A SURVEY ON QUATERNARY CODES AND THEIR BINARY IMAGES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

DERYA ÖZKAYA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

AUGUST 2009

Approval of the Thesis:

A SURVEY ON QUATERNARY CODES AND THEIR BINARY IMAGES

submitted by **DERYA ÖZKAYA** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Ersan AKYILDIZ _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh ÖZBUDAK _____
Head of Department, **Cryptography**

Assoc. Prof. Dr. Melek DİKER YÜCEL _____
Supervisor, **Electrical and Electronics Engineering Dept., METU**

Examining Committee Members

Prof. Dr. Ferruh ÖZBUDAK _____
Department of Mathematics, METU

Assoc. Prof. Dr. Melek DİKER YÜCEL _____
Electrical and Electronics Engineering Dept., METU

Prof. Dr. Yalçın TANIK _____
Electrical and Electronics Engineering Dept., METU

Assoc. Prof. Dr. A. Özgür YILMAZ _____
Electrical and Electronics Engineering Dept., METU

Güzin KURNAZ, Ph.D. _____
TÜBİTAK-SAGE

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Derya ÖZKAYA

Signature :

ABSTRACT

A SURVEY ON QUATERNARY CODES AND THEIR BINARY IMAGES

Özkaya, Derya

M.S., Department of Cryptography

Supervisor: Assoc. Prof. Dr. Melek Diker Yücel

August 2009, 97 pages

Certain nonlinear binary codes having at least twice as many codewords as any known linear binary code can be regarded as the binary images of linear codes over $\mathbb{Z}_4$. This vision leads to a new concept in coding theory, called the $\mathbb{Z}_4$-*linearity* of binary codes. This thesis is a survey on the linear quaternary codes and their binary images under the Gray map. The conditions for the binary image of a linear quaternary code to be linear are thoroughly investigated and the $\mathbb{Z}_4$-linearity of the Reed-Muller and Hamming codes is discussed. The contribution of this study is a simplification on the testing method of linearity conditions via a few new lemmas and propositions. Moreover, binary images (of length 8) of all linear quaternary codes of length 4 are analyzed and it is shown that all 184 binary codes in the nonlinear subset of these images are worse than the (8, 4) Hamming code.

This thesis also includes the Hensel lift and Galois ring which are important tools for the study of quaternary cyclic codes. Accordingly, the quaternary cyclic versions of the well-known nonlinear binary codes such as the Kerdock and Preparata codes and their $\mathbb{Z}_4$-linearity are studied in detail.

Keywords: quaternary code, binary image, Gray map, $\mathbb{Z}_4$-linearity.

ÖZ

DÖRTLÜ KODLAR VE İKİLİ GÖRÜNTÜLERİ ÜZERİNE BİR ARAŞTIRMA

Özkaya, Derya
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi: Doçent Dr. Melek Diker Yücel

Ağustos 2009, 97 sayfa

Bilinen doğrusal ikili kodların en az iki katı kod sözcüğüne sahip bazı doğrusal olmayan ikili kodlar, $\mathbb{Z}_4$ üzerindeki doğrusal kodların ikili görüntüleri olarak görülebilir. Bu bakış, kodlama teorisinde ikili kodların $\mathbb{Z}_4$*-doğrusallığı* diye adlandırılan yeni bir kavrama yol açmıştır. Bu tez, dörtlü kodlar ve onlardan Gray eşlemesiyle elde edilen ikili görüntüleri üzerine bir araştırmadır. İkili görüntülerin doğrusal olması için gereken şartlar ayrıntılı olarak incelenmiş; ayrıca Reed-Muller ve Hamming kodlarının $\mathbb{Z}_4$-doğrusallığı ele alınmıştır. Bu çalışmanın katkısı, doğrusallık koşullarını sınama yönteminin birkaç yeni ön sav ve önermeyle basitleştirilmesidir. Ayrıca, 4 uzunluğundaki bütün doğrusal dörtlü kodların (8 uzunluğundaki) ikili görüntüleri incelenmiş ve bu görüntülerin doğrusal olmayan altkümesindeki toplam 184 kodun, (8, 4) Hamming koddan daha kötü olduğu gösterilmiştir.

Bu tez dörtlü çevrimsel kodların çalışılması için önemli araçlar olan Hensel lift ve Galois halkasını da içermektedir. Bu araçların yardımıyla, tanınmış doğrusal olmayan ikili kodlardan Kerdock, Preparata ve bunların $\mathbb{Z}_4$-doğrusallığı, ayrıntılı olarak çalışılmıştır.

Anahtar Kelimeler: dörtlü kod, ikili görüntü, Gray eşlemesi, $\mathbb{Z}_4$-doğrusallık.

To My Love Hasan Özkaya

and

My Mother Huriye Uysal

ACKNOWLEDGMENTS

I express my sincerest thanks to my supervisor, Assoc. Prof. Dr. Melek Diker Yücel, for her guidance, support, encouragement and valuable contributions during my graduate studies.

I would like to express my deepest gratitude and respect to my love Hasan Özkaya. To feel his endless love, encouragements and patience has always made me stand strong and upright. I also would like to thank my deceased mother Huriye Uysal, my father Salim Uysal, my father-in-law Ömer Ali Özkaya and my mother-in-law Ziynet Özkaya for their love, encouragement and support during not only the thesis but also my whole life.

I am grateful to my brother Kadir Uysal, my sister Şefika Konca and my dear friend Erdal Özkınacı for their encouragement and support.

I wish to thank to METU Department of Cryptography faculty and staff for their help throughout my graduate studies.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

The history of error control coding began in 1948 with the publication of a famous paper by Claude Shannon [45]. The first block codes were introduced by Hamming [24] in 1950. Block codes for error control is a set of *n*-tuples, called *codewords*, in some finite alphabet, usually the finite field $GF(q)$. In applications, the most popular block codes are binary, which are subsets of the vector space over $GF(2)$, especially the linear ones. Linear codes are defined as subspaces of a vector space; hence, the sum of the two codewords is a codeword and any scalar multiple of a codeword is also a codeword. So that the large number of errors can be corrected, it is desirable that codewords be very dissimilar from each other. This dissimilarity is measured by the Hamming distance. The *minimal Hamming distance* of the code, which is defined as the minimum of the distances between any two different codewords, is a measure of the efficiency of the code. Another measure is the *code rate* that is equal to the number of information symbols in the codeword divided by the codeword symbol length. One of the fundamental problems in coding theory is to construct and study codes with large rate subject to the constraint that the minimal distance of the code is some given integer.

Historically, linear codes have been the most important codes since they have a clean structure that makes them simpler to discover, to understand, to encode and decode. However, in order to get the largest possible number of codewords with a fixed block size and correction capability, it is sometimes necessary to consider more general codes, without this special linear structure. Around 1970, several nonlinear binary

codes having at least twice as many codewords as any known linear code with the same length and minimal distance have been constructed. Some of the best known are the Nordstrom-Robinson codes [41] found in 1967, the Preparata codes [43] in 1968, the Kerdock codes [32] in 1972, the Goethals codes [21], [22] in 1974, the Delsarte-Goethals codes [19] in 1975 and the Goethals-Delsarte codes [27] in 1990. Although these nonlinear binary codes are not so easy to describe, to encode and decode as the linear codes, they have great error correcting capabilities as well as remarkable structure. For instance, the Kerdock and Preparata codes are *formal duals* as named by Calderbank, Hammons, Kumar, Sloane and Solé in 1993 in [25]. Actually, *algebraic duality* is defined only for linear codes, whenever they span orthogonal subspaces. Kerdock and Preparata code sets are not orthogonal; however, the weight distribution of one is the MacWilliams transform of the weight distribution of the other, which is a property known to hold for dual linear codes as well [39]. It is also shown that these nonlinear binary codes (except for the Nordstrom-Robinson code) are not unique and large numbers of codes exist with the same weight distribution [1], [13], [29], [30], [31], [50].

In 1989, Solé discovered a family of nearly optimal four-phase sequences of period $2^{2r+1}-1$, with alphabet $\{1,\ i,\ -1,\ -i\}$, $i=\sqrt{-1}$ [48]. This family may be viewed as a linear code over the ring $\mathbb{Z}_4$ after replacing each element i^a by its exponent $a \in \{0,\ 1,\ 2,\ 3\}$. These sequences have low correlation values and possess a large minimal Euclidean distance. Thus, the family has potential for excellent error correcting capability [26].

After this discovery, the study of linear codes over finite rings has gained prominence and several researchers have shown that the well-known nonlinear binary codes are actually equivalent to linear codes over the ring of integers modulo 4, so they were called $\mathbb{Z}_4$*-linear*. In 1989, Nechaev showed that in fact Kerdock codes can be viewed as cyclic codes over $\mathbb{Z}_4$ [40]. Hammons, Kumar, Calderbank,

Sloane and Solé [26] noticed the striking resemblance between the 2-adic expansions of the quaternary codewords and the standard construction of the Kerdock codes. Although the Preparata code is not a $\mathbb{Z}_4$-linear code, a binary code with the same parameters that is called *Preparata-like* is $\mathbb{Z}_4$-linear. Furthermore, Calderbank, Hammons, Kumar, Sloane and Solé explained the fascinating relationship between the weight distributions of Kerdock and Preparata-like codes when they showed in 1993 that these well-known codes are the Gray mapped binary images of the linear quaternary codes that are dual to one another [8], [25], [26]. $\mathbb{Z}_4$-dual of any Preparata-like code is called a Kerdock-like code. The Gray map translates a quaternary code with high minimal Lee or Euclidean distance into a binary code of twice the length with high minimal Hamming distance.

The Kerdock and Preparata codes exist for all lengths $n = 4^k \geq 16$. At length 16, they coincide, giving the Nordstrom-Robinson code, which is the unique binary code of length 16, consisting 256 codewords and minimum distance 6 [41], [47], [23]. Moreover, it is equivalent to a self-dual quaternary code of length 8, called the '*octacode*' [14], [15], [20]. It is discovered that the Goethals codes of minimal distance 8 and the high minimal distance codes of Delsarte and Goethals have simple descriptions as extended cyclic codes over $\mathbb{Z}_4$ [26]. The existence of quaternary versions of Reed-Muller and Hamming codes is also shown [26]. These discoveries lead to a new direction in coding theory, the study of $\mathbb{Z}_4$-cyclic codes that uses the important tools of Galois rings and the Hensel Lift.

1.2 SCOPE OF THE THESIS

This thesis work is a survey on the quaternary codes; using mainly the seminal paper written by Hammons, Kumar, Calderbank, Sloane and Solé [26] and the book by

Wan [52], which is an extended form of lecture notes basically depending on [26]. Our modest contributions appear in Section 3.4, in the second part of Section 3.5 and in some of the examples.

The thesis is arranged as follows. The second chapter gives the basic properties of quaternary codes. The structure of the generator matrices of the linear quaternary codes and their dual codes is discussed. Several kinds of weights and weight enumerators of the quaternary and binary codes are summarized. The relationship between the weight enumerators of the codes and their duals by using the strongest tool, MacWilliams equations, is discussed. Finally, basic definitions of distance enumerators of binary codes that will be used in the following chapters are given.

In the third chapter, the Gray map, and the relations between quaternary codes and their binary images are recalled. The properties of the binary images of the linear quaternary codes and their duals under the Gray map are explained. Moreover, the conditions for the binary image of a linear quaternary code to be linear and for a binary code to be $\mathbb{Z}_4$-linear are given. The construction of linear quaternary codes by using linear binary codes is discussed following the related literature. In Section 3.4, we present some conditions that we derive to simplify the linearity check for the binary image of a linear quaternary code. Finally, in Section 3.5, after discussing the $\mathbb{Z}_4$-linearity of the Reed-Muller and Hamming codes, we analyze all linear quaternary codes of length 4 to answer the question whether or not there is a nonlinear but $\mathbb{Z}_4$-linear code better than the extended Hamming code of length 8.

In the fourth chapter, we study the cyclic codes over $\mathbb{Z}_4$ by means of Galois rings $GR(4^m)$. The basic facts about the polynomials of the polynomial ring $\mathbb{Z}_4[X]$, and then the properties of the Galois ring and the automorphisms, the generalized Frobenius and trace maps of $GR(4^m)$ are given. Finally, the quaternary cyclic codes are defined and the properties of their generator matrices are stated.

In the fifth chapter, we study the well-known nonlinear binary codes. It is firstly shown that Kerdock codes are extended cyclic codes over $\mathbb{Z}_4$ and are simply $\mathbb{Z}_4$-analogues of the first-order Reed-Muller codes. In the second section, it is shown that the binary images of the quaternary duals of the Kerdock codes are the binary images of the quaternary Preparata codes, which are called the Preparata-like codes. The third section defines a family of quaternary Reed-Muller codes, which generalizes the quaternary Kerdock and Preparata-like codes. In the final section, another generalization of Preparata-like codes, the quaternary Goethals codes are explained. Moreover, it is shown that the nonlinear binary Delsarte-Goethals codes are also extended cyclic codes over $\mathbb{Z}_4$, and that their $\mathbb{Z}_4$-duals have essentially the same properties as the Goethals codes and the "Goethals-Delsarte" codes.

The final chapter summarizes the thesis.

CHAPTER 2

QUATERNARY CODES AND WEIGHT ENUMERATORS

An error correcting code is called a block code if the coded information can be divided into blocks of *n* symbols. A binary error correcting code of length *n* is just a subset of the vector space $\mathbb{F}_2^n$, the most standard ones being linear codes which are subspaces of $\mathbb{F}_2^n$. They are easier to construct, encode and decode than nonlinear codes. However, there are well-known families of nonlinear codes with high error correcting capability that are equivalent to linear codes over $\mathbb{Z}_4$, the ring of integers modulo 4.

In this chapter, we discuss codes over $\mathbb{Z}_4$, the so-called *quaternary codes*. Linear codes over $\mathbb{Z}_4$, the structure of their generator matrices, their weight enumerators and their dual codes are studied. Furthermore, the weight and distance enumerators for binary codes are defined for use in later chapters. Examples without any given reference are those that we generate.

2.1 QUATERNARY CODES

Let $\mathbb{Z}_4^n$ be the set of *n*-tuples over $\mathbb{Z}_4$, the ring of integers modulo 4, i.e.,

$$\mathbb{Z}_4^n = \{(x_1,...,x_n) \mid x_i \in \mathbb{Z}_4 \text{ for } i = 1,...,n\}.$$

For all $\mathrm{x} = (x_1,...,x_n)$ and $\mathrm{y} = (y_1,...,y_n) \in \mathbb{Z}_4^n$, component-wise addition is defined by

$$\mathrm{x} + \mathrm{y} = (x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n).$$

Then $\mathbb{Z}_4^n$ is an additive abelian group of order 4^n with respect to component-wise addition.

Definition 2.1.1. [48] Any nonempty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is called a *quaternary code* or a code over $\mathbb{Z}_4$, and *n* is called the *length* of the code $\mathcal{C}$. Each element of the set is a *codeword*.

Definition 2.1.2. [48] If $\mathcal{C}$ is an additive subgroup of $\mathbb{Z}_4^n$ then it is called a *linear quaternary code*, or a linear code over $\mathbb{Z}_4$.

The standard inner product of any two words $\mathrm{x} = (x_1, ..., x_n)$ and $\mathrm{y} = (y_1, ..., y_n)$ in $\mathbb{Z}_4^n$ is defined by

$$\mathrm{x} \bullet \mathrm{y} = x_1 y_1 + ... + x_n y_n.$$

If $\mathrm{x} \bullet \mathrm{y} = 0$, then x and y are said to be orthogonal.

Definition 2.1.3. [48] Let $\mathcal{C}$ be a linear quaternary code of length *n*, its dual $\mathcal{C}^{\perp}$ is the set of words over $\mathbb{Z}_4^n$ that are orthogonal to all codewords of $\mathcal{C}$, i.e.,

$$\mathcal{C}^{\perp} = \{\mathrm{x} \in \mathbb{Z}_4^n \mid \mathrm{x} \bullet \mathrm{y} = 0 \text{ for all } \mathrm{y} \in \mathcal{C}\}.$$

Since $\mathcal{C}^{\perp}$ is a subgroup of $\mathbb{Z}_4^n$, it is also a linear quaternary code, called the *dual code* of $\mathcal{C}$. $\mathcal{C}$ is called a *self-orthogonal code* if $\mathcal{C} \subset \mathcal{C}^{\perp}$, and it is called a *self-dual code* if $\mathcal{C} = \mathcal{C}^{\perp}$.

Two quaternary codes both of length n are said to be *equivalent*, if one can be obtained from the other by permuting the coordinates and changing the signs of certain coordinates. If only coordinate permutations are used, then the codes are called *permutation-equivalent*.

Let $\mathcal{C}$ be a linear quaternary code of length n. A $k \times n$ matrix G over $\mathbb{Z}_4$ is called a *generator matrix* of $\mathcal{C}$ if the rows of G generate $\mathcal{C}$ and no proper subset of the rows of G generates $\mathcal{C}$.

Proposition 2.1.4. [26] Any linear quaternary code $\mathcal{C}$ containing some nonzero codewords is permutation-equivalent to the linear quaternary code with generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}, \tag{2.1}$$

where I_{k_1} and I_{k_2} denote the $k_1 \times k_1$ and $k_2 \times k_2$ identity matrices, respectively, A and D are $\mathbb{Z}_2$-matrices, and B is a $\mathbb{Z}_4$-matrix. Then $\mathcal{C}$ is an abelian group of type $4^{k_1}2^{k_2}$, containing $2^{2k_1+k_2}$ codewords and $\mathcal{C}$ is a free $\mathbb{Z}_4$-modulo if and only if $k_2 = 0$.

Proposition 2.1.4 can be proved by using induction on length n.

The type of a linear quaternary code can be found when vectors in the generator matrix have some specific properties as given in the following lemma. The proof can be found in [17].

Lemma 2.1.5. [17] Let $v_1, ..., v_{k_1}, u_1, ..., u_{k_2}$ be $k_1 + k_2$ linearly independent binary vectors. Then, the linear quaternary code generated by the matrix (2.1) with row vectors $v_1, ..., v_{k_1}, 2u_1, ..., 2u_{k_2}$ is of type $4^{k_1}2^{k_2}$.

Let $m_1, ..., m_{k_1} \in \mathbb{Z}_4$ and $m_{k_1+1}, ..., m_{k_1+k_2} \in \mathbb{Z}_2$, encoding is carried out by writing the information symbols in the form $m = m_1 ... m_{k_1} m_{k_1+1} ... m_{k_1+k_2}$, and matrix multiplication mG.

The following proposition provides the generator matrix of the dual code of a linear quaternary code, where A^{tr} denotes the transpose of the matrix *A*.

Proposition 2.1.6. [26] The dual code $\mathcal{C}^{\perp}$ of the linear quaternary code $\mathcal{C}$ of length *n* with generator matrix (2.1) has the generator matrix

$$G = \begin{pmatrix} -B^{tr} - D^{tr}A^{tr} & D^{tr} & I_{n-k_1-k_2} \\ 2A^{tr} & 2I_{k_2} & 0 \end{pmatrix}. \tag{2.2}$$

$\mathcal{C}^{\perp}$ is an abelian group of type $4^{n-k_1-k_2}2^{k_2}$ and contains $2^{2n-2k_1-k_2}$ codewords.

The matrix (2.2) is called a *parity check matrix* of the linear quaternary code $\mathcal{C}$ generated by the rows of the matrix (2.1). A word $c = (c_1, ..., c_n)$ belongs to $\mathcal{C}$ if and only if c is orthogonal to every row of (2.2).

Example 2.1.7. [52] Let $\mathcal{K}_4$ denote the linear quaternary code with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}. \tag{2.3}$$

By Proposition 2.1.4, $\mathcal{K}_4$ is of type $4^1 2^2$ where $k_1 = 1$ and $k_2 = 2$, and hence $|\mathcal{K}_4| = 16$. By Proposition 2.1.6, $\mathcal{K}_4^{\perp}$ is also of type $4^1 2^2$ and since any two rows of (2.3), distinct or not, are orthogonal, $\mathcal{K}_4 = \mathcal{K}_4^{\perp}$, i.e., $\mathcal{K}_4$ is a self-dual code.

