N^0 **d'ordre: 12/2022 - D/MT**

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediène

Faculté De Mathématiques

THÈSE DE DOCTORAT EN SCIENCES

Presentée pour l'obtention du **grade** de **DOCTEUR**

En : MATHÉMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par: BENYETTOU AMEL

Sujet

Construction de Codes LCD et Formellement Auto-Duaux

Soutenue publiquement, le 06 /07 / 2022, devant le jury composé de :

M. Hernane Mohand Ouamar	Professeur à l'USTHB	Président
Mme. Batoul Aicha	Professeur à l'USTHB	Directeur de thèse
Mme. Guenda Kenza	Professeur à l'USTHB	Examinateur
M. Boumahdi Rachid	Maitre de conférence /A à l'ESI	Examinateur
M. Laib Ilias	Maitre de conférence /A à ENSTP	Examinateur
Mme. Meguedmi Djohra	Maitre de conférence /A à ENST	Examinateur

PEOPLE's DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF SCIENCE AND TECHNOLOGY HOUARI BOUMEDIENNE
FACULTY OF MATHEMATICS

THESIS

Presented to obtain **DOCTORATE in Science**

In : MATHEMATICS

SPECIALITY : ALGEBRA AND NUMBER THEORY

By : BENYETTOU Amel

Subject

Construction of LCD and Formally Self Dual Codes

Publicly defended, on 06/07/2022, in front of the jury composed of:

Mr. Hernane Mohand Ouamar	Professor at USTHB	President
Mrs. Batoul Aicha	Professor at USTHB	Supervisor
Mrs. Guenda Kenza	Professor at USTHB	Examiner
Mr. Boumahdi Rachid	MCA at ESI	Examiner
Mr. Laib Ilias	MCA at ENSTP	Examiner
Mrs. Meguedmi Djohra	MCA at ENST	Examiner

To the sun of Islam that will never set...To the Prophet Mohamed, may God bless him and grant him peace who enjoined upon us knowledge and learning until the last moment of this life.

Acknowledgements

First and above all, I thank my God "Allah", for reconciling me to the right way which guiding me to this research.

I would like to offer my heartfelt thanks to all those people who have contributed directly or indirectly to my academic career.

At first, I would like to express my sincere gratitude to my supervisor Pr. Batoul Aicha, for her consistent guidance and support in every step throughout this thesis. It was her immense encouragement and endless support that has enabled me to complete my research work in a productive manner. I sincerely thank her for giving me her time so generously.

I am extremely grateful to my doctoral committee members Pr. Harnane Mohand Ouamar and Pr. Guenda Kenza for agreeing to evaluate this work.

My heartfelt thanks to Dr. Boumahdi Rachid, Dr. Laib Ilias and Dr. Meguedmi Djohra who are the external examiners of my thesis jury.

I would like to thank all my teachers who have taught me in various stages of my life.

I send my sincere thanks to all my fellow researchers and friends for giving me hope during the difficult times of my life.

Abstract

In this thesis, we are interested in the study of LCD and formally self dual codes over finite chain rings. Recently, it has been proven that a non free LCD code over finite local Frobenius rings does not exist, which motivated and encouraged us to look for free LCD codes on these rings. We have established necessary and sufficient conditions for which all free cyclic codes defined over finite chain rings are LCD codes and this by using only algebraic properties of positive integers which represent the length of these codes. Further, we have provided necessary and sufficient conditions on the existence of non trivial self dual cyclic codes of arbitrary lengths on finite chain rings. Moreover, several constructions of isodual cyclic codes of length $2^a m$ over finite chain rings are given according to the factorization of the polynomial $x^m - 1$. Although our work has mainly a theoretical motivation, we hope that this study will serve as a basis on which results in information theory can be established.

Key-words : LCD codes, Self dual codes, Isodual codes, Chain rings, Principal ideal rings.

Contents

Notations

Symbol	**Meaning**
$\mathbb{N}$	The set of natural numbers.
$\|A\|$	The cardinality of the set A.
R	A finite chain ring.
$\langle\gamma\rangle$	The maximal ideal of R.
e	The nilpotency index of γ.
$\mathbb{F}_q$	A finite field of q elements and the residue field of R.
$\mathbb{Z}_m$	The residue ring of the integer ring $\mathbb{Z}$ modulo m.
$a \mid b$	a divides b.
$a \nmid b$	a does not divide b.
$2^a \parallel n$	a is the highest power of 2 dividing n.
$a \equiv b \mod n$	a is congruent to b modulo n, $(\ (a-b) \mid n)$.
$ord_n(q)$	The smallest integer l such that $q^l \equiv 1 \mod n$.
$f^*(x)$	The reciprocal polynomial of a polynomial f.
ξ	A primitive 2^a-th root of unity.
A^T	The transpose of a matrix A.
P	A permutation matrix.

Introduction

Rings form an important topic in Algebra, both pure and applied, from Number Theory to Algebraic Geometry. Coding theory, on the other hand, is present in our daily life, from mobile phones to flash memories. It is the art of protecting messages from a natural noise. Constructing codes that are easy to encode and decode, can detect and correct many errors and have a sufficiently large number of codewords is the principal aim of coding theory. Rings can interact with codes in two fundamental ways. Firstly, the alphabet of the codes can have a ring structure, a finite field, for instance. Secondly, the code itself can be an ideal of, or a module over, some rings. Until the 1990s the usual alphabet chosen by coding theorist was a finite field. Thereafter, it began the study of codes over rings. This study has grown enormously since the seminal work of Hammons et al [33], which gives an arithmetic explanation of the formal duality of Kerdock and Preparata'codes. They showed that some of the best nonlinear codes over $\mathbb{F}_2$ can be viewed as linear codes over $\mathbb{Z}_4$. These findings further motivated the study of codes over different classes of rings.

Linear complementary dual or LCD codes are linear codes that intersect with their dual trivially. LCD codes have been widely applied in data storage, communications systems, consumer electronics, and cryptography [12, 18, 28]. Carlet et al. [16, 17] and Bringer et al. [15] used LCD codes in counter measures to side channel attacks and fault non invasive attacks. Since then, a lot of works has been devoted to constructing LCD codes. In [43], Li et al. constructed several families of Euclidean LCD cyclic codes over finite fields and analyzed their parameters. In [44] Li et al. studied two special families of LCD BCH codes. Mesnager et al. [55] presented a construction of algebraic geometry Euclidean LCD codes. In [18], Carlet et al. completely determined all q-ary ($q > 3$) and q^2-ary ($q > 2$) Euclidean LCD codes. In their most recent paper, Carlet et al. [19] introduced the concept of linear codes with σ complementary dual ($\sigma - LCD$), which includes known Euclidien LCD codes,

Hermitian LCD codes, and Galois LCD codes. Their results extend those on the classical LCD codes and show that $\sigma-$ LCD codes allow the construction of linear complementary pairs of codes more easily and with more flexibility. An LCD code defined over a finite field $\mathbb{F}_q$ was first introduced by Massey [53], he showed the existence of asymptotically good LCD codes. In [62], Yang and Massey provided a necessary and sufficient condition under which a cyclic code has a complementary dual. Later, Liu and Liu in [47] studied LCD codes over finite chain rings and provided a necessary and sufficient condition for a free linear code to be LCD. Recently, in [13], Bhowmnick et al. proved that there are no non-free LCD codes over finite commutative local Frobenius rings. They were also shown that a free simple root cyclic code C over any finite chain ring is LCD code if and only if C is reversible.

Formally self dual codes are also an important class of codes that have generated a lot of interest since they have weight enumerators that are invariant under the MacWilliams transform and sometimes have better parameters than self dual codes. This gives them a potential for applications in areas such as invariant theory, lattices and designs [26]. Self dual and isodual codes form a sub family of formally self dual codes. They have been studied over a wide variety of rings, including finite fields, Galois rings, chain rings, and principal ideal rings [22, 32, 56]. These last years, in [5–7, 9] the authors gave some specific constructions of self dual and isodual codes over finite fields and finite chain rings. In [24, 27, 48], the authors used the Chinese Remainder Theorem to generalize the structure of LCD and self dual codes defined on chain rings to codes defined over principal ideal rings.

In this thesis we provide some new constructions of LCD, self dual and isodual cyclic codes over finite chain rings. We summarize our realized works as follows: In Chapter 1, we give a brief introduction with elementary definitions and properties of linear and cyclic codes over finite fields and rings. Based on algebraic number theory properties, conditions under which all free cyclic codes over finite chain rings are LCD codes are given in Chapter 2. In Chapter 3, we provide conditions on the existence of non trivial self dual cyclic codes over finite chain rings of arbitrary lengths. In Chapter 4, some new constructions of free isodual cyclic codes over finite chain rings are given. We finish this thesis with a conclusion, some comments and possible directions for future research.

Chapter 1

Preliminaries

In this chapter, we have summarized some fundamental notions on error correcting codes defined over finite fields and commutative rings. For more details we refer the reader to consult the references [2, 14, 23, 34, 37, 46, 49, 51, 59, 61, 63].

1 Basic Concepts of Codes over Finite Fields

In this section, we shall briefly recall some fundamental definitions in Coding Theory and give some examples of codes over $\mathbb{F}_q$, the finite field of order q. (see the Appendix). Since some very interesting results can be obtained by simply taking any set as an alphabet. This is how we will start by taking the most general definition of a code

Definition 1.1 *Let A be any finite set. A code C over A of length n is a subset of A^n.*

Coding theory is concerned with the following problem. Consider an information in the form of sequences $a_1, a_2, ..., a_m$ over a q-element set A. We wish to find a function f encoding $a_1, a_2, ..., a_m$ as another sequence $b_1, b_2, ..., b_n$ such that, if an error of specified type occurs in the sequence (b_i), the sequence (a_i) can still be recovered. There should also be a readily computable function g giving $a_1, a_2, ..., a_m$ from $b_1, b_2, ..., b_n$ with possible errors.

In terms of classical coding theory, the elements of the code are called codewords and the underlying set A is called an alphabet.

1.1 Weights and Distances

An important invariant of a code is the minimum distance between codewords. The principal distance used in coding theory is known as the Hamming distance

Definition 1.2 *Let $v = (v_1, v_2, ..., v_n), w = (w_1, w_2, ..., w_n)$ in A^n where A is any set. Then the Hamming distance $d_H(v, w)$ is defined to be the number of coordinates in which v and w differ.*

$$d_H(v, w) = |\{i, |v_i \neq w_i\}|$$

The minimum Hamming distance of a code C defined over A is the smallest distance between distinct codewords of C

$$d_H(C) = \min\{d_H(v, w)|v, w \in C, v \neq w\}$$

Definition 1.3 *The Hamming weight $wt_H(v)$ of a vector v of A^n is the number of nonzero coordinates in v.*

$$wt_H(v) = |\{i|v_i \neq 0\}|$$

The minimum Hamming weight of a code C is

$$\min\{wt_H(v)|v \in C, v \neq 0\}$$

Example 1.1 *Consider the code $C = \{c_0, c_1, c_2, c_3\}$ where $c_0 = (00000), c_1 = (10110), c_2 = (01011), c_3 = (11101)$. Then*

$$d(c_0, c_1) = 3, d(c_0, c_2) = 3, d(c_0, c_3) = 4, d(c_1, c_2) = 4, d(c_1, c_3) = 3, d(c_2, c_3) = 3$$

Hence, the minimum distance of C is $d = 3$.

During coding the channel, some sensitive letters of the received word can be badly transmitted. The number of errors is the number of those letters and decoding the channel consists of associating the received word to a word of C in order to find the initial submitted word.

Theorem 1.1 *[51] Let C be a code over A of length n and minimum distance d, then*

i. C has detection capability $l = d - 1$;

ii. C has correction capability $t = \frac{d-1}{2}$

Proposition 1.1 *[23] (Singleton Bound) Let C be a code of length n over an alphabet of size q with minimum Hamming distance d. Then*

$$\log_q(|C|) \leq n - d + 1$$

Definition 1.4 *A maximum distance separable code (MDS code) is a code C for which $|C| = |A|^{n-d+1}$.*

Thus, an MDS code C has the property that for any k-tuple ($k = n - d + 1$) of elements of A on any k coordinates, there is a unique codeword of C which agrees with the k-tuple on these k coordinates.

1.2 Linear Codes over Finite Fields

A general code might have no structure and not admit any representation other than listing the entire codebook. We now focus on an important subclass of codes with additional structure called linear codes. Many of the important and widely used codes are linear. Throughout, we will denote by $\mathbb{F}_q$ the finite field with q elements, where q is a prime power.

Definition 1.5 *A linear code of length n and dimension k is a linear subspace C with dimension k of the vector space $\mathbb{F}_q^n$. Such a code is called a q-ary code. If $q = 2$ or $q = 3$, the code is described as a binary code, or a ternary code respectively. The size of a code is the number of codewords and equals q^k.*

In general, finding the minimum distance of a code requires comparing every pair of distinct elements. For a linear code however this is not necessary.

Theorem 1.2 *[34] For $v, w \in \mathbb{F}_q^n$, we have $d_H(v, w) = wt_H(v - w)$. Hence, if C is a linear code over $\mathbb{F}_q$, the minimum distance d is the same as the minimum weight of the nonzero codewords of C.*

As a result of this theorem, for linear codes, the minimum distance is also called the minimum weight of the code. If the minimum weight d of a code C is known, then we refer to the code as an $[n, k, d]$ code.

Example 1.2 *Consider*

$$C_1 = \{(0000), (1000), (0100), (1100)\}$$

and

$$C_2 = \{(0000), (1100), (0011), (1111)\}$$

C_1 and C_2 are both 2-dimensional subspaces of $\mathbb{F}_2^4$. The Hamming distance and weight of C_1 are both 1, whereas for C_2 they are both 2.

There is an important bound on the linear codes parameters, the Gilbert-Varshamov bound which give condition on the existence of a linear code.

Proposition 1.2 *[59] There exist an $[n, k, d]$ linear code over $\mathbb{F}_q$ if the following inequality holds:*

$$q^{n-k} - 1 > \sum_{i=1}^{d-1} \binom{n-1}{i} (q-1)^i$$

Definition 1.6 *Two linear codes are said to be equivalent if one can be obtained from the other by a series of operations of the following two types:*

i. An arbitrary permutation of the coordinate positions, and

ii. In any coordinate position, multiplication by any non-zero scalar.

In such case we say that the codes are monomially equivalent and so, they have the same parameters.

1.3 Generator and Parity Check Matrices

Definition 1.7 *A generator matrix for an $[n, k, d]$ linear code C is any $k \times n$ matrix G whose rows form a basis for C. The matrix G completely defines the code C :*

$$C = \{xG; x \in \mathbb{F}_q^k\}$$

Since the basis of a k-dimensional vector space is not unique, neither is the generator matrix G of a linear code C. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for C. The remaining $r = n - k$ coordinates are termed a *redundancy* set and r is called the redundancy of C. If the first k coordinates form an information set, the code has a unique generator matrix of the form $[I_k \mid A]$ where I_k is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix. Such a generator matrix is in standard form. If a generator matrix in standard form exists for a linear code C, it is unique, and any other generator matrix can be brought to the standard from by the following operations:

- Permutation of the rows;
- Multiplication of a row by a non-zero element in $\mathbb{F}_q$;
- Addition of a scalar multiple of one row to another.

Example 1.3 *Let the code C defined over $\mathbb{F}_2$ by its matrix*

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

apply row operations to find the generator matrix of C in standard form .

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{r_2 \leftrightarrow r_1} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow[r_4 \to r_4 + r_1]{r_3 \to r_3 + r_1} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \xrightarrow{r_3 \to r_3 + r_2} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{r_4 \to r_4 + r_3} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \xrightarrow[r_2 \to r_2 + r_3]{r_1 \to r_1 + r_4} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix};$$

Definition 1.8 *A monomial matrix P is a square matrix with exactly one nonzero entry in each row and column. If all of its no zero elements are equal to 1, then P is said to be a permutation matrix.*

Thus two codes C_1 and C_2 are monomially equivalent provided that there exists a monomial matrix P such that if G_1 is a generator matrix of C_1 then G_1P is a generator matrix of C_2.

Theorem 1.3 *[34] Let C be a linear code. Then C is permutation equivalent to a code which has generator matrix in standard form.*

Example 1.4 *Let C and C' be the binary codes with generator matrices respectively*

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \text{ and } G' = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

We will show that C and C' are equivalent codes as follows. By row operations on G (add row 1 to rows 2 and 3), another generating matrix for C is

$$\widehat{G} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Now, if we select the permutation matrix

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

then $G' = \widehat{G}P$. P interchanges columns 1 and 3 of $\widehat{G}$, and hence interchanges coordinates 1 and 3 in each codeword of C. Thus the two codes are equivalent. Note, however, that these codes are not identical.

Since a linear code is a subspace of $\mathbb{F}_q^n$, it is the kernel of some linear application. In particular, there is an $(n-k) \times n$ matrix H, called a **parity check matrix** for the $[n, k, d]$ code C, defined by

$$C = \ker H = \{x \in \mathbb{F}_q^n \mid Hx^T = 0\}$$

In general, there are also several possible parity check matrices for C. The next theorem gives one of them when C has a generator matrix in standard form.

Theorem 1.4 *[34] If $G = [I_k \mid A]$ is a generator matrix for the $[n, k, d]$ code C in standard form, then $H = [-A^T \mid I_{\text{n-k}}]$ is a parity check matrix for C.*

Example 1.5 *The matrix*

$$G = [I_4 \mid A] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is a generator matrix in standard form for a $[7, 4, 3]$ binary code C. By Theorem 1.4, a parity check matrix for C is

$$H = [A^T \mid I_3] = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

There is an elementary relationship between the weight of a codeword and a parity check matrix for a linear code. This is presented by the following theorem .

Theorem 1.5 *[34] Let C be a linear code with parity check matrix H. If c is in C, the columns of H corresponding to the nonzero coordinates of c are linearly dependent. Conversely, if a linear dependence relation with nonzero coefficients exists among m columns of H, then there is a codeword in C of weight m whose nonzero coordinates correspond to these columns.*

One way to find the minimum weight d of a linear code is to examine all the nonzero codewords. The following corollary shows how to use the parity check matrix to find d.

Corollary 1.1 *[34] A linear code has minimum weight d if and only if its parity check matrix H has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns.*

1.4 Dual Codes

The generator matrix G of an $[n, k, d]$ linear code C is simply a matrix whose rows are independent and span the code. The rows of the parity check matrix H are independent;

hence H is the generator matrix of some code, called the dual or orthogonal of C and denoted $C^{\perp}$. An alternate way to define the dual code is by using the inner product. For $x = (x_1, x_2, ..., x_n), y = (y_1, y_2, ..., y_n)$ in A^n, (A any alphabet), the euclidien inner product is defined by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

We say that x is orthogonal to y if and only if $x \cdot y = 0$. The Euclidean dual code $C^{\perp}$ of C is defined as

$$C^{\perp} = \{x \in A^n : \forall y \in C; x \cdot y = 0\}$$

Theorem 1.6 *[63] If C is an $[n, k]$ code, then $C^{\perp}$ is an $[n, n-k]$ code .*

It is easy to show that if G and H are generator and parity check matrices, respectively, for C, then H and G are generator and parity check matrices, respectively, for $C^{\perp}$.
A code C is said to be self dual if $C = C^{\perp}$ and it is isodual if C is equivalent to $C^{\perp}$. It is called LCD or linear complementary dual if $C \cap C^{\perp} = \{0\}$.
For an $[n, k, d]$ linear code C with generator matrix G and a vector v in $\mathbb{F}_q^n$, we can easily show that v belongs to $C^{\perp}$ if and only if v is orthogonal to every row of G;

$$v \in C^{\perp} \Leftrightarrow Gv^T = 0$$

Example 1.6 *Let C be the ternary linear code C with generator matrix G, in standard form, given by*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}$$

Since $C = \langle v_1 = (1, 0, 1, 1), v_2 = (0, 1, 1, -1) \rangle$ and

$$Gv_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = Gv_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

This code is self-dual.

1.5 Weight Distribution and Weight Enumerators

Let C be an $[n, k, d]$ over $\mathbb{F}_q$ and let $A_i = A_i(C)$ be the number of codewords of weight i in C. The list A_i for $0 \leq i \leq n$ is called the weight distribution or weight spectrum of C. Certain elementary facts about the weight distribution are gathered in the following theorem.

Theorem 1.7 *[34] Let C be an $[n, k, d]$ code over $\mathbb{F}_q$. Then:*

i. $A_0(C) + A_1(C) + ... + A_n(C) = q^k$

ii. $A_0(C) = 1$ *and* $A_1(C) = A_2(C) = ... = A_{d-1}(C) = 0$

iii. If C is a binary code containing the codeword $1 = (111...1)$, then $A_i(C) = A_{n-i}(C)$ for $0 \leq i \leq n$.

The most fundamental result about weight distributions is a set of linear relations between the weight distributions of C and $C^\perp$ which imply, that if we know the weight distribution of C we can determine the weight distribution of $C^\perp$ without knowing specifically the codewords of $C^\perp$ or anything else about its structure.

Lemma 1.1 *[51] Let C be an $[n, k, d]$ linear code over F_q with weight distribution $A_i = A_i(C)$ for $0 \leq i \leq n$, and let the weight distribution of $C^\perp$ be $A_i^\perp = A_i(C^\perp)$. We have*

i. $\sum_{i=0}^{n} A_i = q^k A_0^\perp$.

ii. $\sum_{i=0}^{n-1}(n-i)A_i = q^{k-1}(nA_0^\perp + A_1^\perp)$.

iii. $\sum_{i=0}^{n-j} \binom{n-i}{j} A_i = q^{k-j} \sum_{i=0}^{j} \binom{n-i}{n-j} A_i^\perp$; *for* $0 \leq j \leq n$.

Definition 1.9 *For a code C of length n, we call Hamming weight enumerator the polynomial*

$$W_C(x) = \sum_{i=1}^{n} A_i(C) x^i$$

By replacing x by x/y and then multiplying by y^n, $W_C(x)$ can be converted to the two variables weight enumerator

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

Proposition 1.3 *[20] Two equivalent linear codes have the same weight enumerator. but the converse does not always hold.*

Example 1.7 *Consider the two binary codes C_1 and C_2 with generator matrices G_1 and G_2 respectively, where*

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Both of the codes have weight distribution $A_0 = 1, A_2 = 3, A_4 = 3,$ and $A_6 = 1$. Hence their weight enumerator is

$$W_{C_1}(x, y) = W_{C_2}(x, y) = y^6 + 3x^2y^4 + 3x^4y^2 + x^6 = (y^2 + x^2)^3$$

But C_1 and C_2 are not monomially equivalent since C_2 is self dual code while C_1 is not.

One of the most important results in this area is the MacWilliams identity which, relates the weight enumerator of a linear code C to the weight enumerator of $C^{\perp}$.

