The Islamic University of Gaza
Deanery of Higher Studies
Faculty of Science
Department of Mathematics

A family Of Cyclic Codes Over Finite Chain Rings

Presented by:
Sanaa Yusuf Sabouh

Supervised by:
Dr.: Mohammed Mahmoud AL-Ashker

SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
AT
ISLAMIC UNIVERSITY
GAZA, PALESTINE
2008

DEDICATION

To

My Parents

My sincere friends

and to all knowledge seekers

Contents

Acknowledgements

First of all, gratitude and thanks to **Almighty Allah** who always helps and guides me.

I wish to extend my gratitude and appreciation to my supervisor Dr. Mohammed M. AL-Ashker for his help and advice during the preparation of the thesis. Thanks are also due to the examiners committee Dr. Fayik EL-Naoqe, and Dr. Arwa Ashour. Thanks are also due to the head and the staff members of the Mathematics Department, and the Faculty of Science of the Islamic University.

Abstract

Codes over finite rings have received much attention recently after it was proved that important families of binary non-linear codes are images under a Gray map of linear codes over $\mathbb{Z}_4$. A set of n-tuples over a ring $\mathbb{R}$ is called a code over $\mathbb{R}$ if it is an $\mathbb{R}$-module. A cyclic codes of length n over the ring $\mathbb{R}$ is a linear code with property that if the codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ then the cyclic shift $(c_1, c_2, \ldots, c_0) \in C$. The cyclic codes are ideals in the ring $\mathbb{R}_n = \mathbb{R}[x]/(x^n - 1)$. A commutative ring $\mathbb{R}$ with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion. We study in this thesis to study cyclic codes over finite chain rings. We first give a survey study a bout cyclic codes over the rings $\mathbb{Z}_{p^k}$ of integers modulo p^k for a prime p and $k \geq 1$, in particular $\mathbb{Z}_4$ and $\mathbb{Z}_8$ and study their structures. We will extend this study to cyclic codes for more chain rings $\mathbb{F}_p + u\mathbb{F}_p$, $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ and $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$ for different prime number p and we will define and construct idempotent generators for cyclic over these rings and study their properties.

Introduction

The beginning of coding theory goes back to the middle of the last century with the work of Shannons, Hamming, Golay and others. Historically coding theory originated as the mathematical foundation for the transmission of messages over noisy channels. In fact a multitude of diverse applications have been discovered such as the minimization of noise from compact disc recordings the transmission of financial information a cross telephone lines, data transfer from one computer to another and so on. Coding theory deals with the problem of detecting and correcting transmission errors caused by noise on the channel.

Mathematical background was at the beginning very little but with passing of time, various mathematical tools, such as group theory, ring theory, and linear programming have been applied to coding theory. Thus, coding theory has now become an active part of mathematical research. In many cases, the information to be sent is transmitted by a sequence of zeros and ones called binary codes, which means that the code is defined on the field $\{0, 1\}$. In this thesis we study that any $\mathbb{Z}_4$-cyclic code C has generators of the form $(fh, 2fg)$ where $fgh = x^n - 1$ over $\mathbb{Z}_4$, and $\mid C \mid = 4^{degg} 2^{degh}$. We also study that $C^{\perp}$ has generators of the form $(g^*h^*, 2f^*g^*)$ and show that a $\mathbb{Z}_4$-cyclic code has an idempotent generator. The structure of cyclic codes over $\mathbb{Z}_{p^m}$ was obtained by Galderbank and sloane in [4], and later on, with a different proof by kanwar in [18]. Using the techniques presented in [18], Wan [26] extended Kanwars results to cyclic codes over Galois rings. Cyclic self dual codes and linear simplex codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been extensively studied in the papers [2], [3]. Codes over $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$ have discussed by of a number of authors in [16].

The material of this thesis lies in five chapters.

Chapter 1:- Includes algebraic preliminaries, Basic definitions of coding theory, cyclic codes over finite fields, about Galois rings that are needed in

the thesis.

Chapter 2:- Include generating and dual of cyclic codes over finite chain rings of four elements as $\mathbb{Z}_4$ and "$\mathbb{F}_2 + u\mathbb{F}_2$", where $u^2 = 0$

Chapter 3:- Presents a brief introduction to codes over $\mathbb{Z}_{p^m}$ and "$\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$", cyclic codes over $\mathbb{Z}_{p^m}$ and "$\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$", where $u^k = 0$ and examples.

Chapter 4:- In this chapter we will study idempotent generators of cyclic codes over rings of four elements and present some examples.

Chapter 5:- Includes generating idempotents of cyclic codes over $\mathbb{Z}_{p^m}$, examples on generating idempotents of cyclic codes over $\mathbb{Z}_4$ and $\mathbb{Z}_8$, generating idempotents of cyclic codes over "$\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$", where $u^k = 0$ and also we give some examples on generating idempotents of cyclic codes over "$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$" and "$\mathbb{F}_3 + u\mathbb{F}_3$", where $u^2 = 0$.

Chapter 1

Preliminaries

1.1 Algebraic preliminaries

The purpose of this section is to review some basic facts that will be needed through the thesis.

Rings and Fields

Definition 1.1.1. [23] A nonempty set $\mathbb{R}$, together with two binary operations $+$ and $.$ is said to form a Ring, for all $a,\ b,\ c \in \mathbb{R}$ if the following axioms are satisfied :

(i) $a + (b + c) = (a + b) + c$

(ii) $a + b = b + a$

(iii) $\exists$ some element 0 (called zero) in $\mathbb{R}$ s.t.,
$a + 0 = 0 + a = a$

(iv) for each $a \in \mathbb{R}$, $\exists$ *an element* $(-a) \in \mathbb{R}$, s.t.,
$a + (-a) = (-a) + a = 0$

(v) $a.(b.c) = (a.b).c$

(vi) $a.(b + c) = a.b + a.c$
$(b + c).a = b.a + c.a$

Definition 1.1.2. [23] A ring $\mathbb{R}$ is called a commutative ring if $ab = ba$ for all $a, b \in \mathbb{R}$.
Again if $\exists$ a unique element $e \in \mathbb{R}$ s.t.,

$$ae = ea = a \text{ for all } a \in \mathbb{R}$$

we say, $\mathbb{R}$ is a ring with unity. Unity is generally denoted by 1 (it is also called unit element or multiplicative identity).

Definition 1.1.3. [23] An element a in a ring $\mathbb{R}$ with unity, is called invertible (or a unit) with respect to multiplication if $\exists$ some $b \in \mathbb{R}$ such that $ab = 1 = ba$.

Definition 1.1.4. [23] Let $\mathbb{R}$ be a ring . An element $0 \neq a \in \mathbb{R}$ is called a zero-divisor, if $\exists$ an element $0 \neq b \in \mathbb{R}$ s.t., $ab = 0$ or $ba = 0$.

Definition 1.1.5. [23] A commutative ring with unity is called an integral domain if $ab = 0$ in $\mathbb{R} \implies$ either $a = 0$ or $b = 0$. In other words, a commutative ring is called an integral domain if $\mathbb{R}$ has no zero divisors.

Definition 1.1.6. [19] A field is a nonempty set $\mathbb{F}$ of elements with two binary operations + (called addition) and . (called multiplication) satisfying the following axioms. For all $a,\ b,\ c \in \mathbb{F}$:

(i) $\mathbb{F}$ is closed under + and ..; i.e., $a + b$ and $a.b$ are in $\mathbb{F}$.

(ii) Commutative laws: $a + b = b + a$, $a.b = b.a$.

(iii) Associative laws: $(a + b) + c = a + (b + c)$, $a.(b.c) = (a.b).c$.

(iv) Distributive law: $a.(b + c) = a.b + a.c$.

Furthermore, two distinct identity elements 0 and 1 (called the additive and multiplicative identities, respectively) must exist satisfying the following:

(v) $a + 0 = a$ for all $a \in \mathbb{F}$.

(vi) $a.1 = a$ and $a.0 = 0$ for all $a \in \mathbb{F}$.

(vii) For any a in $\mathbb{F}$, there exist an additive inverse element $(-a)$ in $\mathbb{F}$ such that $a + (-a) = 0$.

(viii) For any $a \neq 0$ in $\mathbb{F}$, there exists a multiplicative inverse element a^{-1} in $\mathbb{F}$ such that $a.a^{-1} = 1$.

We usually write $a.b$ simply as ab, and denote by $\mathbb{F}^*$ the set $\mathbb{F}|\{0\}$.

Definition 1.1.7. [23] A ring $\mathbb{R}$ with unity is called a Division ring or a skew field if all non zero elements of $\mathbb{R}$ have multiplicative inverse.

Definition 1.1.8. [23] A commutative division ring is called a field.

Lemma 1.1.1. *[23] A finite integral domain is a field.*

Corollary 1.1.2. *[23] $\mathbb{Z}_p$ the set of integers* mod p *is a field, for a prime integer p.*

Subring and the characteristic of a ring

Definition 1.1.9. [23] A non empty subset $\mathbb{S}$ of a ring $\mathbb{R}$ is said to be a subring of $\mathbb{R}$ if $\mathbb{S}$ forms a ring under the binary compositions of $\mathbb{R}$. The ring $< \mathbf{Z}, +, . >$ of integers is a subring of the ring $< \mathbf{R}, +, . >$ of real number.
If $\mathbb{R}$ is a ring then 0 and $\mathbb{R}$ are always subrings of $\mathbb{R}$, called trivial subring of $\mathbb{R}$.

Theorem 1.1.3. *[23] A non empty subset $\mathbb{S}$ of a ring $\mathbb{R}$ is a sub-ring of $\mathbb{R}$ if and only if $a,\ b \in \mathbb{S}$, then $ab,\ a-b \in \mathbb{S}$.* □

Definition 1.1.10. [23] Let $\mathbb{R}$ be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in \mathbb{R}$, then $\mathbb{R}$ is said to have finite characteristic and also the smallest such positive integer n is called the characteristic of $\mathbb{R}$.
If no such positive integer exists then $\mathbb{R}$ is said to have characteristic zero (or infinity). Characteristic of $\mathbb{R}$ is denoted by char $\mathbb{R}$ or $ch\mathbb{R}$.

Example 1.1.1.

(i) The characteristics of $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ *are 0, where* $\mathbf{Q}$ *is the set of all rational numbers,* $\mathbf{R}$ *is the set of all real numbers and* $\mathbf{C}$ *is the set of all complex numbers.*

(ii) The characteristic of the field $\mathbb{Z}_p$ is p for any prime p.

Ideals

Definition 1.1.11. [8] A nonempty subset I of a ring $\mathbb{R}$ is called a left ideal if

(i) For all $a, b \in I \Rightarrow$ both a+b and a-b belong *to* I.

(ii) For all $a \in I$ and all $r \in \mathbb{R} \Rightarrow ra \in I$.

Symmetrically, we define a right ideal. A nonempty subset which is both a left and a right ideal is called an ideal, or sometimes, for the sake of emphasis, a two-sided ideal. In a commutative ring the distinction between a left and a right ideal disappears. From condition (i) above it is clear that every left (or right) ideal is a subring. However, the converse need not be true. For example, in the ring $\mathbf{Q}$ of rational numbers, the set $\mathbf{Z}$ of integers is a proper subring, but not an ideal because $\frac{1}{2} \in \mathbf{Q}$, $3 \in \mathbf{Z}$. But $3.\frac{1}{2} \notin \mathbf{Z}$. In any ring, the set $\{0\}$ consisting of the zero element alone is a two-sided ideal. It is called the zero ideal and denoted by $\{0\}$. Similarly, the whole ring $\mathbb{R}$ is a two-sided ideal. If possesses an identity e, then $\mathbb{R}$ is called a unit ideal and is denoted by (e). The two ideals $\{0\}$ and $\mathbb{R}$ are said to be improper, any ideal other than $\{0\}$ and $\mathbb{R}$ is said to be proper.

Theorem 1.1.4. *[8] If $\mathbb{R}$ is a ring with unity, and I is an ideal of $\mathbb{R}$ containing a unit, then $I = \mathbb{R}$.*

Definition 1.1.12. [8]**(Normal Subgroup)** A subgroup H of a group G is **a normal** if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$ denoted $H \triangle G$, or if and only if $xHx^{-1} \subseteq H \ \ \forall x \in G$.

Every subgroup of an Abelian group is normal center of a group $\mathbb{Z}(G)$ is normal.

Quotient Rings

Let $\mathbb{R}$ be a ring and let I be an ideal in the ring $\mathbb{R}$.
Since $a, b \in I \Longrightarrow a - b \in I$, we find I is a subgroup of $< \mathbb{R}, + >$. Again as $< \mathbb{R}, + >$ is Abelian, I is a normal subgroup of $\mathbb{R}$ and thus we can talk of $\mathbb{R}/I$, the quotient group;
$\mathbb{R}/I = \{I + r : r \in \mathbb{R}\}$ = set of all cosets of I in $\mathbb{R}$ (clearly left or right cosets are equal).We know $\mathbb{R}/I$ forms a group under addition defined by

$$(r + I) + (s + I) = (r + s) + I.$$

We now define a binary composition (product) on $\mathbb{R}/I$ by

$$(r + I)(s + I) = rs + I.$$

It is a routine exercise to check that this product is well defined on $\mathbb{R}/I$. Since
$(a + I)[(b + I)(c + I)] = (a + I)(bc + I) = a(bc) + I$
$= (ab)c + I = (ab + I)(c + I) = [(a + I)(b + I)](c + I).$
Associativity holds with respect to this product.
Again, as $(a + I)[(b + I) + (c + I)] = (a + I)(b + c + I) = a(b + c) + I$
$= (ab + ac) + I = (ab + I) + (ac + I) = (a + I)(b + I) + (a + I)(c + I)$
We find distributivity holds. Similarly one can check that right distributivity also holds in $\mathbb{R}/I$ and hence $\mathbb{R}/I$ forms a ring, called the quotient ring or residue class ring of $\mathbb{R}$ by I. More information can be found in [23].

Prime Ideals and Maximal Ideals

We have seen that if $\mathbb{R}$ is a ring and I is an ideal in $\mathbb{R}$, then the set $\mathbb{R}/I$ of residue classes forms a ring. A very natural question arises: When is $\mathbb{R}/I$ an integral domain or a field ? The answer to this question leads us to the following specializations of ideals.

Definition 1.1.13. [8] An ideal $I \neq \mathbb{R}$ in a commutative ring $\mathbb{R}$ is a prime ideal if $ab \in I$ implies that either $a \in I$ or $b \in I$ for every $a, b \in \mathbb{R}$

Definition 1.1.14. [23] Let $\mathbb{R}$ be a ring. An ideal $M \neq \mathbb{R}$ of $\mathbb{R}$ is called a maximal ideal of $\mathbb{R}$ if whenever A is an ideal of $\mathbb{R}$ such that, $M \subseteq A \subseteq \mathbb{R}$ then either $A = M$ or $A = \mathbb{R}$.

Example 1.1.2. *[23]*

(i) A field $\mathbb{F}$ *has only ideals* $\mathbb{F}$ *and* $\{0\}$*. We can see that* $\{0\}$ *is the only maximal ideal of* $\mathbb{F}$*.*

(ii) $\{0\}$ *in the ring* $\mathbf{Z}$ *of integers is a prime ideal as* $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a \in 0$ *or* $b \in 0$*.*
It is an example of a prime ideal which is not maximal because $\{0\} \subsetneq 2\mathbf{Z} \subsetneq \mathbf{Z}$*.*

(iii) $\mathbb{H}_4 = \{4n, n \in \mathbf{Z}\}$ *we can see that it is a maximal ideal in the ring* $\mathbb{E}$ *of even integers.*
$\mathbb{H}_4$*, however, is not a prime ideal as* $2.2 = 4 \in \mathbb{H}_4$ *but* 2 *is not belong* $\mathbb{H}_4$*.*
And also is not maximal ideal because $4\mathbf{Z} \subsetneq 2\mathbf{Z} \subsetneq \mathbf{Z}$*.*
In fact, $\mathbb{H}_4$ *is neither a maximal nor a prime ideal in* $\mathbf{Z}$*.*

In the following two theorems we give alternative criterions for an ideal in an arbitrary commutative ring to be prime or maximal.

Theorem 1.1.5. *[8] Let* $\mathbb{R}$ *be a commutative ring with unity, and let* $I \neq \mathbb{R}$ *be an ideal in* $\mathbb{R}$*. Then* $\mathbb{R}/I$ *is an integral domain if and only if* I *is prime ideal in* $\mathbb{R}$*.* □

Theorem 1.1.6. *[23] Let* $\mathbb{R}$ *be a commutative ring with unity. An ideal* M *of* $\mathbb{R}$ *is maximal ideal of* $\mathbb{R}$ *if and only if* $\mathbb{R}/M$ *is a field.* □

Corollary 1.1.7. *[8] Every maximal ideal in a commutative ring* $\mathbb{R}$ *with unity is a prime ideal, but the converse is not true see Example 1.4.3* (ii)*.*

Definition 1.1.15. [23] Two ideals A and B are called comaximal if

$$A + B = \mathbb{R}.$$

Definition 1.1.16. [24] An ideal I of a ring $\mathbb{R}$ is called a primary ideal provided $ab \in I$ implies that either $a \in I$ or $b^r \in I$ for some positive integer r.

Every prime is primary, but the converse is not true, $4\mathbf{Z}$ *is primary but not prime.*

Definition 1.1.17. [8] An ideal I of a ring $\mathbb{R}$ is called a principal ideal if there exists an element $g \in I$ such that $I =< g >$, where

$$< g >= \{gr : r \in \mathbb{R}\}.$$

The element g is called a generator of I and I is said to be generated by g.
A ring $\mathbb{R}$ is called a principal ideal ring if every ideal of $\mathbb{R}$ is principal.

Example 1.1.3. *[8] The ideal* $< x >$ *in* $\mathbb{F}[x]$ *consist of all polynomials in* $\mathbb{F}[x]$ *having zero constant term.*
Z *is a principal ideal domain. Moreover, given any nonzero ideal* I *of* **Z**, *the smallest positive integer in* I *is a generator for the ideal.*

Definition 1.1.18. [24] A local ring is a ring that has a unique maximal ideal.

Definition 1.1.19. [25] A commutative ring with unity is called a chain ring if all its ideals from a chain under inclusion.

$\mathbb{R}$ *is a commutative integral domain such that any strictly ascending chain of ideal is finite.*
i.e. $I_0 \subsetneqq I_1 \subsetneqq I_2 \ldots \subsetneqq I_n \subsetneqq \ldots$ *must stop after finitly many ideals.*

Theorem 1.1.8. *[12] For a finite commutative ring* $\mathbb{R}$ *the following conditions are equivalent :*

i) $\mathbb{R}$ *is a local ring and the maximal* M *of* $\mathbb{R}$ *is principal;*

ii) $\mathbb{R}$ *is a local principal ideal ring;*

iii) $\mathbb{R}$ *is a chain ring.* □

Homomorphisms and Isomorphisms

Definition 1.1.20. [8] Let $\mathbb{R}$ and $\mathbb{R}'$ be rings (or fields).
A function ψ:$\mathbb{R} \longrightarrow \mathbb{R}'$ is a **homomorphism** if for all $a, b \in \mathbb{R}$,

$$\psi(a+b) = \psi(a) + \psi(b)$$

and

$$\psi(ab) = \psi(a)\psi(b).$$

Definition 1.1.21. [8] An **isomorphism** ψ: $\mathbb{R} \longrightarrow \mathbb{R}'$ is a homomorphism that is one-to-one and onto $\mathbb{R}'$.

Definition 1.1.22. [8] Let f:$\mathbb{R} \longrightarrow \mathbb{R}'$ be a homomorphism, we define **kernel** of f by

$$\ker f = \{x \in \mathbb{R} : f(x) = 0'\}$$

where $0'$ is a zero of $\mathbb{R}'$.

Theorem 1.1.9. *[8] If* f:$\mathbb{R} \longrightarrow \mathbb{R}'$ *is a homomorphism, then*

- $\ker f$ *is an ideal of* $\mathbb{R}$.
- $\ker f =< 0 >$ *if and only if* f *is one-one.* □

Rings of Polynomials

Definition 1.1.23. [8] **Polynomial** Let $\mathbb{R}$ be a ring. A polynomial $f(x)$ with coefficients in $\mathbb{R}$ is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,$$

where $a_i \in \mathbb{R}$ and $a_i = 0$ for all but a finite number of values of i. The a_i are coefficients of $f(x)$. If for some $i \geq 0$ it is true that $a_i \neq 0$, the largest such value of i is the degree of $f(x)$. If all $a_i = 0$, then the degree of $f(x)$ is undefined.

*L*et us agree that if $f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ has $a_i = 0$ for $i > n$, then we may denote $f(x)$ by $a_0 + a_1 x + \ldots + a_n x^n$.
Addition and multiplication of polynomials with coefficients in a ring $\mathbb{R}$ are defined in a way familiar to us. Let

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m,\ a_i \in \mathbb{R},$$

$$g(x) = b_0 + b_1 x + \ldots + b_n x^n,\ b_i \in \mathbb{R},$$

be two polynomials over $\mathbb{R}$, then we say $f(x) = g(x)$ if $m = n$ and $a_i = b_i$ for all i.
Again, addition of polynomials $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$$

*P*roduct is also defined in the usual way
$f(x)g(x) = (a_0 + a_1 x + \ldots + a_m x^m)(b_0 + b_1 x + \ldots + b_n x^n)$
$= a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \ldots = c_0 + c_1 x + c_2 x^2 + \ldots + c_{m+n} x^{m+n}$
where $c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0 = \sum_{r=0}^{k} a_r b_{k-r}$
Let now $\mathbb{R}[x]$ be the set of all polynomials over $\mathbb{R}$. Zero of the ring will be the zero polynomial $O(x) = 0 + 0x + 0x^2 + \ldots$.
Additive inverse of $f(x) = a_0 + a_1 x + \ldots + a_m x^m$ will be the polynomial $-f(x) = -a_0 - a_1 x + \ldots + (-a_m)x^m$. In fact, if $\mathbb{R}$ has unity 1 then the polynomial $e(x) = 1 + 0x + 0x^2 + \ldots$ will be unity of $\mathbb{R}[x]$. $e(x)$ is also sometimes denoted by 1. Instead of a ring $\mathbb{R}$ if we start with a field $\mathbb{F}$ we get the corresponding ring $\mathbb{F}[x]$ of polynomials, see [23].

Theorem 1.1.10. *[23] Let $\mathbb{R}[x]$ be the ring of polynomials over a ring $\mathbb{R}$, then*

(i) $\mathbb{R}$ is commutative if and only if $\mathbb{R}[x]$ is commutative.

(ii) $\mathbb{R}$ has unity if and only if $\mathbb{R}[x]$ has unity. □

Theorem 1.1.11. *[23] Let $\mathbb{R}[x]$ be the ring of polynomial of a ring $\mathbb{R}$ and suppose*

$$f(x) = a_0 + a_1x + \ldots + a_mx^m,$$

$$g(x) = b_0 + b_1x + \ldots + b_nx^n,$$

are two non zero polynomials of degree m and n respectively, then

(i) If $\mathbb{R}$ is an integral domain, $deg(f(x)g(x)) = m + n$.

(ii) $\mathbb{R}$ is an integral domain if and only if $\mathbb{R}[x]$ is an integral domain.

(iii) If $\mathbb{F}$ is a field, $\mathbb{F}[x]$ may not be field. □

Definition 1.1.24. [8] Let $f(x)$ and $g(x)$ be polynomials over the field $\mathbb{F}$. If $\gcd(f(x), g(x)) = 1$, we say that $f(x)$ and $g(x)$ are relatively prime (over $\mathbb{F}$). In particular, $f(x)$ and $g(x)$ are relatively prime if and only if there exist polynomials $a(x)$ and $b(x)$ over $\mathbb{F}$ for which $a(x)f(x) + b(x)g(x) = 1$.

Definition 1.1.25. [8] A polynomial $f(x) \in \mathbb{R}[x]$, is monic provided its leading coefficient is 1.

Definition 1.1.26. [24] Two polynomials f and g in $\mathbb{R}[x]$ are called coprime, or relatively prime if

$$\mathbb{R}[x] =< f > + < g > .$$

Definition 1.1.27. [24] A polynomial $f(x) \in \mathbb{R}[x]$ is primary if the principal ideal
$< f(x) >= \{f(x)g(x),\ g(x) \in \mathbb{R}[x]\}$ is primary ideal.

Theorem 1.1.12. *[8] Every nonzero prime ideal of a principal ideal domain is maximal ideal.* □

Theorem 1.1.13. *[8] If the ring $\mathbb{F}$ is a field, then every ideal in $\mathbb{F}[x]$ is principal ideal domain.* □

Definition 1.1.28. [23] A nonconstant polynomial $f(x) \in \mathbb{F}[x]$ is irreducible if whenever $f(x) = p(x)q(x)$, then one of $p(x)$ or $q(x)$ must be constant.

Definition 1.1.29. [8] Let $p(x)$ is irreducible polynomial in $\mathbb{F}[x]$ and $p(x)|r(x)s(x)$, for $r(x), s(x) \in \mathbb{F}[x]$, then either $p(x)|\ r(x)$ or $p(x)|\ s(x)$.

Theorem 1.1.14. *[8] An ideal $I =< p(x) >\neq 0$ in $\mathbb{F}[x]$ is maximal if and only if $p(x)$ is irreducible over $\mathbb{F}$.* □

Theorem 1.1.15. *[8] Let $\mathbb{F}$ be a field, then the ring $\mathbb{E} = \mathbb{F}[x]/< p(x) >$ is a field if and only if $p(x)$ is irreducible.* □

Definition 1.1.30. [23] Every nonconstant polynomial in $\mathbb{F}[x]$ can be written uniquely (up to order) as a product of irreducible polynomials.

Prime and Irreducible Elements

Definition 1.1.31. [23] Let $\mathbb{R}$ be a commutative ring with unity, then $a,\ b \in \mathbb{R}$ are called associate if $b = ua$ for some unit u in $\mathbb{R}$.

Definition 1.1.32. [23] Let $\mathbb{R}$ be a commutative ring with unity. An element $p \in \mathbb{R}$ is called a **prime element** if

(i) $p \neq 1$, p is not a unit.

(ii) For any $a,\ b \in \mathbb{R}$, if $p|ab$ then $p|a$ or $p|b$.

An element $p \in \mathbb{R}$ is called an **irreducible element** if

(i) $p \neq 0$, p is not a unit.

(ii) Whenever $p = ab$, then one of a *or* b must be a unit.

Theorem 1.1.16. *[23] In a PID an element is prime if and only if it is irreducible.* □

Example 1.1.4. *[23]*

⋆ *In the ring $< \mathbf{Z}, +, . >$ of integers, every prime number is a prime element as well as irreducible element.*

Corollary 1.1.17. *[23] In an integral domain with unity, every prime element is irreducible. The converse is not true.*

Example 1.1.5. *[23]*

⋆ *Consider the ring $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ mod 6.*
2 is a prime element in $\mathbb{Z}_6$ but is not irreducible. Because $2 \otimes 4 = 2$, where neither 2 nor 4 is a unit, we find 2 is not irreducible.
(Note, $\mathbb{Z}_6$ is not an integral domain)

Unique Factorization Domain

Definition 1.1.33. [23] Let $\mathbb{R}$ be an integral domain with unity then $\mathbb{R}$ is called a unique factorization domain (UFD) if

(i) every nonzero, non unit element a of $\mathbb{R}$ can be expressed as a product of finite number of irreducible elements of $\mathbb{R}$ and

(ii) if $a = p_1 p_2 \dots p_m$
$a = q_1 q_2 \dots q_n$
where p_i and q_j are irreducible in $\mathbb{R}$ then $m = n$ and each p_i is an associate of some q_j.

Example 1.1.6. *[23]*

The ring $< \mathbf{Z}, +, . >$ *of integers is a UFD.*

A field $< \mathbb{F}, +, . >$ *is always a UFD as it contains no non zero, non unit elements.*

Vector spaces over finite fields

Definition 1.1.34. [23] Let $\mathbb{F}_q$ be the finite field of order q. A nonempty set V, together with some (vector) addition denoted $+$ and scalar multiplication by elements of $\mathbb{F}_q$, is a vector space (or linear space) over $\mathbb{F}_q$ if it satisfies all of the following conditions. For all $u, v, w \in V$ and for all $\lambda, \mu \in \mathbb{F}_q$:

(i) $u + v \in V$;

(ii) $(u + v) + w = u + (v + w)$;

(iii) there is an element $0 \in V$ with the property $0 + v = v + 0$ for all $v \in V$;

(iv) for each $u \in V$ there is an element of V, called $-u$, such that $u + (-u) = 0 = (-u) + u$;

(v) $u + v = v + u$;

(vi) $\lambda v \in V$;

(vii) $\lambda(u + v) = \lambda u + \lambda v, (\lambda + \mu)u = \lambda u + \mu u$;

(viii) $(\lambda\mu)u = \lambda(\mu u)$;

(ix) if 1 is the multiplicative identity of $\mathbb{F}_q$, then $1u = u$.

Definition 1.1.35. [19] A nonempty subset C of a vector space V is a subspace of V if is itself a vector space with the same vector addition and scalar multiplication as V.

Modules and Submodules

Definition 1.1.36. [6] Let $\mathbb{R}$ be any ring, and let $\mathbb{M}$ be an Abelian group, then M is called a **left $\mathbb{R}$-module** if there exists a scalar multiplication $\psi : \mathbb{R} \times \mathbb{M} \to \mathbb{M}$ denoted by $\psi(r, m) = rm$, for all $r \in \mathbb{R}$ and all $m \in \mathbb{M}$, such that for all $r, r_1, r_2 \in \mathbb{R}$ and all $m, m_1, m_2 \in \mathbb{M}$,

(i) $r(m_1 + m_2) = rm_1 + rm_2$

(ii) $(r_1 + r_2)m = r_1m + r_2m$

(iii) $r_1(r_2m) = (r_1r_2)m$

(iv) $1m = m$. To denote that $\mathbb{M}$ is a left $\mathbb{R}$-modulo.

Example 1.1.7. *[6] If $\mathbb{R}$ is a ring then $\mathbb{R}$ is an $\mathbb{R}$-module (Left $\mathbb{R}$-module and right $\mathbb{R}$-module).*
Vector spaces over $\mathbb{F}$ are $\mathbb{F}$-modules where $\mathbb{F}$ is a field.

Definition 1.1.37. [6] Any subset of $\mathbb{M}$ that is a left $\mathbb{R}$-module under operations induced from $\mathbb{M}$ is called a **submodule**.
The subset $\{0\}$ is called the trivial submodule.
The module $\mathbb{M}$ is a submodule of itself.
i.e. If $\mathbb{M}$ is a left $\mathbb{R}$-module, then a subset $\mathbb{N} \subset \mathbb{M}$ is a **submodule** if and only if it is nonempty, closed under sums, and closed under multiplication by elements of $\mathbb{R}$.

New Ring from old

*L*et $< \mathbb{R}, +, . >$ and $< \mathbb{S}, +, . >$ be two rings, their product is the ring $(\mathbb{R} \times \mathbb{S}, +, .)$ whose underlying set is the Cartesian product of $\mathbb{R}$ and $\mathbb{S}$ and whose binary operations are defined by

$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$

$(r_1, s_1).(r_2, s_2) = (r_1r_2, s_1s_2)$

This ring is called the direct product of $\mathbb{R}$ and $\mathbb{S}$.

One can similarly extend the definition to product of more than two rings.

$\mathbb{R}$ and $\mathbb{S}$ are called the component rings of the direct product.

Theorem 1.1.18. *[8] $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to the ring $\mathbb{Z}_{mn}$ if and only if* $\gcd(m, n) = 1$ □

Theorem 1.1.19. *[8] Let $m = m_1.m_2 \ldots m_r$ where* $\gcd(m_i, m_j) = 1$ *if $i \neq j$. Then $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r}$ is a ring isomorphic to $\mathbb{Z}_m$.* □

Theorem 1.1.20. *[23]* ***Chinese Remainder Theorem***
Let $\mathbb{R}$ be a commutative ring with unity and let I_1 and I_2 be two ideals of $\mathbb{R}$, then

(i) φ: $\mathbb{R} \longrightarrow \mathbb{R}/I_1 \times \mathbb{R}/I_2$, such that, $\varphi(x) = (x + I_1, x + I_2)$ is a homomorphism such that, $Ker\varphi = I_1 \bigcap I_2$.

(ii) If φ is onto, then I_1 and I_2 are comaximal ideals of $\mathbb{R}$.

Proof. (i) We leave it for the reader to verify that φ is homomorphism. Since
$x \in Ker\varphi \Longleftrightarrow \varphi(x) = (I_1, I_2)$
$\Longleftrightarrow (x + I_1, x + I_2) = (I_1, I_2) \Longleftrightarrow x + I_1 = I_1$ and $x + I_2 = I_2$
$\Longleftrightarrow x \in I_1$ and $x \in I_2 \Longleftrightarrow x \in I_1 \bigcap I_2$ we find $Ker\varphi = I_1 \bigcap I_2$.

