The Islamic University of Gaza

Deanery of Higher Studies

Faculty of Science

Department of Mathematics

On Even Length Codes Over Finite Rings

Presented by:

Mohammed Abed Hamoudeh

Supervised by:

Dr. Mohammed Mahmoud AL-Ashker

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF MATHEMATICS

2010

Abstract

Codes over finite rings have been studied in the early 1970. A great deal of attention has been given to codes over finite rings from 1990, because of their new role in algebraic coding theory and their successful application.

The key to describing the structure of cyclic codes over a ring R is to view cyclic codes as ideals in the polynomial ring $R[x]/\langle x^n - 1\rangle$, where n is the length of the code.

In previous studies, some authors determined the structure of cyclic codes over Z_4 for arbitrary even length by finding the generator polynomial, the number of cyclic codes for a given length and the duals for these codes, and also determined the structure of negacyclic codes of even length over the ring Z_{2^a} and their dual codes.

In this thesis, we introduce cyclic codes of an arbitrary length n over the rings $F_2 + uF_2$ with $u^2 = 0 \ mod\ 2$ and $F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \ mod\ 2$. We find a set of generators for these codes. The rank and the dual of these codes are studied as well.

We will extend these results about the rings $F_2 + uF_2$ and $F_2 + uF_2 + u^2F_2$ to more general rings $F_2 + uF_2 + u^2F_2 = \ldots + u^{k-1}F_2$ with $u^k = 0 \ mod\ 2$.

Finally we study the structure of $(1 + u)-$constacyclic codes of even length n over the ring $F_2 + uF_2$ with $u^2 = 0 \ mod\ 2$. Also we extend this study to the ring $F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \ mod\ 2$.

Dedication

To

My Parents

My wife

My sons Abed, Israa and Alaa

and to all knowledge seekers

Contents

Abstract **i**

Dedication **ii**

Table of Contents **iii**

Acknowledgements **v**

Introduction **1**

1 Preliminaries **3-32**

1.1 Rings and fields 3

1.2 Finite fields 11

1.3 Basic concepts of coding theory 16

1.4 Cyclic codes over finite fields 19

1.5 Codes over rings 29

2 Cyclic codes over Z_4 of even length **33-47**

2.1 Background 34

2.2 Construction the ideals of $R_4(u,m) = \mathrm{GR}(4,m)[u]/\langle u^{2^k} - 1\rangle$. 35

2.3 Discrete Fourier Transform 39

2.4 Duals 42

2.5 Examples 46

3 Negacyclic codes of even length over Z_{2^a} **48-60**

3.1 A ring construction 48

3.2 The ideals construction 51

3.3 Dual and self-dual 53

3.4 Examples 57

4 Cyclic codes over the ring $F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ **61-77**

4.1 Background 62

4.2 A generator construction 63

4.3 Ranks and minimal spanning sets for cyclic codes over R_k 68

4.4 Examples 74

5 Constacyclic codes over the rings $F_2 + uF_2$ and $F_2 + uF_2 + u^2F_2$ **78-95**

5.1 Classification of $(1 + u)$, $(1 - u^2)$-constacyclic codes 78

5.2 The dual and the minimal spanning sets of $(1 + u)$, $(1 - u^2)$-constacyclic codes 87

5.3 The Gray map and $(1 + u)$, $(1 - u^2)$-constacyclic codes 92

5.4 Examples 95

Conclusion **96**

Bibliography **97-99**

Acknowledgements

First of all, gratitude and thanks to **Almighty Allah** who always helps and guides me. I would like to express my sincere appreciation and thanks to my supervisor Dr.Mohammed M.AL-Ashker for his ceaseless help and supervision during the preparation of this project. Thanks are also due to all the staff members of mathematics department.

Introduction

Coding theory originated with 1948 publication of the paper (A mathematical theory of communication) by Claude shannon [21]. For the past half century, coding theory has grown into a discipline intersecting mathematics and engineering with applications to almost every area of communication such as satellite and cellular telephone transmission, compact disc recording, and data storage.

Shannon identified a number called the capacity of the channel and proved that arbitrary reliable communication is possible at any rate below the channel capacity. For example, when transmitting images of planets from deep space, it is impractical to retransmit the images. Hence if portions of the data giving the images are altered, due to noise arising in the transmission the data may prove useless. Shannon's results guarantee that the data can be encoded before transmission so that the altered data can be decoded to the specified degree of accuracy. Examples of other communication channels include magnetic storage devices, compact discs, and any kind of electronic communication device such as cellular telephones.

Among all types of codes, linear codes are studied the most. Because of their algebraic structure, they are easier to describe, encode, and decode than nonlinear codes.

Linear and cyclic codes over rings have recently aroused great interest because of their new roles in coding theory and their successful application in combined coding and modulation.

This thesis is organized as follows, we start by recalling background and notations about abstract algebra and coding theory in chapter 1.

Chapter 2 covers the structure of cyclic codes over the ring Z_4 for arbitrary even length n giving the generator polynomial for these codes and describing the duals and self-duals of the cyclic codes.

Chapter 3 examines negacyclic codes of even length over Z_{2^a}. The theory of these codes is an extension to the theory of negacyclic codes of even length over the ring Z_4.

Chapter 4 gives the basic theory of cyclic codes over the rings $F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0 \ mod \ 2$. This work is a generalization of the results in [3].

Chapter 5 includes the structure of constacyclic codes of even length over the rings $F_2 + uF_2$ with $u^2 = 0 \ mod \ 2$ and $F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \ mod \ 2$. This work is a generalization of the results in [2].

Chapter 1

Preliminaries

1.1 Rings and Fields

Definition 1.1.1. [16] A nonempty set R, together with two binary operations addition $(+)$ and multiplication $(.)$ is said to form a ring, if for all $a,\ b,\ c \in\ R$, 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 R s.t.,
$a + 0 = 0 + a = a.$

(iv) for each $a \in\ R,\ \ \exists\ an\ element\ (-a) \in\ R$, 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. [16] A ring R is called a commutative ring if $ab = ba$ for all $a, b \in\ R.$

If $\exists$ a unique element $e \in R$ s.t.,

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

then we say, 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. [16] An element a in a ring R with unity, is called invertible (or a unit) with respect to multiplication if $\exists$ some $b \in R$ such that $ab = 1 = ba$.

Definition 1.1.4. [16] Let R be a ring. An element $a \neq 0 \in R$ is called a zero-divisor, if $\exists$ an element $b \neq 0 \in R$ s.t., $ab = 0$.

Definition 1.1.5. [16] A commutative ring R with unity is called an integral domain if $ab = 0$ in $R \Longrightarrow$ either $a = 0$ or $b = 0$. In other words, a commutative ring R is called an integral domain if R has no zero divisors.

Definition 1.1.6. [16] A field is a nonempty set F of elements with two binary operations $+$ (called addition) and . (called multiplication) satisfying the following axioms. For all $a,\ b,\ c \in F$:

(i) F is closed under $+$ and . i.e., $a + b$ and $a.b$ are in 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 and satisfying the following:

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

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

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

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

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

Definition 1.1.7. [16] A ring R with unity is called a division ring or a skew field if all non zero elements of R have multiplicative inverse.

Definition 1.1.8. [16] A commutative division ring is called a field.

Lemma 1.1.1. *[16] A finite integral domain is a field.*

Corollary 1.1.2. *[16] 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. [16] A non empty subset S of a ring R is said to be a subring of R if S forms a ring under the binary operations of R.

