



Deanship of Graduate Studies and Scientific Research

Master Program of Mathematics

On The Automorphism Groups of Some Linear
Codes

By

Nisreen Mohammad Nashash

Supervised by

Dr. Mahmoud Shalalfeh

This thesis is submitted in partial fulfillment of the requirement
for the degree of Master of Mathematics, Faculty of Graduate
Studies, Hebron University, Palestine.

2019

On The Automorphism Groups Of Some Linear Codes

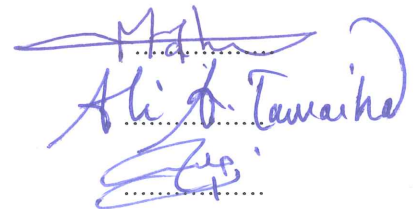
By
Nisreen Mohammad Nashash

This thesis was defended successfully on 30/4/2019 and approved by:

Committee Members:

- | | |
|-------------------------|-------------------|
| • Dr. Mahmoud Shalalfeh | Supervisor |
| • Dr. Ali Altawaiha | Internal Examiner |
| • Dr. Iyad Hreebat | External Examiner |

Signature


The signature block contains three handwritten signatures in blue ink. The first signature is for the Supervisor, the second is for the Internal Examiner (Ali D. Tawaiha), and the third is for the External Examiner. Each signature is written over a dotted line.

Abstract

The Automorphism group of a linear code is a very useful concept in determining the structure of the code, computing weight distribution of a code, classifying codes as well as devising decoding algorithm. In this thesis we study the automorphism group of Hamming codes, Cyclic codes, Reed-Muller codes, Generalized Reed-Muller codes, Affine Invariant codes, and primitive narrow sense BCH codes. In fact, our work is a survey of the main results of the automorphism groups of these codes.

ملخص الرسالة

تعد زمر التشاكل الداخلي للشفيرة الخطية مفهوما مفيدا للغاية في تحديد هيكل الشيفرة الخطية (الكود) و حساب توزيعات الوزن لها وكذلك في تصنيف الشيفرات الخطية و أيضا وضع خوارزمية فك التشفير. في هذه الأطروحة تم دراسة زمر التشاكل الداخلي لبعض الشيفرات الخطية المهمة.

Dedications

To my dearest people, who believed in me and led me to the road of success, to my parents, my husband Mohammad, my children Ahmad, Yara and Shereen, my brothers, and sisters, also I'll never forget my best friends. All dears, to the wonder of your hearts I send this dedication.

Declaration

I declare that the master thesis entitled On The Automorphism Groups Of some Linear codes is my own work, and hereby certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgment is made in the text.

Nisreen Nashash

Signature: _____

Date: _____

Acknowledgements

I would like to thank my supervisor Dr. Mahmoud Shalalfa for having introduced me to this fascinating and beautiful subject. His enthusiasm, his wonderful explanations and guidance have given me a new view on what mathematics means. My deepest thanks to him.

I would like also to thank Dr. Ali Altawaiha and Dr. Iyad Hreebat for encouragement, support, interest and valuable hints.

I am grateful to Hebron University, I wish to pay my great appreciation to all respected Prof's at the department of mathematics.

Finally I would like to say that this work would not have been possible without the constant support of my husband and my family.

Introduction

Historical Background

The history of data-transmission codes began in 1948 with the publication of a famous paper by Claude Shannon 'A Mathematical Theory of Communication' that give birth to the twin disciplines of information theory and coding theory. Shannon showed that associated with any communication channel or storage channel is a number C (measured in bits per second), called the capacity of the channel, which has the following significance: Whenever the information transmission rate R (in bits per second) required of a communication or storage system is less than C then, by using a data-transmission code, it is possible to design a communication system for the channel whose probability of output error is as small as desired. Shannon, however, did not tell us how to find suitable codes; his contribution was to prove that they exist and to define their role.

An interesting concept in coding theory is to find explicit codes which reach the limits predicted by Shannon's original work. From that date of Shannon's paper, many constructions of 'good codes' have been done using various techniques from a surprisingly wide range of pure mathematics: linear algebra, the theory of fields and algebraic geometry.

Throughout the 1950s, much effort was devoted to finding explicit constructions for classes of codes. The first block codes were introduced in 1950 when Hamming described a class of single-error-correcting block codes and he published what is now known as Hamming code, which remains in use in many applications today.

In 1957, Among the first codes used practically were the cyclic codes which were generated using shift registers. It was quickly noticed by Prange that the cyclic codes have a rich algebraic structure, the first indication that algebra would be a valuable tool in code design.

In the 1960s, the major advances came in 1960 when Hocquenghem and Bose and Ray-Chaudhuri found a large class of multiple-error-correcting codes (the BCH codes). The discovery of BCH codes led to a search for practical methods of designing the hardware or software to implement the encoder and decoder. In the same year independently, Reed, Solomon and Arimoto found a related class of codes for nonbinary channels. Concatenated codes were introduced by Forney (1966), later Justesen used the idea of a concatenated code to devise a completely constructive class of long block codes with good performance.

During the 1970s, these two avenues of research began to draw together in some ways and to diverge further in others. Meanwhile, Goppa (1970) defined a class of codes that is sure to contain good codes, though without saying how to identify the good ones.

Not only has coding theory helped to solve problems of vital importance in the world outside mathematics, it also has enriched other branches of mathematics, with new problems as well as new solutions.

Outline of the Chapters

Chapter 1: This chapter includes important concepts from coding theory and field theory that are crucial to the rest of the thesis. Important concepts such as some definitions related to coding theory like binary codes, generating and parity-check matrices, some lower and upper bounds on the parameters of codes, how to construct new codes from old ones, examples of linear codes such as cyclic codes, Hamming codes and some basic codes, finally at the rest of this chapter we study a small portion of field theory, which began with the work of Carl Friedrich Gauss (1777-1855) and Evariste Galois (1811-1832). For a more complete introduction to finite field, we find it in [35].

Chapter 2: This chapter consist of four sections, in the first section we explain the concept of automorphism groups of linear codes. We define the concepts of code equivalence, permutation matrix, the automorphism of the dual code and its relation with the automorphism of group of the code and examples of automorphism group of some codes. In the second section of this chapter we study the automorphism groups of binary codes, for example, we notice that the automorphism group of binary Hamming code of length $n = 2^m - 1$ is isomorphic to the general linear group $GL_m(2)$. In the third section we concentrate on the automorphism groups of cyclic codes and we introduce some interesting theorems which described the automorphism groups of these codes. In the last section we discuss the permutation automorphism groups of q -ary Hamming codes and we conclude that its automorphism groups is isomorphic to the unitriangular group $UT_m(q)$.

Chapter 3: This chapter consists of four sections. In the first section we introduce the

concepts of Reed-Muller codes, while in the second section we give the automorphism groups of these codes. Later in the third section we give the definition of Generalized Reed-Muller codes and some of their relatives. Finally in the fourth section we discuss the automorphism groups of Generalized Reed-Muller codes, for example we see that the automorphism groups of $q - ary$ Reed-Muller code of order $m(q - 1) - v$ is the general linear group $GL(m, q)$.

Chapter 4: Here we introduce the concept of affine invariant codes of length p^m acting on \mathbb{F}_{p^m} . This class of codes includes codes of great interest such as extended narrow-sense BCH-codes. We give some results that are specially important when the alphabet is an extension field. Finally, in the last section we give the automorphism groups of extended narrow-sense BCH-codes defined over any extension field.

On The Automorphism Groups Of Some Linear Codes

By
Nisreen Mohammad Nashash

This thesis was defended successfully on 30/4/2019 and approved by:

Committee Members:

Signature

- | | | |
|-------------------------|-------------------|-------|
| • Dr. Mahmoud Shalalfeh | Supervisor | |
| • Dr. Ali Altawaiha | Internal Examiner | |
| • Dr. Iyad Hreebat | External Examiner | |

Contents

Chapter 1. Preliminaries	2
1.1 Notions about linear codes	2
1.2 Some Bounds On Codes	5
1.3 Modifying Codes	6
1.4 Important Classes of Linear Codes	11
1.5 Finite Fields	17
1.6 General Linear Group Over Finite Field	25
Chapter 2. The Automorphism Groups of Linear codes	27
2.1 Examples	29
2.2 Automorphism group of binary codes	31
2.3 Automorphism Groups of Cyclic Codes	37
2.4 On Permutation Automorphism groups of q -ary Hamming Codes . .	39
Chapter 3. The Automorphism groups of Reed-Muller And Generalized Reed-Muller Codes	44
3.1 Some Concepts of Reed-Muller Codes	44
3.2 Automorphism groups of Reed-Muller codes	49
3.3 Generalized Reed- Muller Codes	52
3.4 The Automorphism groups of GRM-codes	58
Chapter 4. The Automorphism Groups of BCH Codes	65
4.1 Affine-invariant codes	65

4.2	The Automorphism Groups of Affine-Invariant Codes	70
4.3	BCH codes	71
4.4	The Automorphism Groups of Primitive Narrow-Sense BCH-Codes . .	75

Preliminaries

In this chapter, we will introduce the objects which will appear in the thesis, putting in evidence some useful properties and relations.

1.1 Notions about linear codes

In this section we give basic notions and definitions related to linear codes.

Definition 1.1. [39] *let \mathbb{F}_q be a finite field and \mathbb{F}_q^n is an n -dimensional vector space over \mathbb{F}_q . We define a q -ary $[n, k]$ linear code to be a k -dimensional linear subspace of \mathbb{F}_q^n . The parameter n is called the length of the code and k the dimension of the code. The elements of the code are called codewords.*

A binary linear code C of length n is a set of binary n -tuples such that the componentwise modulo 2 sum of any two codewords is contained in C .

Example 1.2. *The following are linear codes:*

- (1) $C = \{(\lambda, \lambda, \dots, \lambda) : \lambda \in \mathbb{F}_q\}$. *This code is often called a repetition code*
- (2) $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

There are two standard ways to describe a k -dimensional linear subspace: one by means of k -independent basis vectors, the other uses $n - k$ linearly independent equations.

Definition 1.3. [3] Let C be an $[n, k]$ linear code over \mathbb{F}_q . We define a generator matrix \mathbf{G} of C to be a $k \times n$ matrix whose rows form a basis of C . A parity check matrix \mathbf{H} of C is an $(n - k) \times n$ matrix over \mathbb{F}_q with rank $n - k$ which satisfies: For every $\mathbf{c} \in \mathbb{F}_q^n$, $\mathbf{c} \in C \Leftrightarrow \mathbf{H}\mathbf{c}^T = \mathbf{0}$.

The generator matrix of an $[n, k]$ linear code is said to be in the standard (systematic) form if it is of the form $(\mathbf{I}_k \mid \mathbf{A})$, where \mathbf{A} is a $k \times (n - k)$ matrix. The corresponding parity check matrix in the standard form is of the shape $(-\mathbf{A}^T \mid \mathbf{I}_{n-k})$.

Example 1.4. The matrix $G = [I_4 \mid A]$, where

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

is a generator matrix in standard form for a $[7, 4]$ binary code that we denote by \mathcal{H}_3 , and with a parity check matrix

$$H = \left[\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right]$$

This code is called the $[7, 4]$ Hamming code.

Theorem 1.5. [1] Let $C \subset \mathbb{F}_q^n$ be a linear code of type $[n, k]_q$ with generator matrix G and parity check matrix H . Then $c \in C$ if and only if $cH^T = \mathbf{0}$.

Any generator matrix can be transformed to standard form by elementary row operations and column permutation.

Let $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathbf{v} = (v_1, \dots, v_n)$ be vectors in \mathbb{F}_q^n , we define the inner product as $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^n u_i v_i$.

Definition 1.6. [3] Let C be an $[n, k]$ linear code with parity check matrix \mathbf{H} . The $[n, n - k]$ linear code generated by \mathbf{H} is called the dual code of C and denoted C^\perp . The hull of the code is defined to be $C \cap C^\perp$ and denoted by $\mathcal{H}(C)$.

Example 1.7. If C is a binary $[5, 3]$ code with generator matrix,

$$G = \left[\begin{array}{ccccc} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array} \right]$$

then we can reduce G to standard form as

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

And the parity-check matrix for C is

$$H = [A^T | I_k] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

The elements of the dual code C^\perp are linear combinations of the rows of H ,

$$C^\perp = \{00000, 10010, 11101, 01111\}.$$

The code C is called weakly self-dual if $C \subseteq C^\perp$ and is called self-dual if $C = C^\perp$. Suppose C is an $[n, k]$ self-dual code, then n must be even and it must satisfy $n = 2k$. In case of weakly self-dual $n > 2k$. Note that, in both cases, self-dual and weakly self-dual, the code is equal to its hull.

Definition 1.8. [13] Let $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathbf{v} = (v_1, \dots, v_n)$ be vectors in \mathbb{F}_q^n then we define the Hamming distance d_H between \mathbf{u} and \mathbf{v} as follows: $d_H(\mathbf{u}, \mathbf{v}) = \#\{i : u_i \neq v_i\}$. Hamming weight of a vector \mathbf{u} is $wt(\mathbf{u}) = d_H(\mathbf{u}, \mathbf{0})$.

Thus the Hamming distance represents the number of coordinates that they differ between the two vectors or codeword where Hamming weight is the number of coordinates that differ from zero in the vector. Thus $d_H(\mathbf{u}, \mathbf{v}) = wt(\mathbf{u} - \mathbf{v})$. Thus we define the minimum distance d of a code C as follows:

Definition 1.9. [13] The minimum distance d of a code C is defined as follows

$$d = \min\{d_H(u, v) : u, v \in C, u \neq v\}.$$

Theorem 1.10. [3] The minimum distance of a linear code C is equal to the minimum weight of C .

Proof. Since C is linear with x and y in C also $x - y$ is in C . The theorem now follows from the two observations:

$$\begin{aligned} d(x, y) &= d(x - y, 0) = wt(x - y), \\ wt(x) &= d(x, 0) \end{aligned}$$

which state that the distance between any two distinct codewords is equal to the weight of some nonzero codeword and vice versa. \square

Example 1.11. The binary linear code $C = \{0000, 1000, 0100, 1100\}$, then we have

$$\begin{aligned} wt(1000) &= 1, \\ wt(0100) &= 1, \\ wt(1100) &= 2. \end{aligned}$$

Hence $d(C) = 1$.

Definition 1.12. [34] Let C be an $[n, k]_q$ code and let A_i be the number of words of C of weight i . The sequence $\{A_i\}_0^n$ is called **the weight distribution** of C .

Example 1.13. If C is a binary code with generator matrix

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Then the elements of C are linear combinations of the rows of G

$$C = \{000000, 110000, 111100, 110011, 001100, 001111, 000011, 111111\}.$$

The weight distribution of C is $A_0 = A_6 = 1$ and $A_2 = A_4 = 3$.

Definition 1.14. Let C be a linear code of length n over \mathbb{F}_q , and let $u \in \mathbb{F}_q^n$ be any vector of length n ; we define the coset of C determined by u to be the set

$$C + u = \{v + u : v \in C\} (= u + C).$$

1.2 Some Bounds On Codes

In this section we introduce some important bounds of a code.

1.2.1 The Singleton Bound

Theorem 1.15. [9] (*Singleton Bound*) For any $[n, k, d]$ -linear code over \mathbb{F}_q we have $d \leq n - k + 1$. An $[n, k, d]$ -linear code is called *Maximum Distance Separable, MDS*, if $d = n - k + 1$.

1.2.2 The Sphere Packing Bound (Hamming Bound)

Let w be a codeword of an $[n, k, d]$ code defined over \mathbb{F}_q . A sphere of radius t and center w in \mathbb{F}_q^n is the set of words in \mathbb{F}_q^n at Hamming distance t or less from w . The number of words in the sphere is given by

$$V_q(n, t) = \sum_{i=0}^t \binom{n}{i} (q-1)^i$$

Theorem 1.16. [3] (*Sphere-Packing Bound*) For any $[n, k, d]$ linear code over \mathbb{F}_q we have:

$$V_q(n, \lfloor \frac{d-1}{2} \rfloor) \leq q^{n-k}$$

An $[n, k, d]$ linear code is called perfect if it satisfies the upper limit of the inequality, i.e., $V_q(n, \lfloor \frac{d-1}{2} \rfloor) = q^{n-k}$.

Definition 1.17. [9] Let n, d be positive integers with $d \leq n$. Then the number $A_q(n, d)$ denote the maximum number of codewords in a code over \mathbb{F}_q of length n and distance d . This maximum, when restricted to linear code, is denoted by $B_q(n, d)$.

Theorem 1.18. Let q be a prime. q -ary codes which satisfy the sphere packing bound have dimension q^r , $r \in \mathbb{Z}^+$

1.2.3 The Gilbert- Varshamov Bound

Theorem 1.19. [5] (*The Gilbert- Varshamov Bound*) Let n, k and d be integer satisfying $2 \leq d \leq n$ and $1 \leq k \leq n$. If

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k},$$

then there exist an $[n, k, d]$ -linear code over \mathbb{F}_q with minimum distance at least d .

1.3 Modifying Codes

Given C an $[n, k, d]$ -linear code we show how to construct other codes from C . The resulting codes sometimes are great importance in many places.

1.3.1 Punctured Codes

Let C be an $[n, k]$ linear code over \mathbb{F}_q . We puncture C in the coordinate i by deleting the coordinate i in all codewords of C . The resulting code is called the punctured code of C at coordinate i and denoted C^* . The generator matrix of C^* is obtained from the generator matrix of C by deleting column i . Puncturing can be done in a set of coordinates $\{i_1, \dots, i_t\}$ with $t < n$. Sometimes puncturing is done in such a way that we preserve the length of the code. Thus we replace coordinate i by zero in all codewords instead of deleting the coordinate. The following theorem gives the length and the minimum distance of the punctured code.

Theorem 1.20. [3] *Let C be an $[n, k, d]$ linear code over \mathbb{F}_q and let C^* be the punctured code at coordinate i then we have two cases*

- (i) *if $d > 1$, C^* is an $[n-1, k, d^*]$ linear code where $d^* = d-1$ if C has a minimum weight codeword with a nonzero i th coordinate; otherwise $d^* = d$.*
- (ii) *if $d = 1$, C^* is an $[n-1, k, 1]$ linear code if C has no codeword of weight 1 whose nonzero entry in coordinate i ; otherwise, if $k > 1$, C^* is an $[n-1, k-1, d^*]$ code with $d^* \geq 1$.*

Example 1.21. *Let C be the $[5, 2, 2]$ binary code with generator matrix*

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Let C_1^ and C_5^* be the code C punctured on coordinate 1 and 5, respectively. They have generator matrices*

$$G_1^* = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad G_5^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

So C_1^ is $[4, 2, 1]$ code, while C_5^* is a $[4, 2, 2]$ code.*

1.3.2 Shortened Codes

Theorem 1.22. [5] (Subcodes) *Suppose there is an $[n, k, d]$ linear code over \mathbb{F}_q . Then there exists an $[n, k-r, d]$ linear code over \mathbb{F}_q for any $1 \leq r \leq k-1$.*

Let C be an $[n, k, d]$ code over \mathbb{F}_q and let T be any set of t coordinates. Consider the set $C(T)$ of codewords which are $\mathbf{0}$ on T ; this set is a subcode of C . Puncturing $C(T)$ on T gives a code over \mathbb{F}_q of length $n - t$ called the code shortened on T and denoted C_T .

There is a strong connection between the punctured and shortened codes that is captured by the following theorem.

Theorem 1.23. [3] *Let C be an $[n, k, d]$ code over \mathbb{F}_q and let T be a set of t coordinates then we have*

- (1) $(C^\perp)_T = (C^*)^\perp$ and $(C^\perp)^* = (C_T)^\perp$, and
- (2) if $t < d$, then C^* and $(C^\perp)_T$ have dimensions k and $n - t - k$, respectively;
- (3) if $t = d$ and T is the set of coordinates where a minimum weight codeword is nonzero, then C^* and $(C^\perp)_T$ have dimensions $k - 1$ and $n - d - k + 1$, respectively.

Example 1.24. *Let C be the $[6, 3, 2]$ binary code with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

C^\perp is also a $[6, 3, 2]$ code with generator matrix

$$G^\perp = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

If the coordinates are labeled $1, 2, \dots, 6$, let $T = \{5, 6\}$. Generator matrices for the shortened code C_T and punctured code C^T are

$$G_T = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad G^* = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Shortening and puncturing the dual code gives the code $(C^\perp)_T$ and $(C^\perp)^T$, which have generator matrices

$$(G^\perp)_T = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \quad (G^\perp)^* = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

From the generator matrices G_T and G^T , we find that the dual of C_T and C^T have generator matrices

$$(G_T)^\perp = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (G^*)^\perp = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

Thus for this example we have shown that $(C^\perp)_T = (C^*)^\perp$ and $(C^\perp)^* = (C_T)^\perp$.

1.3.3 Extended Codes

A linear code C can be extended to other linear codes of bigger length by adding new coordinates. There are many ways to do that but the most common way is to add new coordinate in such a way all codewords sum up to zero. We denote the extended code by \widehat{C} .

$$\widehat{C} = \{(c_1, c_2, \dots, c_{n+1}) : (c_1, c_2, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}.$$

If C is an $[n, k, d]$ binary code, then the extended code \widehat{C} contains only even weight codewords and it has parameters $[n + 1, k, \widehat{d}]$ where $\widehat{d} = d$ if d is even and equals $d + 1$ if d is odd. The generator matrix of \widehat{C} can be obtained from the generator matrix of C by adding extra column to the end so that the sum of each row is zero.

Example 1.25. *If we puncture the binary code C with generator matrix*

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

on its last coordinate and then extend (on the right), the resulting code has generator matrix

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

In this example, our last step was to extend a binary code with only even weight codewords. The extended coordinate was always $\mathbf{0}$. In general, that is precisely happens when we extend a code that has only even-like codewords.

1.3.4 Direct Sums

For $i \in \{1, 2\}$ let C_i be an $[n_i, k_i, d_i]$ code, both over the same finite field \mathbb{F}_q . Then their direct sum is the $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$ code.

$$C_1 \oplus C_2 = \{(c_1, c_2) | c_1 \in C_1, c_2 \in C_2\}.$$

It has generator matrix G_i and parity check matrix H_i , where

$$G_1 \oplus G_2 = \begin{pmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{pmatrix}, \quad H_1 \oplus H_2 = \begin{pmatrix} H_1 & \mathbf{0} \\ \mathbf{0} & H_2 \end{pmatrix}$$

are generator matrix and parity check matrix for $C_1 \oplus C_2$.

Example 1.26. *Let*

$$C_1 = \{000, 110, 101, 011\}$$

be a binary $[3, 2, 2]$ linear code, and let

$$C_2 = \{0000, 1111\}$$

be a binary $[4, 1, 4]$ linear code. Then

$$C_1 \oplus C_2 = \{0000000, 1100000, 1010000, 0110000, 0001111, 1101111, 1011111, 0111111\}$$

is a binary $[7, 3, 2]$ linear code.

The disadvantage of the direct sum construction is that the distance is not increased at all. In the next construction, this is improved:

1.3.5 The $(u|u+v)$ Construction

Let C_i be $[n, k_i, d_i]$ linear codes of the same length over \mathbb{F}_q , $i \in \{1, 2\}$, $(u|u+v)$ construction will give the linear code

$$C = \{(u, u+v) : u \in C_1, v \in C_2\}.$$

The code C is $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$ linear code. [3] Its generator and check matrices are

$$\begin{pmatrix} G_1 & G_1 \\ 0 & G_2 \end{pmatrix}, \quad \begin{pmatrix} H_1 & 0 \\ -H_1 & H_2 \end{pmatrix}$$

respectively.

Example 1.27. *Let*

$$C_1 = \{000, 110, 101, 011\}$$

be a binary $[3, 2, 2]$ linear code and let

$$C_2 = \{000, 111\}$$

be a binary $[3, 1, 3]$ linear code. Then the $(u|u+v)$ construction is

$$C = \{000000, 110110, 101101, 011011, 000111, 110001, 101010, 011100\}$$

is a binary $[6, 3, 3]$ linear code.

1.4 Important Classes of Linear Codes

In this section we introduce important types of codes that are extensively used in practice, that is due to their structures, they have very nice properties, very easy encoding and in principle quite easy decoding.

1.4.1 Some Basic Linear Codes

Recall that a linear code with length n over \mathbb{F}_q is a vector subspace of \mathbb{F}_q^n . We begin with some simple examples of binary linear codes.

Definition 1.28. [25]

- (i) An $[n, 0]$ code, consisting of just the all-zero codeword, called the no information code.
- (ii) The repetition code $C = \{\underbrace{(x, \dots, x)}_n \mid x \in \mathbb{F}_q\}$ is a linear code. So the binary repetition code is an $[n, 1, n]_2$ code consisting of the two vectors $\mathbf{0}$ and $\mathbf{1}$
- (iii) An $[n, n-1]$ code, consisting of all vectors $\{c_0, c_1, \dots, c_{n-1}\}$ such that $\sum_i c_i = 0$, called the single parity-check code.
- (iv) An $[n, n]$ code, consisting of all vectors of length n , called the no parity code.

Definition 1.29. [25] A code C is called even if all of its codewords have even weight: $wt(c) \equiv 0 \pmod{2}$ for all $c \in C$.

Proposition 1.30. If $d \geq 2$ is an even integer and a linear $[n, k, d]$ code exists, then there exists an even $[n, k, d]$ linear code.

Proof. If C is a linear $[n, k, d]$ code, the code produced by puncturing C in one coordinate has parameters $[n-1, k, d \text{ or } d-1]$. Adding a parity check bit to all codewords, we obtain an even $[n, k, d]$ code. \square

Corollary 1.31. If $d \geq 2$ is even and even linear $[n, k, d]$ codes do not exist, then no $[n, k, d]$ code exist.

Definition 1.32. [25] (The binary parity check code) This is an $[n, n-1, 2]_2$ code consists of all vectors in \mathbb{F}_2^n of even Hamming weight.