(ii) Suppose φ is onto. Then given $(1 + I_1, 0 + I_2) \in \mathbb{R}/I_1 \times \mathbb{R}/I_2$, $\exists\, x \in \mathbb{R}$, s.t.,

$$\varphi(x) = (1 + I_1, I_2)$$

$\Longrightarrow (x + I_1, x + I_2) = (1 + I_1, I_2) \Longrightarrow x + I_1 = 1 + I_1$ and $x + I_2 = I_2$
$\Longrightarrow 1 - x \in I_1$ and $x \in I_2 \Longrightarrow (1 - x) + x \in I_1 + I_2 \Longrightarrow 1 \in I_1 + I_2$
$\Longrightarrow I_1 + I_2 = \mathbb{R}$ or that I_1 and I_2 are comaximal. □

Finite Fields

The order of a field is the number of elements in the field. If the order is infinite, we call the field an infinite field, and if the order is finite, we call the field a finite field or a Galois field.

Definition 1.1.38. [23] A finite field with p^m elements is called a Galois field of order p^m and is denoted by $GF(p^m)$.

Theorem 1.1.21. *[23] For any prime p and any positive integer m, there exists a finite field, unique up to isomorphism, with $q = p^m$ elements.* □

Lemma 1.1.22. *[19] For every element β of a finite field $\mathbb{F}$ with q elements, we have $\beta^q = \beta$.*

Definition 1.1.39. [8] The order of a nonzero element $\alpha \in \mathbb{F}_q$, denoted by $ord(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$.

Definition 1.1.40. [23] In an Abelian group. If a has order n and b has order m with $\gcd(m, n) = 1$ them ab has order mn

Definition 1.1.41. [8] **(primitive Root of Unity)** An element α of a field is an nth root of unity if $\alpha^n = 1$.
It is a primitive nth root of unity if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.
An element α in a finite field $\mathbb{F}_q$ is called a primitive element (or a generator) of $\mathbb{F}_q$ if $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.

Theorem 1.1.23. *[24] The elements of $\mathbb{F}_q$ are precisely the roots of the polynomial $x^q - x$.* □

Theorem 1.1.24. *[8]* ***Division Algorithm***
Let $f(x)$ and $g(x)$ be in $\mathbb{F}_q[x]$, where $\mathbb{F}_q[x]$ is the ring of all polynomials over the field $\mathbb{F}_q$ with $g(x)$ nonzero, then

1. *There exist unique polynomials $h(x),\ r(x) \in \mathbb{F}_q[x]$, such that*
   $f(x) = g(x)h(x) + r(x), \quad$ *where deg* $r(x) <$ *deg* $g(x)$ *or* $r(x) = 0$.
2. *If $f(x) = g(x)h(x) + r(x)$, then*
   $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$. □

Corollary 1.1.25. *[23] Let $f(x) \in \mathbb{F}[x]$, then α is root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$ over $\mathbb{F}$*

Theorem 1.1.26. *[24]* ***(Hensels Lemma)***
Let $f(x) \in \mathbb{Z}_4[x]$. Suppose $\mu(f(x)) = h_1(x)h_2(x)\dots h_k(x)$, where $h_1(x), h_2(x), \dots, h_k(x)$ are pairwise coprime polynomials in $\mathbb{F}_2[x]$. Then there exist $g_1(x), g_2(x), \dots, g_k(x) \in \mathbb{Z}_4[x]$ such that:

1. *$\mu(g_i(x)) = h_i(x)$ for $1 \le i \le k$,*
2. *$g_1(x), g_2(x), \dots, g_k(x)$ are pairwise coprime, and*
3. *$f(x) = g_1(x)g_2(x)...g_k(x)$.* □

Extension Field

Definition 1.1.42. [8] **(Extension Field)** A field $\mathbb{E}$ is called an extension of a field $\mathbb{F}$ if $\mathbb{F} \le \mathbb{E}$.
Thus $\mathbf{R}$ is an extension field of $\mathbf{Q}$ and $\mathbf{C}$ is an extension field of both $\mathbf{R}$ and $\mathbf{Q}$.

Theorem 1.1.27. *[8] Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be a nonconstant polynomial. Then there exist an extension $\mathbb{E}$ of $\mathbb{F}$ and $\alpha \in \mathbb{E}$ such that $f(\alpha) = 0$* □

Example 1.1.8. *[8] Let $\mathbb{F} = \mathbf{R}$, and let $f(x) = x^2 + 1$, which is well known to have no zeros in $\mathbf{R}$ and thus is irreducible over $\mathbf{R}$*
by Theorem 1.1.14. Then $< x^2 + 1 >$ is a maximal ideal in $\mathbf{R}[x]$,
so $\mathbf{R}[x]/ < x^2 + 1 >$ is a field.
Identifying $r \in \mathbf{R}$ with $r+ < x^2 + 1 >$ in $\mathbf{R}[x]/ < x^2 + 1 >$, we can view $\mathbf{R}$ as a subfield of $\mathbb{E} = \mathbf{R}[x]/ < x^2 + 1 >$. Let

$$\alpha = x+ < x^2 + 1 > .$$

Computing in $\mathbf{R}[x]/< x^2 + 1 >$,
we find $< \alpha^2 + 1 >= (x+ < x^2 + 1 >)^2 + (1+ < x^2 + 1 >)$
$=< x^2 + 1 > + < x^2 + 1 >= 0$. Thus α is a zero of $x^2 + 1$.

Definition 1.1.43. [8]**(Algebraic, Transcendental)** An element α of an extension field $\mathbb{E}$ of a field $\mathbb{F}$ is algebraic over $\mathbb{F}$ if $f(\alpha) = 0$ for some nonzero $f(x) \in \mathbb{F}[x]$.

If α is not algebraic over $\mathbb{F}$, then α is transcendental over $\mathbb{F}$. $\mathbf{C}$ is an extension field of $\mathbf{Q}$. Since $\sqrt{2}$ is a zero of $x^2 - 2$, we see that $\sqrt{2}$ is an algebraic element over $\mathbf{Q}$.

Also, i is an algebraic element over $\mathbf{Q}$, being a zero of $x^2 + 1$.

It is well known (but not easy to prove) that the real numbers π and e are transcendental over $\mathbf{Q}$. Here e is the base for the natural logarithms.

Definition 1.1.44. [8] If a polynomial $f(x) \in \mathbb{F}[x]$ factors into linear factors $f(x) = a(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ over an extension field $\mathbb{K}$, we say that $f(x)$ splits over $\mathbb{K}$.

Definition 1.1.45. [23] Let $f(x) \in \mathbb{F}[x]$. A splitting field for $f(x)$ is an extension field $\mathbb{K}$ of $\mathbb{F}$ with the property that $f(x)$ splits over $\mathbb{K}$, $f(x) = \beta(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ and that $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

Take for instance, $f(x) = x^2 + 1 \in \mathbf{Q}[x]$, then as

$$x^2 + 1 = (x + i)(x - i),$$

we find splitting field of $f(x)$ over $\mathbf{Q}$ will be $\mathbf{Q}(i)$.

However if $f(x) = x^2 + 1$ is taken as a polynomial over $\mathbf{R}$, then its splitting field over $\mathbf{R}$ is $\mathbf{R}(i) = \mathbf{C}$ the field of complex numbers.

Theorem 1.1.28. *[23] Every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field, and any two splitting fields for $f(x)$ are isomorphic.* □

Definition 1.1.46. [23] The degree of the extension $\mathbb{K}$ of the field $\mathbb{F}$, denoted by $[\mathbb{K} : \mathbb{F}]$, is the dimension of $\mathbb{K}$ as a vector space over $\mathbb{F}$. $\mathbb{K}$ is called a finite extension if $[\mathbb{K} : \mathbb{F}]$ is finite.

Minimal Polynomials

Let $\mathbb{E}$ be a finite extension of $\mathbb{F}_q$. Then $\mathbb{E}$ is a vector space over $\mathbb{F}_q$ and so $\mathbb{E}$= $\mathbb{F}_{q^t}$ for some positive integer t. By Theorem 1.1.23, each element α of $\mathbb{E}$ is a root of the polynomial $x^{q^t} - x$. Thus there is a monic polynomial M_α in $\mathbb{F}_q[x]$ of smallest degree which has α as a root, this polynomial is called the minimal polynomial of α over $\mathbb{F}_q$. In the following theorem we collect some elementary facts about minimal polynomials.

Definition 1.1.47. [19] A minimal polynomial of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is a nonzero monic polynomial $f(x)$ of the least degree such that $f(\alpha) = 0$.

Theorem 1.1.29. *[20] Let $\mathbb{F} < \mathbb{E}$ be fields, and let $\alpha \in \mathbb{E}$ have minimal polynomial $m(x)$ over $\mathbb{F}$.*

1) The polynomial $m(x)$ is the unique monic irreducible polynomial over $\mathbb{F}$ for which $m(\alpha) = 0$.

2) The polynomial $m(x)$ is the unique monic polynomial of smallest degree over $\mathbb{F}$ for which $m(\alpha) = 0$.

3) The polynomial $m(x)$ is the unique monic polynomial over $\mathbb{F}$ with property that, for all $f(x) \in \mathbb{F}[x]$, we have $f(\alpha) = 0$ if and only if $m(x)|f(x)$. □

Definition 1.1.48. [19] Let n be coprime to q. The cyclotomic coset of q (or q-cyclotomic coset) modulo n containing i is defined by

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

A subset $\{i_1, \dots, i_t\}$ of $\mathbb{Z}_n$ is called a complete set representatives of cyclotomic cosets of q modulo n if $C_{i_1}, \dots, C_{i_t}$ are distinct and $\bigcup_j^t C_{i_j} = \mathbb{Z}_n$.

Example 1.1.9. *[19]*

★ *Consider the cyclotomic cosets of* 2 *modulo* 15*:*
$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 9, 12\}$, $C_5 = \{5, 10\}$,
$C_7 = \{7, 11, 13, 14\}$. *Thus,* $C_1 = C_2 = C_4 = C_8$, *and so on.*
The set $\{0, 1, 3, 5, 7\}$ *is complete set of representatives of cyclotomic cosets of* 2 *modulo* 15*.*

Example 1.1.10. *[24] The polynomial $f(x) = 1 + x + x^3$ is irreducible over $\mathbb{F}_2$; if it were reducible, it would have a factor of degree* 1 *and hence a root in $\mathbb{F}_2$, which it does not. So $\mathbb{F}_8 = \mathbb{F}_2 / < f(x) >$, The elements of $\mathbb{F}_8$ are given by:*

Cosets	*Vectors*	*Polynomials in* α	*Power of* α
$0 + < f(x) >$	000	0	0
$1 + < f(x) >$	001	1	$1 = \alpha^0$
$x + < f(x) >$	010	α	α
$x + 1 + < f(x) >$	011	$\alpha + 1$	α^3
$x^2 + < f(x) >$	100	α^2	α^2
$1 + x^2 + < f(x) >$	101	$\alpha^2 + 1$	α^6
$x^2 + x + < f(x) >$	110	$\alpha^2 + \alpha$	α^4
$x^2 + x + 1 + < f(x) >$	111	$\alpha^2 + \alpha + 1$	α^5

The column "power of α" is obtained by using $f(\alpha) = \alpha^3 + \alpha + 1 = 0$, which implies that $\alpha^3 = \alpha + 1$. So $\alpha^4 = \alpha\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha$, $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$, etc.

Example 1.1.11. *[24] The field $\mathbb{F}_8$ was constructed in the Example above. In the table below we give the minimal polynomial over $\mathbb{F}_2$ of each element of $\mathbb{F}_8$ and the associated 2-cyclotomic coset modulo 7.*

Roots	*Minimal polynomial*	$2 -$ *cyclotomic coset*
0	x	
1	$1 + x$	$\{0\}$
$\alpha, \alpha^2, \alpha^4$	$x^3 + x + 1$	$\{1, 2, 4\}$
$\alpha^3, \alpha^5, \alpha^6$	$x^3 + x^2 + 1$	$\{3, 5, 6\}$

1.2 Basic definitions of coding theory

Coding theory deals with the problem of detecting and correcting transmission errors caused by noise on the channel.

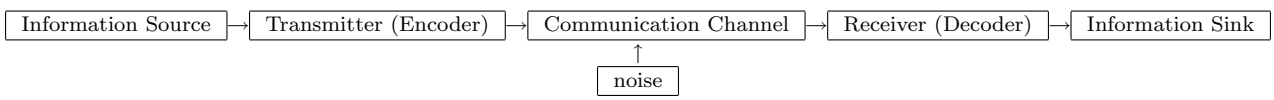
In many cases, the information to be sent is transmitted by a sequence of zeros and ones. We call a 0 or a 1 a digit. A word is a sequence of digits. The length of a word is the number of digits in the word. Thus 0110101 is a word of length seven.

A word is transmitted by sending its digits, one after the other, across a binary channel. The term binary refers to the fact that only two digits 0 and 1 are used. Each digit is transmitted mechanically, electrically, magnetically, or otherwise by one of two types of easily differentiated pluses. A binary code is a set C of words over $\mathbb{Z}_2$. The code consisting of all words of length two is

$$C = \{00, 10, 01, 11\}.$$

A block code is a code having all its words of the same length; this number is called the length of a code.

The following diagram provides a rough idea of a general information transmission system.



The most important part of diagram, as far as we are concerned, is the noise, for without it there would be no need for the theory. In practice, the control we have over this noise is the choice of a good channel to use for transmission and the use of various noise filters to combat certain types of interference which may be encountered. These are engineering problems. Once we have settled on the best mechanical system for solving these problems, we can focus our attention on the construction of the encoder and decoder. Our desire is to construct these in such a way as to effect:

1) Fast encoding of information

2) Easy transmission of encoded messages

3) Fast decoding of received messages

4) Correction of errors introduced in the channel, and

5) Maximum transfer of information per unit time.

Here we will define the terminology that we will use throughout the thesis.

Strings and codes

Definition 1.2.1. [7] Let $\mathcal{A} = \{a_1, a_2.....a_v\}$ be a finite set of v elements. A v-ary code C of length n is a non empty subset of n-tuples with entries in $\mathcal{A}$ i.e.,

$$C \subset (\mathcal{A})^n$$

The elements of the code C are called codewords, and C is called a v-ary block code. The size v of the code alphabet is called the radix of the code. The code C depends on v, a code whose alphabet is $\mathbb{Z}_2 = \{0, 1\}$ is called a binary code or a $\mathbb{Z}_2$-code, a code whose alphabet is $\mathbb{Z}_3 = \{0, 1, 2\}$ is called a ternary code or a $\mathbb{Z}_3$-code and a code whose alphabet consists of four elements such as $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is called quaternary code or a $\mathbb{Z}_4$-code. We denote the number of the codewords in a code C by $|C|$. If $C \subset \mathcal{A}^*$ contains M codewords, then we say that C has length n and size M, and we denote it by (n, M)-code.

Definition 1.2.2. [7]

- The (**Hamming distance**) $d(x, y)$ between two vectors $x,\ y \in \mathbb{F}_q^n$ is defined to be the number of coordinates in which x and y differ.
- The (**Hamming weight**) $wt(x)$ of a vector $x \in \mathbb{F}_q^n$ is the number of nonzero coordinates in x.

Definition 1.2.3. [24] For a code C containing at least two words, the minimum distance of a code C, denoted by $d(C)$, is

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

Theorem 1.2.1. *[24] If $x,\ y \in \mathbb{F}_q^n$, then $d(x, y) = wt(x - y)$. If C is a linear code, the minimum distance d is the same as the minimum weight of the nonzero codewords of C* □

Theorem 1.2.2. *[24] The distance function $d(x, y)$ satisfies the following four properties:*

(i) (non-negativity) $d(x, y) \geq 0$ for all $x,\ y \in \mathbb{F}_q^n$.

(ii) $d(x, y) = 0$ if and only if $x = y$.

(iii) (symmetry) $d(x, y) = d(y, x)$ for all $x,\ y \in \mathbb{F}_q^n$.

(iv) (triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x,\ y,\ z \in \mathbb{F}_q^n$. □

Example 1.2.1. *[19]*
★ *Let $C = \{00000, 00111, 11111\}$ be binary code. Then $d(c) = 2$ since $d(00000, 00111) = 3$, $d(00000, 11111) = 5$, $d(00111, 11111) = 2$. Hence, C is a binary $(5, 3, 2)$-code.*

Theorem 1.2.3. *[24] A code with distance d is an exactly $(d - 1)$ error detecting code.* □

Definition 1.2.4. (Linear codes over fields) Let the alphabet $\mathbb{F}_q$ be the Galois Field of q elements. A q-array linear code of length n and dimension k is a linear subspace $C \subseteq \mathbb{F}_q^n$ of the vector space of dimension n. Namely; for every $c_1,\ c_2 \in C$ and $a_1,\ a_2 \in \mathbb{F}$ we have $a_1c_1 + a_2c_2 \in C$. If C has minimum distance d, then we record that the parameters of C over $\mathbb{F}_q$ as

$$[n, k, d]_q\ .$$

Definition 1.2.5. [24] A generator matrix for an $[n, k]$ code C is any $k \times n$ matrix G whose rows form a basis for C.
Note that a generator matrix for C must have k rows and n columns, and it must have rank k.

Definition 1.2.6. [24] A generator matrix of the form $[I_k|A]$ where I_k is the $k \times k$ identity matrix is said to be in the standard form.

Theorem 1.2.4. *[24] If $G = [I_k|A]$ is a generator matrix for the $[n, k]$ code C is standard form, then $H = [-A^\tau|I_{n-k}]$ is a parity check matrix for C.* □

A matrix H is called a parity-check matrix for a linear code C if the rows of H form a basis for the dual code $C^\perp$. If C has length n and dimension k, then the sum of the dimensions of C and $C^\perp$ is n, any parity-check matrix for C must have n rows, $n - k$ columns and rank $n - k$.

Definition 1.2.7. [24] Let A_i, also denoted $A_i(C)$, 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.

Example 1.2.2. *[24] Let C be binary code with generator matrix*

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

The weight distribution of C is $A_0 = A_6 = 1$ and $A_2 = A_4 = 3$. Notice that only the nonzero A_i are usually listed.

Definition 1.2.8. [24] The single variable weight enumerator of C is

$$W_c(x) = \sum_{i=0}^{n} A_i(C)x^i.$$

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

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

Where the list A_i for $0 \leq i \leq n$ is called the weight distribution.

By Example 1.2.2, the two variable weight enumerator of C is

$$W_c(x, y) = \sum_{i=0}^{n} A_i(C)x^i y^{n-i} = y^6 + 3x^2y^4 + 3x^4y^2 + x^6.$$

Codes over rings

The study of linear codes over finite rings has received much attention lately and many recent developments of coding theory are defined on finite rings in particular over rings of four alphabets. For the purpose of this thesis we will consider alphabets as rings under addition and multiplication.

Quaternary codes

Let $\mathbb{Z}_4$ denote the integers modulo 4. $\mathbb{Z}_4$ is a ring which has 2 as a zero divisor.

Definition 1.2.9. A set C of n-tuples over $\mathbb{Z}_4$ is called a code over $\mathbb{Z}_4$ or a $\mathbb{Z}_4$- code. If C is a $\mathbb{Z}_4$ module we say that C is a linear code over $\mathbb{Z}_4$ or a quaternary code.

Example 1.2.3. *[7] The quaternary code;*

$$C = \{000, 010, 020, 030, 202, 212, 222, 232\}$$

is a linear code.

Example 1.2.4. *[7] For the code,* $C = \{000, 011, 203\}$ *is not linear code since* 011 *and* 203 *are in* C *but* $011 + 203 = 210$ *is not in* C.

Definition 1.2.10. [24] The inner product of vectors $x = x_1 \dots x_n$, $y = y_1 \dots y_n$ in F_q^n is

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

The $\mathcal{C}^{\perp}$ is defined by

$$\mathcal{C}^{\perp} = \{x \in F_q^n : x.c = 0, \ \forall \ c \in \mathcal{C}\}.$$

Definition 1.2.11. [24] A code $\mathcal{C}$ is called self-orthogonal provided $\mathcal{C} \subseteq \mathcal{C}^{\perp}$.

Definition 1.2.12. [24] A code $\mathcal{C}$ is called self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$ and the length n of a self-dual code is even and the dimension is $n/2$.

1.3 Cyclic Codes Over Finite Fields

One of the most important classes of linear codes are the class of cyclic code. These codes have great practical importance and they are also of considerable interest from an algebraic point of view since they are easy to encode. They also include the important family Bose-Chadhuri-Hocquengham (BCH) codes

which are great practical importance for error correction, particulary the number of errors is expected to be small compared with the length of the code. Also cyclic codes are considered important since they are the building blocks for many other codes. We assume throughout our discussion of cyclic codes that n and q are relatively prime. In particular, if $q = 2$ then n must be odd. When examining cyclic codes over $\mathbb{F}_q$, we will most often represent the codewords in polynomial form. There is bijective correspondence between the vectors $\mathbf{c} = c_0c_1 \dots c_{n-1}$ in $\mathbb{F}_q^n$ and the polynomials $c(x) = c_0+c_1x+\dots c_{n-1}x^{n-1}$ in $\mathbb{F}_q[x]$ of degree at most $n-1$. Notice that if $c(x) = c_0 + c_1x + \dots c_{n-1}x^{n-1}$, then $xc(x) = c_{n-1}x^n + c_0x + c_1x^2 + \dots + c_{n-2}x^{n-1}$, which would represent the codeword $\mathbf{c}$ cyclically shifted one to the right if x^n were set equal to 1. More formally, the fact that a cyclic code C is invariant under a cyclic shift implies that if $c(x)$ is in C, then so is $xc(x)$ provided we multiply modulo $x^n - 1$.

Polynomials and Words

The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ of degree at most $n-1$ over field $\mathbb{K}$ may regarded as the word

$v = a_0a_1a_2 \dots a_{n-1}$ of length n in $\mathbb{K}^n$.

For example if $n = 7$,

polynomial	word
$1 + x + x^2 + x^4$	1110100
$1 + x^4 + x^5 + x^6$	1000111
$1 + x + x^3$	1101000

Thus a code of length n can be represented as a set of polynomials over $\mathbb{K}$ of degree at most $n-1$. The word $a_0a_1a_2a_3$ of length 4 is represented by the polynomial $a_0 + a_1x + a_2x^2 + a_3x^3$ of degree 3, for instance.

Definition 1.3.1. [7] Let v be a word of length n, the cyclic shift $\pi(v)$ is the word of length n

$$\pi(v_0, v_1, \dots, v_{n-1}) = (v_{n-1}, v_0, \dots, v_{n-2}).$$

Definition 1.3.2. [7] A code C is said to be cyclic if $\pi(\upsilon) \in C$, whenever $\upsilon \in C$.

Example 1.3.1. *$C_1 = \{102, 210, 021, 201, 120, 012, 222, 111, 000\}$ is a linear cyclic code over Z_3, but $C_2 = \{000, 221, 212, 200, 121, 112, 100, 021, 012\}$ is not cyclic since $\pi(112) = 211$ which is not in C_2*

Theorem 1.3.1. *[24] If C_1 and C_2 are cyclic codes of length n over $\mathbb{F}_q$, then*

(i) $C_1 + C_2 = \{c_1 + c_2 : c_1 \in C_1,\ c_2 \in C_2\}$ *is cyclic.*

(ii) $C_1 \bigcap C_2$ *is cyclic.* □

We remember that since $\mathbb{F}_q[x]$ is principle ideal domain also the ring $\mathbb{R}_n = \mathbb{F}_q[x]/< x^n - 1 >$ is a principle ideal hence the cyclic codes are principle ideals of $\mathbb{R}_n$ when writing a code word of a cyclic code as c(x) we mean the coset $c(x) + < x^n - 1 >$ in $\mathbb{R}_n$.

Corollary 1.3.2. *[24] The number of cyclic codes of cyclic codes in $\mathbb{R}_n$ equal 2^m, where m is the number of q-cyclotomic cosets modulo n. Moreover, the dimensions of cyclic codes in $\mathbb{R}_n$ are all possible sums of the sizes of the q-cyclotomic cosets modulo n.*

Generating polynomial of a cyclic code

Theorem 1.3.3. *[15] A linear code C in $\mathbb{F}_q$ is cyclic $\iff$ C is an ideal in $\mathbb{R}_n = \mathbb{F}_q[x]/(x^n - 1)$.*

Proof. If C is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$ and $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ is any codeword, then $xc(x)$ is also a codeword, i.e $(c_{n-1}, c_0, c_1, \ldots + c_{n-2}) \in C$.

Conversely, if C is cyclic, then $c(x) \in C$ we have $xc(x) \in C$.
Therefore $x^i c(x) \in C$, and since C is linear, then $a(x)c(x) \in C$ for each polynomial $a(x)$. Hence C is an ideal. □

Theorem 1.3.4. *[24] Let C be an ideal in $\mathbb{R}_n$, then*

(i) There is a unique monic polynomial $g(x)$ of minimum degree in $C =< g(x) >$, and it is called the generating polynomial for C.

(ii) The generating polynomial $g(x)$ divides $x^n - 1$.

(iii) If $\deg(g(x)) = r$, then C has dimension $n - r$ and $C =< g(x) >= \{s(x)g(x) : \deg s(x) < n - r\}$.

(iv) If $g(x) = g_0 + g_1x + \ldots + g_rx^r$, *then* $g_0 \neq 0$ *and* C *has the following generator matrix:*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & g_2 & \ldots & g_r & 0 & \ldots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \ldots & g_r & \ldots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \vdots & 0 & g_0 & g_1 & g_2 & \vdots & g_r \end{bmatrix}$$

Proof. (i) Suppose that C contains two distinct monic polynomial g_1 and g_2 of minimum degree r. Then their difference $g_1 - g_2$ would be a nonzero polynomial in C of degree less than r, which is not possible. Hence, there is a unique monic polynomial $g(x)$ of degree r in C. Since $g(x) \in C$ and C is an ideal, we have $< g(x) > \subset C$.
On the other hand, Suppose that $p(x) \in C$, and let

$$p(x) = q(x)g(x) + r(x) \text{ where } r(x) \neq 0 \text{ and } \deg(r(x)) < r.$$

Then $r(x) = p(x) - q(x)g(x) \in C$ has degree less than r, which possible only if $r(x) = 0$. Hence $p(x) = q(x)g(x) \in < g(x) >$, and so $C \subset < g(x) >$. Thus $C = < g(x) >$.

(ii) Dividing $x^n - 1$ by $g(x)$ gives

$$x^n - 1 = q(x)g(x) + r(x), \text{ where } \deg(r(x)) < r.$$

Since in $\mathbb{R}_n$, we see that $r(x) \in C$, and so $r(x) = 0$, which
shows that $g(x)|(x^n - 1)$.

(iii) The ideal generated by $g(x)$ is

$$< g(x) >= \{f(x)g(x) : f(x) \in \mathbb{R}_n\}$$

with the usual reduction mod $(x^n - 1)$. Now $f(x)$ divides $x^n - 1$, and so $x^n - 1 = h(x)g(x)$ for some $h(x)$ of degree $n - r$.
Divide $f(x)$ by $h(x)$, we get $f(x) = q(x)h(x) + s(x)$, where $\deg(s(x)) < n - r$, then

$$f(x)g(x) = q(x)g(x)h(x) + s(x)g(x) = q(x)(x^n - 1) + s(x)g(x).$$

So $f(x)g(x) = s(x)g(x) \in C$. Now let $c(x)$ *be* in C, then

$$c(x) = s(x)g(x) = (a_0 + a_1x + a_2x^2 + \ldots + a_{n-r-1}x^{n-r-1})g(x) = (a_0g(x) + a_1xg(x) + \ldots + a_{n-r-1}x^{n-r-1}g(x).$$

So $c(x) \in < \{g(x), xg(x), \ldots, x^{n-r-1}g(x)\} >$, which shows that the set

$$\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\} \text{ spans C.}$$

Also $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ is linearly independent, since if

$$a_0g(x) + a_1xg(x) + \ldots + a_{n-r-1}x^{n-r-1}g(x) = 0,$$

then $(a_0 + a_1x + a_2x^2 + \ldots + a_{n-r-1}x^{n-r-1})g(x) = 0$ which implies that

$$(a_0 + a_1x + a_2x^2 + \ldots + a_{n-r-1}x^{n-r-1}) = 0,$$

and since $1, x, x^2, \ldots, x^{n-r-1}$ are linearly independent, then $a_0 = a_1 = \ldots = a_{n-r-1} = 0$ and hence $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ forms a basis for C.
Hence $\dim(c) = n - r$.

(iv) If $g_0 = 0$ then $g(x) = xg_1(x)$, where $\deg(g_1(x)) < r$ and $g_1(x) = 1.g_1(x) = x^{n-1}g(x)$, *so* $g_1(x) \in C$ which contradict the fact that no nonzero polynomial in C has degree less than r. Thus $g_0 \neq 0$.
Finally, G is a generator matrix of C since $\{g(x), xg(x), \ldots, x^{n-r-1}g(x)\}$ is a basis for C. □

Theorem 1.3.5. *[24] A monic polynomial $p(x)$ in $\mathbb{R}_n$ is the generator polynomial for an ideal $\iff$ $p(x)|(x^n - 1)$.*

Proof. ($\Longrightarrow$) Was proved by the previous theorem.

($\Longleftarrow$) Assume that $p(x)|(x^n - 1)$, let $g(x)$ be the generator polynomial for an ideal C that contains $p(x)$, then

$$p(x) = a(x)g(x), \text{ where } \deg(a(x)) < n - r.$$

By the previous theorem $g(x)|(x^n - 1)$, so $x^n - 1 = g(x)h(x)$, where $h(x)$ is the check polynomial for C. By assumption $x^n - 1 = p(x)h(x)$, for some polynomial $h(x)$. So

$$x^n - 1 = p(x)h(x) = a(x)g(x)h(x) = a(x)(x^n - 1).$$

So $a(x) = 1$ and therefore, $p(x) = g(x)$. □

The Parity Check Matrix

Since the generating polynomial $g(x)$ of a cyclic $[n, n - r]$-code in $\mathbb{R}_n$ divides $x^n - 1$, says $x^n - 1 = g(x)h(x)$, then $h(x)$ is a polynomial of degree $n - r$, called the parity check polynomial of C.

Theorem 1.3.6. *[20] Let $h(x)$ be the check polynomial for a cyclic code C in $\mathbb{R}_n$, then*

(i) The code C can be described by $C = \{p(x) \in \mathbb{R}_n : p(x)h(x) = 0\}$.

(ii) If $h(x) = h_0 + h_1x + h_2x^2 + \ldots + h_{n-r}x^{n-r}$, then the parity check matrix for C is given by

$$H = \begin{bmatrix} h_{n-r} & \dots & \dots & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_{n-r} & \dots & \dots & \dots & h_0 & 0 & \dots & 0 \\ \dots & 0 & h_{n-r} & \dots & \dots & \dots & h_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & h_{n-r} & \dots & \dots & h_0 \end{bmatrix}$$

Example 1.3.2. *Let C be a cyclic code of length $n = 9$. Since $x^9 - 1$ factors over $\mathbb{F}_2$*

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

Hence, there are $2^3 = 8$ cyclic codes in $\mathbb{R}_9 = F_2/ < x^9 - 1 >$. Take $C =< x^6 + x^3 + 1 >$ with generating polynomial $g(x) = x^6 + x^3 + 1$. Then C has dimension $9 - 6 = 3$ and generating matrix

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

Also C has check polynomial $h(x) = \frac{x^9-1}{g(x)} = (x - 1)(x^2 + x + 1) = x^3 - 1$. Then C has the parity check matrix

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

Idempotents For Linear Codes

We note that all cyclic codes can be obtained from factorization of $x^n - 1$ into monic irreducible factors over $\mathbb{F}_q$. However, factoring $x^n - 1$ is not so easy in general. In fact there are other generators that can be found without factoring $x^n - 1$, and they give another approach to describe cyclic codes. These are called idempotent generators.

Definition 1.3.3. [7] A polynomial $e(x) \in \mathbb{R}_n$ is called an idempotent in $\mathbb{R}_n$ if $e^2(x) \equiv e(x)$.

Example 1.3.3. *[24] In $\mathbb{R}_7 = \mathbb{F}_2[x]/ < x^7 - 1 >$, the polynomial $x^3 + x^5 + x^6$ is an idempotent since $(x^3 + x^5 + x^6)^2 = x^3 + x^5 + x^6$.*

Definition 1.3.4. [23] A ring $\mathbb{R}$ is called a Boolean ring if $x^2 = x$ for all $x \in \mathbb{R}$.

Theorem 1.3.7. *[23]If every element in a ring $\mathbb{R}$ is idempotent, then $\mathbb{R}$ is commutative ring.*

Theorem 1.3.8. *[20] Let C be a cyclic code in $\mathbb{R}_n$ with generator polynomial $g(x)$ and check polynomial $h(x)$. Then $g(x)$ and $h(x)$ are relatively prime and so there exist polynomial $a(x)$ and $b(x)$ for which*

$$a(x)g(x) + b(x)h(x) = 1 \quad (*)$$

The polynomial $e(x) = a(x)g(x)$ mod $(x^n - 1)$ has the following properties:

1) $e(x)$ is the unique identity in C, that is

$$p(x)e(x) \equiv p(x) \ \forall p(x) \in C$$

2) $e(x)$ is the unique polynomial in C that is both idempotent and generates C, that is $C =< e(x) >$.

