FINITE CHAIN RINGS AND APPLICATIONS TO CODING THEORY

by

Ü. Ümare KARA

A thesis submitted to

the Graduate Institute of Sciences and Engineering

of

Fatih University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

June, 2012

Istanbul TURKEY

APPROVAL PAGE

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Professor Feyzi BAŞAR
Head of Department

This is to certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist. Prof. Bahattin YILDIZ
Supervisor

Examining Committee Members

Assist. Prof. Bahattin YILDIZ .....

Prof. Evgenii BASHKIROV .....

Assist. Prof. Tuğrul YANIK .....

It is approved that this thesis has been written in compliance with the formatting rules laid down by the Graduate Institute of Sciences and Engineering.

Assoc. Professor Nurullah ARSLAN
Director

FINITE CHAIN RINGS AND APPLICATIONS TO CODING THEORY

Ü. Ümare KARA

M S, Thesis-Mathematics

Supervisor: Assist. Prof. Bahattin YILDIZ

ABSTRACT

In this thesis, we consider finite chain rings and their connection to Coding theory. After reviewing some of the previously known results about cyclic, negacyclic and constacyclic codes over finite chain rings, we take a special chain ring, $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$, of size 16. Working out some of the structure of the ring, we introduce the Lee distance and Gray maps on this ring and we study the cyclic and constacyclic codes over $\mathcal{S}_4$. In particular, some optimal or near optimal binary codes are obtained from the Gray images of cyclic and $(1+u^2)$-constacyclic codes over $\mathcal{S}_4$.

Keywords: Finite chain rings, Cyclic codes, Negacyclic codes, Constacyclic codes.

SONLU ZİNCİR HALKALARI VE KODLAR TEORİSİNE UYGULAMALARI

Ü. Ümare KARA

Yüksek Lisans Tezi-Matematik

Tez Yöneticisi: Yrd. Doç. Dr. Bahattin YILDIZ

ÖZ

Bu tezde, sonlu zincir halkaları ve bu halkaların kodlar teorisi ile bağlantısı ele alındı. Sonlu zincir halkaları üzerinde tanımlı devirli, nega-devirli ve konsta-devirli kodlar hakkında literatür taraması yapıldıktan sonra 16 elemanlı zincir halkası olan $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ üzerinde çalışıldı. Bu halka üzerinde Lee ağırlık ve bu ağırlıklara karşılık gelen Gray eşlemeler tanımlandı ve $\mathcal{S}_4$ üzeindeki devirli ve konsta devirli kodlar çalışıldı. Bu halka üzerindeki devirli ve $(1+u^2)$-konsta-devirli kodların Gray görüntüleri olarak optimal ve optimale yakın ikili kodlar elde edildi.

Anahtar Kelimeler: Sonlu zincir halkaları, Devirli kodlar, Nega devirli kodlar, Konsta devirli kodlar.

TABLE OF CONTENTS

DEDICATION

To my family, my advisor, my friends.

ACKNOWLEDGEMENTS

I would like to thank first and foremost my supervisor Assist. Prof. Bahattin YILDIZ for his ceaseless help and advice throughout the research.

I would like to express my great appreciation and special thanks to my friend Zeynep Ödemiş Özger for her support, valuable information and comments on my academic and scientific problems.

I would also like to thank my committee for their evaluation and comments.

Finally, I would like to thank my family for their encouragement and patience.

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Coding Theory originated from the work of Shannon as the mathematical foundation for the transmission of messages over noisy channels. Information media are not absolutely reliable in practice because of the noise. Coding theory deals with the problem of detecting and correcting transmission errors caused by noise on the channel. The following diagram provides an idea of a general information transmission system.

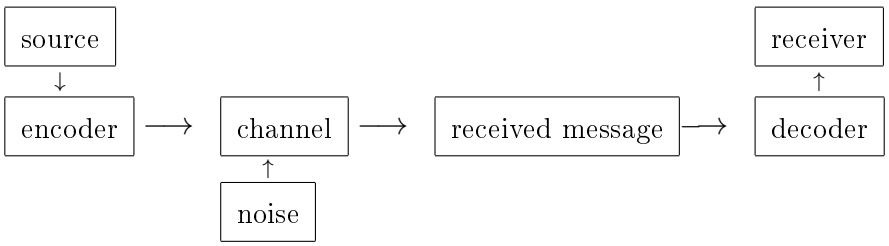

Figure1.1 Transmission process of data.

In early periods of Coding Theory, codes over finite fields, especially the ones over $\mathbb{F}_2$ which are called binary codes were studied. Later rings entered the field of coding theory because of their rich algebraic structure. One of the pioneer works about this idea was "The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes" by Hammons, Kumar et al in 1994. Since it is possible to encode more information with codes over rings than we can do within the same space by using codes over finite fields, the afore mentioned work can be stated as a milestone of Coding Theory.

Codes over rings of order 4 and their generalizations have been extensively studied. Cyclic and negacyclic codes over $\mathbb{Z}_4$ were studied by Wolfmann. In [7], Wolfmann showed that the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ of length n is a distance invariant cyclic code. In [43] he also determined all linear cyclic codes over $\mathbb{Z}_4$ of odd length whose Gray images are linear codes.

Another important alphabet of size 4 besides $\mathbb{Z}_4$ is $\mathbb{F}_2 + u\mathbb{F}_2$ and it has been studied by a lot of researchers [3], [4], [6], [30], [34]. (1+u)-constacyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ of odd length were first introduced by Qian et al. in [6]. (1+u)-constacyclic codes of an arbitrary length over $\mathbb{F}_2 + u\mathbb{F}_2$ were studied by Abualrub and Siap in [1].

In [11], Permouth and Dinh obtained structure theorems for cyclic and constacyclic codes over finite chain rings in a more general setting with the condition that the length of the code is not divisible by the characteristic of the residue field.

The most common type of rings worked in Coding Theory are finite chain rings. Their ideal structure has made it possible to extend many of the properties of codes over finite fields.

In this thesis, we first give a review of the properties of finite chain rings and we focus on cyclic, negacyclic and constacyclic codes over finite chain rings. In particular, we work out codes over $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ in more detail. We introduce a Lee weight and a Gray map for this ring and we work out the structure of cyclic and constacyclic codes over $\mathcal{S}_4$. In addition to the theoretical results, we construct many optimal and near optimal binary codes as images of cyclic and constacyclic codes. The rest of the thesis is organized as follows:

Chapter 2 includes basic definitions of coding theory that are needed in the thesis.

Chapter 3 includes finite chain rings and their properties in general and the most common finite chain rings used in Coding theory are given as examples.

In Chapter 4, linear codes over finite chain rings are introduced and basic concepts generalized to codes over finite chain rings are given.

Chapter 5 covers the structure of cyclic, negacyclic and constacyclic codes over a finite chain ring R as well as some properties related to the structure of the polynomial ring $R[x]/(x^n-1)$, where n is the length of the code. Special cases such as n being relatively prime to the characteristic of the ring are explored.

In Chapter 6, we introduce the ring $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$. We give structure theorems and fundamental properties of the ring. Linear codes over the ring are investigated in a general setting. MacWilliams-like identities are obtained. Lee weight and the corresponding Gray map are defined for the codes over $\mathcal{S}_4$. The binary images of linear codes over $\mathcal{S}_4$ under the Gray map are studied. Cyclic and constacylic codes over $\mathcal{S}_4$ are studied. One-generator cyclic codes are classified.

CHAPTER 2

PRELIMINARIES

We first start with a general overview of some of the basic concepts of Coding Theory. We refer to [16] and [26] for more.

Definition 2.0.1. *Let $\mathbb{F}_q^n$ be the vector space of all n-tuples over the finite field $\mathbb{F}_q$, where q is a prime power.*

1. An (n, M) **code** C **over** $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ of size M.
2. The vectors $(a_1, a_2, \cdots, a_n)$ in C are called **codewords**.
3. The number of codewords in C, denoted by $|C|$, is called the **size** of C.
4. Such a code C is called a $q-$ary code. If $q = 2$, it is called a binary code, and if $q = 3$, then it is called a ternary code.

Definition 2.0.2. *The **(Hamming) distance** $d_H(x, y)$ between two vectors $x, y \in \mathbb{F}_q^n$ is defined to be the number of coordinates in which x and y differ. If $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$, then*

$$d_H(x, y) = d_H(x_1, y_1) + \cdots + d_H(x_1, y_1)$$

where x_i and y_i are regarded as words of length 1, and

$$d_H(x_i, y_i) = \begin{cases} 1 & \text{if } x_i \neq y_i \\ 0 & \text{if } x_i = y_i, \end{cases}$$

Example 2.0.3. *Let x, y be codewords over $\mathbb{F}_2$ such that $x = (0101101)$, $y = (0110110)$, then $d_H(x, y) = 4$.*

Definition 2.0.4. *The **minimum distance of a code** C, denoted by $d(C)$, is the smallest distance between distinct codewords of C, i.e.*

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

The minimum distance of a code is a very important parameter of the code as it determines the error correcting capability of the code. More precisely we have the folllowing theorem:

Theorem 2.0.5. *A code C is u-error-detecting if and only if $d(C) \geq u + 1$; i.e., a code of minimum distance d is an exactly $(d-1)-$error-detecting code.*

Proof. Suppose $d(C) \geq u + 1$. If $c \in C$ and x are such that $1 \leq d(c, x) \leq u < d(C)$, then $x \notin C$; hence, C is u-error-detecting. On the other hand, if $d(C) < u + 1$, i.e., $d(C) \leq u$, then there exist c_1, $c_2 \in C$ such that $1 \leq d(c_1, c_2) = d(C) \leq u$. It is therefore possible that we begin with c_1 and $d(C)$ errors (where $1 \leq d(C) \leq u.$) are incurred such that the resulting word is c_2, another codeword in C. Hence, C is not $(u + 1)-$error-detecting code. □

Theorem 2.0.6. *A code C is u-error-correcting if and only if $d(C) \geq 2u + 1$; i.e., a code with distance d is an exactly $\frac{\lfloor d-1 \rfloor}{2}$-error-correcting code. Here, $\lfloor x \rfloor$ is the greatest integer less than or equal to x.*

Definition 2.0.7. *A code of length n, size M and distance d is referred to as an (n, M, d)-code.*

Example 2.0.8. *Let $C = \{000000, 000111, 111222\}$ be a ternary code. Then $d(C) = 3$ since, $d(000000, 000111) = 3, d(000000, 111222) = 6$ and $d(111222, 000111) = 6$. Hence, C is a ternary $(6, 3, 3) - code$.*

Definition 2.0.9. ***Hamming weight*** *of a codeword is defined as the number of its nonzero coordinates, and is denoted by* w_H*. Here, notice that*

$$d_H(\bar{x}, \bar{y}) = w_H(\bar{x} - \bar{y}),$$

where $d_H(\bar{x}, \bar{y})$ *is the Hamming distance between two codewords* $\bar{x}$ *and* $\bar{y}$*, and* w_H *denotes the Hamming weight.*

In general, a **weight** is a function w from the ambient space to the set of non-negative integers. The weight function can be extended to codewords as follows: If $\bar{c} = (c_{1,}c_{2,} \cdots, c_n) \in C$, then $w(\bar{c}) = w(c_1) + w(c_2) + \cdots + w(c_n)$. In other words, the weight of a codeword is the sum of the weights of its coordinates.

Definition 2.0.10. *Let* C *be a code. The minimum Hamming weight of* C*, denoted* $w_H(C)$*, is the smallest of the weights of the nonzero codewords of* C*.*

Definition 2.0.11. *If* C *is a* k*-dimensional subspace of* $\mathbb{F}_q^n$*, then* C *will be called* ***an*** $[n, k]$ ***linear code over*** $\mathbb{F}_q$*. For codes over finite fields, we determine the size with the dimension. In the above expression,* k *is called the* ***dimension*** *of* C*.*

Definition 2.0.12. *Let* C *be a linear* $[n, k]$ *code. The set*

$$C^{\perp} = \left\{ x \in \mathbb{F}_q^n \mid x \cdot c = 0, \forall c \in C \right\}.$$

is called the dual code for C*, where* $x \cdot c$ *is the usual dot product of the vectors* x *and* c *in* $\mathbb{F}_q$*. Note that* $C^{\perp}$ *is an* $[n, n-k]-$*linear code.*

Theorem 2.0.13. *[16] Let* C *be a linear code of length* n *over* $\mathbb{F}_q$*. Then*

(i) $|C| = q^{\dim(C)}$*;*

(ii) $C^{\perp}$ *is a linear code and* $\dim(C) + \dim(C^{\perp}) = n$*,*

(iii) $\left(C^{\perp}\right)^{\perp} = C$*.*

Definition 2.0.14. *Let C be a linear code. C is called self-orthogonal if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$.*

Proposition 2.0.15. *A self dual-code must have even length.*

Proof. Suppose that C is a linear code of length n. By definition, $\dim(C) = \dim(C^{\perp})$. Recall that for a linear code we have $\dim(C) + \dim(C^{\perp}) = n$. Thus, $\dim(C) = n/2$. Therefore n must be even. □

Theorem 2.0.16. *Let C be a linear code over $\mathbb{F}_q$. Then $d(C) = w_H(C)$.*

Proof. By definition, there exist x', $y' \in C$ such that $d(x', y') = d(C)$, so

$$d(C) = d(x', y') = w_H(x' - y') \geq w(C),$$

since $x' - y' \in C$. Conversely, there is a $z \in C \setminus \{0\}$ such that $w_H(C) = w_H(z)$, so

$$w_H(C) = w_H(z) = d(z, 0) \geq d(C).$$

□

As seen from above, for linear codes it is relatively easier to determine the minimum distance of the code since it is equal to the minimum weight of the code. However, for nonlinear codes, the complexity of the problem of finding the minimum distance is much higher compared to linear codes. For example, consider the binary linear code $C = \{0000, 1000, 0100, 1100\}$.