1.4.2 Cyclic codes

An algebraic correspondence

Definition 1.33. [39] An $[n, k, d]_q$ linear code C is **cyclic** if the cyclic shift of a word is also a word, i.e.

$$(c_0, \dots, c_{n-1}) \in C \implies (c_{n-1}, c_0, \dots, c_{n-2}) \in C.$$

To describe algebraic properties of cyclic codes, we need to introduce a new structure. We consider the univariate polynomial ring $\mathbb{F}_q[x]$ and the ideal $I = \langle x^n - 1 \rangle$. We denote by R the ring $\mathbb{F}_q[x]/I$. We construct a bijective correspondence between the vectors of $(\mathbb{F}_q)^n$ and residue classes of polynomials in R :

$$\mathbf{v} = (v_0, \dots, v_{n-1}) \longleftrightarrow v_0 + v_1x + \dots + v_{n-1}x^{n-1}.$$

We can view linear codes as subsets of the ring R , thanks to the correspondence below. The following theorem points out the algebraic structure of cyclic codes.

Theorem 1.34. [9] Let C be an $[n, k, d]$ code, then C is cyclic if and only if C is an ideal of R .

Proof. Multiplying by x modulo $x^n - 1$ corresponds to a cyclic shift:

$$\begin{aligned} (c_0, c_1, \dots, c_{n-1}) &\rightarrow (c_{n-1}, c_0, \dots, c_{n-2}) \\ x(c_0 + c_1x + \dots + c_{n-1}x^{n-1}) &= c_{n-1} + c_0x + \dots + c_{n-2}x^{n-2}. \end{aligned}$$

□

Since R is a principal ideal ring, if C is not trivial there exists a unique monic polynomial $g(x)$ that generates C . We call $g(x)$ the generator polynomial of C . Note that $g(x)$ divides $x^n - 1$ in $\mathbb{F}_q[x]$. If the dimension of the code C is k , the generator polynomial has degree $n - k$. A generator matrix can be given by using the coefficients of the generator polynomial $g(x) = \sum_{i=0}^{n-k} g_i x^i$:

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix} \quad (1.1)$$

Moreover, a polynomial f in R belongs to the code C if and only if there exists q in R such that $qg = f$. Since the generator polynomial is a divisor of $x^n - 1$ and is unique, the parity-check polynomial of C is well defined as the polynomial $h(x)$ in R such that $h(x) = (x^n - 1)/g(x)$. The parity-check polynomial provides a simple way to check if an $f(x)$ in R belongs to C , since

$$f(x) \in C \Leftrightarrow f(x) = q(x)g(x) \Leftrightarrow f(x)h(x) = q(x)(g(x)h(x)) = 0 \text{ in } R.$$

Proposition 1.35. [9] *Let $h(x)$ and $g(x)$ be, respectively, the parity-check and the generator polynomial of the cyclic code C . The dual code C^\perp is cyclic with generator polynomial*

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

Proof. See [9]. □

Zeros of cyclic codes

Cyclic codes of length n over \mathbb{F}_q are generated by divisors of $x^n - 1$. Let

$$x^n - 1 = \prod_{j=1}^r f_j, \quad f_j \text{ irreducible over } \mathbb{F}_q.$$

Then to any cyclic code of length n over \mathbb{F}_q there corresponds a subset of $\{f_j\}_{j=1}^r$. A very interesting case is when $\gcd(n, q) = 1$. Let $\mathbb{F} = \mathbb{F}_{q^m}$ be the splitting field of $x^n - 1$ over \mathbb{F}_q and let α be a primitive n th root of unity over \mathbb{F}_q . Then $x^n - 1$ factors completely over \mathbb{F}_{q^m} as

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i).$$

In this case the generator polynomial of C has powers of α as roots. We remember that, given $g \in \mathbb{F}_q[x]$, if $g(\alpha^i) = 0$ then $g(\alpha^{qi}) = 0$.

Definition 1.36. [39] *Let C be an $[n, k, d]$ cyclic code with generator polynomial g_C , with $\gcd(n, q) = 1$. The set*

$$S_{C, \alpha} = S_C = \{i_1, \dots, i_{n-k} \mid g_C(\alpha^{i_j}) = 0, j = 1, \dots, n - k\}$$

is called the complete defining set of C .

Definition 1.37. [5] *The cyclotomic coset of q modulo n containing i is:*

$$C_i = \{(i \cdot q^j \pmod{n}) \in \mathbb{Z}_n : j = 0, 1, \dots\}.$$

A subset $\{i_1, \dots, i_t\}$ of \mathbb{Z}_n is called a complete set of representatives of cyclotomic cosets of q modulo n .

We can collect the integers modulo n into q -cyclotomic classes C_i :

$$\{0, \dots, n-1\} = \bigcup C_i, \quad C_i = \{i, qi, \dots, q^r i\},$$

where r is the smallest positive integer such that $i \equiv iq^r \pmod{n}$. So the complete defining set of a cyclic code is collection of q -cyclotomic classes. So we fix a primitive n th root of unity α and we write $S_{C,\alpha} = S_C$. A cyclic code is defined by its complete defining set, since

$$C = \{c \in R \mid c(\alpha^i) = 0, \quad i \in S_C\} \Leftrightarrow g_C = \prod_{i \in S_C} (x - \alpha^i).$$

By this fact it follows that

$$H = \begin{pmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \dots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \dots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_{n-k}} & \alpha^{2i_{n-k}} & \dots & \alpha^{(n-1)i_{n-k}} \end{pmatrix}$$

is a parity-check (defined over \mathbb{F}_{q^m}) matrix for C , since

$$Hc^T = \begin{pmatrix} c(\alpha^{i_1}) \\ c(\alpha^{i_2}) \\ \vdots \\ c(\alpha^{i_{n-k}}) \end{pmatrix} = \underline{0} \Leftrightarrow c \in C.$$

Remark 1.38. H maybe defined over \mathbb{F}_{q^m} , but C is its nullspace over \mathbb{F}_q .

We note that, as S_C is partitioned into cyclotomic classes, there are some subsets S'_C of S_C any of them sufficient to specify the code unambiguously and we call any such S'_C a **defining set**.

1.4.3 Examples of cyclic codes

Hamming and Simplex Codes

Definition 1.39. A code which attains the Hamming bound is called a **perfect code**.

In other words, a code is said to be perfect if for every possible vector v in $(\mathbb{F}_q)^n$ there is a unique word $c \in C$ such that $d_H(v, c) \leq t$. Let C be an $[n, n-r, d]$ code with parity-check matrix $H \in (\mathbb{F}_q)^{r \times n}$. We denote by $\{H_i\}_{i=1}^n$ the set of columns of H . We observe that if two columns H_i, H_j belongs to the same line in $(\mathbb{F}_q)^r$ (i.e. $H_j = \lambda H_i$), then the vector

$$c = (0, \dots, 0, \underbrace{-\lambda}_i, 0, \dots, 0, \underbrace{1}_j, 0, \dots, 0)$$

belongs to C , since $Hc^T = 0$. Then $d(C) \leq 2$. On the other hand, if we construct a parity-check matrix H such that the columns H_i belong to different lines, the corresponding linear code has distance at least 3.

Definition 1.40. A **Hamming Code** is a linear code for which the set of columns of $H \in (\mathbb{F}_q)^{r \times n}$ contains exactly one element different from zero of every line in $(\mathbb{F}_q)^r$.

By the definition above, given two columns H_i, H_j of H , there exists a third column H_k of H , and $\lambda \in \mathbb{F}_q$ such that $H_k = \lambda(H_i + H_j)$. This fact implies that

$$c = (0, \dots, 0, \underbrace{-\lambda}_i, 0, \dots, \underbrace{-\lambda}_j, 0, \dots, 0, \underbrace{1}_k, 0, \dots, 0)$$

is a word, and hence the minimum distance of a Hamming code is 3. In the vector space $(\mathbb{F}_q)^r$ there are $n = \frac{q^r-1}{q-1}$ distinct lines, each with $q-1$ elements different from zero. Hence:

Definition 1.41. [5] Let t be a positive integer. A code C is t -error-correcting if minimum distance is able to correct t or fewer errors. A code C is exactly t -error-correcting if it is t -error-correcting but not $(t+1)$ -error-correcting.

Example 1.42. Consider the binary code $C = \{000, 111\}$. Then we see that:

- if 000 is sent and one error occurs in the transmission, then the received word (100, 010 or 001) will be decoded to 000;

- if 111 is sent and one error occurs in the transmission, then the received word (110, 101 or 011) will be decoded to 111.

In all cases, the single error has been corrected. Hence, C is 1-error-correcting. If at least two errors occur, the decoding rule may produce the wrong codeword. For instance, if 000 is sent and 011 is received, then 011 will be decoded to 111 using the minimum distance rule. Hence, C is exactly 1-error-correcting.

Proposition 1.43. A Hamming code of redundancy ($r > 2$) over the field \mathbb{F}_q , is a linear

$$\left[\frac{q^r - 1}{q - 1}, \frac{q^r - 1}{q - 1} - r, 3, \right]$$

code and it is a perfect 1-error-correcting code.

Proof. see [42]. □

Example 1.44. Let C be the $[7, 4, 3]_2$ code with parity-check matrix:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Then C is an $[7, 4, 3]$ Hamming code. Note that the columns of H are exactly the non-zero vectors of \mathbb{F}_2^3 .

The following theorem state that the Hamming codes are cyclic.

Theorem 1.45. [5] Let $n = \frac{q^r - 1}{q - 1}$. If $\gcd(n, q - 1) = 1$, then the cyclic code over \mathbb{F}_q of length n with defining set $\{1\}$ is a $[n, n - r, 3]$ Hamming code.

Proof. By Proposition (1.43) it is sufficient to show that the distance of C is equal to 3. The Hamming bound applied to C ensures that the distance cannot be greater than 3; we show that it cannot be 2 (it is obvious that it is not one). Let α be a primitive n -th root of unity over \mathbb{F}_q such that $c(\alpha) = 0$ for c in C . If c is a word of weight 2 with nonzero coefficients c_i and c_j ($i < j$), then $c_i \alpha^i + c_j \alpha^j = 0$. Then $\alpha^{j-i} = -c_i/c_j$. Since $c_i/c_j \in \mathbb{F}_q^*$, $\alpha^{(j-i)(q-1)} = 1$. Now $\gcd(n, q - 1) = 1$ implies that $\alpha^{j-i} = 1$, but this is a contradiction since $0 < j - i < n$ and the order of α is n . □

Example 1.46. The Hamming code of Example (1.44) can be viewed as $[7, 4, 3]_2$ cyclic code with generator polynomial $g = 1 + x + x^3$.

We have that the dual code of a cyclic code is cyclic itself. This means in particular that the dual of a Hamming code is cyclic.

Definition 1.47. [3] *The duals of the Hamming codes are called **Simplex codes**.*

The simplex code has the following property:

Proposition 1.48. [3] *A simplex code is a $[(q^r - 1)/(q - 1), r, q^{r-1}]$ constant weight code over \mathbb{F}_q .*

1.5 Finite Fields

Finite field, or Galois Field, is a field with a finite number of elements and it is usually referred to with the symbol $GF(q)$ where q is the number of elements in it. It is a set on which the operations of addition, subtraction, multiplication and division are defined and satisfy certain basic rules.

Theorem 1.49. [5] *A ring of integer numbers \mathbb{Z}_q , is a finite field if and only if q is prime.*

Proof. Suppose that q is a composite number and let $q = ab$ for two integers $1 < a, b < q$. Thus $a \neq 0; b \neq 0$. However, $0 = q = a \cdot b$ in \mathbb{Z}_q . This is a contradiction, (in the field if $ab = 0$ implies $a = 0$ or $b = 0$). Hence \mathbb{Z}_q is not a field.

Now let q be a prime. For any nonzero element $a \in \mathbb{Z}_q$, .i.e., $0 < a < q$, we know that a is prime to q . Thus there exist two integers u, v with $0 \leq u \leq q - 1$ such that $ua + vm = 1$, i.e., $ua \equiv 1 \pmod{q}$. Hence, $u = a^{-1}$, so \mathbb{Z}_q is a field. \square

Definition 1.50. [5] *Let \mathbb{F} be a field. The smallest natural number $n > 0$ such that*

$$n \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{n\text{-times}} = 0,$$

where 1 is the multiplicative identity of \mathbb{F} , is called the characteristic of \mathbb{F} denoted $\text{char}(\mathbb{F}) = n$. If no such n exists, we define the characteristic to be 0 .

Lemma 1.51. [35]

- (1) *If the characteristic of \mathbb{F} is positive, $\text{char}(\mathbb{F})$ is prime.*
- (2) *Finite fields have $\text{char}(\mathbb{F}) > 0$. By the first part of this lemma we even have that a finite field has prime characteristic.*

Proof. (1) Assume on the contrary that there exists a nontrivial factorization $\text{char}(\mathbb{F}) = n = p \cdot q$. Then

$$0 = n \cdot 1 = (p \cdot q) \cdot 1 = p \cdot (q \cdot 1) = (p \cdot 1)(q \cdot 1) = \underbrace{(1 + 1 + \dots, 1)}_{p\text{-times}} \cdot \underbrace{(1 + 1 + \dots, 1)}_{q\text{-times}}.$$

We have that fields have no zero divisors, that means that one of the terms in the product must be zero which contradicts the minimality of the characteristic.

(2) In a finite field not all of $1, 2 \cdot 1, 3 \cdot 1, \dots$ can be distinct, e.g. $r \cdot 1 = s \cdot 1 = 0$ for some $s > r$. Then $\Rightarrow (s - r) \cdot 1 = 0$ and so $\text{char}(\mathbb{F}) \mid s - r > 0$.

□

Lemma 1.52. *Let \mathbb{F} be a field. Then there exists a smallest subfield of \mathbb{F} .*

Proof. Let K_1, K_2 be subfields of \mathbb{F} , then their intersection $K_1 \cap K_2$ is also a subfield of \mathbb{F} . This holds for arbitrary many subfields, thus also for the intersection of all subfields of \mathbb{F} . Obviously, the resulting intersection is the smallest subfield of \mathbb{F} . □

This smallest subfield is an important concept and thus deserves a name.

Definition 1.53. (Prime subfield) *The smallest subfield of a field \mathbb{F} is called the prime subfield or short prime field of \mathbb{F} .*

Lemma 1.54. *Let \mathbb{F} be a finite field of characteristic p . The prime subfield of \mathbb{F} is isomorphic to \mathbb{F}_p , the finite field with p elements.*

Finite fields with a prime number of elements are often referred to as prime fields.

Theorem 1.55. [35] *A finite field \mathbb{F} of characteristic p contains p^n elements for some integer $n \geq 1$.*

Proof. Choose an element α_1 from \mathbb{F}_p^* . We claim that $0 \cdot \alpha_1, 1 \cdot \alpha_1, \dots, (p - 1) \cdot \alpha_1$ are pairwise distinct. Indeed, if $i \cdot \alpha_1 = j \cdot \alpha_1$ for some $0 \leq i \leq j \leq (p - 1)$, then $(j - i) \cdot \alpha_1 = 0$ and $0 \leq j - i \leq p - 1$. As the characteristic of \mathbb{F} is p , this forces $j - i = 0$; i.e., $i = j$.

If $\mathbb{F} = \{0 \cdot \alpha_1, 1 \cdot \alpha_1, \dots, (p - 1) \cdot \alpha_1\}$. we are done, Otherwise, we choose an element $\alpha_2 \in \mathbb{F} \setminus \{0 \cdot \alpha_1, 1 \cdot \alpha_1, \dots, (p - 1) \cdot \alpha_1\}$. We claim that $a_1 \alpha_1 + a_2 \alpha_2$ are pairwise distinct for all $0 \leq a_1, a_2 \leq p - 1$. Indeed, if

$$a_1 \alpha_1 + a_2 \alpha_2 = b_1 \alpha_1 + b_2 \alpha_2 \tag{1.2}$$

for some $0 \leq a_1, a_2, b_1, b_2 \leq p-1$, then we must have $a_2 = b_2$. Otherwise, we would have from (1.2) that $\alpha_2 = (b_2 - a_2)^{-1}(a_1 - b_1)^{-1}\alpha_1$. This is a contradiction to our choice of α_2 . Since $a_2 = b_2$ it follows immediately from (1.2) that $(a_1, a_2) = (b_1, b_2)$. As \mathbb{F} has only finitely many elements, we can continue in this fashion and obtain elements $\alpha_1, \dots, \alpha_n$ such that

$$\alpha_i \in \mathbb{F} \setminus \{a_1\alpha_1 + \dots + a_{i-1}\alpha_{i-1} : a_1, \dots, a_{i-1} \in \mathbb{Z}_p\} \text{ for all } 2 \leq i \leq n,$$

and

$$\mathbb{F} = \{a_1\alpha_1 + \dots + a_n\alpha_n : a_1, \dots, a_n \in \mathbb{Z}_p\}.$$

In the same manner, we can show that $a_1\alpha_1 + \dots + a_n\alpha_n$ are pairwise distinct for all $a_i \in \mathbb{Z}_p$, $i = 1, \dots, n$. This implies that $|\mathbb{F}| = p^n$. \square

So for any finite field the number of elements must be a prime or a prime power. E.g. there exists no finite field with 6 elements since 6 is not a prime or prime power. In the following q denotes a prime power $q = p^n$. We also get conditions on the relative sizes of subfields.

Lemma 1.56. [35] *Let L be a finite field with $|L| = p^n$ and let K be a subfield of L . There exists an integer $m > 1$ so that $|K| = p^m$ and $m|n$. The extension degree of L over K is $[L : K] = n/m$.*

We have a necessary condition on the number of elements in a finite field. The following example studies one finite field which is not a prime field.

Example 1.57. *The number 4 is a prime power, so there could be a finite field with 4 elements. What would $\mathbb{F}_4 = \mathbb{F}_{2^2}$ look like?*

Let 0 be the additive and 1 be the multiplicative neutral element. Let α be one of the other two elements. Since \mathbb{F}_4 is closed under addition the other element must equal $\alpha + 1$, so $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. We now give the addition table which follows easily from the fact that the characteristic is 2, thus $x + x = 0$ for any $x \in \mathbb{F}_4$. Since every element must appear in each row and each column of the table we obtain

$$\alpha \cdot \alpha = \alpha + 1 \text{ and consequently } \alpha \cdot (\alpha + 1) = 1.$$

We were able to fill the tables completely using just necessary conditions. We note that a basis of \mathbb{F}_4 over \mathbb{F}_2 could be given by $\{1, \alpha\}$.

Table 1.1: Addition table

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

Table 1.2: Multiplication table

\cdot	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

Definition 1.58. [5] Let \mathbb{F} be a field. The set

$$\mathbb{F}[x] := \left\{ \sum_{i=0}^n a_i x^i : a_i \in \mathbb{F}, n \geq 0 \right\}$$

is called the polynomial ring over \mathbb{F} .

Theorem 1.59. [35] Let $f(x)$ be a polynomial over a field \mathbb{F} of degree ≥ 1 . Then $\mathbb{F}[x]/(f(x))$, together with addition and multiplication forms a ring. Furthermore, $\mathbb{F}[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Definition 1.60. [5] An element α in a finite field \mathbb{F}_q is called a primitive element (or generator) of \mathbb{F}_q if $\mathbb{F}_q = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1}\}$.

Definition 1.61. [5] The order of a nonzero element $\alpha \in \mathbb{F}_q$, denoted by $\text{ord}(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$.

Proposition 1.62. [5]

- (i) A nonzero element of \mathbb{F}_q is a primitive element if and only if its order is $q - 1$.
- (ii) Every finite field has at least one primitive element.

Lemma 1.63. [35] For every finite field \mathbb{F}_q the multiplicative group \mathbb{F}_q^* of nonzero elements of \mathbb{F}_q is cyclic.

Example 1.64. $p(x) = x^3 + x + 1$, is an irreducible polynomial in $\mathbb{Z}_2[x]$. (It has no zero in \mathbb{Z}_2 ,) the eight polynomials of degree less than 3 in $\mathbb{Z}_2[x]$ form a field with 8 elements, usually called $GF(2^3)$. In $GF(2^3)$ we multiply two elements by multiplying the polynomials and then reducing the product modulo $p(x)$.

product mod $p(x)$	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
0	0	0	0	0	0	0	0	0
1	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
x	0	x	x^2	$x^2 + x$	$x + 1$	1	$x^2 + x + 1$	$x^2 + 1$
$x + 1$	0	$x + 1$	$x^2 + x$	$x^2 + 1$	$x^2 + x + 1$	x^2	1	x
x^2	0	x^2	$x + 1$	$x^2 + x + 1$	$x^2 + x$	x	$x^2 + 1$	1
$x^2 + 1$	0	$x^2 + 1$	1	x^2	x	$x^2 + x + 1$	$x + 1$	$x^2 + x$
$x^2 + x$	0	$x^2 + x$	$x^2 + x + 1$	1	$x^2 + 1$	$x + 1$	x	x^2
$x^2 + x + 1$	0	$x^2 + x + 1$	$x^2 + 1$	x	1	$x^2 + x$	x^2	$x + 1$

Remark 1.65. For a finite field \mathbb{F} , the multiplicative group is cyclic but the additive group of \mathbb{F} is usually not cyclic. When \mathbb{F} contains \mathbb{F}_p , since $p = 0$ in \mathbb{F}_p every nonzero element of \mathbb{F} has additive order p , so \mathbb{F} is not additively cyclic unless $|\mathbb{F}|$ is prime.

Definition 1.66. [25] A minimal polynomial of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to \mathbb{F}_q is a nonzero monic polynomial $f(x)$ of the least degree in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$.

1.5.1 Existence and Uniqueness of Finite Fields

We have now obtained a way of constructing finite fields by using irreducible polynomials over prime fields and mentioned that the same construction can also be used for an arbitrary base field. This raises the need to question whether the constructed fields are the same and whether we can always find an irreducible polynomial of the desired degree. This section is rather technical in nature but establishes a major result towards proving the existence and uniqueness of finite fields of prime power order. The following definition and theorems hold in the context of arbitrary fields.

Definition 1.67. [35] Let $f \in K[x]$ be a polynomial of positive degree and \mathbb{F} an extension field of K . Then we say that f splits in \mathbb{F} if f can be written as a product of linear factors in $\mathbb{F}[x]$, i.e., if there exist elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that

$$f = a(x - \alpha_1) \dots (x - \alpha_n)$$

where a is the leading coefficient of f . The field \mathbb{F} is called *splitting field of f over K* if it splits in \mathbb{F} .

So a splitting field F of a polynomial f over K is an extension field containing all the roots of f , and is smallest possible in the sense that no subfield of \mathbb{F} contains all roots of f .

Theorem 1.68. [35] *Let \mathbb{F}_q be a finite field and \mathbb{F}_r is an extension field. Then*

- \mathbb{F}_r is a simple extension of \mathbb{F}_q , i.e. $\mathbb{F}_r = \mathbb{F}_q(\beta)$ for some $\beta \in \mathbb{F}_r$;
- every primitive element of \mathbb{F}_r can serve as a defining element β of \mathbb{F}_r over \mathbb{F}_q .

So, we can express any finite field K with subfield F , by adjoining to F a root β of an appropriate irreducible polynomial f , which of course must have degree $d = [K : F]$

Theorem 1.69. [35] *(Existence and uniqueness of finite fields)*

For any prime p and any natural number n there exists a finite field with p^n elements. Every field with p^n elements is isomorphic to the splitting field of $f(x) = x^{p^n} - x$ over \mathbb{F}_p .

1.5.2 Automorphisms

In this section, we will once again adopt the viewpoint that a finite extension $F = \mathbb{F}_{q^m}$ of finite field $K = \mathbb{F}_q$ is a vector space of dimension m over K .

Definition 1.70. [35] *Let \mathbb{F}_{q^m} be an extension of \mathbb{F}_q and let $\alpha \in \mathbb{F}_{q^m}$. The elements $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ are called the *conjugates of α with respect to \mathbb{F}_q* .*

The conjugates of $\alpha \in \mathbb{F}_{q^m}$ with respect to \mathbb{F}_q are distinct if and only if the minimal polynomial g of α over \mathbb{F}_q has degree m . Otherwise, the degree d of the minimal polynomial g of α over \mathbb{F}_q is a proper divisor of m , and in this case the conjugates of α with respect to \mathbb{F}_q are the distinct elements $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$, each repeated m/d times.

Theorem 1.71. [35] *The conjugates of $\alpha \in \mathbb{F}_q^*$ with respect to any subfield of \mathbb{F}_q have the same order in the group \mathbb{F}_q^* .*

Proof. Since \mathbb{F}_q^* is a cyclic group by Lemma (1.63), the result follows from that in a finite cyclic group $\langle a \rangle$ of order m , the element a^k generates a subgroup of order $m/\gcd(k, m)$, and the fact that every power of the characteristic of \mathbb{F}_q is relatively prime to the order $q - 1$ of \mathbb{F}_q^* . \square

This immediately implies the following observation.

Corollary 1.72. [35] *If α is a primitive element of \mathbb{F}_{q^m} , then so are all its conjugates with respect to \mathbb{F}_q .*

Example 1.73. (i) *Expressing \mathbb{F}_4 as $\mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha + 1\}$, where $\alpha^2 + \alpha + 1 = 0$ we have that α is a primitive element of \mathbb{F}_4 . The conjugates of $\alpha \in \mathbb{F}_4$ with respect to \mathbb{F}_2 are α and α^2 and we have that $\alpha^2 = \alpha + 1$ is also a primitive element.*

(ii) *Let $\alpha \in \mathbb{F}_{16}$ be a root of $f = x^4 + x + 1 \in \mathbb{F}_2[x]$. Then the conjugates of α with respect to \mathbb{F}_2 are $\alpha, \alpha^2, \alpha^4 = \alpha + 1, \alpha^8 = \alpha^2 + 1$, and all of these are primitive elements of \mathbb{F}_{16} . The conjugates of α with respect to \mathbb{F}_4 are α and $\alpha^4 = \alpha + 1$.*

We next explore the relationship between conjugate elements and certain automorphisms of a finite field.

Definition 1.74. [35] *An automorphism of \mathbb{F}_{q^m} over \mathbb{F}_q is an automorphism σ of \mathbb{F}_{q^m} which fixes the elements of \mathbb{F}_q pointwise. Thus, σ is a one – to – one mapping from \mathbb{F}_{q^m} onto itself with*

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$$

and

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$$

for all $\alpha, \beta \in \mathbb{F}_{q^m}$ and

$$\sigma(a) = a \text{ for all } a \in \mathbb{F}_q.$$

Theorem 1.75. [35] *The distinct automorphisms of \mathbb{F}_{q^m} over \mathbb{F}_q are precisely the mappings $\sigma_0, \sigma_1, \dots, \sigma_{m-1}$ defined by*

$$\sigma_j(\alpha) = \alpha^{q^j}$$

for $\alpha \in \mathbb{F}_{q^m}$ and $0 \leq j \leq m - 1$.