Theorem 1.8 *[51] If C is an $[n, k, d]$ code over $\mathbb{F}_q$, and $C^{\perp}$ is the dual of C, then*

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

Definition 1.10 *A code C is said to be formally self dual code if it has the same weight enumerators as its dual.*

Remark 1.1 *Self dual codes are both isodual and formally self dual codes, but the converse is not true. Formally self dual codes can have better minimum distances than self dual codes of the same lengths.*

1.6 Cyclic codes over finite fields

Linear codes are nice to study and implement, because they have algebraic structures that ensure easy encoding and decoding. However, we can do more to simplify the implementation of codes if we require a cyclic shift of a codeword in C to still be a codeword. This requirement smells like a combinatorial structure, but we shall combine the works of the previous section to show that this has an algebraic structure.

Definition 1.11 *A linear code C of length n over $\mathbb{F}_q$ is called cyclic if $(c_{n-1}, c_0, ..., c_{n-2})$ is in C whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C.*

Since a cyclic code is invariant under a cyclic shift we conclude that a cyclic code contains all cyclic shifts of any codeword. We can describe these codes in algebraic terms since any element $(c_0, c_1, ..., c_{n-1})$ of the vector space $\mathbb{F}_q^n$ can be identified by the residue class of the polynomial $c_0 + c_1x + ... + c_{n-1}x^{n-1}(\mod (x^n - 1))$ over $\mathbb{F}_q$, by the bijection

$$\begin{aligned} \mathbb{F}_q^n &\rightarrow \mathbb{F}_q[x]/\langle x^n - 1\rangle \\ (c_0, c_1, ..., c_{n-1}) &\rightarrow c_0 + c_1x + ... + c_{n-1}x^{n-1} \mod (x^n - 1) \end{aligned}$$

Therefore, any codeword is identified as a vector or as a polynomial. It is clear that if C is a cyclic code and $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ in C then

$$xc(x) = c_0x + c_1x^2 + ... + c_{n-1}x^n = c_{n-1} + c_0x + c_1x^2 + ... + c_{n-2}x^{n-1} \in C$$

Hence, multiplying the polynomial $c(x)$ by x corresponds to a right shift of the vector c. It follows that cyclic codes over $\mathbb{F}_q$ are precisely the ideals of the ring $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$, and vice versa. Therefore, the study of cyclic codes over $\mathbb{F}_q$ is equivalent to the study of ideals in R_n. It is known that R_n is a principapl ideal ring and hence cyclic codes are the principal ideals of R_n. More precisely, C is generated by the monic polynomial of least degree $g(x)$ in C, called the generator polynomial. Then, $g(x)$ is a divisor of $x^n - 1$ in $\mathbb{F}_q$. Any codeword $c(x)$ in C can be uniquely written as $c(x) = \lambda(x)g(x)$, where $\lambda(x)$ has degree less than $n \deg(g(x))$ and the dimension of C is $k = n - \deg g(x)$. This discussion gives the following theorem.

Theorem 1.9 *[34] Let C be a nonzero cyclic code in R_n. There exists a polynomial $g(x)$ in C with the following properties:*

i. $g(x)$ is the unique monic polynomial of minimum degree in C,

ii. $C = \langle g(x)\rangle$ and $g(x)|x^n - 1$.

iii. The dimension of C is $k = n - degg(x)$ and $g(x), xg(x), ..., x^{k-1}g(x)$ is a basis for C,

iv. Every element of C is uniquely expressible as a product $g(x)f(x)$, where $f(x) = 0$ or $\deg f(x) < k$,

v. Assume that $g(x) = \sum_{i=0}^{n-k} g_i x^i$, *where* $g_{n-k} = 1$. *Then:*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & \\ & \cdots & \cdots & \cdots & \cdots & & \\ 0 & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix} \leftrightarrow \begin{pmatrix} g_(x) \\ xg(x) \\ \cdots \\ x^{k-1}g(x) \end{pmatrix}$$

is a generator matrix for C,

vi. If α *is a primitive* n*-th root of unity in some extension field of* $\mathbb{F}_q$, *then* $g(x) = \prod_s m_{\alpha^s}(x)$, *where the product is over a subset of representatives of the* q*-cyclotomic cosets modulo* n.

So there is a one-to-one correspondence between the nonzero cyclic codes and the divisors of $x^n - 1$, not equal to $x^n - 1$. In order to have a bijective correspondence between all the cyclic codes in R_n and all the monic divisors of $x^n - 1$, we define the generator polynomial of the zero cyclic code $\{0\}$ to be $x^n - 1$.

Theorem 1.10 *[34] The dual code of a cyclic code is cyclic.*

Recall that the annihilator of an ideal C, denoted $Ann(C)$, is the ideal whose elements cancel out all the elements in the ideal C. In our case, let C be an $[n, k, d]$ cyclic code with generator polynomial $g(x)$, and let $h(x) = \dfrac{x^n - 1}{g(x)} = h_0 + h_1 x + ... + h_k x^k$. Then $h(x)$ is called the parity check polynomial of C and $Ann(C) = \langle h(x) \rangle$.

Definition 1.12 *Let* $f(x) = a_0 + a_1 x + ... + a_r x^r$ *be a polynomial of* $R[x]$ *of degree* r *such that* $f(0) = a_0$ *is a unit in* R *(where* R *is a finite commutative ring). The monic reciprocal polynomial of* $f(x)$ *is defined by*

$$f^*(x) = f(0)^{-1} x^r f(x^{-1})$$

If $f^*(x) = f(x)$, *the polynomial* $f(x)$ *is called self reciprocal.*

The following Lemma is easily deduced.

Lemma 1.2 *Let* $f(x)$ *and* $g(x)$ *be two polynomials in* $R[x]$ *with* $degf(x) \geq degg(x)$ *and with constants terms are units. Then the following holds.*

i. $[f(x)g(x)]^* = f(x)^* g(x)^*$.

ii. $[f(x)+g(x)]^* = f(x)^* + x^{degf-degg}g(x)^*$.

iii. If $f(x)$ *is monic, then* $\overline{f(x)^*} = \overline{f(x)}^*$.

Theorem 1.11 *[34] Let* C *be an* $[n,k,d]$ *cyclic code with generator polynomial* $g(x)$*. Let* $h(x) = h_0 + h_1x + ... + h_kx^k$ *be the parity check polynomial of* C*. Then the generator polynomial of* $C^\perp$ *is* $h^*(x)$*. Furthermore, a generator matrix for* $C^\perp$*, and hence a parity check matrix for* C*, is*

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & ... & h_0 & & 0 \\ 0 & h_k & h_{k-1} & ... & h_1 & h_0 & \\ & ... & ... & ... & ... & & \\ 0 & & & h_k & h_{k-1} & ... & h_0 \end{pmatrix}$$

Example 1.8 *Let* C *be the binary cyclic code generated by the linear combination of all cyclic shifts of the vector* $(1,1,0,1,0,0,0)$ *. Clearly,* $C = \langle g(x) \rangle$ *where* $g(x) = 1 + x + x^3$*, and then* $h(x) = 1 + x + x^2 + x^4$*. A generator matrix for* C *is*

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

The generator polynomial of $C^\perp$ *is* $h^*(x) = 1 + x^2 + x^3 + x^4$*. Hence a generator matrix for* $C^\perp$ *which is a parity matrix check of* C *is given by*

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Besides the generator polynomial, there are many polynomials that can be used to generate a cyclic code. There is a very specific polynomial, called an idempotent generator, which can be used to generate a cyclic code. (Recall that an idempotent element of a ring is an element e such that $e^2 = e$)

Theorem 1.12 *[34] Let C be a cyclic code in R_n. Then:*

i. There exists a unique idempotent $e(x)$ in C such that $C = \langle e(x) \rangle$,

ii. If $e(x)$ is a nonzero idempotent in C, then $C = \langle e(x) \rangle$ if and only if $e(x)$ is a unity of C,

iii. If $C = \langle e(x) \rangle$. Then the generator polynomial of C is $g(x) = \gcd(e(x), x^n - 1)$ computed in $\mathbb{F}_q[x]$.

Theorem 1.13 *[34] Let C_1 and C_2 be cyclic codes of length n over $\mathbb{F}_q$ with generator polynomial $g_1(x), g_2(x)$ and generating idempotent $e_1(x), e_2(x)$. Then $C_1 \cap C_2$ has generator polynomial $Icm(g_1(x), g_2(x))$ and generating idempotent $e_1(x)e_2(x)$.*

Example 1.9 *Consider the ternary cyclic codes C_1 and C_2 of length $n = 11$ generated by the polynomials $g_1(x) = 1 - x - x^2 - x^3 + x^4 + x^6$ and $g_2(x) = -1 - x + x^2 - x^3 + x^5$, respectively. A simple calcul shows that*

$$e_1(x) = (x^3 - x + 1)g_1(x) = 1 + x + x^3 + x^4 + x^5 + x^9 \text{ and } e_1^2(x) = e_1(x)$$

$$e_2(x) = (-x^5 + x^4 + x^2)g_2(x) = -x^2 - x^6 - x^7 - x^8 - x^{10} \text{ and } e_2^2(x) = e_2(x)$$

Hence $e_1(x)$ and $e_2(x)$ are idempotent generator for the codes C_1 and C_2 respectively. Further since we have

$$x^{11} - 1 = g_1(x)g_2(x) \text{ and } \gcd(g_1(x), g_2(x)) = 1$$

then $C_1 \cap C_2 = \{0\}$. On the other words, C_1 and C_2 are LCD codes.

2 Basic Concepts of Codes over Finite Rings

This section is dedicated to introduce the necessary notions and terminology from classical coding theory over rings that will be needed later. Throughout this thesis, all considered rings are assumed to be commutative and with identity.

2.1 Linear Code over Finite Rings

Definition 2.1 *A linear code over a ring R of length n is a submodule C of R^n. If C is isomorphic to a free R-module, then we say that C is a free code and we define the dimension of C to be $\dim C = rank_R(C)$.*

Since a module over a ring R is a generalization of the notion of vector space over a field. So, much of the theory of codes over rings consists of extending as many as possible the desirable properties of codes over fields. However, codes over rings can be quite a bit more complicated than codes over fields; for instance, since not all modules have bases, then the definition of a generator matrix for example is not trivial.

Definition 2.2 *Let C in R^n be a linear code over any finite ring R. Define a generator matrix of C as a matrix G with rows being a generating set of C with the smallest size.*

This means that the rows of G span C and none of them can be written as a linear combination of the other rows of G. In particular, when C is a free code, then the rows of any generator matrix G are a group of basis elements of C, and so the number of rows of any generator matrix of a free code C is uniquely determined.

Definition 2.3 *Two codes C and C' in R^n, are said to be equivalent if C' can be obtained from C by a combination of a permutation of the coordinates and multiplication of a coordinate by* ***a unit in the underlying ring****.*

As for codes defined over finite fields we have :

Theorem 2.1 *[23] If C is a linear code over a ring R, then the minimum Hamming distance and the minimum Hamming weight are equal.*

The following was first proven by F. MacWilliams in [51]. There, it was proven for codes over finite fields. Later it was proven that we can extend the proof to codes over finite commutative Frobenius rings.

Theorem 2.2 *[23] Let R be a finite commutative Frobenius ring with $|R| = r$. Let C be a linear code over R. Then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (r-1)y, x - y)$$

One of the most important consequences of the MacWilliams relations is the following:

Corollary 2.1 *If C is a linear code over a finite commutative Frobenius ring R, then $|C|.|C^\perp| = |R^n|$.*

2. 1.1 Linear codes over finite chain rings

A finite chain ring is a local Frobenius ring, so the identity above holds for codes over finite chain rings. Further we have many nice results on codes over this class of rings. (For more detail of finite chain rings and Frobenius rings, we refer the reader to see the appendix).

Definition 2.4 *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$ of nilpotency index e and C be a code over R with generator matrix G. We say that G is a generator matrix in standard form if after a suitable permutation of the coordinates, we have*

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \gamma A_{1,e-1} & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \gamma^2 A_{2,e-1} & \gamma^2 A_{2,e} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}$$

Where the columns are grouped into blocks of sizes $k_0, k_1, ..., k_{e-1}, n - \sum_{i=0}^{e-1} k_i$. A code with generator matrix of this form is said to be have type $\{k_0, k_1, ..., k_{e-1}\}$.

Theorem 2.3 *[57] Any linear code C defined over a finite chain ring has a generator matrix in standard form. Further, all generator matrices in standard form for the code C have the same parameters $k_0, k_1, ..., k_{e-1}$ and $|C| = q^{\sum_{j=0}^{e-1}(e-j)k_j}$.*

Theorem 2.4 *[57] Let C be a code with generator matrix G in standard form. For $0 \leq i < j \leq e$, let $B_{i,j} = -\sum_{k=i+1}^{j-1} B_{i,k} A_{e-j,e-k}^T - A_{e-j,e-i}^T$. Then*

$$H = \begin{pmatrix} B_{0,e} & B_{0,e-1} & \cdots & B_{0,1} & I_{n-k(C)} \\ \gamma B_{1,e} & \gamma B_{1,e-1} & \cdot & \gamma I_{k_{e-1}(C)} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \gamma^{e-1} B_{e-1,e} & \gamma^{e-1} I_{k_1(C)} & \cdots & 0 & 0 \end{pmatrix}$$

is a generator matrix for $C^\perp$ and a parity check matrix for C.

Let C be a linear code. We denote by $k(C)$ the number of rows of a generating matrix G in standard form for C, and for $i = 0, 1, ..., e-1$ we denote by $k_i(C)$ the number of rows of G that are divisible by $\langle\gamma^i\rangle$ but not by $\langle\gamma^{i+1}\rangle$. Clearly, $k(C) = \sum_{i=0}^{e-1} k_i(C)$.

Proposition 2.1 *[57] Let C be a linear code. The following assertions are equivalent:*

i. C is a free code.

ii. Any generator matrix in standard form for C is of the form $[I_{k(C)}|M]$ for some matrix M.

iii. $k(C) = k_0(C)$.

iv. $C^{\perp}$ is free.

Example 2.1 *Let $R = \mathbb{Z}_4$ and C the code of length 4 defined over R by the vectors*

$$0000 \quad 1113 \quad 2222 \quad 3331 \quad 0202 \quad 1311 \quad 2020 \quad 3133$$
$$0022 \quad 1131 \quad 2200 \quad 3313 \quad 0220 \quad 1333 \quad 2002 \quad 3111$$

Then C is a linear code over $\mathbb{Z}_4$. A generator matrix of C in the standard form is given by

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

Hence we have $k_0(C) = 1, k_1(C) = 2$ and $k(C) = 3$, so C is not a free code. A parity check matrix of C is given by

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

Clearly $H.G^T = 0$. Since $G.G^T = 0$, we deduce that C is a self dual code.

2.2 Cyclic Codes over Finite Chain Rings

As we have already seen, much of the theory of codes over rings consists of generalizing concepts and properties of codes over finite fields. Cyclic codes over rings has not been studied in depth for a general ring. In this thesis, we will mainly focus on codes over finite chain rings and finite principal ideal rings. As usual, cyclic codes of length n over a ring R are linear codes with the property that the cyclic shift of any codeword is again a codeword.

Proposition 2.2 *[57] A linear code C of length n is a cyclic over R if and only if C is an ideal of $R[x]/\langle x^n - 1\rangle$.*

Proposition 2.3 *[57] The dual of a cyclic code over R is cyclic.*

Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$ of nilpotency index e, and residue field $\mathbb{F}_q$. In this section, we assume n to be a positive integer coprime to q, so that x^n-1 is square free in $\mathbb{F}_q[x]$. Therefore, x^n-1 has a unique decomposition as a product of basic irreducible pairwise coprime polynomials in $R[x]$. A natural way of constructing a cyclic code over R is by lifting the generator polynomial of a cyclic code over $\mathbb{F}_q$.

Definition 2.5 *(Hensel lift of a cyclic code) Let f in $\mathbb{F}_q[x]$ be monic such that $f|(x^n-1)$. The cyclic code $\langle g\rangle$ where g is the Hensel lift of f is called the Hensel lift of the cyclic code $\langle f\rangle$.*

If C is the Hensel lift of a code E then $\bar{C}=E$, but C is not the only cyclic code whose projection is E.

Proposition 2.4 *[57] Let C be a code over R. The following properties are equivalent:*

i. C is the Hensel lift of a cyclic code;

*ii. C is cyclic and **free**;*

iii. There is a g in $R[x]$ such that $C=\langle g\rangle$ and $g|(x^n-1)$;

iv. $C^{\perp}$ is the Hensel lift of a cyclic code.

In general for non-free cyclic codes over a chain ring R, Din et al [22] gave a specific structure of these codes. We have the following Theorems

Theorem 2.5 *[22] Let C be a cyclic code over R of length n. Then there exists a unique family of pairwise coprime polynomials $F_i(x), 0\leq i\leq e$ in $R[x]$ satisfying $F_0(x)F_1(x)...F_e(x)=x^n-1$ such that*

$$C=\left\langle \hat{F}_1(x),\gamma\hat{F}_2(x),...,\gamma^{e-1}\hat{F}_e(x)\right\rangle=\left\langle \hat{F}_1+\gamma\hat{F}_2+...\gamma^{e-1}\hat{F}_e\right\rangle$$

where $\hat{F}_i(x)=\dfrac{x^n-1}{F_i(x)}$ for $0\leq i\leq e$. Moreover

$$|C|=p^{r\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}}$$

Corollary 2.2 *[22] $\dfrac{R[x]}{\langle x^n-1\rangle}$ is a principal ideal ring.(with $\gcd(n,q)=1$).*

Theorem 2.6 *[22] Let C be a cyclic code of length n over R. Then there exist polynomials $g_0, g_1, ..., g_{e-1}$ in $R[x]$ such that $C = \langle g_0, \gamma g_1, ..., \gamma^{e-1} g_{e-1} \rangle$ and $g_{e-1} | g_{e-2} | ... | g_0 | x^n - 1$.*

Theorem 2.7 *[22] Let C be a cyclic code of length n, with notation as in Theorem 2.5, we have*

$$C^{\perp} = \left\langle \hat{F}_0^*(x), \gamma \hat{F}_e^*(x), ..., \gamma^{e-1} \hat{F}_2^*(x) \right\rangle$$

and

$$|C^{\perp}| = p^{r \sum_{i=1}^{e} i \deg F_{i+1}}$$

Where F_i^* is the reciprocal polynomial of $F_i, 0 \leq i \leq e$.

Chapter 2

Construction of LCD Cyclic Codes over Finite Rings

The aim of this chapter is to present some new constructions of LCD cyclic codes, provide necessary and sufficient conditions for which all free cyclic codes over finite chain rings are LCD. We start with some known basic results on LCD codes over finite fields.

1 Generalities on LCD Codes over Finite Fields

Recall that a linear code C over a field $\mathbb{F}_q$ is called an LCD code (linear code with complementary dual) if $C \cap C^{\perp} = \{0\}$, which is equivalent to $C \oplus C^{\perp} = \mathbb{F}_q^n$.

Proposition 1.1 *[53] Let C be a linear code with a generator matrix G and a parity-check matrix H. Then the three following properties are equivalent:*

i. C is an LCD code;

ii. The matrix GG^T is invertible;

iii. The matrix HH^T is invertible.

Corollary 1.1 *Let C be a linear code with generator matrix in standard form $G = [I_k|A]$. Then C is an LCD code if and only if -1 is not an eigen value of AA^T.*

Proof. By a simple calculation we have

$$GG^T = [I_k|A] \left[\frac{I_k}{A^T}\right] = AA^T + I_k$$

The matrix GG^T is invertible if and only if -1 is not an eigen value of AA^T. □

Example 1.1 *Let C be the binary code with generator matrix*

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

The parity-check matrix H of this code is

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Since

$$\det GG^T = \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \neq 0$$

Then this code is an LCD code. we can see also that we have

$$\det HH^T = \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq 0$$

Definition 1.1 *A code C is called reversible if for each code word $(c_0, c_1, ..., c_{n-1})$ in C, the reverse code word $(c_{n-1}, c_{n-2}, ..., c_0)$ is also in C. This means that reversing the order of the components of any codeword gives always again a codeword.*

Proposition 1.2 *[62] A cyclic code is reversible if and only if its generator polynomial is self reciprocal.*

Theorem 1.1 *[62] Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial $g(x)$ such that* $\gcd(n, q) = 1$. *Then the following statements are equivalent.*

i. C is an LCD code.

ii. g is self-reciprocal.

iii. β^{-1} is a root of $g(x)$ for every root β of $g(x)$ over the splitting field of g.

Furthermore, if -1 is a power of q mod n, then every cyclic code over $\mathbb{F}_q$ of length n is reversible.

More generally, if n is not coprime to q, In [62] again Massey et al gave conditions on cyclic codes to be LCD.

Theorem 1.2 *[62] If $g(x)$ is the generator polynomial of a cyclic code C of length n over $\mathbb{F}_q$, then C is an LCD code if and only if $g(x)$ is self-reciprocal and all the monic irreducible factors of $g(x)$ have the same multiplicity in $g(x)$ as in $x^n - 1$.*

Corollary 1.2 *[62] A cyclic code C, whose length n is relatively prime to the characteristic of $\mathbb{F}_q$, is an LCD code if and only if it is a reversible code.*

2 On LCD Codes over Finite Rings

In this part, we will present some judging criterions for cyclic codes over some finite rings to be LCD codes. For linear codes over rings, some structures of LCD codes using generating matrices have been given in [23, 47] .

Lemma 2.1 *[23] Let $v_1, v_2, ..., v_k$ be vectors over a* ***finite commutative Frobenius ring*** *such that $v_i.v_i = 1$ for each i and $v_i.v_j = 0$ for $i \neq j$. Then $C = \langle v_1, v_2, ..., v_k \rangle$ is an LCD code over R.*

Theorem 2.1 *[47] Let C be a code over* ***a finite chain ring*** *R with generator matrix G in standard form. If the $k \times k$ matrix GG^T is invertible, then C is an LCD code, where k is the number of rows of G.*

Liu et al [48] generalized this result to **free codes** over any finite ring.

Theorem 2.2 *[48] Assume R is any finite commutative ring, and assume C is a free code, then C is an LCD code if and only if GG^T is nonsingular.*

Bhowmick et al in [13] proved that there does not exist a non-free LCD code over finite commutative **local Frobenius rings**.

Theorem 2.3 *[13] Over finite commutative local Frobenius rings, any LCD code is free.*

Note that the converse of Theorem 2.3 does not hold in general. To show this we cite the following example.

Example 2.1 *Let C be a linear code over $\mathbb{Z}_4$ with generator matrix*

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

We have that C is free code, but C is not LCD, since $(0,0,0,2,2,0,0) \in C \cap C^{\perp}$.

Cyclic codes have more interesting structures than general linear codes. In [13], Bhowmick et al, generalized the characterization of LCD cyclic codes over finite chain rings.

Lemma 2.2 *[13] Let C be a cyclic code over a finite chain ring R with residue field $\mathbb{F}_q$ of length n such that $\gcd(n,q) = 1$. Let g be a generator polynomial of C. Then C is an LCD code if and only if C is reversible if and only if the polynomial g is self reciprocal .*

Liu and Wang in [48] generalized Massey's criterion for LCD codes over finite field of **any length** to finite chain rings.