Example 1.1.1. *The ring $(\mathbf{Z}, +, .)$ of integers is a subring of the ring $(\mathbf{R}, +, .)$ of real numbers.*

If R is a ring then 0 and R are always subrings of R, called trivial subrings of R.

Theorem 1.1.3. *[16] A non empty subset S of a ring R is a sub-ring of R if and only if $a, b \in S$, then ab, $a - b \in S$.* □

Definition 1.1.10. [16] Let R be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then R is said to have finite characteristic and also the smallest such positive integer n is called the characteristic of R.
If no such positive integer exists then R is said to have characteristic infinity. Characteristic of R is denoted by char R or $ch(R)$.

Example 1.1.2.

(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 Z_p *is* p *for any prime* p*.*

Ideals and Quotient Rings

Definition 1.1.11. [13] A nonempty subset I of a ring R is called a left ideal if

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

(ii) For all $a \in I$ and all $r \in R$, $ra \in I$.

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 R is a two-sided ideal. If possesses an identity e, then R is called a unit ideal and is denoted by (e). The two sided ideals $\{0\}$ and R are said to be improper, any ideal other than $\{0\}$ and R is said to be proper.

Theorem 1.1.4. [*13*] *If* R *is a ring with unity, and* I *is an ideal of* R *containing a unit, then* $I = R$.

Definition 1.1.12. [13] Let R be a ring and let I be an ideal in R. We define the quotient ring R/I as:

$R/I = \{r + I : r \in R\} =$ *set of all cosets of* I *in* R.

Definition 1.1.13. [13] An ideal $I \neq R$ in a commutative ring R is a prime ideal if $ab \in I$ implies that either $a \in I$ or $b \in I$ for every $a, b \in R$.

Definition 1.1.14. [16] Let R be a ring. An ideal $M \neq R$ of R is called a maximal ideal of R if whenever A is an ideal of R such that, $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

Example 1.1.3. [*16*]

(i) *A field F has only ideals F and $\{0\}$. We can see that $\{0\}$ is the only maximal ideal of 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 $\mathbb{E} = 2Z$ of even integers.*
$\mathbb{H}_4$, however, is not a prime ideal in E as $2.2 = 4 \in \mathbb{H}_4$ but 2 is not belong $\mathbb{H}_4$.
And also is not maximal ideal in Z 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. [*13*] *Let R be a commutative ring with unity, and let $I \neq R$ be an ideal in R. Then R/I is an integral domain if and only if I is prime ideal in R.*

Theorem 1.1.6. [*16*] *Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R if and only if R/M is a field.* □

Corollary 1.1.7. [*13*] *Every maximal ideal in a commutative ring R with unity is a prime ideal, but the converse is not true.*

Definition 1.1.15. [13] A sided ideal I of a commutative ring R is called a principal ideal if there exists an element $g \in I$ such that $I =< g >$, where

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

The element g is called a generator of I and I is said to be generated by g.

Example 1.1.4. [13] $\mathbf{Z}$ *is a principal ideal domain. Moreover, given any nonzero ideal* I *of* $\mathbf{Z}$, *the smallest positive integer in* I *is a generator for the ideal* I.

Definition 1.1.16. [5] A local ring is a ring that has a unique maximal ideal.

Homomorphisms and Isomorphisms

Definition 1.1.17. [13] Let R and S be rings (or fields).
A function $\psi{:}R \longrightarrow\ S$ is a **ring homomorphism** if for all $a, b \in\ R$,

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

and

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

Definition 1.1.18. [13] An **isomorphism** $\psi{:}\ R \longrightarrow S$ is a homomorphism that is one-to-one and onto S.

Definition 1.1.19. [13] Let $f{:}R \longrightarrow S$ be a homomorphism, we define **kernel** of f by

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

where 0 is a zero of S.

Theorem 1.1.8. [13] *If* $f{:}R \longrightarrow\ S$ *is a homomorphism, then*

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

Polynomial Rings

Definition 1.1.20. [13] Let R be a ring. A polynomial $f(x)$ with coefficients in 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 $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The $a_i's$ 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 $a_i \neq 0$, then the degree of $f(x)$ is undefined.

Let 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 R are defined in a way familiar to us. Let

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

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

be two polynomials over 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

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

Product 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 $R[x]$ be the set of all polynomials over 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 R has unity 1 then the polynomial $e(x) = 1 + 0x + 0x^2 + \ldots$ will be unity of $R[x]$. $e(x)$ is also sometimes denoted by 1. Instead of a ring R if we start with a field F we get the corresponding ring $F[x]$ of polynomials.

Theorem 1.1.9. *[16] Let $R[x]$ be the ring of polynomials over a ring R, then*

(i) R is commutative if and only if $R[x]$ is commutative.

(ii) R has unity if and only if $R[x]$ has unity. □

Theorem 1.1.10. *[16] Let $R[x]$ be the ring of polynomial of a ring 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 R is an integral domain, $deg(f(x)g(x)) = m + n$.

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

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

Definition 1.1.21. [13] Let $f(x)$ and $g(x)$ be polynomials over the field F. If $\gcd(f(x), g(x)) = 1$, we say that $f(x)$ and $g(x)$ are relatively prime (over F). In particular, $f(x)$ and $g(x)$ are relatively prime if and only if there exist polynomials $a(x)$ and $b(x)$ over F for which $a(x)f(x) + b(x)g(x) = 1$.

Definition 1.1.22. [13] A polynomial $f(x) \in R[x]$, is monic provided its leading coefficient is 1.

Definition 1.1.23. [5] Two polynomials f and g in $R[x]$ are called coprime, or relatively prime if

$$R[x] = < f > + < g > .$$

Definition 1.1.24. [16] A nonconstant polynomial $f(x) \in F[x]$ is irreducible if whenever $f(x) = p(x)q(x)$, then one of $p(x)$ or $q(x)$ must be constant.

1.2 Finite Fields

In this section we want to investigate the fundamental properties of finite fields.

Vector spaces over finite fields

Definition 1.2.1. [17] Let 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 F_q, is a vector space (or linear space) over F_q if it satisfies all of the following conditions. For all $u, v, w \in V$ and for all $\lambda, \mu \in F_q$:

(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 F_q, then $1u = u$.

Definition 1.2.2. [17] 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 1.2.3. [17] Let R be any ring, and let M be an abelian group, then M is called a **left R-module** if there exists a scalar multiplication
$\psi : R \times M \to M$ denoted by $\psi(r, m) = rm$, for all $r \in R$ and all $m \in M$, such that for all $r, r_1, r_2 \in R$ and all $m, m_1, m_2 \in M$,

(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 M is a left R-modulo.

Example 1.2.1. [*17*] *If R is a ring then R is an R-module (Left R-module and right R-module).*
Vector spaces over F are F-modules where F is a field.

Definition 1.2.4. [17] Any subset of M that is a left R-module under operations induced from M is called a **submodule**.
The subset $\{0\}$ is called the trivial submodule.
The module M is a submodule of itself.
i.e.if M is a left R-module, then a subset $N \subset M$ is a **submodule** if and only if it is nonempty, closed under sums, and closed under multiplication by elements of R.

Extension Field

Definition 1.2.5. [16] 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 1.2.6. [16] A finite field with p^m elements is called a Galois field of order p^m and is denoted by $GF(p^m)$.