Example 2.1.8. The linear quaternary code $\mathcal{G}_1$ with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 \end{pmatrix} \tag{2.4}$$

is of type 4^3, where $k_1 = 3$ and $k_2 = 0$, and hence $|\mathcal{G}_1| = 2^{2k_1} = 64$. By Proposition 2.1.6, $\mathcal{G}_1^{\perp}$ is of type 4^2 and hence $|\mathcal{G}_1^{\perp}| = 16$. $\mathcal{G}_1^{\perp}$ has generator matrices

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 0 \\ 3 & 3 & 2 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 3 & 2 \end{pmatrix} \tag{2.5}$$

Example 2.1.9. [52] The linear quaternary code $\mathcal{O}_8$ with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix} \tag{2.6}$$

is of type 4^4 where $k_1 = 4$ and $k_2 = 0$, and hence $|\mathcal{O}_8| = 256$. By Proposition 2.1.6, $\mathcal{O}_8^{\perp}$ is also of type 4^4 and since any two rows of the generator matrix are orthogonal, $\mathcal{O}_8 = \mathcal{O}_8^{\perp}$, i.e., $\mathcal{O}_8$ is self-dual. This special code $\mathcal{O}_8$ having the generator matrix (2.6) is called *octacode.*

2.2 WEIGHT ENUMERATORS

The minimum distance of a linear code tells us how many errors a received word may contain and still be decoded correctly. Often, it is necessary to have more detailed information about the distances in the code. For an arbitrary code, one wants to know the number codewords at any given distance i from the chosen codeword. For linear codes this number is independent of the codeword chosen, and hence depends only on how many codewords there are of each given weight i. This information is provided by the weight enumerator.

In this section, we study the weight and distance properties of binary and quaternary codes, and then discuss the relationship between the weight enumerators of dual codes. Most definitions and properties described here can be found in [26], [33], [39] and [52].

Let C be a binary code of length n over $\mathbb{F}_2$, which is not necessarily linear. The *Hamming weight* of $\mathrm{c} = (c_1, c_2, ..., c_n) \in C$ is the number of nonzero components of c, i.e.,

$$w_H(\mathrm{c}) = |\{ j \mid c_j \neq 0 \}|.$$

This weight function defines also a distance function, which is called the *Hamming distance.* The Hamming distance between two vectors of the same length

$\mathrm{c} = (c_1,\ c_2, ..., c_n)$ and $\mathrm{c}' = (c_1',\ c_2', ..., c_n') \in C$ is defined as the number of components at which the two vectors are different, i.e.,

$$d_H(\mathrm{c},\ \mathrm{c}') = |\{ j \mid 1 \le j \le n,\ c_j \ne c_j' \}|.$$

Let A_i be the number of codewords of Hamming weight i in C, i.e.,

$$A_i = |\{ \mathrm{c} \in C \mid w_H(\mathrm{c}) = i \}|,\ i = 0,\ 1, ..., n.$$

It is easily verified that $A_0 = 1$ when $\mathbf{0} \in C$, and $\sum_{i=0}^{n} A_i = |C|$. The set $\{A_0,\ A_1, ..., A_n\}$ is called the *weight distribution* of code C.

Definition 2.2.1. [39] The *weight enumerator* of the binary code C is defined by

$$W_C(X,\ Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i. \tag{2.7}$$

Weight enumerators are not at all easy to determine. However, the weight enumerator of a given code determines the weight enumerator of its dual in a quite simple manner. Let C be a linear binary code of length n, and $C^{\perp}$ be its dual code, then their weight enumerators $W_C(X,\ Y)$ and $W_{C^{\perp}}(X,\ Y)$ are connected by the *MacWilliams identity*

$$W_{C^{\perp}}(X,\ Y) = \frac{1}{|C|} W_C(X + Y,\ X - Y).$$

For studying the MacWilliams identity, the Krawtchouk polynomial is a good tool which is described in the following definition.

Definition 2.2.2. [49] Let n be a fixed positive integer, q a prime power, and x an indeterminate. The polynomials

$$K_k(x) = K_k(x,\ n) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j}\binom{n-x}{k-j}, \quad k = 0,\ 1,\ 2,..., \tag{2.8}$$

are called the *Krawtchouk polynomials*, where

$$\binom{x}{j} = \begin{cases} \dfrac{x(x-1)\cdots(x-j+1)}{j!}, & \text{if } j \text{ is a positive integer,} \\ 1, & \text{if } j = 0, \\ 0, & \text{otherwise.} \end{cases}$$

The Krawtchouk polynomial gives a relation between weight distributions of two codes that satisfy the MacWilliams identity.

Proposition 2.2.3. [49] Let C and C' be two codes of length n over $\mathbb{Z}_q$ where $q \geq 2$, and A_i and A_i' be the number of codewords of weight i in C and C', respectively. If

$$W_{C'}(X,\ Y) = \frac{1}{|C|} W_C(X+Y,\ X-Y), \tag{2.9}$$

then

$$A_k' = \frac{1}{|C|} \sum_{i=0}^{n} A_i K_k(i), \quad k = 0,\ 1,..., n, \tag{2.10}$$

and conversely.

By Proposition 2.2.3, weight distribution of any two codes which satisfy MacWilliams identity are also related by (2.10) even if they are not dual to each other or not linear.

Thus by Proposition 2.2.3 the weight distribution $\{A_0, A_1, ..., A_n\}$ of a binary code C and the weight distribution $\{A'_0, A'_1, ..., A'_n\}$ of $C^{\perp}$ are connected by (2.10).

Now we study the weight enumerators of quaternary codes. Several weight enumerators are associated with quaternary codes; as will be seen in the following four definitions.

Definition 2.2.4. [33] The *complete weight enumerator* (or *cwe*) of the quaternary code $\mathcal{C}$ is defined to be the homogeneous polynomial of degree n in four indeterminates X_0, X_1, X_2 and X_3 as

$$cwe_{\mathcal{C}}(X_0, X_1, X_2, X_3) = \sum_{c \in \mathcal{C}} X_0^{n_0(c)} X_1^{n_1(c)} X_2^{n_2(c)} X_3^{n_3(c)}, \tag{2.11}$$

where $n_j(c)$ is the number of components of c that are congruent to j (mod 4).

Example 2.2.5. [52] Let $\mathcal{K}_4$ be the linear quaternary code introduced in Example 2.1.7 with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

$\mathcal{K}_4$ has 16 codewords and the numbers $n_j(c)$, where $j \in \mathbb{Z}_4$ and $c \in \mathcal{K}_4$, are shown in the following table.

Table 2. 1 The numbers n_j for $\mathcal{K}_4$.

	n_0	n_1	n_2	n_3
0000	4	0	0	0
1111	0	4	0	0
2222	0	0	4	0
3333	0	0	0	4
0202	2	0	2	0
1313	0	2	0	2
2020	2	0	2	0
3131	0	2	0	2
0022	2	0	2	0
1133	0	2	0	2
2200	2	0	2	0
3311	0	2	0	2
0220	2	0	2	0
1331	0	2	0	2
2002	2	0	2	0
3113	0	2	0	2

Therefore the complete weight enumerator of $\mathcal{K}_4$ can be found as

$$cwe_{\mathcal{K}_4}(X_0, X_1, X_2, X_3) = X_0^4 + X_1^4 + X_2^4 + X_3^4 + 6X_0^2X_2^2 + 6X_1^2X_3^2. \qquad (2.12)$$

Example 2.2.6. Let $\mathcal{C}_1^{\perp}$ be the linear quaternary code introduced in Example 2.1.8 with generator matrix

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 0 \\ 3 & 3 & 2 & 0 & 1 \end{pmatrix}$$

as in (2.5). $\mathcal{C}_1^{\perp}$ has 16 codewords and the numbers $n_j(\mathrm{c})$ for $\mathrm{c} \in \mathcal{K}_4$ are shown in the following table.

Table 2. 2 The numbers n_j for $\mathcal{C}_1^{\perp}$.

	n_0	n_1	n_2	n_3
00000	5	0	0	0
01111	1	4	0	0
02222	1	0	4	0
03333	1	0	0	4
22002	2	0	3	0
20220	2	0	3	0
33201	1	1	1	2
30312	1	1	1	2
31023	1	1	1	2
32130	1	1	1	2
11203	1	2	1	1
12310	1	2	1	1
13021	1	2	1	1
10132	1	2	1	1
23113	0	2	1	2
21331	0	2	1	2

Therefore we have the complete weight enumerator of $\mathcal{C}_1^{\perp}$

$$cwe_{\mathcal{C}_1^{\perp}}(X_0, X_1, X_2, X_3) = X_0^5 + X_0X_1^4 + X_0X_2^4 + X_0X_3^4 + 2X_0^2X_2^3 + 2X_1^2X_2X_3^2 + 4X_0X_1^2X_2X_3 + 4X_0X_1X_2X_3^2. \tag{2.13}$$

Example 2.2.7. [52] The linear quaternary code $\mathcal{O}_8$ introduced in Example 2.1.9 with generator matrix (2.6) has 256 codewords. The complete weight enumerator of the octacode $\mathcal{O}_8$ can be found as

$$cwe_{\mathcal{O}_8}(X_0, X_1, X_2, X_3) = X_0^8 + X_1^8 + X_2^8 + X_3^8 + 14X_0^4X_2^4 + 14X_1^4X_3^4 + 56X_0^3X_1^3X_2X_3 + 56X_0^3X_1X_2X_3^3 + 56X_0X_1^3X_2^3X_3 + 56X_0X_1X_2^3X_3^3. \tag{2.14}$$

Permutation-equivalent quaternary codes have the same complete weight enumerator, but equivalent codes may have distinct *cwe*'s because of the sign changing. The appropriate weight enumerator for an equivalence class of codes is the *symmetrized weight enumerator* (or *swe*), obtained by combining X_1 and X_3 in (2.11).

Definition 2.2.8. [15] The *symmetrized weight enumerator* (or *swe*) of the quaternary code $\mathcal{C}$ is given by

$$swe_{\mathcal{C}}(X_0, X_1, X_2) = cwe_{\mathcal{C}}(X_0, X_1, X_2, X_1) = \sum_{c \in \mathcal{C}} X_0^{n_0(c)} X_1^{n_1(c)+n_3(c)} X_2^{n_2(c)}. \tag{2.15}$$

Example 2.2.9. The symmetrized weight enumerators of $\mathcal{K}_4$, $\mathcal{C}_1^{\perp}$ and $\mathcal{O}_8$ are

$$swe_{\mathcal{K}_4}(X_0, X_1, X_2) = X_0^4 + 8X_1^4 + X_2^4 + 6X_0^2X_2^2, \tag{2.16}$$

$$swe_{\mathcal{C}_1^{\perp}}(X_0, X_1, X_2) = X_0^5 + 2X_0X_1^4 + 2X_0^2X_2^3 + X_0X_2^4 + 2X_1^4X_2 + 8X_0X_1^3X_2, \tag{2.17}$$

$$swe_{\mathcal{O}_8}(X_0, X_1, X_2) = X_0^8 + 16X_1^8 + X_2^8 + 14X_0^4X_2^4 + 112X_0X_1^4X_2(X_0^2 + X_2^2). \tag{2.18}$$

Now, we define other notion of weight and distance for quaternary codes and the appropriate weight enumerators.

In communication schemes that use quaternary modulation, one can model the alphabet as a set of points regularly spaced on a circle. Usually, the four alphabet letters 0, 1, 2, 3 are represented by the signal points $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$, where $i = \sqrt{-1}$, in the complex plane.

The effect of additive, zero-mean Gaussian noise is such that a transmitted symbol is more likely received as a symbol close to it. So, Hamming distance is not a natural metric for measuring errors for quaternary codes. Instead, Lee weight and Lee distance is used for this purpose.

The *Lee weight* of an element *x* of $\mathbb{Z}_4$, with the elements {0, 1, 2, 3}, is defined as

$$w_L(x) = \begin{cases} 0 & \text{if} \quad x = 0 \\ 1 & \text{if} \quad x = 1 \text{ or } 3 \\ 2 & \text{if} \quad x = 2. \end{cases} \tag{2.19}$$

and the Lee weight of a sequence $\mathrm{x} = (x_1, ..., x_n) \in \mathbb{Z}_4^n$ is defined to be the integral sum of its *n* components, i.e. $w_L(\mathrm{x}) = \sum_{i=1}^{n} w_L(x_i)$.

This weight function defines a distance $d_L(\ ,\ )$ on $\mathbb{Z}_4$, which is called the *Lee distance*. The Lee distance between two elements *x* and *y* of $\mathbb{Z}_4$ is the Lee weight of their difference magnitude, i.e., $d_L(x, y) = w_L(x - y)$. The Lee distance between two sequences $\mathrm{x} = (x_1, ..., x_n)$ and $\mathrm{y} = (y_1, ..., y_n)$ of $\mathbb{Z}_4^n$ is defined as the sum of the Lee weights of the component-wise difference magnitudes, i.e.,

$$d_L(\mathrm{x}, \mathrm{y}) = \sum_{i=1}^{n} w_L(x_i - y_i).$$

Calling $d_E^2(i^a, i^b)$, the square of the *Euclidean distance* between i^a and i^b in the complex plane, where $a,\ b \in \mathbb{Z}_4$, one can show that [52]

$$d_L(a,b) = \frac{1}{2} d_E^2(i^a, i^b).$$

More generally, to any $\mathrm{x} = (x_1, ..., x_n) \in \mathbb{Z}_4^n$ there corresponds a complex vector $i^{\mathrm{x}} = (i^{x_1}, ..., i^{x_n})$. For any $\mathrm{x}, \mathrm{y} \in \mathbb{Z}_4^n$, the square of the *Euclidean distance* between i^{x} and i^{y} is given by

$$d_E^2(i^{\mathrm{x}}, i^{\mathrm{y}}) = \sum_{i=1}^{n} d_E^2(i^{x_i}, i^{y_i}).$$

Then the Lee distance in terms of the Euclidean distance is given by

$$d_L(\mathrm{x}, \mathrm{y}) = \frac{1}{2} d_E^2(i^{\mathrm{x}}, i^{\mathrm{y}}). \tag{2.20}$$

Definition 2.2.10. [26] The *Lee weight enumerator* of a quaternary code $\mathcal{C}$

$$Lee_{\mathcal{C}}(X, Y) = \sum_{\mathrm{c} \in \mathcal{C}} X^{2n - w_L(\mathrm{c})} Y^{w_L(\mathrm{c})}, \tag{2.21}$$

is a homogeneous polynomial of degree *2n*.

Since, for all $\mathrm{c} \in \mathbb{Z}_4^n$, $w_L(\mathrm{c}) = n_1(\mathrm{c}) + 2n_2(\mathrm{c}) + n_3(\mathrm{c})$, from (2.15) and (2.21) it is deduced that

$$Lee_{\mathcal{C}}(X, Y) = swe_{\mathcal{C}}(X^2, XY, Y^2). \tag{2.22}$$

Definition 2.2.11. [15] The *Hamming weight enumerator* of the quaternary code $\mathcal{C}$, less useful than the others, is

$$Ham_{\mathcal{C}}(X,Y) = \sum_{c \in \mathcal{C}} X^{n-w_H(c)} Y^{w_H(c)}, \tag{2.23}$$

where $w_H(c)$ is the Hamming weight of $c \in \mathcal{C}$. It is related to other weight enumerators by

$$Ham_{\mathcal{C}}(X,Y) = cwe_{\mathcal{C}}(X,Y,Y,Y) = swe_{\mathcal{C}}(X,Y,Y). \tag{2.24}$$

Example 2.2.12. The Lee weight enumerators of $\mathcal{K}_4$, $\mathcal{C}_1^{\perp}$ and $\mathcal{O}_8$ are

$$Lee_{\mathcal{K}_4}(X,Y) = X^8 + 14X^4Y^4 + Y^8, \tag{2.25}$$

$$Lee_{\mathcal{C}_1^{\perp}}(X,Y) = X^{10} + 2X^6Y^4 + 8X^5Y^5 + 4X^4Y^6 + X^2Y^8, \tag{2.26}$$

$$Lee_{\mathcal{O}_8}(X,Y) = X^{16} + 112X^{10}Y^6 + 30X^8Y^8 + 112X^6Y^{10} + Y^{16}. \tag{2.27}$$

The Hamming weight enumerators of $\mathcal{K}_4$, $\mathcal{C}_1^{\perp}$ and $\mathcal{O}_8$ are

$$Ham_{\mathcal{K}_4}(X,Y) = X^4 + 6X^2Y^2 + 9Y^4, \tag{2.28}$$

$$Ham_{\mathcal{C}_1^{\perp}}(X,Y) = X^5 + 2X^2Y^3 + 11XY^4 + 2Y^5, \tag{2.29}$$

$$Ham_{\mathcal{O}_8}(X,Y) = X^8 + 14X^4Y^4 + 112X^3Y^5 + 112XY^7 + 17Y^8. \tag{2.30}$$

At this point it may be instructive to compare all weight enumerators of the same code, say $\mathcal{K}_4$:

$$cwe_{\mathcal{K}_4}(X_0, X_1, X_2, X_3) = X_0^4 + X_1^4 + X_3^4 + 6X_1^2X_3^2 + 6X_0^2X_2^2 + X_2^4,$$

$$swe_{\mathcal{K}_4}(X_0, X_1, X_2) = X_0^4 + 8X_1^4 + 6X_0^2X_2^2 + X_2^4,$$

$$Lee_{\mathcal{K}_4}(X, Y) = X^8 + 14X^4Y^4 + Y^8,$$

$$Ham_{\mathcal{K}_4}(X, Y) = X^4 + 6X^2Y^2 + 9Y^4.$$

As in the binary case, the strongest tool we have is an expression of the relationship between the weight enumerators of a linear quaternary code and its dual code, the *MacWilliams equation*.

Theorem 2.2.13. (*MacWilliams equation*) [33] Let $\mathcal{C}$ be a linear quaternary code, then

$$cwe_{\mathcal{C}^\perp}(X_0, X_1, X_2, X_3) = \frac{1}{|\mathcal{C}|} cwe_{\mathcal{C}}(X_0 + X_1 + X_2 + X_3,\ X_0 + iX_1 - X_2 - iX_3,\ X_0 - X_1 + X_2 - X_3,\ X_0 - iX_1 - X_2 + iX_3) \tag{2.31}$$

$$swe_{\mathcal{C}^\perp}(X_0, X_1, X_2) = \frac{1}{|\mathcal{C}|} swe_{\mathcal{C}}(X_0 + 2X_1 + X_2,\ X_0 - X_2,\ X_0 - 2X_1 + X_2), \tag{2.32}$$

$$Lee_{\mathcal{C}^\perp}(X, Y) = \frac{1}{|\mathcal{C}|} Lee_{\mathcal{C}}(X + Y,\ X - Y), \tag{2.33}$$

$$Ham_{\mathcal{C}^\perp}(X, Y) = \frac{1}{|\mathcal{C}|} Ham_{\mathcal{C}}(X + 3Y,\ X - Y). \tag{2.34}$$

Theorem 2.2.13 can be proved by using Hadamard transform which is described in [52].

Example 2.2.14. The linear quaternary code $\mathcal{C}_1$ in Example 2.1.7 has 64 codewords. It is not easy to compute the weight enumerators of $\mathcal{C}_1$ directly; but they can be computed by using Theorem 2.2.13. We have previously computed the weight enumerators of $\mathcal{C}_1^{\perp}$ in (2.13), (2.17), (2.26) and (2.29). Then the weight enumerators of $\mathcal{C}_1$ are found as

$$
\begin{aligned}
&cwe_{\mathcal{C}_1}(X_0,X_1,X_2,X_3)\\
&=\frac{1}{16}cwe_{\mathcal{C}_1^{\perp}}(X_0+X_1+X_2+X_3,\ X_0+iX_1-X_2-iX_3,\\
&\qquad X_0-X_1+X_2-X_3,\ X_0-iX_1-X_2+iX_3)\\
&=\frac{1}{16}[(X_0+X_1+X_2+X_3)^5+(X_0+X_1+X_2+X_3)(X_0+iX_1-X_2-iX_3)^4\\
&+(X_0+X_1+X_2+X_3)(X_0-X_1+X_2-X_3)^4+(X_0+X_1+X_2+X_3)(X_0-iX_1-X_2+iX_3)^4\\
&+2(X_0+X_1+X_2+X_3)^2(X_0-X_1+X_2-X_3)^3\\
&+2(X_0+iX_1-X_2-iX_3)^2(X_0-X_1+X_2-X_3)(X_0-iX_1-X_2+iX_3)^2\\
&+4(X_0+X_1+X_2+X_3)(X_0+iX_1-X_2-iX_3)^2(X_0-X_1+X_2-X_3)(X_0-iX_1-X_2+iX_3)\\
&+4(X_0+X_1+X_2+X_3)(X_0+iX_1-X_2-iX_3)(X_0-X_1+X_2-X_3)(X_0-iX_1-X_2+iX_3)^2]
\end{aligned}
$$

$$
\begin{aligned}
&swe_{\mathcal{C}_1}(X_0,X_1,X_2)\\
&=\frac{1}{|16|}swe_{\mathcal{C}_1^{\perp}}(X_0+2X_1+X_2,\ X_0-X_2,\ X_0-2X_1+X_2)\\
&=\frac{1}{|16|}[(X_0+2X_1+X_2)^5+2(X_0+2X_1+X_2)(X_0-X_2)^4\\
&+2(X_0+2X_1+X_2)^2(X_0-2X_1+X_2)^3+(X_0+2X_1+X_2)(X_0-2X_1+X_2)^4\\
&+2(X_0-X_2)^4(X_0-2X_1+X_2)+8(X_0+2X_1+X_2)(X_0-X_2)^3(X_0-2X_1+X_2)]
\end{aligned}
$$

$$Lee_{\mathcal{C}_1}(X,Y) = \frac{1}{|16|} Lee_{\mathcal{C}_1^{\perp}}(X+Y,\ X-Y)$$

$$= \frac{1}{|16|}[(X+Y)^{10} + 2(X+Y)^6(X-Y)^4 + 8(X+Y)^5(X-Y)^5$$

$$+ 4(X+Y)^4(X-Y)^6 + (X+Y)^2(X-Y)^8]$$

$$Ham_{\mathcal{C}_1}(X,Y) = \frac{1}{|16|} Ham_{\mathcal{C}_1^{\perp}}(X+3Y,\ X-Y)$$

$$= \frac{1}{|16|}[(X+3Y)^5 + 2(X+3Y)^2(X-Y)^3$$

$$+ 11(X+3Y)(X-Y)^4 + 2(X-Y)^5]$$

2.3 DISTANCE ENUMERATORS OF BINARY CODES

The distance distributions and distance enumerators play an important role for the understanding of nonlinear binary codes to be studied in the last chapter. All definitions and properties described in this section can be found in [18].