Lemma 2.3 *[48] A cyclic code C of length n over a finite chain ring R with the residue field $\mathbb{F}_q$ is an LCD code if and only if $C = \langle g(x) \rangle$, where $g(x)$ is a monic divisor of $x^n - 1$ such that $g(x) = g^*(x)$, and $g(x)$ and $(x^n - 1)/g(x)$ are coprime.*

Let $q = p^s$ and $n = mp^r$, where $\gcd(m,p) = 1$. Thus the polynomial $x^m - 1$ is a monic square free, hence it factors uniquely as a product of pairwise coprime monic irreducible polynomials $f_1(x), ..., f_l(x)$. Hence the factorization of $x^n - 1$ over $\mathbb{F}_q$ is given by

$$x^n - 1 = x^{mp^r} - 1 = (x^m - 1)^{p^r} = f_1(x)^{p^r} ... f_l(x)^{p^r} \tag{2.1}$$

Denote the factors $f_i(x)$ in the factorization of $x^m - 1$ which are self reciprocal by $g_1(x), \ldots, g_s(x)$ and the remaining $f_j(x)$ grouped in pairs by $h_1(x), h_1^*(x), \ldots, h_t(x), h_t^*(x)$. Hence $l = s + 2t$,

and the factorization given in (2.1) becomes

$$x^n - 1 = g_1(x)^{p^r} g_2(x)^{p^r} ... g_s(x)^{p^r} h_1(x)^{p^r} h_1^*(x)^{p^r} ... h_t(x)^{p^r} h_t^*(x)^{p^r}$$

Using Hensel's Lemma and the properties of the reciprocal polynomial, we get a factorization of $x^n - 1$ over R, which is given by

$$x^n - 1 = G_1(x)G_2(x)...G_l(x)H_1(x)H_1^*(x)...H_t(x)H_t^*(x),$$

where $G_i(x), H_j(x)$ are monic coprime polynomials such that $\overline{G_i(x)} = g_i^{p^r}(x), \overline{H_j(x)} = h_j^{p^r}(x)$. By Lemma 2.3, we obtain a characterization of LCD cyclic codes over finite chain rings. Those are codes generated by

$$C = \left\langle G_1(x)^{k_1} G_2(x)^{k_2} ... G_l(x)^{k_l} H_1(x)^{r_1} H_1^*(x)^{r_1} ... H_t(x)^{r_t} H_t^*(x)^{r_t} \right\rangle,$$

where $k_i, r_j \in \{0, 1\}$ for all $1 \leq i \leq l,\ 1 \leq j \leq t$.

2.1 Some Properties of Positive Integers

In this section, we give some properties of positive integers which are the tools used to prove our results given in [10]. Recall that the multiplicative order of an integer q modulo p denoted by $r = ord_p(q)$ is the smallest integer l such that $q^l \equiv 1 \mod p$. (Note that the first result of the following Lemma is given in [6]).

Lemma 2.4 *Let q be a prime power, p an odd prime number coprime to q, then we have*

(i) If $ord_p(q)$ is even then for all k in $\mathbb{N}^*$, $ord_{p^k}(q)$ are even.

(ii) If there is k in $\mathbb{N}^*$ such that $ord_{p^k}(q)$ is even, then $ord_p(q)$ is also even.

Proof. Since p divides p^k, the congruence $q^{ord_{p^k}(q)} \equiv 1 \mod p^k$ implies that $q^{ord_{p^k}(q)} \equiv 1 \mod p$. Hence $ord_p(q) \mid ord_{p^k}(q)$ Therefore, if $ord_p(q)$ is even then $ord_{p^k}(q)$ is even too.
To prove (ii), assume that there is k in $\mathbb{N}^*$ such that $ord_{p^k}(q)$ is even, and by way of contradiction we suppose that $ord_{p^{k-1}}(q)$ is odd. Therefore, there exist some integer i and there exists m in $\mathbb{N}$, such that $q^{2i+1} = 1 + mp^{k-1}$. Since p is a prime number, it divides the binomial coefficient $\binom{p}{j}$ for all $1 \leq j \leq p-1$. Hence we get $(q^{2i+1})^p = \left(1 + mp^{k-1}\right)^p \equiv 1 \mod p^k$. It follows that $ord_{p^k}(q) \mid (2i+1)p$. Since $(2i+1)p$ is odd, this leads to a contradiction. So that $ord_{p^{k-1}}(q)$ must be even, and by descending recurrence we get that $ord_p(q)$ is even.

□

Lemma 2.5 *Let q be a prime power and p an odd prime number such that* $\gcd(p,q)=1$. *The three following statements are equivalents.*

(i) There exits l in $\mathbb{N}$, such that $q^l \equiv -1 \mod p$.

(ii) For all k in $\mathbb{N}$, there exists l_k in $\mathbb{N}$, such that $q^{l_k} = -1 \mod p^k$.

(iii) There is i in $\mathbb{N}^*$ such that $ord_{p^i}(q)$ is even.

Further, if $q^l \equiv -1 \mod p$, then $l = \frac{1}{2}(1+2m)ord_p(q)$ for some m in $\mathbb{N}$.

Proof. Suppose that (i) is satisfied and we prove (ii) by induction. For $k=1$ we have $q^l \equiv -1 \mod p$. Assume $q^{l_{k-1}} \equiv -1 \mod p^{k-1}$ for $k \geq 2$. Since p is odd, we can write

$$\sum_{i=0}^{p^{k-1}-1} (-q^{l_{k-1}})^i = \frac{(-q^{l_{k-1}})^{p^{k-1}} - 1}{(-q^{l_{k-1}}) - 1} = \frac{q^{l_{k-1}p^{k-1}} + 1}{q^{l_{k-1}} + 1}.$$

On the other hand, we have

$$\sum_{i=0}^{p^{k-1}-1} (-q^{l_{k-1}})^i = \sum_{i=0}^{p^{k-1}-1} (-1)^i (q^{l_{k-1}})^i \equiv \sum_{i=0}^{p^{k-1}-1} (-1)^i (-1)^i \mod p^{k-1} \equiv 0 \mod p^{k-1}$$

which means that $p^{k-1} \mid \sum_{i=0}^{p^{k-1}-1} (-q^{l_{k-1}})^i$. Since $p \mid p^{k-1} \mid q^{l_{k-1}} + 1$, it follows that

$$p^k \mid (q^{l_{k-1}} + 1)\Big(\sum_{i=0}^{p^{k-1}-1} (-q^{l_{k-1}})^i\Big) = q^{l_{k-1}p^{k-1}} + 1.$$

Thus, for $l_k = l_{k-1} \cdot p^{k-1}$, we have that $q^{l_k} \equiv -1 \mod p^k$. Note that when $q^l \equiv -1 \mod p$, then $l_k = l_{k-1} \cdot p^{k-1} = l_{k-2} \cdot p^{k-2} \cdot p^{k-1}$. We obtain that $l_k = l \cdot p^{\frac{k(k-1)}{2}}$. Conversely, if the statement (ii) holds, then the statement (i) follows immediately for $k=1$.
Assume that (iii) is satisfied. So Lemma 2.4 shows that the integer $ord_p(q)$ is also even. We have, $q^{ord_p(q)} \equiv 1 \mod p$ if and only if $p \mid (q^{\frac{1}{2}ord_p(q)} - 1)(q^{\frac{1}{2}ord_p(q)} + 1)$. Since p is prime it must divide one of the factor and it can not divide $(q^{\frac{1}{2}ord_p(q)} - 1)$ because of the definition of the order of q, thus $q^{\frac{1}{2}ord_p(q)} = -1 \mod p$.
Conversely, if (ii) is satisfied, then there exits l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod p$, which means $q^{2l} \equiv 1 \mod p$, so that $ord_p(q) \mid 2l$. If $ord_p(q)$ is odd, then $ord_p(q) \mid l$, which contradicts the fact that $q^l \equiv -1 \mod p$. Hence $ord_p(q)$ must be even and (iii) holds.

It remains to prove that if there exists an integer l such that $q^l \equiv -1 \mod p$, then $l = \frac{1}{2}(1+2m)ord_p(q)$ for some m in $\mathbb{N}$. By the definition of order, the integers $q^{ord_p(q)}$ and q^j are distincts for all $1 \leq j < ord_p(q)$. Since p is odd, we obtain that if l' is the smallest integer such that $q^{l'} \equiv -1 \mod p$, then on the one hand $1 \leq l' < ord_p(q)$ and, on the other hand, $ord_p(q) \mid 2l'$. This gives $2l' = \lambda ord_p(q)$ and $\lambda \geq 1$. Since $l' < ord_p(q)$, then $l' = \frac{1}{2}ord_p(q)$. Further, if l is an integer that satisfies $q^l \equiv -1 \mod p$, then by division algorithm we can write $l = sl' + r$ with $r < l'$. Hence, we get

$$q^l = q^{sl'+r} = (q^{l'})^s q^r \equiv (-1)^s q^r \mod p \equiv -1 \mod p.$$

Which forces that s is odd and $r = 0$. Thus,

$$l = (2m+1)l' = \frac{1}{2}(2m+1)ord_p(q).$$

□

Corollary 2.1 *Let q be a prime power and p an odd prime number coprime to q. Let a be a positive integer such that $2^a \| ord_p(q)$. Then for all k in $\mathbb{N}^*$, we have $2^a \| ord_{p^k}(q)$, where the notation $2^a \| ord_p(q)$ means that $2^a | ord_p(q)$ but $2^{a+1} \nmid ord_p(q)$.*

Proof. Let a be a positive integer such that $2^a \| ord_p(q)$. From Lemma 2.5, there exists l in $\mathbb{N}^*$, such that $q^l \equiv -1 \mod p$ and $l = \frac{1}{2}(1+2m)ord_p(q)$ for some m in $\mathbb{N}$. On the other hand, since $ord_p(q)$ is even, then $ord_{p^k}(q)$ is also even for all $k \in \mathbb{N}^*$. Hence, from Lemma 2.5 again, there exists l_k in $\mathbb{N}^*$, such that $q^{l_k} \equiv -1 \mod p^k$ and $l_k = \frac{1}{2}(1+2m_k)ord_{p^k}(q)$ for some m_k in $\mathbb{N}$. From the proof of Lemma 2.5, we have that $l_k = l \cdot p^{\frac{k(k-1)}{2}}$. Therefore

$$l_k = \frac{1}{2}(1+2m_k)ord_{p^k}(q) = \frac{1}{2}(1+2m)ord_p(q) \cdot p^{\frac{k(k-1)}{2}}.$$

Since $(1+2m)p^{\frac{k(k-1)}{2}}$ and $(1+2m_k)$ are both odd, we conclude that $2^a \| ord_{p^k}(q)$. □

2.2 New Constructions of LCD Cyclic Codes over Finite Chain Rings

Let n be a positive integer and q a prime power coprime to n. For s in $\{0, 1, 2, ..., n-1\}$, let $C_s = \{s, sq, sq^2, ..., sq^{l_s-1}\}$ be the q cyclotomic coset of s modulo n and let β be a primitive n-th root of unity. It is known that (see the appendix) the minimal polynomial $m_s(x)$ of β^s

is given by

$$m_s(x) = \prod_{j \in C_s} \left(x - \beta^j\right)$$

And hence the factorization of $x^n - 1$ into irreducible factors over $\mathbb{F}_q$ is given by

$$x^n - 1 = \prod_{s \in P_{n,q}} m_s(x).$$

where $P_{n,q}$ is the set of the coset leaders of all cyclotomic cosets.

Definition 2.1 *The cyclotomic coset C_s is said to be reversible if and only if $C_{n-s} = C_s$ if and only if $n - s$ is in C_s.*

Lemma 2.6 *[29] If C_1 is reversible then C_s is reversible for all s in $P_{n,q}$.*

Proof. Assume that the cyclotomic coset C_1 is reversible. Then there exists a $k, 1 \leq k \leq ord_n(q)$, such that $q^k \equiv -1 \mod n$. This means that $sq^k \equiv -s \mod n$, and hence $C_s = C_{-s}$. □

Lemma 2.7 *[30] The minimal polynomial $m_s(x)$ is self reciprocal if and only if the cyclotomic coset associated C_s is reversible.*

Now, using the algebraic properties of integers given in Section 2.1, and according to the decomposition of n into products of powers of prime numbers, we give some new constructions of LCD codes over the chain ring R given in [10].

Theorem 2.4 *Let R be a finite chain ring with residue field $\mathbb{F}_q$, and p^k an odd prime power coprime to q. Then, **all free cyclic** codes of length p^k over R are LCD if and only if $ord_p(q)$ is even.*

Proof. Let p^k be an odd prime power coprime to q. From Lemma 2.2 we have that a cyclic code C is an LCD code if it is generated by a self reciprocal polynomial $g(x)$ which devide $x^{p^k} - 1$. On the other hand, Lemma 2.5 shows that if $ord_p(q)$ is even, then there exits l in $\mathbb{N}^*$, such that $q^l \equiv -1 \mod p^k$, which means that -1 is in the cyclotomic coset C_1. Hence, $C_1 = C_{-1} \mod p^k$. In other words, C_1 is reversible, and so all the other cyclotomic cosets are also reversible by Lemma 2.6. Therefore, all divisor of $x^{p^k} - 1$ are self reciprocal.

Conversely, assume that all free cyclic codes of length p^k are LCD, then all divisors of $x^{p^k} - 1$ are self reciprocal. Hence all cyclotomic cosets are reversible and, in particular, the

cyclotomic coset C_1 is reversible. This means that there is an integer l such that $q^l \equiv -1 \mod p^k$. Finally, Lemma 2.5 shows that in such case $ord_p(q)$ is even. □

Example 2.2 *Let $R = \mathbb{Z}_9$ with residue field $\mathbb{F}_3$ and $n = 49$. We have $ord_7(3) = 6$ and the factorization into irreducible polynomials is given by:*

$$\begin{aligned} x^{49} - 1 &= (x+8)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^{42} + x^{35} + x^{28} + x^{21} + x^{14} + x^7 + 1) \\ &= g_1(x)g_2(x)g_3(x) \end{aligned}$$

So, all codes generated by $\left\langle \prod_{i=1}^{3} g_i^{k_i}(x) \right\rangle$, where $0 \leq k_i \leq 1$, are LCD codes over $\mathbb{Z}_9$ of length 49.

Example 2.3 *Let $R = \mathbb{Z}_4$, $n = 17$, we have*

$$\begin{aligned} x^{17} - 1 &= (x+3)(x^8 + 2x^6 + 3x^5 + x^4 + 3x^3 + 2x^2 + 1)(x^8 + x^7 + 3x^6 + 3x^4 + 3x^2 + x + 1) \\ &= g_1(x)g_2(x)g_3(x), \end{aligned}$$

where $g_1(x), g_2(x)$ and $g_3(x)$ are irreducible polynomials over $\mathbb{Z}_4$. Since $ord_{17}(2) = 8$, then all cyclic codes generated by polynomials of the form $\left\langle \prod_{i=1}^{3} g_i^{k_i}(x) \right\rangle$, with $0 \leq k_i \leq 1$, are LCD codes.

Lemma 2.8 *Let q and n be positive integers coprime such that n is odd and the irreducible factorization of n is given by $n = p_1^{k_1} p_2^{k_2} ... p_t^{k_t}$, with $ord_{p_i}(q)$ even for $1 \leq i \leq t$. Let a_i be the positive integers for which $2^{a_i} \| ord_{p_i}(q)$, with $1 \leq i \leq t$. Then we have*

$$a_1 = a_2 = ... = a_t = a \text{ if and only if there exists } l \text{ in } \mathbb{N}^*, \text{ such that } q^l \equiv -1 \mod n.$$

Further, $2^a \| ord_n(q)$.

Proof. Assume that $a_1 = a_2 = ... = a_t = a$. Recall that if $2^a \| ord_{p_i}(q)$ then $2^a \| ord_{p_i^{k_i}}(q)$ for all k_i in $\mathbb{N}$. Thus, we can write $ord_{p_i^{k_i}}(q) = 2^a m_i$, with m_i an odd integer for $1 \leq i \leq t$. From Lemma 2.5 and Corollary 2.1, we deduce that there exits $l_i \in \mathbb{N}^*$, such that $q^{l_i} \equiv -1 \mod p_i^{k_i}$. The smallest integer l_i' satisfying this congruence is $l_i' = \frac{1}{2} ord_{p_i^{k_i}}(q) = 2^{a-1} m_i$, for $1 \leq i \leq t$. Let $m = \prod_{i=1}^{t} m_i$. Since m is odd, we get $q^{2^{a-1}m} \equiv -1 \mod p_i^{k_i}$. Hence,

$p_i^{k_i} \mid q^{2^{a-1}m} + 1$ for all $1 \leq i \leq t$. Therefore, $n = \prod_{i=1}^{t} p_i^{k_i} \mid q^{2^{a-1}m} + 1$. In other words $q^{2^{a-1}m} \equiv -1 \mod n$.

Conversely, assume there is an integer l such that $q^l \equiv -1 \mod n$. Without loss of generality, we suppose $a_1 \neq a_2$ such that $2^{a_1} \| ord_{p_1}(q)$ and $2^{a_2} \| ord_{p_2}(q)$. Write $ord_{p_1}(q) = 2^{a_1} m_1$ and $ord_{p_2}(q) = 2^{a_2} m_2$ for odd integers m_1 and m_2. We have

$$q^l \equiv -1 \mod n \text{ implies } q^l \equiv -1 \mod p_i \text{ which give } q^{2l} \equiv 1 \mod p_i, \text{ for } 1 \leq i \leq t.$$

Hence, $2^{a_1} m_1 \mid 2l$ and $2^{a_2} m_2 \mid 2l$. Since both of a_1 and a_2 are not null, we get $2^{a_1 - 1} m_1 \mid l$ and $2^{a_2 - 1} m_2 \mid l$. Since $a_1 \neq a_2$, we can suppose that $a_1 \rangle a_2$. Consequently, $2^{a_2} m_2 \mid l$. In other words, $q^l \equiv 1 \mod p_2$, which is a contradiction.
Further, we have $n = p_1^{k_1} p_2^{k_2} ... p_t^{k_t}$, so

$$ord_n(q) = lcm(ord_{p_1^{k_1}}(q), ord_{p_2^{k_2}}(q), ..., ord_{p_t^{k_t}}(q)) = 2^a(2k+1), \text{ for some } k \in \mathbb{N}$$

Thus, $2^a \| ord_n(q)$. □

Theorem 2.5 *Let R be a finite chain ring with residue field $\mathbb{F}_q$ and n an odd integer coprime to q such that the factorization of n is given by $n = p_1^{k_1} p_2^{k_2} ... p_t^{k_t}$ with k_i in $\mathbb{N}^*$ for $1 \leq i \leq t$. Assume that the integers $ord_{p_i}(q), 1 \leq i \leq t$ are even and let a_i in $\mathbb{N}^*$ such that $2^{a_i} \| ord_{p_i}(q)$. Then **all free cyclic** codes of length n over R are LCD if and only if $a_1 = a_2 = ... = a_t = a$.*

Proof. Assume that there is a positive integer a such that $2^a \| ord_{p_i}(q), 1 \leq i \leq t$. From Lemma 2.8, there exists an integer l such that $q^l \equiv -1 \mod n$. This means that the q cyclotomic coset C_1 is reversible. Hence, all the other cyclotomic cosets are reversible by Lemma 2.6. Thus all divisor of the polynomial $x^n - 1$ are self reciprocal. Therefore, all free cyclic codes of length n over R are LCD.

Conversely, suppose that all free cyclic codes are LCD. So that all divisor of $x^n - 1$ are self reciprocal. We deduce that all cyclotomic cosets are reversible. In particular C_1 is reversible. Hence -1 is a power of $q \mod n$. The desired result follows immediately from Lemma 2.8. □

As a corollary we construct LCD codes of oddly even length.

Corollary 2.2 *Let R be a finite chain ring with residue field $\mathbb{F}_q$ such that q is an odd integer. Let n be an oddly even integer coprime to q such that the irreducible factorisation of n is*

given by $n = 2p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ *with* k_i *in* $\mathbb{N}^*$ *for* $1 \leq i \leq t$. *Assume that for all* $1 \leq i \leq t$ *the integers* $ord_{p_i}(q)$ *are even. Let* a_i *in* $\mathbb{N}^*$ *such that* $2^{a_i} \| ord_{p_i}(q)$. *Then* $a_1 = a_2 = ... = a_t = a$ *if and only if* ***all free cyclic*** *codes of length* n *over* R *are LCD.*

Proof. On the one hand and according to Lemma 2.8, we have $a_1 = a_2 = ... = a_t = a$ if and only if there exists l in $\mathbb{N}^*$, such that $\prod_{i=1}^{t} p_i^{k_i} \mid q^l + 1$. On the other hand, since q is an odd integer then $2 \mid q^l + 1$. Hence $n = 2\prod_{i=1}^{t} p_i^{k_i} \mid q^l + 1$. This means $q^l \equiv -1 \mod n$. Thus the cyclotomic coset C_1 is reversible, so according to Lemma 2.6 all the other cyclotomic cosets are reversibles. Hence, all free cyclic codes of length n are LCD codes.

Conversely, assume that all codes of length n are LCD. Then, the cyclotomic coset C_1 is reversible. Hence there is an integer l such that $q^l \equiv -1 \mod n$. It follows that $q^l \equiv -1 \mod \prod_{i=1}^{t} p_i^{k_i}$. Therefore, from Lemma 2.8, we get the desired result. □

Example 2.4 *Let* $R = \mathbb{Z}_{25}$, $n = 2646 = 2 \cdot 7^2 \cdot 3^3$. *We have* $ord_7(5) = 6$ *and* $ord_3(5) = 2$. *Since* $2 \| ord_7(5)$ *and* $2 \| ord_3(5)$, *so all free cyclic codes of length* 2646 *are LCD codes.*

In the remainder of this section, we provide necessary and sufficient conditions for cyclic codes to be LCD when the lengths are divisible by 4. The following lemmas are needed.

Lemma 2.9 *[35] The integer* 2^k *has primitive roots for* $k = 1$ *or* 2 *but not for* $k \geq 3$. *If* $k \geq 3$, *then* $\{(-1)^a 5^b;\ a = 0, 1$ *and* $0 \leq b \leq 2^{k-2}\}$ *constitutes a reduced residue system* $\mod 2^k$. *It follows that for* $k \geq 3$, *the group* $(\mathbb{Z}/2^k\mathbb{Z})^*$ *is not cyclic; it is the direct product of two cyclic groups, one of order* 2, *the other of order* 2^{k-2}

Lemma 2.10 *Let* q *be an odd prime power. Assume that there is an integer* l *in* $\mathbb{N}^*$ *such that* $q^l \equiv -1 \mod 2^k$ *with* $k \geq 2$. *Then* $q \equiv -1 \mod 2^k$. *Further, the integer* l *is odd and* $ord_{2^k}(q) = 2$.