Theorem 1.2.1. [*16*] *For any prime p and any positive integer m, there exists a finite field, unique up to isomorphism, with $q = p^m$ elements.* □

Lemma 1.2.2. [*15*] *For every element β of a finite field F with q elements, we have $\beta^q = \beta$.*

Definition 1.2.7. [13] The order of a nonzero element $\alpha \in F_q$, denoted by $ord(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$.

Definition 1.2.8. [13] **(Primitive Root of Unity)** An element α of a field is an nth root of unity if $\alpha^n = 1$, $n = q - 1$.
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 F_q is called a primitive element (or a generator) of F_q if $F_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.

Theorem 1.2.3. [*15*] *The elements of F_q are precisely the roots of the polynomial $x^q - x$.* □

Theorem 1.2.4. [*13*] ***Division Algorithm***
Let $f(x)$ and $g(x)$ be in $F_q[x]$, where $F_q[x]$ is the ring of all polynomials over the field F_q with $g(x)$ nonzero, then

1. *There exist unique polynomials $h(x)$, $r(x) \in F_q[x]$, such that*
   $f(x) = g(x)h(x) + r(x), \qquad \text{where } 0 \leq \ deg \ \ r(x) < deg \ \ g(x) \text{ or } r(x) = 0.$

2. *If $f(x) = g(x)h(x)+r(x)$, then $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$.* □

Corollary 1.2.5. [*16*] *Let $f(x) \in F[x]$, then α is root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$ over F*

Definition 1.2.9. [13] **(Extension Field)** A field E is called an extension of a field F if $F \subseteq E$ and we write $F \leq E$.
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 1.2.6. [*13*] *Let F be a field and let $f(x) \in F[x]$ be a nonconstant polynomial. Then there exist an extension E of F and $\alpha \in E$ such that $f(\alpha) = 0$.*

Example 1.2.2. [*13*] *Let $F = \mathbf{R}$ and let $f(x) = x^2 + 1$, which is well known to have no zeros in $\mathbf{R}$ and thus is irreducible over $\mathbf{R}$.*
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 $E = \mathbf{R}[x]/ < x^2 + 1 >$.

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 $x^2 + 1$.

Minimal Polynomials

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

Definition 1.2.10. [15] A minimal polynomial of an element $\alpha \in F_{q^m}$ with respect to F_q is a nonzero monic polynomial $f(x)$ of the least degree such that $f(\alpha) = 0$.

Theorem 1.2.7. [*16*] *Let $F < E$ be fields, and let $\alpha \in E$ have minimal polynomial $m(x)$ over F.*

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

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

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

Definition 1.2.11. [16] Let n be coprime to q. The cyclotomic coset of q (or q-cyclotomic coset) modulo n containing i is defined by

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

A subset $\{i_1, \dots, i_t\}$ of 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 $\bigcup_j^t C_{i_j} = Z_n$.

Example 1.2.3. [*15*] *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 1.2.4. [*15*] *The polynomial* $f(x) = 1 + x + x^3$ *is irreducible over* F_2*; if it were reducible, it would have a factor of degree* 1 *and hence a root in* F_2*, which it does not. So* $F_8 = F_2 / < f(x) >$*, The elements of* F_8 *for the given polynomial* $f(x)$*, are given by:*

$Cosets$	$Vectors$	$Polynomials\ in\ \alpha$	$Power\ of\ \alpha$
$0+ < f(x) >$	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 1.2.5. [*15*] *The field* F_8 *was constructed in the Example above. In the table below we give the minimal polynomial over* F_2 *of each element of* 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	$\{3,5,6\}$

1.3 Basic Concepts of Coding Theory

Coding theory deals with the problem of detecting and / or 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 poulses.

Codes, generator and parity check matrices

Definition 1.3.1. [15] Let F_q^n denote the vector space of all $n-$tuples over finite field F_q, n is the length of the vectors in F_q^n. An (n, M) code C over F_q is a subset of F_q^n of size M, that is $|C| = M$ =the number of all codewords of C.

We usually write the vectors $(c_1, c_2, \ldots, c_n)$ in F_q^n in the form $c_1c_2\ldots\ c_n$ and call the vectors in C codewords .

A code whose alphabet is $Z_2 = F_2 = \{0, 1\}$ is called a binary code or a Z_2-code, a code whose alphabet is $Z_3 = F_3 = \{0, 1, 2\}$ is called a ternary code or a Z_3-code, and a code whose alphabet consists of four elements such as $Z_4 = \{0, 1, 2, 3\}$ is called quaternary code or a Z_4-code.

Definition 1.3.2. [15] If C is a $k-$dimentional subspace of F_q^n, then C will be called an $[n, k]$ linear code over F_q .

Definition 1.3.3. [13] The **rank** of a matrix over k is the number of nonzero rows in any row echelon form of the matrix.

Definition 1.3.4. [15] 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 1.3.5. [15] 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 or (systematic) form.

Theorem 1.3.1. *[15] If $G = [I_k|A]$ is a generator matrix for the $[n, k]$ code C is in systematic form, then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C.*

Example 1.3.1. *The matrix $G = [I_4|X]$, where*

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

is a generator matrix in standard form for [7,4] binary code by Theorem 1.3.1. A parity-check matrix is $H = [X^T|I_3]$, where

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

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

Dual codes and weight distribution

Definition 1.3.6. [15] Let C be a linear $[n, k]$-code. The set

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

is called the **dual code** for C, where **x.c** is the usual scalar product $x_1c_1+x_2c_2+......+x_nc_n$ of the vectors **x** and **c**. **Note** that $C^{\perp}$ is an $[n, n-k]$ code. Also the generator matrics G for the linear code C=the parity check matrics H for the code $C^{\perp}$.

Definition 1.3.7. [15] The inner product of vectors $x = x_1 \dots x_n$, $y = y_1 \dots y_n$ in F_q^n is

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

Definition 1.3.8. [15]

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

Definition 1.3.9. [15] 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 1.3.2. [*15*] *If $x,\ y \in\ F_q^n$, 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 1.3.3. [*15*] *The distance function $d(x, y)$ satisfies the following four properties:*

(i) (non-negativity) $d(x, y) \geq 0$ for all $x,\ y \in F_q^n$.

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

(iii) (symmetry) $d(x, y) = d(y, x)$ for all $x,\ y \in F_q^n$.

(iv) (triangle inequality) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x,\ y,\ z \in F_q^n$. □

Example 1.3.2. *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.*

Definition 1.3.10. [15]

- The (**Lee weight**) $wt_L(x)$ of a vector $x \in \ F_q^n = n_1(x) + 2n_2(x) + n_3(x)$, where $n_a(x)$ denotes the number of components of x equal to a.
- The (**Lee distance**)$d(x, y)$ between two vectors $x,\ y \in F_q^n = w_L(x - y)$.

Definition 1.3.11. [15] 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 1.3.3. *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 1.3.12. [15] A code $\mathcal{C}$ is called self-orthogonal provided $\mathcal{C} \subseteq \mathcal{C}^{\perp}$.

Definition 1.3.13. [15] A code $\mathcal{C}$ is called self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$.

Remark 1.3.1. [15] The length n of a self-dual code C is even and the dimension of C is $n/2$.