Let A_i be the number of codewords of Hamming weight *i* in *C*. It is easily verified that $A_0 = 1$ when $\mathbf{0} \in C$, and $\sum_{i=0}^{n} A_i = |C|$. The set $\{A_0, A_1, ..., A_n\}$ is called the *weight distribution* of code *C*.

Let C be a binary code of length *n*, which is not necessarily linear. Define

$$B_i = \frac{1}{|C|} |\{(\mathrm{c}, \mathrm{c}') \mid \mathrm{c}, \mathrm{c}' \in \mathrm{C},\ d_H(\mathrm{c}, \mathrm{c}') = i\}|, \quad i = 0,\ 1, ..., n.$$

Clearly $B_0 = 1$ and $\sum_{i=0}^{n} B_i = |C|$. The set $\{B_0, B_1, ..., B_n\}$ is called the *distance distribution* of binary code *C*.

Definition 2.3.1. [18] The *distance enumerator* of the binary code *C* is defined as

$$D_C(X, Y) = \sum_{i=0}^{n} B_i X^{n-i} Y^i .$$

Let *C* be a binary code of length *n* and any $c' \in C$, define

$$C - c' = \{c - c' | c \in C\},$$

and

$$A_i(c') = |\{c \in C | w_H(c - c') = i\}|, \quad i = 0, 1, \ldots, n.$$

Then $\{A_0(c'), A_1(c'), \ldots, A_n(c')\}$ is the weight distribution of $C - c'$, and the weight enumerator can be defined as follows

$$W_{C-c'}(X, Y) = \sum_{i=0}^{n} A_i(c') X^{n-i} Y^i .$$

As the original weight distribution, this weight distribution also satisfies the properties $A_0(c') = 1$ and $\sum_{i=0}^{n} A_i(c') = |C|$.

Definition 2.3.2. [39] Let *C* be a binary code of length *n*. If, for all $c \in C$, $A_i = A_i(c)$, $i = 0, 1, ..., n$, or equivalently, $W_C(X, Y) = W_{C-c}(X, Y)$, then *C* is called *distance invariant*.

For such a code, we also have $B_i = A_i$, $i = 0,1,...,n$ and $D_C(X,Y) = W_C(X,Y)$. Since for linear binary codes, $B_i = A_i = A_i(\mathrm{c})$, $i = 0,1,...,n$ and $D_C(X,Y) = W_C(X,Y) = W_{C-\mathrm{c}}(X,Y)$ for all $\mathrm{c} \in C$; linear codes are distance invariant.

Similar to MacWilliams transform of weight distribution A_i and weight enumerator $W_C(X,Y)$, in the following, the MacWilliams transforms of distance distribution B_i and distance enumerator $D_C(X,Y)$ are defined.

Definition 2.3.3. [18] Let $\{B_0, B_1,..., B_n\}$ be the distance distribution of a binary code *C* of length *n.* Define

$$B'_k = |C|^{-1} \sum_{i=0}^{n} B_i K_k(i), \quad k = 0, 1,\ldots,n, \tag{2.35}$$

where $K_k(i)$ is the value the Krawtchouk polynomial $K_k(x)$ when $q = 2$ at the point $x = i$. $\{B'_0, B'_1,..., B'_n\}$ is called the MacWilliams transform of $\{B_0, B_1,..., B_n\}$. Moreover, the MacWilliams transform of $D_C(X,Y)$ is defined as in (2.9)

$$D'_C(X,Y) = |C|^{-1} D_C(X+Y, X-Y).$$

After the definition of MacWilliams transform of distance distribution, it is expected that $B'_0 = 1$ just as $B_0 = 1$. By using the following lemma, we can generalize this expectation.

Lemma 2.3.4. [18] For any $\mathrm{x} \in \mathbb{Z}_2^n$ with $w_H(\mathrm{x}) = i$,

$$\sum_{\substack{\mathrm{y} \in \mathbb{Z}_2^n \\ w_H(\mathrm{y}) = k}} (-1)^{\mathrm{x}\cdot\mathrm{y}} = K_k(i).$$

Proposition 2.3.5. [18] Let C be a binary code with distance distribution $\{B_0, B_1, ..., B_n\}$ and let $\{B_0', B_1', ..., B_n'\}$ be its MacWilliams transformation. Then $B_0' = 1$ and $B_k' \geq 0$ for $k = 1, 2, \ldots, n$.

From the proof of Proposition 2.3.5, which can be found in [18] and [52], the following corollary describes a new relation between A_k' and B_k' for some special k.

Corollary 2.3.6. [18] Let C be a binary code of length n with weight distribution $\{A_0, A_1, ..., A_n\}$ and distance distribution $\{B_0, B_1, ..., B_n\}$, and let $\{A_0', A_1', ..., A_n'\}$ and $\{B_0', B_1', ..., B_n'\}$ be their MacWilliams transforms, respectively. Assume that $B_k' = 0$ for some k where $0 \leq k \leq n$, then

$$\sum_{x \in C} (-1)^{x \cdot z} = 0,$$

for every $z \in \mathbb{Z}_2^n$ with $w_H(z) = k$ and $A_k' = 0$.

Now, we can finish this section with the following definitions.

Definition 2.3.7. [18] Let C be a binary code of length n with distance distribution $\{B_0, B_1, ..., B_n\}$, and $\{B_0', B_1', ..., B_n'\}$ be its MacWilliams transforms. Then define four parameters as follows.

i. $d = \min\{i \mid i > 0, B_i > 0\}$,

ii. $s = |\{i \mid i > 0, B_i > 0\}|$,

iii. $d' = \min\{i \mid i > 0, B_i' > 0\}$,

iv. $s' = |\{i \mid i > 0, B_i' > 0\}|$.

d is said to be the *minimum distance* of *C*, and s is the number of distinct nonzero distances. Additionally, d' is called the *dual distance*, and s' is said to be the *external distance* of a code *C*. These four parameters are called the *four fundamental parameters* of the code by Delsarte [18]. Moreover, it is clear that, if C is linear, d' is the minimum distance of the dual code $C^{\perp}$.

CHAPTER 3

BINARY IMAGES OF QUATERNARY CODES

Although there are several nonlinear binary codes having more codewords than linear codes with the same length and minimal distance, to describe them are not so easy. Around 1990, it is shown that the well-known nonlinear binary codes can be constructed by converting linear codes over $\mathbb{Z}_4$ into nonlinear codes over $\mathbb{Z}_2$, using a map known as the Gray map [40], [8], [25], [26].

In this chapter, we study the properties of the binary images of the linear quaternary codes under the Gray map. The conditions for the binary image of a linear quaternary code to be a linear code and for a binary code to be $\mathbb{Z}_4$-linear are discussed and a construction of linear quaternary codes by using linear binary codes is given. Most definitions and properties described in the first, second and third sections can be found in [26] and [52].

The last two sections include our contributions. In Section 3.4, we present some conditions for simplifying the linearity check of the binary image of a linear quaternary code, in lemmas and propositions 3.4.1 to 3.4.6. Finally, in Section 3.5, we discuss the $\mathbb{Z}_4$-linearity of the Reed-Muller and Hamming codes and analyze all linear quaternary codes of length 4 to show that there is no nonlinear and $\mathbb{Z}_4$-linear binary code better than the extended Hamming code of length 8. Examples without any given reference are those that we generate.

3.1 THE GRAY MAP

In communication systems employing quadrature phase-shift keying (QPSK), the preferred assignment of two information bits to the four possible phases is the one shown in Figure 3.1, in which adjacent phases differ by only one binary digit. This mapping is called the *Gray map* and has the advantage that, when a quaternary codeword is transmitted across an additive white Gaussian noise channel, the errors most likely to occur are those causing a single erroneously decoded information bit.

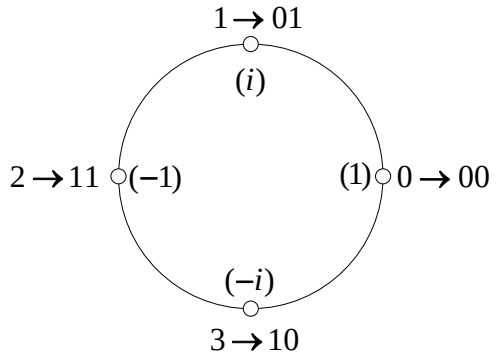

Figure 3. 1 Gray encoding of quaternary symbols and QPSK phases.

The Gray map is a bijection from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ and usually denoted by ϕ, i.e.,

$$\begin{aligned} \phi : \mathbb{Z}_4 &\rightarrow \mathbb{Z}_2^2 \\ 0 &\mapsto 00 \\ 1 &\mapsto 01 \\ 2 &\mapsto 11 \\ 3 &\mapsto 10 \end{aligned}$$

Clearly,

$$w_L(x) = w_H(\phi(x)) \quad \text{for all } x \in \mathbb{Z}_4,$$
$$d_L(x, y) = d_H(\phi(x), \phi(y)) \quad \text{for all } x,\ y \in \mathbb{Z}_4. \tag{3.1}$$

Formally, three maps α, β, γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ are defined by Table 3.1, which can also be expressed as a mapping $(\alpha\,\beta\,\gamma)(x)$ from $x \in \mathbb{Z}_4$ to $\mathbb{Z}_2^3$ as follows

$$\begin{aligned}
&(\alpha\,\beta\,\gamma)(0) = (0\ 0\ 0),\\
&(\alpha\,\beta\,\gamma)(1) = (1\ 0\ 1),\\
&(\alpha\,\beta\,\gamma)(2) = (0\ 1\ 1),\\
&(\alpha\,\beta\,\gamma)(3) = (1\ 1\ 0)
\end{aligned} \tag{3.2}$$

Table 3.1 The maps α, β, γ.

$\mathbb{Z}_4$	α	β	γ
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

Clearly, α is a group homomorphism from $\mathbb{Z}_4$ to $\mathbb{Z}_2$, but β and γ are not. The 2-adic expansion of $x \in \mathbb{Z}_4$ is

$$x = \alpha(x) + 2\beta(x). \tag{3.3}$$

For all $x \in \mathbb{Z}_4$, it is obvious that

$$\alpha(x) + \beta(x) + \gamma(x) \equiv 0 \pmod 2.$$

The Gray map ϕ defined above can be expressed in terms of β and γ as follows:

$$\phi(x) = (\beta(x),\ \gamma(x)) \quad \text{for all } x \in \mathbb{Z}_4. \tag{3.4}$$

For $x = (x_1,...,x_n) \in \mathbb{Z}_4^n$, the maps $\alpha,\ \beta,\ \gamma$ are extended to maps from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^n$ by

$$\alpha(x) = (\alpha(x_1),...,\alpha(x_n)),$$

$$\beta(x) = (\beta(x_1),...,\beta(x_n)),$$

$$\gamma(x) = (\gamma(x_1),...,\gamma(x_n)).$$

Then ϕ is extended to $\mathbb{Z}_4^n$ in an obvious way. Clearly, the extended ϕ is a bijection from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. For any $x \in \mathbb{Z}_4^n$, $\phi(x)$ is called the *binary image* of x under ϕ.

The crucial property of the Gray map is that it preserves distances as stated in the following theorem.

Theorem 3.1.1. [26] ϕ is a distance preserving mapping from

$$(\mathbb{Z}_4^n,\ \textit{Lee distance}) \quad \text{to} \quad (\mathbb{Z}_2^{2n},\ \textit{Hamming distance}).$$

It is easy to see from the definitions of Chapter 2, and (3.1) that

$$w_L(x) = w_H(\phi(x)) \quad \text{for all } x \in \mathbb{Z}_4^n, \tag{3.5}$$

$$d_L(x, y) = d_H(\phi(x), \phi(y)) \quad \text{for all } x,\ y \in \mathbb{Z}_4^n. \tag{3.6}$$

From (2.20), $d_L(\mathrm{x},\mathrm{y}) = \frac{1}{2} d_E^2(i^{\mathrm{x}}, i^{\mathrm{y}})$, and (3.6), the Hamming distance between the binary images $\phi(\mathrm{x})$ and $\phi(\mathrm{y})$ is proportional to the squared Euclidean distance between the complex sequences i^{x} and i^{y}, i.e.,

$$d_H(\phi(\mathrm{x}),\phi(\mathrm{y})) = \frac{1}{2} d_E^2(i^{\mathrm{x}}, i^{\mathrm{y}}) \quad \text{for all } \mathrm{x},\ \mathrm{y} \in \mathbb{Z}_4^n .$$

3.2 BINARY IMAGES OF QUATERNARY CODES

The Gray map gives a relation between quaternary codes and binary codes. In this section, it is discussed the properties of this relation and the duality of the binary images under the Gray map.

Let $\mathcal{C}$ be a quaternary code. The *binary image* of $\mathcal{C}$ under the Gray map is defined by

$$C = \phi(\mathcal{C}) = \{\phi(\mathrm{c}) \mid \mathrm{c} \in \mathcal{C}\} .$$

If $\mathcal{C}$ is of length n, then C is a binary code of length $2n$, i.e. $C \subseteq \mathbb{Z}_2^{2n}$.

We recall that the minimum Hamming weight and distance of a binary code C are

$$\min\{w_H(\phi(\mathrm{c})) \mid \mathrm{c} \in C,\ \mathrm{c} \neq \mathbf{0}\},$$

$$\min\{d_H(\phi(\mathrm{c}),\phi(\mathrm{c}')) \mid \mathrm{c},\mathrm{c}' \in C,\ \mathrm{c} \neq \mathrm{c}'\} .$$

Similarly, the *minimum Lee weight* and *distance* of a quaternary code $\mathcal{C}$ is defined by

$$\min\{w_L(\mathrm{c}) \mid \mathrm{c} \in \mathcal{C},\ \mathrm{c} \neq \mathbf{0}\},$$

$$\min\{d_L(\mathrm{c},\mathrm{c}') \mid \mathrm{c},\mathrm{c}' \in \mathcal{C},\ \mathrm{c} \neq \mathrm{c}'\}.$$

From Theorem 3.1.1 we have

Proposition 3.2.1. [26] Let $\mathcal{C}$ be a quaternary code and $C = \phi(\mathcal{C})$. Then the minimum Lee weight and distance of $\mathcal{C}$ are equal to the minimum Hamming weight and distance of $C = \phi(\mathcal{C})$, respectively.

Example 3.2.2. The linear quaternary code $\mathcal{K}_4$ introduced in Example 2.1.7 with generator matrix (2.3)

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

consists of 16 codewords. Using (3.2) that defines the mapping $(\beta\,\gamma)(x)$ as $(\beta\,\gamma)(0) = (0\ 0),\ (\beta\,\gamma)(1) = (0\ 1),\ (\beta\,\gamma)(2) = (1\ 1),\ (\beta\,\gamma)(3) = (1\ 0)$, and (3.4) that defines $\phi(x) = (\beta(x),\ \gamma(x))$ for all $x \in \mathbb{Z}_4$, we find

$$\phi(0000) = (\beta(0000),\ \gamma(0000)) = (00000000)$$
$$\phi(1111) = (\beta(1111),\ \gamma(1111)) = (00001111)$$
$$\phi(2222) = (\beta(2222),\ \gamma(2222)) = (11111111)$$
$$\phi(3333) = (\beta(3333),\ \gamma(3333)) = (11110000)$$
$$\phi(0022) = (\beta(0022),\ \gamma(0022)) = (00110011)$$
$$\phi(0202) = (\beta(0202),\ \gamma(0202)) = (01010101)$$
$$\phi(0220) = (\beta(0220),\ \gamma(0220)) = (01100110)$$

$$\phi(1133)=(\beta(1133),\ \gamma(1133))=(00111100)$$
$$\phi(1313)=(\beta(1313),\ \gamma(1313))=(01011010)$$
$$\phi(1331)=(\beta(1331),\ \gamma(1331))=(01101001)$$
$$\phi(2002)=(\beta(2002),\ \gamma(2002))=(10011001)$$
$$\phi(2020)=(\beta(2020),\ \gamma(2020))=(10101010)$$
$$\phi(2200)=(\beta(2200),\ \gamma(2200))=(11001100)$$
$$\phi(3113)=(\beta(3113),\ \gamma(3113))=(10010110)$$
$$\phi(3131)=(\beta(3131),\ \gamma(3131))=(10100101)$$
$$\phi(3311)=(\beta(3311),\ \gamma(3311))=(11000011).$$

Therefore the binary image $\phi(\mathcal{K}_4)$ of the linear quaternary code $\mathcal{K}_4$ consists of these 16 codewords. It is easy to see that $\phi(\mathcal{K}_4)$ is a linear binary code with minimum distance 4. Actually, $\phi(\mathcal{K}_4)$ is the extended binary Hamming code of length 8, which has the following generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{3.7}$$

In general, the binary image of a linear quaternary code is not necessarily linear. If it is linear, its generator matrix can be deduced from the generator matrix of the linear quaternary code.

Proposition 3.2.3. [26] Let $C=\phi(\mathcal{C})$ be the binary image of a linear quaternary code $\mathcal{C}$ with generator matrix $G=\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}$, given by (2.1). If C is linear, then C has generator matrix

$$\begin{pmatrix} I_{k_1} & A & \alpha(B) & I_{k_1} & A & \alpha(B) \\ 0 & I_{k_2} & D & 0 & I_{k_2} & D \\ 0 & 0 & \beta(B) & I_{k_1} & A & \gamma(B) \end{pmatrix}, \tag{3.8}$$

where the mapping $(\alpha\,\beta\,\gamma)(x)$ from $x \in \mathbb{Z}_4$ to $\mathbb{Z}_2^3$ is defined by (3.2) as $(\alpha\,\beta\,\gamma)(0) = (0\ 0\ 0)$, $(\alpha\,\beta\,\gamma)(1) = (1\ 0\ 1)$, $(\alpha\,\beta\,\gamma)(2) = (0\ 1\ 1)$, $(\alpha\,\beta\,\gamma)(3) = (1\ 1\ 0)$.

Note that the generator matrix (3.7) of $\phi(\mathcal{K}_4)$ in Example 3.2.2 can be obtained from the generator matrix (2.1) of $\mathcal{K}_4$ of the same example, using Proposition 3.2.3.

We recall that a binary code C is said to be *distance invariant* if the Hamming weight distributions of its translators $\mathrm{u} + C$ are the same for all $\mathrm{u} \in C$ [39]. Clearly, all linear codes are distance invariant, including the linear binary and linear quaternary codes. Although the binary image of a linear quaternary code is not necessarily linear, by Theorem 3.1.1, it has the following property.

Theorem 3.2.4. [26] The binary image $C = \phi(\mathcal{C})$ of a linear quaternary code $\mathcal{C}$ is distance invariant.

The binary image of a linear quaternary code is, in general, not linear because ϕ is not a linear map, and so it need not have a dual code. In [26], it is defined the $\mathbb{Z}_4$-*dual* of $C = \phi(\mathcal{C})$ to be $C_\perp = \phi(\mathcal{C}^\perp)$, as in the figure

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & C = \phi(\mathcal{C}) \\ \downarrow & & \\ \mathcal{C}^\perp & \longrightarrow & C_\perp = \phi(\mathcal{C}^\perp). \end{array}$$

Figure 3. 2 The relation between $C = \phi(\mathcal{C})$ and $C_\perp = \phi(\mathcal{C}^\perp)$.