Proof. Assume that there is an integer l such that $q^l \equiv -1 \mod 2^k$. If $k > 2$, then from Lemma 2.9, q can be writen as $q = (-1)^i \cdot 5^j$, with (i, j) in $\mathbb{N}^2$. Hence $q^l = (-1)^{il} \cdot 5^{jl} \equiv -1 \mod 2^k$, which requires that the integer il must be odd and that the order $ord_{2^k}(5)$ of the integer 5 which equal to 2^{k-2} must divide jl. Thus l is odd and then 2^{k-2} divides j. Write $j = 2^{k-2} \cdot j'$, we get

$$q = (-1)^i \cdot 5^j = (-1)^i \cdot 5^{2^{k-2}j'} \equiv (-1)^i \mod 2^k \equiv -1 \mod 2^k$$

For $k = 2$ and since q is odd we have clearly that $q^l \equiv -1 \mod 4$ leads to $q \equiv -1 \mod 4$. Hence l must be odd. Further, $q \equiv -1 \mod 2^k$ implies $ord_{2^k}(q) = 2$. □

Theorem 2.6 *Let R be a finite chain ring with residue field $\mathbb{F}_q$, and let n be a doubly even integer coprime to q such that the factorization of n is given by $n = 2^{k_0}p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ with $k_i \in \mathbb{N}$ for all $1 \leq i \leq t$ and $k_0 \geq 2$. Then the following statements are equivalent:*

i. $2\|ord_{p_i}(q)$ for $1 \leq i \leq t$ and $2^{k_0} \mid q + 1$.

ii. All free cyclic codes over R of length n are LCD codes.

Proof. Suppose that (i) is satisfied. Proving (ii) is equivalent to proving the existence of an integer l such that $q^l \equiv -1 \mod n$. The assumption $2\|ord_{p_i}(q)$ and Corollary 2.1 give that $ord_{p_i^{k_i}}(q) = 2m_i$, with m_i odd . Using Lemma 2.5, we get $q^{m_i} \equiv -1 \mod p_i^{k_i}$. Therefore, $q^{\prod_{i=1}^t m_i} \equiv -1 \mod p_i^{k_i}$. Hence, there exists $l = \prod_{i=1}^t m_i$ an odd integer such that $q^l \equiv -1 \mod \prod_{i=1}^t p_i^{k_i}$. On the other hand, $q \equiv -1 \mod 2^{k_0}$ implies $q^l \equiv -1 \mod 2^{k_0}$. Consequently $n = 2^{k_0}\prod_{i=1}^t p_i^{k_i}$ devide $q^l + 1$. Thus $q^l \equiv -1 \mod n$.

Conversely, assume that all free cyclic codes over R are LCD. This means that all cyclotomic cosets are reversible and, in particular, the cyclotomic coset C_1. Hence there exists l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod n$. Therefore

$$q^l \equiv -1 \mod p_i^{k_i}, \text{ for } 1 \leq i \leq t \tag{2.2}$$

and

$$q^l \equiv -1 \mod 2^{k_0} \tag{2.3}$$

Equation (2.2) and Lemma 2.5 give that $l = \frac{1}{2}(1 + 2m_i)ord_{p_i}(q)$, for some integers m_i. Equation (2.3) and Lemma 2.10 give $q \equiv -1 \mod 2^{k_0}$ and that the integer l must be odd. It follows that $2l = (1 + 2m_i)ord_{p_i}(q)$. Which means that $2\|ord_{p_i}(q)$. This completes the proof. □

Example 2.5 *Let $R = \mathbb{Z}_9$, $n = 3724 = 2^2 \cdot 7^2 \cdot 19$. We have $ord_7(3) = 6$, $ord_{19}(3) = 18$. Since $2\|6$, $2\|18$ and $2^2 \mid 4$, so all free cyclic codes of length $n = 3724$ are LCD codes.*

Chapter 3

Existence of Self Dual Cyclic Codes over Rings

Self dual cyclic codes constitute an important class of linear codes due to their rich algebraic structures and their wide applications. In this Chapter we focuse on the existence of self dual cyclic codes over finite chain rings of arbitrary length as a generalization of the results obtained in [6].

1 Generalities on Self Dual Codes over Finite Fields

Let C be a linear code over $\mathbb{F}_q$. Recall that C is said to be self dual if and only if $C = C^{\perp}$. It is well know that a linear code C and its dual $C^{\perp}$ verify the property $\dim C + \dim C^{\perp} = n$. Hence, the following result is obvious.

Lemma 1.1 *[58] Let $\mathbb{F}_q$ be a finite field. If C is a self dual code over $\mathbb{F}_q$ of length n, then n must be even.*

Of course, this is not true when the underlying alphabet is not a field. For example, the code $\{0, 2\}$ is a self dual code of length 1 over $\mathbb{Z}_4$.

Lemma 1.2 *[41] Let C be a linear code of length $n = 2n'$ over $\mathbb{F}_q$ with generator matrix $G = [I_{n'}|A]$. Then C is a self dual code if and only if $AA^T = -I_{n'}$.*

Proof. Assume that C is self dual code, then $C = C^{\perp}$. Hence G is also a generator matrix of $C^{\perp}$. Therefore $GG^T = AA^T + I_{n'} = 0$. □

Proposition 1.1 *[41] Let C be a self dual code of length $2n'$ over $\mathbb{F}_q$ with a standard*

generator matrix $G = [I_{n'}|A]$. *Then*

$$A^T G = [A^T| - I_{n'}]$$

is also a generator matrix of C.

Proof. Since C is self dual, then $AA^T = -I$ and $A^{-1} = -A^T$. Thus A^T is not singular. This implies that the rows of the matrix $A^T G$ form a basis of C and

$$A^T G = [A^T I_{n'}|A^T A] = [A^T| - I_{n'}]$$

□

Corollary 1.1 *[41] Let* $G = [I_{n'}|A]$ *and* $G' = [I_{n'}|A^T]$ *be generator matrices of self dual codes* C *and* C'*, respectively. Then* C *and* C' *are equivalent.*

Proof. From Proposition 1.1, we have that $A^T G = [A^T| - I_{n'}]$ generates also the code C and it is a permutation equivalent to $G' = [I_{n'}|A^T]$ □

For cyclic codes, it was shown in [36] that self dual cyclic codes of length n over $\mathbb{F}_q$ exist if and only if q is a power of 2 and n is even. When these conditions are met, there is always a self dual cyclic code with generator polynomial $x^{\frac{n}{2}} - 1$ called a trivial self dual code.

Proposition 1.2 *[36] A cyclic code* C *of length* n *is self dual if and only if* $g(x) = h^*(x)$*; where* $g(x)$ *is the generator polynomial of* C*,* $h(x)$ *is the check polynomial and* $h^*(x)$ *is the reciprocal polynomial of* $h(x)$.

Theorem 1.1 *[36] There exists at least one self dual cyclic code of length* $n = 2n'$ *over* $\mathbb{F}_q$ *if and only if* q *is a power of* 2.

Proof. Suppose that C is a self dual cyclic code of length $n = 2n'$ over $\mathbb{F}_q$. Then $\deg g = \deg h = \frac{n}{2} = n'$. As $g(x)h(x) = x^n - 1$, we have $g_0 h_0 = -1$, where g_0 and h_0 are the constant terms of $g(x)$ and $h(x)$, respectively. Therefore,

$$\begin{aligned} & g(x^{-1})h(x^{-1}) && = x^{-n} - 1 \\ \Rightarrow \quad & (g_0 g^*(x))(h_0 h^*(x)) && = 1 - x^n \\ \Rightarrow \quad & g^*(x)h^*(x) && = x^n - 1 \end{aligned} \tag{3.1}$$

By Proposition 1.2, we have

$$\begin{aligned} g(x) &= h^*(x) \\ \Rightarrow \quad x^{\frac{n}{2}} g(x^{-1}) &= h_0^{-1} h(x) \\ \Rightarrow \quad g_0 g^*(x) &= h_0^{-1} h(x) \\ \Rightarrow \quad g^*(x) &= -h(x) \end{aligned} \tag{3.2}$$

Therefore, we have $g^*(x)h^*(x) = -g(x)h(x) = -(x^n - 1)$. Then by equations (3.1) and (3.2), we have

$$x^n - 1 = -(x^n - 1)$$

Hence, the following identity holds:

$$2(x^n - 1) = 0$$

which implies that the characteristic of the field $\mathbb{F}_q$ is 2, i.e., q is a power of 2. Conversely, if q is a power of 2 , then the polynomial $x^n - 1$ can be written as follows over $\mathbb{F}_q$:

$$x^n - 1 = x^n + 1 = (x^{n'} + 1)^2$$

Hence, we get the trivial self dual cyclic code with generator polynomial $x^{n'} + 1$. □

Assume that $q = 2^m$ and $n = 2^a n'$ such that n' is an odd integer. Each cyclic code over $\mathbb{F}_{2^m}$ is uniquely determined by its generator polynomial, a monic divisor of $x^n - 1$ over $\mathbb{F}_{2^m}$. In order to describe the generator polynomials of $[n, \frac{n}{2}, d]$ self dual cyclic codes, we need to know the factorization of the polynomial $x^n - 1$ over $\mathbb{F}_{2^m}$. The polynomial $x^{n'} - 1$ can be factorized into distinct irreducible polynomials as follows:

$$x^{n'} - 1 = f_1(x)f_2(x)...f_s(x)h_1(x)h_1^*(x)...h_t(x)h_t^*(x)$$

where $f_i(x), (1 \leq i \leq s)$ are monic irreducible self reciprocal polynomials over $\mathbb{F}_{2^m}$ while $h_j(x)$ and its reciprocal polynomial $h_j^*(x), (1 \leq j \leq t)$ are both monic irreducible polynomials over $\mathbb{F}_{2^m}$. Therefore

$$x^n - 1 = (x^{n'} - 1)^{2^a} = f_1(x)^{2^a} f_2(x)^{2^a} ... f_s(x)^{2^a} h_1(x)^{2^a} h_1^*(x)^{2^a} ... h_t(x)^{2^a} h_t^*(x)^{2^a} \tag{3.3}$$

Theorem 1.2 *[36] Let $x^n - 1$ be factorized as in Equation (3.3). A cyclic code C of length*

n is self dual over $\mathbb{F}_{2^m}$ if and only if its generator polynomial is of the form

$$f_1(x)^{2^a-1}f_2(x)^{2^a-1}...f_s(x)^{2^a-1}h_1(x)^{\beta_1}h_1^*(x)^{2^a-\beta_1}...h_t(x)^{\beta_t}h_t^*(x)^{2^a-\beta_t} \tag{3.4}$$

where $0 \leq \beta_i \leq 2^a$ for each $1 \leq i \leq t$.

Proof. Let C be a cyclic code of length n over $\mathbb{F}_{2^m}$ and let $g(x)$ be its generator polynomial. We need to show that C is self dual if and only if $g(x)$ is of the form as in Equation (3.4). Since the generator polynomial $g(x)$ of a cyclic code of length n is monic and divides $x^n - 1$, we may assume that

$$g(x) = f_1(x)^{\alpha_1}f_2(x)^{\alpha_2}...f_s(x)^{\alpha_s}h_1(x)^{\beta_1}h_1^*(x)^{\gamma_1}...h_t(x)^{\beta_t}h_t^*(x)^{\gamma_t}$$

where $0 \leq \alpha_i \leq 2^a$ for each $1 \leq i \leq s$, and $0 \leq \beta_j, \gamma_j \leq 2^a$ for each $1 \leq j \leq t$. Then the check polynomial is

$$h(x) = f_1(x)^{2^a-\alpha_1}f_2(x)^{2^a-\alpha_2}...f_s(x)^{2^a-\alpha_s}h_1(x)^{2^a-\beta_1}h_1^*(x)^{2^a-\gamma_1}...h_t(x)^{2^a-\beta_t}h_t^*(x)^{2^a-\gamma_t}$$

Hence

$$h^*(x) = f_1(x)^{2^a-\alpha_1}f_2(x)^{2^a-\alpha_2}...f_s(x)^{2^a-\alpha_s}h_1^*(x)^{2^a-\beta_1}h_1(x)^{2^a-\gamma_1}...h_t^*(x)^{2^a-\beta_t}h_t(x)^{2^a-\gamma_t}$$

since $f_i(x)(1 \leq i \leq s)$ are self-reciprocal while $h_j(x)$ and $h_j^*(x)(1 \leq j \leq t)$ are reciprocal polynomial pairs over $\mathbb{F}_{2^m}$. By Proposition 1.2, C is self dual if and only if $g(x) = h^*(x)$, i.e.,

$$\begin{cases} \alpha_i = 2^a - \alpha_i & \text{for each} \quad 1 \leq i \leq s \\ \gamma_i = 2^a - \beta_j & \text{for each} \quad 1 \leq j \leq t \end{cases}$$

or, equivalently,

$$\begin{cases} \alpha_i = 2^{a-1} & \text{for each} \quad 1 \leq i \leq s \\ \gamma_i = 2^a - \beta_j & \text{for each} \quad 1 \leq j \leq t \end{cases}$$

□

Example 1.1 *Consider the case: $n = 14$ and $q = 2$. Now $n' = 7$. The factorization of $x^{14} + 1$ over $\mathbb{F}_2$ is*

$$x^{14} + 1 = (x + 1)^2(x^3 + x + 1)^2(x^3 + x^2 + 1)^2$$

It is observed that the polynomial $x+1$ is a self reciprocal polynomial and x^3+x+1 is the reciprocal polynomial of x^3+x^2+1 over $\mathbb{F}_2$. There are 3 binary self dual cyclic codes of length 14 with the following generator polynomials respectively:

$$\begin{aligned}(x+1)(x^3+x+1)^2 &= x^7+x^6+x^3+x^2+x+1;\\ (x+1)(x^3+x+1)(x^3+x^2+1) &= x^7+1;\\ (x+1)(x^3+x^2+1)^2 &= x^7+x^6+x^5+x^4+x+1:\end{aligned}$$

The one with generator polynomial x^7+1 is the trivial self dual cyclic code.

2 Existence of Self Dual Cyclic codes over Finite Rings

2.1 Generalities of Self Dual Codes over Finite Frobenius Rings

We start this part with the following Lemmas which are standard tools to determine when self dual codes exist.

Lemma 2.1 *[23] Let R be a finite commutative Frobenius ring. If $|R|$ is not a square and there exists a self dual code C of length n, then n must be even.*

Proof. We know from Corollary 2.1 that $|C||C^{\perp}| = |R|^n$. This gives that $|C| = |R|^{\frac{n}{2}}$. If $|R|$ is not a square, then $|C|$ is not an integer, which is a contradiction. Hence n must be even. □

Lemma 2.2 *[23] Let R be a finite commutative Frobenius ring and let C and D be self dual codes of length n and m respectively. Then the direct product $C \times D$ is a self dual code of length $n+m$ over R.*

Proof. Let $(v,w),(v',w') \in C \times D$. Then

$$(v,w).(v',w') = (v.v') + (w.w') = 0+0 = 0$$

This gives that $C \times D$ is a self orthogonal code. Since

$$|C \times D| = |C|.|D| = |R|^{\frac{n}{2}}.|R|^{\frac{m}{2}} = |R|^{\frac{n+m}{2}}$$

Therefore $C \times D$ is a self-dual code of length $n+m$.

□

Lemma 2.3 *[23] Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$ such that $R/\mathfrak{m}$ is a field of characteristic p, where p is an odd prime. Let $S_i = R/\mathfrak{m}^i$. If there exists α in S_i with $\alpha^2 = -1$, then there exists β in S_{i+1} with $\beta^2 = -1$.*

Proof. Let α in S_i with $\alpha^2 = -1$. Let $\beta = \alpha + s_i$ be an element in S_{i+1}, where $s_i + \mathfrak{m}^{i+1}$ is in $\mathfrak{m}^i/\mathfrak{m}^{i+1}$. Then we have

$$\begin{aligned}(\alpha + s_i)^2 &\equiv \alpha^2 + 2\alpha s_i + s_i^2 \mod \mathfrak{m}^{i+1}\\ &\equiv \alpha^2 + 2\alpha s_i \mod \mathfrak{m}^{i+1}\\ &\equiv \delta - 1 + 2\alpha s_i \mod \mathfrak{m}^{i+1}\end{aligned}$$

for some δ in $\mathfrak{m}^i$ since $\alpha^2 = -1$ is in S_i. Next we show that there exists an element s_i such that $\delta - 1 + 2\alpha s_i$ is in S_{i+1}. We have

$$\delta - 1 + 2\alpha s_i = -1 \mod \mathfrak{m}^{i+1} \Leftrightarrow \delta = -2\alpha s_i \mod \mathfrak{m}^{i+1}$$

Since p is odd, 2 is relatively prime to p. Hence the element 2 is a unit. Since $\alpha^2 = -1 \mod \mathfrak{m}$, this implies that α is a unit in $R/\mathfrak{m}$. Let $s_i = -\delta(2\alpha)^{-1}$. Then $s_i + \mathfrak{m}^{i+1}$ is in $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ and $\beta^2 = (\alpha + s_i)^2 \equiv \delta - 1 + 2\alpha s_i = -1$ is in S_{i+1} since elements of $\mathfrak{m}^{i+1}$ are 0 in S_{i+1}. □

Corollary 2.1 *[23] Let R be a finite local commutative Frobenius ring with characteristic congruent to* $1 \mod 4$. *Then there exists an α in R with $\alpha^2 = -1$.*

Proof. The field $R/\mathfrak{m}$ has characteristic $1 \mod 4$ and hence has a square root of -1. Then, by induction using Lemma 2.3, we have the result. □
Notice that this result does not necessarily hold when $R/\mathfrak{m}$ has characteristic 2. For example, $\mathbb{Z}_4$ is a local ring and $\mathbb{Z}_4/\langle 2\rangle \cong \mathbb{F}_2$, which has a square root of -1 , but the ring $\mathbb{Z}_4$ does not. We can use this result to get the following theorem

Theorem 2.1 *[23] Let R be a finite local commutative Frobenius ring with characteristic congruent to* $1(\mod 4)$. *Then there exist self dual codes for all even lengths over R.*

Proof. By Corollary 2.1, the ring R has an element α with $\alpha^2 = -1$. Then the code generated by $(1, \alpha)$ is a self dual code of length 2. Then, by applying Lemma 2.2, inductively,

we have the result. □

Lemma 2.4 *[23] Let R be a finite local commutative Frobenius ring with maximal ideal $\mathfrak{m}$ such that $R/\mathfrak{m}$ is a field of characteristic p, where p is an odd prime. Let $S_i = R/\mathfrak{m}^i$. If there exist α, β in S_i with $\alpha^2 + \beta^2 = -1$, then there exist γ, δ in S_{i+1} with $\gamma^2 + \delta^2 = -1$.*

Corollary 2.2 *[23] Let R be a finite local commutative Frobenius ring with characteristic congruent to $3(\mod 4)$. Then there exist α, β in R with $\alpha^2 + \beta^2 = -1$.*

Proof. The field $R/\mathfrak{m}$ has characteristic $3(\mod 4)$ and hence there exist γ, δ with $\gamma^2+\delta^2 = -1$. Then by induction using Lemma 2.4 we have the result □
This result leads naturally to the following theorem.

Theorem 2.2 *[23] Let R be a finite local commutative Frobenius ring with characteristic congruent to $3(\mod 4)$. Then there exist self dual codes for all lengths congruent to $0(\mod 4)$ over R.*

Proof. By Corollary 2.2, the ring R has elements α, β with $\alpha^2 + \beta^2 = -1$. Then the code $C = \langle (1, 0, \alpha, \beta), (0, 1, -\beta, -\alpha) \rangle$ is a self-dual code of length 4. Then, by applying Lemma 2.2 inductively, we have the result. □

2.2 Existence of Self Dual Cyclic Codes over Chain rings

Let R be a finite chain ring with maximal ideal $\langle \gamma \rangle$, residue field $\mathbb{F}_q$ and nilpotency index e of the maximal ideal $\langle \gamma \rangle$, (Recall that R can be considered as a finite local frobenius ring). We have $|R| = |\mathbb{F}_q|^e$ and if C is a code of length n over R, then $|C||C^\perp| = |R|^n$.

Theorem 2.3 *[23] If e is even, then $\mathfrak{a} = \left\langle \gamma^{\frac{e}{2}} \right\rangle$ is a self dual code of length 1, called trivial self dual code.*

Proof. We have that $\left\langle \gamma^{\frac{e}{2}} \right\rangle \left\langle \gamma^{\frac{e}{2}} \right\rangle = \langle \gamma^e \rangle = 0$ and so $\mathfrak{a} \subseteq \mathfrak{a}^\perp$. Assume that $\mathfrak{a} \neq \mathfrak{a}^\perp$. Then $\mathfrak{a}^\perp = \langle \gamma^j \rangle$ with $j < \frac{e}{2}$. Then $\left\langle \gamma^{\frac{e}{2}} \right\rangle \langle \gamma^j \rangle = 0$ contradicting that e is minimal. Therefore $\mathfrak{a} = \mathfrak{a}^\perp$ and is a self dual code of length 1. □
The following results give necessary and sufficient conditions for the existence of non trivial self dual cyclic codes of length n over R .

Corollary 2.3 *[23] If e is even, then there exists self dual codes of length n for all n.*

Proof. The result follows immediately by applying Lemma 2.2 to the self dual code of length 1 in Theorem 2.3. □

Proposition 2.1 *[22] Let C be a cyclic code of length n over R. Assume that $x^n - 1 = F_0F_1...F_{e-1}F_e$ and let $C = \left\langle \hat{F}_1, \gamma\hat{F}_2, ..., \gamma^{e-1}F_e \right\rangle$ be a cyclic code (as in Theorem 2.5 in Chapter 1) such that $\hat{F}_i(x) = \dfrac{x^n - 1}{F_i(x)}$. Then C is self dual if and only if F_i is an associate of F_j^* for all i, j in $\{0, 1, ..., e\}$ such that $i + j \equiv 1 \mod (e + 1)$.*

Cyclic codes of length n which is not divisible by the characteristic of R are called simple root cyclic codes. Batoul et al. [6] proved that there are no simple root self dual cyclic codes over finite chain rings when the nilpotency index of the generator of the maximal ideal is odd.

Theorem 2.4 *[6] If e is odd, then there are no non trivial self dual cyclic codes of length n over R when* $\gcd(n, q) = 1$.

Proof. If $q = 2^k$, then $\gcd(n, q) = 1$ and so n must be odd. Let C be a non trivial cyclic code of length n over R, so that there exist monic coprime polynomials $F_0, F_1, .., F_{e-1}, F_e$ such that $x^n - 1 = F_0F_1...F_{e-1}F_e$ and $C = \left\langle \hat{F}_1, \gamma\hat{F}_2, ..., \gamma^{e-1}F_e \right\rangle$. If C is self-dual, then from Proposition 2.1, F_i is an associate of F_j^* for i, j in $\{0, 1, ..., e\}$ and $i + j \equiv 1 \mod (e + 1)$. Hence $F_i = \xi F_j^*$ for some unit ξ in R. Since e is odd, then $i + i = 2 \not\equiv 1 \mod (e + 1)$ and $F_i \neq F_i^*$ for all $0 \leq i \leq e$. Therefore

$$x^n - 1 = F_0F_0^*F_1F_1^*...F_{\frac{e+1}{2}}F_{\frac{e+1}{2}}^*$$

Thus none of the F_i are self reciprocal. On the other hand, the polynomial $(x-1)$ is a factor of $x^n - 1$, so there is an $0 \leq i_0 \leq e$ such that $F_{i_0} = (x - 1)g(x)$ for some polynomial $g(x)$. Hence

$$F_{i_0}^* = (x - 1)^* g(x)^* = (x - 1)g^*(x) = F_{1-i_0} \mod (1+e)$$

which is impossible since the F_i are coprime for all $0 \leq i \leq e$, and $x^n - 1$ has no repeated roots since $\gcd(n, q) = 1$.