Proof. If $e_1(x)$ and $e_2(x)$ are both identities in $\mathbb{R}$, then

$$e_1(x) \equiv e_1(x)e_2(x) \equiv e_2(x)$$

and so $e_1(x) = e_2(x)$. Thus if an identity exists, then it is unique.
Since $g(x)h(x) = x^n - 1$ has no multiple roots in any extension field, $g(x)$ and $h(x)$ are relatively prime, and so (*) holds. If $p(x) \in C$, then $p(x)h(x) \equiv 0$, see Theorem 1.3.6 and (*) gives

$$a(x)g(x)p(x) \equiv p(x)$$

which says that $e(x) \equiv a(x)g(x)$ $mod(x^n - 1)$ is indeed the identity in C and also that $e(x)$ generates C, since any polynomial in C is a multiple of $e(x)$.
Multiplying (*) by $a(x)g(x)$ gives

$$[a(x)g(x)]^2 + a(x)b(x)g(x)h(x) = a(x)g(x) \text{ and}$$

$$[a(x)g(x)]^2 \equiv a(x)g(x)$$

thus, $e(x)$ is an idempotent.
To complete the proof, need only shows that an idempotent $f(x)$ that also generates C must equal $e(x)$. Since $f(x)$ generates C, there exists $q(x) \in \mathbb{R}_n$ for which $e(x) \equiv q(x)f(x)$. Hence

$$f(x) \equiv e(x)f(x) \equiv q(x)f^2(x) \equiv q(x)f(x) \equiv e(x)$$

which implies that $f(x) = e(x)$. Thus completes the proof. □

Theorem 1.3.9. *[20] The generator polynomial of the code $< e(x) >$ is*

$$g(x) = \gcd(e(x), x^n - 1)$$

Proof. By the previous theorem, since $x^n - 1 = g(x)h(x)$ and $e(x) \equiv a(x)g(x)$, we have

$$\gcd(e(x), x^n - 1) = \gcd(a(x)g(x), h(x)g(x)) = g(x).$$

□

Example 1.3.4. *[24] The following table gives all the cyclic codes C_i of length 7 over $\mathbb{F}_2$ together with their generator polynomials $g_i(x)$ and their generating idempotents $e_i(x)$.*

i	dim	$g_i(x)$	$e_i(x)$
0	0	$1 + x^7$	0
1	1	$1 + x + x^2 + \ldots + x^6$	$1 + x + x^2 + \ldots + x^6$
2	3	$1 + x^2 + x^3 + x^5$	$1 + x^3 + x^5 + x^6$
3	3	$1 + x + x^2 + x^4$	$1 + x + x^2 + x^4$
4	4	$1 + x + x^3$	$x + x^2 + x^4$
5	4	$1 + x^2 + x^3$	$x^3 + x^5 + x^6$
6	6	$1 + x$	$x + x^2 + \ldots + x^6$
7	7	1	1

The two codes of dimension 4 are [7, 4, 3] Hamming codes.

Example 1.3.5. *[24] The following table gives all the cyclic codes C_i of length 11 over $\mathbb{F}_3$ together with their generator polynomials $g_i(x)$ and their generating idempotents $e_i(x)$.*

i	dim	$g_i(x)$	$e_i(x)$
0	0	$1 + x^{11}$	0
1	1	$1 + x + x^2 + \ldots + x^{10}$	$-1 - x - x^2 - \ldots - x^{10}$
2	5	$1 - x - x^2 - x^3 + x^4 + x^6$	$1 + x + x^3 + x^4 + x^5 + x^9$
3	5	$1 + x^2 - x^3 - x^4 - x^5 + x^6$	$1 + x^2 + x^6 + x^7 + x^8 + x^{10}$
4	6	$-1 + x^2 - x^3 + x^4 + x^5$	$-x^2 - x^6 - x^7 - x^8 - x^{10}$
5	6	$-1 - x + x^2 - x^3 + x^5$	$-x - x^3 - x^4 - x^5 - x^9$
6	10	$-1 + x$	$-1 + x + x^2 + \ldots + x^{10}$
7	11	1	1

The two codes of dimension 6 are [11, 6, 5] Hamming codes.

Theorem 1.3.10. *[20] Let C_1 and C_2 be cyclic codes with corresponding generators $g_1(x)$ and $g_2(x)$, and corresponding idempotent generators e_1, e_2, then*

(i) $C_1 \bigcap C_2$ has idempotent $e_1 e_2$

(ii) $C_1 + C_2$ has idempotent $e_1 + e_2 - e_1 e_2$.

Proof. (i) $e_1(x)e_2(x) \in C_1 \bigcap C_2$ and

$$(e_1(x)e_2(x))^2 = (e_1(x))^2(e_2(x))^2 = e_1(x)e_2(x).$$

So $e_1(x)e_2(x)$ is an idempotent in $C_1 \bigcap C_2$.
If $c(x) \in C_1 \bigcap C_2$, then $e_1(x)e_2(x)c(x) = e_1(x)c(x) = c(x)$.
So $e_1(x)e_2(x)$ is an idempotent for $C_1 \bigcap C_2$.

(ii) $e_1(x) + e_2(x) - e_1(x)e_2(x) \in C_1 + C_2$ and it is easy to show that

$$(e_1(x) + e_2(x) - e_1(x)e_2(x))^2 = e_1(x) + e_2(x) - e_1(x)e_2(x).$$

So $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is an idempotent in $C_1 + C_2$.
If $c \in C_1 + C_2$ then $c(x) = c_1(x) + c_2(x)$, for some $c_1(x) \in C_1$ and $c_2(x) \in C_2$.
Hence

$$(c_1(x) + c_2(x))(e_1(x) + e_2(x) - e_1(x)e_2(x)) = c_1(x) + c_2(x).$$

So $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is an idempotent. □

Dual Cyclic Codes

Recall that the dual cyclic code $C^\perp$ of C is $C^\perp = \{\upsilon \in \mathbb{F}_q^n : \upsilon.u = 0, \forall u \in C\}$.

Theorem 1.3.11. *[7] If C is a cyclic code, then $C^\perp$ is also a cyclic code.*

Proof. Let C be a code generated by the word υ, so

$$C =< \{\upsilon, \pi(\upsilon), \ldots, \pi^{n-1}(\upsilon)\} > .$$

Let $u \in C^\perp$, then $\pi^i(\upsilon).u = 0,\ i = 0,\ 1,\ 2,\ \ldots,\ n-1$.
However, this means that $\pi^{i+1}(\upsilon).\pi(u) = 0$ and thus $\pi(u)$ is orthogonal to $< \{\pi(\upsilon), \pi^2(\upsilon), \ldots, \pi^n(\upsilon)\} >= C$.
Since $u \in C^\perp$ implies that $\pi(u) \in C^\perp$, $C^\perp$ is cyclic. □

Theorem 1.3.12. *[7] If C is a linear cyclic code of length n and dimension k with generator polynomial $g(x)$ and if $x^n - 1 = g(x)h(x)$, then $C^\perp$ is a cyclic code of dimension $n-k$ with generator polynomial $g^\perp(x) = x^k h(x^{-1})$ and check polynomial $h^\perp(x) = x^{n-k}g(x^{-1})$.*

Proof. Since C has dimension k, $g(x)$ has degree $n-k$ and thus $h(x)$ has degree k.
Since $g(x)h(x) = x^n - 1$, we have $g(x^{-1})h(x^{-1}) = (x^{-n} - 1)$ and $x^n g(x^{-1})h(x^{-1}) = x^n(x^{-n} - 1)$ so $x^{n-k}g(x^{-1})x^k h(x^{-1}) = x^n - 1$.
Thus $x^k h(x^{-1})$ is a factor of $x^n - 1$, having degree k and hence generator polynomial for a linear cyclic code, $C^\perp$ of dimension $n-k$ containing $x^k h(x^{-1})$. □

Example 1.3.6. *[7] $g(x) = 1 + x + x^3$ is the generator of the cyclic code of length 7 and dimension $k = 7 - 3 = 4$.*
Since $g(x)$ is a factor of $1 + x^7$ we can find $h(x)$ where
$1 + x^7 = g(x)h(x)$ by long division. In this case $h(x) = 1 + x + x^2 + x^4$.
The generator for $C^\perp$ is

$$g^{\perp}(x) = x^4 h(x^{-1}) = x^4(1 + x^{-1} + x^{-2} + x^{-4}) = 1 + x^2 + x^3 + x^4$$

which corresponds to $1011100 = \omega$.
Clearly $g.\omega = (11010000).(1011100) = 0$ *and* $\pi^k(g).\omega = 0$ *as well.*
Note that $g^{\perp}(x) \neq h(x)$.

1.4 Encoding and decoding of cyclic codes

★Encoding With Cyclic Code

There are two rather straightforward ways to encode message strings using a cyclic code one systematic method and one nonsystematic .

The First Way:[24]

Let G be the generator matrix of the cyclic code $C =< g(x) >$, then

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

to encode the message $m \in \mathbb{F}_q^k$ as the codeword $c = mG$. But if we transform $m \in \mathbb{F}_q^k$ to the polynomial $m(x) = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1} \in \mathbb{F}_q[x]$, then to encode $m(x)$ as a codeword $c(x)$ by forming the product $c(x) = m(x)g(x)$. This way is called nonsystematic.

Example 1.4.1. *[24] Let* C *be a binary cyclic code of length* 15 *with generator polynomial* $g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$.
Encode the message $m(x) = 1 + x^2 + x^5$ *using the first encoding procedure(non-systematic encoding)*
$g(x) = 1 + x^4 + x^6 + x^7 + x^8$.
$c(x) = m(x)g(x) = (1 + x^2 + x^5)(1 + x^4 + x^6 + x^7 + x^8) =$
$1 + x^2 + x^4 + x^5 + x^7 + x^{10} + x^{11} + x^{12} + x^{13} \longleftrightarrow (101011010011110)$.

The Second Way:[24]

This way is systematic. The message $m(x)$ associated to the message m is of degree at most $k - 1$ (or is the zero polynomial). The polynomial $x^{n-k}m(x)$

has degree at most $n-1$ and has its first n-k coefficients equal to 0, thus the message is contained in the coefficients of $x^{n-k},\ x^{n-k+1},\ \ldots,\ x^{n-1}$. By the Division Algorithm, $x^{n-k}m(x) = g(x)a(x) + r(x)$, where
$\deg r(x) < n-k$ or $r(x) = 0$.
Let $c(x) = x^{n-k}m(x) - r(x)$, as $c(x)$ is a multiple of $g(x)$, $c(x) \in C$. Also $c(x)$ differs from $x^{n-k}m(x)$ in the coefficients of $1,\ x,\ \ldots,\ x^{n-k-1}$ as $\deg r(x) < n-k$. So $c(x)$ contains the message m in the coefficients of the terms of degree at least $n-k$.

Example 1.4.2. *[24] Let C be a binary cyclic code of length 15 with generator polynomial $g(x) = (1+x+x^4)(1+x+x^2+x^3+x^4)$.*
Encode the message $m(x) = 1+x^2+x^5$ using the second encoding procedure(the first systematic encoding)
$g(x) = 1+x^4+x^6+x^7+x^8$.
$x^{n-k} = x^{15-7} = x^8$.
$x^8m(x) = x^8.(1+x^2+x^5) = x^8+x^{10}+x^{13}$.
Now divide $x^8m(x)$ by $g(x)$.

$$
\begin{array}{r|l}
 & x^5+x^4+x+1 \\
\hline
x^8+x^7+x^6+x^4+1 & x^{13}+\quad\quad\quad+x^{10}+\quad+x^8 \\
 & \underline{x^{13}+x^{12}+x^{11}+\quad\quad+x^9+\quad+x^5} \\
 & x^{12}+x^{11}+x^{10}+x^9+x^8+x^5 \\
 & \underline{x^{12}+x^{11}+x^{10}+\quad\quad+x^8+\quad+x^4} \\
 & x^9+\quad\quad\quad\quad\quad+x^5+x^4 \\
 & \underline{x^9+x^8+x^7+\quad\quad\quad\quad+x^5+\quad+x} \\
 & x^8+x^7+\quad\quad\quad\quad\quad\quad+x^4+x \\
 & \underline{x^8+x^7+x^6+\quad\quad\quad\quad\quad\quad+x^4+1} \\
 & \quad\quad\quad\quad\quad\quad\quad\quad x^6+x+1
\end{array}
$$

$x^8m(x) = g(x).(x^5+x^4+x+1) + (x^6+x+1)$
$C(x) = x^8m(x) + (x^6+x+1) = (x^{13}+x^{10}+x^8) + x^6+x+1$
as a vector $C = (1100001010100 10) \in \mathbb{F}_q^n$

★★*Decoding With Cyclic Code*

Let C be an $[n, k, d]$ cyclic code over $\mathbb{F}_q$ with generator polynomial $g(x)$ of degree $n-k$, C will correct $t = \lfloor (d-1)/2 \rfloor$ errors. Suppose that $c(x) \in C$ is transmitted and y(x) =c(x)+e(x) is recieved, where $e(x) = e_0 + e_1 x + \ldots + e_{n-1}x^{n-1}$ is the error vector with $wt(e(x)) \leq t$.

Definition 1.4.1. [24] For any vector $\nu(x) \in \mathbb{F}_q$, let $R_{g(x)}$ be the unique remainder when $\nu(x)$ is divided by $g(x)$ according to Division Algorithm, that is, $R_{g(x)}(\nu(x)) = r(x)$, where

$$\nu(x) = g(x)f(x) + r(x), \quad with \quad r(x) = 0 \quad or \quad degr(x) < n-k.$$

The function $R_{g(x)}$ satisfies the following properties.

Theorem 1.4.1. *[24] With the preceding notation the following hold:*

(i) $R_{g(x)}(a\nu(x) + b\nu^{'}(x)) = aR_{g(x)}(\nu(x)) + bR_{g(x)}(\nu^{'}(x))$ *for all* $\nu(x),\ \nu^{'}(x) \in \mathbb{F}_q[x]$ *and all* $a, b \in \mathbb{F}_q$.

(ii) $R_{g(x)}(\nu(x) + a(x)(x^n - 1)) = R_{g(x)}(\nu(x))$.

(iii) $R_{g(x)}(\nu(x) = 0$ *if and only if* $\nu(x) \mod (x^n - 1) \in C$.

(iv) If $c(x) \in C$, *then* $R_{g(x)}(c(x) + e(x)) = R_{g(x)}(e(x))$.

(v) If $R_{g(x)}(e(x)) = R_{g(x)}(e^{'}(x))$, *where* $e(x)$ *and* $e^{'}(x)$ *each have weight at most* t, *then* $e(x) = e^{'}(x)$.

(vi) $R_{g(x)}(\nu(x)) = \nu(x)$ *if* $\deg \nu(x) < n-k$. □

Theorem 1.4.2. *[24] Let* $g(x)$ *be a monic divisor of* $x^n - 1$ *of degree* $n-k$. *If* $R_{g(x)}(\nu(x)) = s(x)$, *then*
$R_{g(x)}(x\nu(x) \mod (x^n - 1)) = R_{g(x)}(xs(x)) = xs(x) - g(x)s_{n-k-1}$, *where* s_{n-k-1} *is the coefficient of* x^{n-k-1} *in* $s(x)$. □

The first version of the Meggitt decoding algorithm. The syndrome polynomial $S(\nu(x))$ of any $\nu(x)$ to be $S(\nu(x)) = R_{g(x)}(x^{n-k}\nu(x))$.

step I:

We find all the syndrome polynomials $S(e(x))$ of error patterns $e(x) = \sum_{i=0}^{n-1} e_i x^i$ such that $wt(e(x)) \leq t$ and $e_{n-1} \neq 0$.

Example 1.4.3. *[24] Let C be the $[15, 7, 5]$ binary cyclic code with defining set $T = \{1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12\}$. Let α be a 15th root of unity in $\mathbb{F}_{16}$. Then $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ is the generator polynomial of C and the syndrome polynomial of $e(x)$ is $S(e(x)) = R_{g(x)}(x^8 e(x))$. Step I produces the following syndrome polynomial:*

$e(x)$	$S(e(x))$	$e(x)$	$S(e(x))$
x^{14}	x^7	$x^6 + x^{14}$	$x^3 + x^5 + x^6$
$x^{13} + x^{14}$	$x^6 + x^7$	$x^5 + x^{14}$	$x^2 + x^4 + x^5 + x^6 + x^7$
$x^{12} + x^{14}$	$x^5 + x^7$	$x^4 + x^{14}$	$x + x^3 + x^4 + x^5 + x^7$
$x^{11} + x^{14}$	$x^4 + x^7$	$x^3 + x^{14}$	$1 + x^2 + x^3 + x^4 + x^7$
$x^{10} + x^{14}$	$x^3 + x^7$	$x^2 + x^{14}$	$x + x^2 + x^5 + x^6$
$x^9 + x^{14}$	$x^2 + x^7$	$x + x^{14}$	$1 + x + x^4 + x^5 + x^6 + x^7$
$x^8 + x^{14}$	$x + x^7$	$1 + x^{14}$	$1 + x^4 + x^6$
$x^7 + x^{14}$	$1 + x^7$		

The computation of these syndrome polynomials were aided by Theorem 1.4.1 and 1.4.2. For example, in computing the syndrome polynomial of $x^{12} + x^{14}$, we have
$S(x^{12} + x^{14}) = R_{g(x)}(x^8(x^{12} + x^{14})) = R_{g(x)}(x^5 + x^7) = x^5 + x^7$ using Theorem 1.4.1(vi). In computing the syndrome polynomial for $1 + x^{14}$, first observe that $R_{g(x)}(x^8) = 1 + x^4 + x^6 + x^7$, then
$S(1 + x^{14}) = R_{g(x)}(x^8(1 + x^{14})) = R_{g(x)}(x^8) + R_{g(x)}(x^7) = 1 + x^4 + x^6$.
We see by Theorem 1.4.1 that
$R_{g(x)}(x^9) = R_{g(x)}(xx^8) = R_{g(x)}(x + x^5 + x^7) + R_{g(x)}(x^8) =$
$x + x^5 + x^7 + 1 + x^4 + x^6 + x^7 = 1 + x + x^4 + x^5 + x^6$.
Therefore in computing the syndrome polynomial for $x + x^{14}$, we have
$S(x+x^{14}) = R_{g(x)}(x^8(x+x^{14})) = R_{g(x)}(x^9)+R_{g(x)}(x^7) = 1+x+x^4+x^5+x^6+x^7$.
The others follow similarly.

Step II:

Suppose that $y(x)$ is the received vector. Compute the syndrome polynomial $S(y(x)) = R_{g(x)}(x^{n-k}y(x))$. By Theorem 1.4.1$(iv)$, $S(y(x)) = S(e(x))$, where $y(x) = c(x) + e(x)$ with $c(x) \in C$.

Example 1.4.4. *[24] Suppose that* $y(x) = 1 + x^4 + x^7 + x^9 + x^{10} + x^{12}$ *is received.*

Then $S(y(x)) = x + x^2 + x^6 + x^7$.

Step III:

If $S(y(x))$ is in the list computed in the Step I, then we know the error polynomial $e(x)$ and this can be subtracted from $y(x)$ to the corrected codeword $c(x) = y(x) - e(x)$. If $S(y(x))$ is not the list, go on to Step IV.

Step IV:

Compute the syndrome polynomial of $xy(x)$, $x^2y(x)$, ... in succession until the syndrome polynomial is in the list from Step I. If $S(x^iy(x))$ is in this list and is associated with the error polynomial $e^{'}(x)$, then the received vector is decoded as $y(x) - x^{n-i}e^{'}(x)$.

The computation in Step IV is most easily carried out using Theorem 1.4.2

As $R_{g(x)}(x^{n-k}y(x)) = S(y(x)) = \sum_{i=0}^{n-k-1} s_i x^i$, $S(xy(x)) = R_{g(x)}(x^{n-k}xy(x)) = R_{g(x)}(x(x^{n-k}y(x))) = R_{g(x)}(xS(y(x))) = xS(y(x)) - s_{n-k-1}g(x)$.

Example 1.4.5. *[24] Continuing with Example* 1.4.4*, we have*
$S(y(x)) = x + x^2 + x^6 + x^7$, *that*
$S(xy(x)) = x(x + x^2 + x^6 + x^7) - 1.g(x) = 1 + x^2 + x^3 + x^4 + x^6$, *which is not in the list in Example* 1.4.3
$S(x^2y(x)) = x(1 + x^2 + x^3 + x^4 + x^6) - 0.g(x) = x + x^3 + x^4 + x^5 + x^7$, *which corresponds to the error* $x^4 + x^{14}$ *implying that* $y(x)$ *is decoded as*
$y(x) - (x^2 + x^{12}) = 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$.

Definition 1.4.2. [7] A code C of length n and odd distance $d = 2t + 1$ is called **a perfect code** if

$$|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+...+\binom{n}{t}}.$$

Example 1.4.6. *[7] Let* $n = 7$ *and* $d = 3$, *then* $t = 1$ *and*

$$|C| = \frac{2^7}{\binom{7}{0}+\binom{7}{1}} = \frac{128}{8} = 2^4.$$

Thus, there may exist a linear perfect code with $n = 7$ and $d = 3$. (Hamming codes)

Hamming codes

The family of Hamming codes $H_q(r)$ is probably the most famous of all error-correcting codes. These codes were discovered independently by Marcel in 1949 and Richard Hamming in 1950. In addition, all binary Hamming codes are equivalent to cyclic codes, and some, but not all, non-binary Hamming codes are equivalent to cyclic codes.

Definition 1.4.3. [19] Let $r \geq 2$. A binary linear code of length $n = 2^r - 1$, with parity-check matrix H whose columns consist of all the nonzero vectors of $\mathbb{F}_2^r$ is called a binary Hamming code of length $2^r - 1$. It is denoted by $H_2(r)$.

Example 1.4.7. *[19] $H_2(3)$: A Hamming code of length 7 with parity-check matrix*

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

Properties of the binary Hamming codes:-

(i) All the binary Hamming codes of a given length are equivalent.

(ii) The dimension of $H_2(r)$ is $k = 2^r - 1 - r$.

(iii) The distance of $H_2(r)$ is $d = 3$, hence $H_2(r)$ is exactly single error-correcting.

(iv) Binary Hamming codes are perfect codes.

1.5 About Galois ring

In this section we want to investigate the fundamental properties of Galois rings. We define,

$$GR(p^n, r) = \mathbb{Z}_{p^n}[\xi] = \mathbb{Z}_{p^n}[x]/(G_{(p,r)}(x)),$$

where ξ is a formal root of the monic, basic irreducible polynomial $G_{(p,r)}(x) \in \mathbb{Z}_{p^n}[x]$, determined by the integral version of Hansel Lemma from a primitive polynomial $g_{(p,r)}(x) \in \mathbb{Z}_p[x]$ of degree r, such that

$$\mathbb{F}_{p^r} = GF(p^r) = \mathbb{F}_p[x]/(g_{(p,r)}(x)) \cong \mathbb{Z}(\theta),$$

with $g_{(p,r)}(\theta) = 0$ and $g_{(p,r)}(x) \equiv G_{(p,r)}(x)(\mod p)$. Thus, the polynomial $G_{(p,r)}(x)$ is linked to $g_{(p,r)}(x)$ by the epimorphism

$$\mu : \mathbb{Z}_{p^n}[x] \longrightarrow \mathbb{Z}_p[x],$$

i.e. $\mu(G_{(p,r)}(x)) = g_{(p,r)}(x) \in \mathbb{Z}_p[x]$.

If $g_{(p,r)}(x) \in \mathbb{Z}_p[x]$ is monic, irreducible of the form

$$g_{(p,r)}(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_0.$$

Indeed, in such a case, we have

$$G_{(p,r)}(x) = x^r + (p^n - p + a_{r-1})x^{r-1} + \ldots + (p^n - p + a_0) \in \mathbb{Z}_{p^n}[x].$$

$GR(p^n, r) = \{\sum_{j=0}^{r-1} b_j \xi^j \mid b_j \in \mathbb{Z}_{p^n}, 0 \leq j \leq r-1\}$, with $GR(p,r)(\xi) = 0$.

This ring is a finite, local ring (its cardinality is $(p^n)^r = p^{nr}$), with maximal ideal $pGR(p^n, r)$ and residue field given by $GR(p^n, r)/pGR(p^n, r) \cong \mathbb{F}_{p^r}$.

Note that the elements in the maximal ideal can be uniquely written as $pGR(p^n, r) = \{p\sum_{j=0}^{r-1} b_j \xi^j \mid b_j \in \mathbb{Z}_{p^n}, 0 \leq j \leq r-1\}$, with $GR(p,r)(\xi) = 0$.

more precisely,

$$pGR(p^n, r) = \{\sum_{j=0}^{r-1} b_j \xi^j \mid b_j \in p\mathbb{Z}_{p^n}, 0 \leq j \leq r-1\},$$

where $GR(p,r)(\xi) = 0$ and where $p\mathbb{Z}_{p^n} \subset \mathbb{Z}_{p^n}$ is the maximal ideal of the local ring of the integers mod p^n.

Therefore, $pGR(p^n, r)$ has cardinality equal to $(p^{(n-1)^r}) = p^{r(n-1)}$.

Example 1.5.1. *[9] Take the ring $\mathbb{Z}_8$. In this situation, $p = 2$ and $n = 3$, and assume $r = 3$. Recall that*

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3 + x + 1) = \{a + b\xi + c\xi^2 \mid a,\ b,\ c \in \mathbb{F}_2\},$$

where $\xi^3 = \xi + 1$, i.e.

$$\mathbb{F}_8 = \{0, 1, \xi, \xi^2, 1 + \xi, 1 + \xi^2, \xi + \xi^2, 1 + \xi + \xi^2\}.$$

The polynomial $g_{(2,3)}(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ is the primitive polynomial used for the field extension $\mathbb{F}_2 \subset \mathbb{F}_8$. By Hensels Lemma,

$$G_{(2,3)} = x^3 + (8-2+0)x^2 + (8-2+1)x + (8-2+1) = x^3 + 6x^2 + 7x + 7 \in \mathbb{Z}_8[x].$$

This monic, basic irreducible polynomial determines a proper ideal in $\mathbb{Z}_8[x]$. *We now describe the ring* $GR(2^3, 3)$ *as*

$$G_{(2,3)} = \{b_0 + b_1\xi + b_2\xi^2 \mid b_i \in \mathbb{Z}_8\},$$

where ξ *is a formal root of* $G_{(2,3)}(x) \in \mathbb{Z}_8$, *i.e.* $\xi^3 = 2\xi^2 + \xi + 1$, *therefore,* $|G_{(2,3)}| = 8^3 = 512$. *The maximal ideal* M *in* $\mathbb{Z}_8$ *is* $2\mathbb{Z}_8 = \{0, 2, 4, 6\}$.
We have the following define

$$0 \longrightarrow M \longrightarrow \mathbb{Z}_8 \xrightarrow{\pi} \mathbb{Z}_2 \longrightarrow 0.$$

The epimorphism π *extends to the polynomial ring morphism* μ *from* $\mathbb{Z}_8[x]$ *to* $\mathbb{Z}_2[x]$. *The ideal* $(M, x^3 + 6x^2 + 7x + 7) \subset \mathbb{Z}_8[x]$ *is a proper ideal and*

$$\mathbb{Z}_8/(M, x^3 + 6x^2 + 7x + 7) \cong \mathbb{Z}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_8,$$

since $\mu(x^3 + 6x^2 + 7x + 7) = x^3 + x + 1$.
Next, consider the induced map

$$\tilde{\mu} : GR(8, 3) \cong \mathbb{Z}_8[x]/(x^3 + 6x^2 + 7x + 7) \longrightarrow \mathbb{Z}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_8.$$

The elements of this kernel are of the form

$$2GR(8, 3) = \{2(b_0 + b_1\xi + b_2\xi^2) \,:\, b_0,\ b_1,\ b_2 \in \mathbb{Z}_8\},$$

with $\xi^3 = 2\xi^2 + \xi + 1$.
Clearly,

$$|2GR(8, 3)| = 4^3 = 64,$$

since the coefficients $2b_0, 2b_1, 2b_2 \in M = 2\mathbb{Z}_8$.
Therefore, we can write $2GR(8, 3) = \{\lambda_0 + \lambda_1\xi + \lambda_2\xi^2 | \lambda_i \in M, 0 \leq i \leq 2\}$, *again with* $\xi^3 = 2\xi^2 + \xi + 1$.

Remark 1.5.1. [9]

★ $GR(p^n, r)$ for each prime p and any positive integers $n,\ r$ is a finite, commutative, local ring with maximal ideal $pGR(p^n, r)$. This also implies that such a ring is *principal*, since each ideal is of the form

$$I_k = p^k GR(p^n, r),\ 1 \leq k \leq n - 1.$$

The ideals in the ring $\mathbb{Z}_{p^n}$ form the chain

$$p\mathbb{Z}_{p^n} \supset p^2\mathbb{Z}_{p^n} \supset \ldots \supset p^{n-1}\mathbb{Z}_{p^n} \supset (0).$$

Chapter 2

Cyclic Codes Over Rings Of Four Elements

2.1 Background

In this chapter we study cyclic codes over the rings $\mathbb{Z}_4$ of integers modulo 4 and $\mathbb{F}_2 + u\mathbb{F}_2$. The theory of these codes is compared and contrasted with the theory of linear codes over fields.

$\mathbb{Z}_4$ is a ring which has 2 as a zero divisor. A set of n-tuple over $\mathbb{Z}_4$ is called a code over $\mathbb{Z}_4$ or a $\mathbb{Z}_4$ code if it is a $\mathbb{Z}_4$ module. In this chapter we study that any $\mathbb{Z}_4$-cyclic code C has generators of the form $< fh, 2fg >$ where $fgh = x^n - 1$ over $\mathbb{Z}_4$, and $\mid C \mid = 4^{degg} 2^{degh}$ and also $C^{\perp}$ has generators of the form $< g^*h^*, 2f^*g^* >$, where g^*, h^* and f^* are the reciprocal polynomials of g, h, and f respectively, see page 46.

The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is a commutative chain ring of 4 elements which are

$$\{0, 1, u, \overline{u} = u + 1\} \text{ with } u^2 = 0.$$

Addition and the multiplication operations in the ring $\mathbb{F}_2 + u\mathbb{F}_2$ are given as in the following tables:

+	0	1	u	$\overline{u}$
0	0	1	u	$\overline{u}$
1	1	0	$\overline{u}$	u
u	u	$\overline{u}$	0	1
$\overline{u}$	$\overline{u}$	u	1	0

.	0	1	u	$\overline{u}$
0	0	0	0	0
1	0	1	u	$\overline{u}$
u	0	u	0	u
$\overline{u}$	0	$\overline{u}$	u	1

The ring $\mathbb{F}_2+u\mathbb{F}_2$ shares some properties of both $\mathbb{Z}_4$ and $\mathbb{F}_4$. The multiplication table coincides with that of $\mathbb{Z}_4$, when $1+u$ and u are replaced by respectively 3 and 2. However, the addition table is different. The addition table is similar to that of the Galois field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$, when u and $1 + u$ are replaced respectively by α and α^2. From the definition of ring $\mathbb{F}_2 + u\mathbb{F}_2$, the characteristic is equal 2. So in the structure of alphabets, $\mathbb{F}_2 + u\mathbb{F}_2$ lies in 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 $\mathbb{F}_2 + u\mathbb{F}_2$ and the subspace $\{0, 1\} = \mathbb{F}_2$ is a subring.

2.2 Cyclic Codes Over $\mathbb{Z}_4$

As with cyclic codes over a field, cyclic codes over $\mathbb{Z}_4$ form an important family of $\mathbb{Z}_4$-linear codes. A body of theory has been developed to handle these codes with obvious parallels to the theory of cyclic codes over fields. As with usual cyclic codes over $\mathbb{F}_q$, we view codewords $\mathbf{c} = c_0c_1 \dots c_{n-1}$ in a cyclic $\mathbb{Z}_4$-linear code of length n as polynomial $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \in \mathbb{Z}_4[x]$. If we consider our polynomials as elements of the quotient ring

$$\mathfrak{R}_n = \mathbb{Z}_4[x]/ < x^n - 1 >,$$

has been fully studied in [4] then $xc(x)$ modulo $x^n - 1$ represents the cyclic shift of $c(x)$.

When studying cyclic codes over $\mathbb{F}_q$, we found generator polynomials and generating dual of these codes.

Let $\mu : \mathbb{Z}_4[x] \longrightarrow \mathbb{Z}_2[x]$ be the map which sends 0, 2 to 0; 1, 3 to 1 and x to x.

Definition 2.2.1. [24] A polynomial $f(x) \in \mathbb{Z}_4[x]$ is irreducible in $\mathbb{Z}_4$ if whenever $f(x) = g(x)h(x)$ for two polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}_4[x]$, one of $g(x)$ *or* $h(x)$ is a unit.

Definition 2.2.2. [24] A polynomial $f \in \mathbb{Z}_4[x]$ is basic irreducible if its $\mu(f)$ is irreducible in $\mathbb{Z}_2[x]$.