Although we cannot always add an arrow marked ‘dual’ on the right side to produce a commuting diagram, the following theorem provides a strong relation between $C = \phi(\mathfrak{C})$ and $C_\perp = \phi(\mathfrak{C}^\perp)$. By Theorem 3.1.1 and (2.33), we have

Theorem 3.2.5. [26] Let $\mathfrak{C}$ and $\mathfrak{C}^\perp$ be dual linear quaternary codes, and $C = \phi(\mathfrak{C})$ and $C_\perp = \phi(\mathfrak{C}^\perp)$ be their binary images. Then the weight enumerators $W_C(X,Y)$ and $W_{C_\perp}(X,Y)$ of C and $C_\perp$, respectively, are related by the binary MacWilliams identity

$$W_{C_\perp}(X,Y) = \frac{1}{|C|} W_C(X+Y, X-Y). \tag{3.9}$$

Thus, by Proposition 2.2.3, their weight distributions $\{A_0, A_1, ..., A_{2n}\}$ of $C = \phi(\mathfrak{C})$ and $\{A'_0, A'_1, ..., A'_{2n}\}$ of $C_\perp = \phi(\mathfrak{C}^\perp)$ are the MacWilliams transform of each other.

From Theorem 3.2.5, a new notion of a dual code can be defined as follows.

Definition 3.2.6. [26] If $\mathfrak{C}$ is a linear quaternary code and $\mathfrak{C}^\perp$ is its dual code, then $C = \phi(\mathfrak{C})$ and $C_\perp = \phi(\mathfrak{C}^\perp)$ are called *formally dual.* If $\mathfrak{C}$ is self dual (i.e. $\mathfrak{C}^\perp = \mathfrak{C}$), then $C = C_\perp$ and C is called *formally self-dual.*

3.3 LINEARITY CONDITIONS

In this section, $\mathbb{Z}_4$-linearity of a binary code is defined; then, necessary and sufficient conditions for a binary code to be $\mathbb{Z}_4$-linear and for the binary image of a linear quaternary code to be a linear code are given. Finally, a construction of linear quaternary codes by using linear binary codes is explained.

Definition 3.3.1. [26] A binary code C is called $\mathbb{Z}_4$-linear if after a permutation of its coordinates, it is the binary image of a linear quaternary code $\mathcal{C}$.

There is a trivial necessary condition for a binary code to be $\mathbb{Z}_4$-linear.

Proposition 3.3.2. [52] If a binary code is $\mathbb{Z}_4$- linear , then its length is even.

Define the "swap" map σ, that interchanges the left and right halves of each $2n$- dimensional vector $(x_1,...,x_{2n})$, as follows:

$$\sigma : (x_1,...,x_n,\ x_{n+1},...,x_{2n}) \rightarrow (x_{n+1},...,x_{2n},\ x_1,...,x_n). \tag{3.10}$$

In other words σ applies the permutation $(1,\ n+1)(2,\ n+2)\cdots(n,\ 2n)$ to the coordinates.

Then for any $\mathrm{x} \in \mathbb{Z}_4^n$,

$$\sigma(\phi(\mathrm{x})) = \sigma(\beta(\mathrm{x})\ \gamma(\mathrm{x})) = (\gamma(\mathrm{x})\ \beta(\mathrm{x})) = \phi(-\mathrm{x}), \tag{3.11}$$

as can be verified using (3.2), which defines the three maps $\alpha,\ \beta,\ \gamma$ as $(\alpha\,\beta\,\gamma)(0) =$ $(0\ 0\ 0),\ (\alpha\,\beta\,\gamma)(1) = (1\ 0\ 1),\ (\alpha\,\beta\,\gamma)(2) = (0\ 1\ 1),\ (\alpha\,\beta\,\gamma)(3) = (1\ 1\ 0)$.

Proposition 3.3.3. [26] If a binary code C is $\mathbb{Z}_4$- linear , then after a permutation of its coordinates, $\sigma(C) = C$.

Now, we need the following two lemmas to show the way to the necessary condition for a binary code to be $\mathbb{Z}_4$-linear.

Lemma 3.3.4. [26] For all $x,\ y \in \mathbb{Z}_4^n$,

$$(\phi(x) + \sigma(\phi(x)) * (\phi(y) + \sigma(\phi(y)) = \phi(2\alpha(x) * \alpha(y)),$$

where $*$ denotes the component-wise multiplication of two vectors; $(\alpha\,\beta\,\gamma)(0) = (0\ 0\ 0)$, $(\alpha\,\beta\,\gamma)(1) = (1\ 0\ 1)$, $(\alpha\,\beta\,\gamma)(2) = (0\ 1\ 1)$, $(\alpha\,\beta\,\gamma)(3) = (1\ 1\ 0)$, as defined by (3.2), and $\phi(x) = (\beta(x),\ \gamma(x))$ for all $x \in \mathbb{Z}_4$.

Lemma 3.3.5. [26] For all $x,\ y \in \mathbb{Z}_4^n$,

$$\begin{aligned}\phi(x + y) &= \phi(x) + \phi(y) + (\phi(x) + \sigma(\phi(x))) * (\phi(y) + \sigma(\phi(y))) \\ &= \phi(x) + \phi(y) + \phi(2\alpha(x) * \alpha(y)).\end{aligned} \tag{3.12}$$

Proposition 3.3.6. [26] A binary, not necessarily linear, code C of even length is $\mathbb{Z}_4$-linear if and only if after a permutation of its coordinates,

$$u,\ v \in C \ \Rightarrow\ u + v + (u + \sigma(u)) * (v + \sigma(v)) \in C. \tag{3.13}$$

The proof of Proposition 3.3.6 that can be found in [26] and [52] is done by using Lemma 3.3.4 and 3.3.5.

Corollary 3.3.7. [26] A linear binary code C of even length is $\mathbb{Z}_4$-linear if and only if after a permutation of its coordinates,

$$u,\ v \in C \ \Rightarrow\ (u + \sigma(u)) * (v + \sigma(v)) \in C.$$

The following proposition that can be proved using (3.12) shows when the binary image of a linear quaternary code is linear.

Proposition 3.3.8. [26] The binary image $C = \phi(\mathcal{C})$ of a linear quaternary code $\mathcal{C}$ is linear if and only if

$$x, y \in \mathcal{C} \Rightarrow 2\alpha(x) * \alpha(y) \in \mathcal{C}. \tag{3.14}$$

Corollary 3.3.9. [26] Let $\mathcal{C}$ be a linear quaternary code, $\{x_1,...,x_m\}$ be the set of generators of $\mathcal{C}$, and $C = \phi(\mathcal{C})$. Then, C is linear if and only if $2\alpha(x_i) * \alpha(x_j) \in \mathcal{C}$ for all i, j satisfying $1 \le i \le j \le m$.

The proofs of Lemmas 3.3.4 and 3.3.5 can be found in [52], those of Propositions 3.3.6 and 3.3.8 are in [26].

Example 3.3.10. [52] Consider the linear quaternary code $\mathcal{K}_4$ introduced in Example 2.1.7 with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

It can be easily checked that for any two rows x and y of this generator matrix, $2\alpha(x) * \alpha(y) \in \mathcal{K}_4$. By Corollary 3.3.9, $\phi(\mathcal{K}_4)$ is linear binary code. Since $\mathcal{K}_4$ is a self-dual code, $\phi(\mathcal{K}_4)$ is formally self-dual.

Example 3.3.11. Consider the linear quaternary code $\mathcal{C}_1$ introduced in Example 2.1.8 with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 \end{pmatrix}.$$

If we denote the first and second rows of this matrix by x_1 and x_2, respectively, i.e., $x_1 = (1\ 0\ 0\ 3\ 1)$, $x_2 = (0\ 1\ 0\ 2\ 1)$ we have

$$2\alpha(x_1) * \alpha(x_2) = 2(1\ 0\ 0\ 1\ 1) * (0\ 1\ 0\ 0\ 1) = (0\ 0\ 0\ 0\ 2) \notin \mathcal{C}_1.$$

So, the binary code $\phi(\mathcal{C}_1)$ of length 10 is nonlinear by Corollary 3.3.9. By checking the weights of all the 64 codewords of $\phi(\mathcal{C}_1)$, we find that $\phi(\mathcal{C}_1)$ has minimum weight 3. Since the zero word is in $\phi(\mathcal{C}_1)$, and by Theorem 3.2.4 $\phi(\mathcal{C}_1)$ is distance invariant, we deduce that $\phi(\mathcal{C}_1)$ has minimum distance 3.

Example 3.3.12. [52] Consider the octacode $\mathcal{O}_8$ introduced in Example 2.1.9 with generator matrix (2.6). If we denote the first and second rows of (2.6) by x_1 and x_2, respectively, i.e., $x_1 = (1\ 0\ 0\ 0\ 3\ 1\ 2\ 1)$, $x_2 = (0\ 1\ 0\ 0\ 1\ 2\ 3\ 1)$ we have

$$2\alpha(x_1) * \alpha(x_2) = 2(1\ 0\ 0\ 0\ 1\ 1\ 0\ 1) * (0\ 1\ 0\ 0\ 1\ 0\ 1\ 1) = (0\ 0\ 0\ 0\ 2\ 0\ 0\ 2) \notin \mathcal{O}_8.$$

So, by Corollary 3.3.9, the binary code $\phi(\mathcal{O}_8)$ is nonlinear. It is of length 16 and has 256 codewords. Since $\mathcal{O}_8$ is a self-dual linear quaternary code, $\phi(\mathcal{O}_8)$ is formally self-dual. $\phi(\mathcal{O}_8)$ is called *Nordstrom-Robinson code*. It is easy to check that the minimum weight of $\phi(\mathcal{O}_8)$ is 6. Since the zero word is in $\phi(\mathcal{O}_8)$ and by Theorem 3.2.4 $\phi(\mathcal{O}_8)$ is distance invariant, $\phi(\mathcal{O}_8)$ has minimum distance 6. Puncturing the coordinates of the codewords of $\phi(\mathcal{O}_8)$ at a fixed position, a nonlinear binary code of length 15, with 256 codewords and minimum distance 5 is obtained. This code has higher rate (8/15) than the 2-error-correcting BCH code of length 15 and minimum distance 5 that contains only 128 codewords (so having the rate 7/15).

Linear quaternary codes, if not constructed directly in $\mathbb{Z}_4$, can be alternatively constructed by using two linear binary codes as described in Proposition 3.3.15. Let $\mathcal{C}$ be a linear quaternary code. There are two binary codes $C^{(1)}$ and $C^{(2)}$, which are canonically associated with $\mathcal{C}$, defined by

$$C^{(1)} = \{\alpha(\mathrm{c}) \mid \mathrm{c} \in \mathcal{C}\}, \tag{3.15}$$

$$C^{(2)} = \{\beta(\mathrm{c}) \mid \mathrm{c} \in \mathcal{C},\ \alpha(\mathrm{c}) = \mathbf{0}\}. \tag{3.16}$$

Proposition 3.3.13. [15] Let $\mathcal{C}$ be a linear quaternary code of length n with generator matrix (2.1), and $C^{(1)}$ and $C^{(2)}$ be the binary codes defined by (3.15) and (3.16), respectively. Then $C^{(1)}$ is a linear binary $[n,\ k_1]$ code with generator matrix

$$\begin{pmatrix} I_{k_1} & A & \alpha(B) \end{pmatrix}, \tag{3.17}$$

while $C^{(2)} \supseteq C^{(1)}$ is a linear binary $[n,\ k_1 + k_2]$ code with generator matrix

$$\begin{pmatrix} I_{k_1} & A & \alpha(B) \\ 0 & I_{k_2} & D \end{pmatrix}, \tag{3.18}$$

Proposition 3.3.14. [15] Given two linear binary codes C' and C'', both of length n, with $C' \subseteq C''$, there is a linear quaternary code $\mathcal{C}$ with $C^{(1)} = C'$ and $C^{(2)} = C''$. If, in addition, the Hamming weight of all codewords of C' is divisible by 4 (i.e., C' is doubly even), and $C'' \subseteq C'^{\perp}$, then there is a self-orthogonal linear quaternary code $\mathcal{C}$ with $C^{(1)} = C'$ and $C^{(2)} = C''$. Furthermore, if $C'' = C'^{\perp}$, then $\mathcal{C}$ is self-dual.

Now, the construction of a linear quaternary code from two linear binary codes can be given as follows.

Proposition 3.3.15. [5] Let C' and C'' be two linear binary codes of length n and $C' \subseteq C''$. Define

$$\mathcal{C} = C' + 2C'' = \{a + 2b \mid a \in C',\ b \in C''\}. \tag{3.19}$$

Then $\mathcal{C}$ is a linear quaternary code if and only if

$$a, a' \in C' \Rightarrow a * a' \in C''. \tag{3.20}$$

In this case,

(i) $C^{(1)} = C'$ and $C^{(2)} = C''$.

(ii) $\phi(\mathcal{C}) = \{(u, u + v) \mid u \in C',\ v \in C''\}$.

(iii) If C' is doubly even, and $C'' \subseteq C'^{\perp}$, then $\mathcal{C}$ is a self-orthogonal linear quaternary code if and only if

$$a, a' \in C' \Rightarrow w_H(a * a') \equiv 0 \pmod 4 \tag{3.21}$$

In this case, if $C'' = C'^{\perp}$, then $\mathcal{C}$ is a self-dual linear quaternary code.

Example 3.3.16. [52] Consider the linear quaternary code $\mathcal{K}_4$ studied in Example 2.1.7 with generator matrix (2.3). By Proposition 3.3.13, the generator matrices of the linear binary codes $C^{(1)}$ and $C^{(2)}$ are

$$\begin{pmatrix}1 & 1 & 1 & 1\end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix}1 & 1 & 1 & 1\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\end{pmatrix},$$

respectively.

It is clear that condition (3.21) is satisfied for $C^{(1)} = C'$ and $C^{(2)} = C''$, so $C^{(1)} + 2C^{(2)} = \mathcal{K}_4$ is a linear quaternary code. Since $C^{(1)}$ is doubly even, (3.21) is also fulfilled; additionally $C^{(2)} = C^{(1)\perp}$, so $\mathcal{K}_4$ is self-dual.

3.4 LINEARITY ANALYSIS

In the previous section, the condition for the binary image of a linear quaternary code to be linear, which requires the check of (3.14) for all codewords of the code, was given. We now show that a check over all codewords is not necessary. Through Lemmas 3.4.1, 3.4.2 and 3.4.3; we arrive at Proposition 3.4.4 and Corollary 3.4.5 that reduce the number of codewords to be checked considerably, which in turn diminishes the computational load. Finally, in Proposition 3.4.6, we find some binary codes for which the necessity of such a check is completely eliminated.

Let $\mathcal{C}$ be a linear quaternary code of length n with generator matrix (2.1)

$$G = \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix},$$

and $C = \phi(\mathcal{C})$ be the binary image of $\mathcal{C}$.

Let $\{x_1,...,x_{k_1}, x_{k_1+1},...,x_{k_1+k_2}\}$ be the set of row vectors of the generator matrix (2.1). By Corollary 3.3.9, $C = \phi(\mathcal{C})$ is linear if and only if $2\alpha(x_i) * \alpha(x_j) \in \mathcal{C}$ for all for all i, j satisfying $1 \le i \le j \le m$.

It should be noticed that it is not necessary to check all the row pairs in G. Because the last k_2 rows that contain solely zeros and two's will produce the all zero vector after applying the "α" map (which sends each $\mathbb{Z}_4$ element to the least significant bit in its binary representation). Hence,

Lemma 3.4.1. Let $\mathcal{C}$ be a linear quaternary code of length n with generator matrix (2.1) and let $\{x_1,...,x_{k_1}, x_{k_1+1},...,x_{k_1+k_2}\}$ be the set of row vectors of the generator matrix. Then, for all i, j satisfying $k_1 < i, j \le k_2$,

$$2\alpha(x_i) * \alpha(x_j) = 2(\mathbf{0} * \mathbf{0}) = \mathbf{0} \in \mathcal{C}, \tag{3.22}$$

and for all i, t satisfying $1 \le i \le k_1$ and $k_1 < t \le k_2$,

$$2\alpha(x_i) * \alpha(x_t) = 2(\alpha(x_t) * \mathbf{0}) = \mathbf{0} \in \mathcal{C}. \tag{3.23}$$

Therefore, in order to check the linearity of the binary image of any linear quaternary code, the last k_2 rows in G need not to be considered.

Lemma 3.4.2. Let $\mathcal{C}$ be a linear quaternary code of length n with generator matrix (2.1) and let $\{x_1,...,x_{k_1}, x_{k_1+1},...,x_{k_1+k_2}\}$ be the set of row vectors of the generator matrix. Then, for all i satisfying $1 \le i \le k_1$, $2\alpha(x_i) * \alpha(x_i) \in \mathcal{C}$.

Proof. Let $\{x_1,...,x_{k_1}, x_{k_1+1},...,x_{k_1+k_2}\}$ be the set of row vectors of the generator matrix (2.1). Since the *i*th row of the generator matrix is of the form

$$x_i = (0_1,...,0_{i-1}, 1_i, 0_{i+1},..., 0_{k_1}, x_{k_1+1},..., x_{k_2}, x_{k_2+1}..., x_n) \in \mathcal{C},$$

we have

$$\begin{aligned} &2\alpha(x_i) * \alpha(x_i) = 2\alpha(x_i * x_i) \\ &= 2(0_1,...,0_{i-1},1_i,0_{i+1},...,0_{k_1},(x_{k_1+1}x_{k_1+1}),...,(x_{k_2}x_{k_2}),\alpha(x_{k_2+1}x_{k_2+1}),...,\alpha(x_nx_n)) \end{aligned} \quad (3.24)$$

since for all $x_i \in \mathbb{Z}_4$, $2\alpha(x_ix_i) = 2x_i$, because $\alpha(0.0) = 0$, $\alpha(1.1) = 1$, $\alpha(2.2) = 0$, $\alpha(3.3) = 1$, equation (3.24) is equal to

$$\begin{aligned} 2\alpha(x_i) * \alpha(x_i) &= 2\alpha(x_i * x_i) \\ &= (0_1,...,0_{i-1}, 2_i, 0_{i+1},...,0_{k_1}, 2x_{k_1+1},...,2x_{k_2}, 2x_{k_2+1},...,2x_n) \\ &= 2x_i \in \mathcal{C}. \end{aligned}$$

Finally, the only pairs we should check for the linearity of the binary image of any linear quaternary code are the pairs (x_i, x_j), $i \neq j$, chosen from the first k_1 rows of *G*.

Lemma 3.4.3. Let $\mathcal{C}$ be a linear quaternary code of length n with generator matrix (2.1) and let $\{x_1,...,x_{k_1}, x_{k_1+1},...,x_{k_1+k_2}\}$ be the set of row vectors of the generator matrix. Then, for all *i*, *j* satisfying $1 \leq i < j \leq k_1$, $2\alpha(x_i) * \alpha(x_j)$ is of the form $(0_1,...,0_{k_1}, 2v_{k_1+1},...,2v_n)$, where $v_{k_1+1},...,v_n \in \mathbb{Z}_4$, i.e., contains only zeros and twos.

Proof. Let $\{x_1,...,x_{k_1}, x_{k_1+1},...,x_{k_1+k_2}\}$ be the set of row vectors of the generator matrix. The rows x_i and x_j of the generator matrix are of the form

$$x_i = (0_1,...,0_{i-1}, 1_i, 0_{i+1},...,0_{k_1}, x_{k_1+1},..., x_{k_2}, x_{k_2+1}..., x_n)$$

and

$$x_j = (0_1,...,0_{j-1}, 1_j, 0_{j+1},...,0_{k_1}, y_{k_1+1},..., y_{k_2}, y_{k_2+1}..., y_n).$$

Hence, we have

$$\begin{aligned} 2\alpha(x_i) * \alpha(x_j) &= 2\alpha(x_i * x_j) \\ &= 2\alpha(0_1,...,0_i,...,0_j,...,0_{k_1}, (x_{k_1+1}y_{k_1+1}),..., (x_{k_2}y_{k_2}), (x_{k_2+1}y_{k_2+1}), ..., (x_ny_n)) \\ &= (0_1,...,0_{k_1}, 2\alpha(x_{k_1+1}y_{k_1+1}),..., 2\alpha(x_{k_2}y_{k_2}), 2\alpha(x_{k_2+1}y_{k_2+1}), ..., 2\alpha(x_ny_n)). \end{aligned}$$

Proposition 3.4.4. The binary image of any linear quaternary code with generator matrix $G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$, where $G_1 = \begin{pmatrix} I_{k_1} & A & B \end{pmatrix}$ and $G_2 = \begin{pmatrix} 0 & 2I_{k_2} & 2D \end{pmatrix}$, is linear if and only if for all row pairs $x_i, x_j \in G_1$ such that $i \neq j$, $2\alpha(x_i) * \alpha(x_j) = 2\alpha(x_i * x_j)$ is in the row space of G_2.