Proof. We first establish that the mappings σ_j are automorphisms of \mathbb{F}_{q^m} over \mathbb{F}_q .

- For each σ_j and all $\alpha, \beta \in \mathbb{F}_{q^m}$, we have $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ and $\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta)$, so clearly σ_j is a homomorphism of \mathbb{F}_{q^m} .
- Since $\sigma_j(\alpha) = 0 \Leftrightarrow \alpha = 0$, σ_j injective. Since \mathbb{F}_{q^m} is a finite set, σ_j is also surjective, and hence is an automorphism of \mathbb{F}_{q^m} .
- We have $\sigma_j(a) = a$ for all $a \in \mathbb{F}_q$ and so each σ_j is an automorphism of \mathbb{F}_{q^m} over \mathbb{F}_q .
- The mappings $\sigma_1, \sigma_2, \dots, \sigma_{m-1}$ are distinct as they return distinct values for a primitive element of \mathbb{F}_{q^m} .

Now, suppose σ is an arbitrary automorphism of \mathbb{F}_{q^m} over \mathbb{F}_q ; we show that it is in fact σ_j for some $0 \leq j \leq m-1$.

Let β be a primitive element of \mathbb{F}_{q^m} and let $f = x^m + a_{m-1}x^{m-1} + \dots + a_0 \in \mathbb{F}_q[x]$ be its minimal polynomial over \mathbb{F}_q . Then

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{m-1}\beta^{m-1} + \dots + a_0) \\ &= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \dots + a_0, \end{aligned}$$

so that $\sigma(\beta)$ is a root of f in \mathbb{F}_{q^m} . Thus we have $\sigma(\beta) = \beta^{q^j}$ for some j , $0 \leq j \leq m-1$. Since σ is a homomorphism and β primitive, we get that $\sigma(\alpha) = \alpha^{q^j}$ for all $\alpha \in \mathbb{F}_{q^m}$. \square

Hence the conjugates of $\alpha \in \mathbb{F}_{q^m}$ are obtained by applying all automorphisms of \mathbb{F}_{q^m} over \mathbb{F}_q to the element α .

Remark 1.76. *The automorphisms of \mathbb{F}_{q^m} over \mathbb{F}_q form a group under composition of mappings, called the Galois group of \mathbb{F}_{q^m} over \mathbb{F}_q and denoted $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. From Theorem (1.75), this group of automorphisms is a cyclic group of order m , generated by σ_1 .*

Definition 1.77. [41] *(The Frobenius Identity) Let p be a prime and let \mathbb{F}_p be a finite field with characteristic p . Then $(a + b)^p = a^p + b^p$, for all $a, b \in \mathbb{F}_p$.*

Definition 1.78. [41] *Let \mathbb{F}_p be a finite field. The Frobenius Automorphism of \mathbb{F}_p is the function $\phi : \mathbb{F}_p \rightarrow \mathbb{F}_p$ such that $\phi(a) = a^p$, $\phi(ab) = \phi(a)\phi(b)$ and $\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b)$.*

Example 1.79. *Frobenius Automorphism in $\mathbb{F}_4 = \mathbb{F}_{2^2}$.*

Let $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$ be a field with 4 elements and $\phi : \mathbb{F}_4 \rightarrow \mathbb{F}_4$ be the Frobenius Automorphism $\phi(a) = a^p = a^2$. Then $\phi(0) = 0$, $\phi(1) = 1$, $\phi(x) = x^2 = x + 1$ and $\phi(x + 1) = x^2 + 1 = x$. Thus ϕ fixes 0 and 1 while it switches x with $x + 1$.

1.6 General Linear Group Over Finite Field

In this section we write some basic facts about the general linear group of order n over a given field \mathbb{F}_q that is a finite field with q elements. Let us start with the definitions of some groups of matrices over \mathbb{F}_q .

Definition 1.80. *The general linear group consists of all nonsingular $n \times n$ matrices and is denoted by $GL(n, q)$, or $GL_n(q)$.*

$$GL(n, \mathbb{F}_q) = \{A_{n \times n} : \det(A_{n \times n}) \not\equiv 0 \pmod{q}\}.$$

Definition 1.81. *The set of $n \times n$ matrices with units on the main diagonal and zeros above (under) the diagonal is called the lower (upper) unitriangular group.*

Both these groups are isomorphic to each other. The map taking each lower unitriangular matrix \mathbf{L} to the upper unitriangular matrix $\mathbf{R} = \mathbf{L}^{-T}$ is an isomorphism between these two groups. Taking that into account we will further denote the groups by $UT_n(q)$.

Definition 1.82. *The special linear group $SL(n, q)$ is the normal subgroup of $GL(n, q)$ consisting of matrices of determinant 1.*

Definition 1.83. *The projective general linear group $PGL(n, q) = \frac{SL(n, q)}{Z}$, where $Z = \{\lambda I \mid \lambda^n = 1, \lambda \in GF(q)\}$ is the center of $GL(n, q)$.*

Definition 1.84. *The projective special linear group $PSL(n, q)$ is the quotient of $SL_n(q)$ by the normal subgroup $Z \cap SL_n(q)$.*

If V is a vector space of dimension n over F , we denote by $GL(V)$ the group of invertible linear transformations of V ; thus $GL(V) \cong GL(n, F)$.

Theorem 1.85. [44] *Given any two ordered bases for the vector space V , there is a unique element of $GL(V)$ carrying the first to the second.*

From this theorem it follows that the order of $GL(n, q)$ is equal to the number of ordered bases of $GF(q)^n$, namely

$$|GL(n, q)| = \prod_{i=0}^{n-1} (q^n - q^i) = q^{n(n-1)/2} \prod_{i=0}^{n-1} (q^{n-i} - 1).$$

This can be shown by counting the possible columns of the matrix: the first column can be anything but the zero vector; the second column can be anything but the multiples of the first column; and in general, the k th column can be any vector not in the linear span of the first $k-1$ columns. When p is prime, $GL(n, p)$ is the outer automorphism group of the group Z_p^n and also the automorphism group, because Z_p^n is abelian, so the inner automorphism group is trivial.

Example 1.86. $GL(2, 3)$ has order $(8-1)(8-2)(8-4) = 168$. It is the automorphism group of Z_2^3 , and is also known as $PSL(2, 7)$.

Note that in the limit as $q \rightarrow 1$ the order of $GL(n, q)$ goes to $n!$, which is the order of the symmetric group in the philosophy of the field with one element, one thus interprets the symmetric group as the general linear group over the field with one element: $S_n \cong GL(n, 1)$.

Theorem 1.87. [28] If $A \in GL_n(q)$, then the order of A , $O(A) \leq q^n - 1$.

Proof. see [28]. □

A polynomial of degree n over $GF(q)$ is the characteristic polynomial of a matrix in $SL_n(q)$ if and only if $(-1)^n f(0) = 1$, where $f(x) \in GF(q)[x]$ have the property that $f(0) \neq 0$, i.e., $f(x)$ is not divisible by x .

Lemma 1.88. [28] Let $0 \neq f(x) \in GF(q)[x]$ with degree n has order $\frac{q^n-1}{q-1}$, $n \geq 1$. Then $f(x)$ is irreducible over $GF(q)$ and $(-1)^n f(0) = 1$.

Proof. see [28]. □

Proposition 1.89. [44] The number of elements in $SL_n(\mathbb{F}_q)$ is

$$\left(\prod_{i=0}^{n-1} (q^n - q^i) \right) \setminus (q-1).$$

Corollary 1.90. [44] The group $SL_n(q)$, $n \geq 1$, has an element of order $\frac{q^n-1}{q-1}$.

The Automorphism Groups of Linear codes

In this chapter we introduce the automorphism group of a linear code which is the main object of our dissertation.

An action of a group on a set X is the function $f : G \times X \rightarrow X$ such that $f(g, x)$ is denoted by gx and with the following properties. $((g_1g_2)x = g_1(g_2x))$ and $(ex = x)$. If x, y are in X , we say that $x \sim y$ if there is g in G such that $y = gx$. And if x in X , we define $G_x = \{g \mid gx = x\}$ is called the isotropy or (stabilizer) subgroup of G , or subgroup fixing x .

Let $Sym(A)$ denotes the symmetric group acting on the set A , i.e., the group of all permutations of A . S_n denotes $Sym([n])$ where $[n] = \{1, \dots, n\}$. Permutation groups acting on the permutation domain A are subgroups $G \leq Sym(A)$. If $|A| = n$ then G is a permutation group of *degree* n . For $a \in A$ and $\pi \in G$ we use a^π to denote the image of a under π . The orbit of $a \in A$ is the set $a^G := \{a^\pi : \pi \in G\}$. The orbits partition the permutation domain. The length of an orbit is its size.

Definition 2.1. [33] *Two $[n, k]$ -linear codes over \mathbb{F}_q are equivalent if one can be obtained from the other by combination of operations of the following types:*

- (i) *permutation of the n digits of the codewords;*
- (ii) *multiplication of the symbols appearing in a fixed position by a nonzero scalar.*

So mixing the coordinates of the code gives a new code, which shares many of the same properties with C , like the minimum weight and the weight enumerator. Some of these permutations of coordinates send C into itself: all code words of C

are mapped to (possibly different) code words in C . These permutations together form the *automorphism group of C* , denoted by $\text{Aut}(C)$.

$$\text{Aut}(C) = \{\pi \in S_n : \pi(C) = C\}$$

This is a subgroup of S_n , with composition of functions as operation and the identity function as the identity element [33].

Remark 2.2. It is often convenient to express the permutation between codes in a permutation matrix P .

Definition 2.3. [3] A permutation matrix P is a square matrix with exactly one 1 in each row and column and zeros elsewhere.

Another way to see that two codes are permutation equivalents is if there is a permutation matrix P such that G_1 is a generator for C_1 if and only if G_1P is a generator for C_2 . We define:

$$C_1P = \{y : y = xP \text{ for some } x \in C_1\} = C_2$$

One of the most important results stemming from Definition (2.1) is the following theorem:

Theorem 2.4. [33] Any (n,k,d) -code on the alphabet of size q is equivalent to another (n,k,d) -code on the same alphabet which contains the zero vector.

Proof. Assume a code of length n where all the codewords are of the form $x_1x_2x_3\dots x_n$. Choose a codeword and a $x_i \neq 0$ which appears in the codeword. Perform the mapping:

$$0 \mapsto x_i$$

$$x_i \mapsto 0$$

$$j \mapsto i$$

for each nonzero x_i in the chosen codeword.

We repeat the permutation choosing different all the nonzero values for x_i in our chosen codeword. Then the codeword has been permuted to be $\mathbf{0}$ and so the original code is equivalent to a code which contains $\mathbf{0}$. \square

Proposition 2.5. [3] Any linear code is permutationally equivalent to a linear code in the standard form.

Proof. This is clear since the generator matrix of the standard form is obtained from the generator matrix of the code by elementary row operation in addition to column permutation. \square

Example 2.6. Let C_1 and C_2 have generator matrices

$$\mathbf{G}_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{G}_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

respectively. Note that there is not going to be a permutation matrix P so that $G_1P = G_2$. However, when we write out the codes:

$$C_1 = \{00000, 11000, 01010, 00101, 10010, 11101, 01111, 10111\}$$

$$C_2 = \{00000, 10001, 00011, 01100, 10010, 11101, 01111, 11110\}$$

We notice that the two codes are in fact permutation equivalent.

2.1 Examples

Example 2.7. Let C be the $[n,1]$ binary repetition code. Then, $\text{Aut}(C)$ is the symmetric group S_n because all permutations are automorphisms.

Example 2.8. [6]

Let C be a code of length n , with n prime. If $\text{Aut}(C)$ contains a 2-cycle τ and an n -cycle σ , then $\text{Aut}(C)$ is equal to S_n .

Proof. By renaming the coefficients we can say with out loss of generality that $\tau = (01)$. Since n is prime, all powers of σ^i of σ , with $1 \leq i \leq n - 1$, are again n -cycles.

So, there is a power i of σ such that $\sigma^i = (01\dots)$. By renaming the rest of the coordinates, we can say that $\sigma = (01\dots n - 1)$. Since $\text{Aut}(C)$ is a group, it also contains $\sigma\tau\sigma^{-1} = (12)$, $\sigma(12)\sigma^{-1} = (23), \dots, (n - 2, n - 1)$. These 2-cycles generate S_n . \square

For n not prime this does not necessarily hold. For example, consider the block repetition code generated by $(1 + x^4)$ in $\mathbb{F}_2[x]/(x^8 - 1)$. The automorphism group of this code contains (04) and $(01\dots 7)$, but not the permutation (01) , so it does not contain all S_n .

Example 2.9. [34] Let us compute the automorphism group $\text{Aut}(C)$ of the $[4, 2]$ repetition code $C = \{0000, 0011, 1100, 1111\}$. By writing down all possible permutations of 4 objects that preserve C it is straightforward to see that $\text{Aut}(C)$ is a nonabelian group with 8 elements. One automorphism of C is given by $R = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$.

A simple calculation shows that $R^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, transposes the first and the second, as well as the third and the fourth coefficients, which implies that R has order 4, and that $R^4 = \text{id}$. This shows that $\text{Aut}(C)$ has a cyclic subgroup of order 4. But we also have the transposition $S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ which is different from id , R , R^2 and R^3 . Thus $\text{Aut}(C)$ contains at least the 8 elements of $G = \{S^a \circ R^b : 0 \leq a \leq 1, 0 \leq b \leq 3\}$. How can we show that there are no others? The first step is proving that G is actually a group. This follows almost immediately from the fact that $R \circ S = S \circ R^3$, which allows us to write any product of elements of G in the form $S^a \circ R^b$. For example, the product $(S \circ R) \circ S$ is transformed into $(S \circ R) \circ S = S \circ (R \circ S) = S \circ (S \circ R^3) = (S \circ S) \circ R^3 = \text{id} \circ R^3 = R^3$. Here we have used associativity, which holds since we are dealing with composition of permutations, and the composition of maps is always associative. So now we know that G is a group. Why does this help us? Because this implies that $G \subseteq \text{Aut}(C) \subseteq S_4$, where S_4 is the full group of permutations on 4 objects. Since S_4 has $4! = 24$ elements, and since the order of a subgroup divides the order of a group, we conclude that $8 \mid \#\text{Aut}(C) \mid 24$. Thus either $\text{Aut}(C) = G$ or $\text{Aut}(C) = S_4$. But the last possibility cannot occur: we need only write down a single permutation that does not conserve codewords, for example the transposition of the middle bits, which turns 0011 into 0101 , hence is not an automorphism. Thus $\text{Aut}(C) = G$; in fact, G is isomorphic to the dihedral group D_4 of order 8, because the generators R and S satisfy the relations $R^4 = S^2 = \text{id}$, $SRS = R^3$ of the dihedral group. Now D_4 is the symmetry group of a square, and it is actually possible to make this isomorphism concrete.

Here one of the useful properties about the automorphism group:

Theorem 2.10. [6] *Let C be a linear code over \mathbb{F}_q . Then $\text{Aut}(C) = \text{Aut}(C^\perp)$*

Proof. Let $\pi \in \text{Aut}(C)$. For a codeword $b \in C^\perp$ holds $\langle b, a \rangle = \sum_{i=0}^{n-1} a_i b_i = 0$ for all $a \in C$, so also

$$\langle \pi(b), \pi(a) \rangle = \sum_{i=0}^{n-1} a_{\pi(i)} b_{\pi(i)} = \sum_{i=0}^{n-1} a_i b_i = 0$$

for all $a \in C$. Since $\pi(C) = C$, this means that $\pi(b)$ is perpendicular to every $a \in C$. So $\pi(b)$ is an element of C^\perp , hence

$$\text{Aut}(C) \subset \text{Aut}(C^\perp).$$

Since C is linear, it holds that $(C^\perp)^\perp = C$, hence $\text{Aut}(C^\perp) \subset \text{Aut}((C^\perp)^\perp) = \text{Aut}(C)$. So,

$$\text{Aut}(C^\perp) \subset \text{Aut}(C).$$

So, $\text{Aut}(C) = \text{Aut}(C^\perp)$ □

Let C be a binary code and H be a subgroup of $\text{Aut}(C)$. For a codeword $c \in C$ we know that the number of 1 in the coordinate place of c is the weight of it. Usually, N_i denotes the number of codewords in C of weight i and $N_i(H)$ the number of codewords which are fixed by some element of H . Now, we will investigate a method of using the automorphism group to find out the weight distribution of a given code.

Theorem 2.11. [8] *Let C be a binary code and H be a subgroup of $\text{Aut}(C)$. Then*

$$N_i \equiv N_i(H) \pmod{O(H)}$$

Proof. The codewords of weight i can be divided into two classes those fixed by some element of H . If $c \in C$ is not fixed by any element of H then the $O(H)$ codeword $g \times c$ for $g \in H$ must be distinct. Then $N_i - N_i(H)$ is multiple of $O(H)$. □

2.2 Automorphism group of binary codes

The symmetric group S_n acts on \mathbb{F}_2^n by the group action $v\sigma := (v_{\sigma^{-1}(1)}, \dots, v_{\sigma^{-1}(n)})$ where $v = (v_1, \dots, v_n) \in \mathbb{F}_2^n$ and $\sigma \in S_n$. Let C be a binary code, then if $v\sigma \in C$ for all $v \in C$, then σ is an automorphism of C , and the set of all automorphisms of C is a group, denoted $\text{Aut}(C)$.

Lemma 2.12. [19] *Let C be a code of length n , such that all automorphism of prime order p acts fixed point freely. If $|Aut(C)| = p^a m$, with $(p, m) = 1$, then $a \leq \max\{r \in \mathbb{Z} : p^r | n\}$.*

Proof. Suppose $a > \max\{r \in \mathbb{Z} : p^r | n\}$. By Sylow's theorem, there exists a subgroup $H \leq Aut(C)$ with $|H| = p^a$. The group H acts on the set $\{1, \dots, n\}$. Since all automorphisms of order p acts fixed point freely, then each orbit has p^a elements. Therefore $P^a | n$, a contradiction. \square

Definition 2.13. *Let $\sigma \in Aut(C)$. The fixed code of σ is*

$$F_\sigma(C) := \{v \in C | v\sigma = v\}.$$

Let $\Omega_1, \dots, \Omega_c$ be the cycle sets and let $\Omega_{c+1}, \dots, \Omega_{c+f}$ be the fixed points of σ . Clearly $v \in F_\sigma(C)$ if and only if $v \in C$ and v is a constant on each cycle.

Let $\pi_\sigma : F_\sigma(C) \rightarrow \mathbb{F}_2^{n+f}$ denotes the projection map defined by $\pi_\sigma(v|_{\Omega_i}) = v_j$ for some $j \in \Omega_i$ and $i \in \{1, \dots, c+f\}$.

Example 2.14. *Consider the $[7, 4]_2$ binary code \mathcal{H}_3 , with the following generator matrix:*

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Then the following are automorphisms:

(1) $\sigma_1 = (12)(56) :$

$$\mathbf{G}\sigma_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$G\sigma_1$ is simply the matrix G with the rows 1 and 2 switched, and thus still generates C .

(2) $\sigma_2 = (123)(567)$

$$\mathbf{G}\sigma_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Again, $G\sigma_2$ is simply G with the rows 1, 2, and 3 permuted. It still provides a basis for C .

$$(3) \sigma_3 = (1245736)$$

$$\mathbf{G}\sigma_3 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Through simple row operations, we can transform $G\sigma_3$ into G , so $G\sigma_3$ provides a basis for C .

These three permutations generate a simple, non-abelian group of order 168, which turns out to be a very special group, $PSL(2,7)$.

Consider a linear $[n, k]$ -code C with generator matrix M and a permutation $\pi \in \text{Aut}(C)$. For every basis vector v_i of C , $\pi(v_i)$ can be expressed as a linear combination of the basis vectors of C :

$$\pi(v_i) = b_{i,1}v_1 + b_{i,2}v_2 + \cdots + b_{i,k}v_k.$$

These $b_{i,j}$ together form the invertible $k \times k$ matrix B_π . The generator matrix of the code $\pi(C)$ is given by $B_\pi M$. The permutation π can be seen as a linear map from \mathbb{F}_2^n to \mathbb{F}_2^n that permutes the basis vectors. Let A_π be the transpose of the $n \times n$ permutation matrix that belongs to this map. So A_π mixes the columns of M in the same way as π does, hence A_π satisfies $B_\pi M = M A_\pi$.

The map ϕ maps a permutation $\pi \in \text{Aut}(C)$ to the inverse of the matrix $B_\pi \in GL(k, 2)$:

$$\phi(\pi) = B_\pi^{-1}. \quad (2.1)$$

For every $\pi_1, \pi_2 \in \text{Aut}(C)$ it holds that $A_{\pi_1 \circ \pi_2} = A_{\pi_1} A_{\pi_2}$. So

$$M A_{\pi_1 \circ \pi_2} = M A_{\pi_1} A_{\pi_2} = B_{\pi_2} M A_{\pi_1} = B_{\pi_2} B_{\pi_1} M,$$

and hence

$$\phi(\pi_1 \circ \pi_2) = (B_{\pi_2} B_1)^{-1} = B_{\pi_1}^{-1} B_{\pi_2}^{-1} = \phi(\pi_1) \phi(\pi_2).$$

So the map ϕ is a group homomorphism. If ϕ is injective, then the automorphism group of the code C is isomorphic to a subgroup of $GL(k, 2)$.

Lemma 2.15. [6] *Let C be a linear code. If the map ϕ is not injective for C , then there is a 2-cycle (ij) in $\ker(\pi)$. This means that at least two columns of the generator matrix of C are equal.*

Theorem 2.16. *Let C be a cyclic $[n, k]$ -code. Then $\phi : \text{Aut}(C) \rightarrow GL(k, 2)$ is not injective if and only if C is a block repetition code.*

Lemma 2.17. [6] *The map ϕ is injective for the Hamming code of length $n = 2^m - 1$, for $m \geq 3$.*

Definition 2.18. *Let α be such that $\mathbb{F}_{2^m}^* = \langle \alpha \rangle$ and take $2 \leq \delta \leq n$, $m \geq 1$ and $0 \leq b \leq n$. Let $m_i(x)$ be the minimal polynomial of α^i over \mathbb{F}_2 . Let $g(x)$ be the monic polynomial of lowest degree over \mathbb{F}_2 that has $\alpha^b, \dots, \alpha^{b+\delta-2}$ among its zeros, that is,*

$$g(x) = \text{lcm}(m_b(x), \dots, m_{b+\delta-2}(x)).$$

The $BCH(m, \delta, b)$ code of length $n = 2^m - 1$ is the code generated by $g(x)$. When $b = 1$, the $BCH(m, \delta, 1)$ code is called a narrow sense BCH code.

Theorem 2.19. [6] *The map ϕ is injective for the dual code of a narrow sense $BCH(m, \delta, 1)$ code of length $n = 2^m - 1$, $m \geq 2$.*

Proof. Let α be such that $\mathbb{F}_{2^m}^* = \langle \alpha \rangle$. The generator polynomial $h(x)$ of $BCH(m, \delta, 1)$ is the polynomial of lowest degree over \mathbb{F}_2 that has $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ among its zeros. Let $g(x)$ be the generator polynomial of BCH^\perp , which satisfies $g^*(x)h(x) = x^n - 1$. Suppose that ϕ is not injective for BCH^\perp . Then BCH^\perp is a block repetition code, so there exist $l, p \in \mathbb{Z}$ with $n = lp$ and $p \geq 2$, and $f(x)$ with $f(x)|x^l - 1$ such that

$$g(x) = (1 + x^l + x^{2l} + \dots + x^{n-l})f(x)$$

The reciprocal of $g(x)$ is given by

$$\begin{aligned} g(x)^* &= (1 + x^l + x^{2l} + \dots + x^{n-l})^* f^*(x) \\ &= (1 + x^l + x^{2l} + \dots + x^{n-l}) f^*(x) \end{aligned}$$

So we see that $1+x^l+\cdots+x^{n-l}|g^*(x)$. Furthermore, α is a zero of $1+x^l+\cdots+x^{n-l}$:

$$1 + \alpha^l + \cdots + \alpha^{n-l} = (\alpha^n - 1)/(\alpha^l - 1) = 0;$$

since α is a primitive n -th root of unity and l is a proper divisor of n . So α is a zero of both $h(x)$ and $g^*(x)$, hence α is a multiple zero of $x^n - 1$. However, for odd n , $x^n - 1$ has only single roots:

$$\gcd(x^n - 1, \frac{d}{dx}(x^n - 1)) = \gcd(x^n - 1, x^{n-1}) = 1.$$

This leads to a contradiction, hence ϕ is injective for $BCH(m, \delta, 1)^\perp$. \square

Theorem 2.20. [6] *The automorphism group of the Hamming code H of length $n = 2^m - 1$ is isomorphic to $GL(m, 2)$.*

Proof. To prove this, we consider H^\perp , since the automorphism group of a code is equal to the automorphism group of the dual code. Theorem (2.19) tells us that ϕ is injective for H^\perp for $m \geq 3$. For $m = 2$, H^\perp is equal to the even weight code of length 3, for which ϕ is injective too. Also for the trivial case that $m = 1$ it holds that ϕ is injective for H^\perp . The dimension of H^\perp is m , so there is a basis v_1, \dots, v_m for H^\perp , which form the rows of the $m \times n$ generator matrix M . Let p_0, \dots, p_{n-1} be the n columns of the generator matrix. Since ϕ is injective, we know from lemma (2.15) that the $n = 2^m - 1$ vectors p_i are all different. Moreover, they are all not equal to zero, because H^\perp is cyclic and not equal to the zero code. So p_0, \dots, p_{n-1} are exactly all the nonzero vectors of \mathbb{F}_2^m . For every matrix $K \in GL(k, 2)$, the rows of $K^{-1}M$ give a new basis for H^\perp , so $K^{-1}M$ is also a generator matrix for H^\perp . Hence, the columns of $K^{-1}M$ need to be exactly all the nonzero vectors of \mathbb{F}_2^m . So mixing the columns of $K^{-1}M$ in the right way gives M . Thus there is a permutation matrix A for this permutation, which satisfies $K^{-1}M = MA$. So for every $K \in GL(k, 2)$ there is an automorphism π of H^\perp for which $\phi(\pi) = K$. This means that the map ϕ is not only injective, but also surjective for H^\perp and we can conclude

$$\text{Aut}(H) = \text{Aut}(H^\perp) \cong GL(k, 2).$$

\square

Definition 2.21. [3] *The group $\text{Aut}(C)$ is transitive as a permutation group if for every ordered pair (i, j) of coordinates, there is a permutation in $\text{Aut}(C)$ which sends coordinate i to coordinate j .*

When $\text{Aut}(C)$ is transitive, we have information about the structure of its punctured codes. When $\text{Aut}(\widehat{C})$ is transitive, we have information about the minimum weight of C . This lemma is used to prove part (i) of the next theorem.