□

Throughout the rest of this section, we assume that e is even.

Theorem 2.5 *[22] There exists a non trivial self dual cyclic code over R if and only if there exists a basic irreducible factor $f(x)$ in $R[x]$ of $x^n - 1$ such that $f(x)$ and $f^*(x)$ are*

not associate.

Theorem 2.6 *[6] Non trivial self dual cyclic codes of length n over R exist if and only if for all i in $\mathbb{N}$, we have $q^i \not\equiv -1 \mod n$.*

Proof. Recall that if $f(x)$ is a monic basic irreducible polynomial which divides x^n-1, then $\overline{f(x)}$ is the minimal irreducible polynomial over $\mathbb{F}_q[x]$. And hence there exists a cyclotomic coset C_u associated with $\overline{f(x)}$. Therefore $f(x) = \prod_{i\in C_u}(x-\alpha^i)$, where α is a primitive n^{th} root of unity. The reciprocal polynomial of $\overline{f(x)}$ is the polynomial

$$\overline{f(x)}^* = (\prod_{i\in C_u}(x-\alpha^i))^* = x^r \prod_{i\in C_u}(x^{-1}-\alpha^i) = \prod_{i\in C_{n-u}}(x-\alpha^i)$$

Since we have $\overline{f(x)}^* = \overline{f^*(x)}$, then by Theorems 2.5, a non trivial self dual cyclic code exists if and only if there is a basic irreducible polynomial $f(x)$ which is a factor of x^n-1 such that $f(x)$ and $f^*(x)$ are not associate. We show that this can occur if and only if $q^i \not\equiv -1 \mod n$ for all positive integers i.
Assume now that $q^i \not\equiv -1 \mod n$ for all positive integers i, then $C_1 \neq C_{-1}$. Hence $f(x) \neq f(x)^*$ where $f(x) = \prod_{i\in C_1}(x-\alpha^i)$. Hence the code $\langle f(x)g(x), \gamma^{\frac{e}{2}} f(x)f^*(x)\rangle$ is a non trivial self dual code where $f(x)f^*(x)g(x) = x^n-1$. **Conversely**, if a non trivial self dual cyclic code exists then by Theorem 2.5 there exists a factor $f(x)|x^n-1$ with $f(x) \neq f^*(x)$. Hence $C_u \neq C_{-u}$, and then $C_1 \neq C_{-1}$ where $\overline{f(x)} = \prod_{i\in C_u}(x-\alpha^i)$. Therefore $q^i \not\equiv -1 \mod n$ for all positive integers i. □

In [6], the authors introduce a simple criterion for the existence of non trivial self dual cyclic codes over R when the length of the code is an odd prime power and the nilpotency index of the maximal ideal of the ring is even.

Lemma 2.5 *[6] If n is an odd prime power coprime with q, then there exists a non trivial self dual cyclic code of length n over R if and only if $ord_n(q)$ is odd.*

Using Lemmas 2.8 and 2.6 in Chapter 2, we will generalize this result and provide conditions on the existence of non trivial self dual codes of arbitrary length over R.

Theorem 2.7 *Let n be an odd integer coprime to q such that the factorization of n is given by $n = p_1^{k_1}p_2^{k_2}...p_t^{k_t}$, with k_i in $\mathbb{N}^*$ for all $1 \leq i \leq t$ and $t \geq 2$. Denote by a_i the integers of $\mathbb{N}$ such that $2^{a_i} \| ord_{p_i}(q)$, for all $1 \leq i \leq t$. Then non trivial self dual cyclic codes of length n exist if and only if one of the following statements holds:*

(i) There exist at least $i_0,\ 1 \leq i_0 \leq t$ *such that* $a_{i_0} = 0$.

(ii) For all $1 \leq i \leq t$, $a_i \neq 0$, *and there exist two distinct integers* i_1, i_2 *with* $1 \leq i_1, i_2 \leq t$ *such that* $a_{i_1} \neq a_{i_2}$.

Proof. Assume that there exists $i_0,\ 1 \leq i_0 \leq t$ such that $a_{i_0} = 0$. This means that $ord_{p_{i_0}}(q)$ is odd. Lemma 2.5 garanties that there is no integer l such that $q^l \equiv -1 \mod p_{i_0}$. Hence, for all i in $\mathbb{N}$ we have $q^i \not\equiv -1 \mod n$. Thus, from Lemma 2.6, a non trivial self dual cyclic code over R exists.
Assume now that (ii) is satisfied. Therefore, all $ord_{p_i}(q)$, for $1 \leq i \leq t$, are even. Lemma 2.8 shows that if there exist two distinct integers i_1, i_2, $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$, then there is no integer l such that $q^l \equiv -1 \mod n$. Hence, a non trivial self dual codes over R exist. Conversely, assume that non trivial self dual codes exist. So for any integer l, $q^l \not\equiv -1 \mod n$. We need to prove that either there exists i_0 such that $a_{i_0} = 0$ or every a_i is different to zero and at least two of them are distincts. Suppose that for all $1 \leq i \leq t,\ a_i \neq 0$. This implies that $ord_{p_i}(q)$ is even for all $1 \leq i \leq t$. Since there is no integer l such that $q^l \equiv -1 \mod n$, by Lemma 2.8, we have that there exists i_1, i_2 with $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$. □

Example 2.1 *Let* $R = \mathbb{Z}_4$ *and* $n = 3 \cdot 5$, *we have* $ord_3(2) = 2$ *and* $ord_5(2) = 4$, *and hence* $2^1 \| ord_3(2)$ *and* $2^2 \| ord_5(2)$. *So there exist non trivial self dual codes over* $\mathbb{Z}_4$ *of length* 15. *The factorization of* $x^{15} - 1$ *over* $\mathbb{Z}_4$ *is given by*

$$x^{15} - 1 = f_1(x)f_2(x)f_3(x)f_4(x)f_4^*(x),$$

where

$f_1 = x+3,\ f_2 = x^2+x+1,\ f_3 = x^4+x^3+x^2+x+1, f_4 = x^4+2x^2+3x+1$ *and* $f_4^* = x^4+3x^3+2x^2+1$.

Let $g(x) = f_1(x)f_2(x)f_3(x)$ *and* $h(x) = f_4(x)$. *Then the following codes*

$$\langle g(x)h(x), 2h(x)h^*(x)\rangle \ \text{ and } \ \langle g(x)h^*(x), 2h(x)h^*(x)\rangle$$

are non trivial self dual cyclic codes of length 15.

Example 2.2 *Let* $R = \mathbb{Z}_{16}$ *and* $n = 21$. *We have* $ord_3(2) = 2$ *and* $ord_7(2) = 3$. *Then, there exist non trivial self dual cyclic codes over* R *of length* 21. *The factorization of* $x^{21} - 1$ *over*

R is equal to

$$x^{21} - 1 = f_1(x)f_2(x)f_3(x)f_3^*(x)f_4(x)f_4^*(x),$$

where

$$f_1(x) = x - 1, f_2(x) = x^2 + x + 1, f_3(x) = x^3 + 6x^2 + 5x - 1, f_3^*(x) = x^3 + 11x^2 + 10x - 1,$$

$$f_4(x) = x^6 - 6x^5 - x^4 - x^2 + 5x + 1. \text{ and } f_4^*(x) = x^6 + 5x^5 - x^4 - x^2 + 10x + 1$$

Let $x^{21} - 1 = g(x)h(x)h^*(x)$, where $g(x) = f_1(x)f_2(x)$ is a self reciprocal polynomial and $h(x) = f_3(x)f_4(x)$. Thus, for example, the code $\langle g(x)h(x), 2h(x)h^*(x)\rangle$ is self dual.

We give now the necessary and sufficient conditions for the existence of non trivial self dual cyclic codes when the length is oddly even.

Theorem 2.8 *Let n be an oddly even integer coprime to q such that the irreducible factorization of n is given by $n = 2.p_1^{k_1}p_2^{k_2}...p_t^{k_t}$, where $t \geq 2$, and k_i in $\mathbb{N}^*$ for all $1 \leq i \leq t$. Let $a_i \in \mathbb{N}$ such that $2^{a_i} \| ord_{p_i}(q)$. Then a non trivial self dual cyclic code of length n exists if and only if one of the following statements holds:*

(i) There exists at least $i_0, 1 \leq i_0 \leq t$ such that $a_{i_0} = 0$.

(ii) For all $1 \leq i \leq t$, $a_i \neq 0$, there exist two distincts integers i_1, i_2 with $1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$.

Proof. Since $gcd(n, q) = 1$, then q must be an odd integer. Hence for all l in $\mathbb{N}^*$ we have $2 \mid q^l + 1$. If $a_1 = a_2 = ... = a_t = a$, and $a \neq 0$, by Lemma 2.8, we know that there exists l in $\mathbb{N}^*$ such that $q^l \equiv -1 \mod \prod_{i=1}^t p_i^{k_i}$. Therefore, $q^l \equiv -1 \mod n$. Hence, there do not exist non trivial self dual codes on R by Lemma 2.6.

Conversely, assume (i) holds. Thus, from Lemma 2.5, there is no integer l such that $q^l \equiv -1 \mod p_{i_0}$. Hence, there does not exist an integer l in $\mathbb{N}$, such that $q^l \equiv -1 \mod n$. This proves by Lemma 2.6 that non trivial self dual cyclic codes over R exist.
Assume now that (ii) is satisfied. By Lemma 2.8, if there exist two distinct integers $i_1, i_2, 1 \leq i_1, i_2 \leq t$ such that $a_{i_1} \neq a_{i_2}$, then there is no integer l such that $q^l \equiv -1 \mod \prod_{i=1}^t p_i^{k_i}$. Even if we have 2 divides $q^l + 1$ for all $l \in \mathbb{N}^*$, we cannot find any integr l such that $q^l \equiv -1 \mod n$. Hence by Lemma 2.6, non trivial self dual codes over R exist.

□

Example 2.3 *Let $R = \mathbb{Z}_9$ and $n = 70 = 2 \cdot 5 \cdot 7$. We have $ord_5(3) = 4$, $ord_7(3) = 6$, and hence $2 \| ord_7(3)$ and $2^2 \| ord_5(3)$. So there exist non trivial self dual cyclic codes of length 70 over $\mathbb{Z}_9$. The factorization of $x^{70} - 1$ over $\mathbb{Z}_9$ is given by*

$$x^{70} - 1 = f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x)f_7(x)f_7^*(x)f_8(x)f_8^*(x),$$

where

$$\begin{aligned}
f_1(x) &= x + 1 \\
f_2(x) &= x + 8, \\
f_3(x) &= x^4 + x^3 + x^2 + x + 1, \\
f_4(x) &= x^4 + 8x^3 + x^2 + 8x + 1, \\
f_5(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\
f_6(x) &= x^6 + 8x^5 + x^4 + 8x^3 + x^2 + 8x + 1, \\
f_7(x) &= x^{12} + 4x^{10} + 6x^9 + 8x^8 + x^7 + 3x^6 + 4x^5 + 5x^4 + 7x^3 + 5x^2 + 8x + 1, \\
f_7^*(x) &= x^{12} + 8x^{11} + 5x^{10} + 7x^9 + 5x^8 + 4x^7 + 3x^6 + x^5 + 8x^4 + 6x^3 + 4x^2 + 1 \\
f_8(x) &= x^{12} + 4x^{10} + 3x^9 + 8x^8 + 8x^7 + 3x^6 + 5x^5 + 5x^4 + 2x^3 + 5x^2 + x + 1. \\
f_8^*(x) &= x^{12} + x^{11} + 5x^{10} + 2x^9 + 5x^8 + 5x^7 + 3x^6 + 8x^5 + 8x^4 + 3x^3 + 4x^2 + 1.
\end{aligned}$$

Let $x^{70} - 1 = g(x)h(x)h^*(x)$, where $g(x) = f_1(x)f_2(x)f_3(x)f_4(x)f_5(x)f_6(x)$ is a self reciprocal polynomial and $h(x) = f_7(x)f_8(x)$. Thus, for example, the code $\langle g(x)h(x), 3h(x)h^*(x) \rangle$ is self dual.

Example 2.4 *Let $R = \mathbb{Z}_{49}$ and $n = 30 = 2 \cdot 3 \cdot 5$. We have $ord_3(7) = 1$, $ord_5(7) = 4$. We have that $ord_3(7)$ is odd, so there exist non trivial self dual cyclic codes of length 30 over $\mathbb{Z}_{49}$. The factorization of $x^{30} - 1$ over $\mathbb{Z}_{49}$ is given by*

$$x^{30} - 1 = f_1(x)f_2(x)f_2^*(x)f_3(x)f_3^*(x)f_4(x)f_5(x)f_6(x)f_7(x)f_7^*(x)f_8(x)f_8^*(x),$$

where

$$f_1(x) = x + 1, \qquad f_2(x) = x - 19 \qquad f_2^*(x) = x + 18$$
$$f_3(x) = x - 18, \qquad f_3^*(x) = x + 19 \qquad f_4(x) = x - 1,$$
$$f_5(x) = x^4 + x^3 + x^2 + x + 1, \qquad f_6(x) = x^4 - x^3 + x^2 - x + 1,$$
$$f_7(x) = x^4 - 19x^3 + 18x^2 + x - 19, \quad f_7^*(x) = x^4 + 18x^3 + 30x^2 + x + 18,$$
$$f_8(x) = x^4 - 18x^3 - 19x^2 - x + 18, \quad f_8^*(x) = x^4 + 19x^3 + 18x^2 + 48x + 30,$$

Let $x^{30}-1 = g(x)h(x)h^*(x)$, *where* $g(x) = f_1(x)f_4(x)f_5(x)f_6(x)$ *and* $h(x) = f_2(x)f_3(x)f_7(x)f_8(x)$. *Thus, for example, the code* $\langle g(x)h(x), 7h(x)h^*(x)\rangle$ *is self dual.*

We determine now, necessary and sufficient conditions for the existence of non trivial self dual cyclic codes over R for doubly even lengths.

Theorem 2.9 *Let* n *be a doubly even integer coprime to* q, *such that the irreducible factorisation of* n *is given by* $n = 2^{k_0}p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ *where* k_i *in* $\mathbb{N}^*$ *for all* $1 \leq i \leq t$ *and* $k_0 \geq 2$. *Let* a_i *in* $\mathbb{N}$ *such that* $2^{a_i} \| ord_{p_i}(q)$, *for* $1 \leq i \leq t$. *The following statements are equivalent:*

(i) Non trivial self dual cyclic codes over R *exist.*

(ii) There exits i, $1 \leq i \leq t$, *such that* $a_i \neq 1$ *or* $2^{k_0} \nmid (q+1)$.

Proof. Assume that (ii) is not satisfied. This implies that $a_1 = a_2 = ... = a_t = 1$ and $2^{k_0} \mid (q+1)$. Then from Lemma 2.8, there is an odd integer l such that $q^l \equiv -1 \mod \prod_{i=1}^{t} p_i^{k_i}$. Since $q \equiv -1 \mod 2^{k_0}$ and l is odd, it follows that $q^l \equiv -1 \mod 2^{k_0}$. Thus $q^l \equiv -1 \mod n$. Lemma 2.6 shows that non trivial self dual cyclic code over R does not exist.
Conversely, suppose that it does not exist any non trivial self dual cyclic codes of length n over R. Then, by Lemma 2.6, there exist some positive integer l such that $q^l \equiv -1 \mod n$. Thus, $q^l \equiv -1 \mod 2^{k_0}$. By Lemma 2.10, we have that $q \equiv -1 \mod 2^{k_0}$ and that the integer l is odd. On the other hand $q^l \equiv -1 \mod n$ implies again that $q^l \equiv -1 \mod p_i$. Lemma 2.5 gives that $2l = (1 + 2m_i)ord_{p_i}(q)$, for some integers m_i. Since l is odd, it follows that $2 \| ord_{p_i}(q)$. This means that $a_i = 1$ for each $1 \leq i \leq t$. □

Example 2.5 *Let* $R = \mathbb{Z}_{25}$ *and* $n = 84 = 2^2 \cdot 3 \cdot 7$. *We have that* $2^2 \nmid (5+1)$. *Then there are non trivial self dual cyclic codes of length* 84 *over* $\mathbb{Z}_{25}$. *The factorization of* $x^{84} - 1$ *over*

$\mathbb{Z}_{25}$ is given by

$$x^{84}-1=\prod_{i=1}^{10} f_i(x)\prod_{i=11}^{15} f_i(x)f_i^*(x),$$

where

$f_1(x)=x+1,$ $f_2(x)=x+24,$

$f_3(x)=x^2+x+1,$ $f_4(x)=x^2+24x+1,$

$f_5(x)=x^6+5x^5+22x^4+2x^3+22x^2+5x+1,$ $f_6(x)=x^6+20x^5+22x^4+23x^3+22x^2+20x+1,$

$f_7(x)=x^6+x^5+x^4+x^3+x^2+x+1,$ $f_8(x)=x^6+6x^5+8x^4+9x^3+8x^2+6x+1,$

$f_9(x)=x^6+24x^5+x^4+24x^3+x^2+24x+1,$ $f_{10}(x)=x^6+19x^5+8x^4+16x^3+8x^2+19x+1,$

$f_{11}(x)=x+7,$ $f_{11}^*(x)=x+18$

$f_{12}(x)=x^2+7x+24,$ $f_{12}^*(x)=x^2+18x+24$

$f_{13}(x)=x^6+10x^5+3x^4+11x^3+22x^2+10x+24,$ $f_{13}^*(x)=x^6+15x^5+3x^4+14x^3+22x^2+15x+24,$

$f_{14}(x)=x^6+17x^5+17x^4+12x^3+8x^2+17x+24,$ $f_{14}^*(x)=x^6+8x^5+17x^4+13x^3+8x^2+8x+24,$

$f_{15}(x)=x^6+7x^5+24x^4+18x^3+x^2+7x+24$ $f_{15}^*(x)=x^6+18x^5+24x^4+7x^3+x^2+18x+24$

Let $x^{84}-1=g(x)h(x)h^*(x)$ where $g(x)=\prod_{i=1}^{10} f_i(x)$ and $h(x)=\prod_{i=11}^{15} f_i(x)$. Thus for example the code $\langle g(x)h(x),\ 5h(x)h^*(x)\rangle$ is self dual.

Example 2.6 *Let $R=\mathbb{Z}_{81}$ and $n=140=2^2\cdot 5\cdot 7$. We have that $2^2\mid(3+1)$, $ord_7(3)=6$ and $ord_5(3)=4$. Thus $2^1\|ord_7(3)$ and $2^2\|ord_5(3)$. Therefore, there exist non trivial self dual cyclic codes of length 140 over $\mathbb{Z}_{81}$. The factorization of $x^{140}-1$ over $\mathbb{Z}_{81}$ is given by*

$$x^{140}-1=\prod_{i=1}^{9} f_i(x)\prod_{i=10}^{14} f_i(x)f_i^*(x),$$

where

$f_1(x)=x+1,$ $f_2(x)=x-1,$

$f_3(x)=x^2+1,$ $f_4(x)=x^4+x^3+x^2+x+1,$

$f_5(x)=x^4-x^3+x^2-x+1,$ $f_6(x)=x^6+13x^5+3x^4+13x^3+3x^2+13x+1,$

$f_7(x)=x^6+x^5+x^4+x^3+x^2+x+1,$ $f_8(x)=x^6-13x^5+3x^4-13x^3+3x^2-13x+1,$

$f_9(x)=x^6-x^5+x^4-x^3+x^2-x+1,$ $f_{10}(x)=x^4-20x^3-3x^2+20x+1,$

$$f_{11}(x) = x^{12} - 24x^{11} + 9x^{10} - 17x^9 + 5x^8 + 31x^7 - 4x^6 + 11x^5 - 12x^4 + 4x^3 - 8x^2 + 37x + 1,$$

$$f_{12}(x) = x^{12} + 24x^{11} + 9x^{10} + 17x^9 + 5x^8 + 50x^7 - 4x^6 - 11x^5 - 12x^4 - 4x^3 - 8x^2 + 44x + 1,$$

$$f_{13}(x) = x^{12} - 9x^{11} + 4x^{10} + 15x^9 + 53x^8 + 19x^7 + 12x^6 + 49x^5 + 23x^4 - 2x^3 - 13x^2 + 8x + 1,$$

$$f_{14}(x) = x^{12} + 9x^{11} + 4x^{10} - 15x^9 + 53x^8 - 19x^7 + 12x^6 + 32x^5 + 23x^4 + 2x^3 - 13x^2 - 8x + 1.$$

Let $x^{140} - 1 = g(x)h(x)h^*(x)$ *where* $g(x) = \prod_{i=1}^{9} f_i(x)$ *and* $h(x) = \prod_{i=10}^{14} f_i(x)$. *Thus the code* $\langle g(x)h(x),\ 9h(x)h^*(x)\rangle$ *is self dual.*

Chapter 4

Construction of Isodual cyclic Codes over Finite Rings

In this chapter we will present another class of formally self dual codes called isodual codes, those are codes which are equivalent to their duals. For some parameters, one can prove that there are no cyclic self dual codes over finite fields or finite rings, whereas isodual codes can exist.

1 Generalities of Isodual codes over Finite Fields

For linear codes over finite fields, we have that if C is an $[n, k, d]$ isodual code, then $n = 2k$.

Proposition 1.1 *[60] Let A be a matrix satisfying $A^T = QAQ$, with Q a monomial matrix that satisfies $Q^2 = I$, where I is identity of order n. The code C with generator matrix $G = [I|A]$ is an isodual code of length $2n$.*

Proof. The parity check matrix of C is then $H = [-A^T|I]$. Recall that H spans $C^\perp$. Using the hypothesis, we have $H\bar{Q} = [-QA|Q]$, where $\bar{Q} = \begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}$. Hence $\bar{Q}H\bar{Q} = [-A|I]$, is a matrix which spans an equivalent code to C. The result follows. □

Let a be an integer such that $\gcd(a, n) = 1$. The function μ_a defined on $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ by $\mu_a(i) \equiv ia \mod n$ is a permutation of the coordinate positions $\{0, 1, 2, ..., n-1\}$ and is called a multiplier. Multipliers also act on polynomials and this gives the following ring

automorphism

$$\begin{aligned} \mu_a : \ \mathbb{F}_q[x]/(x^n-1) &\longrightarrow \mathbb{F}_q[x]/(x^n-1) \\ f(x) &\longmapsto \mu_a(f(x)) = f(x^a) \end{aligned}$$

If C is a cyclic code generated by $f(x)$, then $\mu_a(C) = \langle f(x^a)\rangle$. Thus two cyclic codes $C_1 = \langle f(x)\rangle$ and $C_2 = \langle g(x)\rangle$ are multiplier equivalent if there exists a multiplier μ_a such that $g(x) = \mu(f(x)) = f(x^a)$.

Proposition 1.2 *[31] Let C be a cyclic code of length n over $\mathbb{F}_q$ generated by the polynomial $g(x)$ and λ in $\mathbb{F}_q^*$ such that $\lambda^n = 1$. Then the following holds*

i. C is equivalent to the cyclic code generated by $g^*(x)$, and

ii. C is equivalent to the cyclic code generated by $g(\lambda x)$.