Proof. Follows from the proofs of the previous three lemmas. Since the vectors to be tested contain all zeros and two's, the condition $2\alpha(x_i) * \alpha(x_j) \in \mathcal{C}$ of Corollary 3.3.9 needs not to be tested for the row space of G_1.

Corollary 3.4.5. The binary image of any linear quaternary code with generator matrix $G = G_1$, where $G_1 = \begin{pmatrix} I_{k_1} & B \end{pmatrix}$, i.e., $k_2 = 0$, is linear if and only if for all row pairs $x_i, x_j \in G_1 = G$ such that $i \neq j$, $2\alpha(x_i) * \alpha(x_j) = 2\alpha(x_i * x_j) = \mathbf{0}$.

Now, by using these properties we can generalize the following facts.

Proposition 3.4.6. Let $\mathcal{C}$ be a linear quaternary code of length n with generator matrix (2.1). The binary image, $\phi(\mathcal{C})$, is linear if one of the three conditions given below is satisfied:

$$\textbf{(i)}\ k_1 = 0, \qquad \textbf{(ii)}\ k_1 = 1, \qquad \textbf{(iii)}\ n = k_1 + k_2.$$

Proof.

(i) For $k_1 = 0$, the last k_2 rows of G considered in Lemma 3.4.1 become all rows of G, hence they all pass the linearity test.

(ii) If $k_1 = 1$, the generator matrix is of the form

$$G_3 = \begin{pmatrix} 1 & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}, \tag{3.25}$$

where A and B are $1 \times k_2$ matrices. Hence, we have to check only the first row for linearity and this single row passes the linearity test by Lemma 3.4.2.

(iii) If $n = k_1 + k_2$, the generator matrix is of the form

$$\begin{pmatrix} I_{k_1} & A \\ 0 & 2I_{k_2} \end{pmatrix}. \tag{3.26}$$

From Lemma 3.4.1 and 3.4.2, we need to check only the pairs (x_i, x_j), $i \neq j$, chosen from the first k_1 rows of (3.26), and by Lemma 3.4.3 we know that $2\alpha(\mathrm{x}_i) * \alpha(\mathrm{x}_j)$ is of the form $(0_1, ..., 0_{k_1}, 2v_{k_1+1}, ..., 2v_{k_1+k_2})$, where $v_{k_1+1}, ..., v_{k_1+k_2} \in \mathbb{Z}_4$. Since, the last k_2 rows of (3.26) generate all codewords of the form $(0_1, ..., 0_{k_1}, 2v_{k_1+1}, ..., 2v_{k_1+k_2})$, the binary image, $\phi(\mathcal{C})$, of the linear quaternary code $\mathcal{C}$ is linear.

Hence, the binary images of linear quaternary codes with $k_1 = 0$ or 1 or $n = k_1 + k_2$ are linear codes.

Example 3.4.7. Consider the linear quaternary code $\mathcal{K}_4$ introduced in Example 2.1.7 with generator matrix (2.3)

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

Since $k_1 = 1$, the binary image of $\mathcal{K}_4$ can be said to be linear without checking any row pairs of the generator matrix (2.6).

As a final word on the reduction in computational load, the linearity test in Proposition 3.4.4 is applied to only $(k_1(k_1 - 1))/2$ distinct pairs $\mathrm{x}_i, \mathrm{x}_j \in G_1$; and if the search in the row space of G_2 is performed employing the parity check matrix of G_2, it requires computation of $n - k_2$ inner products per pair, since the parity check matrix of G_2 has $n - k_2$ rows. Each inner product takes at most *n* multiplications in $\mathbb{Z}_4$, so the upper bound of required computations is $(n - k_2)n$ $\mathbb{Z}_4$-multiplications per pair $\mathrm{x}_i, \mathrm{x}_j \in G_1$; therefore, $(n - k_2)n(k_1(k_1 - 1))/2$ $\mathbb{Z}_4$-multiplications in total.

It is interesting to note that using the parity check matrix of *G* instead would result in a number of $\mathbb{Z}_4$-multiplications, with an upper bound $(n-k_1)n(k_1(k_1-1))/2$. To make use of the advantage of searching in the row space of G_2 instead of *G*, it may be wiser to use the generator matrices rather than the parity check matrices.

Nevertheless, the ratio of the computational load of the test described in Proposition 3.4.4 over the load of the test in Corollary 3.3.9, seems to be proportional to $(k_1(k_1-1))/2$ divided by the number of all possible row pairs of *G*, which is equal to $(k_1+k_2)+[(k_1+k_2)(k_1+k_2-1)/2]$, independent of the chosen test method.

3.5 ANALYSIS OF SOME BINARY CODES

In 1993, Calderbank, Sloane, Solé discovered the existence of quaternary versions of Reed-Muller and Hamming codes [8] and then Hammons, Kumar, Calderbank, Sloane, Solé proved that binary first- and second-order Reed-Muller codes are $\mathbb{Z}_4$-linear, but the extended Hamming codes of length $n \geq 32$ are not [26].

In this section, it is first explained which of the Reed-Muller and Hamming codes are $\mathbb{Z}_4$-linear. We then analyze all linear quaternary codes of length 4 to answer the question whether or not there is a nonlinear and $\mathbb{Z}_4$-linear binary code better than the extended Hamming code of length 8.

Firstly, we recall the binary Reed-Muller codes.

Let $(v_1, ..., v_{m-1})$ range over $\mathbb{Z}_2^{m-1}$. The binary Reed-Muller code $RM(r, m-1)$ is generated by the vectors corresponding to monomials in the Boolean functions v_i of degree $\leq r$ [39], i.e., the generator matrix of $RM(r, m-1)$ is of the form

$$G(r, m-1) = \begin{pmatrix} 1^{2^{m-1}} \\ v_1 \\ \vdots \\ v_{m-1} \\ v_1 * v_2 \\ \vdots \\ v_{m-2} * v_{m-1} \\ \vdots \\ v_1 * v_2 * \cdots * v_r \\ \vdots \\ v_{m-r+1} * v_{m-r+2} * \cdots * v_{m-1} \end{pmatrix} \quad \text{where} \begin{cases} v_1 = (01)^{2^{m-2}}, \\ v_2 = (0011)^{2^{m-3}}, \\ \vdots \\ v_{m-1} = 0^{2^{m-2}} 1^{2^{m-2}}, \end{cases}$$

and $*$ denotes the component-wise multiplication.

Definition 3.5.1. [8] Let m be an integer and $0 \leq r \leq m$. The linear quaternary code of length 2^{m-1} generated by $RM(r-1, m-1)$ and $2RM(r, m-1)$ over $\mathbb{Z}_4$ is the quaternary version of Reed-Muller code and denoted by $ZRM(r, m-1)$. The matrix

$$\begin{pmatrix} G(r-1, m-1) \\ 2G(r, m-1) \end{pmatrix}$$

generates the linear quaternary code $ZRM(r, m-1)$.

Example 3.5.2. [52] The linear quaternary code $ZRM(2, 3)$ of length $2^{4-1} = 8$ is generated by

$$\begin{pmatrix} G(1,\ 3) \\ 2G(2,\ 3) \end{pmatrix}$$

and, hence, has generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 1^{2^3} \\ \mathrm{v}_1 \\ \mathrm{v}_2 \\ \mathrm{v}_3 \\ 2\mathrm{v}_1 * \mathrm{v}_2 \\ 2\mathrm{v}_1 * \mathrm{v}_3 \\ 2\mathrm{v}_2 * \mathrm{v}_3 \end{pmatrix}. \qquad (3.27)$$

Theorem 3.5.3. [26] The *r*th order binary Reed-Muller code $RM(r,\ m)$ of length $n = 2^m$, $m \geq 1$, is $\mathbb{Z}_4$-linear for $r = 0,\ 1,\ 2,\ m-1$ and *m*. More precisely, it is the binary image of the linear quaternary code $ZRM(r,\ m-1)$ of length 2^{m-1} for $r = 0,\ 1,\ 2,\ m-1$ and *m*.

For example, let $(\mathrm{v}_1,\ ...,\ \mathrm{v}_{m-1})$ range over $\mathbb{Z}_2^m$. $RM(2,\ m)$ is the binary image of the linear quaternary code $ZRM(2,\ m-1)$ generated by the vectors corresponding to $1,\ \mathrm{v}_1,\ ...,\ \mathrm{v}_{m-1},\ 2\mathrm{v}_1\mathrm{v}_2,\ 2\mathrm{v}_1\mathrm{v}_3,\ ...,\ 2\mathrm{v}_{m-2}\mathrm{v}_{m-1}$. If we take $m = 4$, the $(16,\ 11,\ 4)$ code $RM(2,\ 4)$ is the binary image of the linear quaternary code $ZRM(2,\ 3)$ with generator matrix (3.27) in Example 3.5.2.

It is known that the $(m-2)$nd-order Reed-Muller code of length 2^m, $RM(m-2,\ m)$, is the extended binary Hamming code H_{2^m} when $m \geq 3$. In the following theorem it is proved that when $m \geq 5$, $(m-2)$nd-order Reed-Muller code is not $\mathbb{Z}_4$-linear.

Theorem 3.5.4. [26] The extended binary Hamming code $RM(m-2,\ m) = H_{2^m}$ of length 2^m is not $\mathbb{Z}_4$-linear for $m \geq 5$.

Theorem 3.5.5. [28] The Reed-Muller code $RM(r,\ m)$ is not $\mathbb{Z}_4$-linear when $m > 5$ and $2 < r < m-2$.

Theorem 3.5.3 and 3.5.4 are proved in [26], and Theorem 3.5.5 is in [28].

It is worthwhile to remark that a binary code can be $\mathbb{Z}_4$-linear, even though its dual is not. For example, $RM(1,\ m)$ and $RM(m-2,\ m)$ are dual to each other and $RM(1,\ m)$ is $\mathbb{Z}_4$-linear, but $RM(m-2,\ m)$ is not.

By Theorem 3.5.3, $H_{2^4} = RM(4-2,\ 4) = RM(2,\ 4)$ is $\mathbb{Z}_4$-linear. The linear quaternary code $\mathcal{K}_4$ introduced in Example 2.1.7 with generator matrix (2.3) is of type $4^1 2^2$, $k_1 = 1$ and $k_2 = 2$, and consists of 16 codewords with minimal distance 4. Therefore, its binary image is equivalent to the extended Hamming code of length 8.

In order to answer the question whether or not there is a nonlinear and $\mathbb{Z}_4$-linear binary code better than the extended Hamming code of length 8; we check all linear quaternary codes of length 4 whose binary images are nonlinear. The comparison can be done on the basis of number of codewords and the minimal distance. Since the blocklength is fixed, higher number of codewords indicates higher information rate and greater minimal distance yields more error correction capability.

By Proposition 3.4.1, binary images of linear quaternary codes of type $4^{k_1} 2^{k_2}$ are linear when $k_1 = 0,\ 1$ or $n = k_1 + k_2$. We have exhaustively searched all the remaining linear quaternary codes of type 4^2, $4^2 2^1$, 4^3, whose binary images are nonlinear.

There are 112 distinct nonlinear codes, which are the binary images of the linear quaternary codes of type 4^2. These nonlinear binary codes have the same number of codewords, i.e., 16 codewords, with the extended Hamming code; but their minimum distance can be at most 3, whereas that of the extended Hamming code is 4. The codes with the following generator matrices

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 3 & 2 \\ 0 & 1 & 3 & 1 \end{pmatrix}$$

are the examples of the linear quaternary codes of type 4^2, whose binary images are nonlinear with minimal distance 3. Notice that in the above matrices, the constraints of $k_1 = 2$ and $k_2 = 0$ reduce the general form of the generator matrix given by (2.1) as

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix} \quad \text{to} \quad \begin{pmatrix} I_{k_1} & B \end{pmatrix}.$$

As for the linear quaternary codes of type $4^2 2^1$, the binary images result in 40 distinct nonlinear codes. These nonlinear binary codes have 32 codewords, more than that of the extended Hamming code; but their minimum distance can be at most 2. The codes with the following generator matrices

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

are the examples of the linear quaternary codes of type $4^2 2^1$, whose binary images are nonlinear codes with minimal distance 2. Again, as a result of the constraints

$k_1 = 2$ and $k_2 = 1$, the general form of the generator matrix is reduced to $\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2 & 2D \end{pmatrix}$.

Finally, there are 32 distinct nonlinear codes that are the binary images of the linear quaternary codes of type 4^3. These codes have 64 codewords but their minimum distance can be at most 2. The codes with the following generator matrices

$$\begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

are the examples of the linear quaternary codes of type 4^3, whose binary images are nonlinear codes with minimal distance 2. Notice that in the above matrices, the constraint of $k_1 = 3$ and $k_2 = 0$ reduces the general form of the generator matrix given by (2.1) to $\begin{pmatrix} I_{k_1} & B \end{pmatrix}$.

Hence, for the blocklength of 8 we understand that none of the nonlinear binary images of linear quaternary codes can approach to the minimum distance of the extended Hamming code, which is equal to 4.

CHAPTER 4

CYCLIC CODES

For cyclic codes of length *n* over an alphabet of size *q*, it is customary to work in a Galois field $GF(q^m)$, an extension of degree *m* of a ground field $GF(q)$. The ground field $GF(q)$ is identified with the alphabet, and the extension field is chosen so that it contains an *n*th root of unity [39].

A similar approach is used for cyclic codes of length *n* over the ring $\mathbb{Z}_4$, only now one constructs a Galois ring $GR(4^m)$, that is an extension of $\mathbb{Z}_4$ of degree *m* containing an *n*th root of unity [26].

Galois rings have been studied by many authors, MacDonald [38], Liebler and Mena [37], Shankar [44], Solé [48], Yamada [54], Boztaş, Hammons and Kumar [7], Zariski and Samuel [55] and Wan [51]. In this chapter, it is firstly given the basic facts about the polynomials of the ring $\mathbb{Z}_4[X]$; and then the properties of Galois ring $GR(4^m)$ and the automorphisms of $GR(4^m)$, generalized Frobenius and trace maps. The proofs can be found in the above references. After these preparations, it is defined the quaternary cyclic codes and their generator matrices.

4.1 BASIC IRREDUCIBLE POLYNOMIALS AND HENSEL LIFT

A cyclic code over $\mathbb{Z}_4$ can be studied entirely in terms of the polynomials of the ring $\mathbb{Z}_4[X]$. However, just as it is productive to study codes over the field $GF(q)$ in the

larger algebraic field $GF(q^m)$; it is more fruitful to study codes over $\mathbb{Z}_4$ in a larger algebraic system called a *Galois ring*. We need some preparation on irreducible polynomials in $\mathbb{Z}_4[X]$ to define Galois rings.

Definition 4.1.1. [54] Let $f(X)$ be a monic polynomial of degree $m \geq 1$ in $\mathbb{Z}_4[X]$. If $f_2(X) \equiv f(X) \pmod 2$ is irreducible (or primitive) over $\mathbb{Z}_2$, then $f(X)$ is called a *basic irreducible* (or *basic primitive*) *polynomial* of degree *m* in $\mathbb{Z}_4[X]$.

Proposition 4.1.2. [54] Let $f_2(X)$ be a monic irreducible (or primitive) polynomial of degree *m* in $\mathbb{Z}_2[X]$. Then there exists a unique monic basic irreducible (or monic basic primitive) polynomial $f(X) \in \mathbb{Z}_4[X]$ of degree *m* such that $f(X)$ divides $X^n - 1$ in $\mathbb{Z}_4[X]$, where $n = 2^m - 1$ and that $f_2(X) \equiv f(X) \pmod 2$.

The monic basic irreducible (or monic basic primitive) polynomial $f(X)$ over $\mathbb{Z}_4$ in Proposition 4.1.2 satisfies not only the condition that $f_2(X)$ is a monic irreducible (or primitive) over $\mathbb{Z}_2$, but also the condition that $f(X) | (X^{2^m-1} - 1)$ in $\mathbb{Z}_4[X]$. This polynomial $f(X)$ in $\mathbb{Z}_4[X]$ is called the *Hensel lift* of $f_2(X)$ and by Proposition 4.1.2, it exists and is unique.

The Hensel lift $f(X)$ in $\mathbb{Z}_4[X]$ of a monic irreducible (or primitive) polynomial $f_2(X)$ in $\mathbb{Z}_2[X]$ can be calculated using *Graeffe's method* [48], [51], [53] for finding a polynomial whose roots are squares of the roots of $f_2(X)$, as the following proposition shows.

Proposition 4.1.3. [40] Let $f_2(X)$ be a monic irreducible (or primitive) polynomial over $\mathbb{Z}_2$. Write $f_2(X) = e(X) - d(X)$, where $e(X)$ contains only even power terms

and $d(X)$ only odd power terms. Then $e(X)^2 - d(X)^2$, computed in $\mathbb{Z}_4[X]$, is a polynomial having only even power terms and of degree $2\deg f_2(X)$. Let $f(X^2) = \pm(e(X)^2 - d(X)^2)$, where + or − sign is taken, if $\deg e(X) > \deg d(X)$ or $\deg d(X) > \deg e(X)$ respectively; then $f(X)$ is the Hensel lift of $f_2(X)$.

This method is the inverse of the operation $f_2(X) \equiv f(X) \pmod 2$ and lifts an irreducible (or primitive) polynomial in $\mathbb{Z}_2[X]$ to a basic irreducible (or basic primitive) polynomial in $\mathbb{Z}_4[X]$. It is a special case of a result known as Hensel's Lemma.

The following two examples can be useful to understand this method.

Example 4.1.4. [52] For $m=3$ and $n=7$; $f_2(X) = X^3 + X + 1$ is a monic primitive polynomial over $\mathbb{Z}_2$. Then $e(X)=1$ and $d(X)=-X^3 - X$. So, we have

$$f(X^2) = -e(X)^2 + d(X)^2 = X^6 + 2X^4 + X^2 - 1.$$

Hence, $f(X) = X^3 + 2X^2 + X - 1$ is the Hensel lift of $X^3 + X + 1$ and so it is a monic basic primitive polynomial of degree $m=3$ in $\mathbb{Z}_4[X]$.

Example 4.1.5. For $m=4$ and $n=15$, $f_2(X) = X^4 + X^3 + 1$ is a monic primitive polynomial over $\mathbb{Z}_2$. Then $e(X) = X^4 + 1$ and $d(X) = -X^3$. So, we have

$$f(X^2) = e(X)^2 - d(X)^2 = X^8 - X^6 + 2X^4 + 1.$$

Hence, $f(X) = X^4 - X^3 + 2X^2 + 1$ is the Hensel lift of $X^4 + X^3 + 1$ and so it is a monic basic primitive polynomial of degree $m=4$ in $\mathbb{Z}_4[X]$.

Moreover, it is clear that $f_2(X) \equiv f(X) \pmod 2$ for Examples 4.1.4 and 4.1.5.

All primitive basic irreducible polynomials of degree ≤ 10 over $\mathbb{Z}_4$, which are Hensel lifts of binary primitive polynomials are given in [7].

4.2 GALOIS RINGS

The theory of Galois rings is an important tool to study cyclic codes over $\mathbb{Z}_4$, which was developed by W. Krull [34]. In this section, we specifically consider the Galois ring $GR(4^m)$ with 4^m elements.

Definition 4.2.1. [40] Let $h(X)$ be a basic primitive polynomial of degree *m* over $\mathbb{Z}_4$. $\mathbb{Z}_4[X]/(h(X))$, the ring of polynomials modulo $h(X)$, is called the *Galois ring* with 4^m elements and is denoted by $GR(4^m)$.

In general, the elements of Galois ring $GR(4^m)$ may be represented in a variety of ways. One is the definition by $\sum_i a_i X^i$, $a_i \in \mathbb{Z}_4$, as a polynomial in X of degree at most $m-1$.

Although some properties of Galois fields are carried over the Galois rings, other properties do not. In particular, the Galois ring $GR(4^m)$ cannot be generated by a single element. However, there will always be an element with order $2^m - 1$ which is a zero of a basic primitive polynomial over $\mathbb{Z}_4$. It may be called a primitive element though it does not generate the Galois ring in the manner that a primitive element of a Galois field does [2].

The second kind of representation is the 2-adic representation.

Theorem 4.2.2. [10]

(i) In the Galois ring $GR(4^m)$, there exists a nonzero element ξ of order $2^m - 1$, which is a root of a basic primitive polynomial $h(X)$ of degree m over $\mathbb{Z}_4$. Moreover, $h(X)$ is the unique polynomial of degree $\leq m$ over $\mathbb{Z}_4$ having ξ as a root.