We see that

$$w_H(1000) = 1,$$

$$w_H(0100) = 1,$$

$$w_H(1100) = 2.$$

Hence $d_{\min}(C) = 1$.

The encoding and decoding procedure for linear codes are faster and simpler than those for arbitrary nonlinear codes.

In coding theory, a basis for a linear code is often represented in the form of a matrix, called a generator matrix, while a matrix that represents a basis for the dual code is called a parity-check matrix. These matrices play an important role in coding theory.

Definition 2.0.17. *A **generator matrix for** an $[n, k]$ code C is any $k \times n$ matrix G whose rows form a basis for C. A 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, is said to be in the standard form.*

Definition 2.0.18. *The **parity-check matrix** H for a $[n, k]-$ code C is a generator matrix for the dual code $C^{\perp}$. Thus H is an $(n-k) \times n$ matrix satisfiying*

$$C = \left\{ c \in F_q^n \mid Hc^{\perp} = 0 \right\}.$$

Theorem 2.0.19. *If* $G = [I_k \mid A]$ *then* $H = \left[-A^T \mid I_{n-k}\right]$.

Proof. Obviously, the equation $HG^T = 0$ is satisfied. By considering the last $n-k$ coordinates, it is clear that the rows of H are linearly independent. □

Example 2.0.20. *The generating matrix for the binary Hamming code* $Ham(3,2)$*, which is a* $[7,4,3]$*-code, is given by the following:*

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

Hence, by Theorem 5.0.45, a parity-check matrix for $Ham(3,2)$ *is*

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

While certain linear codes may not have a generator matrix in the standard form, after a suitable permutation of the coordinates of the codewords and possibly multiplying certain coordinates with some unit, one can always arrive at a new code which has a generator matrix in the standard form.

Definition 2.0.21. *Two* $(n, M)-$*codes over* $\mathbb{F}_q$ *are* ***equivalent*** *if one can obtained from the other by a combination of operations of the following types:*

i) permutation of the n digits of the codewords;

ii) multiplication of the symbols appearing in a fixed position by a unit.

Example 2.0.22. *Let $q = 2$ and $n = 4$. Apply the permutation $(12)(34)$ to the coordinates, wee see that the code*

$$C = \{0000, 0011, 0110, 0101\}$$

is equivalent to the code

$$C' = \{0000, 0011, 1001, 1010\}.$$

CHAPTER 3

FINITE CHAIN RINGS

In order to explain our work in this thesis, we need to understand finite chain rings. This chapter is dedicated to finite chain rings and their properties in general.

Definition 3.0.23 (Finite Chain Ring)**.** *A finite commutative ring with identity* $1 \neq 0$ *is called a* ***finite chain ring*** *if its ideals are linearly ordered by inclusion.*

Definition 3.0.24 (Local Ring)**.** *A commutative ring* R *is called* ***local*** *if it has a unique maximal ideal.*

Remark 3.0.25. *A finite chain ring has a unique maximal ideal. For example,*$\mathbb{Z}_{p^m}$ *is a chain ring with unique maximal ideal* $p\mathbb{Z}_{p^m}$

For the class of finite commutative chain rings, we have the following equivalent conditions :

Lemma 3.0.26. *[11] For a finite commutative ring* R *the following are equivalent:*

i) R *is a local ring with the maximal ideal* m *of* R *is principal.*
ii) R *is a local principal ideal ring.*
iii) R *is a chain ring.*

We first give some preliminaries about the structure of finite chain rings:

Definition 3.0.27 (Nilpotency Index). *Let R be a finite commutative chain ring and m be its unique maximal ideal, and let γ be the generator of the unique maximal ideal m. Then one has $m = \langle\gamma\rangle = R\gamma$, where $R\gamma = \langle\gamma\rangle = \{\beta\gamma|\beta \in R\}$. Also,one has $R = \langle\gamma^0\rangle \supseteq \langle\gamma^1\rangle \supseteq \cdots \supseteq \langle\gamma^d\rangle \supseteq \cdots$. This chain is finite since R is finite. Suppose for a d, $\langle\gamma^d\rangle = \{0\}$. Let e be the minimal positive integer such that $\langle\gamma^e\rangle = \{0\}$, then e is defined as the **nilpotency index** of γ (of R).*

Let $|R|$ denote the cardinality of R and $R^\times$ the set of all units in R. $R^\times$ is a multiplicative group under the multiplicative operation of R. Let $\bar{R} = R/m = R/\langle\gamma\rangle$ be the residue field with characteristic p, where p is a prime number. There exist integers q and k such that $|\bar{R}| = q = p^k$ and $|\bar{R}^\times| = \bar{R} - \{0\}$. Thus that $|\bar{R}^\times| = p^k - 1$. There is a form of unique factorization in R:

Lemma 3.0.28. *[12] For any $0 \neq a \in R$ there is a unique integer d, $0 \leq d \leq e$ such that $a = \mu\gamma^d$, with μ as a unit. The unit μ is unique modulo γ^{e-d} only.*

Lemma 3.0.29. *[12] Let R be a finite chain ring with maximal ideal $m = \langle\gamma\rangle$, where γ is the generator of m with nilpotency index e. Let $V \subseteq R$ be the set of representatives for the equivalence classes of R under congruence modulo γ. Then,*

1. *There exists unique $a_0, a_1, a_2, \cdots, a_{e-1} \in V$ such that $a = \sum_{d=0}^{e-1} a_d\gamma^d$, where $a \in R$.*
2. *$|V| = |\bar{R}|$.*
3. *$|\langle\gamma^b\rangle| = |\bar{R}|^{e-b}$ for $0 \leq b \leq e-1$.*

By this lemma, it is known that every element $a \in R$ can be written uniquely as $a = a_0 + a_1\gamma, \cdots, a_{e-1}\gamma^{e-1}$ where $a_d \in F_{p^k} \cong R/\langle\gamma\rangle$.

Example 3.0.30. *$R = \mathbb{F}_2 + u\mathbb{F}_2 := \mathbb{F}_2[u] / < u^2 >$ is a commutative ring $\{0, 1, u, 1+u\}$ with $u^2 = 0$. It is easy to verify that R is a local ring with the maximal ideal given by $\{0, u\} = \langle u \rangle$. It is a chain ring with ideals $\{0\} \subseteq \{0, u\} \subseteq R$. The multiplication and addition tables for the ring are given as follows:*

$+$	0	1	u	$u+1$
0	0	1	u	$u+1$
1	1	0	$u+1$	u
u	u	$u+1$	0	1
$u+1$	$u+1$	u	1	0

$\cdot$	0	1	u	$u+1$
0	0	0	0	0
1	0	1	u	$u+1$
u	0	u	0	u
$u+1$	0	$u+1$	u	1

The multiplication coincides with that of $\mathbb{Z}_4$, when u and $1+u$ are replaced by, respectively, 2 and 3. In this sense, R is analogous to $\mathbb{Z}_4$ and here u plays the role of 2. The addition table is similar to that of the Galois field $\mathbb{F}_4 = \{0, 1, \beta, \beta^2 = \beta + 1\}$, when u and $1+u$ are replaced by, respectively, β and β^2. Note that the characteristic of the ring is 2. Thus in the structure of alphabets, R lies between $\mathbb{Z}_4$ and $\mathbb{F}_4$. This ring can also be viewed as a vector space of dimension 2 over $\mathbb{F}_2$. Moreover, the sets $\{0, 1\}$, $\{0, u\}$ and $\{0, 1+u\}$ form three subspaces in R and the subspace $\{0, 1\} = \mathbb{F}_2$ is a subring. This ring can easily be generalized to $\mathbb{F}_2[u] / < u^k >$. Many of the properties are the same.

Example 3.0.31. *$\mathbb{Z}_{p^m} = \mathbb{Z}/p^m\mathbb{Z}$ is a finite chain ring. The ideals in the ring $\mathbb{Z}_{p^m}$ form the chain*

$$p\mathbb{Z}_{p^m} \supset p^2\mathbb{Z}_{p^m} \supset \cdots \supset p^{m-1}\mathbb{Z}_{p^m} \supset p^m\mathbb{Z}_{p^m} = (0)$$

$\mathbb{Z}_{p^m}$ is a local ring with unique maximal ideal $p\mathbb{Z}_{p^m}$.

Example 3.0.32 (Galois Ring)**.** *We define, $GR(p^a, l) = \mathbb{Z}_{p^a}[X]/(f)$ where p is a prime number, $a \geq 1$ and $f \in \mathbb{Z}_{p^a}[X]$ is a monic basic irreducible polynomial of degree l. The ring $GR(p^a, l)$ is called a Galois ring and has p^{al} elements.*

Note that for $l = 1$ we obtain the ring $\mathbb{Z}_{p^a}$. For $a = 1$ we obtain the finite field with p^l elements, $GF(p^l)$. For $a \geq b$, there is a natural projection homomorphism(reduction modulo p^b) of $GR(p^a, l)$ to $GR(p^b, l)$ with kernel $GR(p^a, l)p^b$. For any multiple m of l there is an inclusion homomorphism $GR(p^a, l) \subseteq GR(p^a, m)$. A Galois ring $GR(p^a, l)$ is a finite chain ring with maximal ideal generated by p, the nilpotency index of p is a and the residue field is $GF(p^l)$. Any finite chain ring is a certain homomorphic image of a polynomial ring $GR(p^a, l)[X]$.

For example, for $h(x) = x^3 + x + 1 \in \mathbb{Z}_4[X]$ which is monic, basic irreducible over $\mathbb{Z}_4$, we obtain

$$\begin{aligned} GR(2^2, 3) &= \mathbb{Z}_4[X] / \langle h(x) \rangle \\ &= \{0, 1, 2, 3, x, 1+x, 2+x, 3+x, 2x, 2x+1, 2x+2, 2x+3, 3x, ...\} \end{aligned}$$

It has been shown that Frobenius rings are the largest class of rings for which codes over rings should be studied. Because two classical theorems of MacWilliams generalize to the case of finite Frobenius rings [15].

Proposition 3.0.33. *Finite chain rings are Frobenius rings.*

For the proof of this proposition we use the following result in [15]. If R is a local ring with maximal ideal $m = \langle \gamma \rangle$, and residue field k, then the following conditions on R are equivalent:

1. R is Frobenius
2. $\dim_k Ann(m) = 1$.

Since R is a local ring with maximal ideal $m = \langle \gamma \rangle$, $Ann(m) = \{\gamma^{e-1} a \mid a \in k\} = \langle \gamma^{e-1} \rangle_k$, where e is the nilpotency index of γ. So we have that $\dim_k Ann(m) = 1$. Then R is a Frobenius ring.

CHAPTER 4

CODES OVER FINITE CHAIN RINGS

In this chapter we introduce codes over finite chain rings. Codes over finite chain rings have been studied quite extensively in the literature. For some of these we refer to [2], [7], [11], [22], [27], [29], [35], [1]. We will now give more detailed versions of basic concepts generalized to codes over finite chain rings.

Definition 4.0.34. *Let R be a finite chain ring. A linear code C of length n over R is an $R-$submodule of R^n.*

Let R be a finite chain ring with maximal ideal $m = \langle\gamma\rangle$, where γ is the generator of m with nilpotency index e. C is equivalent to a code with generating matrix of the following form:

$$G = \begin{bmatrix} I_{k_1} & A_1 & \cdot & \cdot & \cdot & A_s \\ 0 & \gamma I_{k_2} & \gamma B_1 & \cdot & \cdot & \gamma B_{s-1} \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & 0 & \gamma^{e-1} I_{k_e} & \gamma^{e-1} C \end{bmatrix}$$

where $A_i, B_j, \cdots, C$ are all matrices over R. Every codeword $\bar{c} \in C$ can be written as a linear combination of the rows of G over R.