Lemma 2.22. [3] *If C is a code and P a permutation where $jP = i$, then*

$$(CP)_i^* = C_j^* P_j^*$$

where P_j^* is the permutation punctured at j , (remove column i and row j).

Theorem 2.23. [3]

(1) *Let C be a binary $[n, k, d]$ linear code, set*

$$C_e = \{c \in C : wt(c) \text{ is even}\}.$$

Then $C = C_e$ has dimension $k - 1$.

(2) *If C is an $[n, k, d]_q$ linear code, set*

$$C_e = \{c \in C : \sum_{i=1}^n c_i = 0 \text{ in } \mathbb{F}_q\}.$$

Elements of C_e are called 'even-like' codewords. All others are called 'odd-like.' Then $C_e = C$ or C_e has dimension $k - 1$.

Theorem 2.24. [3] *Let C be an $[n, k, d]$ code.*

- (i) *Suppose that $\text{Aut}(C)$ is transitive. Then the n codes obtained from C by puncturing C on a coordinate are permutation equivalent.*
- (ii) *Suppose that $\text{Aut}(\widehat{C})$ is transitive. Then the minimum weight d of C is its minimum odd-like weight, d_O . Furthermore, every minimum weight codeword of C is odd-like.*

Proof. • (i) Suppose that $\text{Aut}(C)$ is transitive. Fix $1 \leq i, j \leq n$, and consider C_i^* and C_j^* . Because $\text{Aut}(C)$ is transitive, there is a $P \in \text{Aut}(C)$ that sends i to j . Because $P \in \text{Aut}(C)$, $CP = C$. Now, puncture CP on the j^{th} coordinate and C on the i^{th} coordinate. Because of the lemma, $C_j^* = (CP)_j^* = C_i^* P_i^*$. Hence, C_j^* is permutation equivalent to C_i^* .

- (ii) Again, assume that $\text{Aut}(C)$ is transitive. Applying (i) to \widehat{C} we conclude that puncturing \widehat{C} on any coordinate gives a code permutation equivalent to C . Let c be a minimum weight vector of C and assume that c is even-like. Then $\text{wt}(\widehat{c}) = d$, where $\widehat{c} \in \widehat{C}$ is the extended vector. Puncturing \widehat{C} on a coordinate where c is nonzero gives a vector of weight $d - 1$ in a code permutation equivalent to C , a contradiction.

□

2.3 Automorphism Groups of Cyclic Codes

In this section we will try to say something general about the automorphism groups of cyclic codes. We will discuss whether some specific subgroups of S_n occur as the automorphism group of a cyclic code of length n .

Theorem 2.25. *The automorphism group of a linear code C of length n is equal to S_n if C is one of the following codes: the zero code, \mathbb{F}_2^n , the repetition code or the even weight code.*

Proof. Suppose C contains a codeword a , that has at least one 1 and one 0, so the weight $\text{wt}(a)$ satisfies $1 \leq \text{wt}(a) \leq n - 1$. Suppose that there is a 1 on place i and a 0 on place j . Since the automorphism group is equal to S_n , $\tau = (ij)$ is an element of $\text{Aut}(C)$. So $\tau(a)$ is contained in C , and also $a + \tau(a)$, which has weight 2. From this code word $a + \tau(a)$, we can make each code word of even weight with an appropriate permutation from S_n . So the even weight code is contained in C , and hence C is the even weight code of dimension $n - 1$ or it is equal to \mathbb{F}_2^n . If C has no such code word a , then C is the zero code or the repetition code. □

This theorem holds for linear codes in general. However, when a linear code C has S_n as its automorphism group, then $\text{Aut}(C)$ contains the n -cycle $\sigma = (0, 1, \dots, n - 1)$ and hence the code turns out to be cyclic.

Let $N \in \mathbb{N}$ and let \mathbb{F}_2^N be a vector space of dimension N , with fixed standard basis \mathbf{e}_i indexed by $i = \{1, 2, \dots, N\}$. Put $\mathbf{a} = \sum_{i=1}^N \mathbf{e}_i$. We refer to the following four codes as elementary codes:

$$\varepsilon_0 = \mathbf{0} \quad \varepsilon_1 = \mathbb{F}_2 \mathbf{a} \quad \varepsilon_2 = \{\mathbf{v} \in \mathbb{F}_2^N \mid \text{wt}(\mathbf{v}) \equiv_2 0\} \quad \varepsilon_3 = \mathbb{F}_2^N$$

If $N = 1$, then $\varepsilon_0 = \varepsilon_2$ and $\varepsilon_1 = \varepsilon_3$. Otherwise the four codes are distinct. Clearly, the automorphism group of any of the elementary codes is the full symmetric group S_n .

Proposition 2.26. [7] *Let C be a binary linear code of length n . If $A_n \leq \text{Aut}(C)$ and $n \neq 2$, then C is one of the elementary codes, the zero code, \mathbb{F}_2^n , the repetition code or the even weight code.*

Proof. Suppose that $A_n \leq \text{Aut}(C)$ and $n \geq 3$. We may assume that $C \not\subseteq \varepsilon_1$, so that we find $c \in C$ with $0 < \text{wt}(c) < n$. Put $k = \text{wt}(c)$. As the usual action of A_n on $\{1, 2, \dots, n\}$ is transitive [29], we may assume that $c = \sum_{i=1}^k e_i$ where $1 < k < n$. If $k = 1$, then $C = \varepsilon_3$. If $k \geq 3$, then applying the 3-cycle $\sigma := (1, k, k+1) \in \text{Aut}(C)$, we see that $\mathbf{e}_1 + \mathbf{e}_{k+1} = \mathbf{c} + \mathbf{c}^\sigma \in C$, hence $\varepsilon_2 \subseteq C$. □

Corollary 2.27. *Let C be a binary linear code of length $n \geq 3$. Then $\text{Aut}(C) \neq A_n$.*

Proposition 2.28. [7] *The automorphism group of a binary cyclic code is not isomorphic (as an abstract group) to a non-trivial cyclic group of odd order.*

Proof. Let C be a binary cyclic code of length n such that $G = \text{Aut}(C)$ is cyclic of odd order. Since G contains a regular cyclic subgroup of order n and since any transitive cyclic subgroup of S_n has order precisely n , we deduce that $\text{Aut}(C) = C_n$. We may realise a code isomorphic to C as an ideal \mathcal{I} of the finite ring $\mathcal{R} = \mathbb{F}_2[x] \setminus (x^n - 1)$ equipped with the standard basis $1, X, \dots, X^{n-1}$. The ideal \mathcal{I} is principal and invariant under the Frobenius automorphism of \mathcal{R} . The latter induces a permutation π of the standard basis, given by $x^m \mapsto x^{2m}$ where exponents are to be read as integers modulo n . As π fixes the basis element 1, it can only belong to a regular cyclic group, if it is trivial. Thus $n = 1$ or $n = 2$. Since n is odd, we conclude that $C = 0$, and $\text{Aut}(C)$ is trivial. □

Theorem 2.29. [7] *The automorphism group of a binary cyclic code is not isomorphic (as an abstract group) to an alternating group A_n of degree $n \in \{3, 4, 5, 6, 7\}$ or $n \geq 9$. The group A_8 occurs as the automorphism group of a binary cyclic code of length 15.*

Proof. Let C be a binary cyclic code of length N such that $\text{Aut}(C)$ is isomorphic to an alternating group A_n of degree $n \geq 3$. An exact factorisation of A_n consists of two

subgroups $G, H \leq A_n$ such that $A_n = GH$ and $G \cap H = 1$. Since $\text{Aut}(C)$ contains a regular cyclic subgroup of order N which is complemented by any point stabiliser, this provides an exact factorisation $A_n = GH$ with one of the groups G, H cyclic of order N . Exact factorisations of alternating groups were studied by Wiegold and Williamson. Adhering to the notation in [Wiegold and Williamson paper. Theorem A]. our setting allows for two possibilities. It could be that G is cyclic of odd order $n = N$ and $H \cong A_{n-1}$, but this would contradict (2.27). The only other possibility is that $n = 8$, that $G \cong \text{AGL}(3, 2)$ is an affine group and H is cyclic of order $N = 15$. Noting that $A_8 \cong \text{PSL}(4, 2) = \text{PGL}(4, 2)$, we observe that this group does indeed arise as the automorphism group of the binary Hamming code of length $2^4 - 1 = 15$. \square

2.4 On Permutation Automorphism groups of q -ary Hamming Codes

We have in (2.20) that the permutation automorphism group of the binary Hamming code \mathcal{H}_2^n of length $n = 2^m - 1$ is isomorphic to the general linear group $\text{GL}_m(2)$.

Recall that a mapping $\phi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is called an isometry of the space \mathbb{F}_q^n if for any two vectors $x, y \in \mathbb{F}_q^n$ the following equality holds: $d(x, y) = d(\phi(x), \phi(y))$.

Suppose $\pi \in S_n$, where S_n is the symmetric group on n elements of the ground set $\{1, 2, \dots, n\}$. The action of the permutation π on any vector $x = (x_1, \dots, x_n)$ from \mathbb{F}_q^n is defined by

$$\pi(X) = (x_{\pi^{-1}(1)}, \dots, x_{\pi^{-1}(n)}).$$

Thus we call an isometry $\sigma : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ such that

$$\sigma(x) = (\sigma_1(x_1), \dots, \sigma_n(x_n)),$$

where σ_i are permutations from the symmetric group S_q acting on the field \mathbb{F}_q . the automorphism group of the space \mathbb{F}_q^n is a semidirect product of the group S_n on the group S_q^n of all configurations, i.e.

$$\text{Aut}(\mathbb{F}_q^n) = S_n \ltimes S_q^n = \{(\pi; \sigma) : \pi \in S_n, \sigma = (\sigma_1, \dots, \sigma_n) \in S_q^n\}.$$

The group of all isometries of \mathbb{F}_q^n mapping a code C into itself is called the automorphism group of the code C :

$$\text{Aut}(C) = \{(\pi; \sigma) \in \text{Aut}(\mathbb{F}_q^n) : (\pi; \sigma)(C) = C\}.$$

Multiplying all elements of the field \mathbb{F}_q^n by some nonzero element $\beta \in \mathbb{F}_q^n$ we get the permutation τ_β from S_q

$$\tau_\beta = \begin{pmatrix} 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \\ 0 & \alpha^0\beta & \alpha^1\beta & \cdots & \alpha^{q-2}\beta \end{pmatrix}$$

By S_q^* we denote the set of all $q - 1$ such permutations. Define the monomial automorphism group of a code C as

$$MAut(C) = \{(\pi; \sigma) \in Aut(C) : \sigma \in (S_q^*)^n\}.$$

Let ε be the identity configuration, i.e. all its components are the identity permutations. It is natural to identify the isometry $(\pi; \varepsilon)$ with the permutation π .

Definition 2.30. [10] The permutation automorphism group of a code C is

$$PAut(C) = \{\pi \in Aut(C)\}.$$

As there are three versions of equivalence, there are three possible automorphism groups. Let C be a code over \mathbb{F}_q . We defined the permutation automorphism group $PAut(C)$ as in (2.30). The set of monomial matrices that map C to itself forms the group $MAut(C)$ called the monomial automorphism group of C . Finally, the set of maps of the form $M\gamma$, where M is a monomial matrix and γ is a field automorphism, that map C to itself forms the group $Aut(C)$ called automorphism group of C . In the binary case all three groups are identical. If q is a prime, $MAut(C) = Aut(C)$. In general, $PAut(C) \subseteq MAut(C) \subseteq Aut(C)$.

2.4.1 The group $PAut(\mathcal{H}_q^n)$

In this section we are going to prove that for any $q > 2$ the permutation automorphism group of a q -ary Hamming code of length n is isomorphic to the unitriangular group $\mathbf{UT}_m(\mathbf{q})$ where $n = (q^m - 1)/(q - 1)$.

The parity check matrix H_m of the q -ary Hamming code \mathcal{H}_q^n of length $n = (q^m - 1)/(q - 1)$ consists of n pairwise linear independent column vectors from \mathbb{F}_q^n . Consider all nonzero vectors of length m that have 1 as their first nonzero coordinate. Let α be a primitive element of \mathbb{F}_q . In the case $m = 2$ we have

$$H_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q-2} \end{bmatrix}$$

Let for any m we have $H_m = [h_1 \ h_2 \ \cdots \ h_n]$. Then H_{m+1} can be defined by

$$H_{m+1} = \begin{bmatrix} \mathbf{0} & h_1 & h_1 & \cdots & h_1 & \cdots & h_n & h_n & \cdots & h_n \\ 1 & 0 & \alpha^0 & \cdots & \alpha^{q-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q-2} \end{bmatrix}$$

here $\mathbf{0}$ is the all zero vector of length m . Let T_m denote the column set of the matrix H_m . If $K \in GL_m(q)$, then the multiplication $y = Kx$ gives a linear mapping on \mathbb{F}_q^n .

Lemma 2.31. [10] Any matrix $L \in UT_m(q)$ gives a bijection on the set T_m .

Note that the linear map mentioned above is a bijection on T_m if the matrix L is lower unitriangular (in opposite to an upper unitriangular matrix U in the rule $y = xU$). In the following lemma we will show that in the group $GL_q(m)$ there are no bijections acting on the set T_m besides those described in Lemma (2.31).

Lemma 2.32. [10] If a matrix U belongs to $GL_m(q) \setminus UT_m(q)$, where $m \geq 1$, $q > 2$, then in the set T_m there is a vector h such that $Uh \notin T_m$.

Proof. We prove the statement by induction on m . Consider the Hamming code parity check matrix H_m multiplied on the left by a matrix U . For $m = 1$, there is nothing to prove since $UH_1 = [u_{11}] [1] = [u_{11}]$, where $u_{11} \neq 0$ and $u_{11} \neq 1$. Suppose that the statement is true for matrices of order m . Now we prove it for a matrix U of order $m + 1$. A matrix U can be represented as follows

$$U = \begin{bmatrix} \tilde{U} & b \\ c & \beta \end{bmatrix},$$

where \tilde{U} is a $m \times m$ submatrix, a column vector b and a row vector c have length m and $\beta \in \mathbb{F}_q$. We have

$$UH_{m+1} = \begin{bmatrix} b & \tilde{U}h_1 & \tilde{U}h_1 + \alpha^0 b & \cdots & \tilde{U}h_1 + \alpha^{q-2} b & \cdots & \tilde{U}h_n & \cdots & \tilde{U}h_n + \alpha^{q-2} b \\ \beta & ch_1 & ch_1 + \alpha^0 \beta & \cdots & ch_1 + \alpha^{q-2} \beta & \cdots & ch_n & \cdots & ch_n + \alpha^{q-2} \beta \end{bmatrix}$$

There are the following four possible cases to check

1. If $\det(\tilde{U}) \neq 0$ and $\tilde{U} \notin UT_m(q)$, then by induction hypothesis, there is a vector $h_j \in T_m$ such that $Uh_j \notin T_m$. Hence

$$U \begin{bmatrix} h_j \\ 0 \end{bmatrix} = \begin{bmatrix} \tilde{U}h_j \\ ch_j \end{bmatrix} \notin T_{m+1} \quad \text{and therefore} \quad h = \begin{bmatrix} h_j \\ 0 \end{bmatrix}.$$

2. Let either $\det(\tilde{U}) = 0$ or $\tilde{U} \in UT_m(q)$, and at the same time $b \neq 0$. In this case, the vector b is collinear with some vector of the set T_m . Hence we have $b = \gamma h_k$ for some $\gamma \in \mathbb{F}_q$ and $h_k \in T_m$.

If $\det(\tilde{U}) = 0$, then there is a vector h_j in T_m such that $\tilde{U}h_j = 0$.

on the other hand, if $\tilde{U} \in UT_m(q)$, then we can apply Lemma (2.31). Namely, in the set T_m there is a vector h_j that is assigned the vector h_k under the action of the matrix \tilde{U} . So we have $\tilde{U}h_j = h_k$. Combining these two subcases we can conclude that the matrix $\tilde{U}H_{m+1}$ has a submatrix of the form

$$\begin{bmatrix} \delta h_k & (\delta + \alpha^0 \gamma) h_k & (\delta + \alpha^1 \gamma) h_k & \cdots & (\delta + \alpha^{q-2} \gamma) h_k \\ ch_j & ch_j + \alpha^0 \beta & ch_j + \alpha^1 \beta & \cdots & ch_j + \alpha^{q-2} \beta \end{bmatrix},$$

where δ equals either 0 or 1 in accordance with the subcases considered above. Since the set $\{\delta, \delta + \alpha^0 \gamma, \delta + \alpha^1 \gamma, \dots, \delta + \alpha^{q-2} \gamma\}$ coincides with the set of all field elements, then for $q > 2$ one can find an integer l from $[0, q-2]$ such that $\delta + \alpha^l \gamma \neq 0$ and $\delta + \alpha^l \gamma \neq 1$. Hence,

$$U \begin{bmatrix} h_j \\ \alpha^l \end{bmatrix} = \begin{bmatrix} (\delta + \alpha^l \gamma) h_k \\ ch_j + \alpha^l \beta \end{bmatrix} \notin T_{m+1} \quad \text{and} \quad h = \begin{bmatrix} h_j \\ c\alpha^l \end{bmatrix}.$$

3. If $\tilde{U} \in UT_m(q)$ and $b = 0$, then we have $\beta \neq 0$ for $\det(U) \neq 0$. In addition, we obtain $\beta \neq 1$ for $U \notin UT_{m+1}(q)$. This implies that

$$U \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \beta \end{bmatrix} \notin T_{m+1} \quad \text{and therefore} \quad h = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

4. It should be noted that the conditions $\det(\tilde{U}) = 0$ and $b = 0$ are not compatible since $\det(U) \neq 0$.

□

Theorem 2.33. [10] For any $n = (q^m - 1)/(q - 1)$, where $m \geq 2$, $q > 2$, it is true that

$$PAut(\mathcal{H}_q^n) \cong \mathbf{UT}_m(q).$$

Proof. We have seen that the Hamming code monomial automorphism group is isomorphic to the general linear group, namely $MAut(\mathcal{H}_q^n) \cong GL_m(q)$. The isomorphism $\theta : MAut(\mathcal{H}_q^n) \rightarrow GL_m(q)$ can be defined by

$$\theta : M \mapsto K, \quad \text{where} \quad K^\top H_m = H_m M^\top.$$

Here H_m is the parity check matrix of the Hamming code \mathcal{H}_q^n , the matrix M is a monomial $n \times n$ matrix and $K \in GL_m(q)$.

By Lemmas (2.31) and (2.32) we have $\theta(PAut(\mathcal{H}_q^n)) = UT_m(q)$. Therefore a restriction of the isomorphism θ on the permutation automorphism group $\phi = \theta|_{PAut(\mathcal{H}_q^n)}$ is an isomorphism between $PAut(\mathcal{H}_q^n)$ and $UT_m(q)$. This proves the theorem. \square

The Automorphism groups of Reed-Muller And Generalized Reed-Muller Codes

In this chapter we consider linear codes of length q^m , $q = p^r$ and p is a prime, over a finite field K of characteristic p . Usually these codes are called extended primitive codes. Let \mathbb{F} be the finite field of order q^m ; an automorphism of such a code C is a permutation on \mathbb{F} which preserves C .

3.1 Some Concepts of Reed-Muller Codes

In this section, we introduce the binary Reed-Muller codes. The binary codes were first constructed and explored by Muller in 1954, and a majority logic decoding algorithm for them was described by Reed also in 1954. Although their minimum distance is relatively small, they are of practical importance because of the ease with which they can be implemented and decoded. They are of mathematical interest because of their connection with finite affine and projective geometries.

These codes can be defined in several different ways. One of these is a recursive definition based on the $(u, u + v)$ construction. Let m be a positive integer and r nonnegative integer with $r \leq m$. The binary codes we construct will have length 2^m . For each length there will be $m + 1$ linear codes, denoted $RM(r, m)$ and called the r -th order Reed-Muller code which is a binary linear code of parameters $[2^m, \binom{m}{r} +$

$$\binom{m}{1} + \dots + \binom{m}{r}, 2^{m-r}].$$

Definition 3.1. [5] *The (first order) Reed-Muller codes $RM(1, m)$ are binary codes defined, for all integers $m \geq 1$, recursively as follows:*

(i) $RM(1, 1) = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$

(ii) for $m \geq 1$,

$$RM(1, m + 1) = \{(u, u) : u \in RM(1, m)\} \cup \{(u, (u + 1)) : u \in RM(1, m)\}$$

The codes $RM(0, m)$ and $RM(m, m)$ are trivial codes: the 0th order RM code $RM(0, m)$ is the binary repetition code of length 2^m with basis $\{1\}$, and the m -th order RM code $RM(m, m)$ is the entire space $\mathbb{F}_2^{2^m}$. A generator matrix $G(r, m)$ for $RM(r, m)$ is

$$G(r, m) = \begin{bmatrix} G(r, m - 1) & G(r, m - 1) \\ 0 & G(r - 1, m - 1) \end{bmatrix}.$$

Proposition 3.2. [5]

(i) A generator matrix of $RM(1, 1)$ is

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(ii) If G_m is a generator matrix for $RM(1, m)$, then a generator matrix for $RM(1, m + 1)$ is

$$G_{m+1} = \begin{bmatrix} G_m & G_m \\ 0 \dots 0 & 1 \dots 1 \end{bmatrix}.$$

Proof. see [5]. □

Example 3.3. :

(i) $RM(1, 2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$.

A generator matrix of $RM(1, 2)$ is $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$

(ii)

$$G(2, 3) = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array} \right].$$

From these matrices, notice that $RM(1, 2)$ and $RM(2, 3)$ are both the set of all even weight vectors in \mathbb{F}_2^4 and \mathbb{F}_2^8 , respectively.

Definition 3.4. [5] For any $r \geq 2$, the r th order Reed-Muller codes $RM(r, m)$, are defined, for $m \geq r - 1$, recursively by

$$RM(r, m + 1) = \begin{cases} \mathbb{F}_2^{2^r} & \text{if } m = r - 1, \\ \{(u, u + v) : u \in RM(r, m), v \in RM(r - 1, m)\} & \text{if } m > r - 1. \end{cases}$$

Theorem 3.5. [3] Let r be an integer with $0 \leq r \leq m$. Then the following hold:

- (i) $RM(i, m) \subseteq RM(j, m)$, if $0 \leq i \leq j \leq m$,
- (ii) The dimension of $RM(r, m)$ equals $\binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$,
- (iii) The minimum weight of $RM(r, m)$ equals 2^{m-r} ,
- (iv) $RM(m, m)^\perp = 0$, and if $0 \leq r \leq m$, then $RM(r, m)^\perp = RM(m - r - 1, m)$.

Proof. (i) It is certainly true if $m = 1$ by direct computation and if $j = m$ as $RM(m, m)$ is the full space $\mathbb{F}_2^{2^m}$.

Assume inductively that $RM(k, m - 1) \subseteq RM(\ell, m - 1)$ for all $0 \leq k \leq \ell < m$.

Let $0 < i \leq j < m$. Then:

$$\begin{aligned} RM(i, m) &= \{(u, u + v) | u \in RM(i, m - 1), v \in RM(i - 1, m - 1)\} \\ &\subseteq \{(u, u + v) | u \in RM(j, m - 1), v \in RM(j - 1, m - 1)\} \\ &= RM(j, m). \end{aligned}$$

So (i) follows by induction if $0 < i$. If $i = 0$, we only need to show that the all-one vector of length 2^m is in $RM(j, m)$ for $j < m$. Inductively assume the all-one vector of length 2^{m-1} is in $RM(j, m - 1)$. Then by definition (3.4), we see that the all-one vector of length 2^m is in $RM(j, m)$ as one choice for \mathbf{u} is $\mathbf{1}$ and one choice for \mathbf{v} is $\mathbf{0}$.

(ii) The result is true for $r = m$ as $RM(m, m) = \mathbb{F}_2^{2^m}$ and

$$\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{m} = 2^m.$$

It is also true for $m = 1$ by inspection. Now assume that $RM(i, m - 1)$ has dimension

$$\binom{m-1}{0} + \binom{m-1}{1} + \cdots + \binom{m-1}{i} \text{ for all } 0 \leq i < m.$$

Thus $RM(r, m)$ has dimension the sum of the dimensions of $RM(r, m - 1)$ and $RM(r - 1, m - 1)$, that is,

$$\binom{m-1}{0} + \binom{m-1}{1} + \cdots + \binom{m-1}{r} + \binom{m-1}{0} + \binom{m-1}{1} + \cdots + \binom{m-1}{r-1}.$$

The result follows by the elementary properties of binomial coefficients:

$$\binom{m-1}{0} = \binom{m}{0} \text{ and } \binom{m-1}{i-1} + \binom{m-1}{i} = \binom{m}{i}.$$

(iii) It is again valid for $m = 1$ by inspection and for both $r = 0$ and $r = m$ as $RM(0, m)$ is the binary repetition code of length 2^m and $RM(m, m) = \mathbb{F}_2^{2^m}$. Assume that $RM(i, m - 1)$ has minimum weight 2^{m-1-i} for all $0 \leq i < m$. If $0 < r < m$, then by definition (3.4), $RM(r, m)$ has minimum weight $\min\{2 \cdot 2^{m-1-r}, 2^{m-1-(r-1)}\} = 2^{m-r}$.