1.4 Cyclic Codes over Finite Fields

*O*ne 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. Moreover 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 F_q, we will most often represent the codewords in polynomial form. There is bijective correspondence between the vectors $\mathbf{c} = c_0c_1 \ldots c_{n-1}$ in F_q^n and the polynomials $c(x) = c_0 + c_1x + \ldots c_{n-1}x^{n-1}$ in $F_q[x]$ of degree at most $n-1$. Notice that if $c(x) = c_0 + c_1x + \ldots c_{n-1}x^{n-1}$, then $xc(x) = c_{n-1}x^n + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1}$, 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 $x^n - 1$. Also the cyclic code C will correct $t = \lfloor (d-1)/2 \rfloor$ errors.

Polynomials and Words

The polynomial $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ of degree at most $n-1$ over field $\mathbb{K}$ may regarded as the word $v = a_0a_1a_2 \ldots a_{n-1}$ 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 1.4.1. [14] Let v be a word of length n, the cyclic shift $\pi(v)$ is the word of length n

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

Definition 1.4.2. [15] A code C is said to be cyclic if $\pi(v) \in C$, whenever $v \in C$.

Example 1.4.1. $C_1 = \{102, 210, 021, 201, 120, 012, 222, 111, 000\}$ *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 1.4.1. [15] *If* C_1 *and* C_2 *are cyclic codes of length* n *over* 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 $F_q[x]$ is principle ideal domain also the ring $R_n = F_q[x]/ < x^n - 1 >$ is a principle ideal hence the cyclic codes are principle ideals of R_n when writing a code word of a cyclic code as c(x) we mean the coset $c(x)+ < x^n - 1 >$ in R_n.

Corollary 1.4.2. [15] *The number of cyclic codes in* R_n *equal* 2^m, *where* m *is the number of q-cyclotomic cosets modulo n. Moreover, the dimensions of cyclic codes in* R_n *are all possible sums of the sizes of the q-cyclotomic cosets modulo n.*

Generating polynomial of a cyclic code

Theorem 1.4.3. [15] *A linear code* C *in* F_q *is cyclic* $\iff$ C *is an ideal in* $R_n = F_q[x]/(x^n - 1)$.

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

($\Rightarrow$) 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 1.4.4. [15] *Let* C *be an ideal in* 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 polynomials 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 $< g(x) >\subseteq C$.
On the other hand, Suppose that $p(x) \in C$, then by Division Algorithm $\exists\, q(x),\ r(x)$ such that

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

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 $C \subseteq< g(x) >$. Thus $C =< g(x) >$.

(ii) Dividing $x^n - 1$ by $g(x)$, using Division Algorithm we have

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

Since C is an ideal in $\mathbb{R}_n$, we see that $r(x) \in C$, a contradiction unless $r(x) = 0$, 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 $g(x)$ 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 $\deg(s(x)) < n - r$ or $s(x) = 0$, 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. □

Corollary 1.4.5. [15] *Let C be a nonzero cyclic code in R_n. The following are equivalent:*
(i) $g(x)$ is the monic polynomial of minimum degree in C.
(ii) $C =< g(x) >$, $g(x)$ is monic, and $g(x)|(x^n - 1)$.

The Parity Check Matrix

Theorem 1.4.6. *[15] Let C be a cyclic cod in R_n with generator polynomial $g(x)$, such that deg $g(x) = r$. Let $h(x) = (x^n - 1)/g(x) = \sum_{i=0}^{n-r} h_i x^i$. Then the generator polynomial of $C^\perp$ is $g^\perp(x) = x^{n-r}h(x^{-1})/h(0)$. Furthermore, a generator matrix for $C^\perp$, and hence a 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 1.4.2. *Let C be a cyclic code of length $n = 9$. Since $x^9 - 1$ factors over 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 $R_9 = F_2/ < x^9 - 1 >$. 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

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

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 Procedure:[15]

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

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

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 $m(x) = a_0 + a_1x + \ldots + a_{k-1}x^{k-1} \in \mathbb{F}_q[x]$, then to encode $m(x)$ as a codeword $c(x)$ by forming the product $c(x) = m(x)g(x)$. However, this encoding is not systematic.

Example 1.4.3. *[15] 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 procedure, we have
$g(x) = 1 + x^4 + x^6 + x^7 + x^8$.
$c(x) = m(x)g(x) = (1 + x^2 + x^5)(1 + x^4 + x^6 + x^7 + x^8) =$
$1 + x^2 + x^4 + x^5 + x^7 + x^{10} + x^{11} + x^{12} + x^{13} \longleftrightarrow (101011010011110)$.

The Second Procedure:[15]

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 1.4.4. *[15] 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 procedure, we have
$g(x) = 1+x^4+x^6+x^7+x^8$.
$x^{n-k} = x^{15-7} = x^8$.
$x^8 m(x) = x^8.(1+x^2+x^5) = x^8+x^{10}+x^{13}$.
Now divide $x^8 m(x)$ by $g(x)$.

$$
\begin{array}{l|l}
 & x^5+x^4+x+1 \\ \cline{2-2}
\underline{x^8+x^7+x^6+x^4+1} & x^{13}+ \qquad\qquad +x^{10}+ \quad +x^8 \\
 & \underline{x^{13}+x^{12}+x^{11}+ \quad +x^9+ \quad +x^5} \\
 & x^{12}+x^{11}+x^{10}+x^9+x^8+x^5 \\
 & \underline{x^{12}+x^{11}+x^{10}+ \quad +x^8+ \quad +x^4} \\
 & x^9+ \qquad\qquad\qquad +x^5+x^4 \\
 & \underline{x^9+x^8+x^7+ \qquad\quad +x^5+ \quad +x} \\
 & x^8+x^7+ \qquad\qquad\qquad +x^4+x \\
 & \underline{x^8+x^7+x^6+ \qquad\qquad +x^4+1} \\
 & \qquad\qquad x^6+x+1
\end{array}
$$

$x^8 m(x) = g(x).(x^5+x^4+x+1) + (x^6+x+1)$
$c(x) = x^8 m(x) + (x^6+x+1) = (x^{13}+x^{10}+x^8) + x^6+x+1$
as a vector $C = (110000101010010) \in \mathbb{F}_q^n$.

Decoding With Cyclic Code

Following [15], 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 received, 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 1.4.3. [15] 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

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

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

Theorem 1.4.7. *[15] 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 1.4.8. *[15] 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* $s(x)$. □

We now describe the first version of the Meggitt Decoding Algorithm and use example to illustrate each step. Define 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 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 1.4.5. *[15] 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 computations of these syndrome polynomials were aided by Theorem 1.4.7 and 1.4.8. 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 1.4.7(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 1.4.7 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 1.4.7($iv$), $S(y(x)) = S(e(x))$, where $y(x) = c(x) + e(x)$ with $c(x) \in C$.

Example 1.4.6. *[15] Continuing with Example* 1.4.5, *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 in the list, go on to Step IV.

Step IV:

Compute the syndrome polynomial of $xy(x),\ x^2y(x),\ \ldots$ 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 1.4.8 As $R_{g(x)}(x^{n-k}y(x)) = S(y(x)) = \sum_{i=0}^{n-k-1} s_ix^i$, $S(xy(x)) = R_{g(x)}(x^{n-k}xy(x)) = R_{g(x)}(x(x^{n-k}y(x))) = R_{g(x)}(xS(y(x))) = xS(y(x)) - s_{n-k-1}g(x)$.