Proof. (i.) Consider the multiplier

$$\begin{aligned} \mu_{-1} : \ \mathbb{F}_q[x]/(x^n-1) &\longrightarrow \mathbb{F}_q[x]/(x^n-1) \\ f(x) &\longmapsto \mu_{-1}(f(x)) = f(x^{-1}) \end{aligned}$$

Assume that $\deg(g(x)) = r$. If C_1 is the code generated by $g^*(x)$, then

$$C_1 = \{x^r g^{-1}(0)\mu_{-1}(g(x))f(x) \mod (x^n-1); f(x) \in \mathbb{F}_q[x]/(x^n-1)\}$$

Clearly, we have

$$\{x^r f(x^{-1}) \mod (x^n-1); f(x) \in \mathbb{F}_q[x]/(x^n-1)\} = \{\mu_{-1}(a(x)) \mod (x^n-1); a(x) \in \mathbb{F}_q[x]/(x^n-1)\}$$

So that

$$\{g(0)^{-1}\mu_{-1}(g(x)a(x)) \mod (x^n-1); a(x) \in \mathbb{F}_q[x]/(x^n-1)\} = \mu_{-1}(C)$$

Hence, C is equivalent to C_1 because μ_{-1} is a permutation of the coordinates $\{1, x, x^2, ..., x^{n-1}\}$.
(ii.) Suppose there exists $\lambda \in \mathbb{F}_q^*$ such that $\lambda^n = 1$ and let

$$\begin{aligned} \phi : \ \mathbb{F}_q[x]/(x^n-1) &\longrightarrow \mathbb{F}_q[x]/(x^n-1) \\ f(x) &\longmapsto \phi(f(x)) = f(\lambda x) \end{aligned}$$

For polynomials $f(x), g(x)$ in $\mathbb{F}_q[x]$ we have that $f(x) \equiv g(x) mod(x^n - 1)$ if and only if there exists a polynomial $h(x)$ in $\mathbb{F}_q[x]$ such that

$$f(x) - g(x) = h(x)(x^n - 1)$$

Thus, it must be that

$$\begin{aligned} f(\lambda x) - g(\lambda x) &= h(\lambda x)[(\lambda x)^n - 1] \\ &= h(\lambda x)[(\lambda)^n x^n - 1] \\ &= h(\lambda x)[x^n - 1] \end{aligned}$$

Which is true if and only if $f(\lambda x) \equiv g(\lambda x) mod(x^n - 1)$. Hence for $f(x), g(x)$ in $\mathbb{F}_q[x]/(x^n - 1)$

$$\phi(f(x)) = \phi(g(x))$$

if and only if

$$g(x) = f(x)$$

Therefore ϕ is well defined and is a ring automorphism of $\mathbb{F}_q[x]/(x^n - 1)$. Let C_2 be the cyclic code generated by $g(\lambda x)$. Arguing as in part (i) we have that $C_2 = \phi(C)$. So that C is equivalent to C_2.

Remark 1.1 *With the same assumptions as in Proposition 1.2 we have :*

i. C is equivalent to the cyclic code generated by $g^*(\lambda x)$.

ii. C is equivalent to the cyclic code generated by $(g(\lambda x))^*$.

Proposition 1.3 *[31] Let n be a positive integer . If $f(x)$ and $g(x)$ are polynomials in $\mathbb{F}_q[x]$ such that $x^n - 1 = g(x)f(x)$, then the cyclic code generated by $g(x)$ is equivalent to the dual of the cyclic code generated by $f(x)$.*

Proof. Let C be a cyclic code generated by $g(x)$ and C' a cyclic code generated by $f(x)$. We have that the dual of C' is generated by $g^*(x)$. By Propostion 1.2, C is equivalent to $C'^{\perp}$. □

Theorem 1.1 *[31] Let m be an odd integer and $f(x)$ a polynomial over $\mathbb{F}_q$ such that $x^m - 1 = (x - 1)f(x)$. Then the cyclic codes of length $2m$ generated by $(x - 1)f(-x)$ and $(x + 1)f(x)$ are isodual codes.*

Proof. If $x^m - 1 = (x-1)f(x)$, then $x^m + 1 = (x+1)f(-x)$ and

$$x^{2m} - 1 = (x^m - 1)(x^s + 1) = (x-1)f(x)(x+1)f(-x).$$

Let $g(x) = (x-1)f(-x)$ be the generator polynomial of a cyclic code C. Then the dual code $C^\perp$ is generated by

$$h^*(x) = (x+1)f^*(x) = g^*(-x)$$

Hence from Proposition 1.2, C is equivalent to the cyclic code generated by $g^*(x)$. Further, from Proposition 1.2 again, the cyclic code generated by $g^*(x)$ is equivalent to the cyclic code generated by $g^*(-x) = h^*(x)$, as the latter code is $C^\perp$, so that C is isodual. The same result holds for $g(x) = (x+1)f(x)$ □

The following theorem give a natural construction for cyclic isodual codes.

Theorem 1.2 *Let n be a positive integer such that there exists λ in $\mathbb{F}_q^*$ verifying $\lambda^n = 1$. If $x^n - 1 = \alpha g(x)g(\lambda x)$ or $x^n - 1 = \alpha g(x)g(\lambda x)^*$ for some α in $\mathbb{F}_q^*$, then the code generated by $g(x)$ is isodual.*

Proof. Assume that $x^n - 1 = \alpha g(x)g(\lambda x)^*$. Let C be a code generated by the polynomial $g(x)$. From Proposition 1.3, C is equivalent to the dual of the cyclic code C' generated by $\alpha g(\lambda x)^*$. Up to normalization and since $\lambda^n = 1$ and α in $\mathbb{F}_q^*$, we obtain that the code C' is equivalent to the code generated by $g(x)$ which is C itself. Therfore C is isodual. With the same argument, we get the result for the second part. □

Remark 1.2 *The dual of an isodual cyclic code is also isodual.*

Let m be an odd integer and $n = 2m$. Write the factorization of $x^m - 1$ in $\mathbb{F}_q[x]$ at the form

$$x^m - 1 = (x-1)u(x)v(x)$$

where u, v are arbitrary in $\mathbb{F}_q[x]$. Therefrom we get immediately by the identity $x^n - 1 = (x^m - 1)(x^m + 1)$ the relation

$$x^n - 1 = (x^2 - 1)u(x)u(-x)v(x)v(-x).$$

Corollary 1.1 *[1] Any cyclic code of length n and generated by one of the following polynomial $g(x)$ in the below table is isodual.*

N°	$g(x)$	$\left[\frac{x^n-1}{g(x)}\right]^*$
1	$(x-1)u(x)v(x)$	$[-g(-x)]^*$
2	$(x-1)u(-x)v(x)$	$[-g(-x)]^*$
3	$(x-1)u(-x)v(-x)$	$[-g(-x)]^*$
4	$(x-1)u(x)v(-x)$	$-g(-x)$

Example 1.1 *Let $q = 3, m = 25$ and $n = 2m$. The factorization of $x^{50} - 1$ is given by*

$$\begin{aligned} x^{50}-1 &= (x+1)(x+2)(x^4+x^3+x^2+x+1)(x^4+2x^3+x^2+2x+1) \\ &\quad \times(x^{20}+x^{15}+x^{10}+x^5+1)(x^{20}+2x^{15}+x^{10}+2x^5+1) \end{aligned}$$

Let $f(x) = x - 1, h(x) = x^4 + x^3 + x^2 + x + 1$ and $p(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$. Hence the codes generated by $g(x)$ are isodual, where

$g(x)$	*Minimum weight*	$u(x)$	$v(x)$
$f(x)h(x)p(x)$	2	$h(x)$	$p(x)$
$f(x)h(x)p(-x)$	4	$h(x)$	$p(x)$
$f(x)h(-x)p(x)$	4	$h(-x)$	$p(x)$
$f(-x)h(x)p(x)$	4	$h(x)$	$p(x)$
$f(x)h(-x)p(-x)$	4	$h(-x)$	$p(-x)$
$f(-x)h(x)p(-x)$	4	$h(x)$	$p(-x)$
$f(-x)h(-x)p(x)$	4	$h(-x)$	$p(x)$
$f(-x)h(-x)p(-x)$	2	$h(-x)$	$p(-x)$

As a special case, consider the factorization of x^n-1 in the form $x^n-1 = (x^2-1)u(x)u(-x)$, where u is an irreducible polynomial over $\mathbb{F}_q$ and $\deg(u) = m - 1$.

Corollary 1.2 *[1] The cyclic codes over $\mathbb{F}_q$ of parameters $[2m, m, d]_q$ are all isodual.*

Example 1.2 *Let $q = 5, m = 3$. The factorization of $x^6 - 1$ is given by*

$$x^6 - 1 = (x+1)(x+4)(x^2+x+1)(x^2+4x+1)$$

Let $f(x) = x+1$ *and* $h(x) = x^2+x+1$. *Then* $C = \langle g(x) \rangle$ *is isodual, where*

$g(x)$	*Minimum weight*	$u(x)$
$f(x)h(x)$	4	$h(x)$
$f(x)h(-x)$	2	$h(-x)$
$f(-x)h(x)$	2	$h(x)$
$f(-x)h(-x)$	4	$h(-x)$

2 Construction of Isodual cyclic Codes over Finite Chain Rings

In this section some constructions of monomial isodual free cyclic codes for odd characteristics are presented as a generalization of those obtained in [5].

2.1 Structure of Free Cyclic Codes of Length $2^a m$ over R

Let R be a finite chain ring with residue field $\mathbb{F}_q$ and m an odd integer such that $\gcd(m, q) = 1$. In the following we give the structure of cyclic codes of length $2^a m$ where $a \geq 1$. We begin with the following Lemmas

Lemma 2.1 *[5] There exists a primitive* 2^a*-th root of the unity* ξ *in* R^* *if and only if* $q \equiv 1 \mod 2^a$. *Further,* $x^{2^a} - 1 = \prod_{k=1}^{2^a}(x - \xi^k)$ *in* $R[x]$.

Proof. Since q is an odd prime power, by [[4], Proposition 4.2], there exists a primitive 2^a-th root of the unity in R^* if and only if there exists a primitive 2^a-th root of unity in $\mathbb{F}_q$. If there exists a primitive 2^a-th root of unity ξ in $\mathbb{F}_q$, then $\xi^{2^a} = 1$, so that 2^a divides $q-1$. Conversely, if 2^a divides $q-1$ then there exists an integer k such that $q = k2^a + 1$. If ξ is a primitive element of $\mathbb{F}_q^*$, then $1 = \xi^{q-1} = (\xi^k)^{2^a}$ and

$$ord(\xi^k) = \frac{ord(\xi)}{\gcd(k, ord(\xi))} = \frac{q-1}{\gcd(k, q-1)} = \frac{k2^a}{\gcd(k, k2^a)} = 2^a$$

Let ξ be a primitive 2^a-th root of the unity in R^*. Since $\gcd(2^a, q) = 1$, it must be that $\bar{\xi}$ is a primitive 2^a-th root of unity in $\mathbb{F}_q^*$. So that $x^{2^a} - 1 = \prod_{k=1}^{2^a}(x - \bar{\xi}^k)$ in $\mathbb{F}_q[x]$. By Lemma 2.1, the monic polynomial $x^{2^a} - 1$ factors uniquely as a product of monic basic irreducible pairwise

coprime polynomials over R. Furthermore, there is a one-to-one correspondence between the set of basic irreducible polynomial divisors of $x^{2^a}-1$ in $R[x]$ and the set of irreducible divisors of $x^{2^a}-1$ in $\mathbb{F}_q[x]$. If $x^{2^a}-1=\prod_{k=1}^{2^a}(x-a_k)$, then $(\overline{x-a_k})=(x-\bar{a_k})=(x-\bar{\xi}^k)$. Since $(\overline{x-\xi^k})=(x-\bar{\xi}^k)=(x-\bar{\xi}^k)$, from the unique decomposition of $x^{2^a}-1$ in $R[x]$, the result follows. □

Lemma 2.2 *[5] .*

i. If there exists a primitive 2^a-th root of unity ξ in R^*, then ξ^{2^i} is a primitive 2^{a-i}-th root of unity in R^*; for all $i \leq a$.

ii. Let ξ be a primitive 2^a-th root of the unity in R^*. Then ξ^m is also a primitive 2^a-th root of the unity in R^*.

iii. $\prod_{k=1}^{2^a}\xi^k=1$, if $a \geqslant 2$.

Proposition 2.1 *If R^* contains a primitive 2^a-th root of unity ξ, and $x^m-1=\prod_{i=1}^{l}f_i(x)$, where $f_i(x),\ 1\leq i\leq l$, are monic basic irreducible pairwise coprime factors in $R[x]$, then*

$$x^{2^a m}-1=\prod_{k=1}^{2^a}\prod_{i=1}^{l}f_i(\xi^k x)$$

Proof. Assume that $x^m-1=\prod_{i=1}^{l}f_i(x)$. Let ξ be a primitive 2^a-th root of unity. Then $(\xi^k x)^m-1=\prod_{i=1}^{l}f_i(\xi^k x)$. Thus $x^m-\xi^{-km}=\xi^{-km}\prod_{i=1}^{l}f_i(\xi^k x)$. Since ξ is a primitive 2^a-th root of unity and $\prod_{k=1}^{2^a}\xi^{-km}=1$, we get

$$\begin{aligned} x^{2^a m}-1 &= (x^m)^{2^a}-1=\textstyle\prod_{k=1}^{2^a}(x^m-\xi^k)=\prod_{k=1}^{2^a}(x^m-\xi^{-km}) \\ &= \textstyle\prod_{k=1}^{2^a}(\xi^{-km}\prod_{i=1}^{l}f_i(\xi^k x))=\prod_{k=1}^{2^a}\prod_{i=1}^{l}f_i(\xi^k x)) \end{aligned}$$

□

Corollary 2.1 *[5] If R^* contains a primitive 2^a-th root of unity and $x-1, f_i(x), 1\leq i\leq l$, are the monic basic irreducible pairwise coprime factors of x^m-1 in $R[x]$, then*

$$x^{2^a m}-1=(x^{2^a}-1)\prod_{i=1}^{l}f_i(\xi^k x)$$

We now give a structure of free cyclic codes of length $2^a m$ over R.

Corollary 2.2 *If R^* contains a primitive 2^a-th root of unity ξ and $f_i(x), 1 \leq i \leq l$ are the monic basic irreducible factors of $x^m - 1$ in $R[x]$, then a free cyclic code C of length $n = 2^a m$ is generated by $\prod_{k=1}^{2^a} \prod_{i=1}^{l} f_i^{j_i}(\xi^k x)$ with $0 \leq j_i \leq 1$.*

Proof. The result follows from Proposition 2.1 and from the fact that a free cyclic code is generated by a divisor of $x^{2^a m} - 1$. □

2.2 Construction of Cyclic Isodual Codes over Finite Chain Rings

In this part, explicit constructions of monomial isodual free cyclic codes over finite chain rings are presented. We begin with the following result given in [5] which is a generalisation of the result of the proposition 1.2 to codes over finite chain rings.

Lemma 2.3 *[5] Let R be a finite chain ring and C be a **free** cyclic code of length n over R generated by a polynomial $g(x)$ and δ a unit in R such that $\delta^n = 1$. Then the following holds:*

(i) C is equivalent to the cyclic code generated by $g^*(x)$.

(ii) C is equivalent to the cyclic code generated by $g(\delta x)$.

(iii) C is equivalent to the cyclic code generated by $g^*(\delta x)$ or $(g(\delta x))^*$.

(iv) If n is even, then C is equivalent to the cyclic code generated by $g(-x)$.

Assume we have q an odd prime power such that $q \equiv 1 \mod 2^a$ with $a \geq 1$ and m an odd integer coprime to q. The following give us some constructions of isodual cyclic codes of length $2^a m$ over R.

Theorem 2.1 *Suppose that $x^m - 1 = f_1(x) f_2(x)$. Then the **free** cyclic codes of length $2^a m$ generated by*

$$\prod_{k=1}^{2^{a-1}} f_i(\xi^{2k} x) \prod_{k=0}^{2^{a-1}-1} f_j(\xi^{2k+1} x), \ i,j \in \{1,2\}, i \neq j,$$

and

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k} x) f_2(\xi^{2k} x),$$

and

$$\prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1} x) f_2(\xi^{2k+1} x)$$

are isodual, where ξ is a primitive 2^a-th root of unity.

Proof. Let $x^m - 1 = f_1(x)f_2(x)$. From Proposition 2.1, we have

$$x^{2^a m} - 1 = \prod_{k=1}^{2^a} f_1(\xi^k x)f_2(\xi^k x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k} x)f_2(\xi^{2k} x) \prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1} x)f_2(\xi^{2k+1} x).$$

Let

$$g(x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k} x) \prod_{k=0}^{2^{a-1}-1} f_2(\xi^{2k+1} x).$$

Knowing that $\xi^{2^a} = 1$, we get

$$g(\xi x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k+1} x) \prod_{k=0}^{2^{a-1}-1} f_2(\xi^{2k+2} x) = \prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1} x) \prod_{k=1}^{2^{a-1}} f_2(\xi^{2k} x).$$

In other words, we have that $x^{2^a m} - 1 = g(x)g(\xi x)$. Since $\xi^{2^a m} = 1$, then from Theorem 1.2 the code generated by $g(x)$ is isodual. A similar argument is employed to prove the other cases. □

Corollary 2.3 *[5] Let $f(x)$ be a polynomial such that $x^m - 1 = (x-1)f(x)$. The free cyclic codes of length $2^a m$ generated by*

$$(x^{2^{a-1}} - 1) \prod_{k=0}^{2^{a-1}-1} f(\xi^{2k+1} x)$$

and

$$(x^{2^{a-1}} + 1) \prod_{k=1}^{2^{a-1}} f(\xi^{2k} x)$$

are isodual codes of length $2^a m$.

Proof. Just take $f_1(x) = x - 1$ in the theorem 2.1 and use Lemma 2.1. □

Example 2.1 *Let $R = \mathbb{Z}_{25}$ and $n = 36 = 2^2 \cdot 3^2$, $q = 5 \equiv 1 \mod 2^2$. We have*

$$x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

Thus, we get the isodual codes given in Table (4.1), where ξ is a primitive 4-th root of unity

.

Table 4.1: List of isodual codes obtained of length 36 over $\mathbb{Z}_{25}$.

	Polynomial generator $g(x)$ of the isodual code C
$g(x)=$	$x^9+(\xi-\xi^2)x^6+(\xi^2-\xi^3)x^3-1$
$g(x)=$	$\xi^3x^9+(\xi-1)x^6+(\xi^3-\xi^2)x^3-1$
$g(x)=$	$\xi^3x^9-(\xi^2-\xi)x^8+(\xi^3-1)x^7-(\xi^2-1)x^6+(\xi^2-\xi^3)x^5-$ $(\xi-1)x^4+(\xi-\xi^3)x^3+(\xi^3-1)x^2+(\xi-\xi^2)x-1$
$g(x)=$	$x^9-(\xi^2-\xi^3)x^8-(\xi-\xi^2)x^7+(\xi^2-1)x^6+(\xi-1)x^5-$ $(\xi^3-1)x^4+(\xi^2-1)x^3-(\xi^2-\xi^3)x^2-(\xi-\xi^2)x-1$
$g(x)=$	$\xi^2x^9-(\xi-1)x^8-(\xi^3-1)x^7-(\xi^2-\xi^3)x^6-(\xi-\xi^2)x^5+$ $(\xi-1)x^4-(\xi^3-1)x^3-(\xi^2-\xi^3)x^2-(\xi-\xi^2)x-1$
$g(x)=$	$\xi x^9+(\xi^3-1)x^8+(\xi-\xi^2)x^7+(\xi^3-1)x^6+(\xi-\xi^2)x^5+$ $(\xi^3-1)x^4+(\xi-\xi^2)x^3+(\xi^3-1)x^2+(\xi-\xi^2)x-1$
$g(x)=$	ξ^2x^9-1
$g(x)=$	ξx^9-1

Corollary 2.4 *Let p^k be a prime power. Assume that $x^{p^k}-1=f_1(x)f_2(x)$. Then the cyclic codes generated by*

$$f_1(x)f_2(-x) \text{ or } f_1(-x)f_2(x) \text{ or } x^{p^k}-1 \text{ or } x^{p^k}+1$$

are isodual codes of length $2p^k$. Further, if $ord_p(q)$ is even, then these codes are LCD-isodual codes.

Proof. The result follows from Theorem 2.4 and Theorem 2.1 for $a=1$, $m=p^k$ and $\xi=-1$. □

Corollary 2.5 *Let m be an odd integer such that the irreducible factorisation of m is given by $m=p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ and $x^m-1=f_1(x)f_2(x)$. Assume that there exists a in $\mathbb{N}^*$ such that $2^a \| ord_{p_i}(q)$, for all $1\leq i\leq t$. Then, the cyclic codes generated by*

$$f_1(x)f_2(-x) \text{ or } f_1(-x)f_2(x) \text{ or } x^m-1 \text{ or } x^m+1$$

are LCD-isodual codes of length $2m$.

Proof. The result follows immediately from Theorem 2.5 and Theorem 2.1 with $\xi=-1$. □

Example 2.2 *Let $R = \mathbb{Z}_9$ and $n = 50 = 2 \cdot 5^2$. We have*

$$x^{25} - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)(x^{20} + x^{15} + x^{10} + x^5 + 1).$$

Further $ord_5(3) = 4$. So we get the LCD isodual codes shown in Table (4.2).

Table 4.2: List of LCD-isodual codes obtained of length 50 over $\mathbb{Z}_9$.

	Polynomial generator $g(x)$ of LCD-isodual code C
$g(x) =$	$x^{25} - 2x^{20} + 2x^{15} - 2x^{10} + 2x^5 - 1$
$g(x) =$	$x^{25} + 2x^{20} + 2x^{15} + 2x^{10} + 2x^5 + 1$
$g(x) =$	$-x^{25} - 2x^{24} - 2x^{23} - 2x^{22} - 2x^{21} + 2x^{19} + 2x^{18} + 2x^{17} +$ $2x^{16} - 2x^{14} - 2x^{13} - 2x^{12} - 2x^{11} + 2x^9 + 2x^8 +$ $2x^7 + 2x^6 - 2x^4 - 2x^3 - 2x^2 - 2x - 1$
$g(x) =$	$x^{25} - 2x^{24} + 2x^{23} - 2x^{22} + 2x^{21} - 2x^{19} + 2x^{18} - 2x^{17} +$ $2x^{16} - 2x^{14} + 2x^{13} - 2x^{12} + 2x^{11} - 2x^9 + 2x^8 -$ $2x^7 + 2x^6 - 2x^4 + 2x^3 - 2x^2 + 2x - 1$
$g(x) =$	$x^{25} - 2x^{24} + 2x^{23} - 2x^{22} + 2x^{21} - 2x^{20} + 2x^{19} - 2x^{18} + 2x^{17} -$ $2x^{16} + 2x^{15} - 2x^{14} + 2x^{13} - 2x^{12} + 2x^{11} - 2x^{10} + 2x^9 - 2x^8 +$ $2x^7 - 2x^6 + 2x^5 - 2x^4 + 2x^3 - 2x^2 + 2x - 1$
$g(x) =$	$x^{25} + 2x^{24} + 2x^{23} + 2x^{22} + 2x^{21} + 2x^{20} + 2x^{19} + 2x^{18} + 2x^{17} +$ $2x^{16} + 2x^{15} + 2x^{14} + 2x^{13} + 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^8 +$ $2x^7 + 2x^6 + 2x^5 - 2x^4 + 2x^3 + 2x^2 + 2x + 1$
$g(x) =$	$x^{25} - 1$
$g(x) =$	$x^{25} + 1$

Another construction of isodual cyclic codes is given by the following Theorem.