(iv) To prove it, we first note that $RM(m, m)^\perp$ is $\{\mathbf{0}\}$ since $RM(m, m) = \mathbb{F}_2^{2^m}$. So if we define $RM(-1, m) = \{\mathbf{0}\}$, then $RM(-1, m)^\perp = RM(m - (-1) - 1)$ for all $m > 0$. By direct computation, $RM(r, m)^\perp = RM(m - r - 1, m)$ for all r with $-1 \leq r \leq m = 1$. Assume inductively that if $-1 \leq i \leq m - 1$, then $RM(i, m - 1)^\perp = RM((m - 1) - i - 1, m - 1)$. Let $0 \leq r < m$. To prove $RM(r, m)^\perp = RM(m - r - 1, m)$, it suffices to show that $RM(m - r - 1, m) \subseteq RM(r, m)^\perp$ as $\dim RM(r, m) + \dim RM(m - r - 1, m) = 2^m$ by (ii). Notice that with the definition of $RM(-1, m)$, (3.4) extends to the case $r = 0$. Let $\mathbf{x} = (\mathbf{a}, \mathbf{a} + \mathbf{b}) \in RM(m - r - 1, m)$ where $\mathbf{a} \in RM(m - r - 1, m - 1)$ and $\mathbf{b} \in RM(m - r - 2, m - 1)$, and let $\mathbf{y} = (\mathbf{u}, \mathbf{u} + \mathbf{v}) \in RM(r, m)$ where $\mathbf{u} \in RM(r, m - 1)$ and $\mathbf{v} \in RM(r - 1, m - 1)$. Then $\mathbf{x} \cdot \mathbf{y} = 2\mathbf{a} \cdot \mathbf{u} + \mathbf{a} \cdot \mathbf{v} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v} = \mathbf{a} \cdot \mathbf{v} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v}$. Each term is 0 as follows. As $\mathbf{a} \in RM(m - r - 1, m - 1) = RM(r - 1, m - 1)^\perp$, $\mathbf{a} \cdot \mathbf{v} = 0$. As $\mathbf{b} \in RM(m - r - 2, m - 1) = RM(r, m - 1)^\perp$, $\mathbf{b} \cdot \mathbf{u} = 0$ and $\mathbf{b} \cdot \mathbf{v} = 0$ using

$RM(r-1, m-1) \subseteq RM(r, m-1)$ from (i) we conclude that $RM(m-r-1, m) \subseteq RM(r, m)^\perp$, completing (iv). □

Theorem 3.6. [5] *The dual code $RM(1, m)^\perp$ is (equivalent to) the extended binary Hamming code.*

Proof. A generator matrix of $RM(1, 1)$ is

$$G_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

then G_m is of the form

$$\left[\begin{array}{c|cccc} 1 & 1 & \cdots & 1 \\ \hline 0 & & & \\ \vdots & & H_m & \\ 0 & & & \end{array} \right]$$

where H_m is some matrix. Moving the first coordinate to the last and moving the first row of the matrix to the last, we obtain the following generator matrix G'_m for an equivalent code:

$$\left[\begin{array}{cccc|c} & & & & 0 \\ & & & & \vdots \\ & & H_m & & 0 \\ \hline 1 & \cdots & 1 & & 1 \end{array} \right]$$

Using Theorem 5.1.9 in [5] if we show that H_m is a parity check matrix for $Ham(m, 2)$, then G'_m is the parity check matrix for $\overline{Ham(m, 2)}$, so $RM(1, m)^\perp$ is equivalent to $\overline{Ham(m, 2)}$.

To show H_m is a parity check matrix for $Ham(m, 2)$, we need to show that the columns of H_m consist of all the nonzero vectors of length m . Indeed, when $m = 1, 2$, the columns of H_m consist of all the nonzero vectors of length m . Now suppose that the columns of H_m consist of all the nonzero vectors of length m , for some m . By the definition of G_m it follows readily that the columns of H_{m+1} consist of the following:

$$\begin{pmatrix} c \\ 0 \end{pmatrix}, \begin{pmatrix} c \\ 1 \end{pmatrix}, \text{ and } \begin{pmatrix} \mathbf{0}^T \\ 1 \end{pmatrix},$$

where c is one of the columns of H_m and $\mathbf{0}$ is the zero vector of length m . It is clear that the vectors in this list make up exactly all the nonzero vectors of length $m + 1$. Hence, by induction, the columns of H_m consist of all the nonzero vectors of length m . □

3.2 Automorphism groups of Reed-Muller codes

Let $A = (a_{ij})$ be an invertible $m \times m$ binary matrix and let b be a binary m -tuple.

The transformation

$$T : \text{replace } \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} \text{ by } A \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} + b \quad (3.1)$$

is a permutation of the set 2^m m -tuples which sends 0 to b . We may also think of T as permuting Boolean function:

$$T : \text{replace } f(v_1, \dots, v_m) \text{ by } f(\sum a_{1j}v_j + b_1, \dots, \sum a_{mj}v_j + b_m). \quad (3.2)$$

The set of all such transformations T forms a group, with composition as the group operation.

The order of this group is found as follows:

The first column of A may be chosen in $2^m - 1$ ways, the second in $2^m - 2$, the third in $2^m - 2^2, \dots$. Furthermore there are 2^m choices for b . So this group, which is called the general affine group and is denoted by $GA(m)$, has order

$$|GA(m)| = (2^m)(2^m - 1)(2^m - 2)(2^m - 2^2)\dots(2^m - 2^{m-1}). \quad (3.3)$$

A useful approximation to its order is

$$|GA(m)| = 0.29 2^{m^2+m}, \text{ for } m \text{ large.}$$

It is clear from (3.2) that if f is a polynomial of degree r , so is Tf . Therefore the group $GA(m)$ permutes the codewords of the r th order RM code $RM(r, m)$, and

$$GA(m) \subset \text{Aut } RM(r, m). \quad (3.4)$$

The subgroup of $GA(m)$ consisting of all transformations

$$T : \text{replace } \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} \text{ by } A \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} \quad (3.5)$$

(i.e., for which $b = 0$) is the general linear group $GL(m, 2)$ and has order

$$|GL(m, 2)| = (2^m - 1)(2^m - 2)(2^m - 2^2)\dots(2^m - 2^{m-1}) \approx (0.29)2^{m^2} \text{ for } m \text{ large.} \quad (3.6)$$

Since (3.5) fixes the zero m -tuple, the group $GL(m, 2)$ permutes the codewords of the punctured RM code $RM(r, m)^*$:

$$GL(m, 2) \subset \text{Aut } RM(r, m)^*. \quad (3.7)$$

Some group actions don't just take any element to any other element, but can do so in pairs. Of course, we have to assume our set has at least two elements.

Definition 3.7. A group G of permutations acting on a set Ω is called k -transitive on Ω , if for every ordered k -tuple (a_1, \dots, a_k) of distinct elements of Ω and for every k -tuple (b_1, \dots, b_k) of distinct elements of Ω , there is an element $\sigma \in G$ such that $b_i = \sigma(a_i)$ for $1 \leq i \leq k$. If $k = 1$ we call the group transitive.

Definition 3.8. [29] An action of a group G on a set X , with $|X| \geq 2$, is called doubly transitive when, for any two ordered pairs of distinct elements (x, x') and (y, y') in X , there is a $g \in G$ such that $y = gx$ and $y' = gx'$.

The distinctness of elements means $x \neq x'$ and $y \neq y'$. We say g takes the pair (x, x') to the pair (y, y') .

Proposition 3.9. [1] $GL(m, 2)$ is doubly transitive and $GA(m)$ is triply transitive.

Proof. see [1]. □

Definition 3.10. An m -flat is any subspace of a projective geometry $PG(n, q)$ of dimension m , when the points of a hyperplane H ; that is a subgeometry of co-dimension 1 are removed.

In affine plane, the 1-flats are the lines of the plane and the points are the 0-flats of the plane.

Theorem 3.11. [1] For $1 \leq r \leq m - 1$,

$$(a) \text{Aut}RM(r, m)^* \subset \text{Aut}RM(r + 1, m)^*$$

$$(b) \text{Aut}RM(r, m) \subset \text{Aut}RM(r + 1, m)$$

Proof. (b) Let x_1, \dots, x_B be the minimum weight vectors of $RM(r, m)$. For $\pi \in \text{Aut}RM(r, m)$, let $\pi x_i = x_{i'}$. Now x_i is an $(r - m)$ -flat. If Y is any $(m - r - 1)$ -flat, then for some $i, j, Y = x_i * x_j$. Therefore

$$\begin{aligned} \pi Y &= \pi(x_i * x_j) \\ &= \pi x_i * \pi x_j \\ &= x_{i'} * x_{j'}, \end{aligned}$$

which is the intersection of two $(m - r)$ -flats; and contains 2^{m-r-1} points. Since π is a permutation. Thus πY is an $(m - r - 1)$ -flat. So π permutes the generators of $RM(r + 1, m)$, and therefore preserves the whole code. \square

Proposition 3.12. [1]

(i) $AutRM(r, m)^* = S_{2^{m-1}}$ for $r = 0$ and $m - 1$,

(ii) $AutRM(r, m) = S_{2^m}$ for $r = 0$ $m - 1$, and m .

In the remaining cases we show that equality holds in (3.4) and (3.7).

Theorem 3.13. [1]

(i) $AutRM(r, m)^* = GL(m, 2)$

(ii) $AutRM(r, m) = GA(m)$.

Proof. (i) We have if we add 1 to simplex code H_m^\perp it will be $RM(1, m)^*$ code by Theorem (3.6), and if we puncture 0 coordinate from $RM(1, m)^*$. So, since the automorphism group of the simplex code H_m^\perp is $AutRM(1, m)^*$. From Equation (3.7), and that if the columns of the generator matrix are distinct the automorphism group of a binary linear code of dimension k^m is isomorphic to a subgroup of $GL(k^m, 2)$, since H_m^\perp has dimension m ,

$$AutH_m^\perp = AutRM(1, m)^* = GL(m, 2)$$

Finally, since $AutC = AutC^\perp$, $AutH_m = GL(m, 2)$.

(ii) Let $G_1 = AutRM(1, m)^*$, $G_2 = AutRM(1, m)$. Then, G_1 is a subgroup of G_2 which fixes the 0 coordinate. Since $GA(m)$ is transitive, so is G_2 . Each coset of G_1 in G_2 sends 0 to a different point, so $|G_2| = 2^m |G_1|$. Therefore from (3.3) and (3.6)

$G_2 = GA(m)$. Again since $AutC = AutC^\perp$, $AutRM(m - 2, m) = AutRM(1, m) = GA(m)$.

(iii) From (3.11), (i), and (ii), we have that $GA(m) = AutRM(1, m) \subseteq AutRM(2, m) \subseteq \dots \subseteq AutRM(m - 2, m) = GA(m)$.

$GL(m, 2) = AutRM(1, m)^* \subseteq AutRM(2, m)^* \subseteq \dots \subseteq AutRM(m - 2, m)^* = GL(m, 2)$.

\square

3.3 Generalized Reed- Muller Codes

S.D. Berman showed that the binary Reed-Muller codes may be identified with the powers of the radical of the group algebra over the two elements field \mathbb{F}_2 of an elementary abelian 2-group. P. Charpin gave a generalization of Berman's result for Reed-Muller codes over a prime field. Recently, I.N. Tumaikin studied the connections between Basic Reed-Muller codes and the radical powers of the modular algebra $\mathbb{F}_q[H]$ where H is a multiplicative group isomorphic to the additive group of the field \mathbb{F}_q of order $q = p^r$ where p is a prime number and r is an integer. The index of nilpotency of the radical of $\mathbb{F}_q[H]$ is $r(p - 1) + 1$. The modular algebra $\mathbb{F}_p[X_1, \dots, X_m]/(X_1^p - 1, \dots, X_m^p - 1)$ where $m \geq 1$ is used to represent the ambient space of the codes. It is isomorphic to the group algebra $\mathbb{F}_p[\mathbb{F}_{p^m}]$.

3.3.1 The modular algebra $A = \mathbb{F}_q[X_1, \dots, X_m]/(X_1^q - 1, \dots, X_m^q - 1)$ and the GRM codes

Let $q = p^r$ with p a prime and $r \geq 1$ an integer. We consider the finite field \mathbb{F}_q of order q .

Let $P(m, q)$ be the vector space of the reduced polynomials in m variables over \mathbb{F}_q :

$$P(m, q) := P(Y_1, \dots, Y_m) = \sum_{i_1=0}^{q-1} \dots \sum_{i_m=0}^{q-1} u_{i_1 \dots i_m} Y_1^{i_1} \cdot Y_m^{i_m} | u_{i_1 \dots i_m} \in \mathbb{F}_q.$$

The polynomial functions from $(\mathbb{F}_q)^m$ to \mathbb{F}_q are given by the polynomials of $P(m, q)$.

Let v be an integer such that $0 \leq v \leq m(q - 1)$. Consider the subspace of $P(m, q)$ defined by

$$P_v(m, q) := \{P(Y_1, \dots, Y_m) \in P(m, q) | \deg(P(Y_1, \dots, Y_m)) \leq v\}.$$

Consider the ideal $I = (X_1^q - 1, \dots, X_m^q - 1)$ of the ring $\mathbb{F}_q[X_1, \dots, X_m]$. Set $x_1 = X_1 + I, \dots, x_m = X_m + I$. Then

$$A = \left\{ \sum_{i_1=0}^{q-1} \dots \sum_{i_m=0}^{q-1} a_{i_1 \dots i_m} x_1^{i_1} \dots x_m^{i_m} | a_{i_1 \dots i_m} \in \mathbb{F}_q \right\} \quad (3.8)$$

A is a local ring with maximal ideal M which is the radical of A .

Let d be an integer such that $0 \leq d \leq m(q - 1)$. Consider the power M^d of M .

A linear basis of M^d over \mathbb{F}_q is

$$B_d = \{(x_1 - 1)^{i_1} \dots (x_m - 1)^{i_m} \mid 0 \leq i_1, \dots, i_m \leq q - 1, i_1 + \dots + i_m \geq d\} \quad (3.9)$$

We have the following ascending sequence of ideals:

$$\{0\} = M^{m(q-1)+1} \subset M^{m(q-1)} \subset \dots \subset M^2 \subset M \subset A \quad (3.10)$$

Let us fix an order on the set of monomials

$$\{X_1^{i_1} \dots X_m^{i_m} \mid 0 \leq i_1, \dots, i_m \leq q - 1\}.$$

Then we have the following remark:

Remark 3.14. Each element $\sum_{i_1=0}^{q-1} \dots \sum_{i_m=0}^{q-1} a_{i_1 \dots i_m} x_1^{i_1} \dots x_m^{i_m}$ of A can be identified with the vector $(a_{i_1 \dots i_m}), 0 \leq i_1, \dots, i_m$ of $(\mathbb{F}_q)^{q^m}$ and vice-versa. Hence the modular algebra A is identified with $(\mathbb{F}_q)^{q^m}$. Let α be a primitive element of the finite field \mathbb{F}_q . Then $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$

Set

$$\beta_0 = 0 \quad \text{and} \quad \beta_i = \alpha^{i-1} \quad \text{for} \quad 1 \leq i \leq q - 1. \quad (3.11)$$

When considering $P(m, q)$ and A as vector spaces over \mathbb{F}_q , we have the following isomorphism:

$$\phi : P(m, q) \longrightarrow A$$

$$P(Y_1, \dots, Y_m) \longmapsto \sum_{i_1=0}^{q-1} \dots \sum_{i_m=0}^{q-1} P(\beta_{i_1}, \dots, \beta_{i_m}) x_1^{i_1} \dots x_m^{i_m} \quad (3.12)$$

The generalized Reed-Muller code of length q^m and of order $v (0 \leq v \leq m(q - 1))$ over \mathbb{F}_q is defined by

$$C_v(m, q) = \{(P(\beta_{i_1}, \dots, \beta_{i_m}))_{0 \leq i_1, \dots, i_m \leq q-1} \mid P(Y_1, \dots, Y_m) \in P_v(m, q)\}. \quad (3.13)$$

It is a subspace of $(\mathbb{F}_q)^{q^m}$ and we have the following ascending sequence:

$$\{0\} \subset C_0(m, q) \subset C_1(m, q) \subset \dots \subset C_{m(q-1)}(m, q) = (\mathbb{F}_q)^{q^m} \quad (3.14)$$

We need the following notations:

Notations Set $[0, q - 1] = \{0, 1, 2, \dots, q - 1\}$

Let $S = [0, n], n = q^m - 1$; for each $s \in S$ let us define

$$\phi_s : x \in A \mapsto \phi_s(x) = \sum_{g \in G} x_g g^s, \quad (3.15)$$

where $\phi_s(x)$ can be calculated in an over field of $(\mathbb{F}_q)^{q^m}$ and $\mathbb{F}_q = G$. A code C is an extended cyclic code if and only if $\text{Aut}(C)$ contains the permutations:

$$\pi_{u,0} : x \in A \mapsto \sum_{g \in G} x_g X^{ug}, \quad u \in G^*$$

As α is a primitive element of G . The codeword x is an extension of a polynomial which has the root α^s if and only if $\phi_s = 0$. Thus an extended cyclic code can be uniquely defined by the set $\{s \in S | \phi_s(C) = 0\}$

Definition 3.15. [18] Let T be a subset of S containing 0, and assume that T is invariant under the multiplication by q mod n . Then

$$C = \{x \in A | \phi_s = 0, s \in T\}, \quad (3.16)$$

is an extended cyclic q -ary code. We say that T is the defining-set of C .

The dual of the q -ary RM-code of order $m(q - 1) - v$, denoted by $C_v(m, q)$ with defining set $I_v(m, q) = \{s \in S | \omega_q(s) < v\}$ is the code $C_\mu(m, q)$ with $\mu = m(q - 1) - v + 1$ [31], where the q -weight of $s = \omega(s) = \sum_{i=0}^{m-1} s$ and that for each q' dividing q , we can define a class of q' -ary extended cyclic codes of A . Then we can always define the p -ary RM-codes as codes of A : that is the codes $C_v(rm, p)$, with defining set $I_v(m, p)$.

The following theorem, due to Delsarte, gives a necessary and sufficient condition for cyclic q -ary codes to be invariant under the group $GL(m, q)$.

Theorem 3.16. [18] Let C be a code of A . Then $\text{Aut}(C)$ contains $GL(m, q)$ if and only if C is an extended cyclic q -ary code, the defining set T of which satisfies:

$$s \in T \text{ and } t \text{ satisfies } (I) \Rightarrow t \in T, \quad (3.17)$$

where (I) is the condition

$$(I) : \omega_q(p^k t) \leq \omega_q(p^k s), \quad k \in [0, r - 1]$$

Remark 3.17. The codes $C_v(m, q)$ are invariant under $GL(m, q)$. If $m = 1$. i.e., if we consider codes of length q over $GF(q^e)$ we have the q -weight of s as $\omega_q(s) = s$ for $s \in [0, q - 1]$. Then the condition (I) is equivalent to $t_i \leq s_i$ $i \in [0, r - 1]$ where (s_0, \dots, s_r) and (t_0, \dots, t_r) are respectively the coefficients of the p -ary expansion of s and t .

Theorem (3.16) characterizes the codes of A which are invariant under $GL(rm, p)$. In this case T is invariant under the multiplication by p and the condition (I) becomes: $\omega_p(t) \leq \omega_p(s)$. Thus there is an element v of $[1, rm(p - 1)]$ such that the defining-set T is the set $\{s | \omega_p(s) < v\}$, which is the defining-set $I_v(rm, p)$ of the p -ary RM - code $C_v(rm, p)$. Then a code of A which is invariant under $GL(rm, p)$ is a p -ary RM - code.

Let U and V be two codes of A ; we denote by UV the code generated by the products xy , $x \in U$ and $y \in V$ and we say that UV is the product of U and V . Let $\pi_{M,0} \in GL(m, q)$; we have

$$\pi_{M,0}(xy) = \pi_{M,0}(x)\pi_{M,0}(y)$$

since

$$\pi_{M,0}(X^g X^h) = X^{M(g+h)} = X^{Mg} + X^{Mh}.$$

Hence if U and V are invariant under $\pi_{M,0}$, then the code UV is invariant under $\pi_{M,0}$. In particular, a product of two extended cyclic codes is an extended cyclic code.

Theorem 3.18. [18] Let v and v' be such that $v + v' \leq m(q - 1)$. Then the product of $C_v(m, q)$ and $C_{v'}(m, q)$ satisfies:

$$C_v(m, q)C_{v'}(m, q) \subset C_{v+v'}(m, q)$$

.

Proof. see [18] □

3.3.2 The minimum weight codewords of the GRM-codes

Recall that $A = K[G]$, $G = GF(q^m)$ and $K = GF(q^e)$. For any element x of A , let us define the support of x as the set:

$$\text{supp}(x) = \{g \in G | x_g \neq 0\}, \quad \text{where } x = \sum_{g \in G} x_g X^g. \quad (3.18)$$

The weight of x is: $w(x) = |\text{supp}(x)|$. Let g be a nonzero element of G and let $v \in [1, q - 1]$. We denote by $C_v(\{g\}, q)$ the extended Reed-Solomon code of length q and minimum distance $v + 1$, considered as a code of A in the sense that each codeword has its support in the subspace $gGF(q)$ of G :

$$C_v(\{g\}, q) = \{x \in A \mid x = \sum_{\lambda \in GF(q)} x_{\lambda g} X^{\lambda g} \text{ and } \phi_s(x) = 0, s \in [0, v[\}. \quad (3.19)$$

Let $x \in C_v(\{g\}, q)$ and let $t \in S$ be such that $w_q(t) < v$. Since $\lambda^q = \lambda$, we have:

$$\phi_t(x) = \sum_{\lambda \in GF(q)} x_{\lambda g} (\lambda g)^t = g^t \sum_{\lambda \in GF(q)} x_{\lambda g} \lambda^{w_q(t)} = 0.$$

Then $\phi_t = 0$, for each $t \in I_v(m, q)$. We have the following:

Lemma 3.19. [18] Let $v \in [1, q - 1]$. Then the code $C_v(\{g\}, q)$ is contained in $C_v(m, q)$, for all $g \in G^*$.

Let $k \in [1, m]$ and let V be a k -dimensional subspace of G . Let $x = \sum_{g \in V} X^g$; the following property is proved by Kasami et al. in [18]:

$$s \in S \text{ and } w_q(s) < k(q - 1) \Rightarrow \phi_s(x) = 0 \quad (3.20)$$

In accordance with the definition of $C_{k(q-1)}(m, q)$, this property implies the following.

Lemma 3.20. [18] Let $k \in [1, m]$ and define the subset of A :

$$A_k = \left\{ \sum_{g \in V} X^g \mid V \text{ is a } k\text{-dimensional subspace of } G \right\} \quad (3.21)$$

Then $A_k \subset C_{k(q-1)}(m, q)$.

Now we are able to present a description of the set of the minimum weight codewords (mwc's) of any GRM-code. An (mwc's) can be identified with an element y of an A_k or with an mwc z of a code $C_v(\{g\}, m)$ or with a product of type yz .

In [31] Delsarte et al. gave another description and the enumeration of the mwc's of the GRM-codes of length q^m over $GF(q)$. The following lemma shows that their results are available for $K = GF(q^e)$, $e > 1$. So we can present the enumeration of the mwc's in the context (3.22).

Lemma 3.21. [18] Set $K = GF(q^e)$. Let C be an extended cyclic q -ary code. Let x be an mwc of C . Then $x = \lambda x'$ where $\lambda \in K$ and x' is an mwc of C whose coefficients are in $GF(q)$.

Proof. see [18] □

Theorem 3.22. [31] *Let $v \in [1, m(q-1)[, m(q-1) - v = u(q-1) + v$ with $v \in [0, q-1[$. Then the number of the minimum weight codewords of the code $C_v(m, q)$ is*

$$L_v = |K^*|q^u \prod_{i=0}^{m-u-1} \frac{q^{m-i} - 1}{q^{m-u-i} - 1} N_v, \quad (3.22)$$

where $N_0 = 1$ and, for $v > 0$,

$$N_v = \binom{q}{v} \frac{q^{m-u} - 1}{q - 1}$$

Proof. see [31] □

Theorem 3.23. [18] *Let $v = b(q-1) + a$, $a \in [0, q-1[$, $b \in [0, m[$. A minimum weight codeword (mwc) of the code $C_v(m, q)$ is an element of A of the form:*

$$x = \lambda X^h y z, \quad \lambda \in \mathbb{F}_q^*, \quad h \in G, \quad y \in A, \quad z \in A \quad (3.23)$$

where

- If $b = 0$ then $y = X^0$; otherwise $y \in A_b$.
- If $a = 0$ then $z = X^0$; otherwise there is $g \in G$, $g \notin \text{supp}(y)$; such that z is an mwc of the code $C_a(\{g\}, q)$.

The set A_b and the code $C_a(\{g\}, q)$ are respectively defined by (3.21) and (3.19).

Proof. We have that the minimum distance of the GRM-code $C_v(m, q)$ equals $(a+1)q^b$. When $a > 0$ the codeword z can be considered as an mwc of an extended Reed-Solomon code of length q and minimum distance $a+1$; thus $w(z) = a+1$. From Lemma (3.19), z is an mwc of $C_{b(q-1)}(m, q)$. If $a > 0$ and $b > 0$, the Theorem (3.18) implies that the product yz is an element of $C_{b(q-1)+a}(m, q)$. Moreover:

$$q^b(a+1) \leq w(yz) \leq w(y)w(z) \leq q^b(a+1),$$

which means that $w(x) = (a+1)q^b$. Then a codeword x which has the form (3.23) is an mwc of $C_v(m, q)$. Note that $yz \neq 0$, because the support of yz contains at least two cosets of a b -dimensional subspace of G .

Let R_v be the number of the x 's defined by (3.23) and let $m(q-1) - v = u(q-1) + v$, $v \in [0, q-1[$. We want to prove that $R_v = L_v$ (where L_v is given by 3.22). In all

cases the support of x is contained in an $(m - u)$ -dimensional affine subspace of G . There are

$$\lambda_u = q^u \prod_{i=0}^{m-u-1} \frac{q^{m-i} - 1}{q^{m-u-i} - 1}$$

such affine subspaces. If $v = 0$, we have $a = 0$ and $R_v = \lambda_u |K^*| = L_v$. Suppose now that $v \neq 0$ and fix $g \in G^*$. Then the code $C_a(\{g\}, q)$, is any extended RS-code, satisfies the following property,

Property 1. For each subset Λ of $GF(q)$ such that $|\Lambda| = a + 1$, there is an *mwc* of $C_a(\{g\}, q)$ the support of which is the set $\lambda g | \lambda \in \Lambda$.