For linear codes over rings the concept of dimension does not work but we can define its type. A linear code which has the above matrix G as its generating matrix is said to be of type

$$\{k_1, \cdots, k_e\}$$

In this case we will have

$$|C| = |R/m|^{\sum_{d=0}^{e-1}(e-d)k_{d+1}} = \left|\bar{R}\right|^{\sum_{d=0}^{e-1}(e-d)k_{d+1}}$$

Example 4.0.35. *A linear code over $\mathbb{Z}_{2^s}$ of length j is permutationally equivalent to a code that has a generating matrix of the following form:*

$$\begin{bmatrix} I_{k_1} & A_1 & \cdot & \cdot & \cdot & A_{s-1} \\ 0 & 2I_{k_2} & 2B_1 & \cdot & \cdot & \cdot \\ 0 & 0 & 2^2 I_{k_3} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 2^{s-2}I_{k_{s-1}} & 2^{s-2}D \\ 0 & 0 & \cdot & 0 & 0 & 2^{s-1}I_{k_s} \end{bmatrix}$$

where $A_1, \cdots, A_{s-1}, B_1, \cdots, D$ are matrices over $\mathbb{Z}_{2^s}$. Such a code is said to be of type $(2^s)^{k_1}(2^{s-1})^{k_2} \cdots (2)^{k_s}$, and has size

$$|C| = 2^{sk_1+(s-1)k_2+\cdots+k_s}.$$

Example 4.0.36. *A linear code C over $\mathbb{F}_2 + u\mathbb{F}_2$ has a generating matrix which, after a suitable permutation of the coordinates, can be written in the form:*

$$\begin{bmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

where A, B, D are matrices over $\mathbb{F}_2 + u\mathbb{F}_2$. C contains $4^{k_1}2^{k_2}$ codewords.

We recall some of the well known weight functions for codes over rings:

The Hamming weight, which is mentioned before, can be formulized as

$$w_H(x) := \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise.} \end{cases}$$

A special weight that was used in [14] before is **the Lee weight** on $\mathbb{Z}_4$, which we will denote by w_L, and is defined as

$$w_L(x) := \begin{cases} 0 & \text{if } x = 0 \\ 2 & \text{if } x = 2 \\ 1 & \text{otherwise.} \end{cases}$$

The lee weight a_r of an element r of the ring $\mathbb{F}_2 + u\mathbb{F}_2$ which was defined in [4] is given by

$$a_r := \begin{cases} 0 & \text{if } r = 0 \\ 1 & \text{if } r = 1 \text{ or } 1 + u \\ 2 & \text{if } r = u. \end{cases}$$

The following definition describes the homogenous weight in a more general setting as was explained in [13].

Definition 4.0.37. *A real valued function w on the finite ring R is called a* ***Homogenous weight****, if $w(0) = 0$ and the following are true:*

1. *For all $x, y \in R$, $Rx = Ry$ implies $w(x) = w(y)$*
2. *There exists a real number γ such that $\sum_{y \in Rx} w(y) = \gamma |Rx|$, for all $x \in R \backslash \{0\}$.*

Example 4.0.38. *Let R be a finite chain ring. The homogeneous weight $w_{\text{hom}}(x)$ of $x \in R$ is defined as follows:*

$$w_{\text{hom}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ d_1 & \text{if } 0 \neq x \in \gamma^{e-1}R \\ d_2 & \text{otherwise.} \end{cases}$$

Example 4.0.39. *The homogeneous weight for Galois rings is given by*

$$w_{\text{hom}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ p^{m(l-1)} & \text{if } 0 \neq x \in p^{l-1}GR(p^l, m) \\ (p^m - 1)p^{m(l-2)} & \text{otherwise.} \end{cases}$$

Example 4.0.40. *The homogeneous weight for $\mathbb{Z}_{p^s}$ is described as*

$$w_{\text{hom}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ p^{s-1} & \text{if } 0 \neq x \in p^{s-1}\mathbb{Z}_{p^s} \\ (p-1)p^{s-2} & \text{otherwise.} \end{cases} .$$

Definition 4.0.41 (Gray Map)**.** *A Gray map is a distance preserving map from R^n to $\mathbb{F}_q^{nl}$, where l is suitably defined and depends on R.*

The following are particular cases of the Gray maps for certain rings:

Example 4.0.42. *The Gray map of the Lee weight over* $\mathbb{Z}_4$ *is defined by*

$$\varphi_L : \mathbb{Z}_4 \to \mathbb{Z}_2^2,$$

where φ_L *is as follows:*

$$\varphi_L(0) = (00),\ \varphi_L(1) = (01),\ \varphi_L(2) = (11),\ \varphi_L(3) = (10).$$

Example 4.0.43. *The Gray map of the Lee weight over* $\mathbb{F}_2 + u\mathbb{F}_2$ *is defined by*

$$\varphi_L : \mathbb{F}_2 + u\mathbb{F}_2 \to \mathbb{F}_2^2,$$

where φ_L *is as follows:*

$$\varphi_L(0) = (00),\ \varphi_L(1) = (01),\ \varphi_L(u) = (11),\ \varphi_L(1+u) = (10).$$

CHAPTER 5

CYCLIC, NEGACYCLIC AND CONSTACYCLIC CODES OVER FINITE CHAIN RINGS

The purpose of this chapter is to obtain structure theorems of cyclic, negacyclic and constacyclic codes in a more general setting.

Definition 5.0.44 (Cyclic, Negacyclic and Constacyclic Codes)**.** *Let σ, ν_α ,π be maps from R^n to R^n given by $\sigma(a_0, a_1, a_2, \cdots, a_{n-1}) = (a_{n-1}, a_0, \cdots, a_{n-2})$; for α a unit in R, $\nu_\alpha(a_0, a_1, a_2, \cdots, a_{n-1}) = (\alpha a_{n-1}, a_0, \cdots, a_{n-2})$ and $\pi(a_0, a_1, a_2, \cdots, a_{n-1}) = (-a_{n-1}, a_0, \cdots, a_{n-2})$. Then the linear code C over R is said to be cyclic if $\sigma(C) = C$, $\alpha-$constacyclic if $\nu_\alpha(C) = C$ and negacyclic if $\pi(C) = C$.*

Note that, binary constacyclic and negacyclic codes are indeed cyclic codes.

In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider $P(C)$, the polynomial representation of C, i.e.,

$$P(C) = \left\{ \sum_{d=0}^{n-1} a_d x^d | (a_0, a_1, a_2, \cdots, a_{n-1}) \in C \right\}.$$

If $c(x)$ is a polynomial then $\sigma(c(x))$ corresponds to multiplying $c(x)$ by x in $R[X]/(x^n - 1)$, $\pi(c(x))$ corresponds to multiplying $c(x)$ by x in $R[X]/(x^n + 1)$ and $\nu_\alpha(c(x))$ corresponds to multiplying $c(x)$ by x in $R[X]/(x^n - \alpha)$.

So cyclic, negacyclic and constacyclic codes over R are identified with ideals in the rings $R[X]/(x^n-1)$, $R[X]/(x^n+1)$ and $R[X]/(x^n-\alpha)$. The following result connects ideals and cyclic, negacyclic, constacyclic codes.

Lemma 5.0.45.

(i) A subset C of R^n is a linear cyclic code of length n if and only if $P(C)$ is an ideal in the quotient ring $R[X]/(x^n-1)$.

(ii) A subset C of R^n is a linear α-constacyclic code of length n if and only if $P(C)$ is an ideal in the quotient ring $R[X]/(x^n-\alpha)$.

(iii) A subset C of R^n is a linear negacyclic code of length n if and only if $P(C)$ is an ideal in the quotient ring $R[X]/(x^n+1)$.

Let R be a finite chain ring, m the unique maximal ideal of R, and let $\bar{R}=R/m$ which is a finite field. For example, if $R=\mathbb{F}_2+u\mathbb{F}_2$, then $\bar{R}=\mathbb{F}_2$ and if $R=\mathbb{Z}_{p^m}$, then $\bar{R}=\mathbb{F}_p$.

Definition 5.0.46. *Two polynomials f_1, $f_2 \in R[x]$ are called coprime if $\langle f_1\rangle+\langle f_2\rangle = R[x]$.*

Definition 5.0.47. *A polynomial $f \in R[x]$ is called **basic irreducible** if $\bar{f}$ is irreducible in $\bar{R}[x]$ and called **regular** if it is not a zero divisor. Here $\bar{f}$ denotes the image of f under the canonical epimorphism from R to $\bar{R}=R/m$.*

For example, $f(x)=x^3+2x^2+3x+1$ is a basic irreducible polynomial in $\mathbb{Z}_4[x]$, because $\bar{f}(x)=x^3+x+1$ is an irreducible polynomial in $\mathbb{F}_2[x]$. Similarly, $x^2+(1+u)x+1+u$ is a basic irreducible polynomial in $(\mathbb{F}_2+u\mathbb{F}_2)[x]$, because $\bar{f}(x)$ is an irreducible polynomial in $\mathbb{F}_2[x]$.

Hensel lifting plays a key role in the construction of cyclic codes over R. The following lemma guarantees that factorizations into product of pairwise coprime polynomials in $\bar{R}$ lift to such factorizations over R.

Lemma 5.0.48. *[12](Hensel's Lemma) Let f be a polynomial over R and assume $\bar{f} = g_1 g_2 \cdots g_r$ where $g_1, g_2, ..., g_r$ are pairwise coprime polynomials over $\bar{R}$. Then there exist pairwise coprime polynomials $f_1, f_2, ..., f_r$ over R such that $f = f_1 f_2 \cdots f_r$ and $\bar{f}_i = g_i$ for $i = 1, 2, \cdots, r$.*

We do not have unique factorization in $R[X]$ in general; for example in $\mathbb{Z}_4[x]$ we have two different factorizations for $x^4 - 1$.

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

However we will see that certain non-unit polynomials do factor uniquely into irreducibles. Recall that a polynomial f is called **square-free** if $g^2 \mid f$ implies g is a unit.

Lemma 5.0.49. *[11] If f is a monic polynomial over a finite chain ring R such that $\bar{f}$ is square free, then f factors uniquely as a product of monic basic irreducible pairwise coprime polynomials.*

5.1. Structure Of Cyclic Codes Over Finite Chain Rings

Lemma 5.0.45 tells us that to study cyclic codes over R we need to understand the ring $R[X]/(x^n - 1)$. We assume the length of the code is not divisible by the characteristic of $\bar{R}$, so that $x^n - 1$ is square free in $\bar{R}[x]$ and has a unique decomposition into distinct monic basic irreducible factors in $R[x]$. The following lemma helps us study the cyclic codes over the chain ring R under these conditions:

Lemma 5.1.1. *[11] Let R be a finite chain ring with maximal ideal $m = \langle \gamma \rangle$, where γ is the generator of m with nilpotency index e. 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 $\langle 0 \rangle, \langle 1 \rangle, \langle 1 + \langle f \rangle \rangle, \langle \gamma + \langle f \rangle \rangle, \cdots, \langle \gamma^{e-1} + \langle f \rangle \rangle$.*

Example 5.1.2. *If f is a regular basic irreducible polynomial of the ring $\mathbb{Z}_4[x]$, then the only ideals of $\mathbb{Z}_4[x]/\langle f(x)\rangle$ are $\langle 0\rangle$, $\langle 1+\langle f(x)\rangle\rangle$ and $\langle 2+\langle f(x)\rangle\rangle$.*

Theorem 5.1.3. *[11] Assume R is a finite chain ring with maximal ideal $\langle\gamma\rangle$, and that e is the nilpotency index of γ. Let $x^n-1=f_1f_2\cdots f_r$ be a representation of x^n-1 as a product of basic irreducible polynomials in $R[x]$ for n not divisible by the characteristic of $\bar{R}$. Then any ideal in $\frac{R[x]}{\langle x^n-1\rangle}$ is a sum of ideals of the form $\left\langle \gamma^j\hat{f}_i+\langle x^n-1\rangle\right\rangle$, where $0\le j\le e$, $1\le i\le r$ and $\hat{f}_i=\frac{x^n-1}{f_i}$.*

Example 5.1.4. *Let n be odd. Let $x^n-1=f_1f_2\cdots f_r$ be the factorization of x^n-1 in $(\mathbb{F}_2+u\mathbb{F}_2)[x]$ where f_i 's are basic irreducible polynomials. Then any ideal in the ring $(\mathbb{F}_2+u\mathbb{F}_2)[x]/x^n-1$ is a sum of $\left\langle\hat{f}_i\right\rangle$'s and $\left\langle u\hat{f}_i\right\rangle$'s.*

Corollary 5.1.5. *[11] Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, and e be the nilpotency index of γ. The number of cyclic codes over R of length n, for n not divisible by the characteristic of $\bar{R}$, is $(e+1)^r$, where r is the number of factors in the unique factorization of x^n-1 into a product of monic basic irreducible pairwise coprime polynomials.*

The following theorem characterizes cyclic codes by giving generator polynomial description.