Theorem 2.2 *Assume that we have the factorization $x^m - 1 = f_1(x)f_2(x)f_2^*(x)$, such that the polynomial f_1 is self reciprocal. Then the free cyclic codes of length $2^a m$ over R generated by*

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x) \prod_{k=1}^{2^a} f_2(\xi^k x);$$

and

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2^*(\xi^k x)$$

are isodual, where ξ is a primitive 2^a-th root of unity.

Proof. Let $x^m - 1 = f_1(x)f_2(x)f_2^*(x)$ then

$$x^{2^a m} - 1 = \prod_{k=1}^{2^a} f_1(\xi^k x)f_2(\xi^k x)f_2^*(\xi^k x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}) \prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1})\prod_{k=1}^{2^a} f_2(\xi^k x)f_2^*(\xi^k x)$$

Let $g(x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2(\xi^k x)$. Since $\xi^{2^a} = 1$, we get

$$g(\xi x) = \prod_{k=1}^{2^{a-1}} f_1(\xi^{2k+1}x)\prod_{k=1}^{2^a} f_2(\xi^{k+1}x) = \prod_{k=0}^{2^{a-1}-1} f_1(\xi^{2k+1}x)\prod_{k=1}^{2^a} f_2(\xi^k x).$$

Since the polynomial f_1 is self reciprocal, we get the factorization $x^{2^a m}-1 = g(x)g(\xi x)^*$. The desired result follows from Theorem 1.2. The same result is obtained for codes generated by

$$\prod_{k=1}^{2^{a-1}} f_1(\xi^{2k}x)\prod_{k=1}^{2^a} f_2^*(\xi^k x).$$

□

Example 2.3 *Let $R = \mathbb{Z}_{25}$ and $n = 132 = 2^2 \cdot 33$. We have $5 \equiv 1 \mod 2^2$. The factorization of $x^{33} - 1$ over R is given by*

$$x^{33} - 1 = f_1(x)f_2(x)f_2^*(x)$$

where

$$\begin{aligned} f_1(x) &= (x-1)(x^2+x+1) \\ f_2(x) &= (x^5 - 8x^4 - x^3 + x^2 - 9x - 1)(x^{10} - 9x^9 + 7x^8 + 11x^7 + 9x^6 - 4x^5 - 7x^4 - 6x^3 - 10x^2 + 8x + 1) \\ f_2^*(x) &= (x^5 + 9x^4 - x^3 + x^2 + 8x - 1)(x^{10} + 8x^9 - 10x^8 - 6x^7 - 7x^6 - 4x^5 + 9x^4 + 11x^3 + 7x^2 - 9x + 1) \end{aligned}$$

Thus, for example, the codes generated by

$$\left\langle f_1(x)f_1(\xi^2 x)f_2(x)f_2(\xi^2 x)f_2(\xi^3 x)\right\rangle$$

and

$$\left\langle f_1(x)f_1(\xi^2 x)f_2^*(x)f_2^*(\xi x)f_2^*(\xi^2 x)f_2^*(\xi^3 x)\right\rangle$$

are isodual, where ξ is a primitive 4-th root of unity.

Corollary 2.6 *Let p be an odd prime number and k in $\mathbb{N}$ such that $x^{p^k}-1 = f_1(x)f_2(x)f_2^*(x)$. Assume that $ord_p(q)$ is even. Then the cyclic codes of length $2p^k$ generated by*

$$f_1(x)f_2(x)f_2(-x) \text{ and } f_1(x)f_2^*(x)f_2^*(-x)$$

are LCD-isodual codes.

Proof. The result follows from Theorem 2.4 and Theorem 2.2 with $\xi = -1$. □

Corollary 2.7 *Let m be an odd integer such that the irreducible factorisation of m is given by $m = p_1^{k_1}p_2^{k_2}...p_t^{k_t}$ and $x^m - 1 = f_1(x)f_2(x)f_2^*(x)$. Assume that there exists a in $\mathbb{N}^*$ such that $2^a \| ord_{p_i}(q)$, for all $1 \leq i \leq t$. Then the cyclic codes of length $2m$ generated by*

$$f_1(x)f_2(x)f_2(-x) \text{ and } f_1(x)f_2^*(x)f_2^*(-x)$$

are LCD-isodual codes.

Proof. The result follows immediately from Theorem 2.5 and Theorem 2.2 with $\xi = -1$. □

Example 2.4 *Let $R = \mathbb{Z}_{27}$ and $n = 70 = 2 \cdot 5 \cdot 7$. We have $x^{35} - 1 = f_1(x)f_2(x)f_2^*(x)$, where*

$$f_1(x) = (x-1)(x^4+x^3+x^2+x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$$

$$f_2(x) = x^{12} - 9x^{11} + 4x^{10} - 12x^9 - 3x^8 - 7x^7 + 12x^6 - 5x^5 - 4x^4 - 2x^3 + 14x^2 + 8x + 1.$$

$$f_2^*(x) = x^{12} + 8x^{11} + 14x^{10} - 2x^9 - 4x^8 - 5x^7 + 12x^6 - 7x^5 - 3x^4 - 12x^3 + 4x^2 - 9x + 1$$

So the cyclic codes of length 70 over $\mathbb{Z}_{27}$ generated by

$$g(x) = f_1(x)f_2(x)f_2(-x)$$

and

$$h(x) = f_1(x)f_2^*(x)f_2^*(-x)$$

are isodual.

We cite now construction of isodual codes as a direct sum of isoduals codes. For this , the following Lemma is needed.

Lemma 2.4 *[5] Let C_1 and C_2 be linear codes of lengths n_1 and n_2, respectively over R. Define the direct sum as $C_1 \oplus C_2 = \{(c_1, c_2), c_1 \in C_1, c_2 \in C_2\}$. Then the following holds*

i. $(C_1 \oplus C_2)^{\perp} = C_1^{\perp} \oplus C_2^{\perp}$.

ii. If C_1 and C_2 are isodual codes with minimum weights d_1 and d_2, respectively, then $C_1 \oplus C_2$ is an isodual code of length $n_1 + n_2$ with minimum weight $\min(d_1, d_2)$.

Theorem 2.3 *[5] Let R be a finite chain ring with residue field $\mathbb{F}_q$, q an odd prime power and m an odd integer such that* $\gcd(m, q) = 1$. *Let $C_i, 1 \leq i \leq 2a$ ($a \geq 1$ an integer), be cyclic isodual codes over R of length m. We then have*

i. $C_i \oplus C_j, \forall i, j, 1 \leq i, j \leq 2^a$, are cyclic isodual codes of length $2m$ over R.

ii. If $q \equiv 1 \mod 2^a$ ($a \geq 2$), then the direct sum $\oplus_{i=1}^{2^a} C_i$ is a cyclic isodual code of length $2^a m$ over R.

Chapter 5

Conclusion

Finding new construction methods for LCD and formally self dual codes opens up new venues of research and possibilities for researchers working on these codes. Finite chain rings have recently been shown to be of interest in finding new construction methods since they can be considered as Frobenius rings. In our work we have used only algebraic properties to find new LCD, self dual and isodual cyclic codes of arbitrary lengths over finite chain rings. We have shown the effectiveness of these constructions by producing several of these codes. There are a some possible directions for future research. One consists in trying to construct new LCD and isodual negacyclic codes or more generally constacyclic and quasi cyclic codes over rings. the second possible direction is to try to construct repeated root LCD and isodual codes. the third possible direction is to construct Hermetien LCD codes or more generally the $\sigma-$ LCD cyclic codes.

Appendix

This Chapter covers the main basic concepts, Definitions and Theorems from abstract algebra, which have been used in our construction of codes. For more details the reader is referred to some basic texts on commutative algebra such as [3, 14, 21, 37, 42, 46, 52, 54]

1 Whole Numbers

Definition 1.1 *We say that an integer d in $\mathbb{Z}$ divides m in $\mathbb{Z}$ if and only if $m = dq$ for some q in $\mathbb{Z}\backslash\{0\}$. This is denoted $d \mid m$.*

If d does not divide m, then we write $d \nmid m$.

Definition 1.2 *An integer p in $\mathbb{N}^*\backslash\{1\}$ is prime if it is only divisible by ± 1 and $\pm p$.*

Definition 1.3 *The greatest common divisor of a, b in $\mathbb{Z}$ is the largest k in $\mathbb{Z}$ such that $k \mid a$ and $k \mid b$. This element is denoted* $\gcd(a, b)$.

If $\gcd(a, b) = 1$, then we say that a is coprime to b.

Lemma 1.1 *For any integers a, b in $\mathbb{N}\backslash\{1\}$, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Theorem 1.1 *Any number a in $\mathbb{N}^*\backslash\{1\}$ can be expressed uniquely as a product of primes, $a = \prod_{i=1}^{r} p_i^{k_i}$, where $k_i \geq 1$ and $p_{i+1} > p_i$.*

Definition 1.4 *Given an integer $n > 1$, two integers a and b are said to be congruent modulo n, if n is a divisor of their difference. So we write*

$$a \equiv b \mod n \Leftrightarrow n \mid (a - b)$$

Definition 1.5 *Let a be an element of $\mathbb{Z}$ and n a positive integer such that $\gcd(a,n)=1$, the multiplicative order of a modulo n is the smallest positive integer $l, 0<l<n$ such that $a^l \equiv 1 \mod n$. We write $ord_n(a)=l$*

2 Finite Fields

Definition 2.1 *A finite field is a finite set which is a field; this means that multiplication, addition, subtraction and division (excluding division by zero) are defined and satisfy the rules of arithmetic known as the field axioms.*

Definition 2.2 *The characteristic of a field F is denoted $char(F)$ and is the smallest positive integer k such that $k.1=0$. If no such integer exists, then the characteristic is defined to be 0.*

A finite field with q elements will be denoted by $\mathbb{F}_q$, in such case the number q is called order of $\mathbb{F}_q$.

Theorem 2.1 *Let $\mathbb{F}_q$ be a finite field of q elements, then we have*

i. q is a prime power p^k, where p is a prime number and k is a positive integer.

ii. The characteristic of $\mathbb{F}_q$ is p.

iii. Every element a in $\mathbb{F}_q$ satisfies $a^q=a$.

iv. The multiplicative group $\mathbb{F}_q^*=\mathbb{F}_q-\{0\}$ is cyclic (i.e. generated by one element).

v. $(\alpha \pm \beta)^{p^m}=\alpha^{p^m} \pm \beta^{p^m}$, for all m in $\mathbb{N}$ and α, β in $\mathbb{F}_q$.

Theorem 2.2 *All finite fields of the same size are isomorphic to each other.*

Example 2.1 *The set $\mathbb{Z}/p\mathbb{Z}=\{0,1,...,p-1\}$, is a field if and only if p is a prime number.*

Definition 2.3 *An element α in $\mathbb{F}_q$ is primitive if its multiplicative order satisfies $ord(\alpha)=q-1$. It is a generator of the cyclic group $\mathbb{F}_q^*$. In such case we have $\mathbb{F}_q=\{0,\alpha,\alpha^2,...,\alpha^{q-1}\}$.*

Theorem 2.3 *The $q-1$ elements of $\mathbb{F}_q^*$ have the following properties:*

i. They are in one-to-one correspondence to the roots of the polynomial $x^{q-1}-1$ and

$$x^{q-1}-1=\prod_{\lambda \in \mathbb{F}_q^*}(x-\lambda)$$

ii. There exists a primitive element α in $\mathbb{F}_q$ and

$$x^{q-1} - 1 = \prod_{i=0}^{q-2}(x - \alpha^i)$$

2.1 Extension Fields and Minimal Polynomials

Definition 2.4 *An extension field K of a field $\mathbb{F}_q$ is a field which contains $\mathbb{F}_q$ as a proper subfield.*

Definition 2.5 *A non-constant polynomial $f(x)$ with coefficients in the field $\mathbb{F}_q$ is called reducible over $\mathbb{F}_q$ if it can be written as a product of multiple non-constant polynomials in $\mathbb{F}_q[x]$. Otherwise, it is called irreducible over $\mathbb{F}_q$.*

Theorem 2.4 *The quotient ring $K = \mathbb{F}_q[x]/\langle f(x)\rangle$ is an extension field of $\mathbb{F}_q$ with q^m elements if and only if $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree m. In such case we denote $\mathbb{F}_{q^m} = \mathbb{F}_q[x]/\langle f(x)\rangle$.*

Theorem 2.5 *If f is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m, then f has a root α in $\mathbb{F}_{q^m}$. Furthermore, all the roots of f are simple and are given by the m elements $\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{m-1}}$, which are called the conjugates of α in $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$.*

Definition 2.6 *The minimal polynomial of α in $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is the unique minimal-degree monic irreducible polynomial $m_\alpha(x)$ in $\mathbb{F}_q[x]$ such that $m_\alpha(\alpha) = 0$.*

Assume that we have the minimal polynomial of a primitive element α in $\mathbb{F}_{q^m}$, we would like to find the minimal polynomial of α^s, for any s. In order to do so, we have to start with cyclotomic cosets

Definition 2.7 *Let n be coprime to q. The cyclotomic coset of q (or q-cyclotomic coset) modulo n containing s is defined by*

$$C_s = \left\{s, sq, sq^2, ..., sq^{l_s-1}\right\},$$

where l_s is the smallest positive integer such that $s \equiv sq^{l_s} (\mod n)$.

The smallest integer in C_s is called the coset leader of C_s. Let $P_{n,q}$ be the set of all the coset leaders. Then we have $C_s \cap C_t = \emptyset$ for any two distinct elements s and t in $P_{n,q}$, and

$$\bigcup_{s \in P_{n,q}} C_s = \{0, 1, 2, ..., n-1\}.$$

Hence, the distinct q-cyclotomic cosets modulo n form a partition of $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$.

Example 2.2 *Consider the cyclotomic cosets of $q = 2$ modulo $n = 15$:*

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}, C_3 = \{3, 6, 9, 12\}, C_5 = \{5, 10\}, C_7 = \{7, 11, 13, 14\}$$

Hence

$$P_{15,2} = \{0, 1, 3, 5, 7\}$$

Theorem 2.6 *Let α be a primitive element of $\mathbb{F}_{q^m}$. Then the minimal polynomial of α^s with respect to $\mathbb{F}_q$ is*

$$m_s(x) = \prod_{j \in C_s} \left(x - \alpha^j\right)$$

where C_s is the unique cyclotomic coset of q modulo $q^m - 1$ containing s.

Remark 2.1

i. The degree of the minimal polynomial of α^s is equal to the size of the cyclotomic coset containing s.

ii. From Theorem 2.6 we know that α^s and α^t have the same minimal polynomial if and only if s, t are in the same cyclotomic coset.

Example 2.3 *Let $\alpha \in \mathbb{F}_9$ be a root of $2 + x + x^2$ in $\mathbb{F}_3[x]$; i.e.,*

$$2 + \alpha + \alpha^2 = 0 \tag{5.1}$$

Then the minimal polynomial of α as well as α^3 is $2 + x + x^2$. The minimal polynomial of α^2 is

$$m_2(x) = \prod_{j \in C_2} \left(x - \alpha^j\right) = (x - \alpha^2)(x - \alpha^6) = \alpha^8 - (\alpha^2 + \alpha^6) + x^2$$

Since $\alpha \in \mathbb{F}_9$ then $\alpha^8 = \alpha$. To find $m_2(x)$, we have to simplify $\alpha^2 + \alpha^6$. We make use of the relationship 5.1 to obtain

$$\alpha^2 + \alpha^6 = (1 - \alpha) + (1 - \alpha)^3 = 2 - \alpha - \alpha^3 = 2 + \alpha + \alpha^2$$

Hence, the minimal polynomial of α^2 is $1 + x^2$. In the same way, we may obtain the minimal polynomial $2 + 2x + x^2$ of α^5.

Theorem 2.7 *Let n be a positive integer coprime with q. Suppose that m is a positive integer satisfying $n \mid q^m - 1$. Let α be a primitive element of $\mathbb{F}_{q^m}$ and let $m_s(x)$ be the minimal polynomial of $\alpha^{\frac{q^m-1}{n}s}$ with respect to $\mathbb{F}_q$. Then the polynomial $x^n - 1$ has the factorization into monic irreducible polynomials over $\mathbb{F}_q$:*

$$x^n - 1 = \prod_{s \in P_{n,q}} m_s(x)$$

It follows that the number of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ is equal to the number of distinct cyclotomic cosets of q modulo n.

3 Finite Commutative Rings

A finite commutative ring is a finite set R equipped with two binary operations called addition and multiplication, such that R is an additive abelian group with identity element 0, the multiplication holds the distributive laws and it is abelian and associative. We say that R is a ring with unit if R has a multiplicative identity denoted $1 = 1_R$.

An element r in R is nilpotent if $r^n = 0$, for some positive integer n. So, a nilpotent element is a zero-divisor in R.

An element e in R is called idempotent if $e^2 = e$.

An invertible element (unit) x in R is an element for which there exists y in R such that $xy = 1$. The subset $U(R) = \{x \in R \mid \exists y \in R, xy = 1\}$ of R is a multiplicative group and its elements are called the units of R.

A ring R is a field if every non-zero element is a unit, i.e $U(R) = R^* = R/\{0\}$.

Definition 3.1 *Let R and R' be two rings. A ring homomorphism $\phi : R \to R'$ is an application that preserves both operations of R, so for all a, b in R:*

i. $\phi(a + b) = \phi(a) + \phi(b)$;

ii. $\phi(ab) = \phi(a)\phi(b)$;

iii. $\phi(1_R) = 1_{R'}$.

Definition 3.2 *A sub set I in R is an ideal if I is an additive subgroup of R and "ar" is in I, for all a in I and for all r in R.*

Definition 3.3 *Let $S = \{s_1, s_2, ..., s_k\} \subseteq R$. The set $\{\sum_{i=1}^{k} r_i s_i \mid r_i \in R\}$ is an ideal of R called ideal generated by S. So we write*

$$\langle S\rangle = \langle s_1, s_2, ..., s_k\rangle = \{\sum_{i=1}^{k} r_i s_i \mid r_i \in R\}$$

Definition 3.4 *A ring $\Re$ is said to be principal ideal ring if each ideal of $\Re$ is generated by one element.*

For ideals I and J of a ring R, their sum is

$$I + J = \{i + j \mid i \in I \text{ and } j \in J\}$$

it is just the ideal generated by $I \cup J$.
And their product is

$$IJ = \{i_1 j_1 + i_2 j_2 + ... + i_n j_n \mid i_k \in I \text{ and } j_k \in J \text{ for } n = 1, 2...\}$$

Note that the product IJ is contained in the intersection of I and J. The sum $I + J$ is called a direct sum if each element a in $I + J$ is uniquely expressible in the form $a = i + j$ with i in I and j in J. If the sum is a direct sum we write it as $I + J = I \oplus J$.

Definition 3.5 *Two ideals I and J in a ring R are called coprime if $I + J = R$.*

Proposition 3.1 *Let R be a ring and $I_1, I_2, ..., I_k$ be ideals of R. We have*

i. If whenever $i \neq j$, I_i and I_j are coprime then $\cap_{i=1}^{k} I_i = \prod_{i=1}^{k} I_i$.

ii. If I_i and I_j are coprime, then I_i^m and I_j^m are coprime for all m in $\mathbb{N}^*$.

Definition 3.6 *An ideal I of a ring R is a maximal ideal if there does not exist any other ideal I' such that $I \subset I' \subset R$. A ring R is a local ring if it has a unique maximal ideal.*

Definition 3.7 *The nilradical of R consists of the nilpotent elements of the ring.*

Given an ideal I of finite commutative ring R, we may define a relation $\sim$ on R as follows: $a \sim b$ if and only if $a - b$ is in I. Using the ideal properties, it is not difficult to check that $\sim$ is an equivalence relation. The equivalence class of the element a modulo I in R is given by

$$[a] = a + I = \{a + r, r \in I\}$$

The set of all such equivalence classes is denoted by R/I; it becomes a ring, for the usual composition laws and it's called the quotient ring of R modulo I.

$$R/I = \{a + I, a \in R\}$$

Theorem 3.1 *Let R be a commutative ring. The ideal I is maximal R if and only if the quotient ring R/I is a field.*

Theorem 3.2 *Let $I_1, I_2, ..., I_k$ be ideals in a ring R, and consider the ring homomorphism*

$$\begin{aligned} \psi : \quad R &\longrightarrow R/I_1 \times R/I_2 \times ... \times R/I_k \\ a &\longrightarrow (a + I_1, a + I_2, ..., a + I_k) \end{aligned}$$

Then we have

i. ψ is injective if and only if $I_1 \cap I_2 \cap ... \cap I_k = \{0\}$.

ii. ψ is surjective if and only if $I_1, I_2, ..., I_k$ are pairwise coprime.

A finite family $(I_i, i = 1, ..., k)$ of ideals of R, such that the homomorphism ψ is an isomorphism is called a direct decomposition of R.

Proposition 3.2 *Let $I_1, I_2, ..., I_k$ be ideals of R. The following are equivalent:*

i. A family $(I_i, i = 1, ..., k)$ is a direct decomposition of R;

ii. For $i \neq j$, I_i and I_j are coprime and $\cap_{i=1}^{k} I_i = \{0\}$;

iii. There exists a family $(e_1, e_2, ..., e_k)$ of idempotents of R such that $e_i e_j = 0$ for $i \neq j$, $\sum_{i=1}^{k} e_i = 1$ and $I_i = (1 - e_i)R$ for $i = 1, 2, ..., k$.

3.1 Modules

In this part, we give the definition of a module over a commutative ring and some of its properties.

Definition 3.8 *A module M over a commutative ring R is a set of objects, which can be added, subtracted and multiplied by scalars (members of the underlying ring). Thus M is an additive abelian group, and scalar multiplication is distributive over the operation of addition between elements of the ring or module and is compatible with the ring multiplication.*

Definition 3.9 *If N is a nonempty subset of an R-module M, we say that N is a submodule of M if for every $x, y \in N$ and $r, s \in R$, we have $rx + sy \in N$.*

Example 3.1

i. If I is an ideal of a ring R, then I is an $R-$module.

ii. For all n in $\mathbb{N}^*$, R^n is an $R-$module.

iii. If I is an ideal of R and M is an R-module, then $M/IM = \{m + IM, m \in M\}$ is also an R-module.