Definition 2.2.3. [24] An ideal I of a ring $\mathbb{Z}_4$ is called a primary ideal provided $ab \in I$ implies that either $a \in I$ or $b^r \in I$ for some positive integer r.

Definition 2.2.4. [24] A polynomial $f(x) \in \mathbb{Z}_4[x]$ is primary if the principal ideal
$< f(x) >= \{f(x)g(x),\ g(x) \in \mathbb{Z}_4[x]\}$ is primary ideal.

Lemma 2.2.1. *[24] If $f(x)$ is a basic irreducible polynomial, then $f(x)$ is primary or* ***"semiprime"****.*

Proof. Suppose $g(x)h(x) \in < f(x) >$. Since $\mu f(x)$ is irreducible,

$$d = \gcd(\mu g(x), \mu f(x)) \text{ is either 1 or } \mu f(x).$$

If $d = 1$, then by definition 1.1.24 there exist polynomials $a(x)$ and $b(x)$ in $\mathbb{Z}_4[x]$ such that $\mu(a(x))\mu(g(x)) + \mu(b(x))\mu(f(x)) = 1$.
Hence $a(x)g(x) + b(x)f(x) = 1 + 2s(x)$ for some $s(x) \in \mathbb{Z}_4[x]$. Therefore

$$a(x)g(x)h(x)(1+2s(x)) + b(x)f(x)h(x)(1+2s(x)) = h(x)(1+2s(x))^2 = h(x),$$

implying that $h(x) \in < f(x) >$.
Suppose now that $d = \mu(f(x))$. Then there exists $a(x) \in \mathbb{Z}_4[x]$ such that $\mu(g(x)) = \mu(f(x))\mu(a(x))$, implying that

$$g(x) = f(x)a(x) + 2s(x) \text{ for some } s(x) \in \mathbb{Z}_4[x].$$

Hence $g(x)^2 = (f(x)a(x))^2 \in < f(x) >$. Thus $f(x)$ is a semiprime polynomial. □

If $R = \mathbb{Z}_4[x]$ *or* $\mathbb{F}_2[x]$, then two polynomials $f(x)$ and $g(x)$ in R are called coprime, or relatively prime provided that

$$R =< f > + < g > .$$

Lemma 2.2.2. *[24] Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}_4[x]$. Then $f(x)$ and $g(x)$ are coprime if and only if $\mu(f(x))$ and $\mu(g(x))$ are coprime polynomials in $\mathbb{F}_2[x]$.*

Proof. If $f(x)$ and $g(x)$ are coprime, then

$$a(x)f(x) + b(x)g(x) = 1 \text{ for some } a(x) \text{ and } b(x) \text{ in } \mathbb{Z}_4[x].$$

Then $\mu(a(x))\mu(f(x)) + \mu(b(x))\mu(g(x)) = \mu(1) = 1$, implying that
$\mu(f(x))$ and $\mu(g(x))$ are coprime.

Conversely, suppose that $\mu(f(x))$ and $\mu(g(x))$ are coprime. Then there exist $a(x)$ *and* $b(x)$ in $\mathbb{Z}_4[x]$ such that $\mu(a(x))\mu(f(x)) + \mu(b(x))\mu(g(x)) = 1$.
Thus $a(x)f(x) + b(x)g(x) = 1 + 2s(x)$ for some $s(x) \in \mathbb{Z}_4[x]$. But then

$$a(x)(1+2s(x))f(x) + b(x)(1+2s(x))g(x) = (1+2s(x))^2 = 1$$

showing that $f(x)$ and $g(x)$ are coprime.

□

We introduce, without proof, another method that will produce the factorization; this method is due to Graeffe [24] but was adapted to $\mathbb{Z}_4$-linear codes:

i) Let $h(x)$ be an irreducible factor of $x^n + 1$ in $\mathbb{F}_2[x]$. Write $h(x) = e(x) + o(x)$, where $e(x)$ is the sum of the terms of $h(x)$ with even exponents and $o(x)$ is the sum of the terms of $h(x)$ with odd exponents.

ii) Then $g(x)$ is the irreducible factor of $x^n - 1$ in $\mathbb{Z}_4[x]$ with $\mu(g(x)) = h(x)$, where $g(x^2) = \pm(e(x)^2 - o(x)^2)$.

Example 2.2.1. *[24] In* $\mathbb{F}_2[x]$, $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ *is the factorization of* $x^7 + 1$ *into irreducible polynomials. We apply Graffes method to each factor to obtain the factorization of* $x^7 - 1$ *into monic irreducible polynomials of* $\mathbb{Z}_4[x]$.

- *If* $h(x) = x+1$, *then* $e(x) = 1$ *and* $o(x) = x$. *So* $g(x^2) = -(1-x^2) = x^2-1$ *and thus* $g(x) = x - 1$.
- *If* $h(x) = x^3 + x + 1$, *then* $e(x) = 1$ *and* $o(x) = x^3 + x$. *So* $g(x^2) = -(1 - (x^3 + x)^2) = x^6 + 2x^4 + x^2 - 1$ *and thus* $g(x) = x^3 + 2x^2 + x - 1$.
- *If* $h(x) = x^3 + x^2 + 1$, *then* $e(x) = x^2 + 1$ *and* $o(x) = x^3$. *So* $g(x^2) = -((x^2+1)^2 - (x^3)^2) = x^6 - x^4 + 2x^2 - 1$ *and thus* $g(x) = x^3 - x^2 + 2x - 1$. *Therefore* $x^7 - 1 = (x - 1)(x^3 + 2x^2 + x - 1)(x^3 - x^2 + 2x - 1)$ *is the factorization of* $x^7 - 1$ *into monic irreducible polynomials in* $\mathbb{Z}_4[x]$.

If $\mathbb{R}$ is a local ring, the polynomial ring $\mathbb{R}[x]$ may not be a unique factorization domain. But some special polynomials in $\mathbb{R}[x]$ may have the unique factorization domain property. An example of such polynomials are regular polynomials. A regular polynomial is a polynomial which is not a zero divisor in $\mathbb{R}[x]$.

In our case the local ring in $\mathbb{Z}_4$ and any polynomial which has some nonzero coefficient not equal to 2 is regular. In particular, $x^n - 1$ is regular. By Hansel Lemma, $x^n - 1$ is the product of basic irreducible polynomials and such polynomials are primary by Lemma 2.2.1. Hence by factorization theorem, we immediately get the following.

Lemma 2.2.3. *[24] If $x^n - 1 = f_1 f_2 \dots f_r$, where the f_i are basic irreducible and pairwise-coprime polynomials, then this factorization is unique.*

To study cyclic codes over $\mathbb{F}_q$ we need to find the ideals of $\mathbb{F}_q / < x^n - 1 >$. Similarly, we need to find the ideals of $\mathfrak{R}_n$ in order to study cyclic codes over $\mathbb{Z}_4$. We first need to know the ideal structure of $\mathbb{Z}_4 / < f(x) >$, where $f(x)$ is a basic irreducible polynomial.

Lemma 2.2.4. *[22] If $f(x)$ is in $\mathbb{Z}_4$ and is basic irreducible, then the only ideals of $\mathbb{Z}_4 / < f(x) >$ are $< 0 >$, $< 1 >$ and $< 2 >$.*

Proof. Suppose I is a nonzero ideal of the ring $\mathbb{Z}_4[x] / < f(x) >$ and $g(x) + < f(x) >$ is in I for some $g(x)$ which is not belong $< f(x) >$. Since

$$\gcd(\mu g(x), \mu f(x)) = 1 \text{ or } \mu f(x),$$

$g(x) + < f(x) >$ is either invertible in the ring $\mathbb{Z}_4[x] / < f(x) >$ or is an element of $(2 + < f(x) >)$. If $g(x) + < f(x) >$ is invertible, then

$$I = \mathbb{Z}_4[x] / < f(x) >.$$

Otherwise,

$$I \subseteq (2 + < f(x) >).$$

In this case there is an element $(2r(x) + < f(x) >) \neq 0 \in I$. We can suppose $\mu r(x)$ which is not belong $(\mu f(x))$, since otherwise there are $u(x)$, $v(x)$ in $\mathbb{Z}_4[x]$ such that

$$r(x) = f(x)u(x) + 2v(x).$$

Then $2r(x) = 2f(x)u(x)$, which implies $2r(x) + (f(x)) = 0$ in the ring $\mathbb{Z}_4 / < f(x) >$. So, if $\mu r(x)$ is not in $(\mu f(x))$, then

$$\gcd(\mu r(x), \mu f(x)) = 1.$$

Hence there are $u(x)$, $v(x)$ and $w(x)$ in $\mathbb{Z}_4[x]$ such that

$$r(x)u(x) + f(x)v(x) = 1 + 2w(x).$$

Therefore,

$$2r(x)u(x) + 2f(x)v(x) = 2,$$

i.e, $2 + < f(x) >$ is in I because it is an ideal. Hence $I = (2 + < f(x) >)$. □

Let $\mathfrak{R}_n = \mathbb{Z}_4[x]/ < x^n - 1 >$. As usual, if C is a $\mathbb{Z}_4$ cyclic code of length n, an element $c = (a_0, a_1, \ldots, a_{n-1})$ in C is identified with a polynomial $a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ modulo $x^n - 1$. under this correspondence, a code is $\mathbb{Z}_4$ cyclic if and only if it is an ideal in the ring $\mathfrak{R}_n$.

Theorem 2.2.5. *[22] Let $x^n - 1 = f_1 f_2 \ldots f_r$, be a product of basic irreducible and pairwise-coprime polynomials for odd n, and let $\hat{f}_i$ denote the product of all f_j except f_i. Then any ideal in the ring $\mathfrak{R}_n$ is a sum of ideal $< \hat{f}_i >$ and $< 2\hat{f}_j >$.*

Proof. By Hansels Lemma 1.1.26, such a factorization of $x^n - 1$ exists and is unique.
Since the f_i are basic irreducible and pairwise coprime we have

$x^n - 1 =< f_1 > \bigcap < f_2 > \bigcap < f_3 > \bigcap \ldots \bigcap < f_r >$, and for $1 \leq i, j \leq r, i \neq j$

$$\mathbb{Z}_4[x] =< f_i > + < f_j > .$$

Thus by Chinese Remainder Theorem 1.1.20

$\mathfrak{R}_n = \mathbb{Z}_4[x]/ < f_1 > \bigcap < f_2 > \bigcap < f_3 > \bigcap \ldots \bigcap < f_r >$
$\cong \oplus \sum_{i=1}^{r} \mathbb{Z}_4[x]/ < f_i >$.
Consequently, if I is an ideal of $\mathfrak{R}_n$, then

$$I \cong I_1 \oplus I_2 \oplus \ldots \oplus I_r,$$

where I_i is an ideal of the ring $\mathbb{Z}_4[x]/ < f_i >$, for $i = 1, 2, \ldots, r$.
By Lemma 2.2.5,

$$I_i = 0,\ \mathbb{Z}_4[x]/ < f_i >\ \ or\ (2+ < f_i >).$$

If $I_i = \mathbb{Z}_4[x]/ < f_i >$, then it corresponds to the ideal $(\hat{f}_i)$ in the ring $\mathfrak{R}_n$, if $I_i = (2+ < f_i >)$, then it corresponds to the ideal $< 2\hat{f}_j >$. In any case, the ideal I is a sum of $< \hat{f}_i >$ and $< 2\hat{f}_j >$.

□

Theorem 2.2.6. *[22] Suppose C is a $\mathbb{Z}_4$-cyclic code of odd length n. Then there exist are unique monic polynomials f, g and h such that $x^n - 1 = fgh$ and $C =< fh > \oplus < 2fg >$. Furthermore, C has type $4^{degg}2^{degh}$.*
When $h = 1$, $C =< f >$ and $|C| = 4^{n-degf}$.
When $g = 1$, $C =< 2f >$ and $|C| = 2^{n-degf}$.

Proof. We know that $x^n - 1$ has a unique factorization such that $x^n - 1 = f_1 f_2 \ldots f_r$, where the f_i are basic irreducible and pairwise coprime, We also know, by theorem 2.2.5, that C is a sum of $< \hat{f}_i >$ and $< 2\hat{f}_j >$. By permuting the subscripts of f_i, we can suppose that C is a sum of

$$< \hat{f}_{k+1} >, < \hat{f}_{k+2} >, \ldots, < \hat{f}_{k+l} >, < 2\hat{f}_{k+l+1} >, < 2\hat{f}_{k+l+2} >, \ldots, < 2\hat{f}_r > .$$

Then

$$C =< f_1 f_2 \ldots f_k f_{k+l+1} f_{k+l+2} \ldots f_r, 2f_1 f_2 \ldots f_k f_{k+1} \ldots f_{k+l} >=< fh, 2fg >,$$

where

$$f = f_1 f_2 \ldots f_k,\ g = f_{k+1} f_{k+2} \ldots f_{k+l} \text{ or } 1 \text{ if } l = 0$$

and

$$h = f_{k+l+1} f_{k+l+2} \ldots f_r \text{ or } 1 \text{ if } k + l = r.$$

When $h \neq 1$, fh and g are coprime, $< fh > \bigcap < 2fg >= 0$. Therefore

$$|C| = |fh||2fg| = 4^{n-ged(f)-deg(h)} 2^{n-deg(f)-deg(g)}.$$

When $h = 1$, the above identity is still true because in this case $C =< f >$ and

$$|C| = |fh||2fg| = 4^{n-ged(f)-deg(h)} 2^{n-ged(f)-deg(g)} = 4^{n-ged(f)}.$$

When $g = 1$, the above identity is still true because in this case $C =< 2f >$ and

$$|C| = |fh||2fg| = 4^{n-ged(f)-deg(h)} 2^{n-ged(f)-deg(g)} = 2^{n-ged(f)}.$$

□

The following corollary is also in [24]

Corollary 2.2.7. *Let n be odd. Assume $x^n - 1$ is a product of k irreducible polynomial in $\mathbb{Z}_4[x]$. Then there are $(3)^k$ cyclic codes over $\mathbb{Z}_4$ of length n.*

Proof. Let $x^n - 1 = g_1(x)g_2(x)\ldots g_k(x)$ be the factorization of $x^n - 1$ into monic irreducible polynomials. If C is a cyclic code, by theorem 2.2.6,

$$C =< f(x)g(x) > \oplus < 2f(x)h(x) > \text{ where } x^n - 1 = f(x)g(x)h(x).$$

Each $g_i(x)$ is a factor of exactly one of $f(x),\ g(x),\ or\ h(x)$. □

Example 2.2.2. *[24] By Example 2.2.1, $x^7 - 1 = g_1(x)g_2(x)g_3(x)$, where $g_1(x) = (x-1)$, $g_2(x) = (x^3 + 2x^2 + x - 1)$, and $g_3(x) = (x^3 - x^2 + 2x - 1)$ are the monic irreducible factors of $x^7 - 1$. By Corollary 2.2.7, there are $3^3 = 27$ cyclic codes over $\mathbb{Z}_4$ of length 7. In table 2.1 we give the generator polynomials of the 25 nontrivial cyclic codes of length 7 as described in Theorem 2.2.6.*

If $C =< f(x)h(x) > \oplus < 2f(x)g(x) >$, as in Theorem 2.2.6, we can easy write down a generator matrix G for C.

Example 2.2.3. *[24] Consider $C =< g_1g_3, 2g_2 >$ in table 2.1.*
Since $g_1(x)g_3(x) = 1 + x + 3x^2 + 2x^3 + x^4$ and $2g_2(x) = 2 + 2x + 2x^3$, then the generator matrix for this code is

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

Let $f(x) = a_dx^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}_4[x]$, with $a_d \neq 0$, define the **reciprocal polynomial** f^* to be

$$f^* = \pm x^d f(x^{-1}) = \pm(a_0x^d + a_1x^{d-1} + \ldots + a_d)$$

The following theorem can be found in [24].

Theorem 2.2.8. *Let*

$$a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

and

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

then $a(x)b^*(x) = 0$ in $\mathfrak{R}_n$ if and only if the vector $(a_0, a_1, \ldots, a_{n-1})$ is orthogonal to the vector $(b_{n-1}, b_{n-2}, \ldots, b_0)$ and all its cyclic shifts.

The next theorem discusses the dual of C

Theorem 2.2.9. *[22] Let $C =< fh, 2fg >$ is a $\mathbb{Z}_4$-cyclic code of odd length n, where f, g and h are monic polynomials and such that $fgh = x^n - 1$ and $|C| = 4^{deg(g)}2^{deg(h)}$. Then*

$$C^{\perp} =< g^*h^*, 2g^*f^* > \text{ and } |C^{\perp}| = 4^{deg(f)}2^{deg(h)}.$$

If $h = 1$, then $C =< f >$ and $C^{\perp} =< g^* >$.
If $g = 1$, then $C =< 2f >$ and $C^{\perp} =< h^*, 2f^* >$, where f^*, g^* and h^* are respectively reciprocal polynomials of f, h and g.

Proof. We know that

$$< g^*h^* > \subseteq < g^* > \subseteq < fh, 2fg >^{\perp}$$

and similarly

$$< 2g^*f^* > \subseteq < g^* > \subseteq < fh, 2fg >^{\perp}.$$

Therefore,

$$< g^*h^*, 2g^*f^* > \subseteq < fh, 2fg >^{\perp}.$$

Since

$$| < g^*h^*, 2g^*f^* > | = 4^{n-deg(g)-deg(h)}2^{n-deg(g)-deg(f)} = | < fh, 2fg >^{\perp} |$$

we have $< g^*h^*, 2g^*f^* > = < fh, 2fg >^{\perp}$.

□

2.3 Self-Dual Cyclic Codes Over $\mathbb{Z}_4$

Theorem 2.2.6 gives a pair of generating polynomials for cyclic codes. The next theorem, gives conditions on these polynomials that lead to self-dual codes.

Theorem 2.3.1. *[24] Let $C = < f(x)g(x) > \oplus < 2f(x)h(x) >$ be cyclic code over $\mathbb{Z}_4$ of odd length n, where $f(x)$, $g(x)$, and $h(x)$ are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$. Then C is self-dual if and only if $f(x) = h^*(x)$ and $g(x) = g^*(x)$.*

Proof. Any irreducible factor of $x^n - 1$ is not equal to either 0 or 2. In particular, by definition f^*, g^*, and h^* are all monic and $f^*g^*h^* = x^n - 1$. Suppose that $f(x) = h^*(x)$ and $g(x) = g^*(x)$. By theorem 2.2.9,

$C^{\perp} = < h^*(x)g^*(x) > \oplus < 2h^*(x)f^*(x) > = < f(x)g(x) > \oplus < 2h(x)f(x) >$

$= C$ and C is self-dual.

Now assume that C is self-dual. Since $C = < f(x)g(x) > \oplus < 2h(x)f(x) >$ and $C^{\perp} = < h^*(x)g^*(x) > \oplus < 2h^*(x)f^*(x) >$ and these decompositions are unique, we have

$$f(x)g(x) = h^*(x)g^*(x), \qquad \text{and} \qquad (2.1)$$

$$f(x)h(x) = h^*(x)f^*(x). \qquad (2.2)$$

From (2.1), $x^n - 1 = f(x)g(x)h(x) = h^*(x)g^*(x)h(x)$.
As $f^*(x)g^*(x)h^*(x) = x^n - 1$, we have

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

By the unique factorization of $x^n - 1$ into monic irreducible polynomials, $f^* = h(x)$.

Similarly, using (2.2),
$x^n - 1 = f(x)g(x)h(x) = h^*(x)f^*(x)g(x) = h^*(x)f^*(x)g^*(x)$, implying that $g(x) = g^*(x)$.

□

Example 2.3.1. *[24] Code No.*24 *in table 2.1 has* $f(x) = f_2(x)$, $g(x) = f_3(x)$, *and* $h(x) = f_1(x)$. *Hence its dual is*

$< f_1^*(x)f_3^*(x) > \oplus < 2f_1^*(x)f_2^*(x) >=< f_1(x)f_2(x) > \oplus < 2f_1(x)f_3(x) >$
*which is code No.*20.
Code No.18 has $f(x) = 1$, $g(x) = f_1(x)f_3(x)$, *and* $h(x) = f_2(x)$. *So its dual is* $< f_1^*(x)f_2^*(x)f_3^*(x) > \oplus < 2f_2^*(x) >=< 2f_3(x) >$, *which is code No.10.*

*Code No.*21 *has* $f(x) = f_2(x)$, $g(x) = f_1(x)$, *and* $h(x) = f_3(x)$. *Its dual is* $< f_3^*(x)f_1^*(x) > \oplus < 2f_3^*(x)f_2^*(x) >=< f_2(x)f_1(x) > \oplus < 2f_2(x)f_3(x) >$, *making the code self-dual. There are three cyclic self-dual codes of length* 7.

Example 2.3.2. *[22] We found that the factorization of* $x^{15} - 1$ *over* $\mathbb{Z}_4$ *is given by*

$x^{15} - 1 = g_1(x)g_2(x)g_3(x)g_4(x)g_4^*(x)$,

where $g_1(x) = x - 1$, $g_2(x) = x^4 + x^3 + x^2 + x + 1$, $g_3(x) = x^3 + x + 1$, *and* $g_4(x) = x^4 + 2x^2 + 3x + 1$. *Let* $C =< f(x)g(x) > \oplus < 2f(x)h(x) >$ *be self-dual cyclic code of length* 15. *By Theorem 2.3.1,* $f^*(x) = h(x)$ *and* $g^*(x) = g(x)$. *This implies that if* $g(x)$ *contains a given factor, it must also contain the reciprocal polynomial of that factor. Also if an irreducible factor of* $x^{15} - 1$ *is its own reciprocal polynomial, it must be a factor of* $g(x)$. *Thus there are only the following possibilities:*

(a) $f(x) = g_4(x)$, $g(x) = g_1(x)g_2(x)g_3(x)$, *and* $h(x) = g_4^*(x)$

(b) $f(x) = g_4^*(x)$, $g(x) = g_1(x)g_2(x)g_3(x)$, *and* $h(x) = g_4(x)$

(c) $f(x) = 1$, $g(x) = x^{15} - 1$, *and* $h(x) = 1$.

The code in (a) *and* (b) *are type* $4^4 2^7$ *and the code in* (c) *is the trivial self-dual code with generator matrix* $2I_{15}$.

We can list all non-trivial cyclic codes along with their generators polynomial and their dual codes (see Table 2.1).

Table 2.1: Generators of cyclic codes over $\mathbb{Z}_4$ of length 7.

Code number	Generator polynomials	Type	Dual polynomial
1	2	2^7	2 (self-dual)
2	f_1	4^6	f_2f_3
3	f_2	4^4	f_1f_2
4	f_3	4^4	f_1f_3
5	f_1f_2	4^3	f_2
6	f_2f_3	4	f_1
7	f_1f_3	4^3	f_3
8	$2f_1$	2^6	$< f_2f_3, 2f_1 >$
9	$2f_2$	2^4	$< f_1f_2, 2f_3 >$
10	$2f_3$	2^4	$< f_1f_3, 2f_2 >$
11	$2f_2f_3$	2	$< f_1, 2f_2f_3 >$
12	$2f_1f_2$	2^3	$< f_2, 2f_1f_3 >$
13	$2f_1f_3$	2^3	$< f_3, 2f_1f_2 >$
14	$< f_1, 2f_2f_3 >$	$4^6.2$	$2f_2f_3$
15	$< f_2, 2f_1f_3 >$	$4^4.2^3$	$2f_1f_2$
16	$< f_3, 2f_1f_2 >$	$4^4.2^3$	$2f_1f_3$
17	$< f_1f_2, 2f_3 >$	$4^3.2^4$	$2f_2$
18	$< f_1f_3, 2f_2 >$	$4^3.2^4$	$2f_3$
19	$< f_2f_3, 2f_1 >$	4.2^6	$2f_1$
20	$< f_1f_2, 2f_1f_3 >$	$4^3.2^3$	$< f_2f_3, 2f_1f_2 >$
21	$< f_1f_2, 2f_2f_3 >$	$4^3.2$	$< f_1f_2, 2f_2f_3 >$ (self-dual)
22	$< f_1f_3, 2f_1f_2 >$	$4^3.2^3$	$< f_2f_3, 2f_1f_3 >$
23	$< f_1f_3, 2f_3f_2 >$	$4^3.2$	$< f_1f_3, 2f_3f_2 >$ (self-dual)
24	$< f_2f_3, 2f_1f_2 >$	4.2^3	$< f_1f_2, 2f_1f_3 >$
25	$< f_2f_3, 2f_1f_3 >$	4.2^3	$< f_1f_3, 2f_1f_2 >$

2.4 Cyclic Codes Over $\mathbb{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$

The set of $\mathbb{R}_{2,2}^n$ of n-tuples from $\mathbb{R}_{2,2}$ is an $\mathbb{R}_{2,2} - module$. By a linear code C over $\mathbb{R}_{2,2}$ (or a $\mathbb{R}_{2,2} - code$), we mean an additive submodule of $\mathbb{R}_{2,2}^n$. Duality for codes is understood with respect to the form $xy = \sum_i x_i y_i$. C is said to be self-dual if $C = C^{\perp}$. Two codes are equivalent if one can be obtained from the other by permuting the coordinates and if necessary exchanging 1 and $\overline{u}$ in certain coordinates.

The Lee weight w_L of $x = (x_1, \ldots, x_n)$ is defined as $n_1(x) + 2n_2(x)$, where $n_1(x)$ and $n_2(x)$ are respectively the number of u symbols and the number of 1 or $\overline{u}$ symbols in x. Anon-zero linear code C over $\mathbb{R}_{2,2}$, has generator matrix which after a suitable permutation of the coordinates can be written in the

form

$$\mathbf{G} = \begin{pmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{pmatrix}$$

where A and B are matrices over $\mathbb{R}_{2,2}$ and D is an $\mathbb{F}_2$ matrix. The code C then contains all codewords $[v_0, v_1]G$, where v_0 is a vector of length k_1 over $\mathbb{R}_{2,2}$ and v_1 is a vector of length k_2 over $\mathbb{F}_2$. Thus C contains a total of $4^{k_1}2^{k_2}$ codewords. The parameters of C are given by $[n, 4^{k_1}2^{k_2}, d_{Lee}]$, where d_{Lee} represent the minimum Lee distance of C. Following [3], we associate to the code C two binary codes.

The residue code C_1 defined as $C_1 = \{x \in \mathbb{F}_2^n,\ \exists y \in \mathbb{F}_2^n,\ x + uy \in C\}$ and the torsion code C_2 defined as $C_2 = \{x \in \mathbb{F}_2^n : ux \in C\}$.

A cyclic code of length n over $\mathbb{R}_{2,2}$ is a linear code with the property that if $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(c_1, c_2, \ldots, c_0) \in C$. We assume that n is odd and represent codewords by polynomials, then cyclic codes are ideals in the ring

$$R_n^{(k)} = \mathbb{R}_{2,2}[x]/ < x^n - 1 >.$$

Definition 2.4.1. [3] Let $\mathbb{R}_{2,2}[x]$ be the ring of polynomials over $\mathbb{R}_{2,2}$. We have a natural homomorphic mapping, from $\mathbb{R}_{2,2}$ to its residue field $\mathbb{F}_2$. For any $a \in \mathbb{R}_{2,2}$, let $\hat{a}$ denote the polynomial reduction modulo u.
Now, define a polynomial reduction mapping $\phi : \mathbb{R}_{2,2}[x] \longrightarrow \mathbb{F}_2[x]$ in the obvious way:

$$f(x) = \sum_{i=0}^{n} a_i x^i \xrightarrow{\phi} \sum_{i=0}^{n} \hat{a}_i x^i.$$

A monic polynomial f over $\mathbb{R}_{2,2}[x]$ is said to a basic irreducible polynomial if its projection $\phi(f)$ is irreducible over $\mathbb{F}_2[x]$.
The Galois ring of $\mathbb{R}_{2,2}$ denoted as $GR(\mathbb{R}_{2,2}, r)$ is defined as $\mathbb{R}_{2,2}[x]/ < f(x) >$, where $f(x)$ is a basic monic irreducible polynomial of degree r over $\mathbb{R}_{2,2}$. Hence the ring $GR(\mathbb{R}_{2,2}, r)$ is a module over $\mathbb{R}_{2,2}$.

Remark 2.4.1. [3]

(a) Any irreducible polynomial over $\mathbb{F}_2$ which is subring of $\mathbb{R}_{2,2}$ is obviously irreducible over the ring $\mathbb{R}_{2,2}$.
Thus any monic irreducible polynomial f(x) over $\mathbb{F}_2$ is a basic monic irreducible over $\mathbb{R}_{2,2}$ can be lifted from a monic over $\mathbb{F}_2$.

(b) If any factors over a subring, it also factors over the ring. Thus, the factorization $x^n - 1 = f_1 f_2 \dots f_r$ carries over $\mathbb{R}_{2,2}$, where $x^n - 1$ factors uniquely as a product of a pairwise irreducible polynomial.

To study cyclic codes over $\mathbb{F}_q$ we needed to find the ideals of $\mathbb{F}_q/(x^n - 1)$. Similarly, we need to find the ideals of $R_n^{(k)}$ in order to study cyclic codes over $\mathbb{R}_{2,2}$. We first need to know the ideal structure of $\mathbb{R}_{2,2} = \mathbb{F}_2(u)/(w(u)^k)$, $k > 1$, where $w(u)$ is an irreducible polynomial of degree $m \geq 1$ over $\mathbb{F}_2$. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is a special case of these rings when $w(u) = u$ and $k = 2$.

Lemma 2.4.1. *[3] The only ideals of $GR(\mathbb{R}_{2,2}, r)$ are $< 0 >$, $< 1 >$, and $< u >$.*

Proof. The proof is similar to the proof given in lemma 2.2.4 for ideals in $\mathbb{Z}_4[x]/ < x^n - 1 >$, by replacing 2 by u. □

Lemma 2.4.2. *[3] If $x^n - 1 = f_1 f_2 \dots f_r$, where the $f_i (1 \leq i \leq r)$ are basic irreducible and pairwise-coprime polynomials, then the factorization is obtained from factorization of the binary polynomial $x^n - 1$.*

Lemma 2.4.3. *[3] Let n be odd. Let $x^n - 1 = f_1 f_2 \dots f_r$, where the f_i $(1 \leq i \leq r)$ are basic irreducible and pairwise-coprime polynomials. Let $\hat{f}_i$ denote the product of all f_j except f_i. Then any ideal in the ring is a sum of $\hat{f}_i$ and $< u\hat{f}_j >$.*

Proof. The proof is similar to the proof given in 2.2.5, for ideals in $\mathbb{Z}_4[x]/ < x^n - 1 >$ as in this case also ideals $R_n^{(k)}$ can be written as

$$I \cong I_1 \oplus I_2 \oplus \dots \oplus I_r,$$

where I_i is an ideal of the ring $\mathbb{R}_{2,2}[x]/ < f_i >$, for $i = 1, 2, \dots, r$.
By Lemma 2.4.1, The only ideals in $\mathbb{R}_{2,2}[x]/ < f_i >$ are $< 0 >$, $< 1 >$ *or* $< u >$.

The ideals $< 1 >$ *and* $< u >$ in $I_i = \mathbb{R}_{2,2}[x]/(f_i)$ corresponds respectively to the ideals (f_i) and $(u\hat{f}_j)$ in the ring $R_n^{(k)}$. In any case, the ideal I is a sum of $(\hat{f}_i)$ and $(u\hat{f}_j)$.

□

As a consequence of the above theorem, the number of cyclic codes over $\mathbb{R}_{2,2}$ of length n is 3^t, where t is the number of basic irreducible polynomial factors in $x^n - 1$ over $\mathbb{R}_{2,2}$. The following theorem characterize cyclic codes by giving generator polynomial description.

Theorem 2.4.4. *[3] Suppose C is a cyclic code of odd length n over $\mathbb{R}_{2,2}$, then there are unique monic polynomials f, g and h such that $C =< fh, ufg >$ where $fgh = x^n - 1$ and $|C| = 4^{deg(g)}2^{deg(h)}$,*
when $h = 1$, $C =< f >$ and $|C| = 4^{n-deg(f)}$,
when $g = 1$, $C =< uf >$ and $|C| = 2^{n-deg(f)}$.

Proof. The proof of Theorem 2.2.6, is the same as the proof of this Theorem, by replacing 2 by u. □

For a polynomial $f \in \mathbb{R}_{2,2}$, of degree k, f^* will donate its **reciprocal polynomial** $x^k f(x^{-1})$. The proof of Theorem 2.2.9 also proves the following Theorem. If we replace 2 by u.