Theorem 5.1.6. *[11] Let C be a cyclic code of length n over a finite chain ring R (R has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ, n not divisible by the characteristic of $\bar{R}$). Then there exists a unique family of pairwise coprime monic polynomials $F_0,F_1,\cdots F_e$ in $R[x]$ such that $F_0F_1\cdots F_e=x^n-1$ and $C=\left\langle\hat{F}_1,\gamma\hat{F}_2,\cdots,\gamma^{e-1}\hat{F}_e\right\rangle$, where $\hat{F}(x)=\frac{x^n-1}{F(x)}$ Moreover*

$$|C|=\left(\left|\bar{R}\right|\right)^{\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}}.$$

Example 5.1.7. *Let us consider $\mathbb{Z}_4$-cyclic codes of length 7. Over $\mathbb{F}_2$*

$$x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

By Hensel lifting we find over $\mathbb{Z}_4$

$$x^7 - 1 = (x-1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3) = f_0 f_1 f_2.$$

Number of $\mathbb{Z}_4$ cyclic codes of length 7 is $3^3 = 27$. By the decomposition above, any ideal I of $\mathbb{Z}_4[x]/\langle x^7 - 1\rangle$ is a sum of some $\left\langle \hat{f}_i \right\rangle$ and $\left\langle 2\hat{f}_i \right\rangle$. As a result we get the following $\mathbb{Z}_4$ cyclic codes of length 7 :

$$\langle 0,0,0\rangle, \langle f_1 f_2, f_0 f_2, f_0 f_1\rangle, \langle f_1 f_2, 2f_0 f_2, f_0 f_1\rangle, \langle 0, f_1 f_2, f_0 f_1\rangle,$$
$$\langle f_1 f_2, f_0 f_2, 2f_0 f_1\rangle, \langle 0, f_1 f_2, f_0 f_2\rangle, \langle f_1 f_2, 2f_0 f_2, 2f_0 f_1\rangle, \langle 2f_1 f_2, f_0 f_2, f_0 f_1\rangle$$
$$\langle 2f_1 f_2, 2f_0 f_2, f_0 f_1\rangle, \langle 2f_1 f_2, f_0 f_2, 2f_0 f_1\rangle, \langle f_1 f_2, f_0 f_2, f_0 f_1\rangle \cdots$$

Example 5.1.8. *Cyclic codes of length 15 over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2$. We know that $\mathbb{F}_2$ is a subring of R and that $x^n - 1$ factors uniquely as a product of pairwise-coprime irreducible polynomials over the binary field. If any polynomial factors over a subring, it also factors over the ring. Thus, the factorization is given by $x^{15} + 1 = f_0 f_1 f_2 f_3 f_4$, where*

$$\begin{aligned} f_0 &= x+1,\ f_1 = x^2 + x + 1,\ f_2 = x^4 + x + 1, \\ f_3 &= x^4 + x^3 + 1,\ f_4 = x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Then any ideal in the ring is a sum of $\left\langle \hat{f}_i \right\rangle$ and $\left\langle u\hat{f}_i \right\rangle$. There are 3^5 different cyclic codes of length 15: $\langle f_0 f_3, u f_0 f_1 f_2 f_3\rangle$, $\langle f_0 f_3, u f_0 f_1 f_3 f_4\rangle$, $\langle f_3 f_4, u f_0 f_1 f_2 f_3\rangle$, $\langle 0, u f_0 f_2 f_4\rangle \cdots$

Theorem 5.1.9. *[11] Let C be a cyclic code of length n over a finite chain ring R, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ, and n not divisible by the characteristic of $\bar{R}$. Then there exist polynomials $g_1, g_2, \cdots, g_{e-1}$ in $R[x]$ such that $C = \langle g_1, \gamma g_2, \cdots, \gamma^{e-1} g_{e-1}\rangle$ and $g_{e-1}|g_{e-2}|\cdots|g_1|g_0|(x^n-1)$.*

Theorem 5.1.10. *[11] Let C be a cyclic code of length n over a finite chain ring R, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ, n not divisible by the characteristic of $\bar{R}$ and with notations in a previous theorem, and $F = \hat{F}_1 + \gamma\hat{F}_2 + \cdots + \gamma^{e-1}\hat{F}_e$. Then F is the generating polynomial of C, i.e., $C = \langle F\rangle$.*

Corollary 5.1.11. *[11] Let R be a finite chain ring. If n is a positive integer not divisible by the characteristic of $\bar{R}$, then $\frac{R[x]}{\langle x^n-1\rangle}$ is a principal ideal ring.*

5.2. Structure of Negacyclic Codes Over Finite Chain Rings

In 1968, Berlekamp started the study of negacyclic codes over finite fields [40]. Wolfmann gave various results about negacyclic codes of odd length over $\mathbb{Z}_4$ [7]. Permouth and Dinh studied negacyclic codes of odd length in a more general setting, namely, over finite chain rings and negacyclic codes of length 2^t over $\mathbb{Z}_{2^m}$ [11].

We discuss the structure of negacyclic codes of odd length n over a finite chain ring R, with the same hypotheses as in cyclic codes, i.e., R is a finite chain ring with maximal ideal $m = \langle\gamma\rangle$, where γ is the generator of m with nilpotency index e., $\bar{R} = R/m$, $|\bar{R}| = p^l$, $|R| = p^{lt}$, the characteristic of R and $\bar{R}$ are powers of p; n is not divisible by the characteristic of the residue field $\bar{R}$, that means x^n+1 is square-free in $\bar{R}[x]$, therefore x^n+1 has a unique decomposition into basic irreducible pairwise coprime polynomials in $R[x]$.

Lemma 5.2.1. *[11] Let ξ be a map $\xi : \frac{R[x]}{\langle x^n-1\rangle} \to \frac{R[x]}{\langle x^n+1\rangle}$ given by $\xi(f(x)) = f(-x), \forall f \in \frac{R[x]}{\langle x^n-1\rangle}$. If n is odd then ξ is a ring isomorphism.*

Lemma 5.2.2. *[11] Let n be odd. Let*

$A \subseteq \frac{R[x]}{\langle x^n-1\rangle}$, $B \subseteq \frac{R[x]}{\langle x^n+1\rangle}$ be such that $\xi(A) = B$. Then A is an ideal of $\frac{R[x]}{\langle x^n-1\rangle}$ if and only if B is an ideal of $\frac{R[x]}{\langle x^n+1\rangle}$. Equivalently, A is a cyclic code of length n over R if and only if B is a negacyclic code of length n over R.

The condition that the length n is odd is critical here, as the one to one correspondence between cyclic and negacyclic codes of the same length does not hold when the length is even. In fact, Blackford has showed that over $\mathbb{Z}_4$, there are 1183 cyclic codes of length 14, but only 125 negacyclic codes of length 14 [28].

Using the isomorphism ξ in previous lemma, the results about cyclic codes of length n over R, are valid for negacyclic codes of length n over R.

Theorem 5.2.3. *[11] Assume R is a finite chain ring with maximal ideal $\langle\gamma\rangle$, and that e is the nilpotency index of γ. Let n be a positive odd integer not divisible by the characteristic of the residue field $\bar{R}$ Let $x^n + 1 = f_1 f_2 \cdots f_r$ be a representation of $x^n - 1$ as a product of basic irreducible polynomials in $R[x]$. Then any ideal in $\frac{R[x]}{\langle x^n+1\rangle}$ is a sum of ideals of the form $\left\langle \gamma^j \hat{f}_i + \langle x^n + 1\rangle \right\rangle$, where $0 \leq j \leq e$, $1 \leq i \leq r$ and $\hat{f}_i = \frac{x^n+1}{f_i}$.*

Corollary 5.2.4. *[11] Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, and e be the nilpotency index of γ. Let n be a positive odd integer not divisible by the characteristic of the residue field $\bar{R}$. The number of negacyclic codes over R of length n is $(e+1)^r$, where r is the number of factors in the unique factorization of $x^n + 1$ into a product of monic basic irreducible pairwise coprime polynomials.*

Theorem 5.2.5. *[11] Let C be a negacyclic code of length n over a finite chain ring R (R has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ). Let n be a positive odd integer not divisible by the characteristic of the residue field $\bar{R}$. Then there exists a unique family of pairwise coprime monic polynomials $F_0, F_1, \cdots F_e$ in $R[x]$ such that $F_0F_1\cdots F_e = x^n+1$ and $C = \left\langle \hat{F}_1, \gamma\hat{F}_2, \cdots, \gamma^{e-1}\hat{F}_e \right\rangle$, where $\hat{F}(x) = \frac{x^n+1}{F(x)}$. Moreover*

$$|C| = \left(\left|\bar{R}\right|\right)^{\sum_{i=0}^{e-1}(e-i)\deg F_{i+1}}.$$

Theorem 5.2.6. *[11] Let C be a negacyclic code of length n over a finite chain ring R, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ. Let n be a positive odd integer not divisible by the characteristic of the residue field $\bar{R}$. Then there exist polynomials $g_1, g_2, \cdots, g_{e-1}$ in $R[x]$ such that $C = \langle g_1, \gamma g_2, \cdots, \gamma^{e-1}g_{e-1}\rangle$ and $g_{e-1}|g_{e-2}|\cdots|g_1|g_0|(x^n+1)$.*

Theorem 5.2.7. *[11] Let C be a negacyclic code of length n over a finite chain ring R, which has maximal ideal $\langle\gamma\rangle$ and e is the nilpotency of γ, and with notations in a previous theorem, and $F = \hat{F}_1 + \gamma\hat{F}_2 + \cdots + \gamma^{e-1}\hat{F}_e$. Let n be a positive odd integer not divisible by the characteristic of the residue field $\bar{R}$. Then F is the generating polynomial of C, i.e., $C = \langle F\rangle$.*

Corollary 5.2.8. *[11] Let R be a finite chain ring. If n is a positive odd integer not divisible by the characteristic of the residue field $\bar{R}$, then $\frac{R[x]}{\langle x^n+1\rangle}$ is a principal ideal ring.*

5.3. Structure of Constacyclic Codes Over Finite Chain Rings

Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been studied by Siap and Abualrub [1]. Recently, Qian et.al, also studied constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ [36]. In 2010, Dinh published a paper on constacyclic codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ of length p^s [41].

In [7], Wolfmann proved that the Gray image of a linear negacyclic code over $\mathbb{Z}_4$ of length n is a binary distance invariant(not necessarily linear) cyclic code and in the case when n is odd, the Gray image of a linear cyclic code over $\mathbb{Z}_4$ is equivalent to a binary cyclic code (not necessarily linear). Qian et.al, used the analogy of this work to study $(1+u)$-constacyclic codes over the ring $\mathbb{F}_2+u\mathbb{F}_2$ of odd lengths in [6].

In this subsection, we study constacyclic codes over finite chain rings.

$\bar{R} = R/m$, $|\bar{R}| = p^l$, $|R| = p^{lt}$, the characteristic of R and $\bar{R}$ are powers of p; n is not divisible by the characteristic of the residue field $\bar{R}$, that means $x^n - a$ square-free in $\bar{R}[x]$, therefore $x^n - a$ has a unique decomposition into basic irreducible pairwise coprime polynomials in $R[x]$. (a is a unit in R)

Remember that, to study constacyclic codes over the ring R, we are interested in the ring $\frac{R[x]}{\langle x^n-a\rangle}$. Then we first find a factorization of (x^n-a) into basic irreducible polynomials in R:

$$x^n - a = f_1 f_2 \cdots f_r.$$

Assume n is not divisible by the characteristic of the residue field $\bar{R}$, that means f_i's are all pairwise coprime. Now, the ideal structure of $\frac{R[x]}{\langle x^n-a\rangle}$ can be described by the following theorem analogous to what was done for cyclic and negacyclic codes:

Theorem 5.3.1. *Let R be a finite chain ring with maximal ideal $m = \langle\gamma\rangle$, where γ is the generator of m with nilpotency index e. Let $x^n - a = f_1 f_2 \cdots f_r$ be the representation as a product of basic irreducible pairwise-coprime polynomials in $R[x]$, for n not divisible by the characteristic of the residue field $\bar{R}$. Then any ideal in $\frac{R[x]}{\langle x^n-a\rangle}$ is a sum of ideals of the form $\left\langle \gamma^j \hat{f}_i + \langle x^n - a\rangle \right\rangle$, where $0 \le j \le e$, $1 \le i \le r$ and $\hat{f}_i = \frac{x^n-a}{f_i}$.*

Example 5.3.2. *2-constacyclic codes over* $R = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ *of length* 4. *Over* $\mathbb{F}_3$ *we have*

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

Note that this factorization carries over R *as well. So we can take* $f_1 = x^2 + x + 2$ *and* $f_2 = x^2 - x + 2$. *We have* $\hat{f}_1 = f_2$ *and* $\hat{f}_2 = f_1$ *Thus any ideal in* $\frac{R[x]}{\langle x^n - 2\rangle}$ *is a sum of ideals of the form* $\langle u^t f_i\rangle$. *As a result we get the following 2-constacyclic codes over* $R = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ *of length* 4*:*

$$\langle f_1, f_2\rangle, \langle uf_1, f_2\rangle, \left\langle u^2 f_1, f_2\right\rangle, \langle f_1, uf_2\rangle, \left\langle f_1, u^2 f_2\right\rangle, \langle uf_1, uf_2\rangle, ...$$

In general finding a factorization of $x^n - a$ into basic irreducible polynomials is extremely difficult. There are special cases in which this is relatively easier. Let us mention a special case:

Example 5.3.3. $(1 + u)-$*constacyclic codes over* $R = \mathbb{F}_2 + u\mathbb{F}_2$*:*

Qian considered $(1 + u)-$constacyclic codes over $R = \mathbb{F}_2 + u\mathbb{F}_2$. Note that $(1 + u)^n = 1 + u$ if n is odd and $(1 + u)^n = 1$ if n is even. So for odd n we have the following lemma:

Lemma 5.3.4. *Let* ξ *be a map* $\xi : \frac{R[x]}{\langle x^n - 1\rangle} \to \frac{R[x]}{\langle x^n - (1+u)\rangle}$ *given by* $\xi(f(x)) = f((1 + u)x), \forall f \in \frac{R[x]}{\langle x^n - 1\rangle}$. *If* n *is odd, then* ξ *is a ring isomorphism.*

As an immediate consequence, we observe that $(1 + u)-$constacyclic codes over R of odd lengths can easily been obtained from cyclic codes over R of the same length. Instead of factorizing $x^n - (1+u)$ into basic irreducibles, we would factorize $x^n - 1$ into irreducibles. Since the factorization of $x^n - 1$ over $\mathbb{F}_2$ is still valid over $\mathbb{F}_2 + u\mathbb{F}_2$, we would solve the problem of classifying constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$.