There are

$$\frac{q^{m-u}}{q-1}$$

possibilities for the choice of g in an $(m - u)$ -dimensional affine subspace of G . Then we have

$$R_v = |K^*| \binom{q}{a+1} \frac{q^{m-u}}{q-1} \lambda_u = L_v$$

since $\lambda_0 = 1$ and $\binom{q}{a+1} = \binom{q}{v}$. □

3.4 The Automorphism groups of GRM-codes

We denote by $\Theta = \{\theta | i \in [0, r - 1]\}$ the Galois group of the field $GF(q)$, $q = p^r$. Since the field $GF(q^m)$, here denoted G , is an F_p -vector-space, each element of Θ can be considered as a linear permutation on G , $\theta_i : g \in G \rightarrow g^{p^i}$, involving a transformation on A . We denote by $\bar{G}(m, q)$ the set of the permutations on G :

$$\theta(M, h, i) : g \in G \mapsto (Mg)^{p^i} + h, \quad h \in G, i \in [0, r - 1], \quad (3.24)$$

where M is a nonsingular matrix of order m over $GF(q)$. The group $\bar{G}(m, q)$ is usually called the group of semi-affine bijection on G (denoted $GSA_f(E)$, $F = GF(q)$ and $E = G$.) The group $\bar{G}(m, q)$ contains $GL(m, q)$; if $q = p$, Θ contains only the identity and we have $\bar{G}(m, q) = GL(m, q)$.

Let C be an extended cyclic q -ary code in A , with defining set T . Then θ_i is contained in $Aut(C)$ if and only if T is invariant under the multiplication by p^i modulo $q^m - 1$. Indeed we have, for any $x \in C$ and any $s \in T$:

$$\phi_s(\theta_i(x)) = \phi_s \left(\sum_{g \in G} x_g X^{g^{p^i}} \right) = \sum_{g \in G} x_g (g^{p^i})^s = \phi_{sp^i}(x)$$

where ϕ_s is defined by (3.15) and C by (3.18). In particular, we shall show that, in general, q -ary RM-code cannot be invariant under $\theta_i, i \neq 0$.

Lemma 3.24. [18] *Let $q = p^r, r > 1, v \in [2, m(q-1) - 1]$. Then, for all $i \in [1, r-1]$, the set $I_v(m, q)$ is not invariant under the multiplication by p^i modulo $q^m - 1$. In other words, the set $\Theta \cap \text{Aut}(C_v(m, q))$ is reduced to the identity.*

Proof. The dual of the code $C_v(m, q)$ is $C_\mu(m, q), \mu = m(q-1) - v + 1$. Two dual codes have the same automorphism group. So we need to prove the lemma only for

$$v < \frac{m(q-1) + 1}{2}$$

We state the property:

H_v : For each $i, i \in [1, \lfloor \frac{r}{2} \rfloor]$, there is $s \in I_v(m, q)$ such that $p^i s \notin I_v(m, q)$,

where $\lfloor \frac{r}{2} \rfloor$ denotes the integer part of $\frac{r}{2}$.

Assume that H_v is true. Suppose that there is a $j, j \in]\lfloor \frac{r}{2} \rfloor, r-1]$, such that $I_v(m, q)$ is invariant under the multiplication by p^j . Let $i = r - j$; thus $p^r = q = p^i p^j$, with $i \in [1, \lfloor \frac{r}{2} \rfloor]$. Since $I_v(m, q)$ is invariant under the multiplication by q , the hypothesis on j contradicts H_v . That means: if H_v is true then the lemma is proved for v . So we shall prove the lemma in proving H_v , by induction on $v, v < \frac{(m(q-1)+1)}{2}$. Recall that $I_v(m, q)$ is the set of those $s \in S$ such that $\omega_q(s) < v$.

If $v = 2$, we have $1 \in I_2(m, q)$ while $p^i \notin I_2(m, q)$; indeed the q -weight of p^i equals p^i . Then H_2 is true. We suppose now that $H_{v'}$ is true for all $v' \in [2, v[$ and we want to prove H_v .

Let $i \in [1, \lfloor \frac{r}{2} \rfloor]$. Since H_{v-1} is true, we know that there is $s \in I_{v-1}(m, q)$ such that $p^i s \notin I_{v-1}(m, q)$. If $\omega_q(p^i s) > v - 1$ then $p^i s \notin I_v(m, q)$ and H_v is true. So only the case $\omega_q(p^i s) = v - 1$ remains. For $\lambda \in [0, q - 1]$, let us define:

$$[\lambda p^i] = \begin{cases} \lambda p^i \text{ modulo } q - 1 & \text{if } \lambda < q - 1, \\ q - 1 & \text{if } \lambda = q - 1 \end{cases}$$

If $\sum_{l=1}^{m-1} s_l q^l$ is the q -ary expansion of s , we have [18]

$$\omega_q(p^i s) = \sum_{l=0}^{m-1} [s_l p^i]. \tag{3.25}$$

Now we get:

$$t = s + q^k \text{ with } k \in [0, m - 1] \text{ such that } [p^i s_k] + p^i < q.$$

Note that this property implies: $[p^i(s_k + 1)] = [p^i s_k] + p^i$.

This choice of k is always possible. Indeed

$$[p^i s_k] \geq q - p^i, \forall k \rightarrow \omega_q(p^i s) \geq m(q - p^i),$$

from (3.25), but $\omega_q(p^i s) = v - 1$ and $v - 1 < \frac{m(q-1)}{2}$. Thus

$$m(q - p^i) < \frac{m(q - 1)}{2} \rightarrow 2p^i - q - 1 > 0,$$

which contradicts $i < \lfloor \frac{r}{2} \rfloor$.

Then we have:

$$\omega_q(t) = \sum_{l \neq k} s_l + (s_k + 1) = \omega_q(s) + 1 < v,$$

Thus $t \in I_v(m, q)$. Moreover;

$$\omega_q(p^i t) = \sum_{l \neq k} [p^i s_l] + ([p^i s_k] + p^i) = \omega_q(p^i s) + p^i,$$

which proves that $p^i t \notin I_v(m, q)$. Therefore H_v is true. \square

The automorphism group of the GRM-codes are known in the following cases:[18]

- for $q = 2$, $\text{Aut}(C_v(m, 2)) = GL(m, 2)$;
- if $m = 1$, $C_v(1, q)$ is an extended Reed-Solomon code and its automorphism group is $GL(1, q)$;
- if $v = 1$ or $v = m(q - 1)$, each permutation on G is an automorphism of $C_v(m, q)$.

So we suppose now that: $q > 2$, $m > 1$ and $v \in [2, m(q - 1) - 1]$. Recall that Theorem (3.16) implies that in all cases the automorphism group of $C_v(m, q)$ contains $GL(m, q)$.

Theorem 3.25. [18] Let $v \in [2, m(q - 1) - 1]$. The automorphism group of the q -ary **RM**-code of order $m(q - 1) - v$ is $GL(m, q)$ -i.e. $\text{Aut}(C_v(m, q)) = GL(m, q)$.

To prove this theorem we first need some definitions and to describe the fundamental theorem of affine geometry for finite fields. We denote by E a vector-space over a field \mathbb{F} .

Definition 3.26. An application $f : E \rightarrow E$ is semi-linear if there is an automorphism τ of the field \mathbb{F} such that:

- (1) $f(x + y) = f(x) + f(y)$, $x \in E$ and $y \in E$.
- (2) $f(\lambda x) = \tau(\lambda)f(x)$, $x \in E$ and $\lambda \in \mathbb{F}$.

Definition 3.27. An application $f' : E \rightarrow E$ is semi-affine if there is $a \in E$ and $f : E \rightarrow E$ semi-linear such that:

$$f'(x) = f(x) + a, \quad x \in E.$$

The group of semi-linear bijections is denoted by $\mathbf{GSL}_{\mathbb{F}}(\mathbf{E})$; the group of semi-affine bijections is denoted by $\mathbf{GSA}_{\mathbb{F}}(\mathbf{E})$.

Theorem 3.28. [18] Suppose that the dimension of E is strictly greater than 1 and that \mathbb{F} is not the finite field of order 2. Let $f : E \rightarrow E$ be a bijection satisfying: if a , b and c are collinear in E , then $f(a)$, $f(b)$ and $f(c)$ are collinear in E . Then f is an element of $\mathbf{GSA}_{\mathbb{F}}(\mathbf{E})$.

From now on assume that \mathbb{F} is the finite field \mathbb{F}_q , $q > 2$, and that E is the finite field \mathbb{F}_q^m , $m > 1$, considered as an F -vector-space.

Corollary 3.29. [18] let $s \in [1, m - 1]$ and $f : E \rightarrow E$ be a bijection which transforms any s -dimensional affine subspace into an s -dimensional affine subspace. Then f is an element of $\mathbf{GSA}_{\mathbb{F}}(\mathbf{E})$.

Proof. If $s = 1$, the Theorem (3.28) implies $f \in \mathbf{GSA}_{\mathbb{F}_q}(\mathbf{E})$. Suppose that $s > 1$. Each i -dimensional affine subspace L has q elements and can be considered as an intersection of some s -dimensional affine subspaces. By hypothesis $f(L)$ has q elements and is an intersection of some s -dimensional affine subspaces. Then we can apply the Theorem (3.28). □

This corollary (3.29) characterize the permutations on the field $GF(q^m)$ which preserve the affine subspaces of equal dimension. When \mathbb{F} is a finite field $GF(q)$, with $q = p^r$ (p is a prime and $r \geq 0$), the group of automorphisms of the field \mathbb{F} is

$$\Theta = \{\theta_i : \mathbb{F} \rightarrow \mathbb{F} | \theta_i(g) = g^{p^i}, \quad i \in [0, r - 1]\}.$$

Since E is a field of characteristic p , each θ_i is an automorphism of the field E ; thus for any $h : E \rightarrow E$, h being a linear bijection, the application $\theta_i \circ h$ is an element of $\mathbf{GSL}_{\mathbb{F}}(\mathbf{E})$.

Conversely let $f \in \mathbf{GSL}_{\mathbb{F}}(\mathbf{E})$ be associated with the automorphism θ_i . By definition, the application $\theta_{-i} \circ f$ is linear; hence $f = \theta_i \circ h$, h is linear and bijective. Then we can state:

$$\mathbf{GSL}_{\mathbb{F}}(\mathbf{E}) = \{\theta_i \circ h \mid \theta_i \in \Theta, \ h \text{ linear and bijective}\}, \quad (3.26)$$

and deduce

$$\mathbf{GSA}_{\mathbb{F}}(\mathbf{E}) = \{\theta_i \circ h + b \mid \theta_i \in \Theta, \ h \text{ linear bijective}, b \in E\} \quad (3.27)$$

The formula (3.27) means that the group composed of these permutations is exactly the group $\bar{G}(m, q)$.

Now we can prove theorem (3.25)

Proof. Define a permutation σ on G as a transformation on A :

$$\sigma : \sum_{g \in G} x_g X^g \mapsto \sum_{g \in G} x_g X^{\sigma(g)} = \sum_{g \in G} x_{\sigma^{-1}(g)} X^g$$

Thus a permutation $\sigma \in \text{Aut}(C_v(m, q))$. We denote by Mw_v the set of all minimum weight codewords (mwc's) of $C_v(m, q)$. So σ can be considered as a permutation on G ; so, for simplification, we shall apply σ on A or on G . It is clear that, by definition, $\sigma(Mw_v) = Mw_v$. We shall prove the theorem in describing the action of σ on the elements of Mw_v . We distinguish four cases:

Case 1: $v = b(q - 1)$, $b \in [1, m - 1]$.

From theorem (3.23), we have:

$$Mw_v = \{\lambda X^h \sum_{g \in L} X^g \mid \lambda \in \mathbb{F}_q^*, \ h \in G, \ L \text{ is a } b\text{-dim.subspace of } G\}$$

That means that σ transforms any b -dimensional affine subspace of G into another. From Corollary (3.29) and Equation (3.27), that yields $\sigma \in \bar{G}(m, q)$. Applying lemma (3.24), we obtain $\sigma \in GL(m, q)$.

Case 2: $v = b(q - 1) + a$, $b \in [0, m - 1]$, $a \in [2, q - 1]$.

Let $V = h + L$ be any $(b + 1)$ -dimensional affine subspace of G , where h is any element of G and L is any $(b + 1)$ -dimensional subspace of G . Let $\{e_1, \dots, e_{b+1}\}$ be

a basis of L ; let L' be the b -dimensional subspace of G generated by $\{e_2, \dots, e_{b+1}\}$. From Theorem (3.23) the following codewords are elements of Mw_v :

$$x = yz, \quad y = X^h \sum_{g \in L} X^g, \quad z \in C_a(\{e_1\}, q) \quad \text{and} \quad \omega(z) = a + 1, \quad (3.28)$$

where $C_a(\{e_1\}, q)$ is defined by (3.19)-by convention, if $b = 0$ then $y = X^h$ and $L' = \phi$. It is clear that the support of x is contained in V . Now the code $C_a(\{e_1\}, q)$, which is in fact an extended RS-code of minimum distance $a + 1$, satisfies the **Property 1**. Since $a > 1$, the minimum distance of $C_a(\{e_1\}, q)$ is at least 3. So we can define two distinct *mwc*'s of $C_a(\{e_1\}, q)$, say z and z' , satisfying:

$$|\text{supp}(z) \cap \text{supp}(z')| \geq 2 \quad (3.29)$$

Let y be defined by (3.28) and:

$$x = yz \quad \text{and} \quad x' = yz', \quad U = \text{supp}(x) \quad \text{and} \quad U' = \text{supp}(x').$$

By definition, an *mwc* of $C_v(m, q)$ has its support contained in only one $(b + 1)$ -dimensional affine subspace of G . Since $\sigma(x) \in Mw_v$ and $\sigma(x') \in Mw_v$, we have two $(b + 1)$ -dimensional affine subspaces of G , say W and W' , containing respectively $\text{supp}(\sigma(x))$ and $\text{supp}(\sigma(x'))$. But $\sigma(U \cap U') = \sigma(U) \cap \sigma(U')$; moreover (3.28) and (3.29) yield

$$|\sigma(U \cap U')| \geq 2q^b.$$

We then obtain:

$$2q^b \leq |\sigma(U) \cap \sigma(U')| \leq |W \cap W'| \leq q^{b+1}$$

Since $W \cap W'$ is an affine subspace of G , we can conclude that $W = W'$.

Applying the **Property 1**, we can construct a sequence,

$$x_0, \dots, x_k, \dots, x_\zeta, \quad x_k = yz_k,$$

such that

- z_k is an *mwc* of $C_a(\{e_1\}, q)$
- for each $k > 0$, z_{k-1} and z_k satisfy (3.29)
- $\bigcup_{k=0}^{\zeta} \text{supp}(x_k) = V$.

Let $U_k = \text{supp}(x_k)$ and let W_k be the $(b + 1)$ -dimensional affine subspace of G containing $\sigma(U_k)$. Applying the preceding result to x_{k-1} and x_k , for each $k > 0$, we obtain:

$$W_0 = W_1 = \dots = W_\zeta.$$

Moreover any element of V is containing in an U_k . Then $\sigma(V)$ equals W_0 . We have proved that σ transforms any $(b + 1)$ -dimensional affine subspace of G into a $(b + 1)$ -dimensional affine subspace of G . From Corollary (3.29), $\sigma \in \bar{G}(m, q)$. Therefore from Lemma (3.24), $\sigma \in GL(m, q)$.

Case 3: $v = b(q - 1) + 1$, $b \in [1, m - 1]$.

The dual of $C_v(m, q)$ is $C_\mu(m, q)$, with

$$\mu = m(q - 1) - v + 1 = (m - b)(q - 1).$$

Then, from case 1, $\text{Aut}(C_v(m, q)) = \text{Aut}(C_\mu(m, q)) = GL(m, q)$.

Case 4: $v = (m - 1)(q - 1) + a$, $a \in [2, q - 2]$.

The dual of $C_v(m, q)$ is $C_\mu(m, q)$, with

$$\mu = m(q - 1) - v + 1 = q - a \quad \text{where } q - a \in [2, q - 2].$$

Then, from Case 2., $\text{Aut}(C_v(m, q)) = \text{Aut}(C_\mu(m, q)) = GL(m, q)$. □

In the parts Case 1 and Case 2 of the proof of Theorem (3.25), we prove in fact that a permutation σ on G , which preserves Mw_v , is an element of the group $\bar{G}(m, q)$. Then we have immediately the following.

Corollary 3.30. [18] *Set $m > 1$ and $q > p$. Let $v \in [2, (m - 1)(q - 1)]$, $v \in b(q - 1) + a$ with $a = 0$ or $a \in [2, q - 1[$. Let C be an extended cyclic q -ary code such that the set of mwc's of C equals Mw_v . Then $\text{Aut}(C) \subset \bar{G}(m, q)$.*

The Automorphism Groups of BCH Codes

In this chapter we will look at extending certain cyclic codes and examine an important class of codes called affine-invariant codes in section (4.1). Reed-Muller codes and some BCH codes in section (4.3) are affine invariant.

We will present a new setting for primitive cyclic codes that will assist us in the description of affine-invariant codes.

4.1 Affine-invariant codes

A primitive cyclic code over \mathbb{F}_q is a cyclic code of length $n = q^t - 1$ for some t . To proceed, we need some notation.

Let \mathcal{I} denote the field of order q^t , which is then an extension field of \mathbb{F}_q . The set \mathcal{I} will be the index set of our extended cyclic codes of length q^t . Let \mathcal{I}^* be the nonzero elements of \mathcal{I} , and suppose α is a primitive n th root of unity in \mathcal{I} and hence a primitive element of \mathcal{I} . The set \mathcal{I}^* will be the index set of our primitive cyclic codes of length $n = q^t - 1$. With X an indeterminate, let

$$\mathbb{F}_q[\mathcal{I}] = \left\{ a = \sum_{g \in \mathcal{I}} a_g X^g \mid a_g \in \mathbb{F}_q \text{ for all } g \in \mathcal{I} \right\}.$$

The set $\mathbb{F}_q[\mathcal{I}]$ is actually an algebra under the operations

$$c \sum_{g \in \mathcal{I}} a_g X^g + d \sum_{g \in \mathcal{I}} b_g X^g = \sum_{g \in \mathcal{I}} (ca_g + db_g) X^g$$

for $c, d \in \mathbb{F}_q$, and

$$\sum_{g \in \mathcal{I}} a_g X^g \sum_{g \in \mathcal{I}} b_g X^g = \sum_{g \in \mathcal{I}} \left(\sum_{h \in \mathcal{I}} a_h b_{g-h} \right) X^g.$$

The zero and unity of $\mathbb{F}_q[\mathcal{I}]$ are $\sum_{g \in \mathcal{I}} 0X^g$ and X^0 , respectively. This is the group algebra of the additive group of \mathcal{I} over \mathbb{F}_q . Let

$$\mathbb{F}_q[\mathcal{I}^*] = \left\{ a = \sum_{g \in \mathcal{I}^*} a_g X^g \mid a_g \in \mathbb{F}_q \text{ for all } g \in \mathcal{I}^* \right\}.$$

$\mathbb{F}_q[\mathcal{I}^*]$ is a subspace of $\mathbb{F}_q[\mathcal{I}]$ but not a subalgebra. So elements of $\mathbb{F}_q[\mathcal{I}^*]$ are of the form

$$\sum_{i=0}^{n-1} a_{\alpha^i} X^{\alpha^i},$$

while elements of $\mathbb{F}_q[\mathcal{I}]$ are of the form

$$a_0 X^0 + \sum_{i=0}^{n-1} a_{\alpha^i} X^{\alpha^i}.$$

Let $\text{Sym}(\mathcal{I})$ be the symmetric group acting on \mathcal{I} . Any permutation σ in $\text{Sym}(\mathcal{I})$ acts naturally on the elements of $\mathbb{F}_q[\mathcal{I}]$,

$$\sigma \left(\sum_{g \in \mathcal{I}} x_g X^g \right) = \sum_{g \in \mathcal{I}} x_g X^{\sigma(g)}.$$

Definition 4.1. [36] The permutation group $\text{Per}(C)$ of any code C is the subgroup of $\text{Sym}(\mathcal{I})$ which leaves the code globally invariant. More precisely, in the ambient space $\mathbb{F}_q[\mathcal{I}]$, it is the subgroup of those σ satisfying

$$\sum_{g \in \mathcal{I}} x_g X^{\sigma(g)} \in C \text{ for all } x = \sum_{g \in \mathcal{I}} x_g X^g, x \in C.$$

The vector space $\mathbb{F}_q[\mathcal{I}^*]$ will be the new setting for primitive cyclic codes, and the algebra $\mathbb{F}_q[\mathcal{I}]$ will be the setting for the extended cyclic codes. So in fact both codes are contained in $\mathbb{F}_q[\mathcal{I}]$, which makes the discussion of affine-invariant codes more tractable. Suppose that C is a cyclic code over \mathbb{F}_q of length $n = q^t - 1$. The coordinates of C have been denoted $\{0, 1, \dots, n-1\}$. In R_n , the i th component c_i of a codeword $\mathbf{c} = c_0 c_1 \dots c_{n-1}$, with associated polynomial $c(x)$, is the coefficient of the

term $c_i x^i$ in $c(x)$; the component c_i is kept in position x^i . Now we associate \mathbf{c} with an element $C(X) \in \mathbb{F}_q[\mathcal{I}^*]$ as follows:

$$\mathbf{c} \leftrightarrow C(X) = \sum_{i=0}^{n-1} C_{\alpha^i} X^{\alpha^i} = \sum_{g \in \mathcal{I}^*} C_g X^g, \quad (4.1)$$

where $C_{\alpha^i} = c_i$. Thus the i th component of \mathbf{c} is the coefficient of the term $C_{\alpha^i} X^{\alpha^i}$ in $C(X)$; the component c_i is kept in the position X^{α^i} .

Example 4.2. Consider the element $c(x) = 1 + x + x^3$ in R_7 over \mathbb{F}_2 . So $n = 7 = 2^3 - 1$. Let α be a primitive element of \mathbb{F}_8 . Then $c_0 = C_{\alpha^0} = 1$, $c_1 = C_{\alpha^1} = 1$, and $c_3 = C_{\alpha^3} = 1$, with the other $c_i = C_{\alpha^i} = 0$. So

$$c(x) = 1 + x + x^3 \leftrightarrow C(X) = X + X^\alpha + X^{\alpha^3}.$$

We now need to examine the cyclic shift $xc(x)$ under the correspondence (4.1). We have

$$xc(x) = c_{n-1} + \sum_{i=1}^{n-1} c_{i-1} x^i \leftrightarrow \sum_{i=1}^{n-1} C_{\alpha^{i-1}} X^{\alpha^i} = \sum_{i=0}^{n-1} C_{\alpha^i} X^{\alpha \alpha^i}.$$

Example 4.3. We continue with Example 4.2. Namely,

$$xc(x) = x + x^2 + x^4 \leftrightarrow X^\alpha + X^{\alpha^2} + X^{\alpha^4} = X^{\alpha^1} + X^{\alpha^2} + X^{\alpha^4}.$$

Definition 4.4. [2] Let C be a cyclic code of length n over \mathbb{F}_q . The defining set T of C is the largest subset of the range $[0, n-1]$, invariant under the multiplication by $q \pmod{n}$, such that any codeword $x \in C$ satisfies

$$\rho_s(x) = x(\alpha^s) = 0 \quad \forall s \in T.$$

The set T is a union of q -cyclotomic cosets modulo n ; any $s \in T$ corresponds to a zero of C , say α^s .

Definition 4.5. A primitive cyclic code over \mathbb{F}_q of length $n = q^t - 1$ is any subset C of $\mathbb{F}_q[\mathcal{I}^*]$ such that

$$\sum_{i=0}^{n-1} C_{\alpha^i} X^{\alpha^i} = \sum_{g \in \mathcal{I}^*} C_g X^g \in C$$

if and only if

$$\sum_{i=0}^{n-1} C_{\alpha^i} X^{\alpha \alpha^i} = \sum_{g \in \mathcal{I}^*} C_g X^{\alpha g} \in C \quad (4.2)$$

Definition 4.6. Let $n = q^t - 1$. Let us denote by $\mathbf{a} = (a_g)_{g \in \mathcal{I}}$ any element of $(\mathbb{F}_q^*)^{q^t}$ where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The monomial group $M_n(\mathbb{F}_q) = (\mathbb{F}_q^*)^{q^t} \rtimes \text{Sym}(\mathcal{I})$ is the set of transformations $(\mathbf{a}; \sigma)$ which acts on \mathcal{A} as follows:

$$(\mathbf{a}; \sigma) \left(\sum_{g \in \mathcal{I}} x_g X^g \right) = \sum_{g \in \mathcal{I}} a_g x_g X^{\sigma(g)},$$

where $\mathcal{A} = \mathbb{F}_q[\mathcal{I}]$ is the ambient space, and x_g is the extended codeword of $C(X) = \sum_{g \in \mathcal{I}^*} C_g X^g$ which is defined as $x_g = \widehat{C}(X) = \sum_{g \in \mathcal{I}} C_g X^g$ such that $\sum_{g \in \mathcal{I}} C_g = 0$.

The automorphism group $\text{Aut}(C)$ of a code C is then the subgroup of $M_n(\mathbb{F}_q)$ which leaves the code globally invariant. Since \mathcal{I} is an extension field of $\mathbf{k} = \mathbb{F}_q$ with degree m' ; the field \mathcal{I} will be generally be identified with \mathbb{F}_{p^m} where $q = p^r$, $m = rm'$ from (4.2), together with the observation that $X^{\alpha^0} = X^0 = 1$, in this terminology we can define an extended cyclic code as follows

Definition 4.7. [2] An extended cyclic code is a subspace \widehat{C} of $\mathbb{F}_q[\mathcal{I}]$ such that

$$\sum_{g \in \mathcal{I}} C_g X^g \in \widehat{C} \text{ if and only if } \sum_{g \in \mathcal{I}} C_g X^{\alpha^g} \in \widehat{C} \text{ and } \sum_{g \in \mathcal{I}} C_g = 0.$$

With this new notation we want to see where the concepts of zeros and defining sets come in. This can be done with the assistance of a function ϕ_s .