Theorem 2.4.5. *[3] Suppose $C =< fh, ufg >$ is a cyclic code of odd length n over $\mathbb{R}_{2,2}$, where f, g and h are monic polynomials such that $fgh = x^n - 1$ and $|C| = 4^{deg(g)}2^{deg(h)}$, then the dual of C is $C^{\perp} =< g^*h^*, ug^*f^* >$ and $| C^{\perp}| = 4^{deg(f)}2^{deg(h)}$. If $h = 1$, $C =< f >$ and $C^{\perp} =< g^* >$. If $g = 1$, $C =< uf >$ and $C^{\perp} =< h^*, uf^* >$, where f^*, g^* and h^* are respectively reciprocal polynomials of f, h and g.* □

For any element of $\mathbb{R}_{2,2}$ expressed as $x + uy$, the Gray map ϕ from $\mathbb{R}_{2,2}$ to $\mathbb{F}_2^2$ is defined by $\phi(x + uy) = (y, x + y)$, where $x,\ y\ \in\ \mathbb{F}_2$. We define a new weight function for codes over $\mathbb{R}_{2,2}$. The Gray weight $Gw(x)$ of a codeword $x = (x_1, x_2, \ldots, x_n)$ is defined as $\sum_{i=1}^{n} Gw(x_i)$ where

$$Gw(x_i) = \begin{cases} 0, & \text{if } x_i = 0; \\ 1, & \text{if } x_i = 1,\ \overline{u}; \\ 2, & \text{if } x_i = u. \end{cases}$$

Using the following map ϕ from $\mathbb{R}_{2,2}$ to $\mathbb{F}_2^2$

x_i	$\phi(x_i)$
0	00
1	01
u	11
$\overline{u}$	10

Lemma 2.4.6. *[3] If a code C is linear or self-dual so is $\phi(C)$. The minimum Lee weight of C is equal to the minimum Hamming weight of $\phi(C)$.*

Proof. Let $t = x + uy$, $t^{'} = x^{'} + uy^{'} \in \mathbb{R}_{2,2}$, then $t + t^{'} = x + x^{'} + u(y + y^{'})$ and $\phi(t + t^{'}) = (y + y^{'}, x + x^{'} + y + y^{'}) = (y, x + y) + (y^{'}, x^{'} + y^{'}) = \phi(t) + \phi(t^{'})$, also $\phi(\alpha t) = \alpha\phi(t)$. so ϕ is a linear map.
Now let $c_i = x_i + uy_i$, where $i = 1, 2$. And let $w_i = \phi_{GL}(c_i)$, $i = 1, 2$. Then $\phi(c_1+c_2) = (y_1+y_2, x_1+x_2+y_1+y_2) = (y_1, x_1+y_1)+(y_2, x_2+y_2) = \phi(c_1)+\phi(c_2)$. This implies that $\phi(C)$ is linear binary code over $\mathbb{F}_2$.
Since the generalized Gray map ϕ_{GL} is an isometry from

$$(\mathbb{R}_1, GL) \text{ to } (\mathbb{F}_2^{2n}, Hamming\ distance),$$

and from the definition of Gray map,

$$wt_H(\phi(c)) = wt_{GL}(\phi(c)), c \in C,$$
$$d_H(wt_{GL}(\phi(c_1)), wt_{GL}(\phi(c_2))) = d_{GL}(c_1, c_2),\ c_1, c_2 \in C,$$

then the minimum generalized Lee weight of C is the same as minimum Hamming weight of $\phi_{GL}(C)$. □

2.5 Self-dual Codes Over $\mathbb{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$

The condition for a cyclic code of odd length n to be self-dual is given by the following theorem.

Theorem 2.5.1. *[3] Let C be a cyclic code over $\mathbb{R}_{2,2}$, $C =< fh, ufg >$, where $x^n - 1 = fgh$, n odd length. Then C is self-dual if and only if $f = g^*$ and $h = h^*$.*

Proof. The proof of Theorem 2.3.1, is the same as the proof of this Theorem, if we replace 2 by u. □

Theorem 2.5.2. *[3] Non trivial cyclic self-dual of length n exist if and only if $-1 \neq 2^i (mod n)$ for any i.* □

As a consequence of above theorem, non trivial self-dual cyclic codes do not exist for lengths 17 and 19. Similarly to $\mathbb{Z}_4$ case.

Example 2.5.1. *[3] The factorization of $x^{21}-1$ is equal to $f_1 f_2 f_3 f_4 f_5 f_6$, where*
$f_1 = x - 1$
$f_2 = x^2 - x - 1$
$f_3 = x^3 - x - 1$
$f_4 = x^3 - x^2 - 1$
$f_5 = x^6 - x^4 - x^2 - x + 1$ *and*

$f_6 = x^6 - x^5 - x^4 - x^2 + 1$.
The most interesting code is $C =< fh, ufg >$ *where* $f = f_5$, $g = f_6$ *and* $h = f_1 f_2 f_3 f_4$. *It is a self-dual code of parameters* $[21, 4^6 2^9, 6]$.

Example 2.5.2. *[3] Table 2.2 presents all the* $3^3 - 2 = 25$ *non-trivial cyclic codes of length 7.*
$x^7 - 1 = (x + \overline{u})(x^3 + ux^2 + x + \overline{u})(x^3 + \overline{u}x^2 + ux + \overline{u}) = f_1 f_2 f_3$,
where u *and* $\overline{u}$ *are replaced respectively by* 2 *and* 3.

Table 2.2
Generators of cyclic codes over $\mathbb{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$ *of length 7.*

Code number	*Generator polynomials*	*Type*	*Binary Image*	*Dual polynomial*
1	u	2^7	$[14, 7, 2]$	u *(self-dual)*
2	f_1	4^6	$[14, 12, 2]$	$f_2 f_3$
3	f_2	4^4	$[14, 8, 3]$	$f_1 f_2$
4	f_3	4^4	$[14, 8, 3]$	$f_1 f_3$
5	$f_1 f_2$	4^3	$[14, 6, 4]$	f_2
6	$f_2 f_3$	4	$[14, 2, 7]$	f_1
7	$f_1 f_3$	4^3	$[14, 6, 4]$	f_3
8	uf_1	2^6	$[14, 6, 4]$	$< f_2 f_3, uf_1 >$
9	uf_2	2^4	$[14, 4, 6]$	$< f_1 f_2, uf_3 >$
10	uf_3	2^4	$[14, 4, 6]$	$< f_1 f_3, uf_2 >$
11	$uf_2 f_3$	2	$[14, 1, 14]$	$< f_1, uf_2 f_3 >$
12	$uf_1 f_2$	2^3	$[14, 3, 8]$	$< f_2, uf_1 f_3 >$
13	$uf_1 f_3$	2^3	$[14, 3, 8]$	$< f_3, uf_1 f_2 >$
14	$< f_1, uf_2 f_3 >$	$4^6.2$	$[14, 13, 2]$	$uf_2 f_3$
15	$< f_2, uf_1 f_3 >$	$4^4.2^3$	$[14, 11, 2]$	$uf_1 f_2$
16	$< f_3, uf_1 f_2 >$	$4^4.2^3$	$[14, 11, 2]$	$uf_1 f_3$
17	$< f_1 f_2, uf_3 >$	$4^3.2^4$	$[14, 10, 2]$	uf_2
18	$< f_1 f_3, uf_2 >$	$4^3.2^4$	$[14, 10, 2]$	uf_3
19	$< f_2 f_3, uf_1 >$	4.2^6	$[14, 8, 2]$	uf_1
20	$< f_1 f_2, uf_1 f_3 >$	$4^3.2^3$	$[14, 9, 4]$	$< f_2 f_3, uf_1 f_2 >$
21	$< f_1 f_2, uf_2 f_3 >$	$4^3.2$	$[14, 7, 4]$	$< f_1 f_2, uf_2 f_3 >$ *(self-dual)*
22	$< f_1 f_3, uf_1 f_2 >$	$4^3.2^3$	$[14, 9, 4]$	$< f_2 f_3, uf_1 f_3 >$
23	$< f_1 f_3, uf_3 f_2 >$	$4^3.2$	$[14, 7, 4]$	$< f_1 f_2, uf_3 f_2 >$ *(self-dual)*
24	$< f_2 f_3, uf_1 f_2 >$	4.2^3	$[14, 5, 6]$	$< f_1 f_2, uf_1 f_3 >$
25	$< f_2 f_3, uf_1 f_3 >$	4.2^3	$[14, 5, 6]$	$< f_1 f_3, uf_1 f_2 >$

In Table 2.2 we list all nontrivial cyclic $\mathbb{R}_{2,2}$ codes of length 7.

Chapter 3

Cyclic Codes Over Rings Of Higher Orders

3.1 Introduction

The goal of this chapter is to generalize the results of Pless and Qian and those of Sloe for cyclic $\mathbb{Z}_4$-codes to cyclic $\mathbb{Z}_{p^m}$-codes. Second, we establish connections between this new development and results on $\mathbb{Z}_{p^m}$-codes obtained by Calderbank and Sloane.

Also we study cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$, and describe the structure of Galois extension ring and cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$. More information can be found in [1], [4], [13], [16], [17], [18],.

3.1.1 Introduction to codes over $\mathbb{Z}_{p^m}$

A subset C of $\mathbb{Z}_{p^m}^n$ is called a $\mathbb{Z}_{p^m}$-codes if C is a $\mathbb{Z}_{p^m}$-submodule of $\mathbb{Z}_{p^m}^n$. C is called cyclic if whenever $a = (a_0, a_1, \ldots, a_{n-1}) \in C$; its cyclic shift $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also in C. As is customary, if a polynomial $f(x)$ divides $x^n - 1$ (say $x^n - 1 = f(x)g(x)$), we refer to $g(x) = x^n - 1/f(x)$ as $\hat{f}(x)$. For a $\mathbb{Z}_{p^m}$-code C we shall use $C^\perp$ to denote the dual (orthogonal) code of C. A code is called self-dual if it is its own dual. For a polynomial f of degree k, f^* will denote its reciprocal polynomial $x^k f(x^{-1})$.

Definition 3.1.1. A polynomial $f \in \mathbb{Z}_p[x]$ is called nilpotent if there exists a positive integer n such that $f^n = 0$.

Also, $f \neq 0$ is called regular if it is not a zero divisor, i.e., if for $g \in \mathbb{Z}_{p^m}[x]$, $fg = 0$ implies $g = 0$.

Definition 3.1.2. [18] A commutative ring $\mathbb{R}$ is called local if it has a unique maximal ideal. For example, $\mathbb{Z}_{p^m}$ is a local ring with unique maximal ideal $p\mathbb{Z}_{p^m}$.

By $\pi : \mathbb{Z}_p^m[x] \longrightarrow \mathbb{Z}_p[x]$, we will denote the ring homomorphism that maps $a + (p^m)$ to $a + (p)$, where $a \in \mathbb{Z}_p^m$, and the variable x to x. Observe that $f \in \mathbb{Z}_{p^m}[x]$ is unit if and only if πf is a unit, f is regular if and only if $\pi f \neq 0$ if and only if f is not nilpotent, if and only if a_i is not nilpotent for some i.

Definition 3.1.3. [18] Two polynomials f and g in $\mathbb{Z}_{p^m}[x]$ are called coprime if $\mathbb{Z}_{p^m}[x] =< f > + < g >$.

Lemma 3.1.1. *[18] If $f,\ g \in \mathbb{Z}_{p^m}[x]$ are regular then $f,\ g$ are coprime if and only if $\pi f,\ \pi g$ are coprime.*

Proof. If f and g are coprime, then there exist $f_1,\ g_1 \in \mathbb{Z}_{p^m}[x]$ such that $1 = ff_1 + gg_1$ and therefore $\pi f \neq 0 \neq \pi g$ and $1 = \pi f \pi f_1 + \pi g \pi g_1$.
Thus πf and πg are coprime.

Conversely, if πf and πg are coprime then there exist f_1, g_1, and r in $\mathbb{Z}_{p^m}[x]$ such that $f(x)f_1(x) + g(x)g_1(x) = 1 + p^k r(x)$ for some positive integer k.
Since $1 + p^k r(x)$ is invertible in $\mathbb{Z}_{p^m}[x]$, it follows that $1 \in < f > + < g >$ and consequently f and g are coprime. □

Definition 3.1.4. [18] A polynomial f in $\mathbb{Z}_{p^m}[x]$ is basic irreducible if πf is irreducible in $\mathbb{Z}_p[x]$. Also, f is called primary if $< f >$ is a primary ideal, that is, if the relation $gh \in < f >$ implies that either $g \in < f >$ or $h^k \in < f >$ for some positive integer k.

The following Lemma is a generalization of Lemma 2.2.1, see [24].

Lemma 3.1.2. *[18] If f is a basic irreducible polynomial, then f is primary.*

Proof. Suppose $g(x)h(x) \in < f(x) >$. Since f is basic irreducible, $\pi f(x)$ is irreducible in $\mathbb{Z}_p[x]$ so that

$$\gcd(\pi f(x), \pi g(x)) = 1 \text{ or } \pi f(x).$$

If $\gcd(\pi f(x), \pi g(x)) = 1$, then by Lemma 3.1.1, f and g are coprime. Thus

$$1 = f(x)f_1(x) + g(x)g_1(x) \text{ for some } f_1(x),\ g_1(x) \in \mathbb{Z}_{p^m}[x]$$

so that $h(x) = f(x)h(x)f_1(x) + g(x)h(x)g_1(x)$. Since $g(x)h(x) \in < f(x) >$ it follows that $f(x) \mid h(x)$.
If $\gcd(\pi f(x), \pi g(x)) = \pi f(x)$ then there exist $u(x), v(x) \in \mathbb{Z}_{p^m}[x]$ such that

$$g(x) = f(x)u(x) + p^k v(x) \text{ for some positive integer } k < m.$$

But then $g^m(x) \in < f(x) >$. Thus $f(x)$ is a primary polynomial. □

3.2 Cyclic codes over $\mathbb{Z}_{p^m}$

The next Lemma discuss the structure of the ideals of the ring $\mathbb{Z}_{p^m}[x]/ < f(x) >$ for a basic irreducible polynomial f in $\mathbb{Z}_{p^m}[x]$. This Lemma is a generalization of Lemma 2.2.4 in [22]. It will play a crucial rule in the characterization of generators for cyclic $\mathbb{Z}_{p^m}$-codes.

Lemma 3.2.1. *[18] If $f(x) \in \mathbb{Z}_{p^m}[x]$ is a basic irreducible polynomial, then the ideals of $\mathbb{Z}_{p^m}[x]/ < f(x) >$ are precisely $< 0 >$, $(1+ < f(x) >)$, $(p+ < f(x) >)$, $\ldots$, $(p^{m-1}+ < f(x) >)$.*

Proof. Let I be a nonzero ideal of $\mathbb{Z}_{p^m}[x]/ < f(x) >$. Let $g(x)+ < f(x) >$ be a nonzero element of I. By Definition 3.1.4, πf is an irreducible polynomial and, hence, $\gcd(\pi f(x), \pi g(x)) = 1$ *or* $\pi f(x)$.
If $\gcd(\pi f(x), \pi g(x)) = 1$, then by Lemma 3.1.1, f and g are coprime. Hence, there exist $u(x)$ and $v(x)$ such that

$$1 = f(x)u(x) + g(x)v(x).$$

But then $(g(x)+ < f(x) >)(v(x)+ < f(x) >) = 1+ < f(x) >$.
Therefore $g(x)+ < f(x) >$ is invertible. Consequently, $I = \mathbb{Z}_{p^m}[x]/ < f(x) >$.
On the other hand, if $\gcd(\pi f(x), \pi g(x)) = \pi f(x)$, then there exist $u(x),\ v(x) \in \mathbb{Z}_{p^m}[x]$ such that $g(x) = f(x)u(x) + p^k v(x)$, where $\gcd(\pi f(x), \pi v(x)) = 1$ and k is some positive integer less than m. Thus

$$g(x)+ < f(x) > \in (p^k+ < f(x) >).$$

Hence, there exist $1 \leq l < m$ such that $I \subset (p^l+ < f(x) >)$.
Let k_0 be the largest positive integer l less than m such that
$I \subset (p^l+ < f(x) >)$. In particular, there exist a nonzero element $h(x)+ < f(x) >$ in I such that $h(x) = f(x)u(x) + p^{k_0} r(x)$ and $\gcd(\pi f(x), \pi r(x)) = 1$. Thus

$$p^{k_0} r(x)+ < f(x) > \in I \text{ and } \gcd(\pi f(x), \pi r(x)) = 1.$$

But then, by Lemma 3.1.1, $f,\ r$ are coprime. Hence, there exist $a(x),\ b(x) \in \mathbb{Z}_{p^m}[x]$ such that $1 = r(x)a(x) + f(x)b(x)$.
Thus $p^{k_0}+ < f(x) > = (p^{k_0} r(x)+ < f(x) >)(a(x)+ < f(x) >) \in I$.

Consequently $I = (p^{k_0} + < f(x) >)$. This concludes the proof of the Lemma.

□

Recall that a code over $\mathbb{Z}_{p^m}$ is cyclic if and only if it is an ideal in the ring $\mathcal{R}_n = \mathbb{Z}_{p^m}/ < x^n - 1 >$. The next Theorem describes the ideals in $\mathcal{R}_n$. This is a generalization of Theorem 2.2.5 in [22].

Theorem 3.2.2. *[18] Let p be a prime such that p does not divide n. Let $x^n - 1 = f_1 f_2 \dots f_r$, be the representation of $x^n - 1$ as a product of basic irreducible pairwise-coprime polynomials in $\mathbb{Z}_{p^m}[x]$. Then any ideal in $\mathcal{R}_n$ is a sum of ideals of the type $< p^j \hat{f}_i > + < x^n - 1 >$, where $0 \leq j \leq m-1$, $1 \leq i \leq r$ and, for $1 \leq i \leq r$, $\hat{f}_i =< x^n - 1 > / f_i = \pi_{j \neq i} f_i$.*

Proof. Since the f_i are pairwise-coprime, we have

$$< x^n - 1 >=< f_1 > \bigcap < f_2 > \bigcap < f_3 > \bigcap \dots \bigcap < f_r >,$$

and for $1 \leq i,\ j \leq r, i \neq j$, $\mathbb{Z}_{p^m}[x] =< f_i > + < f_j >$.
Thus, by the Chinese Remainder Theorem 1.1.20,

$$\mathcal{R}_n = \mathbb{Z}_{p^m}[x]/\bigcap_{i=1}^{r} < f_i > \cong \oplus \sum_{i=1}^{r} \mathbb{Z}_{p^m}[x]/ < f_i >.$$

Consequently, if I is an ideal of $\mathcal{R}_n$, then $I = \bigoplus \sum I_i$, where I_i is an ideal of the ring $\mathbb{Z}_{p^m}[x]/ < f_i >$. By Lemma 3.2.1, for each i, $1 \leq i \leq r$,

$$I_i =< 0 > \ \text{or}\ (p^k + < f_i >) \text{ for some } k,\ 0 \leq k \leq m-1.$$

But then I_i will correspond to $(p^k \hat{f}_i + < x^n - 1 >)$ in $\mathcal{R}_n$. Hence, I is a sum of ideals of the type $(p^j \hat{f}_i + < x^n - 1 >)$.

□

Corollary 3.2.3. *[18] The number of cyclic codes over $\mathbb{Z}_{p^m}$-codes of length n is $(m+1)^r$, where r is the number of factors in a factorization of $x^n - 1$ as a product of basic irreducible pairwise-coprime polynomials.*

Theorem 3.2.4. *[18] Suppose p is a prime not dividing n and C is a cyclic $\mathbb{Z}_{p^m}$-code, then there exist a collection of pairwise-coprime polynomials $F_0, F_1, \dots, F_m$ (possibly equal to 1) such that $F_0 F_1 \dots F_m = x^n - 1$, and C is generated by $\{\hat{F}_1, p\hat{F}_2, \dots, p^{m-1}\hat{F}_m\}$; i.e.,*

$$C =< \hat{F}_1, p\hat{F}_2, \dots, p^{m-1}\hat{F}_m >.$$

The polynomials $F_0,\ F_1,\ \ldots,\ F_m$ *are unique in the sense that if*

$$C =< \hat{H_1}, p\hat{H_2}, \ldots, p^{m-1}\hat{H_m} >,$$

where $H_0H_1 \ldots H_m = x^n - 1$ *then for* $0 \leq i \leq m$, F_i *is an associate of* H_i. *In particular, if we require* $F_i s$ *to be monic then the representation is unique. Moreover,* $|C| = p^k$, *where* $k = \sum_{i=0}^{m-1}(m-i)\deg F_{i+1}$. □

Remark 3.2.1. Some of the generators above may be equal to zero.
Namely, if for some k, $1 \leq k \leq m$, $F_k = 1$, then
$\hat{F_k} = F_0F_1 \ldots F_{k-1}F_{k+1} \ldots F_m = 0\ (mod < x^n - 1 >)$.

Corollary 3.2.5. *[18] Suppose* p *is a prime not dividing* n *and* C *is a cyclic* $\mathbb{Z}_{p^m}$*-code. Then there exist polynomials* $f_0,\ f_1,\ \ldots,\ f_{m-1}$ *such that*

$$f_{m-1}|f_{m-2}| \ldots |f_0|x^n - 1$$

and

$$C =< f_0, pf_1, p^2f_2, \ldots, p^{m-1}f_{m-1} > .$$

Proof. With the notation of Theorem 3.2.4

$$C =< \hat{F_1}, p\hat{F_2}, \ldots, p^{m-1}\hat{F_m} >.$$

For $0 \leq i \leq m-2$, let $f_i = F_0F_{i+2} \ldots F_m$ and $f_{m-1} = F_0$. Then $f_{m-1}|f_{m-2}| \ldots |f_0|x^n - 1$. Also for all i, $0 \leq i \leq m-1$,

$$p^i\hat{F}_{i+1} = p^iF_0F_1 \ldots F_iF_{i+2} \ldots F_m = p^if_iF_1F_2 \ldots F_i.$$

Hence, $C \subset< f_0, pf_1, \ldots, p^{m-1}f_{m-1} > .$
To prove the reverse inclusion first observe that $f_0 \in C$. Again as F_1 and F_2 are coprime, there exist polynomials $a(x),\ b(x) \in \mathbb{Z}_{p^m}$ such that

$$1 = a(x)F_1(x) + b(x)F_2(x).$$

Thus, $pf_1 = pF_0F_3 \ldots F_m = pa(x)F_0F_1F_3 \ldots F_m + pb(x)f_0$
$= pa(x)\hat{F_2} + pb(x)f_0 \in C.$
Proceeding like this we get $p^if_i \in C$ for all i, $0 \leq i \leq m-1$.
Thus, $C =< f_0, pf_1, \ldots, p^{m-1}f_{m-1} > .$

□

Theorem 3.2.6. *[12] Let C be a cyclic code of length n with notation as in Theorem 3.2.4, and $F = \hat{F}_1 + p\hat{F}_2 + \ldots + p^{m-1}\hat{F}_m$. Then F is a generating polynomial of C, i.e., $C =< F >$.*

Proof. For any distinct $i,\ j \in \{0, \ldots, m\}$, we have $(x^n - 1)|\hat{F}_i\hat{F}_j$, so $\hat{F}_i\hat{F}_j = 0$ in $\mathbb{Z}_{p^m}[x]/(x^n - 1)$. Moreover, for any i with $1 \leq i \leq m$, $F_i,\ \hat{F}_i$ are coprime, hence, there exist $u_i,\ v_i \in \mathbb{Z}_{p^m}[x]$ such that $u_iF_i + v_i\hat{F}_i = 1$
Thus, for any integer $j \in \{1, \ldots, m\}$, we have $\Pi_{i=0}^{j}(u_iF_i + v_i\hat{F}_i) = 1$.
Multiplying the left-hand side of this equation out, we get that there exist polynomials $w_{j_0}, \ldots, w_{j_j}$ such that
$w_{j0}F_1F_2 \ldots F_j + w_{j_1}\hat{F}_1F_2 \ldots F_j + w_{j_2}F_1\hat{F}_2 \ldots F_j + \ldots + w_{j_j}F_1F_2 \ldots F_{j-1}\hat{F}_j = 1$.
In particular, when $j = m - 1$, we have
$w_{m-1,0}F_1F_2 \ldots F_{m-1} + w_{m-1,1}\hat{F}_1F_2 \ldots F_{m-1} + \ldots + w_{m-1,m-1}F_1F_2 \ldots F_{m-2}\hat{F}_{m-1} = 1$.
Multiplying both sides of the above equation by $p^{m-1}\hat{F}_m$ yields

$$p^{m-1}\hat{F}_m w_{m-1,0}F_1F_2 \ldots F_{m-1} = p^{m-1}\hat{F}_m.$$

By hypothesis $F = \hat{F}_1 + p\hat{F}_2 + \ldots + p^{m-1}\hat{F}_m$ which implies
$FF_1F_2 \ldots F_{m-1}w_{m-1,0} = p^{m-1}\hat{F}_mF_1F_2 \ldots F_{m-1}w_{m-1,0} = p^{m-1}\hat{F}_m$.
Therefore, $p^{m-1}\hat{F}_m \in < F >$. Continuing this process, we obtain that

$$p^{m-1}\hat{F}_m,\ p^{m-2}\hat{F}_{m-1}, \ldots p\hat{F}_2,\ \hat{F}_1 \in < F > .$$

Consequently, $C =< F >$. □

Remark 3.2.2. It is also possible to obtain the generators in Theorem 3.2.4 from those in Corollary 3.2.5, by writing $F_0 = f_{m-1}$, $F_1 = (x^n - 1)/f_0$, and for $2 \leq i \leq m$, $F_i = f_{i-2}/f_{i-1}$.

Corollary 3.2.7. *[18] If p is a prime not dividing n, then $\mathcal{R}_n$ is a principal ideal ring.*

Proof. With the notations of Theorem 3.2.4, $C =< \hat{F}_1, p\hat{F}_2, \ldots, p^{m-1}\hat{F}_m >$.
let $G = \hat{F}_1 + p\hat{F}_2 + \ldots + p^{m-1}\hat{F}_m$. we shall prove that $C =< G >$.
First observe that for $0 \leq i,\ j \leq m$, $i \neq j$, we have $\hat{F}_i\hat{F}_j = 0$ in $\mathcal{R}_n$. Also, since for all i such that $1 \leq i \leq m$, $\hat{F}_i,\ F_i$ is a pair of coprime polynomials, there exist $b_i,\ c_i$ such that $b_i\hat{F}_i + c_iF_i = 1$. It follows that, for all k such that $1 \leq k \leq m$, $\prod_{i=1}^{k}(b_i\hat{F}_i + c_iF_i) = 1$.

Therefore, for all k, there exist polynomials a_{k_0}, a_{k_1}, $\ldots$, a_{k_k} such that $a_{k_0}F_1F_2\ldots F_k + a_{k_1}\hat{F_1}F_2\ldots F_k + a_{k_2}F_1\hat{F_2}\ldots F_k + \ldots + a_{k_k}F_1F_2\ldots F_{k-1}\hat{F_k} = 1$.
Multiplying by $p^{m-1}\hat{F_m}$ on both sides of the version of the above equation with $k = m-1$, we obtain $p^{m-1}\hat{F_m} = p^{m-1}a_{m-1,0}F_1F_2\ldots F_{m-1}\hat{F_m}$.
On the other hand, $F_1F_2\ldots F_{m-1}G = p^{m-1}F_1F_2\ldots F_{m-1}\hat{F_m}$.
Consequently, $p^{m-1}\hat{F_m} \in < G >$ and thus, $H = \hat{F_1} + p\hat{F_2} + \ldots + p^{m-2}\hat{F}_{m-1} \in < G >$.
A similar argument yields $p^{m-2}\hat{F}_{m-1} = p^{m-2}a_{m-2,0}F_1F_2\ldots F_{m-2}\hat{F}_{m-1}$ and $F_1F_2\ldots F_{m-2}H = p^{m-2}F_1F_2\ldots F_{m-2}\hat{F}_{m-1}$. So, we get $p^{m-2}\hat{F}_{m-1} \in < G >$ and hence, $\hat{F_1} + p\hat{F_2} + \ldots + p^{m-3}\hat{F}_{m-2} \in < G >$.
Continuing on like this, we conclude that $\hat{F_1}, p\hat{F_2}, p^2\hat{F_3}, \ldots, p^{m-1}\hat{F_m} \in < G >$.
This completes the proof. □

Dual and Self-dual codes

Recall that, for a $\mathbb{Z}_{p^m}$-code C, we shall use notation $C^\perp$ to denote the dual code of C. A code is called self-dual if it is own dual.

The number of elements in any nonzero linear code C over $\mathbb{Z}_{p^m}$ is of the form p^k. Furthermore, the dual code $C^\perp$ has p^l codewords where $k + l = mn$.

Theorem 3.2.8. *[18] Suppose p is a prime not dividing n and*

$$C = < \hat{F_1}, p\hat{F_2}, \ldots, p^{m-1}\hat{F_m} >,$$

where $F_0F_1\ldots F_m = x^n - 1$. Then

$$C^\perp = < \hat{F_0^*}, p\hat{F_m^*}, p^2\hat{F^*}_{m-1}, \ldots, p^{m-1}\hat{F_2^*} >.$$

Proof. We assume that $F_i \neq 1$ for all i, $1 \leq i \leq m$. The case when some $F_i = 1$ can be dealt with similarly.
Let $C_1 = < \hat{F_0^*}, p\hat{F_m^*}, p^2\hat{F^*}_{m-1}, \ldots, p^{m-1}\hat{F_2^*} >$. First observe that for $0 \leq i, j \leq m-1$, $(p^i\hat{F}_{i+1})(p^i\hat{F^*}_{m-j+1})^*$ is divisible by $x^n - 1$ if $i + 1 \neq m - j + 1$ and by p^m if $i + 1 = m - j + 1$. In any case $(p^i\hat{F}_{i+1})(p^i\hat{F^*}_{m-j+1})^* = 0 \ (mod\ x^n - 1)$.
Thus $C_1 \subset C^\perp$. Also

$$|C_1| = p^{m\ degF_0^*}p^{(m-1)\ degF_m^*\cdots}p^{degF_2^*} = p^t,$$

where $t = \sum_{i=1}^{m} i \deg F_{i+1}$, with $F_{m+1} = F_0$.

On the other hand, $|C^{\perp}| = p^l$, where $l + k = n$. By Theorem 3.2.4, above, $k = \sum_{i=0}^{m-1}(m-i)\deg F_{i+1}$. It follows that $l = \Sigma_{i=1}^{m} i \deg F_{i+1} = t$ (with $F_{m+1} = F_0$). Hence, $C^{\perp} = C_1$ and the proof is complete. □

Theorem 3.2.9. *[12] With the notation as in Theorem 3.2.8, let* $G = \hat{F_0^*} + p\hat{F_m^*} + p^2\hat{F^*}_{m-1} + \ldots + p^{m-1}\hat{F_2^*}$. *Then* G *is a generating polynomial of* $C^{\perp}$, *i.e.,* $C^{\perp} =< G >$.

Proof. A similar arguement as in the proof of Theorem 3.2.6 gives the result. □

Theorem 3.2.10. *[18] Let* $F_0F_1 \ldots F_m = x^n - 1$ *and* $C =< \hat{F}_1, p\hat{F}_2, \ldots p^{m-1}\hat{F}_m >$ (*as in Theorem* 3.2.4), *then* C *is self-dual if and only if* F_i *is an associate of* F_j^* *for all* $i,\ j \in \{0, \ldots, m\}$ *such that* $i + j \equiv 1\ (mod\ m+1)$.

Proof. By Theorem 3.2.8, $C^{\perp} =< \hat{F_0^*}, p\hat{F_m^*}, p^2\hat{F^*}_{m-1}, \ldots, p^{m-1}\hat{F_2^*} >$, If F_i is an associate of F_j^* for all $i,\ j \in \{0, \ldots, m\}$ such that $i + j \equiv 1\ (mod\ m+1)$, then $C^{\perp} =< \hat{F_0^*}, p\hat{F_m^*}, p^2\hat{F^*}_{m-1}, \ldots, p^{m-1}\hat{F_2^*} >=< \hat{F}_1, p\hat{F}_2, \ldots p^{m-1}\hat{F}_m >= C$ i.e., C is self-dual.