Example 1.4.7. *[15] Continuing with Example* 1.4.6*, 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* 1.4.5
$S(x^2y(x)) = x(1 + x^2 + x^3 + x^4 + x^6) - 0.g(x) = x + x^3 + x^4 + x^5 + x^7$*, which corresponds to the error $x^4 + x^{14}$ implying that $y(x)$ is decoded as*
$y(x) - (x^2 + x^{12}) = 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$.

1.5 Codes over Rings

Definition 1.5.1. [20] $R_2 = F_2 + uF_2$ is a commutative ring $\{0, 1, u, 1 + u\}$ with $u^2 = 0$, where F_2 is a binary field with two elements $\{0, 1\}$. Addition and multiplication operations for $F_2 + uF_2$ are given in the following tables:

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

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

Definition 1.5.2. [4] $R_3 = F_2 + uF_2 + u^2F_2$ is a commutative ring of 8 elements which are $\{0, 1, u, u^2, v, v^2, uv, v^3\}$, where $u^3 = 0$, $v = 1 + u$, $v^2 = 1 + u^2$, $v^3 = 1 + u + u^2$, $uv = u + u^2$. Addition and multiplication operations over R 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

$\cdot$	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^3	uv	1	u^2	u	v	v^2

Definition 1.5.3. [3] A code of length n over a commutative ring R is a nonempty subset of R^n, and a code is linear over R if it is an R-submodule of R^n.

Definition 1.5.4. [15] Let Z_{p^n} be the ring of integer modulo p^n, where p is a prime number and n a positive integer. A polynomial $f(x) \in Z_{p^n}[x]$ is said to be irreducible if whenever $f(x) = g(x)h(x)$ for two polynomials $g(x)$ and $h(x)$ in $Z_{p^n}[x]$, one of $g(x)$ or $h(x)$ is a unit.

Definition 1.5.5. [15] Define $\mu : Z_4[x] \rightarrow F_2[x]$ by $\mu\big(f(x)\big) = f(x)$ $(mod\ 2)$. The map μ called reduction homomorphisim. A polynomial $f(x) \in Z_4[x]$ is basic irreducible if

$\mu\big(f(x)\big)$ is irreducible in $F_2[x]$; it is monic if its leading coefficient is 1. A polynomial $f(x) \in Z_4[x]$ is primary if the principal ideal $< f(x) >= \{f(x)g(x) \mid g(x) \in Z_4[x]\}$ is a primary ideal.

Definition 1.5.6. [15] An ideal I of a ring R is called a primary ideal provided $ab \in I$ implies that $a \in I$ *or* $b^r \in I$ for some positive integer r.

Definition 1.5.7. [5] Let Z_{p^n} be the ring of integer modulo p^n, where p is a prime number and n a positive integer. A monic irreducible polynomial $f(x) \in Z_{p^n}[x]$ is said to be basic irreducible if its reduction modulo p is irreducible.

Theorem 1.5.1. [*15*] ***(Hensels Lemma)***
Let $f(x) \in Z_4[x]$. 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 $F_2[x]$. Then there exist $g_1(x), g_2(x), \dots, g_k(x) \in Z_4[x]$ 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. *$f(x) = g_1(x)g_2(x)...g_k(x)$.* □

Graeffe's method[15]
(1). Let $h(x)$ be an irreducible factor of $x^n + 1$ in $F_2[x]$. 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.
(2). Then $g(x)$ is the irreducible factor of $x^n - 1$ in $Z_4[x]$, with $\mu\big(g(x)\big) = h(x)$, where $g(x^2) = \pm\big(e(x)^2 - o(x)^2\big)$.

Example 1.5.1. *In $F_2[x]$, $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ is the factorization of $x^7 + 1$ into irreducible polynomials. We apply Graeffe's method to each factor to obtain the factorization of $x^7 - 1$ into monic irreducible polynomials of $Z_4[x]$.*
(1). If $h(x) = x^1 + x^0 = x + 1$, then $e(x) = 1$ and $o(x) = x$. So $g(x^2) = -(1 - x^2) = x^2 - 1$

and thus $g(x) = x - 1$. *Also* $\mu\big(g(x)\big) = g(x)\ (mod\ 2) = x - 1\ (mod\ 2) = (x+1)\ (mod\ 2) = h(x)$.

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

(3). 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* $Z_4[x]$.

Definition 1.5.8. [5]The **Galois ring** $GR(p^n, m)$ is defined as :

$$GR(p^n, m) = Z_{p^n}[x]/\langle f(x)\rangle$$

where $f(x) \in Z_{p^n}[x]$ is a monic, basic, irreducible polynomial of degree m dividing $x^{p^{m-1}} - 1$ and $\langle f(x)\rangle$ is the ideal of $Z_{p^n}[x]$ generated by $f(x)$.

Example 1.5.2. *[5]*

- $GR(p, m) = F_{p^m}$, $\quad GR(p^s, 1) = Z_{p^s}$.

- *Let* $h(x) = x^3 + x + 1 \in Z_4[x]$ *which is monic, basic irreducible over* Z_4. *Then* $GR(2^2, 3) = Z_4[x]/\langle h(x)\rangle$.

- *Let* $g(x) = x^3 + 2x^2 + x - 1 \in Z_4[x]$ *which is also monic, basic, irreducible over* Z_4. *Then* $GR(2^2, 3) = Z_4[x]/\langle g(x)$.

Chapter 2

Cyclic Codes over Z_4 of Even Length

Cyclic codes are important class of codes from both a theoretical and a practical viewpoint. The key to describe the structure of cyclic codes over a ring R is to view cyclic codes as ideals in the polynomial ring $R[X]/\langle X^n - 1\rangle,$ where n is the length of the code. For this purpose, it is useful to obtain the divisors of $X^n - 1$, but this becomes difficult when the characteristic of the ring is not relatively prime to the length of the code, because then $X^n - 1$ does not factor uniquely over the ring. For codes over $Z_4,$ this case corresponds to the case, when the length is even. The structure of cyclic codes over rings of odd length n has been discussed in Bonnecaze and Udaya [7], Calderbank [8], Dougherty and Shiromoto [11], and van Lint [22]. Calderbank and Sloane [9], and Pless [19] presented a complete structure of cyclic codes over Z_4 of odd length. In[1], Abualrub and Oehmke determine the generators for cyclic codes over Z_4 for lengths of the form 2^k and in [6], Blackford determines the generators of cyclic codes over Z_4 for lengths of the form $2n$ where n is odd. In this chapter we shall complete the classification by examining cyclic codes over Z_4 of length $N = 2^k n,$ where n is odd.

2.1 Background

Definition 2.1.1. [12] Let C be a code of length n over a finite chain ring R of characteristic 4 with unique maximal ideal m, then we can define the torsion and residue codes over the residue field $F := R/m$ of characteristic 2 by

$$\mathrm{Tor}(C) = \{v \in F^n : 2v \in C\} \text{ and } \mathrm{Res}(C) = \{v \in F^n : \exists u \text{ such that } v + 2u \in C\}.$$

We can describe the generator matrices of these codes over Z_4. A linear code over Z_4 has a generator matrix that is permutation-equivalent to the standard matrix $\begin{bmatrix} I_{k_1} & A & A' \\ 0 & 2I_{k_2} & 2A'' \end{bmatrix}$, where I_{ki} is the identity matrix of size k_i, A and A'' are matrices with entries from $\{0,1\}$, and A' is a matrix with entries from Z_4. A code of this form is said to be of type $\{k_1, k_2\}$. It contains $4^{k_1}2^{k_2}$ elements. The code over $F_2 = \{0,1\}$ with generator matrix $\begin{bmatrix} I_{k_1} & A & \overline{A'} \end{bmatrix}$, where $\overline{A'}$ is the reduction modulo 2 of A', is the residue code. The code over F_2 with generator matrix $\begin{bmatrix} I_{k_1} & A & \overline{A'} \\ 0 & I_{k_2} & A'' \end{bmatrix}$ is the torsion code .
Notice that $\big|\mathrm{Tor}(C)\big|\big|\mathrm{Res}(C)\big| = 2^{k_1}2^{k_1+k_2} = 4^{k_1}2^{k_2} = |C|$.
Notation: We assume throughout this chapter that n is an odd integer and $N = 2^k n$ will denote the length of a cyclic code over Z_4.