CHAPTER 6

CYCLIC AND CONSTACYCLIC CODES OVER $\mathcal{S}_4 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$

6.1. The Ring $\mathcal{S}_4$

Let $\mathcal{S}_4$ be the ring $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ with $u^4 = 0$, where $\mathbb{F}_2 = \{0, 1\} = \mathbb{Z}_2$. The ring $\mathcal{S}_4 = \mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ is a commutative finite chain ring of 16 elements, where $u^4 = 0$. The elements of $\mathcal{S}_4$ can be listed as

$$\begin{aligned}\mathcal{S}_4 \;=\; & \{0, 1, u, u^2, u^3, 1+u, 1+u^2, 1+u^3, u+u^2, u+u^3, u^2+u^3, 1+u+u^2,\\ & 1+u+u^3, 1+u^2+u^3, u+u^2+u^3, 1+u+u^2+u^3\}.\end{aligned}$$

Let $a_1 + ub_1 + u^2c_1 + u^3d_1$ and $a_2 + ub_2 + u^2c_2 + u^3d_2$ be elements in $\mathcal{S}_4$. Then addition is given by

$$\begin{aligned}&(a_1 + ub_1 + u^2c_1 + u^3d_1) + (a_2 + ub_2 + u^2c_2 + u^3d_2)\\ &= a_1 + a_2 + (b_1 + b_2)u + (c_1 + c_2)u^2 + (d_1 + d_2)u^3\end{aligned}$$

and multiplication by

$$\begin{aligned}&(a_1 + ub_1 + u^2c_1 + u^3d_1)(a_2 + ub_2 + u^2c_2 + u^3d_2)\\ &= a_1a_2 + (a_1b_2 + b_1a_2)u + (a_1c_2 + b_1b_2 + c_1a_2)u^2 + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2)u^3\end{aligned},$$

where a_i,b_i,c_i,$d_i \in \mathbb{F}_2$.

The group of units of $\mathcal{S}_4$, is given by

$$\begin{aligned}(\mathcal{S}_4)^* &= \left\{1, 1+u, 1+u^2, 1+u^3, 1+u+u^2, 1+u+u^3, 1+u^2+u^3, 1+u+u^2+u^3\right\}. \\ &= < 1+u, 1+u^2+u^3 >\end{aligned}$$

The non-units are

$$\left\{0, u, u^2, u^3, u+u^2, u+u^3, u^2+u^3, u+u^2+u^3\right\} =< u >$$

The ideals of $\mathcal{S}_4$ are (0), (1),(u),(u^2) and (u^3). We have

$$\mathcal{S}_4 \supset u\mathcal{S}_4 \supset u^2\mathcal{S}_4 \supset u^3\mathcal{S}_4 \supset u^4\mathcal{S}_4 = 0.$$

It is also a local ring with the unique maximal ideal $u\mathcal{S}_4$, moreover $\mathcal{S}_4/u\mathcal{S}_4 \cong \mathbb{F}_2$ is the residue field.

6.2. Linear Codes Over $\mathcal{S}_4$

Linear codes over the ring $\mathcal{S}_4$ are defined as :

Definition 6.2.1. *A linear code C of length n over the ring $\mathcal{S}_4$ is an $\mathcal{S}_4$-submodule of $\mathcal{S}_4^n$.*

A non-zero linear code C over $\mathcal{S}_4$, has a generator matrix which after a suitable permutation of the coordinates can be written in the form:

$$G = \begin{bmatrix} I_{k_1} & A_1 & A_2 & A_3 & A_4 \\ 0 & uI_{k_2} & uB_1 & uB_2 & uB_3 \\ 0 & 0 & u^2I_{k_3} & u^2C_1 & u^2C_2 \\ 0 & 0 & 0 & u^3I_{k_4} & u^3D \end{bmatrix}$$

where A_i, B_j, C_k and D are all matrices over $\mathcal{S}_4$. A linear code that has a such generating matrix is said to be of type $(16)^{k_1}(8)^{k_2}(4)^{k_3}(2)^{k_4}$ and consequently has size $2^{4k_1+3k_2+2k_3+k_4}$.

6.2.1. The Lee Weight and The Gray Map for Linear Codes over $\mathcal{S}_4$

In [9], the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ was taken as a natural extension of the ring $\mathbb{F}_2 + u\mathbb{F}_2$ and accordingly, the definition of the Lee weight was extended from $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. We will adopt a similar technique here.

For codes over $\mathcal{S}_4$, we will denote the Lee weight by w_L and the ordinary Hamming weight by w_H, and so we set

$$w_L\left(a + ub + u^2c + u^3d\right) = w_H\left(a + b + c + d, c + d, b + d, d\right) \forall a, b, c, d \in \mathbb{F}_2.$$

The definition of the weight immediately leads to a Gray map from $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ to $\mathbb{F}_2^4$ which can naturally be extended to $(\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n$:

$$\phi_L : ((\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n, \text{ Lee weight}) \longrightarrow (\mathbb{F}_2^{4n}, \text{ Hamming weight}).$$

$$\phi_L : ((\bar{a} + u\bar{b} + u^2\bar{c} + u^3\bar{d})) = (\bar{a} + \bar{b} + \bar{c} + \bar{d}, \bar{c} + \bar{d}, \bar{b} + \bar{d}, \bar{d}), \text{ where } \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{F}_2^n.$$

From the definition of the map ϕ_L we obtain the following theorem:

Theorem 6.2.2. *If C is a linear code over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ of length n, size 2^k and minimum Lee weight d, then $\phi_L(C)$ is a binary linear code with parameters $[4n, k, d]$.*

In the following table, we list the elements of $\mathcal{S}_4$ together with the corresponding Lee weights and Gray maps:

c	$w_L(c)$	$\phi_L(c)$
0	0	0000
1	1	1000
u	2	1010
u^2	2	1100
u^3	4	1111
$1+u$	1	0010
$1+u^2$	1	0100
$1+u^3$	3	0111
$u+u^2$	2	0110
$u+u^3$	2	0101
u^2+u^3	2	0011
$1+u+u^2$	3	1110
$1+u+u^3$	3	1101
$1+u^2+u^3$	3	1011
$u+u^2+u^3$	2	1001
$1+u+u^2+u^3$	1	0001

6.2.2. MacWilliams Identities For Codes Over $\mathcal{S}_4$

In this section, we consider some weight enumerators, in particular the complete weight enumerators of linear codes. We first give the necessary definitions and theorems, then we obtain MacWilliams-like identities for complete weight enumerators for codes over $\mathcal{S}_4$.

Definition 6.2.3. *Let C be a linear code of length n over a finite field $\mathbb{F}$, and A_i be the number of codewords of weight i in C, the homogenous polynomial*

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i \tag{6.1}$$

of degree n in indeterminates x and y is called the weight enumerator of C. Observe that

$$W_C(x,y) = \sum_{\bar{u}\in C} x^{n-w_H(\bar{u})} y^{w_H(\bar{u})}, \tag{6.2}$$

where $w_H(\bar{u})$ is the ordinary Hamming weight.

And by setting $x = 1$, one can have the weight enumerator in one indeterminate y,

$$A(y) = W_C(1,y) = W_C(y) = \sum_{i=0}^{n} A_i y^i. \tag{6.3}$$

The weight enumerator of the dual code $C^{\perp}$ is

$$\sum_{i=0}^{n} A'_i x^{n-i} y^i \tag{6.4}$$

Theorem 6.2.4 (MacWilliams theorems for binary linear codes,[26]). *If C is an $[n, k]$ code with dual $C^{\perp}$, then*

$$W_{C^{\perp}}(x, y) = \frac{1}{|C|} W_C(x + y, x - y) \tag{6.5}$$

where $|C|$ is the size of the code C. Equivalently,

$$\sum_{k=0}^{n} A'_i x^{n-k} y^k = \frac{1}{|C|} \sum_{i=0}^{n} A_i (x + y)^{n-i} (x - y)^i, \tag{6.6}$$

or

$$\sum_{\bar{u} \in C} x^{n - w_H(\bar{u})} y^{w_H(\bar{u})} = \frac{1}{|C|} \sum_{\bar{u} \in C} (x + y)^{n - w_H(\bar{u})} (x - y)^{w_H(\bar{u})}. \tag{6.7}$$

Equations (6.5)-(6.7) are sometimes called the MacWilliams identities.

The MacWilliams identities relate the Hamming weight enumerators of a linear code and its dual code. The following theorem from [26] and [25] illustrates the MacWilliams identities in a slightly different form:

Theorem 6.2.5. *[26], [25] Let C be an $[n, k]$ code over $\mathbb{F}_q$ with weight enumerator $A(z)$ and let $B(z)$ be the weight enumerator of $C^{\perp}$. Then*

$$B(z) = q^{-k} (1 + (q - 1)z)^n A\left(\frac{1 - z}{1 + (q - 1)z}\right). \tag{6.8}$$

In (6.8) by setting $q = 2$, we get the ordinary MacWilliam identity for binary linear codes, i.e.

$$B(z) = \frac{1}{|C|} (1 + z)^n A\left(\frac{1 - z}{1 + z}\right).$$

These identities have been generalized in various ways to other kinds of weight enumerators, such as the complete weight enumerator and also to linear codes over finite rings.

Definition 6.2.6. *For a code C over a ring $R = \{a_1, a_2, \cdots, a_q\}$ of length n, the complete weight enumerator is defined by*

$$cwe_C(x_1, x_2, \cdots, x_q) = \sum x_1^{n_{a_1}(\bar{c})} x_2^{n_{a_2}(\bar{c})} \cdots x_q^{n_{a_q}(\bar{c})},$$

where $n_{a_i}(\bar{c})$ is the number of appearences of a_i in the vector $\bar{c}$.

As stated earlier, J. Wood showed that MacWilliams identies apply for codes over Frobenius rings. Again, J. Wood observed that Theorem 6.2.5 remains true when $\mathbb{F}$ is exchanged by any finite Frobenius ring R([15]).

Throughout this thesis, our definition of a character will be as follows:

Definition 6.2.7. *Let G be a finite abelian group under addition. A character of G is a group homomorphism*

$$\chi : G \longrightarrow C^*$$

where C^* is the multiplicative group of nonzero complex numbers. And the set of all characters of G is called the character group of G and denoted by $\hat{G}$.

Remark 6.2.8. *For a finite abelian group G, G is isomorphic to $\hat{G}$.*

Let us recall that a generating character for a module is a character that is non-trivial when restricted to any non-trivial submodule.

Theorem 6.2.9. *[15] If R is a commutative Frobenius ring and T is the matrix of the character formed from the generating character χ, i.e. $T_{ij} = \chi(ij)$, then we can determine the complete weight enumerator of $C^{\perp}$ by*

$$cwe_{C^{\perp}} = \frac{1}{|C|} cwe(T \cdot (\mathbf{x_1}, \mathbf{x_2}, \cdots, \mathbf{x_q})).$$

For the rest of this section our aim is to modify definitions to our ring and obtain MacWilliams-like identities for linear codes over $\mathcal{S}_4$.

In order to define the dual of a code over $\mathcal{S}_4$, we first need to define an inner product on $\mathcal{S}_4$. The definition of the inner product is just like the natural Euclidean product, i.e. we define

$$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

where the operations are performed in the ring $\mathcal{S}_4$.

Note that we can actually define the same inner product in terms of the ordinary dot product in $\mathbb{F}_2$ as follows:

$$\begin{aligned} &< \overline{a}_1 + u\overline{b}_1 + u^2c_1 + u^3\overline{d}_1, \overline{a}_2 + u\overline{b}_2 + u^2\overline{c}_2 + u^3\overline{d}_2 > \\ &= \overline{a}_1 \cdot \overline{a}_2 + u(\overline{a}_1 \cdot \overline{b}_2 + \overline{a}_2 \cdot \overline{b}_1) + u^2(\overline{a}_1 \cdot \overline{c}_2 + \overline{b}_1 \cdot \overline{b}_2 + \overline{c}_1 \cdot \overline{a}_2) + \\ &u^3(\overline{a}_1 \cdot \overline{d}_2 + \overline{b}_1 \cdot \overline{c}_2 + \overline{c}_1 \cdot \overline{b}_2 + \overline{d}_1 \cdot \overline{a}_2) \end{aligned}$$

where $\overline{a} \cdot \overline{x}$ denotes the ordinary dot product in $\mathbb{F}_2$ of the binary vectors $\overline{a}$ and $\overline{x}$.

We are now ready to define the dual of a linear code C over $\mathcal{S}_4$:

Definition 6.2.10. *Let C be a linear code over $\mathcal{S}_4$ of length n, then we define the dual of C as*

$$C^{\perp} := \{\overline{y} \in (\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2)^n | < \overline{y}, \overline{x} >= 0, \forall \overline{x} \in C\}.$$

Note that from the definition of the inner product, it is obvious that $C^{\perp}$ is also a linear code over $\mathcal{S}_4$ of length n.