Let $\widehat{\mathcal{N}} = \{s | 0 \leq s \leq n\}$. For $s \in \widehat{\mathcal{N}}$ define $\phi_s : \mathbb{F}_q[\mathcal{I}] \rightarrow \mathcal{I}$ by

$$\phi_s \left(\sum_{g \in \mathcal{I}} C_g X^g \right) = \sum_{g \in \mathcal{I}} C_g g^s,$$

where by convention $0^0 = 1$ in \mathcal{I} . Thus $\phi_0(\widehat{C}(X)) = \sum_{g \in \mathcal{I}} C_g$ implying that $\widehat{C}(X)$ is the extended codeword of $C(X)$ if and only if $\phi_0(\widehat{C}(X)) = 0$. In particular, if \widehat{C} is extended cyclic, then $\phi_0(\widehat{C}(X)) = 0$ for all $\widehat{C}(X) \in \widehat{C}$. As $0^s = 0$ in \mathcal{I} ,

$$\phi_s(\widehat{C}(X)) = \sum_{i=0}^{n-1} C_{\alpha^i} (\alpha^i)^s = \sum_{i=0}^{n-1} C_{\alpha^i} (\alpha^s)^i = \sum_{i=0}^{n-1} c_i (\alpha^s)^i = c(\alpha^s), \quad (4.3)$$

where $c(x)$ is the polynomial in $R_n = \mathbb{F}_q[x]/(X^n - 1)$ associated to $C(X)$ in $\mathbb{F}_q[\mathcal{I}^*]$. If the original code C defined on R_n had defining set T relative to the n th root of unity α . Then (4.3) shows that if $1 \leq s \leq n - 1$, $s \in T$ if and only if $\phi_s(\widehat{C}(X)) = 0$ for all $\widehat{C}(X) \in \widehat{C}$. Finally, for $\phi_n(\widehat{C}(X))$ equation (4.3) works in this case as well, implying that $\alpha^n = 1$ is a zero of C if and only if $\phi_n(\widehat{C}(X)) = 0$ for all $\widehat{C}(X) \in \widehat{C}$.

But $\alpha^0 = \alpha^n = 1$. Hence we have that $0 \in T$ if and only if $\phi_n(\widehat{C}(X)) = 0$ for all $\widehat{C}(X) \in \widehat{C}$.

We can now describe the extended cyclic code in terms of defining set as follows: a code \widehat{C} of length q^t is an extended cyclic code with defining set \widehat{T} provided $\widehat{T} \subseteq \widehat{N}$ is a union of q -cyclotomic cosets module $n = q^t - 1$ with $0 \in \widehat{T}$ and

$$\widehat{C} = \{\widehat{C}(X) \in \mathbb{F}_q[\mathcal{I}] \mid \phi_s(\widehat{C}(X)) = 0 \text{ for all } s \in \widehat{T}\}. \quad (4.4)$$

Recall that the set of coordinate permutations that map a code C to itself forms a group, that is, a set with an associative binary operation which has an identity and where all elements have inverses, called the permutation automorphism group of C . This group is denoted by $\text{Aut}(C)$. So if C is a code of length n , then $\text{PAut}(C)$ is a subgroup of the symmetric group Sym_n . Thus a permutation σ of \mathcal{I} acts on \widehat{C} as follows:

$$\left(\sum_{g \in \mathcal{I}} C_g X^g \right) \sigma = \sum_{g \in \mathcal{I}} C_g X^{g\sigma}.$$

So for any divisor e of m , we can consider $G = \mathcal{I}$ as a vector-space of dimension m/e over the subfield \mathbb{F}_{p^e} . Then we have the following subgroups of the symmetric group $\text{Sym}(G)$: [36]

- The group of the Frobenius mappings

$$\gamma_{p^k} : g \longmapsto g^{p^k}.$$

- The linear group $GL(\mathcal{I}) = GL(m/e, p^e)$, which is the group of \mathbb{F}_{p^e} -linear permutation of \mathcal{I} .
- The affine group $AGL(m/e, p^e)$, which is the group generated by the linear group $GL(m/e, p^e)$ and by the transformation of G -i.e, those mappings $g \mapsto g + b, b \in G$. In particular

$$AGL(1, p^m) = AGL_1(\mathcal{I}) = \{\sigma_{a,b} \mid a \in \mathcal{I}^*, b \in \mathcal{I}\},$$

where $\sigma_{a,b} = ag + b$. Notice that the maps $\sigma_{a,0}$ are merely the cyclic shift on the coordinates $\{\alpha^n, \alpha^1, \dots, \alpha^{n-1}\}$ each fixing the coordinate 0. The group $AGL_1(\mathcal{I})$ has order $(n+1)n = q^t(q^t - 1)$.

- The semi-linear group $\Gamma L(m/e, p^e)$, which is the group generated by the linear group $GL(m/e, p^e)$ and by the Frobenius mapping γ_p .

- The semi-affine group $AGL(m/e, p^e)$, which is the group generated by the affine group $AGL(m/e, p^e)$ and by the Frobenius mapping γ_p .

Definition 4.8. [21] An affine-invariant code is a proper subspace of \mathcal{A} invariant under the affine permutation acting on G . In other words it is a code of \mathcal{A} whose automorphism group contains $AGL(1, p^m)$.

Thus we can decide which extended cyclic codes are affine-invariant by examine there defining sets. In order to do this we introduce a partial ordering \preceq on $\widehat{\mathcal{N}}$. Suppose that $q = p^m$, where p is a prime. Then $\widehat{\mathcal{N}} = \{0, 1, \dots, n\}$, where $n = q^t - 1 = p^{mt} - 1$. So every element $s \in \widehat{\mathcal{N}}$ can be written in its p -ary expansion

$$s = \sum_{i=0}^{mt-1} s_i p^i, \quad \text{where } 0 \leq s_i < p \text{ for } 0 \leq i < mt.$$

We say that $r \preceq s$ provided $r_i \leq s_i$ for all $0 \leq i < mt$, where $r = \sum_{i=0}^{mt-1} r_i p^i$ is the p -adic expansion of r . We also need a result called Lucas' Theorem.

Theorem 4.9. [3] (Lucas') Let $r = \sum_{i=0}^{mt-1} r_i p^i$ and $s = \sum_{i=0}^{mt-1} s_i p^i$ be the p -ray expansions of r and s . Then

$$\binom{s}{z} = \prod_{i=0}^{mt-1} \binom{s_i}{r_i} \pmod{p}$$

We can now determine the affine-invariant codes from their defining sets, a result due to Kasami, Lin, and Peterson, a proof of which can be found in [21].

Theorem 4.10. [3] [Kasami, Lin, and Peterson] Let \widehat{C} be an extended cyclic code of length q^t with defining set \widehat{T} . The code \widehat{C} is affine-invariant if and only if whenever $s \in \widehat{T}$ then $r \in \widehat{T}$ for all $r \in \widehat{\mathcal{N}}$ with $r \preceq s$.

4.2 The Automorphism Groups of Affine-Invariant Codes

In this section we will state some theorems about the automorphism groups of affine-invariant codes as follows

Theorem 4.11. [21] (Berger and Charpin) Let C be a nontrivial affine-invariant code of \mathcal{A} of length p^m over \mathbb{F}_q , $q = p^r$, $m = rm'$. Then there exist a divisor e of m and a divisor ℓ of e such that the permutation group $Per(C)$ of C is generated by $AGL(m/e, p^e)$ together with the Frobenius mapping γ_{p^ℓ}

Let \widehat{N} be the defining of C . Then ℓ is the smallest integer such that \widehat{N} is invariant under multiplication by p^ℓ . Moreover r divides e and ℓ divides r . Berger proved later that the full automorphism group of any affine-invariant code is deduced from its permutation group:

Theorem 4.12. [21] *If C is a non-trivial affine-invariant code, with permutation group $Per(C)$, then*

$$Aut(C) = \mathbb{F}_q^* \rtimes Per(C).$$

More precisely, the elements of $Aut(C)$ are of the form

$$\sum_{g \in \mathcal{I}} x_g X^g \mapsto a \sum_{g \in \mathcal{I}} x_g X^{\sigma(g)}, \quad a \in \mathbb{F}_q^*, \quad \sigma \in Per(C).$$

Thus knowledge of the permutation group is sufficient for the complete description of the automorphism group of any affine-invariant code. In accordance with Theorem (4.11), this is achieved as soon as we know the values of the two parameters, ℓ and e .

Theorem 4.13. [21] *Let C be an affine-invariant code with defining set T . Let e be a divisor of m . Then the code C is invariant under $AGL(m/e, p^e)$ if and only if*

$$t \in T \text{ and } j \preceq t \Rightarrow t + j(p^e - 1) \in T.$$

4.3 BCH codes

BCH Code is most famous code in the field of coding theory because they have very effective encoding and decoding algorithms. These codes are best considered as cyclic codes. The class of Bose, Chaudhuri and Hocquenghem (BCH) codes is, in fact, a generalization of the Hamming codes for multiple-error correction (recall that Hamming codes correct only one error). Binary BCH codes were first discovered by A. Hocquenghem in 1959 and independently by R. C. Bose and D. K. Ray-Chaudhuri in 1960. Generalizations of the binary BCH codes to q -ary codes were obtained by D. Gorenstein and N. Zierler in 1961.

4.3.1 Definitions

Suppose we have t nonzero polynomials $f_1(x), \dots, f_t(x) \in \mathbb{F}_q[x]$. The least common multiple of $f_1(x), \dots, f_t(x)$ is the monic polynomial of the lowest degree which is a multiple of all of $f_1(x), \dots, f_t(x)$, denoted by $\text{lcm}(f_1(x), \dots, f_t(x))$.

Remark 4.14. If $f_1(x), \dots, f_t(x) \in \mathbb{F}_q[x]$ have the following factorizations:

$$f_1(x) = a_1 \cdot p_1(x)^{e_{1,1}} \dots p_n(x)^{e_{1,n}}, \dots, f_t(x) = a_t \cdot p_1(x)^{e_{t,1}} \dots p_n(x)^{e_{t,n}},$$

where $a_1, \dots, a_t \in \mathbb{F}_q^*$, $e_{i,j} \geq 0$ and $p_i(x)$ are distinct monic irreducible polynomials over \mathbb{F}_q , then

$$\text{lcm}(f_1(x), \dots, f_t(x)) = p_1(x)^{\max\{e_{1,1}, \dots, e_{t,1}\}} \dots p_n(x)^{\max\{e_{1,n}, \dots, e_{t,n}\}}.$$

Example 4.15. Consider the binary polynomials

$$f_1(x) = (1+x)^2(1+x+x^4)^3, \quad f_2(x) = (1+x)(1+x+x^2)^2, \quad f_3(x) = x^2(1+x+x^4).$$

Then we have by the above remark that

$$\text{lcm}(f_1(x), f_2(x), f_3(x)) = x^2(1+x)^2(1+x+x^2)^2(1+x+x^4)^3.$$

Lemma 4.16. Let $f(x), f_1(x), f_2(x), \dots, f_t(x)$ be polynomials over \mathbb{F}_q . If $f(x)$ is divisible by every polynomial $f_i(x)$ for $i = 1, 2, \dots, t$, then $f(x)$ is divisible by $\text{lcm}(f_1(x), f_2(x), \dots, f_t(x))$ as well.

Proof. see [5] □

Example 4.17. The polynomial $f(x) = x^{15} - 1 \in \mathbb{F}_2[x]$ is divisible by $f_1(x) = 1+x+x^2 \in \mathbb{F}_2[x]$, $f_2(x) = 1+x+x^4 \in \mathbb{F}_2[x]$ and $f_3(x) = (1+x+x^2)(1+x^3+x^4) \in \mathbb{F}_2[x]$ respectively. Then $f(x)$ is also divisible by

$$\text{lcm}(f_1(x), f_2(x), f_3(x)) = (1+x+x^2)(1+x+x^4)(1+x^3+x^4)$$

Example 4.18. [5] Fix a primitive element α of \mathbb{F}_{q^m} and denote by $M^i(x)$ the minimal polynomial of α^i with respect to \mathbb{F}_q . Each root β of $M^i(x)$ is an element of \mathbb{F}_{q^m} , and therefore β satisfies $\beta^{q^m-1} - 1 = 0$; i.e., $x - \beta$ is a linear divisor of $x^{q^m-1} - 1$. Since $M^i(x)$ has no multiple roots. Hence, $M^i(x)$ is a divisor of $x^{q^m-1} - 1$. For a subset I of Z_{q^m-1} , the least common multiple $\text{lcm}(M^i(x))_{i \in I}$ is a divisor of $x^{q^m-1} - 1$ as well by Lemma (4.16).

Example (4.18) provides a method to find some divisors of $x^{q^m-1} - 1$. These divisors can be chosen as generator polynomials of cyclic codes of length $q^m - 1$.

Definition 4.19. [5] Let α be a primitive element of \mathbb{F}_{q^m} and denote by $M^i(x)$ the minimal polynomial of α^i with respect to \mathbb{F}_q . A (primitive) BCH code over F_q of length $n = q^m - 1$ with designed distance δ is a q -ary cyclic code generated by

$$g(x) = \text{lcm}(M^a(x), M^{a+1}(x), \dots, M^{a+\delta-2}(x))$$

for some integer a . Furthermore, the code is called narrow-sense if $a = 1$.

Example 4.20. [5]

- (i) Let α be a primitive element of \mathbb{F}_{2^m} . Then a narrow-sense binary BCH code with designed distance 2 is a cyclic code generated by $M^{(1)}(x)$. It is in fact a Hamming code.
- (ii) Let $\alpha \in \mathbb{F}_8$ be a root of $1 + x + x^3$. Then it is a primitive element of \mathbb{F}_8 . The polynomials $M^{(1)}(x)$ and $M^{(2)}(x)$ are both equal to $1 + x + x^3$. Hence, a narrow-sense binary BCH code of length 7 generated by $\text{lcm}(M^{(1)}(x), M^{(2)}(x)) = 1 + x + x^3$ is a $[7, 4]$ code. In fact it is a binary $[7, 4, 3]$ -Hamming code.
- (iii) Let β be a root of $1 + x + x^2 \in \mathbb{F}_2$, then $\mathbb{F}_4 = \mathbb{F}_2[\beta]$. Let α be a root of $\beta + x + x^2 \in \mathbb{F}_4[x]$. Then α is a primitive element of \mathbb{F}_{16} . Consider the narrow-sense 4-ary BCH code of length 15 with designed distance 4. Then the generator polynomial is

$$g(x) = \text{lcm}(M^{(1)}(x), M^{(2)}(x), M^{(3)}(x)) = 1 + \beta x + \beta x^2 + x^3 + x^4 + \beta^2 x^5 + x^6.$$

4.3.2 Parameters Of BCH Codes

The length of a BCH code is clearly $q^m - 1$. We consider the dimension of BCH codes first.

Theorem 4.21. [3]

- (i) The dimension of a q -ary BCH code of length $q^m - 1$ generated by

$$g(x) = \text{lcm}(M^{(a)}(x), M^{(a+1)}(x), \dots, M^{(a+\delta-2)}(x))$$

is independent of the choice of the primitive element α .

- (ii) A q -ary BCH code of length $q^m - 1$ with designed distance δ has dimension at least $q^m - 1 - m(\delta - 1)$.

Proof. (i) Let C_i be the cyclotomic coset of q modulo $q^m - 1$, containing i . Put $S = \bigcup_{i=a}^{a+\delta-2} C_i$. Then we have

$$g(x) = \text{lcm}\left(\prod_{i \in C_a} (x - \alpha^i), \prod_{i \in C_{a+1}} (x - \alpha^i), \dots, \prod_{i \in C_{a+\delta-2}} (x - \alpha^i)\right) = \prod_{i \in S} (x - \alpha^i).$$

Hence, the dimension is equal to $q^m - 1 - \deg(g(x)) = q^m - 1 - |S|$. As the set S is independent of the choice of α , the desired result follows.

(ii) By part (i) the dimension k satisfies

$$\begin{aligned} k &= q^m - 1 - |S| \\ &= q^m - 1 - \left| \bigcup_{i=a}^{a+\delta-2} C_i \right| \\ &\geq q^m - 1 - \sum_{i=a}^{a+\delta-2} |C_i| \\ &\geq q^m - 1 - \sum_{i=a}^{a+\delta-2} m \\ &= q^m - 1 - m(\delta - 1). \end{aligned}$$

□

Theorem(4.21) shows that, in order to find the dimension of a q -ary BCH code of length $q^m - 1$ generated by $g(x) = \text{lcm}(M^{(a)}(x), M^{(a+1)}(x), \dots, M^{(a+\delta-2)}(x))$, it is sufficient to check the cardinality of $\bigcup_{i=a}^{a+\delta-2} C_i$, where C_i is the cyclotomic coset of q modulo $q^m - 1$ containing i .

Example 4.22. For $t \geq 1$, t and $2t$ belong to the same cyclotomic coset of 2 modulo $2^m - 1$. This is equivalent to the fact that $M^{(t)}(x) = M^{(2t)}(x)$. Therefore,

$$\text{lcm}(M^{(1)}(x), \dots, M^{(2t+1)}(x)) = \text{lcm}(M^{(1)}(x), \dots, M^{(2t)}(x));$$

i.e., the narrow-sense binary BCH codes of length $2^m - 1$ with designed distance $2t + 1$ are the same as the narrow-sense binary BCH codes of length $2^m - 1$ designed distance $2t$.

Proposition 4.23. [5] A narrow-sense q -ary BCH code of length $q^m - 1$ with designed distance δ has dimension exactly $q^m - 1 - m(\delta - 1)$ if $q \neq 2$ and $\gcd(q^m - 1, e) = 1$ for all $1 \leq e \leq \delta - 1$.

Theorem 4.24. [39] (*BCH bound*) A BCH code with designed distance δ has minimum distance at least δ

Proof. [39] □

The next theorem shows that many Hamming codes are narrow-sense BCH codes.

Theorem 4.25. [3] Let $n = \frac{q^r-1}{q-1}$ where $\gcd(r, q-1) = 1$. Let C be a narrow-sense BCH code with defining set $T = C_1$. Then C is the Hamming code $H_{q,r}$.

Corollary 4.26. [3] Every binary Hamming code is a primitive narrow-sense BCH code.

4.4 The Automorphism Groups of Primitive Narrow-Sense BCH-Codes

In this section we will give the automorphism groups of primitive narrow-sense BCH codes defined on any extension field. Recall that from now on $\mathbf{k} = \mathbb{F}_q$, $q = p^r$ and $m = rm'$, $r > 1$. The extended primitive BCH code over \mathbf{k} of length p^m and designed distance δ will be denoted by $B_q(\delta)$; it is the code with defining set

$$T_\delta = \bigcup_{j=0}^{\delta-1} cl_q(j),$$

where $cl_q(j)$, $1 \leq j \leq p^m-1$, is the orbit of j under multiplication by q , by convention we suppose that δ is the smallest element of $cl_q(\delta)$.

The primitive BCH code of length $p^m - 1$ and designed distance δ over \mathbf{k} , (whose extension is $B_q(\delta)$) will be denoted by $B_q^*(\delta)$. We will study the extension of BCH codes, because we want to work in the ambient space of GRM-codes; our ambient space is the algebra $\mathcal{A} = \mathbf{k}[(\mathbb{F}_{q^{m'}}, +)]$ So the length of any of the codes is $p^m = q^{m'}$, $m = m'r$.

In accordance with Theorem (4.11) we must determine for any code $B_q(\delta)$, a divisor e of m and a divisor ℓ of e such that its permutation group is generated by $AGL(m/e, p^e)$ together with the Frobenius mapping γ_{p^e} . We begin by proving that generally $\ell = r$. We next examine some particular cases, called 'exceptional'. Actually we will prove that e is equal to m when $B_q(\delta)$ is not exceptional. Here Let $n = p^m - 1$.

Lemma 4.27. [21] *Let $1 \leq \delta \leq n$, where δ is the smallest element of its q -cyclotomic coset. Let ℓ be the smallest integer such that T_δ is invariant under multiplication by p^ℓ . Then $\ell = r$ except when $\delta = 1$ or $p^m - 1$, and when $\delta = 3$ for $q = 4$.*

Proof. According to Theorem (4.11), ℓ must divide r . Recall that $cl_{p^u}(s)$, for some u dividing m , denotes the orbit of s under multiplication by p^u modulo n , i.e., the p^u -cyclotomic coset containing s .

First consider some particular values of δ . The cases $\delta = 1$ and $\delta = p^m - 1$ are trivial cases where obviously $\ell = 1$. Suppose that $q = 4$. We have $T_2 = \{0\} \cup cl_4(1)$ where clearly $2 \notin T_2$ implying $\ell = 2 = r$. But

$$T_3 = \{0\} \cup cl_4(1) \cup cl_4(2) = \{0\} \cup cl_2(1).$$

So if $\delta = 3$ and $q = 4$ then $\ell = 1$.

Denote by L the number of q -cyclotomic cosets modulo n . Let \mathcal{C} be the following set of coset representatives

$$\mathcal{C} = \left\{ \delta_i \mid i \in [1, L], \delta_i < \delta_{i+1}, \delta_i = \min cl_q(\delta_i) \right\} \quad (4.5)$$

Note that $T_{\delta_i} = cl_q(\delta_{i-1}) \cup T_{\delta_{i-1}}$, $\delta_1 = 1$, $\delta_L = n = p^m - 1$. We are going to prove by induction on i , $2 \leq i \leq L$, the following property:

(H_i) Assume that $3 < i$ when $q = 4$. Then for any ℓ dividing r , $\ell < r$, there is an $s \in T_{\delta_i}$ such that $p^\ell s \notin T_{\delta_i}$.

We first prove that (H_i) is true for the smallest value of i . Suppose that $q > 4$ and $i = 2$, i.e. $\delta_2 = 2$. Then $T_2 = \{0\} \cup cl_q(1)$ and clearly p^ℓ is not in T_2 since $1 \leq \ell < r$; so (H_2) is true. If $q = 4$ and $i = 4$ we have $\delta_4 = 5$ and

$$T_5 = T_3 \cup cl_4(3) = \{0\} \cup cl_2(1) \cup cl_4(3).$$

In this case, the only possible value for ℓ is 1. (H_4) is true because $6 = 2 \times 3$ is not in T_5 .

Now suppose that (H_i) is true for $i \in [3, j[$ when $q > 4$ and for $i \in [4, j[$ otherwise. We are going to prove that (H_j) is true. We have

$$T_{\delta_j} = cl_q(\delta_{j-1}) \cup T_{\delta_{j-1}}$$

and we assume that

$$\forall \ell, \ell | r, \exists s \in T_{\delta_{j-1}} \text{ such that } p^\ell s \notin T_{\delta_{j-1}}.$$

If $p^\ell s \notin cl_q(\delta_{j-1})$ then $p^\ell s \notin T_{\delta_j}$ and (H_j) is true. Assume that $p^\ell s \in cl_q(\delta_{j-1})$; so $\delta_{j-1} \equiv q^u p^\ell s \pmod{n}$, for some u . Moreover we can suppose that s is the smallest element of its q -cyclotomic coset because the condition ($s \in T_{\delta_{j-1}}$ and $p^\ell s \notin T_{\delta_{j-1}}$) is satisfied for $q^k s$, for any k .

So we have: $\delta_{j-1} \equiv q^u p^\ell s \pmod{n}$ and $s < \delta_{j-1}$. Considering the p -ary expansion of s , $s = [s_0, \dots, s_{m-1}]$, set $t = s + p^i$ where i is the smallest index such that $s_i < p - 1$. We remark that this implies $s \geq p^i - 1$. By construction we have $s < t$, implying $q^u p^\ell s < q^u p^\ell t$. Note that t is not in $cl_p(s)$. In particular, this implies $t \neq \delta_{j-1}$.

Since $B_q(\delta_{j-1})$ is affine-invariant then $q^u p^\ell t \in T_{\delta_{j-1}}$ would imply that $q^u p^\ell s$ (and any element of $cl_q(p^\ell s)$) is in $T_{\delta_{j-1}}$. So there is no element of $cl_q(p^\ell t)$ in $T_{\delta_{j-1}}$. If $t < \delta_{j-1}$ then $t \in T_{\delta_{j-1}}$ with $p^\ell t \notin T_{\delta_{j-1}}$, implying that (H_j) is true.

Suppose that $t > \delta_{j-1}$. Since

$$\delta_{j-1} - t = q^u p^\ell s - s - p^i = s(q^u p^\ell - 1) - p^i,$$

we must have: $0 < s(q^u p^\ell - 1) < p^i$. When $p > 2$ or $p = 2$ with $q^u p^\ell \neq 2$, this implies $s < p^i - 1$ which is not in accordance with the choice of i . So we must have $p = 2$, $u = 0$ and $\ell = 1$. According to the choice of i , one obtains

$$s = 2^i - 1 \quad \text{and} \quad \delta_{j-1} = 2s = 2(2^i - 1). \quad (4.6)$$

We are going to prove that (H_j) is true for $\delta_{j-1} = 2s$, with $s \in T_{\delta_{j-1}}$, with $q = 2^r$. Note that $cl_2(s)$ has cardinality m , because of the form of s . Since δ_{j-1} is the smallest element of its q -cyclotomic coset, it is clear that $i \leq m - 2$. Thus we have $s < 2s$ and $2s$ is smaller than any $t \in cl_2(s)$ unless $t = s$. Moreover $cl_2(s)$ is the union of the r classes $cl_q(2^\ell s)$, $0 \leq \ell \leq r - 1$. Each such class has cardinality m/r .

When $q = 2^r$ with $r > 2$ we deduce that $cl_q(4s)$ is not contained in T_{δ_j} ; in particular $4s \notin T_{\delta_j}$, i.e. (H_j) is true.

Suppose that $q = 4$. By hypothesis $\delta_{j-1} \geq 5$; so, according to (4.6), $i \geq 2$, $s \geq 3$ and $\delta_{j-1} \geq 6$. If $s = 3$ we have clearly that $5 \in T_{\delta_{j-1}}$ and $10 \notin T_{\delta_j}$. More generally, suppose that $s \geq 7$ and take $u = s + 2^i - 2^{i-1}$, i.e. $u = 2^{i+1} - 1 - 2^{i-1}$. The 2-ary expansions of u and $2u$ are respectively

$$[1, \dots, 1, 0, \overbrace{1}^i, 0, \dots] \quad \text{and} \quad [0, 1, \dots, 1, 0, \overbrace{1}^{i+1}, 0, \dots]$$

(recall that $i \leq m - 2$). We have $s < u < 2s$; moreover, even when $i = m - 2$, it appears that the smallest element of $cl_4(2u)$ is strictly greater than $2s$ implying

$2u \notin T_{\delta_j}$ while $u \in T_{\delta_j}$, i.e. (H_j) is true.