Define the ring $R = Z_4[u]/\langle u^{2^k} - 1\rangle$. We have a module isomorphism $\psi : R^n \to (Z_4)^{2^k n}$ defined by

$$\psi\Big(u\big(\sum_{j=0}^{2^k-1} a_{n-1,j}u^j\big),\ \sum_{j=0}^{2^k-1} a_{0,j}u^j,\ \sum_{j=0}^{2^k-1} a_{1,j}u^j, \ldots,\ \sum_{j=0}^{2^k-1} a_{n-2,j}u^j\Big)$$
$$= \big(a_{n-1,2^k-1}, a_{0,0}, a_{1,0}, \ldots, a_{n-2,2^k-1}\big).$$

This gives that a cyclic shift in $(Z_4)^{2^k n}$ corresponds to a constacyclic shift in R^n by u. For a positive integer m, we define the following Galois ring

$$\mathrm{GR}(4, m) = Z_4[X]/\langle h_m(X)\rangle,$$

where $h_m(X)$ is a monic basic irreducible polynomial in $Z_4[X]$ of degree m that divides $X^{2^m-1}-1$. This ring is local with maximal ideal $\langle 2\rangle$ and residue field F_{2^m}. The polynomial h_m is chosen so that $\xi = X + \langle h(X)\rangle$ is a primitive (2^m-1) st root of unity.

Definition 2.1.2. [12] The set $\tau_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$ is a complete set of coset representatives modulo 2 and is called the Teichmüller set.

Each $z \in \mathrm{GR}(4, m)$ has a unique 2-adic expansion $z = z_0 + 2z_1$, with $z_0, z_1 \in \tau_m$. Define the ring $R_4(u, m) = \mathrm{GR}(4, m)[u]/\langle u^{2^k} - 1\rangle$.

2.2 Construction the Ideals of $R_4(u, m) = \mathrm{GR}(4, m)[u]/\langle u^{2^k} - 1\rangle$.

Lemma 2.2.1. *[12] Let $S = R_4(u, m)$.*

(i) Every element $z \in S$ is uniquely written as

$$z = \sum_{i=0}^{2^k-1} \big(z_{i,0} + 2z_{i,1}\big)\big(u-1\big)^i,\ z_{i,j} \in \tau_m.$$

(ii)An element $z \in S$, written as in (i), is a unit if and only if $z_{0,0} \neq 0$.

(iii) S is local ring with maximal ideal $\langle 2, u-1\rangle$ and residue field F_{2^m}.

(iv) The ideals of S are:

- $\langle 0\rangle$,
- $\langle 1\rangle$,
- $\langle 2(u-1)^i\rangle$, *where* $0 \leq i \leq 2^k - 1$,
- $\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j\rangle$, *where* $1 \leq i \leq 2^k - 1$, *and* $s_j \in \tau_m \forall\ j$,
- $\langle 2(u-1)^l, (u-1)^i + 2\sum_{j=0}^{l-1} s_j(u-1)^j\rangle$, *where* $1 \leq i \leq 2^k - 1$, $l < i$ *and* $s_j \in \tau_m \forall\ j$.

Proof. (i) Since every element $z \in \mathrm{GR}(4, m)$ has a unique 2-adic expansion $z = z_0 + 2z_1$, with $z_0, z_1 \in \tau_m$. Then, we choose to expand in $(u-1)$ rather in u to get the result.

(ii) If $z \in S$ is a unit, then $z \mod 2$ is a unit in $F_{2^m}[u]/\langle (u-1)^{2^k}\rangle$, which is equivalent to $z_{0,0} \neq 0$. Conversely, for an element $z = x + 2y \in S$, Suppose $z \mod 2$ is a unit in $F_{2^m}[u]/\langle (u-1)^{2^k} \rangle$. Then there exists $x' \in S$ such that $x'x = 1 \mod 2$, i.e, $x'x = 1 + 2\mu$, for some $\mu \in S$. Then

$$\begin{aligned}(x+2y)\big(x' + 2(-\mu - x'y)x'\big) &= xx' + 2\big(yx' + xx'(-\mu - x'y)\big)\\ &= 1 + 2\big(yx' - \mu - x'y + \mu\big) = 1,\end{aligned}$$

so $x' + 2(-\mu - x'y)x'$ is an inverse of z, i.e z is a unit in S.

(iii) We have that $S/\langle 2, u-1 \rangle \cong F_{2^m}$ a field, so $\langle 2, u-1 \rangle$ is a maximal. To show this ideal is the unique maximal ideal, we shall show that any element not in the ideal $\langle 2, u-1 \rangle$ is a unit.

If $z = \sum_{i=0}^{2^k-1} (z_{i,0} + 2z_{i,1})(u-1)^i$ not in $\langle 2, u-1 \rangle$, then $z_{0,0} \neq 0$ and therefore z is a unit by (ii).

(iv) We have the trivial ideals $\langle 0 \rangle$ and $S = \langle 1 \rangle$. Let I be an ideal of S, distinct from $\langle 0 \rangle$ and $\langle 1 \rangle$. If $I \subseteq \langle 2 \rangle$, any element I can be written in the form

$$2s_0 + 2s_1(u-1) + \ldots + 2s_{2^k-1}(u-1)^{2^k-1}, \text{ where } s_j \in \tau_m.$$

Let $s \in I$ be an element with the smallest i with $s_i \neq 0$.

For all $t \in I$, $t = 2\big(u-1\big)^i\big(t_i + t_{i+1}(u-1) + \ldots + t_{2^k-1}(u-1)^{2^k-1-i}\big)$, where $t_j \in \tau_m$. Therefore $I \subseteq \big\langle 2(u-1) \big\rangle$.

Since $s = 2\big(u-1\big)^i\big(s_i + s_{i+1}(u-1) + \ldots + s_{2^k-1}(u-1)^{2^k-1-i}\big)$, where $s_j \in \tau_m$ and $s_i \neq 0$, this means that $\big(s_i + s_{i+1}(u-1) + \ldots + s_{2^k-1}(u-1)^{2^k-1-i}\big)$ is invertible and hence $2(u-1)^i \in I$, which implies, $I = \big\langle 2(u-1)^i \big\rangle$.

Hence all ideals contained in $\langle 2 \rangle$ are of the form $\big\langle 2(u-1)^i \big\rangle$, $0 \leq i \leq 2^k - 1$.