On the other hand, assume $C = C^{\perp}$, and let c_i denote the constant of F_i, $0 \leq i \leq m$. Since $F_0F_1 \ldots F_m = x^n - 1$, it follows that $c_0c_1 \ldots c_m = -1$. Therefore, c_i are invertible elements of $\mathbb{Z}_{p^m}$ and c_i are leading coefficients of F_i. For all $i,\ j \in \{0, \ldots, m\}$ such that $i + j \equiv 1(mod\ m+1)$, denote $G_i = u_iF_j^*$, where u_i are suitable invertible elements in $\mathbb{Z}_{p^m}$ such that G_i are monic polynomials. Note that $u_i = c_i^{-1}$, and $u_0u_1 \ldots u_m = c_0^{-1}c_i^{-1} \ldots c_m^{-1} = -1$. Now

$$C =< \hat{F_0^*}, p\hat{F_m^*}, \ldots, p^{m-1}\hat{F_2^*}) =< \hat{G}_1, p\hat{G}_2, \ldots, p^{m-1}\hat{G}_m >.$$

Also,

$$\begin{aligned} G_0G_1 \ldots G_m &= (u_0u_1 \ldots u_m)\hat{F_0^*}\hat{F_1^*} \ldots \hat{F_m^*} = -\hat{F_0^*}\hat{F_1^*} \ldots \hat{F_m^*} \\ &= -x^{deg\ F_0 + deg\ F_1 + \ldots + deg\ F_m} F_0(x^{-1})F_1(x^{-1}) \ldots F_m(x^{-1}) \\ &= -x^n(x^{-n} - 1) = x^n - 1. \end{aligned}$$

From the uniqueness in Theorem 3.2.4, $F_i = G_i$ and the proof is complete. □

EXAMPLES

Example 3.2.1. *[18] (Cyclic $\mathbb{Z}_8$-codes of length 7).*
$x^7 - 1 = (x-1)(7 + 5x + 6x^2 + x^{3)})(7 + 2x + 3x^2 + x^3) = f_0 f_1 f_2$.
the number of cyclic codes $(3+1)^3 = 64$ *cyclic codes. In Table I we list some nontrivial cyclic* $\mathbb{Z}_8$*-codes of length* 7 *along with their duals.*

***Table I**: Cyclic codes over $\mathbb{Z}_8$-codes of length 7.*

Generator of the code	*Generator of the dual code*	*Order of the code*
2	2^2	4^7
2^2	2	2^7
f_0	$f_1 f_2$	8^6
f_1	$f_0 f_1$	8^4
f_2	$f_0 f_2$	8^4
$2f_0$	$< f_1 f_2, 2^2 f_0 >$	4^6
$2f_1$	$< f_0 f_1, 2^2 f_2 >$	4^4
$2f_2$	$< f_0 f_2, 2^2 f_1 >$	4^4
$2^2 f_0$	$< f_1 f_2, 2 f_0 >$	2^6
$2^2 f_1$	$< f_0 f_1, 2 f_2 >$	2^4
$2^2 f_2$	$< f_0 f_2, 2 f_1 >$	2^4
$f_0 f_1$	f_1	8^3
$f_0 f_2$	f_2	8^3
$f_1 f_2$	f_0	8
$2 f_0 f_1$	$< f_1, 2^2 f_0 f_2 >$	4^3
$2 f_0 f_2$	$< f_2, 2^2 f_0 f_1 >$	4^3
$2 f_1 f_2$	$< f_0, 2^2 f_1 f_2 >$	4
$2^2 f_1 f_2$	$< f_0, 2 f_1 f_2 >$	2
$2^2 f_0 f_1$	$< f_1, 2 f_0 f_2 >$	2^3
$2^2 f_0 f_2$	$< f_2, 2 f_0 f_1 >$	2^3
$< f_0, 2 f_1 f_2 >$	$2^2 f_1 f_2$	$8^6.4$
$< f_1, 2 f_0 f_2 >$	$2^2 f_0 f_1$	$8^4.4^3$
$< f_2, 2 f_0 f_1 >$	$2^2 f_0 f_2$	$8^4.4^3$
$< f_0 f_1, 2 f_2 >$	$2^2 f_1$	$8^3.4^4$
$< f_0 f_2, 2 f_1 >$	$2^2 f_2$	$8^3.4^4$

Example 3.2.2. *(Cyclic $\mathbb{Z}_{16}$-codes of length 7).*
$x^7 - 1 = (x-1)(15 + 13x + 14x^2 + x^{3)})(15 + 10x + 11x^2 + x^3) = f_0 f_1 f_2$.
The number of cyclic codes $(4+1)^3 = 125$ *cyclic codes.*

$$f_0^*(x) = x f(x^{-1)} = x(x^{-1} - 1) = -f_0,\ f_1^*(x) = x^3 f(x^{-1)} = -f_2 \text{ and}$$
$$f_2^*(x) = x^3 f(x^{-1)} = -f_1.$$

Table Π*: Cyclic codes over* $\mathbb{Z}_{16}$*-codes of length* 7*.*

Code number	*Generator of the code*	*Generator of the dual code*	*Order of the code*
1	2	2^3	8^7
2	2^2	2^2	4^7
3	2^3	2	2^7
4	f_0	f_1f_2	16^6
5	f_1	f_0f_1	16^4
6	f_2	f_0f_2	16^4
7	$2f_0$	$< f_1f_2, 2^3f_0 >$	8^6
8	$2f_1$	$< f_0f_1, 2^3f_2 >$	8^4
9	$2f_2$	$< f_0f_2, 2^3f_1 >$	8^4
10	2^2f_0	$< f_1f_2, 2^2f_0 >$	4^6
11	2^2f_1	$< f_0f_1, 2^2f_2 >$	4^4
12	2^2f_2	$< f_0f_2, 2^2f_1 >$	4^4
13	2^3f_0	$< f_1f_2, 2f_0 >$	2^6
14	2^3f_1	$< f_0f_1, 2f_2 >$	2^4
15	2^3f_2	$< f_0f_2, 2f_1 >$	2^4
16	f_0f_1	f_1	16^3
18	f_0f_2	f_2	16^3
17	f_1f_2	f_0	16
19	$2f_0f_1$	$< f_1, 2^3f_0f_2 >$	8^3
20	$2f_0f_2$	$< f_2, 2^3f_0f_1 >$	8^3
21	$2f_1f_2$	$< f_0, 2^3f_1f_2 >$	8
22	$2^2f_1f_2$	$< f_0, 2^2f_1f_2 >$	4
23	$2^2f_0f_1$	$< f_1, 2^2f_0f_2 >$	4^3
24	$2^2f_0f_2$	$< f_2, 2^2f_0f_1 >$	4^3
25	$2^3f_1f_2$	$< f_0, 2f_1f_2 >$	2
26	$2^3f_0f_1$	$< f_1, 2f_0f_2 >$	2^3
27	$2^3f_0f_2$	$< f_2, 2f_0f_1 >$	2^3
28	$< f_0, 2f_1f_2 >$	$2^3f_1f_2$	$16^6.8$
29	$< f_0, 2^2f_1f_2 >$	$2^3f_1f_2$	$16^6.4$
30	$< f_0, 2^3f_1f_2 >$	$2f_1f_2$	$16^6.2$
31	$< 2f_0, 2^2f_1f_2 >$	$< 2^2f_1f_2, 2^3f_0 >$	$8^6.4$
32	$< 2f_0, 2^3f_1f_2 >$	$< 2f_1f_2, 2^3f_0 >$	$8^6.2$
33	$< 2^2f_0, 2^3f_1f_2 >$	$< 2f_1f_2, 2^2f_0 >$	$4^6.2$
34	$< f_1, 2f_0f_2 >$	$2^3f_0f_1$	$16^4.8^3$
35	$< f_1, 2^2f_0f_2 >$	$2^2f_0f_1$	$16^4.4^3$
36	$< f_1, 2^3f_0f_2 >$	$2f_0f_1$	$16^4.2^3$
37	$< 2f_1, 2^2f_0f_2 >$	$< 2f_2, 2^2f_0f_1 >$	$8^4.4^3$
38	$< 2f_1, 2^3f_0f_2 >$	$< 2f_0f_1, 2^3f_2 >$	$8^4.2^3$
39	$< 2^2f_1, 2^3f_0f_2 >$	$< 2f_0f_1, 2^2f_2 >$	$4^4.2^3$
40	$< f_2, 2f_0f_1 >$	$2^3f_0f_2$	$16^4.8^3$
41	$< f_2, 2^2f_0f_1 >$	$2^2f_0f_2$	$16^4.4^3$
42	$< f_2, 2^3f_0f_1 >$	$2f_0f_2$	$16^4.2^3$
43	$< 2f_2, 2^2f_0f_1 >$	$< 2^2f_0f_2, 2^3f_1 >$	$8^4.4^3$
44	$< 2f_2, 2^3f_0f_1 >$	$< 2f_0f_2, 2^3f_1 >$	$8^4.2^3$
45	$< 2^2f_2, 2^3f_0f_1 >$	$< 2f_0f_2, 2^2f_1 >$	$4^4.2^3$
46	$< f_0f_1, 2f_2 >$	2^3f_1	$16^3.8^4$

Table Π-*continued*

Cyclic codes over $\mathbb{Z}_{16}$*-codes of length* 7.

Code number	*Generator of the code*	*Generator of the dual code*	*Order of the code*
47	$< f_0f_1, 2^2f_2 >$	2^2f_1	$16^3.4^4$
48	$< f_0f_1, 2^3f_2 >$	$2f_1$	$16^3.2^4$
49	$< 2f_0f_1, 2^2f_2 >$	$< 2f_0f_2, 2^2f_1 >$	$8^3.4^4$
50	$< 2f_0f_1, 2^3f_2 >$	$< 2f_1, 2^3f_0f_2 >$	$8^3.2^4$
51	$< 2^2f_0f_1, 2^3f_2 >$	$< 2f_1, 2^2f_0f_2 >$	$4^3.2^4$
52	$< f_0f_2, 2f_1 >$	2^3f_2	$16^3.8^4$
53	$< f_0f_2, 2^2f_1 >$	2^2f_2	$16^3.4^4$
54	$< f_0f_2, 2^3f_1 >$	$2f_2$	$16^3.2^4$
55	$< 2f_0f_2, 2^2f_1 >$	$< 2^2f_2, 2^3f_0f_1 >$	$8^3.4^4$
56	$< 2f_0f_2, 2^3f_1 >$	$< 2f_2, 2^3f_0f_1 >$	$8^3.2^4$
57	$< 2^2f_0f_2, 2^3f_1 >$	$< 2f_2, 2^2f_0f_1 >$	$4^3.2^4$
58	$< f_1f_2, 2f_0 >$	2^3f_0	16.8^6
59	$< f_1f_2, 2^2f_0 >$	2^2f_0	16.4^6
60	$< f_1f_2, 2^3f_0 >$	$2f_0$	16.2^6
61	$< 2f_1f_2, 2^2f_0 >$	$< 2^2f_0, 2^3f_1f_2 >$	8.4^6
62	$< 2f_1f_2, 2^3f_0 >$	$< 2f_0, 2^3f_1f_2 >$	8.2^6
63	$< 2^2f_1f_2, 2^3f_0 >$	$< 2f_0, 2^2f_1f_2 >$	4.2^6
64	$< f_0f_1, 2f_0f_2 >$	$< f_1f_2, 2^3f_0f_1 >$	$16^3.8^3$
65	$< f_0f_1, 2^2f_0f_2 >$	$< f_1f_2, 2^2f_0f_1 >$	$16^3.4^3$
66	$< f_0f_1, 2^3f_0f_2 >$	$< f_1f_2, 2f_0f_1 >$	$16^3.2^3$
67	$< 2f_0f_1, 2^2f_0f_2 >$	$< f_1f_2, 2^2f_0f_1, 2^3f_0f_2 >$	$8^3.4^3$
68	$< 2f_0f_1, 2^3f_0f_2 >$	$< f_1f_2, 2f_0f_1, 2^3f_0f_2 >$	$8^3.2^3$
69	$< 2^2f_0f_1, 2^3f_0f_2 >$	$< f_1f_2, 2f_0f_1, 2^2f_0f_2 >$	$4^3.2^3$
70	$< f_0f_1, 2f_1f_2 >$	$< f_1f_0, 2^3f_1f_2 >$	$16^3.8$
71	$< f_0f_1, 2^2f_1f_2 >$	$< f_1f_0, 2^2f_1f_2 >$	$16^3.4$
72	$< f_0f_1, 2^3f_1f_2 >$	$< f_1f_0, 2f_1f_2 >$	$16^3.2$
73	$< 2f_0f_1, 2^2f_1f_2 >$	$< f_1f_0, 2^2f_1f_2, 2^3f_0f_2 >$	$8^3.4$
74	$< 2f_0f_1, 2^3f_1f_2 >$	$< f_1f_0, 2f_1f_2, 2^3f_0f_2 >$	$8^3.2$
75	$< 2^2f_0f_1, 2^3f_1f_2 >$	$< f_1f_0, 2f_1f_2, 2^2f_0f_2 >$	$4^3.2$
76	$< f_0f_2, 2f_0f_1 >$	$< f_1f_2, 2^3f_0f_2 >$	$16^3.8^3$
77	$< f_0f_2, 2^2f_0f_1 >$	$< f_1f_2, 2^2f_0f_2 >$	$16^3.4^3$
78	$< f_0f_2, 2^3f_0f_1 >$	$< f_1f_2, 2f_0f_2 >$	$16^3.2^3$
79	$< 2f_0f_2, 2^2f_0f_1 >$	$< f_1f_2, 2^2f_0f_2, 2^3f_0f_1 >$	$8^3.4^3$
80	$< 2f_0f_2, 2^3f_0f_1 >$	$< f_1f_2, 2f_0f_1, 2^3f_0f_2 >$	$8^3.2^3$
81	$< 2^2f_0f_2, 2^3f_0f_1 >$	$< f_1f_2, 2f_0f_2, 2^2f_0f_1 >$	$4^3.2^3$
82	$< f_0f_2, 2f_1f_2 >$	$< f_0f_1, 2f_1f_2 >$	$16^3.8$
83	$< f_0f_2, 2^2f_1f_2 >$	$< f_0f_2, 2^2f_1f_2 >$	$16^3.4$
84	$< f_0f_2, 2^3f_1f_2 >$	$< f_0f_2, 2f_1f_2 >$	$16^3.2$
85	$< 2f_0f_2, 2^2f_1f_2 >$	$< f_0f_2, 2^2f_1f_2, 2^3f_0f_1 >$	$8^3.4$
86	$< 2f_0f_2, 2^3f_1f_2 >$	$< f_0f_2, 2f_1f_2, 2^3f_0f_1 >$	$8^3.2$
87	$< 2^2f_0f_2, 2^3f_1f_2 >$	$< f_0f_2, 2f_1f_2, 2^2f_0f_1 >$	$4^3.2$
88	$< f_1f_2, 2f_1f_0 >$	$< 2f_0f_1, 2^3f_0f_2 >$	16.8^3
89	$< f_1f_2, 2^2f_1f_0 >$	$< f_0f_1, 2^2f_0f_2 >$	16.4^3
90	$< f_1f_2, 2^3f_1f_0 >$	$< f_0f_1, 2f_0f_2 >$	16.2^3
91	$< 2f_1f_2, 2^2f_1f_0 >$	$< f_0f_1, 2^2f_0f_2, 2^3f_1f_2 >$	8.4^3
92	$< 2f_1f_2, 2^3f_1f_0 >$	$< f_0f_1, 2f_0f_2, 2^3f_1f_2 >$	8.2^3
93	$< 2^2f_1f_2, 2^3f_1f_0 >$	$< f_0f_1, 2f_0f_2, 2^2f_1f_2 >$	4.2^3

Table Π-continued

Cyclic codes over $\mathbb{Z}_{16}$-codes of length 7.

Code number	Generator of the code	Generator of the dual code	Order of the code
94	$< f_1f_2, 2f_0f_2 >$	$< f_0f_2, 2^3f_0f_1 >$	16.8^3
95	$< f_1f_2, 2^2f_0f_2 >$	$< f_0f_2, 2^2f_0f_1 >$	16.4^3
96	$< f_1f_2, 2^3f_0f_2 >$	$< f_0f_2, 2f_0f_1 >$	16.2^3
97	$< 2f_1f_2, 2^2f_0f_2 >$	$< f_0f_2, 2f_0f_1, 2^3f_1f_2 >$	8.4^3
98	$< 2f_1f_2, 2^3f_0f_2 >$	$< f_0f_2, 2f_0f_1, 2^3f_1f_2 >$	8.2^3
99	$< 2^2f_1f_2, 2^3f_0f_2 >$	$< f_0f_2, 2f_0f_1, 2^2f_1f_2 >$	4.2^3
100	$< f_0f_1, 2f_0f_2, 2^2f_1f_2 >$	$< 2^2f_1f_2, 2^3f_0f_1 >$	$16^3.8^3.4$
101	$< f_0f_1, 2^2f_0f_2, 2^3f_1f_2 >$	$< 2f_1f_2, 2^2f_0f_1 >$	$16^3.4^3.2$
102	$< 2f_0f_1, 2^2f_0f_2, 2^3f_1f_2 >$	$< 2f_1f_2, 2^2f_0f_1, 2^3f_0f_2 >$	$8^3.4^3.2$
103	$< f_0f_1, 2f_1f_2, 2^2f_0f_2 >$	$< 2^2f_1f_0, 2^3f_1f_2 >$	$16^3.8.4^3$
104	$< f_0f_1, 2^2f_1f_2, 2^3f_0f_2 >$	$< 2f_0f_1, 2^2f_1f_2 >$	$16^3.4.2^3$
105	$< 2f_0f_1, 2^2f_1f_2, 2^3f_0f_2 >$	$< 2f_0f_1, 2^2f_1f_2, 2^3f_0f_2 >$	$8^3.4.2^3$
106	$< f_0f_2, 2f_0f_1, 2^2f_1f_2 >$	$< f_0f_1, 2f_0f_2, 2^2f_1f_2 >$	$16^3.8^3.4$
107	$< f_0f_2, 2^2f_0f_1, 2^3f_1f_2 >$	$< 2f_1f_2, 2^2f_0f_2 >$	$16^3.4^3.2$
108	$< f_0f_2, 2f_1f_2, 2^2f_1f_0 >$	$< 2^2f_0f_2, 2^3f_0f_1 >$	$16^3.8.4^3$
109	$< f_0f_2, 2^2f_1f_2, 2^3f_0f_1 >$	$< 2f_0f_2, 2^2f_1f_2 >$	$16^3.4.2^3$
110	$< 2f_0f_2, 2^2f_0f_1, 2^3f_1f_2 >$	$< 2f_1f_2, 2^2f_0f_2, 2^3f_0f_1 >$	$8^3.4^3.2$
111	$< 2f_0f_2, 2^2f_1f_2, 2^3f_1f_0 >$	$< 2f_0f_2, 2^2f_1f_2, 2^3f_0f_1 >$	$8^3.4.2^3$
112	$< f_1f_2, 2f_0f_1, 2^2f_0f_2 >$	$< 2^2f_0f_1, 2^3f_0f_2 >$	$16.8^3.4^3$
113	$< f_1f_2, 2^2f_0f_1, 2^3f_0f_2 >$	$< 2f_0f_1, 2^2f_0f_2 >$	$16.4^3.2^3$
114	$< 2f_1f_2, 2^2f_0f_1, 2^3f_0f_2 >$	$< 2f_0f_1, 2^2f_0f_2, 2^3f_1f_2 >$	$8.4^3.2^3$
115	$< f_1f_2, 2f_0f_2, 2^2f_0f_1 >$	$< 2^2f_0f_2, 2^3f_0f_1 >$	$16.8^3.4^3$
116	$< f_1f_2, 2^2f_0f_2, 2^3f_0f_1 >$	$< 2f_0f_2, 2^2f_0f_1 >$	$16.4^3.2^3$
117	$< 2f_1f_2, 2^2f_0f_2, 2^3f_0f_1 >$	$< 2f_0f_2, 2^2f_0f_1, 2^3f_1f_2 >$	$8.4^3.2^3$
118	$< f_0f_1, 2f_0f_2, 2^3f_1f_2 >$	$< 2f_1f_2, 2^3f_0f_1 >$	$16^3.8^3.2$
119	$< f_0f_1, 2f_2f_1, 2^3f_0f_2 >$	$< 2f_1f_0, 2^3f_1f_2 >$	$16^3.8.2^3$
120	$< f_0f_2, 2f_0f_1, 2^3f_1f_2 >$	$< 2f_1f_2, 2^3f_0f_2 >$	$16^3.8^3.2$
121	$< f_0f_2, 2f_2f_1, 2^3f_0f_1 >$	$< 2f_0f_2, 2^3f_1f_2 >$	$16^3.8.2^3$
122	$< f_1f_2, 2f_0f_1, 2^3f_0f_2 >$	$< 2f_0f_1, 2^3f_0f_2 >$	$16.8^3.2^3$
123	$< f_1f_2, 2f_0f_2, 2^3f_0f_1 >$	$< 2f_0f_2, 2^3f_0f_1 >$	$16.8^3.2^3$

In Table Π we list all nontrivial cyclic $\mathbb{Z}_{16}$-codes of length 7 along with their duals, orders.

Example 3.2.3. *Code No.*113 *in Table* Π *has* $F_0 = 1,\ F_1 = f_0,\ F_2 = 1,\ F_3 = f_2,\ F_4 = f_1$. *Hence its dual is*
$< \hat{F}_0^*, 2\hat{F}_4^*, 2^2\hat{F}_3^*, 2^3\hat{F}_2^* > = < \hat{F}_1^*\hat{F}_2^*\hat{F}_3^*\hat{F}_4^*, 2\hat{F}_0^*\hat{F}_1^*\hat{F}_2^*\hat{F}_3^*, 2^2\hat{F}_0^*\hat{F}_1^*\hat{F}_2^*\hat{F}_4^*, 2^3\hat{F}_0^*\hat{F}_1^*\hat{F}_3^*\hat{F}_4^* >$
$< f_0^*f_1^*f_2^*, 2f_0^*f_2^*, 2^2f_0^*f_1^*, 2^3f_0^*f_1^*f_2^* > = < 2f_0f_1, 2^2f_0f_2 >$.
*Code No.*114 *has* $F_0 = 1,\ F_1 = 1,\ F_2 = f_0,\ F_3 = f_2,\ F_4 = f_1$. *Hence its dual is* $< f_0^*f_1^*f_2^*, 2f_0^*f_2^*, 2^2f_0^*f_1^*, 2^3f_1^*f_2^* > = < 2f_0f_1, 2^2f_0f_2, 2^3f_1f_2 >$. *Code*

No.99 has $F_0 = f_2,\ F_1 = 1,\ F_2 = 1,\ F_3 = f_0,\ F_4 = f_1$. *Hence its dual is* $< f_0^* f_1^*, 2f_0^* f_2^*, 2^2 f_2^* f_1^*, 2^3 f_0^* f_1^* f_2^* >=< 2f_0 f_2, 2f_0 f_1, 2^2 f_1 f_2 >$.

Code No.123 has $F_0 = 1,\ F_1 = f_0,\ F_2 = f_1,\ F_3 = 1,\ F_4 = f_2$. *Hence its dual is* $< f_0^* f_1^* f_2^*, 2f_0^* f_1^*, 2^2 f_0^* f_1^* f_2^*, 2^3 f_0^* f_2^* >=< 2f_0 f_2, 2^3 f_0 f_1 >$.

3.2.1 Introduction to codes over $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$

The general case of such rings over $\mathbb{R}_{k,p} = \mathbb{F}_p[u]/(w(u)^k)$, where $k > 1$, p is any prime and $w(u)$ is an irreducible polynomial of degree $m \geq 1$ over $\mathbb{F}_p$ was studied in [10]. The ring $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$ is a special of these rings when $w(u) = u$.

Throughout this thesis, we let $\mathbb{R}_{k,p}$ denote this ring $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$. Two words x, y are called orthogonal if $x.y = 0$. For a code C over $\mathbb{R}_{k,p}$, its dual code $C^\perp$ is the set of words over $\mathbb{R}_{k,p}$ that are orthogonal to all codewords of C, i.e.,

$$C^\perp = \{x : x.y = 0, \forall y \in C\}.$$

A code C is called self-dual if $C = C^\perp$.

Definition 3.2.1. [16] A cyclic code of length n over $\mathbb{R}_{k,p}$ is a linear code with the property that if $(c_0, c_1, \ldots, c_n) \in \mathcal{C}$ then $(c_1, c_2, \ldots, c_n, c_0) \in \mathcal{C}$. We assume that p is not divisible by n, and we represent codeword by polynomials, then the cyclic codes are ideals of the ring

$$\mathbf{R}_n = \mathbb{R}_{k,p}[x]/(x^n - 1),$$

where $\mathbb{R}_{k,p}[x]$ be the ring of polynomials over $\mathbb{R}_{k,p}$.

Definition 3.2.2. [16] Let $\mathbb{R}_{k,p}[x]$ be the ring of polynomials over $\mathbb{R}_{k,p}$. We have a natural homomorphic mapping, from $\mathbb{R}_{k,p}$ to its residue field $\mathbb{F}_p$. For any $a \in \mathbb{R}_{k,p}$, let $\hat{a}$ denote the polynomial reduction modulo u.

Now define a polynomial reduction mapping $\alpha : \mathbb{R}_{k,p}[x] \longrightarrow \mathbb{F}_p[x]$ in the obvious way:

$$f(x) = \sum_{i=0}^{r} a_i x^i \xrightarrow{\alpha} \sum_{i=0}^{r} \hat{a}_i x^i.$$

A monic polynomial f over $\mathbb{R}_{k,p}[x]$ is said to be a basic irreducible polynomial if its projection $\alpha(f)$ is irreducible over $\mathbb{F}_p[x]$.
The Galois ring of $\mathbb{R}_{k,p}$ denoted as $\mathbf{GR}(\mathbb{R}_{k,p}, r)$ is defined as $\mathbb{R}_{k,p}[x]/ < f(x) >$, where $f(x)$ is a basic monic irreducible polynomial of degree r over $\mathbb{R}_{k,p}$. Hence $\mathbf{GR}(\mathbb{R}_{k,p}, r)$ is a module over $\mathbb{R}_{k,p}$.

The basic monic irreducible polynomial of degree r over $\mathbb{R}_{k,p}$ can be lifted from a monic irreducible polynomial over $\mathbb{F}_p$. The trick is to consider a monic irreducible polynomial over $\mathbb{F}_p$ which is a subring of $\mathbb{R}_{k,p}$.
Any monic irreducible polynomial over the subring is irreducible polynomial over the ring. Thus any monic irreducible polynomial $f(x)$ over $\mathbb{F}_p[x]$ is a basic monic irreducible polynomial over $\mathbb{R}_{k,p}$.

3.3 Cyclic codes over $\mathbb{R}_{k,p} = \mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$

Cyclic codes over $\mathbb{R}_{k,p}$ are studied in [16]. There is a lot of similarity between the structure of codes over $\mathbb{R}_{k,p}$ and the structure of codes over $\mathbb{F}_2 + u\mathbb{F}_2$.

Lemma 3.3.1. *[16] If $x^n - 1 = f_1 f_2 \ldots f_r$, where f_i are basic irreducible and pairwise-coprime, then this factorization is unique.*

Lemma 3.3.2. *[16] The only ideals of $\mathbf{GR}(\mathbb{R}_{k,p}, r)$ are $< 0 >$, $< 1 >$, $\ldots$, $< u^{k-1} >$.*

In Lemma 3.3.2, we have given the structure of prime ideals in $\mathbb{R}_{k,p}[x]/ < f(x) >$. Now we study the structure of all ideals in $\mathbf{R}_n$.

Lemma 3.3.3. *[16] Let p is not divisible by n and $x^n - 1 = f_1 f_2 \ldots f_r$, where the $f_i (1 \leq i \leq r)$ are basic irreducible and pairwise-coprime polynomials. Let $\hat{f}_i$ denote the product of all f_j except f_i . Then any ideal in the ring is a sum of $< u^j \hat{f}_i >$, $0 \leq j \leq k-1$, $1 \leq i \leq r$.*

Proof. The proof is similar to the proof given in Lemma 3.2.2 for ideals in $(\mathbb{F}_2 + u\mathbb{F}_2)/ < x^n - 1 >$ as in this case also, ideals in $\mathbf{R}_n$ can be written as:

$$I \cong I_1 \oplus I_2 \oplus \ldots \oplus I_r,$$

where $I_i, i = 1,\ 2,\ 3,\ \ldots,\ r$, is an ideal of the Galois ring $\mathbb{R}_{k,p}[x]/ < f_i >$. The only an ideals in $\mathbb{R}_{k,p}[x]/ < f_i >$ are $< 0 >$ *or* $< u^j >$, $0 \leq j \leq k-1$. But then I_i will correspond to $< u^j \hat{f}_i >$ in $\mathbf{R}_n$. In any case, the ideal I is a sum of $< u^j \hat{f}_i >$. □

Corollary 3.3.4. *[16] The number of cyclic codes over $\mathbb{R}_{k,p}$ of length n is $(k+1)^r$, where r is the number of basic irreducible polynomial factors in $x^n - 1$ over $\mathbb{R}_{k,p}$.*

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

Theorem 3.3.5. *[16] Suppose C is a cyclic code of length n over $\mathbb{R}_{k,p}$, p is not divisible by n, then there are unique monic polynomials $F_0, F_1, \ldots, F_k$ such that $C =< \hat{F}_1, u\hat{F}_2, \ldots, u^{k-1}\hat{F}_k >$, where $F_0F_1 \ldots F_k = x^n - 1$, and $|C| = p^s$, where $s = \sum_{i=0}^{k-1}(k-i)\deg F_{i+1}$.*

Proof. By Lemma 3.3.1, $x^n - 1$ has a unique factorization into basic irreducible polynomials $x^n - 1 = f_1 f_2 \ldots f_r$. By Theorem 3.3.2, C is a sum of some of $(u^j \hat{f}_i)$. By rearranging $f_1,\ f_2,\ \ldots,\ f_r$, we can assume that C is the sum of

$$(\hat{f}_{t_1+1}),\ (\hat{f}_{t_1+2}),\ \ldots,\ (\hat{f}_{t_1+t_2});\ (u\hat{f}_{t_1+t_2+1}), \ldots, (u\hat{f}_{t_1+t_2+t_3});$$
$$\ldots (u^{k-1}\hat{f}_{t_1+t_2+\ldots+t_k+1}), \ldots, (u^{k-1}\hat{f}_r).$$

where $t_1, t_2, \ldots, t_k \geq 0$, and $t_1 + t_2 + \ldots, t_k + 1 \leq r$. Let $t_0 = 1$ and t_{k+1} be a nonnegative integer such that $t_1 + t_2 + \ldots + t_{k+1} = r$. For $0 \leq i \leq k$, define

$$F_i = \begin{cases} 1 & t_{i+1} = 0; \\ f_{t_0+t_1+\ldots+t_i+1} \ldots f_{t_0+t_1+\ldots+t_i+1} & t_{i+1} \neq 0. \end{cases}$$

then it is easy to show that $C =< \hat{F}_1, u\hat{F}_2, \ldots, u^{k-1}\hat{F}_k >$.
If each $F_i \neq 1$ $(1 \leq i \leq k)$, they are pairwise-coprime and thus

$$C = (\hat{F}_1) \oplus (u\hat{F}_2) \oplus \ldots \oplus (u^{k-1}\hat{F}_k).$$

Therefore,
$|C| = |(\hat{F}_1)||(u\hat{F}_2)| \ldots |(u^{k-1}\hat{F}_k)| = p^{k(n-deg\hat{F}_1)}p^{(k-1)(n-deg\hat{F}_2)} \ldots p^{(n-deg\hat{F}_k)} = p^s$,
where $s = \sum_{i=0}^{k-1}(k-i)\deg F_{i+1}$. □

Theorem 3.3.6. *[16] Let C be a cyclic code of length n over $\mathbb{R}_{k,p}$, p is not divisible by n. Then there exist polynomials $f_0,\ f_1,\ \ldots,\ f_{k-1}$ such that*

$$f_{k-1}|f_{k-2}|\ldots|f_0|x^n-1$$

and

$$C =< f_0, uf_1, u^2f_2, \ldots, u^{k-1}f_{k-1} > .$$

Proof. By Theorem 3.3.5, there exist a family of pairwise coprime monic polynomials $F_0, F_1, \ldots, F_k$ such that $F_0F_1\ldots F_k = x^n-1$ and

$$C =< \hat{F}_1, u\hat{F}_2, \ldots, u^{k-1}\hat{F}_k >.$$

Define

$$f_i = \begin{cases} F_0F_{i+2}\ldots F_k, & 0 \le i \le k-2 \\ F_0, & i = k-1, \end{cases}$$

Then $f_{k-1}|f_{k-2}|\ldots|f_0|x^n-1$. Also for all i, $0 \le i \le k-1$,

$$u^i\hat{F_{i+1}} = u^iF_0F_1\ldots F_iF_{i+2}\ldots F_k = u^if_iF_1F_2\ldots F_i.$$

Hence, $C \subset< f_0, uf_1, \ldots, u^{k-1}f_{k-1} > .$

To prove the reverse inclusion we first observe that $f_0 \in C$. For F_1 and F_2 are coprime, there exist polynomials $a(x),\ b(x) \in \mathbb{R}_{k,p}$ such that

$$1 = a(x)F_1(x) + b(x)F_2(x).$$

Thus, $uf_1 = uF_0F_3\ldots F_k = ua(x)F_0F_1F_3\ldots F_k + ub(x)f_0$
$= ua(x)\hat{F}_2 + ub(x)f_0 \in C.$

Continuing this process, we obtain $u^if_i \in C$ for all i, $0 \le i \le k-1$.

Thus, we have $C =< f_0, uf_1, \ldots, u^{k-1}f_{k-1} > .$

□

Cyclic Dual Codes

Recall that, for a code C over a ring $\mathbb{R}_{k,p}$ (or an $\mathbb{R}_{k,p}$-code), a code is called self-dual if it is its own dual. For a polynomial f of degree k, f^* will denote its reciprocal polynomial $x^kf(x^{-1})$.