We have proved that (H_j) is true, for $2 \leq j \leq L$. Obviously (H_1) means that the defining set of BCH code of designed distance δ_1 , over the field of order p^r , is not invariant by multiplication by p^ℓ , ℓ dividing r and $\ell < r$, completing the proof. \square

Theorem 4.28. [21] *Suppose that the code $B_q(\delta)$ is invariant under $AGL(m'', p^e)$. Moreover we suppose that δ , q and e are such that*

$$q \neq 2, \quad p^e \leq \delta \quad \text{and} \quad \delta \neq p^m - 1$$

(where δ is the smallest element of its q -cyclotomic coset). Then the q -ary expansion of δ , say $(d_0, \dots, d_{m'-1})_q$ is

$$\delta = (\underbrace{q-1, \dots, q-1}_{\kappa}, d_\kappa, \underbrace{0, \dots, 0}_{\lambda})_q, \quad (4.7)$$

where κ denotes the biggest i such that $d_i \neq 0$ and $\lambda = m' - (\kappa + 1)$. Moreover, if $\delta \leq p^{m-e} - 1$ then $d_\kappa = 1$.

Proof. see [21] \square

Recall that the most important classes of affine-invariant codes are the primitive extended narrow-sense BCH codes and the generalized Reed-Muller (GRM) codes. Here we will state the definition of (GRM) codes.

Definition 4.29. [21] *Recall that $\mathbf{k} = \mathbb{F}_q$, $q = p^r$, $m = rm'$ and $\mathcal{A} = \mathbb{F}_q[\mathcal{I}]$.*

For any μ , $1 \leq \mu \leq m'(q-1)$, The GRM-code of length p^m over \mathbf{k} and of index μ is the code $GRM_q(\mu)$ of \mathcal{A} with defining set

$$L(\mu) = \{t \in S \mid 0 \leq wt_q(t) < \mu\}.$$

where $S = \mathbb{Z}_n$ and the integer $v = m'(q-1) - \mu$ is the order of $GRM_q(\mu)$.

We have that, for each divisor e of m , we can define the v -ary expansion and the v -weight expansion of any $s \in S$ [36] :

$$s = \sum_{i=0}^{m''} s_i v^i \quad \text{and} \quad wt_v(s) = \sum_{i=0}^{m''} s_i, \quad v_i \in [0, v-1], \quad (4.8)$$

where $v = p^e$ and $m'' = m/e$.

Lemma 4.30. [21] *For the following values of q and δ , the code $B_q(\delta)$ has a permutation group greater than $\langle \text{AGL}(1, p^m), \gamma_{p^r} \rangle$. These cases, listed below, will be called 'exceptional'.*

Some extended BCH codes are in fact GRM codes:

(E1) $\delta = 1$ or $\delta = q^{m'} - 1$, for any q . The codes $B_q(\delta)$ are the trivial GRM codes, $\text{GRM}_q(1)$ and $\text{GRM}_q(m'(q-1))$, respectively. Their permutation group is the full symmetric group $\text{Sym}(G)$, $G = \mathbb{F}_{p^m}$.

(E2) $\delta = 2$, for any q . The code $B_q(2)$ is equal to $\text{GRM}_q(2)$; thus $\text{Per}(B_q(2)) = \text{AGL}(m', q)$.

(E3) $\delta = q^{m'} - q^{m'-1} - 1$, for any q . The code $B_q(q^{m'} - q^{m'-1} - 1)$ is equal to $\text{GRM}_q(m'(q-1) - 1)$; thus $\text{Per}(B_q(\delta)) = \text{AGL}(m', q)$.

(E4) $m' = 2$, and $\delta = q^2 - 2q - 1$. The code $B_q(q^2 - 2q - 1)$ is equal to $\text{GRM}_q(2q - 4)$; thus $\text{Per}(B_q(\delta)) = \text{AGL}(2, q)$.

(E5) $q = 4$ and $\delta = 3$. The code $B_4(3)$ is equal to $\text{GRM}_2(2)$, with scalars extended to \mathbb{F}_4 , and $\text{Per}(B_4(3)) = \text{AGL}(m, 2)$.

There is one exception where $B_q(\delta)$ is not a GRM code:

(E6) $q = 2^r$, with $r > 2$ (i.e q even and $q \geq 8$), and $\delta = 3$. Then $\text{Per}(B_q(3)) = \text{AGL}(m', 2^r)$.

Proof. Recall that the defining set of $\text{GRM}_q(\mu)$, the GRM code of index μ and length $q^{m'}$ over \mathbb{F}_q is denoted by $L(\mu)$. The permutation group of $\text{GRM}_q(\mu)$ is $\text{AGL}(m', q)$ see [18], when $1 < \mu < m'(q-1)$. If $\mu = 1$ or $\mu = m'(q-1)$ then $\text{GRM}_q(\mu)$ is a trivial code whose permutation group is the symmetric group over $G = \mathbb{F}_{q^m}$ the extension field of K .

(E1) This case is obvious because the defining sets are

$$T_1 = \{0\} \quad \text{and} \quad T_{q^{m'}-1} = \{0, 1, \dots, q^{m'} - 2\}.$$

They correspond to the code containing any word for whom the sum of the coordinates is zero and the code containing the constant vector only, respectively.

(E2) It is easy to check that

$$T_2 = \{0\} \cup cl_q(1) = L_2.$$

(E3) We have that $T_{q^{m'} - q^{m'-1} - 1}$ is the set of s , $s \in [0, q^{m'} - 1]$ such that $0 \leq wt_q(s) < m'(q - 1) - 1$. This is exactly the defining set $L(m'(q - 1) - 1)$ of $GRM_q(m'(q - 1) - 1)$. These codes are the duals of those in (E2).

(E4) We remark that $\delta = (q - 1, q - 3)_q$. Let $s = (s_1, s_2)_q$. Then s is in $T_{q^2 - 2q - 1}$ if and only if

- $s_1 < q - 3$ or $s_2 < q - 3$; or
- $s_1 = q - 3$ and $s_2 < q - 1$; or
- $s_2 = q - 3$ and $s_1 < q - 1$.

This occurs if and only if $wt_q(s) < 2q - 4$. So $T_{q^2 - 2q - 1}$ is the defining set of $GRM_q(2q - 4)$.

(E5) We have seen in the proof of the previous lemma (4.27) that $T_3 = \{0\} \cup cl_2(1)$, when $q = 4$. Thus T_3 is the defining set of $GRM_2(2)$.

(E6) We have already proved that the value of ℓ is always r (cf. Lemma 4.27). We apply Theorem (4.13) when the defining set is

$$T_3 = \{0\} \cup cl_q(1) \cup cl_q(2), \quad q = 2^r, \quad r > 2.$$

We consider the pairs (s, t) , such that $s \in T_3$ and $t \preceq s$, and compute $s' = s + t(2^r - 1)$:

- If $(s, t) = (0, 0)$ then $s' = 0$.
- If $s \neq 0$ and $t = 0$ then $s' = 0$.
- If $s \neq 0$ and $t \neq 0$ the only possibility is $s = t$, implying $s' = s2^r$; hence $s' \in cl_q(\delta)$.

In any case we have $s' \in T_3$; so we have proved that the corresponding pair (s, t) cannot be a disqualifying pair for r . Hence $B_q(3)$ is invariant under $AGL(m', q)$. Now for any $e = rv$ the group $AGL(m/e, p^e)$ is contained in $AGL(m', q)$. We can conclude that the permutation group of $B_q(3)$ is $AGL(m', q)$, the permutation group

of the non-trivial GRM codes over \mathbb{F}_q . Note that T_3 is not the defining set of a GRM code, since $wt_q(1+q) = 2 = wt_q(2)$ where $2 \in T_3$ and $1+q \notin T_3$. \square

Theorem 4.31. [21] *Let $\mathbf{k} = \mathbb{F}$, $q = p^r$, p a prime, $r > 1$. Let $B_q(\delta)$ be the extended BCH-code of length p^m , r dividing m over \mathbf{k} . Then the permutation group of $B_q(\delta)$ is*

$$\langle AGL(1, p^m), \gamma_{q^r} \rangle$$

except when q , δ and m satisfy the hypothesis of one of the exceptions (E1) to (E6) listed in Lemma(4.30). When the permutation group of any $B_q(\delta)$ is generated by $AGL(m/e, p^e)$ and γ_{p^ℓ} for some ℓ and some e , then the permutation group of the corresponding BCH code $B_q^*(\delta)$ is generated by $GL(m/e, p^e)$ and γ_{p^ℓ} .

The automorphism group of $B_q(\delta)$ is $\mathbf{k}^* \times Per(B_q(\delta))$.

Proof. According to Theorem (4.11), it remains to determine the value of e , since the value of ℓ is known to be generally r (see Lemma (4.27)). So T_δ is invariant under multiplication by p^r and r is the smallest integer such that this property holds. Recall that $e = rv$, for some v .

The difficulty of the proof comes from the number of particular cases for δ . We have chosen to treat separately the *small* values of δ , the *medium* values of δ and the *big* values of δ . However the notion of 'small', or 'big' is relative and depends on the value of e . In particular $m = m'r = m''vr = m''e$; note that $p^e = q^v$. Recall that $q = p^r$ with $1 < r < m$, i.e. $4 \leq q < p^m$, since the cases $r = 1$ and $r = m$ were treated with.

From now on, we fix $e < m$, i.e. $v < m'$. This implies $e \leq m/2$ since e divides m . In order to determine if $B_q(\delta)$ is, or is not, invariant under $AGL(m/e, p^e)$, we will try to produce a disqualifying pair for e , $e = rv$ and $1 < r < m$. Generally, the defining pair will be (s, t) and $s' = s + t(p^e - 1)$.

We generally identify δ with its q -ary expansion, which is denoted by $(d_0, \dots, d_{m'-1})_q$. In the proof, κ will be the biggest suffix j such that $d_j \neq 0$; setting $\lambda = m' - 1 - \kappa$, we have:

$$\delta = (d_0, \dots, d_\kappa^{\neq 0}, \underbrace{0, \dots, 0}_\lambda)_q$$

The p^e -ary expansion of δ will be denoted, as previously, by $(\delta_0, \dots, \delta_{m''-1})_{p^e}$. Notice that $\delta_i = (d_{vi}, d_{vi+1}, \dots, d_{v(i+1)-1})_q$.

(1) **The first case** : $\delta \leq p^e - 1$. We have $\kappa < v$ implying

$$\delta_1 = \dots = \delta_{m''-1} = 0 \text{ and } \lambda \geq m' - v.$$

Suppose that $p = 2$. We consider $3 < \delta$, because the cases where $\delta \in \{1, 2, 3\}$ were already treated- see the exceptions (E1), (E2), (E5) and (E6) in Lemma (4.30). The pair $(s, t) = (3, 1)$ is disqualifying for e . Indeed we have clearly $3 \in T_\delta$ and $1 \prec 3$; moreover s' is not in T_δ . Indeed $s' = s + t(2^e - 1) = 2^e + 2$ has the following expansions:

$$s' = (2, 1, \underbrace{0, \dots, 0}_{m''-2})_{2^e} = (2, \underbrace{0, \dots, 0}_{v-1}, 1, \underbrace{0, \dots, 0}_{m'-(v+1)})_{2^r}.$$

Since $v \leq m'/2$ then $m' - (v + 1) \geq v - 1$, implying that s' is the smallest element of its q -cyclotomic coset. As $\delta \leq p^e - 1$, $\delta < s'$; so s' is not in T_δ .

When $p > 2$, $\delta = 1$ and $\delta = 2$ are exceptions. We suppose $\delta > 2$. The pair $(s, t) = (2, 1)$ is disqualifying for e , since $2 \in T_\delta$, $1 \prec 2$ and $s' = p^e + 1$ has expansions

$$s' = (1, 1, \underbrace{0, \dots, 0}_{m''-2})_{p^e} = (1, \underbrace{0, \dots, 0}_{v-1}, 1, \underbrace{0, \dots, 0}_{m'-(v+1)})_q.$$

As above, we have $s' \notin T_\delta$.

- (2) **The second case** : $p^e - 1 < \delta \leq p^{m-e} - 1$. Note that $p^{m-e} - 1 = q^{m'-v} - 1$. We have $v \leq \kappa < m' - v$ and $\delta_{m''-1} = 0$. Moreover, according to Theorem (4.28), we have to treat those δ whose q -ary expansion has the form

$$\delta = (\underbrace{q-1, \dots, q-1}_\kappa, \overbrace{1}^\kappa, \underbrace{0, \dots, 0}_{\lambda \geq v})_q,$$

i.e. $\delta = 2q^\kappa - 1$. Take $(s, t) = (\delta - 1, q^{\kappa-v})$. Then $\delta - 1 \in T_\delta$ and we have that $q^{\kappa-v} \prec \delta - 1$ when $\kappa > v$. If $\kappa = v$ then $t = 1$ and we have $t \prec s$ unless $p = 2$. We will treat later the case where $p = 2$ and $\kappa = v$. We have $s' = s + t(q^v - 1) = 2q^\kappa + (q^\kappa - q^{\kappa-v} - 2)$ whose q -ary expansion is

$$s' = (q-2, q-1, \dots, q-1, \overbrace{q-2}^{\kappa-v}, q-1, \dots, q-1, \overbrace{2}^\kappa, \underbrace{0, \dots, 0}_{\lambda \geq v})_q,$$

when $\kappa > v$. If $\kappa = v$ then $s' = 2q^v + q^v - 3$, which yields

$$s' = (q-3, q-1, \dots, q-1, \overbrace{2}^\kappa, \underbrace{0, \dots, 0}_{\lambda \geq v})_q. \quad (4.9)$$

In any case s' is the smallest element of its q -cyclotomic coset and $\delta < s'$, implying $s' \notin T_\delta$. So (s, t) is disqualifying for e . If $p = 2$ and $\kappa = v$, we choose $(s, t) = (\delta - q^v, 2)$. We have $s = q^v - 1$, $2 \prec s$ and $s' = 2q^v + (q^v - 3)$. Since s' has the q -ary expansion (4.9), we conclude that (s, t) is disqualifying for e .

- (3) **The third case** : $p^{m-e} - 1 < \delta$. We have $\kappa \geq m' - v$; thus $\delta_{m''-1} \neq 0$ and $\lambda < v$ ($\lambda = m' - 1 - \kappa$). Moreover, according to Theorem (4.28), we have to treat those δ whose q -ary expansion has the form

$$\delta = (\underbrace{q-1, \dots, q-1}_\kappa, d_\kappa, \underbrace{0, \dots, 0}_{\lambda < v})_q.$$

Recall that $m' = vm''$, $m'' > 1$; so $m' = v + 1$ if and only if $m'' = 2$ (and $v = 1$).

- (3.1) We first suppose that $m' > 2$ (then $m' > v + 1$) and consider the pair $(s, t) = (\delta - 1, q^{m'-v-1})$, where clearly $\delta - 1 \in T_\delta$. Since $\kappa > m' - (v + 1)$, we have that $t \prec s$ and

$$\begin{aligned} s' &= s + t(p^e - 1) = d_\kappa q^\kappa + q^\kappa - 2 + q^{m'-v-1}(q^v - 1) \\ &= q^{m'-1} + d_\kappa q^\kappa + (q^\kappa - q^{m'-v-1} - 2). \end{aligned}$$

Whenever $s' \notin T_\delta$, we can conclude that the pair (s, t) is a disqualifying pair for e . We distinguish three cases:

- If $\lambda \geq 2$, we have

$$s' = (q-2, \underbrace{q-1, \dots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v-1}, q-1, \dots, q-1, \underbrace{d_\kappa, 0, \dots, 0}_{\lambda-1}, 1)_q.$$

The smallest element of the q -cyclotomic coset of s' is

$$(1, q-2, \underbrace{q-1, \dots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v}, q-1, \dots, q-1, \underbrace{d_\kappa}_{\kappa+1}, \underbrace{0, \dots, 0}_{\lambda-1})_q.$$

which is greater than δ , implying $s' \notin T_\delta$.

- If $\lambda = 1$, then

$$s' = (q-2, \underbrace{q-1, \dots, q-1}_{m'-v-2}, \overbrace{q-2}^{m'-v-1}, q-1, \dots, q-1, \underbrace{d_\kappa}_\kappa, 1)_q.$$

Then, s' is the smallest element of its the q -cyclotomic coset, since $q = p^r$ with $r > 1$. Then s' is greater than δ which yields $s' \notin T_\delta$.

- If $\lambda = 0$, then

$$s' = (q - 2, \underbrace{q - 1, \dots, q - 1}_{m'-v-2}, \overbrace{q - 2}^{m'-v-1}, \underbrace{q - 1, \dots, q - 1}_{v-1}, d_\kappa + 1)_q.$$

When $d_\kappa < q - 3$, we have that $s' \notin T_\delta$, because s' is the smallest member of its q -cyclotomic coset.

If $d_\kappa = q - 3$, s' is not in T_δ because the coefficient of its q -ary expansion are $q - 1$ or $q - 2$, implying that any element of its q -cyclotomic coset is greater than δ

If $d_\kappa = q - 2$ then $\delta = q^{m'} - q^{m'-1} - 1$; we obtain the exception (E3) of Lemma (4.30).

- (3.2)** We now treat the particular case where $m' = 2$. Then $e = r$, $v = 1$ and $\delta = (q - 1) + d_1q$, i.e. $\delta = (q - 1, d_1)_q$.

We remark that $d_1 = q - 2$ corresponds to the exception (E3) ($\delta = q^2 - q - 1$) and $d_1 = q - 3$ to the exception (E4) ($\delta = q^2 - 2q - 1$). Thus we assume that $d_1 \leq q - 4$; since $d_1 \neq 0$ we then assume $q > 4$. We will distinguish when the characteristic is 2 or odd.

- If $p > 2$, we choose $(s, t) = (\delta - 1, 1)$. We have clearly $\delta - 1 \in T_\delta$ and $1 \prec \delta - 1$. Moreover

$$s' = s + t(q - 1) = d_1q + 2q - 3 \quad \text{i.e., } s' = (q - 3, d_1 + 1)_q.$$

Since $d_1 \leq q - 4$, it follows that s' is the smallest member of its q -cyclotomic coset. As $s' > \delta$, $s' \notin T_\delta$. Thus (s, t) is a disqualifying pair for r .

- Assume that $p = 2$. When $d_1 \leq q - 5$ we choose the pair $(s, t) = (\delta - 2, 1)$. We have $\delta - 2 \in T_\delta$, $1 \prec (\delta - 2)$ and

$$s' = s + t(q - 1) = d_1q + 2q - 4 \quad \text{i.e. } s' = (q - 4, d_1 + 1)_q.$$

Again, s' is the smallest member of its q -cyclotomic coset and $s' > \delta$; i.e. (s, t) is a disqualifying pair for r .

When $d_1 = q - 4$, then $\delta = q^2 - 3q - 1$, i.e. $\delta = (q - 1, q - 4)_q$. We

choose the pair $(s, t) = (q^4 - 4q - 1, 2)$. Since $s = (q - 1, q - 5)_q$, it is clear that $s \in T_\delta$ and $t \prec s$. Moreover

$$s' = s + t(q - 1) = q^2 - 2q - 3 \text{ i.e. } s' = (q - 3, q - 3)_q;$$

s' is the only element of its q -cyclotomic coset and is greater than δ ; so (s, t) is a disqualifying pair for r .

We have proved that any $B_q(\delta)$ which is not exceptional cannot be invariant under $AGL(m/e, p^e)$, for any e such that $e = rv$, $1 \leq v < m'$. We conclude that $e = m$ is the only possibility, implying that the permutation group of $B_q(\delta)$ is generated by $AGL(1, p^m)$ and γ_q . Then the permutation group of $B_q^*(\delta)$ is $\langle GL(1, p^m), \gamma_q \rangle$. The automorphism group of $B_q(\delta)$ is immediately deduced, according to Theorem (4.12). \square

Bibliography

- [1] *F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam: North-Holland, 1977.*
- [2] *V. S. Pless, W. C. Huffman, Handbook of Coding Theory, Part 1: Algebraic Coding, Cambridge University Press, Cambridge, 1998.*
- [3] *W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.*
- [4] *Jay Grossman, Coding Theory: Introduction To Linear Codes And Applications, Rivier Academic Journal, Volume 4, Number 2, Fall 2008.*
- [5] *San Ling and Chaoping Xing, Coding Theory A First Course, Cambridge University Press, Cambridge, 2004.*
- [6] *A.R.F. Everts, Automorphism groups of cyclic codes, University of Groningen, 2009.*
- [7] *R. Bienert and B. Klopsch, Automorphism groups of cyclic codes, J Algebr Comb, 31, 33-52, 2010.*
- [8] *Naser Amiri, Automorphism of Cyclic Codes, Intelligent Information Management, 4, 309-310, 2012.*
- [9] *D. Augot, E. Betti, and E. Orsini, An introduction to linear and cyclic codes, Journal of Symbolic Computation, 4, 47-68, 2009.*
- [10] *Evgeny V. Gorkunov, On permutation automorphism groups of q-ary Hamming codes, Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, 119-124, 2008.*

- [11] *S. A. Malyugin*, Perfect codes with trivial automorphism group, *Proc. Second Intern. Workshop OCRT, Sozopol, Bulgaria, 163-167, 1998.*
- [12] *T. Shah, M. Khan and A. A. Andrade*, A BCH Code and a Sequence of Cyclic Codes, *International Journal of Algebra, Vol. 8, 547-556, 2014.*
- [13] *D. R. Shier and K. T. Wallenius*, Applied Mathematical Modeling: A Multi-disciplinary Approach, *Chapman and Hall-CRC Press, Boca Raton, 1999.*
- [14] *J.C.Moreira and P.G.Farrell*, Essential of Error-Control Coding, *John Wiley and Sons Ltd, England, 2006.*
- [15] *T.Martini and T.Erseghe*, Reed-Solomon Codes, *Department of Information Engineering, University of Padova, 2013.*
- [16] *Janne I. Kokkala and Patric R. J. Ostergard*, Further Results on the Classification of MDS Codes, *Aalto University School of Electrical Engineering, Finland, 2015.*
- [17] *E. F. Assmus, Jr and J. D. Key*, Polynomial Codes and Finite Geometries.
- [18] *T. Berger and P. Charpin*.The automorphism group of Generalized Reed-Muller codes. *Discrete Math., 117, 1-17, 1993.*
- [19] *Sarah S. Adams*, Introduction to Algebraic Coding Theory, *Franklin W. Olin College of Engineering, 2008.*
- [20] *Robert H. Morelos-Zaragoza and Shu Lin*, On Primitive BCH Codes with Unequal Error Protection Capabilities, *IEEE Transactions on Information Theory, Vol. 41, NO. 3, MAY 1995.*
- [21] *T. P. Berger and P. Carpin*, The Automorphism Groups of BCH Codes and of Some Affine-Invariant Codes Over Extension Fields, *Designs, Codes and Cryptography, 18, 29-53, 1999.*
- [22] *Massey, J. Costello and D. Justesen*, Polynomial weights and code constructions, *IEEE Transactions on Information Theory, 19(1), 101-110, 1973.*
- [23] *I. A. Joundan, S. Nouh, A. Namir*, A New Powerful Scheme Based on Self Invertible Stabilizer Multiplier Permutation to Find the Minimum Distance

- for large BCH Codes, *American Journal of Computer Science and Technology*, 1(2), 39-43, 2018.
- [24] Vijay K. Bhargava, Qing Yang and David J. Peterson, Coding Theory and its Applications in Communication Systems, *Defence Science Journal*, Vol 43, No 1, pp 59-69, January 1993.
- [25] Ron M. Roth, Introduction To Coding Theory, *Cambridge. Univ. Press.*, 2006.
- [26] Bill Lyle, A Linear-Algebra Problem From Algebraic Coding Theory, *LINEAR ALGEBRA AND ITS APPLICATIONS*, 22, 223-233, 1978.
- [27] P. J. Cameon, Finite Permutation Groups And Finite Simple Groups, *Bull. London Math. SOC*, 13, 1-22, 1981.
- [28] M.R. Darafsheh, Order of elements in the groups related to the general linear group, *Finite Fields and Their Applications* 11, 738-747, 2004.
- [29] K. Conrad, Transitive Group Action, *University of Connecticut, Department of Mathematics*.
- [30] Harinaivo Andriatahiny. The Generalized Reed-Muller codes and the radical powers of a modular algebra, *arXiv, Article ID 1601.07633v1*, 14 Pages, 2016.
- [31] P. Delsarte, J. M. Goethal and F. J. Mac Williams, On Generalized Reed-Muller Codes and Their Relatives, *Information And Control* 16, 403-442, 1970.
- [32] E. Weiss, Generalized Reed-Muller Codes, *Information And Control* 5, 213-222, 1962.
- [33] Iliya G. Bouyukliev, About the code equivalence, *Bulgarian National Science Fund under Contract No MM 1304*, 126-151, 2003.
- [34] Franz Lemmermeyer, Error-correcting Codes, *Bilkent University, Faculty of Science*, 2005.
- [35] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, *Cambridge University Press*, 1986.

-
- [36] *T. P. Berger and P. Charpin*, The permutation group of affine-invariant extended cyclic codes, *IEEE Transactions on Information Theory*, Vol. 42. pp. 2194-2209, 1996.
- [37] *A. Haily, D. Harzalla*, On the Automorphism Group of Distinct Weight Codes, *Intelligent Information Management*, 7, 80-92, 2015.
- [38] *M. Borello*, On the automorphism groups of binary linear codes, *Mathematics Subject Classification, IEEE, Italy*, 2010.
- [39] *D.W.C. Kuijsters* Coding Theory: Algebraic coding theory, *Master's Thesis, Riethoven, the Netherlands*, 2017.
- [40] *Yann Laigle-Chapuy*, Permutation polynomials and applications to coding theory, *Finite Fields and Their Applications* 13, 58-70, 2007.
- [41] *Derek J. S. Robinson*, An Introduction to Abstract Algebra, *Walter de Gruyter GmbH and Co. KG, 10785 Berlin, Germany*, 2003.
- [42] *J.I.Hall*, Notes on Coding Theory, *Department of Mathematics. Michigan State University*, 2003.
- [43] *D. Harzalla*, Binary Linear Codes and Binary Matrices, *General Letters in Mathematics Vol. 2, No. 2, pp.67-72, April 2017*.
- [44] *Peter J. Cameron*, Matrix groups, *Discrete Mathematics and its Applications* 39, *Chapman and Hall/CRC*, 2006.