Now assume I is not contained in $\langle 2 \rangle$. Let

$$I' = \{v : v \equiv w \mod 2,\ w \in I\}.$$

Then I' is an ideal in $F_{2^m}[u]/\langle (u-1)^{2^k} \rangle$. Since I is not contained in $\langle 2 \rangle$, I' is not the zero ideal $\langle 0 \rangle$. The nonzero ideals in $F_{2^m}[u]/\langle (u-1)^{2^k} \rangle$, distinct from $\langle 1 \rangle$, are of the form $\big\langle (u-1)^i \big\rangle$, $1 \leq i \leq 2^k - 1$. Therefore $I' = \big\langle (u-1)^i \big\rangle$ with $1 \leq i \leq 2^k - 1$. Hence there exists an element $(u-1)^i + 2s \in I,$ for some $s \in S$. Without loss of generality, we may write

$$(u-1)^i + 2s = (u-1)^i + 2\sum_{j=0}^{2^k-1} s_j (u-1)^j, \text{ where } s_j \in \tau_m.$$

Since $2(u-1)^i = 2\big((u-1)^i + 2s\big) \in I,$ it follows that $2s_j(u-1)^j \in I$ for all $i \leq j \leq 2^k - 1$. Therefore $(u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \in I$.

Now we divide into two subcases.

Subcase 1:

$I = \Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle.$

This is the fourth type of ideals in the list of lemma 2.2.1 (iv).

Subcase 2: $\Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle \subset I$

Let $g = (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j$. Let $r \in I/\Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle$. There exists r' such that $z = r - r'g \in\ I$ can be written as

$$z = (z_{0,0} + 2z_{0,1}) + (z_{1,0} + 2z_{1,1})(u-1) + \ldots + (z_{i-1,0} + 2z_{i-1,1})(u-1)^{i-1}.$$

Denoting the image of z in $F_{2^m}[u]/\big\langle (u-1)^{2^k} \big\rangle$ by $\overline{z}$, we have $\overline{z} \in \big\langle (u-1)^i \big\rangle$, so

$$z_{0,0} = z_{1,0} = \ldots = z_{i-1,0} = 0.$$

Thus we have

$z = 2(u-1)^\lambda\big(z_{\lambda,1} + z_{\lambda+1,1}(u-1) + \ldots + z_{i-1,1}(u-1)^{i-1-\lambda}\big)\ \ldots\ \ \ldots\ \ \ldots(\star)$, with $z_{\lambda,1} \neq 0$, for some $\lambda < i$. Since $z_{,1} \neq 0$, (ii) shows that $z_{\lambda,1} + z_{\lambda+1,1}(u-1) + \ldots + z_{i-1,1}(u-1)^{i-1-\lambda}$ is a unit. Consequently, $2(u-1)^\lambda \in\ I$. For each $r \in\ I\backslash\big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \big\rangle$, we obtain such a λ. Let l be the smallest of these λ. Then

$$\Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j, 2(u-1)^l \Big\rangle \subseteq I.$$

By $(\star)$ and the definition of l for every $r \in\ I$, there exists some $r' \in\ I$ such that $r - r'g \in \big\langle 2(u-1)^l \big\rangle$ $\Big($*when* $r \in \Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle$, *there exists* r' *such that* $r - r' =$

$0 \in \langle 2(u-1)^l \rangle$, so

$$r \in \Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j,\ 2(u-1)^l \Big\rangle.$$

Therefore, $I = \big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j,\ 2(u-1)^l \big\rangle$.

Since $2(u-1)^l \in I$, it follows that, for $l \le j \le i-1$, we have $2s_j(u-1)^j \in I$. Therefore, it follows that

$$I = \Big\langle (u-1)^i + 2\sum_{j=0}^{l-1} s_j(u-1)^j,\ 2(u-1)^l \Big\rangle.$$

$\square$

Remark 2.2.1. [12] The ideal of the type $\Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle$, where $0 \le i \le 2^k - 1$, and $s_j \in \tau_m$ for all j, can be written in the form $\big\langle (u-1)^i + 2(u-1)^t h(u) \big\rangle$, where $0 \le t \le i-1$, and $h(u)$ is either 0 or a unit. Furthermore, we may write

$h(u) = \sum_j h_j(u-1)^j$, where $h_j \in \tau_m$ for all j. In particular, when $h(u)$ is a unit, then one of the following must hold:

(i) $h(u) = 1$;

(ii) $h(u) = 1 + (u-1)^\tau\, \widetilde{h}(u)$, where $\tau \ge 1$ and $\widetilde{h}(u)$ is a unit;

(iii) $h(u) = \displaystyle\sum_{j=0}^{i-t-1} h_j(u-1)^j$, with $h_0 \in \tau_m \backslash \{0,1\}$.

Suppose that T is the smallest integer such that $2(u-1)^T \in \Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle$. For an ideal of the type $\Big\langle 2(u-1)^l, (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle$, we may assume, without loss of generality, that $l < T$. Otherwise this ideal is actually $\Big\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j(u-1)^j \Big\rangle$. Notice that ideals in the ring S may be viewed equivalently as cyclic codes of length 2^k over $\mathrm{GR}(4,m)$.

Lemma 2.2.2. [*12*] *Let C be an ideal in S (or equivalently, a cyclic code of length 2^k over* $\mathrm{GR}(4,m)$ *). Then we have that*

$$\big|\mathrm{Res}(C)\big|\big|\mathrm{Tor}(C)\big| = \big|C\big|.$$

Proof. Consider the surjective reduction $\mod 2$ map $C :\to \text{Res}(C)$. The kernel of this map is $\{c \in C : c = 2v \text{ for some } v\}$. By identifying F_{2^m} with the Teichmüller set τ_m in GR(4,m), it follows that there is a natural bijection between this kernel and Tor(C). Hence, by the First Isomorphism Theorem of finite groups, we have

$$\big|\text{Tor}(C)\big| = \big|C\big| / \big|\text{Res}(C)\big|.$$

□

Theorem 2.2.3. *[12]*
The number of distinct ideals in $S = R_4(u,m) = \text{GR}(4,m)[u]/\langle u^{2^k} - 1\rangle$ *is*

$$5 + (2^m)^{2^{k-1}} + \big[(5.2^m) - 1\big](2^m)\frac{(2^m)^{2^{k-1}-1} - 1}{(2^m-1)^2} - 4\frac{2^{k-1}-1}{2^m-1}.$$

2.3 Discrete Fourier Transform

Following [12], we use the Discrete Fourier Transform to give the structure of cyclic codes in the ring $Z_4[X]/\langle X^N - 1\rangle$ where $N = 2^k n,\ n$ is odd as a direct sum of ideals in the ring $R_4(u,m)$. Let M be the order of 2 modulo n and let ζ denote a primitive nth root of unity in GR(4,M).

Definition 2.3.1. [12] Let
$c = \big(c_{0,0}, c_{1,0}, \ldots, c_{n-1,0}, c_{0,1}, c_{1,1}, \ldots, c_{n-1,1}, \ldots, c_{0,2^k-1}, c_{1,2^k-1}, \ldots, c_{n-1,2^k-1}\big) \in \big(Z_4\big)^N$, $N = 2^k n$ (n *odd*), with $c(x) = \displaystyle\sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j}x^{i+jn}$ the corresponding polynomial. The Discrete Fourier Transform of $c(x)$ is the vector

$$(\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{n-1}) \in R_4(u,M)^n$$

with $\hat{c}_n = c\big(u^{\acute{n}}\zeta^h\big) = \displaystyle\sum_{i=0}^{n-1}\sum_{j=0}^{2^k-1} c_{i,j^{u^{\acute{n}i+j}}\zeta^{hi}}$
for $0 \leq h < n$, where $n\acute{n} \equiv 1 \mod 2^k$.
Define the Mattson-Solomon polynomial of c to be $\hat{c}(Z) = \sum_{h=0}^{n-1} c_{n-h}Z^h$ (Here, $\hat{c}_0 = \hat{c}_n$).