Before we go on to produce generators for the dual codes, we need to state the following well-known results [16]

Lemma 3.3.7. *[16] The number of elements in any nonzero linear code C over $\mathbb{R}_{k,p}$ is p^s. Furthermore, the dual code $C^\perp$ has p^t codewords where $s + t = kn$.*

Theorem 3.3.8. *[16] Suppose p is prime not dividing n and*

$$C =< \hat{F}_1, u\hat{F}_2, \ldots, u^{k-1}\hat{F}_k >.$$

where $F_0F_1 \ldots F_k = x^n - 1$, then

$$C^\perp =< \hat{F}_0^*, u\hat{F}_k^*, u^2\hat{F}^*{}_{k-1}, \ldots, u^{k-1}\hat{F}_2^* >$$

Proof. Let $C_1 =< \hat{F}^*{}_0, u\hat{F}^*{}_k, u^2\hat{F}^*{}_{k-1}, \ldots, u^{k-1}\hat{F}^*{}_2 >$. For
$i,\ j \in \{0, 1, \ldots, t-1\}$, if $i + 1 = k - j + 1$, i.e., $i = k - j$, then
$(u^i\hat{F}_{i+1})(u^j\hat{F}^*{}_{k-j+1})^* = 0$; and if $i + 1 \neq k - j + 1$, i.e., $i \neq k - j$, then
$< x^n - 1 > |(u^i\hat{F}_{i+1})(u^j\hat{F}^*{}_{k-j+1})^*$.
In any case, we have $(u^i\hat{F}_{i+1})(u^j\hat{F}^*{}_{k-j+1})^* \equiv 0(modx^n - 1)$. Thus $C_1 \subset C^\perp$
and $|C_1| = p^r$, where $r = \Sigma_{i=1}^k i \deg F_{i+1}$ with $F_{k+1} = F_0$.
On the other hand, by Lemma 3.3.7, $|C^\perp| = p^t$, where $t + s = kn$.
By Theorem 3.3.5, we have $s = \Sigma_{i=0}^{k-1}(k - i) \deg F_{i+1}$.
It follows that $t = \Sigma_{i=1}^k i \deg F_{i+1} = r$ (with $F_{k+1} = F_0$).
Hence, $C^\perp = C_1$, and the proof is complete. □

Chapter 4

Idempotents of cyclic codes over rings of four elements

In this chapter we study the idempotent generator of cyclic codes over $\mathbb{Z}_4$ and $\mathbb{R}_{2,2} = F_2 + uF_2$. The following result was proved in [1], [2], [3], [22], [24].

4.1 Generating idempotents of cyclic codes over $\mathbb{Z}_4$

An idempotent in $\mathbb{Z}_4[x]$ is defined to be a polynomial $e(x)$ such that

$$e(x)^2 = e(x) \ (mod\ x^n - 1).$$

Theorem 4.1.1. *[22] Let C be a $\mathbb{Z}_4$-cyclic code of odd length n*

(i) If $C =< f >$, where $fg = x^n - 1$ for some g, then C has idempotent generator in $\mathbb{Z}_4$.

(ii) If $C =< 2f >$, where f divides $x^n - 1$, then $C =< 2e >$, where e is binary generator of (μf).

(iii) If $C =< fh, 2fg >$, where $fgh = x^n - 1$, then $C =< e, 2\nu >$ where e is an idempotent in $\mathbb{Z}_4$, ν is an idempotent in $\mathbb{Z}_2$.

Proof. In (i), because f and g are coprime, there are a, b in $\mathbb{Z}_4[x]$ such that, $fa + gb = 1$. Set $e = fa$, then

$$e = 1 - gb \text{ and } e^2 = e - \text{geb} = e - gfab = e \ (mod\ x^n - 1).$$

$fe = f-$fgb$= f(\bmod x^n - 1)$. Hence $< e >=< f >$.

In (i), let $\mu : \mathbb{Z}_4[x] \longrightarrow \mathbb{F}_2[x]$ be a surjective ring homomorphism with $\ker(2) = \{2s(x) | s(x) \in \mathbb{Z}_4[x]\}$, such that

$$\mu(f(x)) = f(x)(mod\ 2);$$

that is, μ is determined by $\mu(0) = \mu(2) = 0$, $\mu(1) = \mu(3) = 1$,
and $\mu(x) = x$.
Since $f/x^n - 1$ in $\mathbb{Z}_4$, μf divides $x^n - 1$ in $\mathbb{F}_2[x]$.

By (i) $< 2f >=< 2e >$ follows from the fact that $< uf >=< u\mu f >$ and (μf) has binary idempotent e.

In (iii), It is clear from (i) and (ii) that $< fh >$ has idempotent e in $\mathbb{Z}_4$ and $< \mu fg >$ has binary idempotent ν.
Therefore $< fh, 2fg >=< e, 2\nu >$.

□

The next theorem is also in [24]

Theorem 4.1.2. *If a $\mathbb{Z}_4$-cyclic code C has the idempotent generator $e(x)$, then $C^\perp$ has idempotent generator $1 - e(x^{-1})$.*

Proof. Since $e(x)(1 - e(x)) = 0$ in $\mathfrak{R}_n$, by Theorem 2.2.9, then
$e(x)$ is orthogonal to $1 - e(x^{-1})$. That is, $1 - e(x^{-1}) \in C^\perp$.
On the other hand, if C has generator polynomial g and $gh = x^n - 1$, then
$C^\perp$ has generator polynomial (h^*).
Since $1 - e(x)$ is the idempotent generator of (h), and the map:$x \longrightarrow x^{-1}$
sends (h) to (h^*), $1 - e(x^{-1})$ is the idempotent generator of $C^\perp$. □

Theorem 4.1.3. *[24] Let C_1 and C_2 be cyclic codes with idempotent generators e_1, e_2, then $C_1 \bigcap C_2$ has the idempotent generator e_1e_2 and $C_1 + C_2$ has the idempotent generator $e_1 + e_2 - e_1e_2$.*

Proof. Clearly $e_1(x)e_2(x)$ is in $C_1 \bigcap C_2$ and

$$(e_1(x)e_2(x))^2 = (e_1(x))^2(e_2(x))^2 = e_1(x)e_2(x).$$

So $e_1(x)e_2(x)$ is an idempotent in $C_1 \bigcap C_2$.
If $c(x) \in C_1 \bigcap C_2$, then $e_1(x)e_2(x)c(x) = e_1(x)c(x) = c(x)$.
So $e_1(x)e_2(x)$ is an idempotent for $C_1 \bigcap C_2$.
Clearly $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is in $C_1 + C_2$ and

$$(e_1(x) + e_2(x) - e_1(x)e_2(x))^2 = e_1(x) + e_2(x) - e_1(x)e_2(x).$$

So $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is an idempotent in $C_1 + C_2$.
If $c(x) \in C_1 + C_2$ then $c(x) = c_1(x) + c_2(x)$, for some $c_1(x) \in C_1$ and $c_2(x) \in C_2$.
Hence

$$(c_1(x) + c_2(x))(e_1(x) + e_2(x) - e_1(x)e_2(x)) = c_1(x) + c_2(x).$$

So $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is an idempotent. □

For odd n, $x^n - 1 = f_1 f_2 \dots f_r$ is a product of basic irreducible, pairwise coprime polynomials. We study that there are binary idempotents $e_1,\ e_2,\ \dots,\ e_r$ with $< \mu \hat{f_i} > = < e_i >$ such that

$$e_1 + e_2 + \dots + e_r = 1 \text{ and } e_i e_j = 0, \text{ if } i \neq j.$$

These e_i are called primitive idempotent and any binary idempotent is the sum of some e_i.
In $\mathbb{Z}_4$, let $\theta_i = e_i^2$, for $i = 1, 2, \dots, r$. It was shown in [24], that the θ_i are $\mathbb{Z}_4$ idempotents. Moreover, it can also be shown that $\sum_{i=1}^{r} \theta_i = 1$ and $\theta_i \theta_j = 0$ for $i \neq j$.

4.2 Generating idempotents of cyclic codes over $\mathbb{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$

Theorem 4.2.1. *Let C be a cyclic code over $\mathbb{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$ of odd length n*

(i) If $C =< f >$, where $fg = x^n - 1$ for some g, then C has idempotent generator in $\mathbb{R}_{2,2}$.

(ii) If $C =< uf >$, where f divides $x^n - 1$, then $C =< ue >$ where e is binary generator of $< \phi f >$.

(iii) If $C =< fh, ufg >$, where $fgh = x^n - 1$, then $C =< e, uv_1 >$where e is an idempotent in $\mathbb{R}_{2,2}$, v_1 is an idempotent in $\mathbb{F}_2$.

Proof. In (i), because f and g are coprime, there are a, b in $\mathbb{R}_{2,2}[x]$ such that, $fa + gb = 1$. Set $e = fa$, then

$$e = 1 - gb \text{ and } e^2 = e - \text{geb} = e - gfab = e(\mod x^n - 1).$$

$fe = f - \text{fgb} = f(\mod x^n - 1)$. Hence $< e >=< f >$;

In (ii), let $\phi : \mathbb{R}_{2,2}[x] \longrightarrow \mathbb{F}_2[x]$ be a natural homomorphic mapping from $\mathbb{R}_{2,2}$ to its residue field $\mathbb{F}_2$. For any $a \in \mathbb{R}_{2,2}$, let $\hat{a}$ donate the polynomial reduction modulo u such that:

$$f(x) = \sum_{i=0}^{n} a_i x^i \xrightarrow{\phi} \sum_{i=0}^{n} \hat{a}_i x^i.$$

Since $f/(x^n - 1)$ in $\mathbb{R}_{2,2}[x]$, ϕf divides $x^n - 1$ in $\mathbb{F}_2[x]$.

By (i) $< uf >=< ue >$ follows from the fact that $< uf >=< u\phi(f) >$ and (ϕf) has binary idempotent e.

In (iii), It is clear from (i) and (ii) that $< fh >$ has idempotent e in $\mathbb{R}_{2,2}$ and $< \phi(fg) >$ has binary idempotent v_1.
Therefore $< fh, ufg >=< e, uv_1 >$.

□

The idempotent of the dual code of a code C can be described in terms of the idempotent of C. If $a(x) = a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} \in \mathbb{R}_{2,2}[x]$, set

$$a^*(x) = x^{m-1}a(1/x) = a_0x^{m-1} + \ldots + a_{m-1}.$$

Then the following holds.

Theorem 4.2.2. *If a code C over $\mathbb{R}_{2,2}$ has the idempotent generator $e(x)$, then $C^\perp$ has idempotent generator $1 - e(x^{-1})$.*

Proof. The proof is similar to proof given in Theorem 4.1.2 □

4.3 Examples

In this section we shall obtain nontrivial cyclic $\mathbb{Z}_4$-codes of length 7 and nontrivial cyclic $\mathbb{F}_2 + u\mathbb{F}_2$-codes of length 7.

Example 4.3.1. *[3] $\mathbb{Z}_4$ cyclic code of length 7*
$x^7 - 1 = (x-1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3) = f_0f_1f_2.$
Let

$$e_1 = x + x^2 + x^4 \text{ and } e_2 = x^3 + x^5 + x^6$$

be binary idempotents. Then we know that in the binary case,

$$h = 1 + e_1 + e_2$$

is the idempotent generator of $\mu f_1 \mu f_2$,

$$1 + e_1$$

is idempotent generator of $\mu f_0 \mu f_2$, and

$$1 + e_2$$

is idempotent generator of $\mu f_0 \mu f_1$.

It is easy to verify that $\theta_0 = h^2 = 3h$ is an idempotent of f_1f_2,
$\theta_1 = (1 + e_1)^2 = 1 + 3e_1 + 2e_2$ is an idempotent of f_0f_2, and
$\theta_2 = (1 + e_2)^2 = 1 + 3e_2 + 2e_1$ is an idempotent of f_0f_1.

By Theorem(4.1.2)

$1 - \theta_0(x^{-1}) = 1 - 3h = e_1 + e_2 + 2$ is an idempotent generator of f_0,
$1 - \theta_1(x^{-1}) = 1 - \theta_2 = e_2 + 2e_1$ is an idempotent generator of f_2,
also $1 - \theta_2(x^{-1}) = 1 - \theta_1 = e_1 + 2e_2$ is an idempotent generator of f_1.

From this we can list some non-trivial cyclic codes along with their idempotent generators and their dual codes (see Table 4.1).

Table 4.1

Idempotents of cyclic codes over $\mathbb{Z}_4$ *of length* 7.

Codes number	*Generator code*	*Idempotent of generator code*
1	f_0	$e_1 + e_2 + 2$
2	f_1	$e_1 + 2e_2$
3	f_2	$e_2 + 2e_1$
4	$2f_0$	$2e_1 + 2e_2$
5	$2f_2$	$2e_2$
6	$2f_1$	$2e_1$
7	2	2
8	$f_1 f_2$	$3h$
9	$f_0 f_1$	$1 + 3e_2 + 2e_1$
10	$f_0 f_2$	$1 + 3e_1 + 2e_2$
11	$2f_1 f_2$	$2h$
12	$2f_0 f_1$	$2(1 + e_2)$
13	$2f_0 f_2$	$2(1 + e_1)$
14	$< f_1 f_2, 2f_0 f_1 >$	$< 3h, 2(1 + e_2) >$
15	$< f_1 f_2, 2f_0 f_2 >$	$< 3h, 2(1 + e_1) >$
16	$< f_0 f_1, 2f_1 f_2 >$	$< 1 + 3e_2 + 2e_1, 2h >$
17	$< f_0 f_2, 2f_1 f_2 >$	$< 1 + 3e_1 + 2e_2, 2h >$

Example 4.3.2. $\mathbb{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2$ *cyclic code of length* 7
$x^7 - 1 = (x + \overline{u})(x^3 + ux^2 + x + \overline{u})(x^3 + \overline{u}x^2 + ux + \overline{u}) = f_1 f_2 f_3$.
Let

$$e_1 = x + x^2 + x^4 \quad \textit{and} \quad e_2 = x^3 + x^5 + x^6$$

be binary idempotent. Then we know that in the binary case,

$$h = 1 + e_1 + e_2$$

is the idempotent generator of $\phi f_2 \phi f_3$,

$$1 + e_1$$

is idempotent generator of $\phi f_1 \phi f_3$, *and*

$$1 + e_2$$

is idempotent generator of $\phi f_1 \phi f_2$.

It is easy to verify that $\xi_0 = h^2 = \overline{u}h$ *is an idempotent of* f_2f_3,
$\xi_1 = (1+e_1)^2 = 1+\overline{u}e_1+ue_2$ *is an idempotent of* f_1f_3, *and*
$\xi_2 = (1+e_2)^2 = 1+\overline{u}e_2+ue_1$ *is an idempotent of* f_1f_2.
By Theorem (4.2.2)
$1-\xi_0(x^{-1}) = 1-\overline{u}h = e_1+e_2+u$ *is an idempotent generator of* f_1,
$1-\xi_1(x^{-1}) = 1-\xi_2 = e_2+ue_1$ *is an idempotent generator of* f_3,
also $1-\xi_2(x^{-1}) = 1-\xi_1 = e_1+ue_2$ *is an idempotent generator of* f_2.

From this we can list all non-trivial cyclic codes along with their idempotent generators and their dual codes (see Table 4.2).

Table 4.2

Idempotents of cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$ *of length* 7.

Generator code	*Idempotent of generator code*	*Dual generator code*	*Idempotent of dual generated code*
f_1	e_1+e_2+u	f_2f_3	$\overline{u}h$
f_3	e_2+ue_1	f_1f_3	$1+\overline{u}e_1+ue_2$
f_2	e_1+ue_2	f_1f_2	$1+\overline{u}e_2+ue_1$
uf_1	ue_1+ue_2	$< f_2f_3, uf_1 >$	$< \overline{u}h, ue_1+ue_2 >$
uf_3	ue_2	$< f_1f_3, uf_2 >$	$< 1+\overline{u}e_1+ue_2, ue_1 >$
uf_2	ue_1	$< f_1f_2, uf_3 >$	$< 1+\overline{u}e_2+ue_1, ue_2 >$
$< f_1f_2, uf_3 >$	$< 1+\overline{u}e_2+ue_1, ue_2 >$	uf_2	ue_1
$< f_1f_3, uf_2 >$	$< 1+\overline{u}e_1+ue_2, ue_1 >$	uf_3	ue_2
$< f_2f_3, uf_1 >$	$< \overline{u}h, ue_1+ue_2 >$	uf_1	ue_1+ue_2
$< f_1f_2, uf_1f_3 >$	$< 1+\overline{u}e_2+ue_1, u+ue_1 >$	$< f_2f_3, uf_1f_2 >$	$< \overline{u}h, u+ue_2 >$
$< f_1f_2, uf_2f_3 >$	$< 1+\overline{u}e_2+ue_1, uh >$	$< f_2f_1, uf_2f_3 >$	$< 1+\overline{u}e_2+ue_1, uh >$
$< f_1f_3, uf_1f_2 >$	$< 1+\overline{u}e_1+ue_2, u+ue_2 >$	$< f_2f_3, uf_3f_1 >$	$< \overline{u}h, u+ue_1 >$
$< f_1f_3, uf_3f_2 >$	$< 1+\overline{u}e_1+ue_2, uh >$	$< f_2f_1, uf_3f_2 >$	$< 1+\overline{u}e_2+ue_1, uh >$
$< f_2f_3, uf_2f_1 >$	$< \overline{u}h, u+ue_2 >$	$< f_1f_2, uf_1f_3 >$	$< 1+\overline{u}e_2+ue_1, u+ue_1 >$
$< f_2f_3, uf_3f_1 >$	$< \overline{u}h, u+ue_1 >$	$< f_1f_3, uf_1f_2 >$	$< 1+\overline{u}e_1+ue_2, u+ue_2 >$
u	u	u	u
$< f_1, uf_3f_2 >$	$< u+e_1+e_2, uh >$	uf_2f_3	uh
$< f_3, uf_1f_2 >$	$< e_2+ue_1, u+ue_2 >$	uf_1f_3	$u+ue_1$
$< f_2, uf_1f_3 >$	$< e_1+ue_2, u+ue_1 >$	uf_1f_2	$u+ue_2$
f_1f_2	$1+\overline{u}e_2+ue_1$	f_2	e_1+ue_2
f_1f_3	$1+\overline{u}e_1+ue_2$	f_3	e_2+ue_1
f_2f_3	$\overline{u}h$	f_1	$u+e_1+e_2$
uf_1f_2	$u+ue_2$	$< f_2, uf_1f_3 >$	$< e_1+ue_2, u+ue_1 >$
uf_1f_3	$u+ue_1$	$< f_3, uf_1f_2 >$	$< e_2+ue_1, u+ue_2 >$
uf_2f_3	uh	$< f_1, uf_3f_2 >$	$< u+e_1+e_2, uh >$

Chapter 5

Idempotents of cyclic codes over Rings of higher orders

When n is odd we study a pair of polynomials idempotents that "generate" any cyclic codes of length n over $\mathbb{Z}_{p^m}$ and $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$.

5.1 Generating idempotents of cyclic codes over $\mathbb{Z}_{p^m}$

Theorem 5.1.1. *[18]*

(i) Suppose p is a prime not dividing n and C is an ideal of $\mathcal{R}_n$. If C is generated by a divisor f of $x^n - 1$, then C has an idempotent generator e. Furthermore whenever, $0 \leq k \leq m-1$ then, $< p^k f >=< p^k e >$.

(ii) Suppose p is a prime not dividing n and f is divisor of $x^n - 1$, then for each k such that $0 \leq k \leq m-1$ there exists an idempotent $e_k \in \mathbb{Z}_{p^{m-k}}[x]/ < x^n - 1 >$ such that $< p^k f >=< p^k e_k >$.

(iii) If p is a prime not dividing n, f is a divisor of $x^n - 1$ and $e(x)$ is the binary idempotent generator of $\pi f \subseteq \mathbb{Z}_2[x]/ < x^n - 1 >$, then $< 2^{m-1} f >=< 2^{m-1} e >$.

Proof. In (i), since p does not divide n and f divides $x^n - 1$, there exists $g \in \mathcal{R}_n^{(m)}$ such that (as polynomials) $fg = x^n - 1$ and f and g are coprime. Thus, there exist $a(x),\ b(x) \in \mathbb{Z}_{p^m}[x]$ such that $af + bg = 1$.

Let $e \in \mathcal{R}_n^{(m)}$ be congruent to $af(\mod x^n - 1)$. Then $e \equiv 1 - bg$.
Thus

$$e^2 \equiv e(1 - bg) = e - ebg = e - abfg \equiv e.$$

It follows that $fe = f - fbg \equiv f(\mod x^n - 1)$.
Thus e is an idempotent and $< f >=< e >$. Clearly, this also implies that, for $1 \leq k \leq m-1$, $< p^k f >=< p^k e >$.

In (ii), For $0 \leq k \leq m-1$, let $\pi_k : \mathbb{Z}_{p^m}[x] \longrightarrow \mathbb{Z}_{p^{m-k}}[x]$ be the ring homomorphism that maps $a + (p^m)$ to $a + (p^{m-k})$, and x to x.
Since $f/(x^n - 1)$ in $\mathbb{Z}_{p^m}[x]$, $\pi_k f$ divides $x^n - 1$ in $\mathbb{Z}_{p^{m-k}}[x]$. By (i), there exists

$$e_k \in \mathbb{Z}_{p^{m-k}}[x]/ < x^n - 1 > \text{ such that } < \pi_k f >=< e_k >.$$

Since $< p^k f >=< p^k \pi_k f >$, it follows that $< p^k f >=< p^k e_k >$.

In (iii), Follows from (ii). □

If C_1 and C_2 be a cyclic $\mathbb{Z}_{p^m}$-codes with idempotent generator e_1 and e_2 respectively, then $e_1 e_2$ and $e_1 + e_2 - e_1 e_2$ are idempotent generators of $C_1 \bigcap C_2$ and $C_1 + C_2$ respectively.

Corollary 5.1.2. *[18] Suppose* $C =< \hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m >$ *where* $F_0, F_1, ..., F_m$ *are pairwise coprime polynomials in* $\mathbb{Z}_{p^m}[x]$ *such that* $F_0 F_1 ..., F_m = x^n - 1$. *Then*

$$C =< e_0, pe_1, ..., p^{m-1}e_{m-1} >,$$

where for each k *such that* $0 \leq k \leq m-1$, e_k *is an idempotent in* $\mathbb{Z}_{p^{m-k}}[x]/ < x^n - 1 >$.

Theorem 5.1.3. *[18] If* $e(x)$ *is an idempotent generator of a cyclic* $\mathbb{Z}_{p^m}$*-code then* $1 - e(x^{-1})$ *is an idempotent generator of* $C^{\perp}$.

Proof. Since $e(x)[1 - e(x)] = e(x) - e^2(x) = 0$ in $\mathcal{R}_n$, then $e(x)$ is orthogonal to $1 - e(x^{-1})$. That is, $1 - e(x^{-1}) \in C^{\perp}$.
One the other hand, if C has generator polynomial g and $gh = x^n - 1$, then $C^{\perp}$ has generator polynomial h^*, where $h^* = x^{degh(x)} h(x^{-1})$.

Since $e(x)$ is the idempotent generator of $C =< g >$, we have $e(x) = u(x)g(x)$ for some $u(x) \in \mathbb{Z}_{p^m}[x]$

$$\begin{aligned} &\implies h(x)(1-e(x)) = h(x)(1-u(x)g(x)) \\ &\implies h(x)(1-e(x)) = h(x) \in \mathbb{Z}_{p^m}[x]/(x^n-1). \\ \implies x^{degh}h(x^{-1})[1-e(x^{-1})] &= x^{degh}h(x^{-1}) \implies h^*[1-e(x^{-1})] = h^* \end{aligned}$$

so that $h^* \in (1-e(x^{-1}))$.
Since $1-e(x^{-1}) \in C^{\perp} =< h^* >$, we have $C^{\perp} = 1-e(x^{-1})$.
Clearly $1-e(x^{-1})$ is the idempotent generator of $C^{\perp}$. □

An ideal I in a ring $\mathbb{R}$ is a minimal ideal provided there is no proper ideal between $\{0\}$ and I. See in [24].

Theorem 5.1.4. *Suppose p is a prime not dividing n and suppose $x^n - 1 = f_1 f_2 \dots f_r$ is representation of $x^n - 1$ as a product of basic irreducible, pairwise-coprime polynomials in $\mathbb{Z}_{p^m}[x]$, suppose $e_1, e_2, \dots, e_r \in \mathbb{Z}_p[x]/ < x^n - 1 >$ are primitive idempotents with $< \pi \hat{f}_i >=< e_i >$ for $1 \leq i \leq r$, let $\theta_i = e_i^{p^{m-1}}$ viewed as elements of $\mathbb{Z}_{p^m}[x]/ < x^n - 1 >$ then, there are k minimal ideals $C_1, C_2, \dots, C_k$ with generator $\theta_1, \theta_2, \dots, \theta_k$. These θ_i satisfy the following conditions:-*

(i) $\theta_i \theta_j = 0$, *for* $1 \leq i, j \leq r$ *with* $i \neq j$,

(ii) $\sum_{i=1}^{r} \theta_i(x) = 1$. *Furthermore, any cyclic code C is a sum of minimal ideals $C_i = (\hat{f}_i)$, and its idempotent $\theta(x)$ is the sum of idempotents θ_i for C_i.*

Proof. Since C_i are minimal ideals, $C_i \bigcap C_j = 0$ for $i \neq j$ so that, $\theta_1\theta_2 = 0$ for $i \neq j$ because $\theta_i\theta_j$ is in $C_i \bigcap C_j$.
Now $C_1 + C_2$ has idempotent generator $\theta_1(x) + \theta_2(x) - \theta_1(x)\theta_2(x) = \theta_1(x) + \theta_2(x)$, and it can be shown that $C_1 + C_2 + \ldots + C_k$ has idempotent $\theta_1(x) + \theta_2(x) + \ldots + \theta_k(x)$. We know that $C_1 + C_2$ has generator polynomial equals $\gcd(f_{1^n}, f_{2^n})$, it follows by finite induction that the generator polynomial of $C_1 + C_2 + \ldots + C_k$ is the $\gcd(f_{1^n}, \ldots, f_{k^n})$. But $\gcd(f_{1^n}, \ldots, f_{k^n}) = 1$, hence

$$\theta_1(x) + \theta_2(x) + \ldots + \theta_k(x) = 1.$$

If C is any ideal, then C has idempotent generator $\theta(x)$ and

$$\theta(x) = \theta(x)\theta_1(x) + \theta(x)\theta_2(x) + ... + \theta(x)\theta_k(x).$$

The ideal $C \bigcap C_i$ is contained in C_i and so is either 0 or C_i. If $C \bigcap C_i = C_i$ then $C_i \subseteq C$ and C itself is the sum of the C_i that are contained in it. □

5.2 Example on Generating idempotents of cyclic codes over $\mathbb{Z}_8$ and $\mathbb{Z}_{16}$

In this section we shall obtain nontrivial cyclic $\mathbb{Z}_8$-codes of length 7 and nontrivial cyclic $\mathbb{Z}_{16}$-codes of length 7.

Example 5.2.1. *[18] (Cyclic $\mathbb{Z}_8$- code of length 7)*
$x^7 - 1 = (x-1)(7 + 5x + 6x^2 + x^{3)})(7 + 2x + 3x^2 + x^3) = f_0 f_1 f_2$.
The number of cyclic codes $(3+1)^3 = 64$ *cyclic codes.*
We observe that $f_0^* = -f_0$, $f_1^* = -f_2$, $f_2^* = -f_1$.
Let

$$e_1 = x + x^2 + x^4 \quad and \quad e_2 = x^3 + x^5 + x^6,$$

then e_1, e_2 *are binary idempotents*
also, $e_1 + e_2$, e_1, e_2,$1 + e_2$, $1 + e_1$, $1 + e_1 + e_2$ *are binary idempotents generators* πf_0, πf_1, πf_2, $\pi f_0 \pi f_1$, $\pi f_0 \pi f_2$, $\pi f_1 \pi f_2$ *respectively.*
Let

$$h = 1 + e_1 + e_2.$$

By Theorem (5.1.4) we have

$\theta_0 = h^4 = 7h$ *is an idempotent generators of* $f_1 f_2$.
$\theta_1 = (1 + e_1)^4 = 5 + 3e_1 + 6e_2$ *is an idempotent of* $f_0 f_2$.
$\theta_2 = (1 + e_2)^4 = 5 + 6e_1 + 3e_2$ *is an idempotent of* $f_0 f_1$.

By Theorem (5.3.3) we have

$1 - \theta_0(x^{-1}) = 1 - \theta_0 = e_1 + e_2 + 2$ *is an idempotent generator of* f_0,
$1 - \theta_1(x^{-1}) = 1 - \theta_2 = 4 + 5e_2 + 2e_1$ *is an idempotent generator of* f_2,
also $1 - \theta_2(x^{-1}) = 1 - \theta_1 = 4 + 5e_1 + 2e_2$ *is an idempotent generator of* f_1.

***Table 5.1**: Idempotents of cyclic codes over $\mathbb{Z}_8$ of length 7.*

Code number	*Generator of the code*	*Idempotent-induced generator*
1	2	2
2	2^2	2^2
3	f_0	e_1+e_2+2
4	f_1	$4+5e_1+2e_2$
5	f_2	$4+5e_2+2e_1$
6	$2f_0$	$4+2e_2+2e_1$
7	$2f_1$	$2e_1+4e_2$
8	$2f_2$	$4e_1+2e_2$
9	2^2f_0	$2^2(e_2+e_1)$
10	2^2f_1	2^2e_1
11	2^2f_2	2^2e_2
12	f_0f_1	$5+3e_2+6e_1$
13	f_0f_2	$5+3e_1+6e_2$
14	f_1f_2	$7h$
14	$2f_0f_1$	$2+4e_1+6e_2$
15	$2f_0f_2$	$2+6e_1+4e_2$
16	$2f_1f_2$	$6h$
17	$2^2f_1f_2$	2^2h
18	$2^2f_0f_1$	$2^2(1+e_2)$
18	$2^2f_0f_2$	$2^2(1+e_1)$
19	$< f_0, 2f_1f_2 >$	$< 2+e_1+e_2, 6h >$
20	$< f_1, 2f_0f_2 >$	$< 4+5e_1+2e_2, 2+6e_1+4e_2 >$
21	$< f_2, 2f_0f_1 >$	$< 4+2e_1+5e_2, 2+4e_1+6e_2 >$
22	$< f_0f_1, 2f_2 >$	$< 5+6e_1+3e_2, 4e_1+2e_2 >$

Example 5.2.2. *(Cyclic $\mathbb{Z}_{16}$- code of length 7)*

$x^7-1=(x-1)(15+13x+14x^2+x^{3)}(15+10x+11x^2+x^3)=f_0f_1f_2$.

The number of cyclic codes $(4+1)^3=125$ cyclic codes.

We observe that $f_0^*=-f_0$, $f_1^*=-f_2$, $f_2^*=-f_1$.

Let

$$e_1=x+x^2+x^4 \quad and \quad e_2=x^3+x^5+x^6,$$

then e_1, e_2 are binary idempotents

also, e_1+e_2, e_1, e_2,$1+e_2$, $1+e_1$, $1+e_1+e_2$ are binary idempotents generators πf_0, πf_1, πf_2, $\pi f_0\pi f_1$, $\pi f_0\pi f_2$, $\pi f_1\pi f_2$ respectively.

Let

$$h=1+e_1+e_2.$$

By Theorem (5.1.4) we have

$\theta_0 = h^8 = 15h$ *is an idempotent generators of* $f_1 f_2$.

$\theta_1 = (1+e_1)^8 = 1 + 15e_1 + 14e_2$ *is an idempotent of* $f_0 f_2$.

$\theta_2 = (1+e_2)^8 = 1 + 15e_2 + 14e_1$ *is an idempotent of* $f_0 f_1$.

By theorem (5.3.3) we have

$1 - \theta_0(x^{-1}) = 1 - \theta_0 = e_1 + e_2 + 2$ *is an idempotent generator of* f_0,

$1 - \theta_1(x^{-1}) = 1 - \theta_2 = e_2 + 2e_1$ *is an idempotent generator of* f_2,

also $1 - \theta_2(x^{-1}) = 1 - \theta_1 = e_1 + 2e_2$ *is an idempotent generator of* f_1.

Table 5.2*:Idempotents of cyclic codes over* $\mathbb{Z}_{16}$*-codes of length* 7.

Code number	*Generator of the code*	*Idempotent-induced generator*	*Order of the code*
1	2	2	8^7
2	2^2	2^2	4^7
3	2^3	2^3	2^7
4	f_0	$e_1 + e_2 + 2$	16^6
5	f_1	$e_1 + 2e_2$	16^4
6	f_2	$e_2 + 2e_1$	16^4
7	$2f_0$	$4 + 2e_2 + 2e_1$	8^6
8	$2f_1$	$4e_2 + 2e_1$	8^4
9	$2f_2$	$4e_1 + 2e_2$	8^4
10	$2^2 f_0$	$4e_1 + 4e_2 + 8$	4^6
11	$2^2 f_1$	$4e_1 + 8e_2$	4^4
12	$2^2 f_2$	$4e_2 + 8e_1$	4^4
13	$2^3 f_0$	$8e_2 + 8e_1$	2^6
14	$2^3 f_1$	$2^3 e_1$	2^4
15	$2^3 f_2$	$2^3 e_2$	2^4
16	$f_0 f_1$	$1 + 15e_2 + 14e_1$	16^3
17	$f_0 f_2$	$1 + 15e_1 + 14e_2$	16^3
18	$f_1 f_2$	$15h$	18
19	$2f_0 f_1$	$2 + 12e_1 + 14e_2$	8^3
20	$2f_0 f_2$	$2 + 14e_1 + 12e_2$	8^3
21	$2f_1 f_2$	$14h$	8
22	$2^2 f_1 f_2$	$12h$	4
23	$2^2 f_0 f_1$	$4 + 12e_2 + 8e_1$	4^3
24	$2^2 f_0 f_2$	$4 + 12e_1 + 8e_2$	4^3
25	$2^3 f_1 f_2$	$8h$	2
26	$2^3 f_0 f_1$	$8 + 8e_2$	2^3

5.3 Generating idempotents of cyclic codes over $\mathbb{R}_{k,p} = \mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$

Cyclic self dual codes and linear simplex codes over $\mathbb{F}_2 + u\mathbb{F}_2$ have been extensively studied in the papers [2], [3]. Codes over $\mathbb{F}_p + u\mathbb{F}_p + \ldots + u^{k-1}\mathbb{F}_p$ have discussed by of a number of authors in [16].