Definition 3.10 *Let X be a subset of an R-module M. Then*

i. X is said to be linearly independent if

$$\lambda_1 x_1 + \lambda_2 x_2 + ... + \lambda_k x_k = 0 \Rightarrow \lambda_1 = \lambda_2 = ... = \lambda_k = 0$$

for λ_i in R and distinct x_i in X.

ii. X spans or generates M if every m in M can be writen as

$$m = \lambda_1 x_1 + \lambda_2 x_2 + ... + \lambda_k x_k$$

for λ_i in R and x_i in X.

iii. X is a basis of M if X is linearly independent and X spans M.

Definition 3.11 *An R- module M is said to be free if it has a nonempty basis X.*

Example 3.2 *R^n is a free R-module,*

Definition 3.12 *Let M and N be two R-modules. The direct sum of M and N, denoted $M \oplus N$, is the R-module, which as a set is the Cartesian product of M and N, with addition and multiplication defined coordinate by coordinate:*

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2) \text{ and } r(m,n)=(rm,rn)$$

Note that if $\{M_i \mid i \in I\}$ is a collection of R modules, their Cartisien product $\prod_{i\in I} M_i$ is the set of all tuples $(m_i)_{i\in I}$ with m_i in M_i. The direct sum $\oplus_{i\in I} M_i$ of M_i is a submodule of $\prod_{i\in I} M_i$ consisting of all tuples $(m_i)_{i\in I}$ in which only a finite number of (m_i) are nonzero. When I is a finite then $\prod_{i\in I} M_i \simeq \oplus_{i\in I} M_i$.

Proposition 3.3 *A module M of a ring R is a free if it is a direct sum of isomorphic copies of R.*

Any two bases for a vector space over a field have the same cardinality. This property does not hold for arbitrary free modules, but the following result covers quite a few cases.

Theorem 3.3 *Any two bases for a free module M over a* ***commutative*** *ring R have the same cardinality, which is called rank of M.*

Definition 3.13 *Let M and N be two R-modules. An R-module homomorphism is a map*

$$\phi : M \longrightarrow N$$

such that

$$\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2) \text{ and } \phi(rm) = r\phi(m), (m_i \in M; r \in R)$$

We also say that ϕ is a R-linear map. In such case the set

$$\ker \phi = \{m \in M; \phi(m) = 0_N\}$$

is a submodule of M and it is called the kernel of ϕ.

Proposition 3.4 *Let $I_1, I_2, ..., I_k$ be ideals of R, relatively prime in pairs and let $I = \cap_{i=1}^{k} I_i$. For every R-module M, the canonical homomorphism $\phi : M \longrightarrow \prod_{i=1}^{k}(M/I_iM)$ is surjective and its kernel is IM. Further if $(I_i, i = 1, 2, ..., k)$ is a direct decomposition of R, then ϕ is an isomorphism.*

3.2 Finite Chain Rings

Definition 3.14 *A finite commutative ring with identity is called a finite chain ring if its ideals are linearly ordered by inclusion.*

Proposition 3.5 *Let R be a finite commutative ring the following conditions are equivalent:*

i. R is a local ring and the maximal ideal M of R is principal;

ii. R is a local principal ideal ring;

iii. R is a chain ring.

Let R be a finite chain ring, $\mathfrak{m}$ the unique maximal ideal of R, and let γ be a generator of $\mathfrak{m}$. Then, γ is nilpotent and we denote its nilpotency index by e. The ideals of R form a chain

$$\{0\} = \langle \gamma^e \rangle \subsetneq \langle \gamma^{e-1} \rangle \subsetneq \ldots \subsetneq \langle \gamma \rangle \subsetneq R,$$

The nilradical of R is $\mathfrak{m} = \langle \gamma \rangle$, so all the elements of $\mathfrak{m}$ are nilpotent. Therefore, the group of units of R is $R^* = R \backslash \langle \gamma \rangle$. Since $\mathfrak{m}$ is maximal, the residue ring $R/\mathfrak{m}$ is a field with q elements which we denote by $\mathbb{F}_q$.

Proposition 3.6 *Let R be a finite commutative chain ring, with maximal ideal $\mathfrak{m} = \langle \gamma \rangle$, and let e be the nilpotency index of $\mathfrak{m}$. Then we have the following statements.*

i. $|R| = |\mathbb{F}_q|^e$

ii. $|R/\gamma^j R| = |\langle \gamma^j \rangle| = |\mathbb{F}_q|^{e-j}$ *for* $0 \leq j \leq e-1$.

Example 3.3 *Let p be a prime number, $n \in \mathbb{N}^*$ and $a \in \mathbb{Z}_{p^n}$. We represent a in $\mathbb{Z}$ as the number which lies in $\{0, 1, ..., p^n - 1\}$. Then $\gcd(a, p^n) \in \{0, 1, p, p^2, ..., p^{n-1}\}$ and $a\mathbb{Z}_{p^n} = \gcd(a, p^n)\mathbb{Z}_{p^n}$. We obtain, that the principal ideals of $\mathbb{Z}_{p^n}$ are exactly*

$$\mathbb{Z}_{p^n}, p\mathbb{Z}_{p^n}, p^2\mathbb{Z}_{p^n}, ..., p^n\mathbb{Z}_{p^n} = \{0_{\mathbb{Z}_{p^n}}\}$$

We get the chain

$$\{0_{\mathbb{Z}_{p^n}}\} = p^n\mathbb{Z}_{p^n} \subset p^{n-1}\mathbb{Z}_{p^n} \subset p^{n-2}\mathbb{Z}_{p^n} \subset ... \subset p\mathbb{Z}_{p^n} \subset \mathbb{Z}_{p^n}$$

Hence $\mathbb{Z}_{p^n}$ is a finite chain ring with maximal ideal $\langle \gamma \rangle = \langle p \rangle$. The characteristic of $\mathbb{Z}_{p^n}$ is p and the residue field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Denote by $(-)$ the natural surjective ring morphism given by

$$\begin{aligned} - : R &\longrightarrow \mathbb{F}_q \\ a &\longmapsto \bar{a} = a \bmod \gamma \end{aligned} \tag{5.2}$$

The map given in (5.2) extends naturally to a map from $R[x] \longrightarrow \mathbb{F}_q[x]$.

Definition 3.15 *A polynomial $f(x)$ of $R[x]$ is called **basic** irreducible if $\overline{f(x)}$ is irreducible in $\mathbb{F}_q[x]$. It is a unit in $R[x]$ if and only if $\overline{f(x)}$ is a unit in $\mathbb{F}_q[x]$ and it is a zero divisor if and only if $\overline{f(x)} = 0$. otherwise it is called regular.*
(Recall that a polynomial $f(x)$ is irreducible in $R[x]$ if f is not unit and whenever $f = gh$ then g or h is unit).

Proposition 3.7 *Let $f(x) = a_0 + a_1x + ... + a_nx^n$ be an element of $R[x]$. The following conditions are equivalent:*

i. f is a unit in $R[x]$;

ii. $\bar{f}$ is a unit in $\mathbb{F}_q[x]$;

iii. a_0 is a unit in R and $a_1, ..., a_n$ are nilpotent.

Lemma 3.1 *If $f(x)$ is a monic polynomial over R such that $\overline{f(x)}$ is square free (has no multiple root), then $f(x)$ factors uniquely as product of monic basic irreducible pairwise comprime polynomials.*

Let D denote the set of all polynomials f in $R[x]$ such that $\overline{f}$ has distinct zeros in the algebraic closure of $\mathbb{F}_q$. The following proposition explores the relationships between irreducibility and basic irreducibility for regular polynomials and for elements of D .

Proposition 3.8 *Let f be a regular polynomial in $R[x]$. Then we have the following.*

i. If f is basic irreducible then f is irreducible .

ii. If f is irreducible then $\bar{f} = ug^k$, where u in $\mathbb{F}_q$ and g is monic irreducible in $\mathbb{F}_q[x]$.

iii. If f is in D then f is irreducible if and only if f is basic irreducible.

Definition 3.16 *Two polynomials $f(x)$ and $g(x)$ in $R[x]$ are called coprime if $\langle f(x)\rangle + \langle g(x)\rangle = R[x]$. The polynomials f and g are called associated if there exists an invertible element u of R such that $f = ug$.*

The following so-called Hensel's lemma guarantees that factorizations into product of pairwise coprime polynomials in $\mathbb{F}_q$ lift to such factorizations over R.

Lemma 3.2 *Let $g(x)$ be a monic polynomial in $R[x]$. Assume that there are monic, pairwise coprime polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ in $\mathbb{F}_q[x]$ such that $\overline{g(x)} = \prod_{i=1}^{i=k} f_i(x)$, then there are monic pairwise coprime polynomials $g_1(x), g_2(x), ..., g_k(x)$ in $R[x]$ such that $g(x) = \prod_{i=1}^{i=k} g_i(x)$ and $\overline{g_i(x)} = f_i(x)$, for all $0 \leq i \leq k$.*

Lemma 3.3 *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, and e be the nilpotency of γ. If f is a regular basic irreducible polynomial of the ring $R[x]$, then $R[x]/\langle f\rangle$ is also a chain ring with precisely the following ideals*

$$\langle 0\rangle, \langle 1\rangle, \langle 1 + \langle f\rangle\rangle, \langle \gamma + \langle f\rangle\rangle, \langle \gamma^2 + \langle f\rangle\rangle, ..., \langle \gamma^{e-1} + \langle f\rangle\rangle$$

Theorem 3.4 *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, and e is the nilpotency of γ. Let $x^n-1=f_1f_2...f_r$ be a representation of x^n-1 as a product of basic irreducible pairwise-coprime polynomials in $R[x]$. Then any ideal in $R[x]/\langle x^n-1\rangle$ is a sum of ideals of the form $\langle\gamma^j\widehat{f}+\langle x^n-1\rangle\rangle$ where $0\leq j\leq e$, $0\leq i\leq r$ and $\widehat{f}=\dfrac{x^n-1}{f}$.*

3.3 Frobenius Rings

Definition 3.17 *Let R be a commutative ring. Then the Jacobson radical $J(R)$ of R is the intersection of all maximal ideals of R.*

Definition 3.18 *A module M over R is simple if it is non-zero and does not admit a proper non-zero submodule. And it is semisimple if it is a sum of simple submodules. Thus, simple modules are cyclic.*

‘

Definition 3.19 *Let M be an R-module. Then its socle is the submodule*

$$SocM=\sum\{N|N \text{ is a simple submodule of } M\}$$

So the socle of M is the largest submodule of M generated by simple modules, or equivalently, it is the largest semisimple submodule of M. It is also the sum of the minimal R -submodules.

Definition 3.20 *An R-module M is injective if for all R-module homomorphisms $\phi:E\longrightarrow F$ and $\psi:E\longrightarrow M$ where ϕ is injective, there exists an R-linear homomorphism $\theta:F\longrightarrow M$ such that $\theta o\phi=\psi$.*

Theorem 3.5 *An R-module M is injective if and only if every R-module homomorphism $\mathfrak{m}\longrightarrow M$, where $\mathfrak{m}$ is an ideal, extends to an homomorphism $R\longrightarrow M$.*

Definition 3.21 *A commutative finite ring R is Frobenius if R as R-module is injective. Alternatively, we can say a finite ring R is Frobenius if $R/J(R)$ is isomorphic to $soc(R)$ (as R-modules)*

Bibliography

[1] A. Alahmadi, S. Alsulami, R. Hijazi, P. Sole, Isodual Cyclic Codes over Finite Fields of odd Characteristic, Discrete Mathematics, vol. 339, pp. 344-353, 2016

[2] E. F. Assmus, J. D. Key, Designs and Their Codes, Cambridge, Cambridge Univ. Press, 1992.

[3] M. F. Atiyah, I. G. Macdonald, Introduction To Commutative Algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. (1969)

[4] A. Batoul, K. Guenda and T. A. Gulliver, Some Constacyclic Codes over Finite Chain Rings, Advances in mathematics of communications, Vol. 10, no 4, pp. 683-694, 2016.

[5] A. Batoul, K. Guenda, T. A. Gulliver and N. Aydin, On Isodual Cyclic Codes over Finite Chain Rings, In : EL Hajji S., Nitaj A., Souidi E. (eds) Codes, Cryptology, and Information Security C2SI-Carlet. Lecture Notes in Computer Science, Vol 10194, pp. 176-194, 2017.

[6] A. Batoul, K. Guenda and T. A. Gulliver, Constacyclic Codes over Finite Principal Ideal Rings. In : EL Hajji S., Nitaj A., Souidi E. (eds) Codes, Cryptology, and Information Security C2SI-Carlet. Lecture Notes in Computer Science, Vol 10194, pp. 161-175, 2017.

[7] A. Batoul, K. Guenda and T. A. Gulliver, Repeated-Root Isodual Cyclic Codes over Finite Fields. In : EL Hajji S., Nitaj A., Carelet C., Souidi E. (eds) Codes, Cryptology, and Information Security C2SI-Carlet. Lecture Notes in Computer Science, Vol 9084, pp. 119-132, 2015.

[8] A. Batoul, K. Guenda, A. Kaya, and B. Yildiz: Cyclic Isodual and Formally Self-Dual Codes over $\mathbb{F}_q + v\mathbb{F}_q$. EJPAM Vol. 8, No.1, pp. 64-80, 2015.

[9] F. Benahmed, K. Guenda, A. Batoul and T. A. Gulliver, Some New Constructions of Isodual and LCD Codes over Finite Fields. Advances in Mathematics of Communications, Vol. 13, No. 2, pp. 281-296, 2019.

[10] Benyettou, A., Batoul, A. and Fernández-Córdoba, C. On LCD, Self Dual and Isodual Cyclic Codes over Finite Chain Rings. Finite fields and their applications. 2022.

[11] N. Benbelkacem, J. Borges, S. T. Dougherty and C. Fernandez-Cordoba, On $\mathbb{Z}_2\mathbb{Z}_4$-Additive Complementary Dual Codes and Related LCD Codes, Finite Fields Appl., Vol. 62, 2020.

[12] D.J. Bernstein, J. Buchmann and E. Dahmen, Post-Quantum Cryptography. Library of Congress Control Number: 2008937466. Mathematics Subject Classification Numbers (2000): 94A60.

[13] S. Bhowmick, A. Fotue-Tabue, E. Martinez-Moro, R. Bandi, S. Bagchi, Do Non-Free LCD Codes over Finite Commutative Frobenius Rings Exist?, Designs, Codes and Cryptography, Vol. 88, pp. 825-840, 2020.

[14] G. Bini and F. Flamini : Finite Commutative Rings and Their Applications, book April 24, 2015

[15] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi; Orthogonal Direct Sum Masking a Smartcard Friendly Computation Paradigm in a Code, With Builtin Protection Against Side-Channel and Fault Attacks In WISTP, volume 8501 of Lecture Notes in Comput. Sci., pp. 40-56. Springer, Berlin, 2014.

[16] C. Carlet and S. Guilley, Complementary Dual Codes For Counter Measures To Side-Channel Attacks, in Coding Theory and Applications (CIM Series in Mathematical Sciences), vol. 3, E. R. Pinto et al., Eds. Cham, Switzerland: Springer-Verlag, 2014.

[17] C. Carlet, S. Guilley, Complementary Dual Codes For Counter Measures To Side-Channel Attacks. Adv. Math. Commun. 10(1), pp. 131-150, 2016.

[18] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaam, Linear Codes over $\mathbb{F}_q$ Are Equivalent To LCD Codes For $q > 3$. IEEE Trans. Inf. Theory 64(4), pp. 3010-3017, 2018.

[19] C. Carlet, S. Mesnager, C. Tang and Y. Qi, On σ -LCD Codes, preprint arXiv:1707.08789, 2017.

[20] E. J. Cheon, Equivalence Of Linear Codes With The Same Weight Enumerator, Scientiae Mathematicae Japonicae Online, e-2006, pp 567âĂŞ576

[21] M. Demazure, Cours DâĂŹAlgebre : Primalite, Divisibilit, Codes, Cassini, Paris, 1997.

[22] H. Q. Dinh and S. R. López-Permouth, Cyclic and Negacyclic Codes over Finite Chain Rings, IEEE Transactions on Information Theory, Vol. 50, No. 8, pp. 1728-1744, 2004.

[23] S. T. Dougherty: Algebraic Coding Theory Over Finite Commutative Rings. SpringerBriefs in Mathematics ISBN 978-3-319-59805-5. 2017.

[24] S. T. Dougherty, J. Kim, H. Kulosman, MDS Codes over Finite Principal Ideal Rings. Des. Codes and Cryptogr. 50(1), pp. 77-92 2009.

[25] S. T. Dougherty and K. Shiromoto , MDR Codes over $\mathbb{Z}_k$. IEEE Trans. Inform Theory, 46; pp. 265-269, 2000.

[26] S. T. Dougherty, J. Gildea, A. Kaya and B. Yildiz, New Self Dual and Formally Self Dual Codes From Group Rings Constructions. Advances in Mathematics of Communications. Volume 14, No. 1, pp. 11-22, 2020.

[27] S. T. Dougherty, M. Harada, P. Solé, Self-Dual Codes over Rings and The Chinese Remainder Theorem. Hokkaido Math. J. 28, pp. 253-283, 1999.

[28] V. Dragoiy, T. Richmondz, D. Bucerzan, and A. Legayz. Code-Based Cryptography: from Theoretical to Physical Cryptanalysis. Published in: 2018 7th International Conference on Computers Communications and Control (ICCCC).

[29] K. Guenda, Sur l'équivalence des codes; thèse, USTHB 2010.

[30] K. Guenda and T. A. Gulliver, Self dual repeated root cyclic and negacyclic codes over finite fields. IEEE International Symposium on Information Theory Proceedings. doi:10.1109/isit.2012.6284057. 2012.

[31]] K. Guenda and T.A. Gulliver, On The Equivalence of Cyclic and QuasiCyclic Codes over Finite Fields, J. Algebra Comb. Discrete Appl., vol. 4, no. 3, pp. 261-269, 2017.

[32] K. Guenda and T. A. Gulliver, MDS and Self-Dual Codes over Rings, Finite Fields Appl., Vol. 18, pp. 1061-1075, 2012.

[33] A. R. Hammons, J. P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes, IEEE Trans. Inform. Theory, Vol. 40, No. 2, pp. 301-319, 1994.

[34] W. Cary Huffman and Vera S. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[35] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory. Springer-Verlag, New York, 1982.

[36] Y. Jia, S. Ling, and C. Xing, On Self-Dual Cyclic Codes over Finite Fields, IEEE Trans. Inf. Theory 57, pp. 2243-2251, 2011

[37] D. Jungnickel, Finite Fields: Structure and Arithmetics, Mannheim, BI-Wiss.-Verl., 1993.

[38] X. Kai, S. Zhu, On cyclic Self-Dual codes, Appl. Algebra Eng., Commun. Comput. 19 , pp. 509-525, 2008.

[39] P. Kanwar, S.R. Lopez-Permouth: Cyclic Codes over The Integers Modulo p^m. Finite Fields Appl. 3(4), pp. 334-352 (1997).

[40] J. Kaur. Cyclic Codes over Galois Rings Ph.D Thesis PEC University of Technology (2017).

[41] J. L. Kim and W. H. Choi; Self Dual codes Over $GF(q)$ With Symmetric Generator Matrices. arXiv:2009.06609v2.

[42] T. Y. Lam, : Lectures on Modules and Rings. Graduate Texts in Mathematics, vol. 189. SpringerVerlag, New York (1999).

[43] C. Li, C. Ding, and S. Li, LCD Cyclic Codes Over Finite Fields. IEEE Trans. Inform. Theory, Vol. 63, pp. 4344-4356, 2017.

[44] S. Li, C. Li, C. Ding, and H. Liu, Two Families of LCD BCH Codes, IEEE Trans. Inf. Theory, vol 63, no. 9, pp. 5699-5717, 2017.

[45] E. R. Lina and E. G. Nocon, On the Construction of Some LCD Codes over Finite Fields, Manila Journal of Science, Vol. 9, pp. 67-82, 2016.

[46] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge, Cambridge University Press, 1986.

[47] X. Liu and H. Liu, LCD Codes over Finite Chain Rings. Finite Fields and Appl., Vol. 34, pp. 1-19, 2015.

[48] Z. Liu and J. Wang, Linear Complementary Dual Codes over Rings. Designs, Codes and Cryptography, Vol. 87, pp. 3077-3086, 2019.

[49] R. J. Mc Eliece, Finite Fields for Computer Scientists and Engineers, Boston, Kluwer Accademic Publ., 1987.

[50] F. J. Mac Williams, N. J. A. Sloane, and J. M. Goethal, The MacWilliams Identities for Nonlinear Codes. Îď he Bell System Technical Journal, Vol. 51, No. 4 , April, 1972 .

[51] F. J. MacWilliams, N. J. A. Sloane : The Theory of Error-Correcting Codes. North-Holland, Amsterdam, 1981.

[52] H. Matsumura : Commutative Ring Theory, 2nd edn. Cambridge Studies in Advanced Mathematics, vol. 8. Cambridge University Press, Cambridge, 1989. (Translated from the Japanese by M. Reid).

[53] J. L. Massey, Linear Codes With Complementary Duals, Discrete Math, 106/107, pp. 337-342, 1992.

[54] B. R. McDonald, Finite Rings With Identity, Pure and Applied Math., 28, Marcel Dekker, New York, NY, 1974.

[55] S. Mesnager, C. Tang and Y. Qi, Complementary Dual Algebraic Geometry Codes, IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 2390- 2397, 2018.

[56] G. Nebe, E. M. Rains and N. J. A. Sloane. Self-Dual Codes and Invariant Theory. SpringerVerlag, 2006

[57] G. H. Norton and A. Salagean, On The Structure of Linear and Cyclic Codes over a Finite Chain Ring, Appl. Algebra Engr. Comm. Comput., Vol. 10, No. 6, pp. 489-506, 2000.

[58] E. M. Rains and N. J. A. Sloane, Self Dual Codes; Information Sciences Research ATT Labs-Research 180 Park Avenue Florham Park NJ 07932-0971. May 98.

[59] N. Sendrier, Linear codes with complementary duals meet the GilbertâĂŞVarshamov bound, Discrete Mathematics 285, pp 345 âĂŞ 347, 2004

[60] M. Shi, L. Xu, P. Sole; Construction of isodual codes from polycirculant matrices. Designs, Codes and Cryptography https://doi.org/10.1007/s10623-020-00799-8.

[61] M. Shi, A. Alahmadi, P. Sole; Codes and Rings, Paperback ISBN: 9780128133880, eBook ISBN: 9780128133910.

[62] X. Yang and J. L. Massey, The Condition for a Cyclic Code To Have a Complementary Dual, Discrete Math, Vol. 126, pp. 391-393, 1994.

[63] S. A. Vanstone and P. Van Oorschot; Introduction To Error Correcting Codes With Applications, Library of Congress Cataloging-In-Publication Data, ISBN 978-1-4419-5117-5 ISBN 978-1-4757-2032-7 (eBook), 1989.

[64] J. Wood, Duality for Modules over Finite Rings and Applications To Coding Theory, Am. J. Math. 121, pp. 555-575, 1999.

[65] J. Wood, Weight Functions and The Extension Theorems For Linear Codes over Finite Rings : Finite Fields: Theory, Applications and Algorithms, in: Contemp. Math., vol. 225, AMS, Providence, pp. 231-243, 1999.