-th row of the matrix H;

NCD[1:n,1:n]: an integer matrix with NCD[i,j] = the number of linear combinations of weight j, consisting of i rows of the matrix H.

```
(A) procedure count(p, j0, s0, per, k);
    value p, j0, per, k; integer p, j0, per, k;
    integer array s0[*];
    begin integer j; integer array s1[0:n-1];
        if p < k
        then for j := j0 + 1 step 1 until n - 2
(B)          do if B[j mod per] = 0
                then B[j] := 0
                else begin
(C)                      if if n - (j ÷ per) * per ≥ per
                         then true
(D)                      else Bpos((n-1) mod per, n - 1 - j)
                         then begin
                                  B[j] := 1;
                                  s1   := sum(s0, H(j));
                                  count(p+1, j, s1, per, k);
                                  B[j] := 0
                              end;
(E)                      per := j + 1
                     end
        else begin
                 i := ones(s0);
(F)              if n mod per = 0 and not Bpos((n-1)mod per, n - 1 - j0)
                 then pd := per
                 else pd := n;
                 NCD[k,i] := NCD[k,i] + pd;
             end
    end procedure count;
```

We shall explain this procedure by giving the array B[0:n-1] in the situations (A), ..., (F).

Let in situation (A) the array B be given by

```
1101100 1101100 1101100 11......
        ———————          ↑     ↑
          per            j0    n-1
```

Then it is forbidden to place a 1 on position j0 + 1, since otherwise we can

obtain, by a cyclic shift over per positions to the left, a lexicographically greater circular permutation, i.e. a circular permutation which we have already constructed. This corresponds with situation (B).
Hence in situation (C) we have

```
1101100 1101100 1101100 110 .....
        ———————          ↑   ↑   ↑
          per            t   j   n-1
```

Here t = (j ÷ per) * per.
If n - t ≥ per then the circular permutation can always be constructed on. However if n - t < per, then it is only allowed to place a 1 on position j if the array B contains at least one 1 on the positions (j+1) mod per, ..., (n-1) mod per. Otherwise we can obtain again by cyclic shifting a lexicographically greater circular permutation. This corresponds with (D).
When we arrive in situation (E) the 1 on position j has been changed into an 0. That means that the period per becomes equal to j + 1, as illustrated in the following example

```
1101100 1101100 1101100 1100 ...
└———————————————————————————┘
            per
```

After completing a circular permutation, i.e. when p = k, the variable per is equal to the period of the circular permutation iff per | n and B[j] = 0 for (j0+1) mod per ≤ j ≤ (n-1) mod per. This corresponds with (F).

We have executed our programs on the Burroughs B7700. On this computer each word consists of 48 bits. A bit, the basic unit of hardware in the computer, can be considered as a variable with only two possible values: 0 and 1. A word therefore can be considered as an "array row" consisting of 48 "variables" each "variable" capable of storing the values 0 or 1. The Burroughs B7700 provides the means by which to the individual bits of any word may be referenced directly. It is called partial word notation.
We have made use of this partial word notation. In the binary case one needs one single word to store a vector of length n, n ≤ 48. In fact we have replaced in our programs the arrays B, s0 and s1 by words. Using partial word operations we needed only one single word to store the circulant matrix H. The addition operation was replaced by logical operations on the words. Due to this partial word operations the execution time could be reduced with at least a factor n.

In the ternary case we have also been able to use this partial word notation. In this case we needed two words to store a ternary vector, namely one word to store the 1's and 0's and another word to store the -1's and 0's. Also in this case we have replaced the addition operations by logical operations, which were of course in the ternary case more complicated than in the binary case.
To reduce the computation time still more we have, in the binary case, made use of some of the theory developed in [11].
In order to give an indication of the computation time we shall give four examples.
The minimum weight of the binary [88,44,16] respectively [92,46,8] double circulant code could be determined in 108 respectively 0.3 seconds.
The minimum weight of the ternary [64,32,18] respectively [72,36,12] code could be determined in 1256 respectively 4.5 seconds.

REFERENCES

[1] F.J.MacWilliams and N.J.A.Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, 1978.