(ii) Let $\mathcal{T} = \{0, 1, \xi, ..., \xi^{2^m-2}\}$, then any element $c \in GR(4^m)$ can be written uniquely as

$$c = a + 2b, \tag{4.1}$$

where $a, b \in \mathcal{T}$.

The representation (4.1), called 2-adic representation, accounts for all 4^m elements of the ring $GR(4^m)$. With the convention that $\xi^{-\infty} = 0$, every element of $GR(4^m)$ can be written in the 2-adic representation as $\xi^i + 2\xi^j$.

The following proposition tells how to calculate the representation $\xi^i + 2\xi^j$ from any other representation of $c \in GR(4^m)$.

Proposition 4.2.3. [10] Let $c = a + 2b$ denote the 2-adic representation of $c \in GR(4^m)$. Then $a = c^{2^m}$.

For adding elements of $\mathcal{T}$ by using 2-adic representation the following formulas are useful which are found in [35].

Corollary 4.2.4. [35] Let $c_1,\ c_2 \in \mathcal{T}$, and express

$$c_1 + c_2 = a + 2b, \quad a, b \in \mathcal{T}\ , \tag{4.2}$$

then

$$a = c_1 + c_2 + 2(c_1 c_2)^{1/2}\ , \tag{4.3}$$

$$b = (c_1 c_2)^{1/2}\ , \tag{4.4}$$

where $(c_1 c_2)^{1/2}$ denotes the unique element in $\mathcal{T}$ such that $((c_1 c_2)^{1/2})^2 = c_1 c_2$.

The formulas will now be extended to the generalization, in which there are *k* terms in the sum.

Corollary 4.2.5. [35] Let $c_1,\ c_2, ..., c_k \in \mathcal{T}$, and express

$$\sum_{i=1}^{k} c_i = a + 2b, \quad a, b \in \mathcal{T}\ , \tag{4.5}$$

then

$$a = \sum_{i=1}^{k} c_i + 2 \sum_{1 \le i < j \le k} (c_i c_j)^{1/2}\ , \tag{4.6}$$

$$b = \sum_{1 \le i < j \le k} (c_i c_j)^{1/2}\ . \tag{4.7}$$

Moreover, each element $c \in GR(4^m)$ has a unique 'additive' representation

$$c = \sum_{i=0}^{m-1} a_i \xi^i,\ a_i \in \mathbb{Z}_4\ ,$$

where ξ is a root of a basic primitive polynomial $h(X)$ of degree m over $\mathbb{Z}_4$, of order $2^m - 1$.

The following example gives the additive representation of every element of $GR(4^m)$ by using (4.1).

Example 4.2.6. [26] Let $m = 3$ and $h(X) = X^3 + 2X^2 + X - 1$ be a basic primitive polynomial from Example 4.1.4, and $\xi = X$ is a root of $h(X)$ of order $2^3 - 1 = 7$. The additive representations for the elements $\mathcal{T}$ and $2\mathcal{T}$ are

element	b_0	b_1	b_2	$2b_0$	$2b_1$	$2b_2$
0	0	0	0	0	0	0
ξ^0	1	0	0	2	0	0
ξ^1	0	1	0	0	2	0
ξ^2	0	0	1	0	0	2
ξ^3	1	3	2	2	2	0
ξ^4	2	3	3	0	2	2
ξ^5	3	3	1	2	2	2
ξ^6	1	2	1	2	0	2

Therefore

$$\mathcal{T} = \{0,\ 1,\ \xi,\ \xi^2,\ 2\xi^2 + 3\xi + 1,\ 3\xi^2 + 3\xi + 2,\ \xi^2 + 3\xi + 3,\ \xi^2 + 2\xi + 1\}.$$

$$2\mathcal{T} = \{0,\ 2,\ 2\xi,\ 2\xi^2,\ 2\xi + 2,\ 2\xi^2 + 2\xi,\ 2\xi^2 + 2\xi + 2,\ 2\xi^2 + 2\}.$$

By using the elements of $\mathcal{T}$ and $2\mathcal{T}$, the additive representation of every elements of $GR(4^m)$ is obtained.

Another difference between $GR(4^m)$ and a Galois field is that $GR(4^m)$ contains zero divisors. The following proposition gives the properties of the elements of $GR(4^m)$.

Proposition 4.2.7. [52] Express any element $c \in GR(4^m)$ in 2-adic form $c = a + 2b$, where $a, b \in \mathcal{T}$. Then

(i) all the elements c with $a \neq 0$ are invertible and form a multiplicative group of order $(2^m - 1)2^m$, which is a direct product $\langle \xi \rangle \times \mathcal{E}$ where $\langle \xi \rangle$ is a cyclic group of order $(2^m - 1)$ generated by ξ and $\mathcal{E} = \{1 + 2b \mid b \in \mathcal{T}\}$ has the structure of an abelian group of type 2^m and is isomorphic to the additive group of $\mathbb{F}_{2^m}$.

(ii) all the nonzero elements c with $a = 0$ are zero divisors and with the zero element they form the ideal (2) of $GR(4^m)$.

(iii) The order of c is a divisor of $(2^m - 1)$ if and only if $a \neq 0$ and $b = 0$.

(iv) Any element $\eta \in GR(4^m)$ of order $2^m - 1$ is of the form ξ^i, where $\gcd(i, 2^m - 1) = 1$ and is a root of a basic primitive polynomial of degree m over $\mathbb{Z}_4$ and $\mathcal{T} = \{0, 1, \eta, \eta^2, ..., \eta^{2^m - 2}\}$.

4.3 FROBENIUS AND TRACE MAPS

In $GR(4^m)$, the square of the ring element $c = a + 2b$ is always $c^2 = a^2$, independent of b because $4 = 0$ in this ring. In this sense, squaring is a lossy operation. A useful variant of the squaring function is the *Frobenius function.*

Recall that the Frobenius map of the Galois field $\mathbb{F}_{2^m}$ is defined by

$$\begin{aligned} f_2 \ : \ \mathbb{F}_{2^m} &\to \mathbb{F}_{2^m} \\ a &\to a^2 \end{aligned}$$

Definition 4.3.1. [26] The *generalized Frobenius map* f is the ring automorphism and defined by

$$\begin{aligned} f \ : \ GR(4^m) &\to GR(4^m) \\ c = a + 2b &\to c^f = a^2 + 2b^2. \end{aligned}$$

f generates the Galois group of $GR(4^m)$ and f^m is the identity map.

Recall that the trace map Tr from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined by

$$Tr(a) = a + a^{f_2} + a^{f_2^2} + \cdots + a^{f_2^{m-1}} \quad \text{for all } a \in \mathbb{F}_{2^m}.$$

Definition 4.3.2. [26] Define the *generalized trace map T* from $GR(4^m)$ to $\mathbb{Z}_4$ by

$$T(c) = c + c^f + c^{f^2} + \cdots + c^{f^{m-1}} \quad \text{for all } c \in GR(4^m).$$

The following properties of these maps are easily verified:

Proposition 4.3.3. [26] Let f be the generalized Frobenius map of $GR(4^m)$ and T be the generalized trace map from $GR(4^m)$ to $\mathbb{Z}_4$. Then

(i) $T(c + c') = T(c) + T(c')$ for all $c, c' \in GR(4^m)$,

(ii) $T(ac) = aT(c)$ for all $a \in \mathbb{Z}_4$ and $c \in GR(4^m)$,

(iii) The following commutativity relationship satisfied, i.e., $— \circ f = f_2 \circ —$,

(iv) The following commutativity relationship satisfied, i.e., $— \circ T = Tr \circ —$.

In particular, since *Tr* is not identically zero, it follows that the generalized trace T is nontrivial. In fact, T is an onto map from $GR(4^m)$ to $\mathbb{Z}_4$. The set of elements of $GR(4^m)$ invariant under f is identical with $\mathbb{Z}_4$.

We must be careful when working with Galois ring $GR(4^m)$. Since it is not a unique factorization domain, a polynomial in $GR(4^m)$ may have more than one factorization into irreducible polynomials in $GR(4^m)[X]$. For this reason, the following proposition is useful.

Proposition 4.3.5. [52] Let $h(X)$ be a basic irreducible polynomial of degree *m* over $\mathbb{Z}_4$ and η be a root of $h(X)$ in $GR(4^m)$ then $h(X)$ has the following unique factorization into linear factors in $GR(4^m)[X]$:

$$h(X) = (X - \eta)(X - \eta^f) \cdots (X - \eta^{f^{m-1}}). \tag{4.8}$$

In particular, if $h(X)$ is a basic primitive polynomial of degree *m*, $h(X) \mid (X^{2^m - 1} - 1)$ in $\mathbb{Z}_4[X]$, and ξ is a root of $h(X)$ in $GR(4^m)$, then $\xi, \xi^2, \xi^{2^2}, ..., \xi^{2^{m-1}}$ are all the distinct roots of $h(X)$ in $GR(4^m)$ and $h(X)$ has the following unique factorization:

$$h(X) = (X - \xi)(X - \xi^2) \cdots (X - \xi^{2^{m-1}}). \tag{4.9}$$

Example 4.3.6. By Example 4.1.4, $h(X)=X^3+2X^2+X-1$ is a basic primitive polynomial of degree $m=3$, and ξ is a root of $h(X)$. Then all distinct roots of $h(X)$ are ξ, ξ^2, $\xi^4=3\xi^2+3\xi+2$. Hence, the unique factorization of $h(X)$ is

$$h(X)=(X-\xi)(X-\xi^2)(X-3\xi^2-3\xi-2).$$

4.4 QUATERNARY CYCLIC CODES

As in the binary case, a cyclic code over the ring $\mathbb{Z}_4$ is a linear code over $\mathbb{Z}_4$ with the property that the cyclic shift of any codeword is another codeword.

Definition 4.4.1. [40] A linear quaternary code $\mathcal{C}$ of length *n* is called a *quaternary cyclic code* (or *cyclic code over* $\mathbb{Z}_4$) if

$$(c_0,\ c_1,...,c_{n-1})\in\mathcal{C}\ \Rightarrow\ (c_{n-1},\ c_0,\ c_1,...,c_{n-2})\in\mathcal{C}. \tag{4.10}$$

As in the binary case, when studying quaternary cyclic codes of length *n* in general, it is convenient to represent codewords of the quaternary cyclic codes by polynomials modulo X^n-1. The codeword $\mathrm{c}=(c_0,\ c_1,...,c_{n-1})\in\mathcal{C}$ is identified with the polynomial $\mathrm{c}(X)=c_0+c_1X+\cdots+c_{n-1}X^{n-1}$ in the ring $\mathcal{R}=\mathbb{Z}_4[X]/(X^n-1)$, which will also be called a codeword of $\mathcal{C}$. The property (4.10) is equivalent to

$$c_0+c_1X+\cdots+c_{n-1}X^{n-1}\in\mathcal{C}\ \Rightarrow\ X(c_0+c_1X+\cdots+c_{n-1}X^{n-1})\in\mathcal{C}. \tag{4.11}$$

As in the binary case there is a relationship between the ring $\mathcal{R}=\mathbb{Z}_4[X]/(X^n-1)$ and quaternary cyclic code.

Proposition 4.4.2. [20] A nonempty set of $\mathbb{Z}_4^n$ is a quaternary cyclic code if and only if after identified its elements with the polynomials it is an ideal in the ring $\mathcal{R} = \mathbb{Z}_4[X]/(X^n - 1)$.

One way to form a quaternary cyclic code is as the set of polynomial multiples of a polynomial. Let $g(X)$ be a monic polynomial over $\mathbb{Z}_4$ dividing $X^n - 1$ and let $\mathcal{C} = (g(X))$ consist of all multiples of $g(X)$ of degree at most $n-1$. Then $\mathcal{C}$ is called the quaternary cyclic code with *generator polynomial* $g(X)$. Hence every codeword has the form $c(X) = a(X)g(X)$, where $a(X) \in \mathbb{Z}_4[X]$.

Let $h(X) = (X^n - 1)/g(X)$, then $h(X)g(X) \equiv 0 \pmod{X^n - 1}$. Let $\deg g(X) = m$, then $\deg h(X) = n - m$. Write

$$g(X) = g_0 + g_1 X + \cdots + g_m X^m$$

and

$$h(X) = h_0 + h_1 X + \cdots + h_{n-m} X^{n-m},$$

then $g_m = h_{n-m} = 1$ and $g_0 = h_0 = \pm 1$. Since $h(X)g(X) \equiv 0 \pmod{X^n - 1}$, $X^{n-m}g(X)$ can be expressed as a linear combination of $g(X), Xg(X), \ldots, X^{n-m-1}g(X)$. Therefore the codewords $g(X), Xg(X), \ldots, X^{n-m-1}g(X)$ of $\mathcal{C}$ form a basis of the code $\mathcal{C}$. That is, the $(n-m) \times n$ matrix

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_m & & & \\ & g_0 & g_1 & \cdots & g_m & & \\ & & \ddots & & & \ddots & \\ & & & g_0 & g_1 & \cdots & g_m \end{pmatrix} \tag{4.12}$$

is a generator matrix of $\mathcal{C}$ and $\mathcal{C}$ is of type 4^{n-m}.

Clearly, a word $c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$ is a codeword of $\mathcal{C}$ if and only if $c(X)h(X) = \mathbf{0}$. In particular, $h(X)$ is called the *check polynomial* of $\mathcal{C}$. Define an $m \times n$ matrix H by

$$H = \begin{pmatrix} h_{n-m} & \cdots & h_1 & h_0 & & \\ & h_{n-m} & \cdots & h_1 & h_0 & \\ & & \ddots & & & \ddots \\ & & & h_{n-m} & \cdots & h_1 \quad h_0 \end{pmatrix} \tag{4.13}$$

It is easy to verify that the codewords $g(X)$, $Xg(X)$,..., $X^{n-m-1}g(X)$ of $\mathcal{C}$ are orthogonal to every row of H. Clearly, the system of linear equations

$$H^T(X_0, X_1, ..., X_{n-1}) = \mathbf{0}$$

has 4^m solutions. Therefore, a word is orthogonal to each row of H if and only if it is a codeword of $\mathcal{C}$. Thus H is the *parity check matrix* of the quaternary cyclic code $\mathcal{C}$.

Define the reciprocal polynomial $\overline{h}(X)$ to $h(X)$ to be

$$\overline{h}(X) = h_{n-m} + \cdots + h_1 X^{n-m-1} + h_0 X^{n-m}.$$

Then the quaternary cyclic code with $\overline{h}(X)$ as its generator polynomial is the *dual code* of $\mathcal{C}$.

Proposition 4.4.3. [20] Let $g(X)$ be a monic polynomial over $\mathbb{Z}_4$ dividing $X^n - 1$ and $h(X) = (X^n - 1)/g(X)$. Let $\mathcal{C} = (g(X))$ be the quaternary cyclic code, whose generator polynomial is $g(X)$. Then $\mathcal{C}^{\perp}$ is a quaternary cyclic code whose generator polynomial $\overline{h}(X)$ is the reciprocal polynomial to $h(X)$.

4.5 GENERATOR POLYNOMIALS

The subject of cyclic codes over $\mathbb{Z}_4$ has many similarities to the subject of cyclic codes over a field, but there are also considerable differences. Various properties that hold for cyclic codes over a field do not hold for cyclic codes over a ring. One difference is that there is no unique factorization theorem in the ring of polynomials over a ring. Many polynomials over $\mathbb{Z}_4$ have multiple distinct factorizations. It should also be noticed that the number of distinct roots of a polynomial of degree *m* over $\mathbb{Z}_4$ in an extension ring of $\mathbb{Z}_4$ may be greater than *m*. Therefore we must be careful when working with the residue class ring $\mathcal{R} = \mathbb{Z}_4[X]/(X^n - 1)$.

Not every polynomial over $\mathbb{Z}_4$ is suitable as a generator polynomial for a cyclic code over $\mathbb{Z}_4$. For the code to be a proper quaternary cyclic code, one must respect the algebraic structure of $\mathbb{Z}_4[X]$. Just as one can form cyclic codes of length *n* over $GF(2)$ by using the irreducible factors of $X^n - 1$ over $GF(2)$ and their products, one can also form quaternary cyclic codes of length *n* over $\mathbb{Z}_4$ by using the basic irreducible factors of $X^n - 1$ and their products. However, the possibilities are more extensive. Let $g(X)$ be any basic irreducible factor of $X^n - 1$ over $\mathbb{Z}_4$. Then $g(X)$ can be used as the generator polynomial of a cyclic code over $\mathbb{Z}_4$ of length *n*. Moreover, $2\,g(X)$ can also be used as the generator polynomial of a different

quaternary cyclic code of length *n*. Besides these, there are other possibilities. The following proposition generalizes these possibilities.

Proposition 4.5.1. [42] Let n be an odd positive integer, $X^n-1=f_1(X)f_2(X)\cdots f_r(X)$ be the unique factorization of X^n-1 into basic irreducible polynomials, and $\hat{f}_i(X)$ be the product of all $f_j(X)$ except $f_i(X)$. Then any ideal of the ring $\mathcal{R}=\mathbb{Z}_4[X]/(X^n-1)$ is a sum $\hat{f}_i(X)$ and $2\hat{f}_i(X)$.

By Proposition 4.4.2, quaternary cyclic codes of length n are precisely the ideals in the residue class ring $\mathcal{R}=\mathbb{Z}_4[X]/(X^n-1)$. Hence, we have

Corollary 4.5.2. [42] The number of quaternary cyclic codes of odd length *n* is 3^r, where *r* is the number of basic irreducible polynomial factors in X^n-1.

Proposition 4.5.3. [42] Let $2\nmid n$ and I be an ideal of $\mathcal{R}$. Then these are the unique monic polynomials $f(X)$, $g(X)$ and $h(X)$ over $\mathbb{Z}_4$ such that $I=(f(X)h(X),\ 2f(X)g(X))$, where $f(X)g(X)h(X)=X^n-1$ and $I=4^{\deg g(X)}2^{\deg h(X)}$.

The proof of Proposition 4.5.3 can be found in [42].

Corollary 4.5.4. [42] Let $\mathcal{C}$ be a quaternary cyclic code of odd length *n* and assume that $\mathcal{C}=(f(X)h(X),\ 2f(X)g(X))$, where $f(X)$, $g(X)$, $h(X)$ are monic polynomials over $\mathbb{Z}_4$ such that $f(X)g(X)h(X)=X^n-1$. Then $\mathcal{C}^{\perp}$ is also a quaternary cyclic code, $\mathcal{C}^{\perp}=(\overline{g}(X)\overline{h}(X),\ 2\overline{g}(X)\overline{f}(X))$, where $\overline{f}(X)$, $\overline{g}(X)$, $\overline{h}(X)$ are reciprocal polynomials to $f(X)$, $g(X)$, $h(X)$, respectively, and $\left|\mathcal{C}^{\perp}\right|=4^{\deg f(X)}2^{\deg h(X)}$.

CHAPTER 5

$\mathbb{Z}_4$-LINEARITY OF SOME BINARY NONLINEAR CODES

Around 1970, several nonlinear binary codes have been constructed. Although these nonlinear binary codes are not so easy to describe, to encode and decode as the linear codes, they contain more codewords than any known linear codes. The well-known of these are the codes constructed by Nordstrom-Robinson, Kerdock, Preparata, Goethals and Delsarte-Goethals ([41], [32], [43], [21], [22], [19] and [27]). Since these codes have great error correcting capability, several researchers have investigated them and showed that they can be constructed as binary images under the Gray map of linear codes over $\mathbb{Z}_4$ and are actually extended cyclic codes over $\mathbb{Z}_4$.

In this chapter, we study these well-known nonlinear binary codes and the quaternary version of the linear binary Reed-Muller code. Firstly, the quaternary Kerdock code, its generator matrix and trace description are given. It is then shown that the Kerdock codes are extended cyclic codes over $\mathbb{Z}_4$ and are simply $\mathbb{Z}_4$-analogues of the first-order Reed-Muller codes. By using these results, the weight distribution of the Kerdock codes is given. Secondly, the quaternary Preparata codes are defined and the binary images of the quaternary duals of the Kerdock codes are shown to be the binary images of the quaternary Preparata codes, which are called the *Preparata-like* codes. The third section defines a family of quaternary Reed-Muller codes, which generalizes the quaternary Kerdock and Preparata-like or "*Preparata*" codes. In the final section, the quaternary Goethals codes, i.e., another generalization of "Preparata" codes are reviewed. It is shown that the nonlinear binary Delsarte-Goethals codes are also extended cyclic codes over $\mathbb{Z}_4$, and their $\mathbb{Z}_4$-duals have

essentially the same properties as the Goethals codes and the "Goethals-Delsarte" codes.

Most of the definitions and propositions of this chapter are taken from [26] and [52] by inserting some explanations whenever needed.