6.2.3. The Complete Weight Enumerator and MacWilliams Identities for Codes Over $\mathcal{S}_4$

In this section, we consider the complete weight enumarators of linear codes over $\mathcal{S}_4$ and we obtain MacWilliams-like identities for codes over $\mathcal{S}_4$.

Let $\mathcal{S}_4 = \{g_1, g_2, \ldots, g_{16}\}$ in some order. For example, we might assume $g_1 = 0, g_2 = 1, \ldots$ and so on.

The complete weight enumerator of a linear code C over $\mathcal{S}_4$ is given by

$$cwe_C(X_1, X_2, \ldots, X_{16}) = \sum_{\overline{c} \in C} (X_1^{n_{g_1}(\overline{c})} X_2^{n_{g_2}(\overline{c})} \ldots X_{16}^{n_{g_{16}}(\overline{c})})$$

where $n_{g_i}(\overline{c})$ is the number of appearances of g_i in the vector $\overline{c}$.

Remark 6.2.11. *Note that $cwe_C(X_1, X_2, \ldots, X_{16})$ is a homogeneous polynomial in 16 variables with the total degree of each term being n, the length of the code. Since $\overline{0} \in C$, we see that the term X_1^n always appears in $cwe_C(X_1, X_2, \ldots, X_{16})$.*

We also observe that

$$cwe_C(1, 1, \ldots, 1) = |C|.$$

$\mathcal{S}_4$ is a Frobenius ring and hence by definition it possesses a generating character, i.e, a character whose restriction to any non-trivial ideal is non-trivial.

Lemma 6.2.12. *Let $a+bu+cu^2+du^3 \in S_4$. Then $\bar{c}=(a,b,c,d)$ can be thought of as a binary vector of length 4. Let $w_H(\bar{c})$ be the Hammig weight of this vector. Then*

$$\chi(a+bu+cu^2+du^3) = (-1)^{w_H(\bar{c})}.$$

This is the generating character of the ring $\mathcal{S}_4$.

Proof. Let x,$y \in \mathcal{S}_4$. Then

$$\begin{aligned}
&\chi(\bar{x}+\bar{y}) = (-1)^{w_H(\bar{x}+\bar{y})} \\
&= (-1)^{w_H(\bar{x})+w_H(\bar{y})-2w_H(\bar{x}*\bar{y})} \\
&= (-1)^{w_H(\bar{x})+w_H(\bar{y})} \\
&= \chi(\bar{x})\chi(\bar{y}).
\end{aligned}$$

Therefore, χ is a character. And observe that

$$\begin{aligned}
&\chi(0) = 1, \\
&\chi(1) = \chi(u) = \chi(u^2) = \chi(u^3) = -1, \\
&\chi(1+u) = \chi(1+u^2) = \chi(1+u^3) = \chi(u+u^2) = \chi(u+u^3) = \chi(u^2+u^3) = 1, \\
&\chi(1+u+u^2) = \chi(1+u+u^3) = \chi(1+u^2+u^3) = \chi(u+u^2+u^3) = -1, \\
&\chi(1+u+u^2+u^3) = 1.
\end{aligned}$$

As seen from here χ restricted to any non-trivial ideal is non-trivial. □

Let T be a square 16 by 16 matrix indexed by the elements of $\mathcal{S}_4$ in the order

$$\begin{aligned}
&g_1 = 0,\ g_2 = 1,\ g_3 = u,\ g_4 = u^2,\ g_5 = u^3, \\
&g_6 = 1+u,\ g_7 = 1+u^2,\ g_8 = 1+u^3,\ g_9 = u+u^2,\ g_{10} = u+u^3,\ g_{11} = u^2+u^3, \\
&g_{12} = 1+u+u^2,\ g_{13} = 1+u+u^2,\ g_{14} = 1+u^2+u^3,\ g_{15} = u+u^2+u^3, \\
&g_{15} = 1+u+u^2+u^3.
\end{aligned}$$

Define

$$T_{g_i,g_j} = \chi(g_i g_j) = (-1)^{wt(g_i g_j)}.$$

Then we obtain the matrix T to be

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}	g_{16}
g_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
g_2	1	−1	−1	−1	1	1	1	1	1	1	1	−1	−1	−1	−1	1
g_3	1	−1	1	−1	1	−1	1	−1	−1	1	−1	1	−1	1	−1	1
g_4	1	−1	−1	1	1	1	−1	−1	−1	−1	1	1	1	−1	−1	1
g_5	1	−1	1	1	1	−1	−1	−1	1	1	1	−1	−1	−1	1	−1
g_6	1	1	−1	1	−1	−1	1	−1	−1	1	−1	−1	1	−1	1	1
g_7	1	1	1	−1	−1	1	−1	−1	−1	−1	1	−1	−1	1	1	1
g_8	1	1	−1	−1	−1	−1	−1	−1	1	1	1	1	1	1	−1	1
g_9	1	1	−1	−1	1	−1	−1	1	1	−1	−1	1	−1	−1	1	1
g_{10}	1	1	1	−1	1	1	−1	1	−1	1	−1	−1	1	−1	−1	−1
g_{11}	1	1	−1	1	1	−1	1	1	−1	−1	1	−1	−1	1	−1	−1
g_{12}	1	−1	1	1	−1	−1	−1	1	1	−1	−1	−1	1	1	−1	1
g_{13}	1	−1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	1	−1
g_{14}	1	−1	1	−1	−1	−1	1	1	−1	−1	1	1	1	−1	1	−1
g_{15}	1	−1	−1	−1	1	1	1	−1	1	−1	−1	−1	1	1	1	−1
g_{16}	1	1	1	1	−1	1	1	−1	1	−1	−1	1	−1	−1	−1	−1

By the results of Theorem 6.2.9, we have the following theorem:

Theorem 6.2.13. *Let C be a linear code over $\mathcal{S}_4$ then*

$$cwe_{C^\perp} = \frac{1}{|C|} cwe(T \cdot \mathbf{X}), \tag{6.9}$$

where T is the matrix in above table and $\mathbf{X} = (\mathbf{x}_1, x_2, \cdots, x_{16})^T$.

Noticing that

$$cwe_C(x, y, y, \cdots, y) = W_C(x, y), \tag{6.10}$$

and by (6.9), the usual Hamming weight enumerator, MacWilliams relations follow, that is:

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (|S_4| - 1)y, x - y). \tag{6.11}$$

Here $W_C(x, y)$ denotes the Hamming weight enumerator of C and $|\mathcal{S}_4|$ is 16.

6.3. Cyclic Codes Over $\mathcal{S}_4$

Cyclic codes over finite chain rings have been studied in different contexts by numerous authors. In all of these cases, the common ground is the finite chain structure of the rings over which the codes are defined. This allows defining the generating and check matrices for the codes in standard forms. In addition, when the length of the code and the characteristic of the ring are relatively prime, then $R[x]/(x^n - 1)$ turns out to be a principal ideal ring. What we have related in the previous chapters are naturally valid for $\mathcal{S}_4$ as well:

Lemma 6.3.1. *A subset C of $\mathcal{S}_4^n$ is a linear cyclic code of length n if and only if $P(C)$ is an ideal in the quotient ring $\mathcal{S}_4[X]/(x^n - 1)$.*

So cyclic codes over $\mathcal{S}_4$ are identified with ideals in the ring $\mathcal{S}_4[X]/(x^n - 1)$. That is why it is necessary to study the ideal structure of $\mathcal{S}_4[X]/(x^n - 1)$. The ideal structure of similar rings have been studied in the literature and we will make use of the same ideas.

We assume the length of the code is odd, so that $x^n - 1$ is square free in $\mathbb{F}_2[x]$ and has a unique decomposition into distinct monic basic irreducible factors in $\mathcal{S}_4[x]$.

Note that $x^n - 1$ is a regular polynomial in $\mathcal{S}_4[x]$. A factorization of $x^n - 1$ in $\mathbb{F}_2[x]$ can be lifted uniquely to the same factorization in $\mathcal{S}_4[x]$ since $\mathcal{S}_4$ is a local ring [12]. Hence we have the following lemma:

Lemma 6.3.2. *[12] Let $x^n - 1 = f_1 f_2 \cdots f_r$ be the factorization of $x^n - 1$ into irreducible monic polynomials f_i in $\mathbb{F}_2[x]$. Then $x^n - 1$ has the same factorization into irreducible polynomials in $\mathcal{S}_4[x]$.*

Theorem 6.3.3. *Assume that n is odd. Let $x^n - 1 = f_1 f_2 \cdots f_r$ be a representation of $x^n - 1$ as a product of basic irreducible polynomials in $\mathcal{S}_4[x]$. Then any ideal in $\frac{S_4[x]}{\langle x^n - 1\rangle}$ is a sum of ideals of the form $\left\langle u^j \hat{f}_i + \langle x^n - 1\rangle \right\rangle$, where $0 \le j \le 4$, $1 \le i \le r$ and $\hat{f}_i = \frac{x^n - 1}{f_i}$.*

As a consequence of the above theorem, the number of cyclic codes over $\mathcal{S}_4$ of length n is 5^r, where r is the number of basic irreducible polynomial factors in $x^n - 1$ over $\mathcal{S}_4$.

The following theorem characterizes cyclic codes over $\mathcal{S}_4$ by giving generator polynomial description.

Theorem 6.3.4. *Let C be a cyclic code of odd length n over $\mathcal{S}_4$, then there exists a unique family of pairwise coprime monic polynomials F_0, F_1, F_2, F_3, F_4 in $R[x]$ such that $F_0 F_1 F_2 F_3 F_4 = x^n - 1$ and $C = \left\langle \hat{F}_1, u\hat{F}_2, u^2\hat{F}_3, u^3\hat{F}_4 \right\rangle$, where $\hat{F}(x) = \frac{x^n - 1}{F(x)}$. Moreover,*

$$|C| = 2^{\sum_{i=0}^{3} (4-i) \deg F_{i+1}}.$$

Corollary 6.3.5. *Suppose n is odd, and C is a cyclic code over $\mathcal{S}_4$. Then there exist polynomials g_0, g_1, g_2, g_3 in $\mathcal{S}_4[x]$ such that $C = \langle g_0, ug_1, u^2 g_2, u^3 g_3\rangle$ and $g_3 | g_2 | g_1 | g_0 | (x^n - 1)$.*

Theorem 6.3.6. *Let C be a cyclic code over $\mathcal{S}_4$ of odd length n, with notations in a previous theorem, let $F = \hat{F}_1 + u\hat{F}_2 + u^2\hat{F}_3 + u^3\hat{F}_4$. Then F has generating polynomial of C, i.e., $C = \langle F \rangle$.*

Corollary 6.3.7. *If n is an positive odd integer, then $\mathcal{S}_4[x]/(x^n - 1)$ is a principal ideal ring.*

This corollary implies that all odd length cyclic codes are principally generated.

Example 6.3.8. *Cyclic codes of length 5 over $\mathcal{S}_4$.*

$$x^5 - 1 = (x+1)(x^4 + x^3 + x^2 + x + 1) = g_1 g_2$$

The nonzero cyclic codes of length 5 over $\mathcal{S}_4$ with generator polynomials are given in the following table:

Table 6.1 . Cyclic codes of length 5 over $\mathcal{S}_4$.

Nonzero generator polynomial
$\langle g_1 \rangle$,$\langle g_1, g_2 \rangle$, $\langle g_1, ug_2 \rangle$, $\langle g_1, u^2 g_2 \rangle$, $\langle g_1, u^3 g_2 \rangle$
$\langle ug_1 \rangle$,$\langle ug_1, g_2 \rangle$, $\langle ug_1, ug_2 \rangle$, $\langle ug_1, u^2 g_2 \rangle$, $\langle ug_1, u^3 g_2 \rangle$
$\langle u^2 g_1 \rangle$,$\langle u^2 g_1, g_2 \rangle$, $\langle u^2 g_1, ug_2 \rangle$, $\langle u^2 g_1, u^2 g_2 \rangle$, $\langle u^2 g_1, u^3 g_2 \rangle$
$\langle u^3 g_1 \rangle$,$\langle u^3 g_1, g_2 \rangle$, $\langle u^3 g_1, ug_2 \rangle$, $\langle u^3 g_1, u^2 g_2 \rangle$, $\langle u^3 g_1, u^3 g_2 \rangle$
$\langle g_2 \rangle$,$\langle ug_2 \rangle$, $\langle u^2 g_2 \rangle$, $\langle u^3 g_2 \rangle$
$\langle 0 \rangle$

6.3.1. One-generator Cyclic Codes Of Some Particular Lengths

In this subsection, we give some practical results for cyclic codes generated by one generator, $C = \langle g(x) \rangle$, with $g(x)$ is a polynomial in $\mathcal{S}_4[x]/(x^n - 1)$ and the parameters of the binary images under ϕ_L. The ones marked with * denote the optimal codes by [5].

The following lemma helps us obtain non-trivial cyclic codes over $\mathcal{S}_4$.