[2] J.H.van Lint, Coding Theory, Springer Lecture Notes in Mathematics, No 201, Springer-Verlag, Berlin, 1971.

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

[4] C.L.Chen, W.W.Peterson and E.J.Weldon, Jr., Some Results on Quasi-Cyclic Codes, Info. and Control, 15, 1969, 407-423.

[5] S.E.Tavares, V.K.Bhargava and S.G.S.Shiva, Some Rate-p/(p+1) Quasi-Cyclic Codes, IEEE. Trans. Information Theory, vol.IT-20 , 1974, 133-135.

[6] J.M.Stein and V.K.Bhargava, Equivalent Rate-½ Quasi-Cyclic Codes, IEEE Trans. Information Theory, vol. IT-21, 1975, 588-589.

[7] V.K.Bhargava, S.E.Tavares and S.G.S.Shiva, Difference Sets of the Hadamard Type and Quasi-Cyclic Codes, Info. and Control,26, 1974, 341-350.

[8] V.K.Bhargava and J.M.Stein, (v,k,λ) Configurations and Self-Dual Codes, Info. and Control, 28, 1975, 352-355.

[9] T.Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate ½, IEEE Trans. Information Theory, 20, 1974, 679.

[10] R.A.Jenson, A Double Circulant Presentation of Quadratic Residue Codes, IEEE Trans. Information Theory, vol. IT-26, 1980, 223-227.

[11] M.Karlin, New binary coding results by circulants, IEEE Trans.Information Theory, 15, 1969, 81-92.

[12] V.Pless, Symmetry codes over GF(3) and new 5-designs, J.Combinatorial Theory, 12, 1972, 119-142.

[13] M.Hall, Jr., Combinatorial Theory, John Wiley&Sons, Inc., 1967.

[14] Susan Geldof en Frans Beenker , Gewichtsbepaling in Symmetry codes, unpublished manuscript.

[15] C.L.Mallows, V.Pless and N.J.A.Sloane, Self-dual codes over GF(3), SIAM J. Applied Math., 31, 1976, 649-666.

[16] Robert Calderbank, A square root bound on the minimum weight in quasi-cyclic codes, to appear.

[17] M.Karlin, V.K.Bhargava, and S.E.Tavares, A Note on Extended Quaternary Quadratic Residue Codes and Their Binary Images, Info. and Control, 38, 1978, 148-153.

[18] F.J.MacWilliams, A.M.Odlyzko, N.J.A.Sloane and H.N.Ward, Self-dual codes over GF(4), J.Combinatorial Theory, 25A, 1978, 288-318.

[19] J.H.van Lint and F.J.MacWilliams, Generalized Quadratic Residue Codes, IEEE Trans. Information Theory, IT-24, 1978, 730-737.

Index

alphabet 1
automorphism 2

bound
  Gilbert-Varshamov 6

code
  cyclic 2
  double circulant 4
  dual 1
  equivalent 2
  error-correcting 1
  extended 2
  Golay 23
  Hamming 22
  linear 1
  quadratic residue 7
  self-dual 2
  symmetry 9
codeword 1
configuration
  (v,k,λ) 6

decoding
  double circulant code 6
difference set 6
dimension 1
distance
  Hamming 1
  minimum distance 1

encoding
  double circulant code 3

field, finite
  Galois 1
feasible 20, 44

group
  automorphism group 2
  PSL(2,q) 7

ideal
  principal 2
idempotent 24
image
  binary 16
  ternary 41
innerproduct 1

length
  of a codeword 1

nonresidue 6

mapping
  GF(4) into binary 16
  GF(9) into ternary 41
matrix
  circulant 3
  generator 2
  Hadamard 61
  monomial 2
  Paley 16
  parity check 2

order of q mod m 21
overall parity check 2

polynomial
  generator 2

quadratic residue 6

support 5

theorem
  Assmus-Mattson 5
  Gleason-Prange 7
  Mallows-Sloane 39, 67
  Perron 54

weight
  Hamming 1
  minimum 1
weight enumerator 2