5.1 KERDOCK CODES

In 1972, Kerdock introduced the nonlinear binary Kerdock codes K_{m+1} where m is odd integer ≥ 3 [32]. These codes contain at least twice as many codewords as the best linear binary code with the same length and minimum distance. In 1989, Nechaev studied the Kerdock codes [40] by using Galois rings and trace descriptions of some $\mathbb{Z}_4$-sequences and proved that this code has the cyclic form.

Now, we firstly give the quaternary construction of Kerdock codes.

Let $h(X)$ be a basic primitive polynomial of degree $m \geq 2$ over $\mathbb{Z}_4$ such that $h(X) \mid (X^{2^m-1}-1)$. From Proposition 4.1.2, the existence of the polynomial $h(X)$ is guaranteed and it is the Hensel lift of the binary primitive polynomial $h_2(X) \equiv h(X) \pmod 2$ of degree *m*.

Let $g(X)$ be the reciprocal polynomial to the polynomial $(X^{2^m-1}-1)/((X-1)h(X))$.

Definition 5.1.1 [25] The *quaternary Kerdock code* $\mathcal{K}(m)$ is obtained from the quaternary cyclic code $\mathcal{K}(m)^-$ of length 2^m-1 with generator polynomial $g(X)$ by adjoining a zero-sum check symbol to each codeword of $\mathcal{K}(m)^-$ at position ∞, which is situated in front of the position 0.

Note that the polynomial $(X-1)h(X)$ is the parity check polynomial of $\mathcal{K}(m)^{-}$. There are two equivalent generator matrices for $\mathcal{K}(m)$. The first one can be given as follows.

Proposition 5.1.2. [25] Let ξ be a root of $h(X)$ over $\mathbb{Z}_4$. Then the $(m+1)\times 2^m$ matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{pmatrix} \tag{5.1}$$

is a generator matrix of $\mathcal{K}(m)$, where the entries ξ^j for $0 \le j \le n-1$, in the second row are to be replaced by the corresponding m tuples $(b_{1j}, b_{2j},...,b_{mj})^t$ obtained from $\xi^j = b_{1j} + b_{2j}\xi + \cdots + b_{mj}\xi^{m-1}$.

By Proposition 5.1.2 and Theorem 4.2.2 (ii) different basic primitive polynomials of the same degree m over $\mathbb{Z}_4$ define permutation-equivalent quaternary Kerdock codes.

The second form of the generator matrix is given in the following proposition.

Proposition 5.1.3. [25] Let $g(X) = \sum_{j=0}^{\delta} g_j X^j$, where $\deg g(X) = \delta = 2^m - m - 2$ and $g_j \in \mathbb{Z}_4$ and $g_\infty = -(g_0 + g_1 + \cdots + g_\infty)$. Then the $(m+1)\times 2^m$ matrix

$$\begin{pmatrix} g_\infty & g_0 & g_1 & \cdots & g_\delta & 0 & \cdots & 0 \\ g_\infty & 0 & g_0 & \cdots & g_{\delta-1} & g_\delta & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ g_\infty & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_\delta \end{pmatrix} \tag{5.2}$$

is also a generator matrix of $\mathcal{K}(m)$.

The following example gives the two forms of the generator matrix of $\mathcal{K}(3)$.

Example 5.1.4. [26] Let $h(X)=X^3+2X^2+X-1$ be the basic primitive polynomial of degree 3, then $g(X)=X^3+2X^2+X-1=h(X)$. So $\mathcal{K}(3)$ is self dual. By Proposition 5.1.2 and 5.1.3, the generator matrices of $\mathcal{K}(3)$ are

$$\begin{pmatrix} 1 & 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 1 & 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 1 & 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{pmatrix}.$$

It is easy to prove that the above two matrices and the matrix (2.6) generate the same code. Therefore $\mathcal{K}(3)$ is the octacode $\mathcal{O}_8$.

From the definitions of $\mathcal{K}(m)$ and $\mathcal{K}(m)^-$ the following two facts are clear.

Corollary 5.1.5. [25] The codes $\mathcal{K}(m)^-$ and $\mathcal{K}(m)$ are linear quaternary codes of type 4^{m+1}.

Corollary 5.1.6. [25] The linear binary code $K^{(1)}$, associated with $\mathcal{K}(m)$,with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \eta & \eta^2 & \cdots & \eta^{n-1} \end{pmatrix} \tag{5.3}$$

where $\eta^i = \xi^i \pmod 2,\ i=1,...,n-1$, is equivalent to $RM(1,\ m)$.

In [26], Hammons *et al*. verified the codewords of quaternary Kerdock code by using its trace description over $GR(4^m)$.

Proposition 5.1.7. [26] The codes $\mathcal{K}(m)^-$ and $\mathcal{K}(m)$ have the following trace description over the ring $GR(4^m)=\mathbb{Z}_4[\xi]$, where ξ is a root of the basic primitive polynomial $h(X)$ in $GR(4^m)$.

(i) $\mathcal{K}(m)^- = \{\varepsilon\mathbf{1}+\mathrm{v}^{(\lambda)} \mid \varepsilon\in\mathbb{Z}_4,\ \lambda\in GR(4^m)\}$ where

$$\mathrm{v}^{(\lambda)} = (T(\lambda\xi^0),\ T(\lambda\xi^1),\ T(\lambda\xi^2),...,T(\lambda\xi^{n-1})). \tag{5.4}$$

Thus $\mathrm{c}=(c_0,\ c_1,...,c_{n-1})$ is a codeword in $\mathcal{K}(m)^-$ if and only if $c_t = T(\lambda\xi^t)+\varepsilon$, $t\in\{0,\ 1,...n-1\}$.

(ii) $\mathcal{K}(m) = \{\varepsilon\mathbf{1}+\mathrm{u}^{(\lambda)} \mid \varepsilon\in\mathbb{Z}_4,\ \lambda\in GR(4^m)\}$ where

$$\mathrm{u}^{(\lambda)} = (T(\lambda\xi^\infty),\ T(\lambda\xi^0),\ T(\lambda\xi^1),...,T(\lambda\xi^{n-1})) \tag{5.5}$$

with the convention that $\xi^\infty = 0$.

Thus $\mathrm{c}=(c_\infty,\ c_0,\ c_1,...,c_{n-1})$ is a codeword in $\mathcal{K}(m)$ if and only if $c_t = T(\lambda\xi^t)+\varepsilon$, $t\in\{\infty,\ 0,\ 1,...,n-1\}$.

From Proposition 5.1.7, the following proposition can be verified.

Proposition 5.1.8. [26] Let $\mathrm{c}=(c_\infty,\ c_0,\ c_1,...,c_{n-1})\in\mathcal{K}_m$ and $m\geq 2$ be an integer. Then c_t has 2-adic expansion

$$c_t = a_t + 2b_t, \qquad t \in \{\infty, 0, 1, \ldots, n-1\} \tag{5.6}$$

given by

$$a_t = Tr(\pi\theta^t) + A, \tag{5.7}$$

$$b_t = Tr(\eta\theta^t) + \sum_{0 \le j \le k \le m-1} (\pi\theta^t)^{2^j + 2^k} + B, \tag{5.8}$$

where the elements $\theta = \xi \pmod 2$, π, $\eta \in GF(2^m)$ and $A, B \in \mathbb{Z}_2$ are arbitrary and the convention that $\theta^\infty = 0$. When m is odd, let

$$Q(x) = \sum_{j=1}^{(m-1)/2} Tr(x^{1+2^j}) \quad \text{for all } x \in GF(2^m), \tag{5.9}$$

Then b_t can be written as

$$b_t = Tr(\eta\theta^t) + Q((\pi\theta^t)) + B. \tag{5.10}$$

Now, we can give the properties of the binary image of the quaternary Kerdock code. We denote the binary image of the quaternary Kerdock code $\mathcal{K}(m)$ by $K(m)$, i.e., $K(m) = \phi(\mathcal{K}(m))$, where *m* is an integer ≥ 2.

Theorem 5.1.9. [26] Let *m* be an integer ≥ 2. Then $K(m)$ is a nonlinear binary code of length 2^{m+1} and with 4^{m+1} codewords. This code is distance invariant and all its codewords are of even weight.

Proposition 5.1.10. [26] Let m be an integer ≥ 2. The codewords c for which $\lambda \in 2GR(4^m)$ in the trace description (5.5) and for which $\pi = 0$ in the 2-adic representation (5.6)-(5.8) form a linear subcode of $\mathcal{K}(m)$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 2 & 2\xi & 2\xi^2 & \cdots & 2\xi^{n-1} \end{pmatrix}, \tag{5.11}$$

whose binary image is the first-order Reed-Muller code $RM(1, m+1)$ contained in the Kerdock code $K(m)$.

Our new aim is to give the relation between the Kerdock code $K(m)$ and the nonlinear binary Kerdock code K_{m+1}. Recall that, for $m \geq 3$ odd, the nonlinear binary Kerdock code K_{m+1} of length 2^{m+1} is the union of $2^m - 1$ cosets of $RM(1, m+1)$ in $RM(2, m+1)$.

Now, we have

Theorem 5.1.11. [26] Let m be an odd integer ≥ 3. Then $K(m) = K_{m+1}$.

The weight distribution of the Kerdock code K_{m+1}, where m is an odd integer ≥ 3 was computed by Kerdock in [32]. Moreover, in [26] Hammons *et al*. determined the weight distribution of any Kerdock code by using the quaternary description.

Theorem 5.1.12. [26] Let m be odd and ≥ 3. The nonlinear binary Kerdock code $K_{m+1} = K(m)$ of length 2^{m+1} with 4^{m+1} codewords, minimal distance $2^m - 2^{(m-1)/2}$, has the weight distribution given in Table 5.1.

Table 5. 1 Weight distribution of $K(m)$ (m odd)

Weight(i)	No. of codewords(A_i)
0	1
$2^m - 2^{(m-1)/2}$	$2^{m+1}(2^m - 1)$
2^m	$2^{m+2} - 2$
$2^m + 2^{(m-1)/2}$	$2^{m+1}(2^m - 1)$
2^{m+1}	1

When m is even, $m \geq 2$, a similar argument shows that $K(m) = \phi(\mathcal{K}(m))$ is a nonlinear code of length 2^{m+1}, with 4^{m+1} codewords, minimal distance $2^m - 2^{m/2}$, and the weight distribution given in Table 5.2.

Table 5. 2 Weight distribution of $K(m)$ (m even)

Weight(i)	No. of codewords(A_i)
0	1
$2^m - 2^{m/2}$	$2^m(2^m - 1)$
2^m	$2^{m+1}(2^m + 1) - 2$
$2^m + 2^{m/2}$	$2^m(2^m - 1)$
2^{m+1}	1

Note that this code is not as good as a double-error-correcting BCH code. The double error correcting BCH code has parameters $n = 2^m - 1$ and $k \geq n - 2m$ and the code rate $\geq \frac{2^m - 1 - 2m}{2^m - 1}$ which is greater than the code rate $\frac{m+1}{2^{m+1}}$ of the $K(m)$, where m is even.

5.2 PREPARATA CODES

In 1968, the nonlinear binary Preparata codes were introduced by Preparata in [43] and their weight distribution were obtained by Semankov and Zinovév in 1969, which can be found in [39]. After the Kerdock codes were introduced by Kerdock in 1972, it was proved that the weight enumerator of the Preparata code is the MacWilliams transform of the weight enumerator of the Kerdock code. Although, the Preparata code is not a $\mathbb{Z}_4$-linear code; in 1993, Calderbank, Hammons, Kumar, Sloane and Solé proved that a code with the same parameters, which is called Preparata-like code, is $\mathbb{Z}_4$-linear. Furthermore, they explained the mystery in coding theory by showing that these well known codes are the binary images of the linear codes over the ring $\mathbb{Z}_4$ under the Gray map that are dual to one another. Moreover, at length 16, Kerdock and Preparata codes coincide and give the unique code with the interesting property, the Nordstrom-Robinson code [41]. This code has strictly larger minimum distance than any linear code with the same length and size. In 1993, Forney, Sloane and Trott showed that the Nordstrom-Robinson code is the binary image of the octacode, the linear quaternary code presented in Example 2.1.9 [20].

As in the previous section, we firstly give the quaternary construction of Preparata codes following [26]. Let $h(X)$ be a basic primitive polynomial of degree $m \geq 2$, dividing $(X^{2^m-1}-1)$ in $\mathbb{Z}_4[X]$, ξ be a root of $h(X)$ over $\mathbb{Z}_4$, and $g(X)$ be the reciprocal polynomial to the polynomial $(X^{2^m-1}-1)/((X-1)h(X))$.

Definition 5.2.1 [26] Let $\mathcal{P}(m)^-$ be the quaternary cyclic code of length $n = 2^m - 1$ with generator polynomial $h(X)$. The linear quaternary code $\mathcal{P}(m)$ is obtained from the quaternary cyclic code $\mathcal{P}(m)^-$ by adding a zero-sum check symbol to each codeword of $\mathcal{P}(m)^-$ is called the *quaternary Preparata code*.

Since $\mathcal{P}(m)^{-}$ has parity check polynomial $g(X)$, we have

Proposition 5.2.2. [26] Let ξ be a root of $h(X)$ over $\mathbb{Z}_4$. Then $\mathcal{P}(m)^{-}$ has parity check matrix

$$\begin{pmatrix} 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{pmatrix} \tag{5.12}$$

$\mathcal{P}(m)$ is the dual code of $\mathcal{K}(m)$ and hence the matrices (5.1) and (5.2) are the parity check matrices of $\mathcal{P}(m)$.

From Definition 5.2.1 and Proposition 5.2.2, we have

Corollary 5.2.3. [26] Both the codes $\mathcal{P}(m)^{-}$ and $\mathcal{P}(m)$ are linear quaternary codes of type 4^{2^m-m-1}.

Corollary 5.2.4. [26] The linear binary code $P^{(1)}$ associated with $\mathcal{P}(m)$, with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \eta & \eta^2 & \cdots & \eta^{n-1} \end{pmatrix} \tag{5.13}$$

where $\eta^i = \xi^i \pmod 2$, $i = 1, \ldots, n-1$, is equivalent to $RM(m-2, m)$.

Proposition 5.2.5. [26] Let m be an integer ≥ 2, then all codewords of $\mathcal{P}(m)$ are of even Lee weight. Moreover, when m is even and ≥ 2, $\mathcal{P}(m)$ has minimum Lee distance 4 and when m is odd and ≥ 3, $\mathcal{P}(m)$ has minimum Lee distance 6.

Now, we can give the properties of the binary image of the quaternary Preparata code. We denote the binary image of the quaternary Preparata code $\mathcal{P}(m)$ by $P(m)$, i.e., $P(m) = \phi(\mathcal{P}(m))$.

Theorem 5.2.6. [26] Let *m* be an integer ≥ 2. Then $P(m)$ is a binary code of length 2^{m+1}, with $2^{2^{m+1}-2m-2}$ codewords and minimal distance 6. This code is distance invariant, all its codewords are of even weight and it is the formal dual of $K(m)$. Moreover, its weight enumerator is the MacWilliams transform of the weight enumerator of the Kerdock code of the same length, i.e.,

$$W_{P(m)}(X,Y) = \frac{1}{4^{m+1}} W_{K(m)}(X+Y,\ X-Y). \tag{5.14}$$

By Proposition 5.2.5, when $m \geq 3$, $P(m)$ is nonlinear. When *m* is even and ≥ 2, $P(m)$ has minimum Lee distance 4 and when *m* is odd and ≥ 3, $P(m)$ has minimum Lee distance 6.

Since $P(m)$ is not the same code as the original version of the Preparata code , it is called the Preparata-like code or the “Preparata” code, when *m* is an odd integer ≥ 3. In [26], the quotation mark is used to distinguish it from the Preparata’s original code P_{m+1}. Although $P(m)$ and P_{m+1} have the same code length, the same number of codewords, the same minimum distance, and the same weight enumerator, there is an essential difference between them.

To give the relation between the “Preparata” code $P(m)$ and the original Preparata code P_{m+1}, we will review Preparata’s original work in 1968.

Let m be an odd integer ≥ 3 and $n = 2^m - 1$ and (x,y) be the vectors in $\mathbb{F}_2^{2^{m+1}}$, where $x, y \in \mathbb{F}_2^{2^m}$, and for $\alpha \in \mathbb{F}_{2^m}$, x_α and y_α denote the components at the αth positions in x and y, respectively.

Definition 5.2.7. [43] The *Preparata code* P_{m+1} of length 2^{m+1} consists of all codewords (x, y) where $x, y \in \mathbb{F}_2^{2^m}$, satisfying

(i) Both $w_H(x)$ and $w_H(y)$ are even.

(ii) $\sum_{x_\alpha=1} \alpha = \sum_{y_\alpha=1} \alpha$.

(iii) $\sum_{x_\alpha=1} \alpha^3 + \left(\sum_{x_\alpha=1} \alpha\right)^3 = \sum_{y_\alpha=1} \alpha^3$.

The code obtained by deleting the first coordinates is denoted by $P(m)^-$.

Proposition 5.2.8. [26] The binary code P_{m+1} is distance invariant, has minimum distance 6, and $2^{2^{m+1}-2m-2}$ codewords.

Corollary 5.2.9. [26] The code $P(m)^-$ is a binary code of length $2^m - 1$ and has minimum distance 5.

Since the weight enumerator of the Preparata code P_{m+1} is the MacWilliams transform of the weight enumerator of the Kerdock code K_{m+1} and by Theorem 5.2.6, $P(m)$ is the formal dual of $K(m) = K_{m+1}$, we have the following proposition.

Proposition 5.2.10. [26] Let m be an odd integer ≥ 3. The Preparata code P_{m+1} and the "Preparata" code $P(m)$ have the same length, the same number of codewords, the same minimum distance, and the same weight enumerator.

The following two propositions give one essential difference between $P(m)$ and P_{m+1} as asserted in [26].

Proposition 5.2.11. [26] For odd $m \geq 5$, $P(m)$ is contained in a nonlinear code with the same weight distribution as the extended binary Hamming code of the same length, and the linear code spanned by the codewords of $P(m)$ has minimum weight 2.

Proposition 5.2.12. [26] The Preparata code P_{m+1} of length 2^{m+1} is a subcode of the extended binary Hamming code of the same length.

Moreover, there is an interesting relationship between Kerdock, Preparata and "Preparata" codes. When $m = 3$, these three codes coincide and give the Nordstrom-Robinson code. This is the unique binary code of length 16, minimal distance 6, containing 256 codewords. In this case $\mathcal{K}(3)$ is the "octacode", whose generator matrix is given in Example 5.1.4. The octacode may also be characterized as the unique self-dual linear quaternary code of length 8 and minimal Lee weight 6 as in Example 2.1.9. Thus we have the following proposition.

Proposition 5.2.13. [20] The Nordstrom-Robinson code is the binary image of the octacode under the Gray map.

Theorem 5.2.14. [26] When $m = 3$, the "Preparata" code $P(m)$ coincides with Preparata's original code P_{m+1}.

Finally, both $P(m)$ and P_{m+1} have the same length and minimum distance as the $[2^{m+1}, 2^{m+1}-2m-3, 6]$ extended BCH code, but contain twice as many codewords. Moreover, in [39], it is shown that P_{m+1} has the greatest possible number of codewords for this minimum distance [39].

5.3 QUATERNARY REED-MULLER CODES

In Section 3.5, it is defined a quaternary code $ZRM(r, m-1)$ whose image under the Gray map ϕ is the binary Reed-Muller code $RM(r, m)$ for $r \in \{0, 1, 2, m-1, m\}$. From the previous sections, we see that the quaternary codes $\mathcal{K}(m)$ and $\mathcal{P}(m)$ can be regarded as the $\mathbb{Z}_4$-analogs of the binary first-order Reed-Muller code $RM(1, m)$ and the $(m-2)$th-order Reed-Muller code $RM(m-2, m)$, respectively. In [26], Hammons *et al.* define another quaternary Reed-Muller code $QRM(r, m)$, whose image under the map α is $RM(r, m)$ for all r, $0 \le r \le m$, and which includes the codes $\mathcal{K}(m)$ and $\mathcal{P}(m)$ as special cases.

Definition 5.3.1. [52] Let m be an integer ≥ 2, $n = 2^m - 1$, and r be an integer such that $0 \le r \le m$. Let $h(X)$ be a basic primitive polynomial of degree m dividing $X^n - 1$ and ξ be one of its root of order $2^m - 1$. Consider the $(m+1) \times 2^m$ matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \end{pmatrix} \tag{5.15}$$

Denote the ith row of the matrix (5.15) by v_i. The *quaternary rth-order Reed-Muller code* $QRM(r, m)$ is the code generated by all 2^m-tuples of the form

$$\mathrm{v}_{i_1}\mathrm{v}_{i_2}\cdots\mathrm{v}_{i_s}, \qquad 1\le i_1<i_2<\cdots<i_s\le m, \quad 0\le s\le r.$$

Now, we recall the cyclotomic coset to give an equivalent definition of the quaternary Reed-Muller code $QRM(r, m)$, $0\le r\le m$.