Lemma 6.3.9. *Let ψ be the map $\psi : \mathcal{S}_4 \to \mathbb{F}_2$ such that*

$$\psi(a + bu + cu^2 + du^3) = a.$$

Let $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in S_4[x]/(x^n - 1)$. Then $C = \langle g(x) \rangle$ is a non-trivial cyclic code if and only if

$$GCD(\ \psi(g(x)), x^n - 1) \neq 1.$$

Table 6.2 . Some cyclic codes of length 2 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x >$	$[8, 1, 8]^*$
$< u + ux >$	$[8, 3, 4]^*$
$< 1 + u^2 + u^3 + (1 + u^2)x >$	$[8, 4, 4]^*$
$< 1 + u^2 + u^3 + (1 + u + u^3)x >$	$[8, 6, 2]^*$

Table 6.3 . Some cyclic codes of length 3 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^3x^2 >$	$[12, 1, 12]^*$
$< u^3 + u^3x >$	$[12, 2, 8]^*$
$< u + ux + ux^2 >$	$[12, 3, 6]^*$
$< u^3 + u^2x + u^2x^2 >$	$[12, 5, 4]^*$
$< u + ux >$	$[12, 6, 4]^*$
$< u^3 + ux + ux^2 >$	$[12, 7, 4]^*$
$< 1 + u + u^2 + (1 + u^2)x + (u + u^2)x^2 >$	$[12, 9, 2]^*$
$< 1 + u + u^2 + u^3 + ux + (1 + u + u^2)x^2 >$	$[12, 11, 2]^*$

Table 6.4 . Some cyclic codes of length 4 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^3x^2 + u^3x^3 >$	$[16, 1, 16]$*
$< u^3 + u^3x >$	$[16, 3, 8]$*
$< 1 + u + u^2 + u^3 + (1 + u + u^3)x + (1 + u + u^2 + u^3)x^2 + (1 + u + u^3)x^3 >$	$[16, 4, 8]$*
$< 1 + u + u^2 + u^3 + (1 + u^3)x + (1 + u + u^3)x^2 + (1 + u^2)x^3 >$	$[16, 5, 8]$*
$< 1 + u + u^3 + (1 + u + u^3)x + (1 + u + u^2 + u^3)x^2 + (1 + u + u^2)x^3 >$	$[16, 6, 6]$*
$< u^2 + u^3 + u^2x + (u + u^3)x^2 >$	$[16, 8, 4]$*
$< 1 + u + (1 + u^2 + u^3)x + (1 + u^3)x^2 + (1 + u + u^2 + u^3)x^3 >$	$[16, 9, 4]$*
$< u + (1 + u + u^2)x^2 + (1 + u^3)x^3 >$	$[16, 12, 2]$*

Table 6.5 . Some cyclic codes of length 5 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^3x^2 + u^3x^3 + u^3x^4 >$	$[20, 1, 20]$*
$< u^2 + u^3 + u^3x + (u + u^2 + u^3)x^2 + (u + u^2)x^3 + (u^2 + u^3)x^2 >$	$[20, 12, 4]$*
$< u^3 + (u + u^3)x + (u + u^2 + u^3)x^2 + u^3x^3 + (u^2 + u^3)x^4 >$	$[20, 13, 4]$*
$< u^3 + (1 + u)x + (u + u^2 + u^3)x^2 + u^3x^3 + (1 + u^2)x^4 >$	$[20, 17, 2]$*
$< 1 + (u + u^3)x + (u^2 + u^3)x^2 + (1 + u + u^3)x^4 >$	$[20, 18, 2]$*
$< 1 + u + u^2x + (1 + u + u^3)x^3 + (u + u^2 + u^3)x^4 >$	$[20, 19, 2]$*

6.4. $(1 + u^2)$-Constacyclic Codes Over $\mathcal{S}_4$ Of Odd Length

In this subsection we study $(1 + u^2)$-constacyclic codes over $\mathcal{S}_4$ of odd lengths.

Lemma 6.4.1. *A subset C of $\mathcal{S}_4^n$ is a linear $(1 + u^2)$-constacyclic code of length n over $\mathcal{S}_4$ if and only if its polynomial representation is an ideal in the quotient ring $\mathcal{S}_4[x]/(x^n - (1 + u^2))$.*

In the previous section, cyclic codes over $\mathcal{S}_4$ of odd lengths were classified. We use this classification to study $(1+u^2)$-constacyclic codes over $\mathcal{S}_4$ by introducing the following isomorphism from $\mathcal{S}_4[x]/(x^n - 1)$ to $\mathcal{S}_4[x]/(x^n - (1 + u^2))$.(from [10])

Proposition 6.4.2. *Let* $\mu : \mathcal{S}_4[x]/(x^n-1) \to \mathcal{S}_4[x]/(x^n-(1+u^2))$ *be defined as* $\mu(c(x)) = c((1+u^2)x)$. *If* n *is odd, then* μ *is a ring isomorphism from* $\mathcal{S}_4[x]/(x^n-1)$ *to* $\mathcal{S}_4[x]/(x^n-(1+u^2))$.

Proof. Note that $(1+u^2)^2 = 1$. But, this implies that if n is odd, then $(1+u^2)^n = (1+u^2)$. Now, suppose $a(x) \equiv b(x) \pmod{x^n-1}$, i.e., $a(x)-b(x) = (x^n-1)q(x)$ for some $q(x) \in \mathcal{S}_4[x]$. Then $a((1+u^2)x)-b((1+u^2)x) = ((1+u^2)^n x^n-1)q((1+u^2)x) = ((1+u^2)x^n-(1+u^2)^2)q((1+u^2)x) = (1+u^2)(x^n-(1+u^2))q((1+u^2)x)$, which means if $a(x) = b(x) \pmod{x^n-1}$, then $a((1+u^2)x) = b((1+u^2)x) \pmod{x^n-(1+u^2)}$. But the converse can easily be shown as well which means $a(x) = b(x) \pmod{x^n-1} \Leftrightarrow a((1+u^2)x) = b((1+u^2)x) \pmod{x^n-(1+u^2)}$. Note that one side of the implication tells us that μ is well defined and the other side tells us that it is injective, but since the rings are finite this proves that μ is an isomorphism. □

The following is a natural corollary of the proposition:

Corollary 6.4.3. *I is an ideal of $\mathcal{S}_4[x]/(x^n-1)$ if and only $\mu(I)$ is an ideal of $\mathcal{S}_4[x]/(x^n-(1+u^2))$ when n is odd.*

Corollary 6.4.4. *Let $\overline{\mu}$ be the map that acts on $\mathcal{S}_4^n$ with odd length n as follows:*

$$\overline{\mu}(c_0, c_1, \cdots, c_{n-1}) = (c_0, (1+u^2)c_1, (1+u^2)^2 c_2, \cdots, (1+u^2)^{n-1} c_{n-1})$$

Then C is a linear cyclic code over $\mathcal{S}_4$ of odd length n if and only if $\overline{\mu}(C)$ is a linear $(1+u^2)$-constacylic code of length n over $\mathcal{S}_4$.

Corollary 6.4.5. *C is a cyclic code over $\mathcal{S}_4$ of parameters $[n, 2^k, d]$ if and only if $\overline{\mu}(C)$ is a $(1+u^2)$-constacyclic code over $\mathcal{S}_4$ of parameters $[n, 2^k, d]$, where n is odd.*

Now we refer to previous section in which we obtained tables for cyclic codes over $\mathcal{S}_4$ generated by one generator and by modifying the generators by μ, we get the following tables for constacyclic codes over $\mathcal{S}_4$. The ones marked by * denote the optimal ones by [5].

Table 6.6 . Some cyclic codes of length 6 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^2x^2 + u^2x^3 + u^2x^4 >$	$[24, 8, 6]$
$< 1 + u^3 + (1 + u + u^2)x + u^2x^2 + (1 + u + u^2)x^3 + (1 + u^2 + u^3)x^4 + ux^5 >$	$[24, 14, 4]$
$< u^3 + (1 + u^2 + u^3)x + x^2 + (u^2 + u^3)x^3 + (1 + u + u^2)x^4 + (1 + u + u^2)x^5 >$	$[24, 15, 4]$*
$< 1 + u + u^3 + (1 + u^2 + u^3)x + (1 + u + u^2 + u^3)x^2 + (1 + u^2 + u^3)x^3 + x^4 + (1 + u^2 + u^3)x^5 >$	$[24, 16, 4]$*
$< 1 + u + u^3 + (1 + u + u^3)x + ux^2 + (u + u^2)x^4 + (1 + u^2)x^5 >$	$[24, 20, 2]$*

Table 6.7 . Some cyclic codes of length 7 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u + u^2 + (u + u^3)x + u^2x^2 + (u^2 + u^3)x^3 + (u + u^2)x^4 + u^3x^5 + u^2x^6 >$	$[28, 12, 8]$*
$< 1 + u + u^3 + u^2x + (1 + u + u^2)x^3 + (1 + u)x^4 + (1 + u + u^3)x^5 + (u^2 + u^3)x^6 >$	$[28, 15, 4]$
$< 1 + u^3 + (1 + u + u^3)x + (1 + u + u^2)x^2 + (1 + u^2 + u^3)x^3 + (1 + u^2 + u^3)x^4 + x^5 + (1 + u + u^2 + u^3)x^6 >$	$[28, 16, 4]$
$< 1 + u + ux + (1 + u^3)x^2 + (u + u^2 + u^3)x^3 + (1 + u^3)x^5 + (1 + u + u^2 + u^3)x^6 >$	$[28, 18, 4]$
$< 1 + u^2 + (1 + u + u^3)x + u^3x^2 + (u^2 + u^3)x^3 + (1 + u)x^4 + ux^5 + (1 + u + u^3)x^6 >$	$[28, 21, 4]$*
$< u^2 + u^3 + (1 + u + u^2)x + (1 + u + u^3)x^2 + (1 + u)x^3 + (u + u^2 + u^3)x^5 + (1 + u^2)x^6 >$	$[28, 22, 2]$*
$< u^2 + (u + u^2)x + (1 + u + u^2 + u^3)x^2 + x^3 + (1 + u + u^2 + u^3)x^4 + (1 + u + u^3)x^5 + u^3x^6 >$	$[28, 24, 2]$*
$< 1 + u^3 + (1 + u^2 + u^3)x + u^2x^2 + (u + u^2)x^3 + (u + u^2)x^4 + (1 + u^2 + u^3)x^5 + (u^2 + u^3)x^6 >$	$[28, 25, 2]$*
$< (1 + u^3)x + u^3x^2 + (u + u^3)x^4 + (1 + u^2)x^5 + (u + u^3)x^6 >$	$[28, 26, 2]$*
$< u^2 + u^3x + (u^2 + u^3)x^2 + x^3 + u^3x^4 + (u^2 + u^3)x^5 + (1 + u)x^6 >$	$[28, 27, 2]$*

Table 6.8 . Some cyclic codes of length 8 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< 1 + u^3 + (1 + u^2 + u^3)x + u^3x^3 + (1 + u^2)x^4 + x^5 >$	$[32, 14, 8]$*
$< u + ux + (1 + u^2 + u^3)x^2 + (u + u^2)x^3 + u^2x^4 + (u^2 + u^3)x^5 + (1 + u + u^2)x^6 + u^2x^7 >$	$[32, 16, 8]$*
$< 1 + u + (1 + u + u^3)x + (1 + u^2)x^2 + (u + u^2)x^3 + (u + u^3)x^4 + (u + u^2)x^6 + (1 + u + u^3)x^7 >$	$[32, 24, 4]$*
$< 1 + u + u^2 + (u + u^3)x + u^2x^2 + (1 + u)x^4 + (u + u^3)x^5 + (1 + u^2 + u^3)x^6 + (1 + u^2)x^7 >$	$[32, 28, 2]$*

Table 6.9 . Some constacyclic codes of length 2 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x >$	$[8, 1, 8]^*$
$< u + (u + u^3)x >$	$[8, 3, 4]^*$
$< 1 + u^2 + u^3 + x >$	$[8, 4, 4]^*$
$< 1 + u^2 + u^3 + (1 + u + u^2)x >$	$[8, 6, 2]^*$

Table 6.10 . Some constacyclic codes of length 3 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^3x^2 >$	$[12, 1, 12]^*$
$< u^3 + u^3x >$	$[12, 2, 8]^*$
$< u + (u + u^3)x + ux^2 >$	$[12, 3, 6]^*$
$< u^3 + u^2x + u^2x^2 >$	$[12, 5, 4]^*$
$< u + (u + u^3)x >$	$[12, 6, 4]^*$
$< u^3 + (u + u^3)x + ux^2 >$	$[12, 7, 4]^*$
$< 1 + u + u^2 + x + (u + u^2)x^2 >$	$[12, 9, 2]^*$
$< 1 + u + u^2 + u^3 + (u + u^3)x + (1 + u + u^2)x^2 >$	$[12, 11, 2]^*$