In this thesis we will define and construct idempotent generators and dual generators for cyclic over these rings and study their properties which is an open problem posed in [16] are considered.

In this thesis, we describe cyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3$ and there properties over the chain ring $\mathbb{F}_3 + u\mathbb{F}_3$. Also, we give some application of the idempotent generator for cyclic over these rings such that $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ and $\mathbb{F}_3 + u\mathbb{F}_3$.

Recall that, for the sake of simplicity, we use the same notation to represent the polynomials in $\mathbb{R}_{k,p}[x]$ of degree less than n and corresponding elements of

$$\mathbf{R}_n = \mathbb{R}_{k,p}[x]/ < x^n - 1 >.$$

Theorem 5.3.1.

(i) Suppose p is a prime not dividing n and C is an ideal of $\mathbf{R}_n$. If C is generated by a divisor f of $x^n - 1$, then C has an idempotent generator e. Furthermore whenever, $0 \leq k \leq m-1$ then, $< u^k f >=< u^k e >$.

(ii) Suppose p is a prime not dividing n and f is divisor of $x^n - 1$, then for each k such that $0 \leq k \leq m-1$ there exists an idempotent $e_k \in \mathbb{F}_{p^{m-k}}[x]/ < x^n - 1 >$ such that $< u^k f >=< u^k e_k >$.

(iii) If p is a prime not dividing n, f is divisor of $x^n - 1$ and $e(x)$ is the binary idempotent generator of $\alpha f \subseteq \mathbb{F}_2[x]/ < x^n - 1 >$, then $< u^{m-1} f >=< u^{m-1} e >$.

Proof. In (i), since p does not divide n and f divides $x^n - 1$, there exists $g \in \mathbf{R}_n^{(m)}$ such that (as polynomials) $fg = x^n - 1$ and f and g are coprime. Thus, there exist $a(x),\ b(x) \in \mathbb{R}_{k,p}[x]$ such that $af + bg = 1$.

Let $e \in \mathbf{R}_n^{(m)}$ be congruent to $af(\mod x^n - 1)$. Then $e \equiv 1 - bg$.

Thus

$$e^2 \equiv e(1-bg) = e - ebg = e - abfg \equiv e.$$

It follows that $fe = f - fbg \equiv f(\mod x^n - 1)$.
Thus e is an idempotent and $< f >=< e >$. Clearly, this also implies that, for $1 \leq k \leq m-1$, $< u^k f >=< u^k e >$.

In (ii), For $0 \leq k \leq m-1$, let $\alpha_k : \mathbb{R}_{k,p}[x] \longrightarrow \mathbb{F}_{p^{m-k}}[x]$ be the ring homomorphism that maps $\sum_{i=0}^{r} a_i x^i$ to $\sum_{i=0}^{r} \hat{a}_i x^i$, for any $a \in \mathbb{R}_{k,p}$ and $\hat{a}$ denote the polynomial reduction modulo u.
Since $f/(x^n-1)$ in $\mathbb{R}_{k,p}[x]$, $\alpha_k f$ divides x^n-1 in $\mathbb{F}_{p^{m-k}}[x]$. By (i), there exists

$$e_k \in \mathbb{F}_{p^{m-k}}[x]/ < x^n - 1 > \text{ such that } < \alpha_k f >=< e_k >.$$

Since $< u^k f >=< u^k \alpha_k f >$, it follows that $< u^k f >=< u^k e_k >$.

In (iii), Follows from (ii). □

Remark 5.3.1. Let C_1 and C_2 be a cyclic $\mathbb{R}_{k,p}$ - codes with idempotent generator e_1 and e_2 respectively. Then $e_1 e_2$ and $e_1 + e_2 - e_1 e_2$ are idempotent generators of $C_1 \bigcap C_2$ and $C_1 + C_2$ respectively.

Corollary 5.3.2. *Suppose* $C =< \hat{F_1}, u\hat{F_2}, ..., u^{m-1}\hat{F_m} >$ *where* $F_0, F_1, ..., F_m$ *are pairwise coprime polynomials in* $\mathbb{R}_{k,p}[x]$ *such that* $F_0 F_1 ... F_m = x^n - 1$. *Then*

$$C =< e_0, ue_1, ..., u^{m-1} e_{m-1} >,$$

where for each k *such that* $0 \leq k \leq m-1$, e_k *is an idempotent in* $\mathbb{F}_{p^{m-k}}[x]/ < x^n - 1 >$.

Theorem 5.3.3. *If* $e(x)$ *is an idempotent generator of cyclic* $\mathbb{R}_{k,p}$*-code then* $1 - e(x^{-1})$ *is an idempotent generator of* $C^{\perp}$.

Proof. The proof is similar to the proof given in Theorem 5.1.3 □

5.4 Examples on Generating idempotents of cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ and $\mathbb{F}_3+u\mathbb{F}_3$

5.4.1 Back ground on the cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$

Codes over ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ have been widely studied in[1], [13], [17] $\mathbb{R}_{3,2} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 = \mathbb{F}_2(u)/ < u^3 >$ is a commutative chain ring of 8 elements which are $\{0, 1, u^2, v^2, v, uv, v^3\}$, where $u^3 = 0$, $v = 1+u, v^2 = 1+u^2$, $v^3 = 1 + u + u^2$, $uv = u + u^2$. The elements of $\mathbb{R}_{3,2}$ are the polynomials over $\mathbb{F}_2$ modulo the ideal $< u^3 >$ of $\mathbb{F}_2[u]$ where $\mathbb{F}_2$ is the binary field $\{0, 1\}$. Addition and multiplication operations over $\mathbb{R}_{3,2}$ are given in the following tables:

+	0	1	u	v	u^2	uv	v^2	v^3
0	0	1	u	v	u^2	uv	v^2	v^3
1	1	0	v	u	v^2	v^3	u^2	uv
u	u	v	0	1	uv	u^2	v^3	v^2
v	v	u	1	0	v^3	v^2	uv	u^2
u^2	u^2	v^2	uv	v^3	0	u	1	v
uv	uv	v^3	u^2	v^2	u	0	v	1
v^2	v^2	u^2	v^3	uv	1	v	0	u
v^3	v^3	uv	v^2	u^2	v	1	u	0

.	0	1	u	v	u^2	uv	v^2	v^3
0	0	0	0	0	0	0	0	0
1	0	1	u	v	u^2	uv	v^2	v^3
u	0	u	u^2	uv	0	u^2	u	uv
v	0	v	uv	v^2	u^2	u	v^3	1
u^2	0	u^2	0	u^2	0	0	u^2	u^2
uv	0	uv	u^2	u	0	u^2	uv	u
v^2	0	v^2	u	v^3	u^2	uv	1	v
v^3	0	v^2	uv	1	u^2	u	v	v^2

Table 5.1: Multiplication and addition tables for the ring $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$.

For any element of $\mathbb{R}_{3,2}$ expressed as $x + uy + u^2z$, the Gray map α from $\mathbb{R}_{3,2}$ to $\mathbb{F}_2^4$ is defined by $\alpha(x + uy + u^2z) = (z, x + z, y + z, x + y + z)$, where $x,\ y\ and\ z \in\ \mathbb{F}_2$. We define a new weight function for codes over $\mathbb{R}_{3,2}$. Using the following map α from $\mathbb{R}_{3,2}$ to $\mathbb{F}_2^4$

x_i	$\alpha(x_i)$	x_i	$\alpha(x_i)$
0	0000	1	0101
u	0011	v	0110
u^2	1111	v^2	1010
uv	1100	v^3	1001

Example 5.4.1. *(Cyclic $\mathbb{R}_{3,2} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ code of length 7)*
$x^7 - 1 = (x + v^3)(v^3 + v^2x + uvx^2 + x^{3)}(v^3 + ux + vx^2 + x^3) = f_0f_1f_2$.
The number of cyclic codes $(3 + 1)^3 = 64$ *cyclic codes.*
We observe that $f_0^* = v^3f_0$, $f_1^* = v^3f_2$, $f_2^* = v^3f_1$.
Let

$$e_1 = x + x^2 + x^4 \quad \textit{and} \quad e_2 = x^3 + x^5 + x^6,$$

then e_1, e_2 *are binary idempotents*
also, $e_1 + e_2$, e_1, e_2,$1 + e_2$, $1 + e_1$, $1 + e_1 + e_2$ *are binary idempotents generators* αf_0, αf_1, αf_2, $\alpha f_0\alpha f_1$, $\alpha f_0\alpha f_2$, $\alpha f_1\alpha f_2$ *respectively.*
Let

$$h = 1 + e_1 + e_2.$$

By Theorem (5.1.4) we have

$\psi_0 = h^4 = v^3h$ *is an idempotent generators of* f_1f_2.
$\psi_1 = (1 + e_1)^4 = v^2 + ve_1 + uve_2$ *is an idempotent of* f_0f_2.
$\psi_2 = (1 + e_2)^4 = v^2 + uve_1 + ve_2$ *is an idempotent of* f_0f_1.

By theorem (5.3.3) we have
$1 - \psi_0(x^{-1}) = 1 - \theta_0 = e_1 + e_2 + u$ *is an idempotent generator of* f_0,
$1 - \psi_1(x^{-1}) = 1 - \theta_2 = u^2 + v^2e_2 + ue_1$ *is an idempotent generator of* f_2,
also $1 - \theta_2(x^{-1}) = 1 - \psi_1 = u^2 + v^2e_1 + ue_2$ *is an idempotent generator of* f_1.

***Table 5.3**:-Idempotents of cyclic codes over $\mathbb{R}_{3,2} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ of length 7.*

Generator of the code	*Idempotent-induced generator*	*Generator of the code*	*Idempotent-induced generator*
u	u	$< f_1f_2, u^2f_0 >$	$< v^3h, u^2e_1 + u^2e_2 >$
f_0	$e_1 + e_2 + u$	$< f_0f_1, uf_1f_2 >$	$< v^2 + uve_1 + ve_2, uvh >$
f_2	$u^2 + v^2e_2 + ue_1$	uf_0	$ue_1 + ue_2 + u^2$
uf_1	$ue_1 + u^2e_2$	uf_2	$ue_2 + u^2e_1$
u^2f_0	$u^2e_1 + u^2e_2$	u^2f_1	u^2e_1
u^2f_2	u^2e_2	f_0f_1	$v^2 + uve_1 + ve_2$
f_0f_2	$v^2 + ve_1 + uve_2$	f_1f_2	v^3h
uf_0f_1	$u + u^2e_1 + uve_2$	$< f_0f_1, uf_2 >$	$< v^2 + uve_1 + ve_2, ue_2 + u^2e_1 >$
uf_0f_2	$u + uve_1 + u^2e_2$	$u^2f_0f_1$	$u^2 + u^2e_2$
$u^2f_0f_2$	$u^2 + u^2e_1$	$u^2f_1f_2$	u^2h
uf_1f_2	uvh	$< f_0f_2, uf_1 >$	$< v^2 + ve_1 + uve_2, ue_1 + u^2e_2 >$
$< f_1f_2, uf_0 >$	$< v^3h, ue_1 + ue_2 + u^2 >$	$< f_0, uf_1f_2 >$	$< e_1 + e_2 + u, uvh >$
$< f_0f_1, u^2f_2 >$	$< v^2 + uve_1 + ve_2, u^2e_2 >$	$< uf_1f_2, u^2f_0 >$	$< uvh, u^2e_1 + u^2e_2 >$
$< f_0f_2, u^2f_1 >$	$< v^2 + ve_1 + uve_2, u^2e_1 >$	$< f_0, u^2f_1f_2 >$	$< e_1 + e_2 + u, u^2h >$
$< uf_1f_2, u^2f_0f_2 >$	$< uvh, u^2 + u^2e_1 >$	$< uf_0f_2, u^2f_1f_2 >$	$< u + uve_1 + u^2e_2, u^2h >$
$< uf_0f_1, u^2f_1f_2 >$	$< u + u^2e_1 + uve_2, u^2h >$	$< uf_1f_2, u^2f_0f_1 >$	$< uvh, u^2 + u^2e_2 >$
f_1	$u^2 + v^2e_1 + ue_2$	$< uf_0f_1, u^2f_2 >$	$< u + u^2e_1 + uve_2, u^2e_2 >$
$< uf_0f_2, u^2f_1 >$	$< u + uve_1 + u^2e_2, u^2e_1 >$	u^2	u^2
$< f_0f_1, u^2f_1f_2 >$	$< v^2 + uve_1 + ve_2, u^2h >$	$< f_0f_2, uf_1f_2 >$	$< v^2 + ve_1 + uve_2, uvh >$
$< f_1f_2, u^2f_0f_1 >$	$< v^3h, u^2 + u^2e_2 >$	$< uf_0, u^2f_1f_2 >$	$< ue_1 + ue_2 + u^2, u^2h >$
$< f_1, uf_0f_2 >$	$< u^2 + v^2e_1 + ue_2, u + uve_1 + u^2e_2 >$	$< f_1f_2, u^2f_0f_2 >$	$< v^3h, u^2 + u^2e_1 >$
$< f_2, uf_0f_1 >$	$< u^2 + v^2e_2 + ue_1, u + u^2e_1 + uve_2 >$	$< f_1f_2, uf_0f_1 >$	$< v^3h, u + u^2e_1 + uve_2 >$
$< f_1f_2, uf_0f_2 >$	$< v^3h, u + uve_1 + u^2e_2 >$	$< uf_2, u^2f_0f_1 >$	$< ue_2 + u^2e_1, u^2 + u^2e_2 >$
$< uf_1, u^2f_0f_2 >$	$< ue_1 + u^2e_2, u^2 + u^2e_1 >$	$< f_1, u^2f_0f_2 >$	$< u^2 + v^2e_1 + ue_2, u^2 + u^2e_1 >$

In Table 5.3 we list all nontrivial cyclic $\mathbb{R}_{3,2} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$-codes of length 7 along with the idempotent-induced generators.

5.4.2 Cyclic codes over $\mathbb{R}_{2,3} = \mathbb{F}_3 + u\mathbb{F}_3$

We introduce linear cyclic codes over the ring $\mathbb{R}_{2,3} = \mathbb{F}_3 + u\mathbb{F}_3 = \{0, 1, 2, u, 2u, \nu, \lambda, \kappa, \beta\}$, where $u^2 = 0$, $\nu = 1 + u$, $\lambda = 2 + u$, $\kappa = 1 + 2u$ and $\beta = 2 + 2u$.

The ring $\mathbb{F}_3 + u\mathbb{F}_3$ is a commutative ring $\{a + ub : a, b \in \mathbb{F}_3\}$ of order 9 with $u^2 = 0$. A linear code C over $\mathbb{F}_3 + u\mathbb{F}_3$ of length n is an $\mathbb{F}_3 + u\mathbb{F}_3$-submodule of $(\mathbb{F}_3 + u\mathbb{F}_3)^n$. A nonlinear code over $\mathbb{F}_3 + u\mathbb{F}_3$ of length n is a subset of $(\mathbb{F}_3 + u\mathbb{F}_3)^n$. The ring is a commutative chain ring with maximal ideal $\{0, u\}$. The multiplication and addition table for the ring is given in Table 2.3, the multiplication table coincides with that of $\mathbb{Z}_9$, when u, ν, λ, $2u$, κ and β are replaced by respectively 3, 4, 5, 6, 7 and 8.

In this sense $\mathbb{R}_{2,3}$ is analogous to $\mathbb{Z}_9$ and here u plays the role of 3. However the addition table is different. The addition table is similar to that of the Galois field $\mathbb{F}_9 = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\}$, when 1, 2, u, u+1, u+2, $2u$, $2u$+1, and $2u + 2$ are replaced respectively by $\alpha^8, \alpha^4, \alpha^6, \alpha, \alpha^7, \alpha^2, \alpha^3, \alpha^5$.
Addition and multiplication operations over $\mathbb{R}_{2,3}$ are given in the following tables:

+	0	1	2	u	ν	λ	$2u$	κ	β
0	0	1	2	u	ν	λ	$2u$	κ	β
1	1	2	u	ν	λ	$2u$	κ	β	0
2	2	u	ν	λ	$2u$	κ	β	0	1
u	u	ν	λ	$2u$	κ	β	0	1	2
ν	ν	λ	$2u$	κ	β	0	1	2	u
λ	λ	$2u$	κ	β	0	1	2	u	ν
$2u$	$2u$	κ	β	0	1	2	u	ν	λ
κ	κ	β	0	1	2	u	ν	λ	$2u$
β	β	0	1	2	u	ν	λ	$2u$	κ

.	0	1	2	u	ν	λ	$2u$	κ	β
0	0	0	0	0	0	0	0	0	0
1	0	1	2	u	ν	λ	$2u$	κ	β
2	0	2	ν	$2u$	β	1	u	λ	κ
u	0	u	$2u$	0	u	$2u$	0	u	$2u$
ν	0	ν	β	u	ν	2	$2u$	1	λ
λ	0	λ	1	$2u$	2	κ	u	β	ν
$2u$	0	$2u$	u	0	$2u$	u	0	$2u$	u
κ	0	κ	λ	u	1	β	$2u$	ν	2
β	0	β	κ	$2u$	λ	ν	u	2	0

Table 5.2: Multiplication and addition tables for the ring $\mathbb{F}_3 + u\mathbb{F}_3$.

We assume that n is odd and represent codewords by polynomial, then cyclic codes are ideals in the ring $\mathbf{R}_n^{'} = \mathbb{R}_{2,3}[x]/ < x^n - 1 >$.
This ring shares many properties of $\mathbb{Z}_9$ and $\mathbb{F}_9$ and admits a linear "Gray map".

Galois extension ring of $\mathbb{R}_{2,3} = \mathbb{F}_3 + u\mathbb{F}_3$.

The method of constructing Galois rings over $\mathbb{R}_{2,3}$ is similar to the construction of Galois rings over $\mathbb{Z}_9$. The general case of such rings over $\mathbb{R}_{2,3} = \mathbb{F}_3[u]/(w(u)^k)$, $k > 1$, where $w(u)$ is an irreducible polynomial of $m \geq 1$ over $\mathbb{F}_3$ has studied in [24]. The ring $\mathbb{R}_{2,3}$ is a special case of $\mathbf{R}_n^{'}$ when $w(u) = u$ and $k = 2$.

Definition 5.4.1. Let $\mathbb{R}_{2,3}[x]$ be the ring of polynomials over $\mathbb{R}_{2,3}$. We have a natural homomorphic mapping, from $\mathbb{R}_{2,3}$ to its residue field $\mathbb{F}_3$. For any $b \in \mathbb{R}_{2,3}$, let $\hat{b}$ denote the polynomial reduction modulo u.
Now, define a polynomial reduction mapping $\alpha : \mathbb{R}_{2,3}[x] \longrightarrow \mathbb{F}_3[x]$ is defined by:

$$f(x) = \sum_{i=0}^{r} a_i x^i \xrightarrow{\alpha} \sum_{i=0}^{r} \hat{a}_i x^i.$$

A monic polynomial f over $\mathbb{R}_{2,3}[x]$ is said to a basic irreducible polynomial if its projection $\alpha(f)$ is irreducible over $\mathbb{F}_3[x]$.
The Galois ring of $\mathbb{R}_{2,3}$ denoted as $GR(\mathbb{R}_{2,3}, r)$ is defined as $\mathbb{R}_{2,3}[x]/ < f(x) >$, where $f(x)$ is a basic monic irreducible polynomial of degree r over $\mathbb{R}_{2,3}$. Hence the ring $GR(\mathbb{R}_{2,3}, r)$ is a module over $\mathbb{R}_{2,3}$.

We study a new weight function for codes over $\mathbb{F}_3 + u\mathbb{F}_3$. The Gray weight $Gw(x)$ of a codeword x= $(x_1, x_2, \ldots, x_n)$ is defined as $\sum_{i=1}^{n} Gw(x_i)$ where

$$Gw(x_i) = \begin{cases} 0, & \text{if } x_i = 0; \\ 1, & \text{if } x_i = 1,\ 2,\ u,\ \textit{and}\ 2u; \\ 2, & \text{otherwise.} \end{cases}$$

The Gray distance $Gd(x, y)$ between two codewords x and y is the Gray weight of $x - y$. Using the following map α from $\mathbb{F}_3 + u\mathbb{F}_3$ to $\mathbb{F}_3^2$.

Table [⋆]

x_i	$\alpha(x_i)$	x_i	$\alpha(x_i)$
0	00	1	01
1	01	2	02
u	10	$1+u$	11
$2+u$	12	$2u$	20
$1+2u$	21	$2+2u$	22

Lemma 5.4.1. *[21]*

The Gray map α is a distance-preserving map from

$$((\mathbb{F}_3 + u\mathbb{F}_3)^n, \textit{Gray distance}) \text{ to } (\mathbb{F}_3)^{2n}, \textit{Hamming distance})$$

Proof. From the definitions, it is clear that

$$Gd(x, y) = d(\alpha(x), \alpha(y)),$$

where x *and* $y\ \in (\mathbb{F}_3 + u\mathbb{F}_3)^n$ □

If C is linear, the minimum Gray distance is the same as the minimum Gray weight. If the linear code C of length n over the ring $\mathbb{R}_{2,3}$ with $|C| = 9^k$ and minimum Gray distance d, then $\alpha(C)$ is a ternary linear $[2n, 2k, d]$.

Example 5.4.2. *(Cyclic $\mathbb{R}_{2,3} = \mathbb{F}_3 + u\mathbb{F}_3$ of length 11) In $\mathbb{F}_3[x] + u\mathbb{F}_3[x]$,*
$x^{11} - 1 = (x + \beta)(x^5 + \beta x^3 + x^2 + \beta x + \beta)(x^5 + x^4 + \beta x^3 + x^2 + \beta) = f_0 f_1 f_2$,
where $f_0 = (x+\beta)$, $f_1 = (x^5+\beta x^3+x^2+\beta x+\beta)$, $f_2 = (x^5+x^4+\beta x^3+x^2+\beta)$.
Observe that f_0, f_1, f_2 are basic irreducible, pairwise-coprime and $f_0^* = -f_0$,
$f_1^* = -f_2$, $f_2^* = -f_1$.
The number of cyclic codes $(2+1)^3 = 27$ cyclic codes.
Let

$$e_1 = -x - x^3 - x^4 - x^5 - x^9 \text{ and } e_2 = -x^2 - x^6 - x^7 - x^8 - x^{10}$$

then e_1, e_2 are ternary idempotents also $-(1 + e_1 + e_2)$, e_1, e_2, $-1 + e_1 + e_2$,
$1 - e_1$, $1 - e_2$ are ternary idempotents generators of αf_0, αf_1, αf_2, $\alpha f_1 \alpha f_2$,
$\alpha f_0 \alpha f_2$ and $\alpha f_0 \alpha f_1$ respectively.

Let $h = -1 + e_1 + e_2$ then with the notations of theorem 5.1.4
$\psi_0 = (-1 + e_1 + e_2)^3 = \beta h$,
$\psi_1 = (1 - e_1)^3 = 1 + \beta e_1 + 2ue_2$,
$\psi_2 = (1 - e_2)^3 = 1 + \beta e_2 + 2ue_1$ *are idempotents generators of $f_1 f_2$, $f_0 f_2$ and*
$f_0 f_1$ respectively.
Observe that $1 - \psi_0(x^{-1}) = 1 - \psi_0 = 1 + e_1 + e_2$
$1 - \psi_1(x^{-1}) = 1 - \psi_2 = e_2 + ue_1$
$1 - \psi_2(x^{-1}) = 1 - \psi_1 = e_1 + ue_2$.
By theorem 5.3.3, idempotents generators of (f_0), (f_1), (f_2) are $1 - \psi_0$,
$1 - \psi_1$, $1 - \psi_2$ respectively.
From this we can list all non-trivial cyclic codes along with their idempotents generators and their dual codes (see Table 5.4).

***Table 5.4**:-Idempotents of cyclic codes over* $\mathbb{R}_{2,3} = \mathbb{F}_3 + u\mathbb{F}_3$ *of length* 11.

Code number	*Generator of the code*	*Generator of the dual code*	*Idempotent-induced generator*
1	u	u	u
2	f_0	$f_1 f_2$	$1 + e_1 + e_2$
3	f_1	$f_0 f_1$	$e_1 + ue_2$
4	f_2	$f_0 f_2$	$e_2 + ue_1$
5	uf_0	$< f_1 f_2, uf_0 >$	$u + ue_1 + ue_2$
6	uf_1	$< f_0 f_1, uf_2 >$	ue_1
7	uf_2	$< f_0 f_2, uf_1 >$	ue_2
8	$f_0 f_1$	f_1	$1 + \beta e_2 + 2ue_1$
9	$f_0 f_2$	f_2	$1 + \beta e_1 + 2ue_2$
10	$f_1 f_2$	f_0	βh
11	$uf_0 f_1$	$< f_1, uf_0 f_2 >$	$1 + 2ue_2$
12	$uf_0 f_2$	$< f_2, uf_0 f_1 >$	$1 + 2ue_1$
13	$uf_1 f_2$	$< f_0, uf_1 f_2 >$	$2uh$
14	$< f_1, uf_0 f_2 >$	$uf_0 f_1$	$< e_1 + ue_2, 1 + 2ue_1 >$
15	$< f_2, uf_0 f_1 >$	$uf_0 f_2$	$< e_2 + ue_1, 1 + 2ue_2 >$
16	$< f_0, uf_1 f_2 >$	$uf_1 f_2$	$< 1 + e_1 + e_2, 2uh >$
17	$< f_0 f_1, uf_2 >$	uf_1	$< 1 + \beta e_2 + 2ue_1, ue_2 >$
18	$< f_0 f_2, uf_1 >$	uf_2	$< 1 + \beta e_1 + 2ue_2, ue_1 >$
19	$< f_1 f_2, uf_0 >$	uf_0	$< \beta h, u + ue_1 + ue_2 >$
20	$< f_0 f_1, uf_0 f_2 >$	$< f_1 f_2, uf_0 f_1 >$	$< 1 + \beta e_2 + 2ue_1, 1 + 2ue_1 >$
21	$< f_0 f_1, uf_1 f_2 >$	$< f_0 f_1, uf_1 f_2 >$	$< 1 + \beta e_2 + 2ue_1, 2uh >$
22	$< f_0 f_2, uf_0 f_1 >$	$< f_1 f_2, uf_0 f_2 >$	$< 1 + \beta e_1 + 2ue_2, 1 + 2ue_2 >$
23	$< f_0 f_2, uf_1 f_2 >$	$< f_0 f_2, uf_1 f_2 >$	$< 1 + \beta e_1 + 2ue_2, 2uh >$
24	$< f_1 f_2, uf_0 f_1 >$	$< f_0 f_1, uf_0 f_2 >$	$< \beta h, 1 + 2ue_2 >$
25	$< f_1 f_2, uf_0 f_2 >$	$< f_0 f_2, uf_0 f_1 >$	$< \beta h, 1 + 2ue_1 >$

In Table 5.4 we list all nontrivial cyclic $\mathbb{F}_3 + u\mathbb{F}_3$*-codes of length* 11 *along with their duals and idempotent-induced generators.*

Conclusion

In this thesis, we have study cyclic codes over rings $\mathbb{Z}_4$, $\mathbb{F}_2 + u\mathbb{F}_2$ and constructed some interesting self-dual cyclic codes over those rings. We generalize the results of Pless and Qian and those of Pless, Sloe, and Qian for cyclic $\mathbb{Z}_4$-codes to $\mathbb{Z}_p^m$-codes. We study and produce generators for the cyclic $\mathbb{Z}_p^m$-codes which are analogs to those for cyclic $\mathbb{Z}_4$-codes, these may be used to produce a single generator for such codes. Generators for dual codes of cyclic $\mathbb{Z}_p^m$-codes are produced from the generators of the corresponding cyclic $\mathbb{Z}_p^m$-codes.

Also we generalize the results to linear cyclic codes over the commutative chain rings "$\mathbb{F}_p + u\mathbb{F}_p + ... + u^{k-1}\mathbb{F}_p$" where p is prime number.

Finally, we construct idempotent generators of cyclic codes over the rings $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ "$\mathbb{F}_2 + u\mathbb{F}_2$", "$\mathbb{F}_3 + u\mathbb{F}_3$", "$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$", and study their properties.

Bibliography

[1] AL-Ashker M., *Simplex codes over the Ring* $\sum_{n=0}^{s} u^n F_2$, The Turk.J.Math, PP. 221-233, 2005.

[2] AL-Ashker M., *Simplex codes over* $F_2 + uF_2$, The Arabian Journal for Science and engineering, vol.30, num.2A, PP. 227-285, 2005.

[3] A. Bonnecaze and P.Udaya, *Cyclic codes and self-dual codes over* F_2+uF_2, IEEE Trans. Inf. Theory, vol.45, no.4, PP. 1250-1255, 1999.

[4] A.R. Galder and N.J.A. Sloane *Modular and p-aidic Cyclic codes*, Designs Codes Cryptogr., vol.6, pp.21-35, 1995.

[5] B.R.Mc.Donald, *Finite Rings with identity*, Dekker, NY, 1974.

[6] C. Musili, *Introduction to Rings and Modules*, University of Hyderabad, Second Revised Edition, 1994.

[7] D. Hofman, *Coding theory*, Markel Dekker, 1990.

[8] Fraleigh. John B., *First course in abstract algebra*, 5th Edition, 1993.

[9] Gilberto Bini and Flaminio Flamini, *Finite commutative rings and their a pplications*, University of Michigan, Universita degli Studi Roma Tre, U.S.A and Italy, 2002.

[10] H.Tapia-Recillas, *On the Gray image of linear cyclic codes over Galois rings*, UAM-I, Mexico, D.F., MEXICO, Merseille-Luminy, France, 26-30 September, 2005.

[11] H.Tapia-Recillas, *The Simplex Code over Galois Rings*, UAM-L, Mexico, D.F., MEXICO, Merseille-Luminy, France, 2005.

[12] H.Q.Dinh and SE. R.Lopez-Permouth, *Cyclic and Negacyclic codes over Finite Chain Rings*, IEEE Transactions on Fundamental Theory, vol.50, no.8, 2004.

[13] J.Qian, Li Zhang and Shi Zhu, *Contstacyclic and cyclic codes over* $F_2 + uF_2 + u^2F_2$, IEICE Transactions on Fundamental of electronics and computer sciences archive.vol.E89-A, Iss4 6, pp1863-1885, (June 2006).

[14] Joseph A.Gallian, *Contemporary Abstract Algebra*, University of Minnesota, Duluth, Second Revised Edition, 1990.

[15] J.H.Van Lint, *Introduction to coding theory*, Markel Dekker, 1999.

[16] J. Qian, Li Zhang and Shi Zhu, *Cyclic codes over* $F_p + uF_p + ... + u^{k-1}F_p$, IEICE Trans. Fundamentals, vol E88-A, No.3, pp795-779, March 2005.

[17] Naji A., *Linear codes over* $F_2+uF_2+u^2F_2$ *of Constant Lee weight*, The second conference of the Islamic University on Mathematical Science-Gaza, 27-28 Aug.2002.

[18] P. Kanwar and S.R. Lopez-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields Appl., vol.3, pp.334-352, 1997.

[19] Sanling Chaoping xing, *Coding theory a first course*, Springer-Verlag, 1998.

[20] Steven Roman, *Coding and information theory*, Springer-Verlag, 1992.

[21] T. Aaron Gulliver and Masaaki Harada, *Codes over* $F_3 + uF_3$, University of Canterbury and Yamagata University, New Zealand and Japan, June 2, 1998.

[22] V. Pless and Z. Qian, *Cyclic Codes and Quadratic Residue Codes over* $\mathbb{Z}_4$, IEEE Trans.Inform. Theory, 42:1594-1600, 1996.

[23] Vijay K. Khanna, *Acourse in abstract algebra*, University of Delhi, Second Revised Edition, 1998.

[24] W.C. Huffman and V. Pless, *Fundementals of Error-Correcting Codes*, Cambridge, U.K.:Cambridge Univ. Press, 2003.

[25] Xiang-dong Hou., *Commutative Chain Rings*, Wright state university, Dayton, Ohio, 2001.

[26] Z.X.Wan, *Cyclic codes over Galois rings*, Algbr.Colloq., vol.6, pp.291-304, 1999.