Let m be a fixed positive integer and r, s be integers such that $0\le r, s\le 2^m-2$. It is defined r and s to be equivalent, if there is a non-negative integer i such that $2^i r\equiv s \pmod{2^m-1}$. So, this defines an equivalence relation in the set of integers $\{0, 1, 2, \ldots, 2^m-2\}$. The equivalence classes are called the *cyclotomic cosets* mod 2^m-1. A number in a cyclotomic coset is called *a representative of the cyclotomic coset*.

Definition 5.3.2. [26] Let m be an integer ≥ 2. Then $QRM(0, m)$ is the quaternary repetition code $\{\varepsilon\mathbf{1}|\varepsilon\in\square_4\}$ of length 2^m, and for $1\le r\le m$ $QRM(r, m)$ is generated by $QRM(0, m)$ together with all vectors of the form

$$(T(\lambda_j\xi^{\infty}),\ T(\lambda_j\xi^{0}),\ T(\lambda_j\xi^{j}),\ T(\lambda_j\xi^{2j}),\ldots,\ T(\lambda_j\xi^{(n-1)j})) \tag{5.16}$$

where j ranges over all representatives of cyclotomic cosets mod 2^m-1 for which $wt(j)\le r$, and λ_j runs through $GR(4^m)$. Moreover, $QRM(r, m)$ is of type 4^k, where

$$k=1+\binom{m}{1}+\binom{m}{2}+\cdots+\binom{m}{r}.$$

The following proposition is clear from Definition 5.3.1 and Proposition 5.1.2.

Proposition 5.3.3. [26] Let m be an integer ≥ 2. Then

$$QRM(1,\ m)\ =\ \mathcal{K}(m).$$

$$QRM(m-2,\ m)\ =\ \mathcal{P}(m)$$

$$\alpha(QRM(r,\ m))\ =\ RM(r,\ m).$$

$$QRM(r,\ m)^{\perp}\ =\ QRM(m-r-1,\ m).$$

5.4 QUATERNARY GOETHALS, DELSARTE-GOETHALS AND GOETHALS-DELSARTE CODES

In the previous section, we have seen one generalization of constructions of $\mathcal{K}(m)$ and $\mathcal{P}(m)$. As another generalization of quaternary Preparata codes, Hammons *et al.* introduced the quaternary Goethals codes in [26] as follows.

Definition 5.4.1. [26] Let m be an odd integer ≥ 3 and ξ be an element of order $n=2^m-1$ in the Galois ring $GR(4^m)$. *The quaternary Goethals code* $\mathcal{G}(m)$ of length 2^m is defined to be the linear quaternary code with parity check matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \\ 0 & 2 & 2\xi^3 & 2\xi^6 & \cdots & 2\xi^{3(n-1)} \end{pmatrix}. \tag{5.17}$$

If the first components of the codewords of $\mathcal{G}(m)$ are deleted, the obtained code, $\mathcal{G}(m)^-$, has parity check matrix

$$\begin{pmatrix} 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \\ 2 & 2\xi^3 & 2\xi^6 & \cdots & 2\xi^{3(n-1)} \end{pmatrix} \tag{5.18}$$

and is a quaternary cyclic code of length $2^m - 1$.

Proposition 5.4.2. [26] Let m be an odd integer ≥ 3. The quaternary Goethals code $\mathcal{G}(m)$ of length 2^m is of type $4^{2^m-2m-1}2^m$ and of minimal Lee distance 8. Moreover, the quaternary cyclic code $\mathcal{G}(m)^-$ of length $2^m - 1$ is of type $4^{2^m-2m-1}2^m$ and of minimal Lee distance 7.

The original Goethals code G_{m+1}, where m is any odd integer ≥ 5, was introduced by Goethals [21], [22]. It is a distance invariant nonlinear binary code of length 2^{m+1}, contains $2^{2^{m+1}-3m-2}$ codewords and has minimum distance 8. The binary image, $\phi(\mathcal{G}(m))$, of $\mathcal{G}(m)$ is a nonlinear binary code and it has the same length, the same number of codewords, the same minimum distance, and the same weight and distance enumerators as the original Goethals code. Now, let us study the code $\phi(\mathcal{G}(m))$, which is called the "*Goethals*" code.

Proposition 5.4.3. [26] Let m be an odd integer ≥ 3. The "Goethals" code $\phi(\mathcal{G}(m))$ is a binary code of length 2^{m+1}. It is distance invariant, has $2^{2^{m+1}-3m-2}$ codewords and minimal Hamming distance 8. When $m \geq 5$, it is nonlinear, but, for $m = 3$, is linear.

Goethals ([21], [22]) also introduced the formal dual $\phi(\mathcal{G}(m)^\perp)$ of $\phi(\mathcal{G}(m))$, computed the weight distributions of both G_{m+1} and $\phi(\mathcal{G}(m)^\perp)$ and observed that the weight enumerator of G_{m+1} is the MacWilliams transform of that of $\phi(\mathcal{G}(m)^\perp)$. Since the weight enumerator of $\phi(\mathcal{G}(m))$ is the MacWilliams transform of that of $\phi(\mathcal{G}(m)^\perp)$, G_{m+1} and $\phi(\mathcal{G}(m))$ also have the same weight enumerator.

Table 5. 3 Weight distribution of $\phi(\mathcal{G}(m)^{\perp})$, $m=2t+1$

Weight(i)	No. of codewords(A_i)
0 or 2^{2t+2}	1
$2^{2t+1}\pm 2^{t+1}$	$2^{2t}(2^{2t+1}-1)(2^{2t+2}-1)/3$
$2^{2t+1}\pm 2^{t}$	$2^{2t+2}(2^{2t+1}-1)(2^{2t+1}+4)/3$
2^{2t+1}	$2(2^{2t+2}-1)(2^{4t+1}-2^{2t}+1)$

Note that both G_{m+1} and $\phi(\mathcal{G}(m))$ contain four times as many codewords as the extended triple-error correcting BCH code of the same length.

The binary Delsarte-Goethals and Goethals-Delsarte codes were introduced and studied by Delsarte and Goethals in [19] and Hergert in [27] respectively.

Finally, we study the quaternary Delsarte-Goethals and Goethals-Delsarte codes which are the generalization of the quaternary Goethals and its $\mathbb{Z}_4$ duals.

Definition 5.4.4. [26] Let m be an odd integer ≥ 3, $m=2t+1$, $1\leq r\leq t$, and ξ be an element of order $n=2^m-1$ in the Galois ring $GR(4^m)$. The *quaternary Delsarte-Goethals code* $\mathcal{DG}(m,\ \delta)$, where $\delta=(m+1)/2-r$ is the linear quaternary code with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{n-1} \\ 0 & 2 & 2\xi^3 & 2\xi^6 & \cdots & 2\xi^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 2 & 2\xi^{1+2^j} & 2\xi^{2(1+2^j)} & \cdots & 2\xi^{(1+2^j)(n-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 2 & 2\xi^{(1+2^r)} & 2\xi^{2(1+2^r)} & \cdots & 2\xi^{(1+2^r)(n-1)} \end{pmatrix} \tag{5.19}$$

The quaternary Goethals-Delsarte code $\mathcal{GD}(m,\ \delta)$ is the linear quaternary code with the matrix (5.19) as its parity check matrix.

It is clear that, when $r=1$, $\mathcal{GD}(m,\ \delta)$ is the quaternary Goethals code $\mathcal{G}(m)$.

If we denote the binary images of $\mathcal{DG}(m,\ \delta)$ and $\mathcal{GD}(m,\ \delta)$ by $\phi(\mathcal{DG}(m,\ \delta))$ and $\phi(\mathcal{GD}(m,\ \delta))$, respectively, we have

Proposition 5.4.5. [26] Let m be an odd integer ≥ 3, $m=2t+1$, $1\leq r\leq t$, and $\delta=(m+1)/2-r$.

i. The quaternary Delsarte-Goethals code $\mathcal{DG}(m,\ \delta)$ is of length 2^m and has type $4^{m+1}2^{rm}$ and minimal Lee weight $2^m-2^{m-\delta}$. Its binary image $\phi(\mathcal{DG}(m,\ \delta))$ is the Delsarte-Goethals code $DG(m+1,\ \delta)$, which is a binary code of length 2^{m+1}, is distance invariant, and has $2^{2(m+1)+rm}$ codewords and minimal Hamming distance $2^m-2^{m-\delta}$. When $m\geq 5$, $DG(m+1,\ \delta)$ is nonlinear.

ii. The quaternary Goethals- Delsarte code $\mathcal{GD}(m,\ \delta)$ is of length 2^m, and has type $4^{2^m-(r+1)m-1}2^{rm}$ and minimal Lee weight 8. Its binary image $\phi(\mathcal{GD}(m,\ \delta))$ is a binary code of length 2^{m+1}, is distance invariant, and has $2^{2^{m+1}-(r+2)m-2}$ codewords. It has the same weight distribution as the binary Goethals-Delsarte code $GD(m+1,\ \delta)$. When $m\geq 5$, $\phi(\mathcal{GD}(m,\ \delta))$ is nonlinear.

CHAPTER 6

CONCLUSIONS

Historically, linear codes have been the most important codes since they have a clean structure that makes them simpler to discover, to understand, to encode and decode. However, in order to get the largest possible number of codewords with a fixed block size and correction capability, it is necessary to consider the nonlinear codes as well.

Around 1970, several nonlinear binary codes having at least twice as many codewords as any known linear code with the same length and minimal distance have been constructed. Several researchers have studied these codes and shown in early 1990's that the well-known nonlinear binary codes can be constructed as binary images under the Gray map of linear codes over $\mathbb{Z}_4$. This has led to a new direction in coding theory, the study of linear quaternary codes and their binary images.

This thesis is dedicated to the analysis of linear quaternary codes and their binary images, which can be either linear, or nonlinear but $\mathbb{Z}_4$-linear. We have mainly made use of the seminal paper written by Hammons, Kumar, Calderbank, Sloane and Solé [26] and the book by Wan [52], which is an extended form of lecture notes basically depending on [26]. Basic properties of quaternary codes are discussed, relationships between the weight enumerators of algebraic and formal dual codes are investigated by using the MacWilliams equations. Properties of the binary images of the linear quaternary codes and their duals under the Gray map are studied.

Conditions for the binary image of a linear quaternary code to be linear and for a binary code to be $\mathbb{Z}_4$-linear are thoroughly investigated. The first contribution of our thesis involves the simplification of the linearity test for the binary image of a linear

quaternary code, via new lemmas and propositions. Through Lemmas 3.4.1, 3.4.2 and 3.4.3, we arrive at Proposition 3.4.4 that reduces the number of codewords to be checked considerably, which in turn diminishes the computations. For a linear quaternary code $\mathcal{C}$ of type $4^{k_1}2^{k_2}$, containing $2^{2k_1+k_2}$ codewords and having the generator matrix $G=\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}$, where I_{k_1} and I_{k_2} denote the identity matrices, A and D are $\mathbb{Z}_2$-matrices, and B is a $\mathbb{Z}_4$-matrix; the ratio of the computational load of the test described in Proposition 3.4.4 over the computational load of the usual test, is proportional to $(k_1(k_1-1))/2$ divided by the number of all possible row pairs of G, which is equal to $(k_1+k_2)+[(k_1+k_2)(k_1+k_2-1)/2]$. Finally, in Proposition 3.4.6, we find the values of k_1 and k_2 for which the binary image is already linear, so that the necessity of linearity check is eliminated.

After a discussion on the $\mathbb{Z}_4$-linearity of the Reed-Muller and Hamming codes, our second contribution is the analysis of all linear quaternary codes of length 4 to find out whether there is any nonlinear and $\mathbb{Z}_4$-linear binary code better than the extended Hamming code of length 8, rate ½ and minimal distance 4. The answer is negative, since none of the 184 nonlinear and $\mathbb{Z}_4$-linear binary code can achieve a minimal distance of 4.

Hensel lift and Galois ring, which are the important tools for the study of quaternary cyclic codes, are also discussed. Accordingly, the quaternary cyclic versions of nonlinear binary Kerdock and Preparata codes and their binary images are studied in detail. The generalizations of the quaternary Kerdock and Preparata-like codes, the quaternary Reed-Muller codes and the quaternary Goethals codes are explained. Moreover, it is shown that the nonlinear binary Delsarte-Goethals codes are extended cyclic codes over $\mathbb{Z}_4$, and that their $\mathbb{Z}_4$-duals have essentially the same properties as the Goethals codes and the “Goethals-Delsarte” codes.

REFERENCES

[1] R. D. Baker, J. H. van Lint and R. M. Wilson, *On the Preparata and Goethals codes,* IEEE Trans. Inform. Theory **29**, 342–345, 1983.

[2] R. E. Blahut, *Algebraic codes on lines, planes, and curves,* Cambridge Univ. Press, 2008.

[3] I. F. Blake, *Codes over certain rings*, Inform. Cont. **20**, 396–404, 1972.

[4] A. Bonnecaze and I. M. Duursma, *Translates of linear codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **43**, 1218–1230, 1997.

[5] A. Bonnecaze, P. Solé and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory **41**, 366–377, 1995.

[6] S. Boztaş, *Near-optimal 4-phase sequences and optimal binary sequences for CDMA*, Ph.D. dissertation, Univ. Southern Calif., Los Angeles, 1990.

[7] S. Boztaş, A. R. Hammons, Jr., and P. V. Kumar, *4-Phase sequences with near-optimum correlation properties*, IEEE Trans. Inform. Theory **38**, 1101–1113, 1992.

[8] A. R. Calderbank, A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane and P. Solé, *A linear construction for certain Kerdock and Preparata codes*, Bull. Amer. Math. Soc. **29**, 218–222, 1993.

[9] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, $\mathbb{Z}_4$*-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets*, to appear in Proc. London Math. Soc., 1997.

[10] A. R. Calderbank, W. –C. W. Li and B. Poonen, *A 2-adic approach to the analysis of cyclic codes*, IEEE Trans. Inform. Theory **43**, 977–986, 1997.

[11] A. R. Calderbank and G. McGuire, $\mathbb{Z}_4$*-linear codes obtained as projections of Kerdock and Delsatre-Goethals codes,* Linear Algebra Appl. **226–228**, 647–665, 1995.

[12] A. R. Calderbank, G. McGuire, P. V. Kummer and T. Helleseth, *Cyclic codes over* $\mathbb{Z}_4$*, locator polynomials, and Newton's identities*, IEEE Trans. Inform. Theory **42**, 217–226, 1996.

[13] C. Carlet, *A simple description of Kerdock codes*, Lect. Notes Computer Science **388**, 202–208, 1989.

[14] J. H. Conway and N. J. A. Sloane, *Sphere-packings, lattices and groups*, 2nd ed., Springer-Verlag, NY, 1992.

[15] J. H. Conway and N. J. A. Sloane, *Self-dual codes over the integers modulo 4*, J. Comb. Theory, Series A, **62**, 30–45, 1993.

[16] J. H. Conway and N. J. A. Sloane, *Quaternary constructions for the binary single-error correcting codes of Julin, Best, and others*, Designs, Codes and Cryptography **41**, 31–42, 1994.

[17] K. F. Córdoba, *On Reed-Muller and related quaternary codes*, Ph.D. Thesis, Universitat Autónoma de Barcelona, 2005.

[18] P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance,* Inform. Control **23**, 407–438, 1973.

[19] P. Delsarte and J. M. Goethals, *Alternating bilinear forms over* $GF(q)$, J. Combinatorial Theory, Series A **19**, 26–50, 1975.

[20] G. D. Forney, Jr., N. J. A. Sloane and M. D. Trott, *The Nordstrom-Robinson code is the binary image of the octacode*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **14** (AMS), 19-26, 1993.

[21] J. M. Goethals, *Two dual families of nonlinear binary codes*, Electronics Letters **10**, 471–472, 1974.

[22] J. M. Goethals, *Nonlinear codes defined by quadratic forms over* $GF(2)$, Inform. Control **31**, 43–74, 1976.

[23] J. M. Goethals, *The extended Nadler code is unique*, IEEE Trans. Inform. Theory **23**, 132–135, 1977.

[24] R. W. Hamming, *Error detecting and error correcting codes*, Bell Syst. Tech. J. **29**, 147-160, 1950.

[25] A. R. Hammons, Jr. and P. V. Kumar, *On the apparent duality of the Kerdock and Preparata codes*, IEEE International Symposium on Information Theory, San Antonio, Texas, January 17–22, 1993.

[26] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40**, 301–319, 1994.

[27] F. B. Hergert, *On the Delsarte-Goethals codes and their formal duals*, Discrete Math. **83**, 249–263, 1990.

[28] X. –D. Hou, S. Koponen and J. Lahtonen, *On the $\mathbb{Z}_4$-linearity of the Reed-Muller codes*, Abstracts IEEE Inform. Theory Workshop, Longyearbyen, Norway, July 6-12, 11, 1997.

[29] W. M. Kantor, *An exponential number of generalized Kerdock codes*, Inform. Control **53**, 74–80, 1982.

[30] W. M. Kantor, *Spreads, translation planes and Kerdock sets*, SIAM J. Alg. Discr. Math. **3**, 151–165 and 308–318, 1982.

[31] W. M. Kantor, *On the inequivalence of generalized Preparata codes*, IEEE Trans. Inform.Theory **29**, 345–348, 1983.

[32] A. M. Kerdock, *A class of low-rate nonlinear binary codes*, Inform. Control **20**, 182–187, 1972.

[33] M. Klemm, *¨Uber die Identit¨at von MacWilliams für die Gewichtsfunktion von Codes*, Arch. Math. **49**, 400–406, 1987.

[34] W. Krull, *Algebraische theorie der ringe*, Math. Ann. **92**, 183-213, 1924.

[35] P. V. Kumar, T. Helleseth, A. R. Calderbank and A. R. Hammons, Jr., *Large families of quaternary sequences with low correlation*, IEEE Trans. Inform. Theory **42**, 578–592, 1996.

[36] C. Y. Lee, *"Some properties of nonbinary error-correcting codes,"* IRE Trans. Inform. Theory **4**, 77–82, 1958.

[37] R. A. Liebler and R. A. Mena, *Certain distance-regular digraphs and related rings of characteristic 4*, J. Combin. Theory, Series A, **47**, 111–123, 1988.

[38] B. R. MacDonald, *Finite rings with identity*, Marcel Dekker, NY, 1974.

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

[40] A. A. Nechaev, *The Kerdock code in a cyclic form*, Discrete. Mat. **1**, 123–139, 1989. English translation in Discrete Math. Appl. **1**, 365–384, 1991.

[41] A. W. Nordstrom and J. P. Robinson, *An optimum nonlinear code*, Inform. Control **11**, 613–616, 1967.

[42] V. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **42**, 1594-1600, 1996.

[43] F. P. Preparata, *A class of optimum nonlinear double-error correcting codes*, Inform.Control **13**, 378–400, 1968.

[44] P. Shankar, *On BCH codes over arbitrary integer rings*, IEEE Trans. Inform. Theory **25**, 480–483, 1979.

[45] C. E. Shannon, *The Mathematical Theory of Information*, Urbana, IL: University of Illinois Press, 1949 (reprinted in 1998).

[46] N. J. A. Sloane and D. S. Whitehead, *A new family of single-error correcting codes*, IEEE Trans. Inform. Theory **16**, 717–719, 1970.

[47] S. L. Snover, *The uniqueness of the Nordstrom-Robinson and the Golay binary codes*, Ph.D. Dissertation, Michigan State Univ., 1973.

[48] P. Solé, *A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties,* Lect. Notes Computer Science **388**, 193–201, 1989.

[49] P. Solé, *An inversion formula for Krawtchouk polynomials with application to coding theory*, J. Inform. Optimization Sciences **11**, 207–213, 1990.

[50] J. H. van Lint, *Kerdock and Preparata codes*, Cong. Numer. **39**, 25–41, 1983.

[51] Z. –X. Wan, *Introduction to Abstract and Linear Algebra*, Chatwell Bratt, Bromley, UK and Studentlitteratur, Lund, Sweden, 1992**.**

[52] Z. –X. Wan, *Quaternary codes*, World Scientific, 1997.

[53] J. V. Uspensky, *Theory of equations*, McGraw-Hill, NY, 1948.

[54] M. Yamada, *Distance-regular digraphs of girth 4 over an extension ring of* $\mathbb{Z}/4\mathbb{Z}$ *,* Graphs and Combinatorics **6**, 381–394, 1990.

[55] O. Zariski and P. Samuel, *Commutative algebra*, 2 volumes, Van Nostrand, Princeton, NJ, 1960.