Table 6.11 . Some constacyclic codes of length 4 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^3x^2 + u^3x^3 >$	$[16, 1, 8]^*$
$< u^3 + u^3x >$	$[16, 3, 8]^*$
$< 1 + u + u^2 + u^3 + (1 + u + u^2)x + (1 + u + u^2 + u^3)x^2 + (1 + u + u^2)x^3 >$	$[16, 4, 8]^*$
$< 1 + u + u^2 + u^3 + (1 + u^2 + u^3)x + (1 + u + u^3)x^2 + x^3 >$	$[16, 5, 8]^*$
$< 1 + u + u^3 + (1 + u + u^2)x + (1 + u + u^2 + u^3)x^2 + (1 + u + u^3)x^3 >$	$[16, 6, 6]^*$
$< u^2 + u^3 + u^2x + ux^2 >$	$[16, 8, 4]^*$
$< 1 + u + (1 + u^3)x + (1 + u^3)x^2 + (1 + u)x^3 >$	$[16, 9, 4]^*$
$< u + (1 + u + u^2)x^2 + (1 + u^2 + u^3)x^3 >$	$[16, 12, 2]^*$

Table 6.12 . Some constacyclic codes of length 5 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^3x^2 + u^3x^3 + u^3x^4 >$	$[20, 1, 20]$*
$< u^2 + u^3 + u^3x + (u + u^2 + u^3)x^2 + (u + u^2 + u^3)x^3 + (u^2 + u^3)x^2 >$	$[20, 12, 4]$*
$< u^3 + ux + (u + u^2 + u^3)x^2 + u^3x^3 + (u^2 + u^3)x^4 >$	$[20, 13, 4]$*
$< u^3 + (1 + u + u^2 + u^3)x + (u + u^2 + u^3)x^2 + u^3x^3 + (1 + u^2)x^4 >$	$[20, 17, 2]$*
$< 1 + ux + (u^2 + u^3)x^2 + (1 + u + u^3)x^4 >$	$[20, 18, 2]$*
$< 1 + u + u^2x + (1 + u + u^2)x^3 + (u + u^2 + u^3)x^4 >$	$[20, 19, 2]$*

Table 6.13 . Some constacyclic codes of length 6 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u^3 + u^3x + u^2x^2 + u^2x^3 + u^2x^4 >$	$[24, 8, 6]$
$< 1 + u^3 + (1 + u + u^3)x + u^2x^2 + (1 + u + u^3)x^3 + (1 + u^2 + u^3)x^4$ $+(\mathrm{u}+\mathrm{u}^3)x^5 >$	$[24, 14, 4]$
$< u^3 + (1 + u^3)x + x^2 + (u^2 + u^3)x^3 + (1 + u + u^2)x^4 + (1 + u + u^3)x^5 >$	$[24, 15, 4]$*
$< 1 + u + u^3 + (1 + u^3)x + (1 + u + u^2 + u^3)x^2 + (1 + u^3)x^3 + x^4$ $+(1+\mathrm{u}^3)x^5 >$	$[24, 16, 4]$*
$< 1 + u + u^3 + (1 + u + u^2)x + ux^2 + (u + u^2)x^4 + (1 + u^2)x^5 >$	$[24, 20, 2]$*

Table 6.14 . Some constacyclic codes of length 7 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< u + u^2 + ux + u^2x^2 + (u^2 + u^3)x^3 + (u + u^2)x^4 + u^3x^5 + u^2x^6 >$	$[28, 12, 8]$*
$< 1 + u + u^3 + u^2x + (1 + u + u^3)x^3 + (1 + u)x^4 + (1 + u + u^2)x^5 + (u^2 + u^3)x^6 >$	$[28, 15, 4]$
$< 1 + u^3 + (1 + u + u^2)x + (1 + u + u^2)x^2 + (1 + u^3)x^3 + (1 + u^2 + u^3)x^4 + (1 + u^2)x^5 + (1 + u + u^2 + u^3)x^6 >$	$[28, 16, 4]$
$< 1 + u + (u + u^3)x + (1 + u^3)x^2 + (u + u^3)x^3 + (1 + u^2 + u^3)x^5 + (1 + u + u^2 + u^3)x^6 >$	$[28, 18, 4]$
$< 1 + u^2 + (1 + u + u^2)x + u^3x^2 + (u^2 + u^3)x^3 + (1 + u)x^4 + (u + u^3)x^5 + (1 + u + u^3)x^6 >$	$[28, 21, 4]$*
$< u^2 + u^3 + (1 + u + u^3)x + (1 + u + u^3)x^2 + (1 + u + u^2 + u^3)x^3 + (u + u^2 + u^3)x^5 + (1 + u^2)x^6 >$	$[28, 22, 2]$*
$< u^2 + (u + u^2 + u^3)x + (1 + u + u^2 + u^3)x^2 + (1 + u^2)x^3 + (1 + u + u^2 + u^3)x^4 + (1 + u + u^2)x^5 + u^3x^6 >$	$[28, 24, 2]$*
$< 1 + u^3 + (1 + u^3)x + u^2x^2 + (u + u^2 + u^3)x^3 + (u + u^2)x^4 + (1 + u^3)x^5 + (u^2 + u^3)x^6 >$	$[28, 25, 2]$*
$< (1 + u^2 + u^3)x + u^3x^2 + (u + u^3)x^4 + x^5 + (u + u^3)x^6 >$	$[28, 26, 2]$*
$< u^2 + u^3x + (u^2 + u^3)x^2 + (1 + u^2)x^3 + u^3x^4 + (u^2 + u^3)x^5 + (1 + u)x^6 >$	$[28, 27, 2]$*

Table 6.15 . Some constacyclic codes of length 8 and the binary images.

$g(x)$	$\phi_{\mathrm{L}}(< g(x) >)$
$< 1 + u^3 + (1 + u^3)x + u^3x^3 + (1 + u^2)x^4 + (1 + u^2)x^5 >$	$[32, 14, 8]$*
$< u + (u + u^3)x + (1 + u^2 + u^3)x^2 + (u + u^2 + u^3)x^3 + u^2x^4 + (u^2 + u^3)x^5 + (1 + u + u^2)x^6 + u^2x^7 >$	$[32, 16, 8]$*
$< 1 + u + (1 + u + u^2)x + (1 + u^2)x^2 + (u + u^2 + u^3)x^3 + (u + u^3)x^4 + (u + u^2)x^6 + (1 + u + u^2)x^7 >$	$[32, 24, 4]$*
$< 1 + u + u^2 + (u + u^3)x + u^2x^2 + (1 + u)x^4 + ux^5 + (1 + u^2 + u^3)x^6 + x^7 >$	$[32, 28, 2]$*

REFERENCES

[1] Abualrub, T. and Siap, I., *Constacylic Codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, J. Frank. Inst., **346**, (2009), pp. 520–529.

[2] Abualrub, T. and Siap, I., *Cyclic Codes over the rings* $\mathbb{Z}_2+u\mathbb{Z}_2$ *and* $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$, Des. Codes Crypt. **42**, (2007), pp. 273–287

[3] Bonnecaze, A. and Udaya, P., *Cyclic Codes and Self-Dual Codes Over* $\mathbb{F}_2+u\mathbb{F}_2$, IEEE Trans. Inform. Theory, vol. 45. pp. 1250-1255, 1999.

[4] Dougherty, S.T., Gaborit, P., Harada, M. and Solé, P., *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Infrom. Theory, **45** (1999), 32–45.

[5] Grassl, M., *Bounds on the minimum distance of linear codes and quantum codes*, Online available at **www.codetables.de.** Accessed on 2010/08/01.

[6] Qian, J.F., Zhang, L.N., Zhu, S.X., *(1+u) constacyclic and cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, Applied Mathematics Letters, **19**, (206), pp. 820–823.

[7] Wolfmann, J., *Negacyclic and Cyclic Codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, **45**, (1999), pp. 2527–2532

[8] Yildiz, B., Karadeniz, S., *Linear Codes over* $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Des. Codes Crypt., **54**, (2010), pp. 61–81.

[9] Yildiz, B., Karadeniz, S., *Cyclic Codes over* $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Des. Codes Crypt., vol.58, no.3, pp. 221–234 2011.

[10] Yildiz, B., Karadeniz, S., *(1+v)-Constacyclic Codes over* $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, J. Frank. Inst., **347**, (2010), pp. 1888–1894.

[11] Quang Dinh, H. and Lopez-Permóuth, S., *Cyclic and negacyclic codes over finite chain rings.* IEEE Trans. Infrom. Theory, **50**, 1728–1744 (2004).

[12] McDonald, Bernard R., *Finite Rings with Identity,* Dekker, New York, 1974.

[13] Gerefroth, M., McGuire, G. and O'Sullivan, M.E., *On Plotkin-Optimal Codes over Finite Frobenius Rings,* J.Algebra App., vol. 5, **6**,pp. 799-845 (2006)

[14] Hammons, A. R., Jr., Kumar, P. V., Calderbank, A. R., Sloane, N.J. A., and Solé, P., *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes,*

IEEE Trans. Inform. Theory, **IT-40**, (1994), pp. 301-319.

[15] Wood, J., *"Duality for modules over finite rings and applications to coding theory,"* Amer. J. Math., vol.121, pp. 555-575, 1999.

[16] Ling, S. and Xing, C., Coding Theory: A First Course: Cambridge University Press, 2004.

[17] Huffman, W. and Pless, V., *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.

[18] Grefrath, M., O'Sullivan, ME., *On bounds for codes over Frobenious rings under homogeneous weight*, J. Disc. Mathematics, vol. 289, pp. 11-24, 2004.

[19] Betsumiya, K., Ling, S., Nemenzo, FR., *Type II codes over* $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$, Discrete Math. 275:43-65, 2004.

[20] Wilson, RM., *A lemma on polynomials modulo* p^m *and applications to coding theory*, Discrete Mathematics, vol. 306, pp. 3154-3165, 2006.

[21] Calderbank, A.R., and Sloane, N.J.A., *Modular and p-adic cyclic codes*, Designs, Codes and Cryptography, 6, 1995, 21–35.

[22] Norton, G.H. and Sălăgean, A., *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Alg. Engrg. Comm. & Comput., 10, 2000, 489–506.

[23] Konmar, P., and Lopez-Permouth, S. K., *Cyclic Codes over Integers Modulo* p^m, Finite Fields and Applications, Vol 3, pp. 334–352, 2007.

[24] Pless, V.S. and Qian, Z., *Cyclic codes and quadratic residue codes over* $\mathbb{Z}_4$, IEEE-IT, 42, No. 5, September 1996, 1594–1600.

[25] Van Lint, J. H., *Introduction to Coding Theory (Graduate Texts in Mathematics),* 3rd ed.: Springer, 1998.

[26] MacWilliams, F. J. and Sloane, N.J.A., *The Theory of Error Correcting Codes.* Amsterdam, North-Holland , 1977.

[27] Dougherty, S. T. and Ling, S., *Cyclic codes over* $\mathbb{Z}_4$ *of even length*, Designs, Codes and Cryptography, 2006, 127–153

[28] Blackford, T., *Cyclic codes over* $\mathbb{Z}_4$ *of oddly even length,* Discrete Applied Math, vol. 128, pp. 27-46, 2003.

[29] Yıldız, B. and Sıap, I., *Cyclic codes over* $\mathbb{F}_2[u]/(u^4-1)$ *and applications to DNA codes ,*

[30] Huffman, W.C., *Decompositions and external Type II codes over* $\mathbb{F}_2+u\mathbb{F}_2$.

IEEE Trans. Inform. Theory, 45 (1999), 32-45.

[31] Kai, X., Zhu, S. and Li, P., *(1+λu)-constacyclic codes over* $\mathbb{F}_p[u]/(u^m)$, J. Frank. Inst., Vol. 347, No 5, p.751-762, 2010.

[32] Ozen, M. and Siap, I., *Linear codes over* $\mathbb{F}_q[u]/(u^s)$ *with respect to the Rosenbloom-Tsfasman metric*, Designs, Codes and Cryptography, Vol.38, 2006, p. 17–29.

[33] Abualrub, T. and Oehmke, R., *On generators of* $\mathbb{Z}_4$ *cyclic codes of length* 2^e, IEEE-IT, 49, No. 9, September 2003, 2126–2133

[34] Udaya, P. and Bonnecaze, A., *Decoding of cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45 (1999), 2527-2532.

[35] Honold, T. and Landjev, I., *Linear codes over finite chain rings*, Electron J. Combin. 7 (2000).

[36] Qian, J., Li Zhang and Shi Zhu, *Constacyclic and cyclic odes over* $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, IEICE Transactions on Fundamental of electronics and computer sciences archive. vol.E89-A, Iss4 6 , pp 1863-1885, (June 2006).

[37] Ling, S. and Solé, P., *On the algebraic structure of quasi-cyclic codes II: chain rings,* Des., Codes & Crypto., 30, 2003, 113–130.

[38] Bini, G. and Flamini, F., *Finite Commutative Rings and Applications*, Kluwer Academic Publishers, 2002.

[39] Yildiz, B., *Weights modulo* p^e *of linear codes over rings*, Designs, Codes and Cryptography, vol. 43, pp. 147-165, 2007.

[40] Berlekamp, E. R., *Negacyclic codes for the Lee metric*, in Proc. Conf. Combinatorial Mathematics and its application s, Chapel Hill, NC, 1968, pp. 298-316.

[41] Dinh, H. Q., *Constacyclic codes of length* p^s *over* $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$, J. Algebra, 324 (2010), 940-950.

[42] Karadeniz, S., *Linear codes over the ring* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and their binary images, PhD thesis, Fatih University, Turkey, 2010.

[43] Wolfmann, J., *Binary images of Cyclic Codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, **47**, (2001), pp. 1773-1779.