Lemma 2.3.1. (**Inversion formula**)[*12*]
Let $c \in (Z_4)^N$, *where* $N = 2^k n$ (n *odd*), *with* $\hat{c}(Z)$ *its Mattson-Solomon polynomial as defined above. Then*

$$c = \psi\Big[\big(1, u^{-\acute{n}}, u^{-2\acute{n}}, \ldots, u^{-(n-1)\acute{n}}\big) * \frac{1}{n}\big(\hat{c}(1), \hat{c}(\zeta), \ldots, \hat{c}(\zeta^{n-1})\big)\Big]$$

where $*$ *indicates componentwise multiplication.*

Proof. Let $0 \le t \le n-1$. Then

$$\begin{aligned}
\hat{c}(\zeta^t) &= \sum_{h=0}^{n-1} \hat{c}_h \zeta^{-ht} \\
&= \sum_{h=0}^{n-1} \Big(\sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{\acute{n}i+j} \zeta^{hi}\Big) \zeta^{-ht} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{\acute{n}i+j} \sum_{h=0}^{n-1} \zeta^{h(i-t)} \\
&= (n u^{\acute{n}t}) \sum_{j=0}^{2^k-1} c_{t,j} u^j.
\end{aligned}$$

Hence $u^{-\acute{n}t}(\frac{1}{n})\hat{c}(\zeta^t) = \sum_{j=0}^{2^k-1} c_{t,j} u^j$. Noting that $u^{-i} = u^{2^{k+1}-i}$ in $R_4(u, M)$, we get the result. □

Notation: Let J denote a complete set of representatives of the 2-cyclotomic cosets modulo n and, for each $\alpha \in J$, let m_α denote the size of the 2-cyclotomic coset containing α.

The following theorem allows us to describe cyclic codes which are ideals in $Z_4[X]/\langle X^N - 1\rangle$ where $N = 2^k n$, n is odd in terms of ideals of $R_4(u, m_\alpha)$ which we have previously described.

Theorem 2.3.2. [*12*] *The map* $\gamma = Z_4[X]/\langle X^N - 1\rangle \to \bigoplus_{\alpha \in J} R_4(u, m_\alpha)$ *is a ring isomorphism, where* $\gamma\big(c(X)\big) = [\hat{c}_\alpha]_{\alpha \in J}$ *for* $c(X) \in Z_4[X]/\langle X^N - 1\rangle$.

Since a cyclic code of length $N = 2^k n$ over Z_4 can be regarded as an ideal in $Z_4[X]/\langle X^N - 1\rangle$, we have the following corollary.

Corollary 2.3.3. [*12*] *If C is a cyclic code of length $N = 2^k n$ over Z_4, then C is isomorphic $\bigoplus_{\alpha \in J} C_\alpha$, where for each $\alpha \in J$, C_α is an ideal in $R_4(u, m_\alpha)$.*

Proof. By Theorem 2.3.2 $Z_4[X]/\langle X^N - 1\rangle \cong \bigoplus_{\alpha \in J} R_4(u, m_\alpha)$, but C is an ideal in $Z_4[X]/\langle X^n - 1\rangle$ and $\forall \alpha \in J$, C_α is an ideal in $R_4(u, m_\alpha)$. So $C \cong \bigoplus_{\alpha \in J} C_\alpha$ over Z_4. $\square$

Notation: For each $\alpha \in J$, let N_α denote the number of distinct ideals in $R_4(u, m_\alpha)$, as given in Theorem 2.2.3, then the following result follows:

Corollary 2.3.4. [*12*] *The number of distinct cyclic codes over Z_4 of length $N = 2^k n$, (n odd) is $\prod_{\alpha \in J} N_\alpha$.*

Proof. Let N_α denote the number of distinct ideals in $R_4(u, m_\alpha)$ which is equivalent to the number of cyclic codes in $R_4(u, m_\alpha) \Rightarrow$ by Th.2.3.3 and Corollary 2.3.3, The number of distinct cyclic codes over Z_4 of length $N = 2^k n$ (n odd) is $\prod_{\alpha \in J} N_\alpha$ $\square$

Example 2.3.1. *(i) Consider cyclic codes of length 16 over Z_4,*
$\Rightarrow\ 16 = 2^4.1 \ \Rightarrow\ k = 4,\ n = 1,\ J = \{0\}$
$\Rightarrow$ *the 2-cyclotomic coset containing* 0 *is* $\{0\} \mod 1 \ \Rightarrow\ m_0 = 1 \ \Rightarrow$ *by Theorem 2.2.3*
$N_0 = 5 + 2^8 + (9)(2)(2^7 - 1) - 4(2^3 - 1) = 2519 \Rightarrow$ *by Corollary* 2.3.4*, there are 2519 cyclic codes of length 16 over Z_4.*
(ii) Consider cyclic codes of length 28 over $Z_4 \Rightarrow\ 28 = 2^2(7) \ \Rightarrow\ k = 2,\ n = 7$. The two cyclotomic cosets $\mod 7$ *are* $c_0 = \{0\},\ c_1 = \{1, 2, 4\},\ c_6 = \{6, 5, 3\}$
$\Rightarrow\ J = \{0, 1, 6\} \Rightarrow m_0 = 1,\ m_1 = 3,\ m_6 = 3$
$\Rightarrow\ N_0 = 5 + (2^1)^{2^{2-1}} + \left[(5.2^1) - 1\right](2^1)\frac{(2^1)^{2^{2-1}-1} - 1}{(2^1 - 1)^2} - 4\left(\frac{2^{2-1}}{2^1 - 1}\right) = 23,$
$N_1 = 5 + (2^3)^{2^{2-1}} + \left[(5.2^3) - 1\right](2^3)\frac{(2^3)^{2^{2-1}-1} - 1}{(2^3 - 1)^2} - 4\left(\frac{2^{2-1}}{2^3 - 1}\right) = 113.$ *Similarly $N_6 = 113$.*
$\Rightarrow$ *by Corollary* 2.3.4*, there are* $23.113.113 = 293687$ *cyclic codes of length 28 over Z_4.*

Remark 2.3.1. [12] (1) If $N = 2^k$, then $J_0 = \{0\}$. In this case $m_0 = 1$, then the number of cyclic codes of length 2^k is
$5 + 2^{2^{k-1}} + (9)(2)\left(2^{2^{k-1}} - 1\right) - 4\left(2^{2^{k-1}} - 1\right)$
$= 10.2^{2^{k-1}} - 4(2^{2^{k-1}}) - 9.$

(2) If $k=1$, then $N=2n \Rightarrow$ the number of ideals in $R_4(u,m_\alpha)$ is $5+2^{m_\alpha}$. Hence the number of cyclic codes of length $2n$ is $\prod_{\alpha\in J}(5+2^{m_\alpha})$.

2.4 Duals

Definition 2.4.1. [12] For an ideal C of $S=R_4(u,m)$, the annihilator $A(C)$ of C is defined to be the ideal $A(C)=\{g(u):g(u)f(u)=0,\ \forall f(u)\in C\}$.

Theorem 2.4.1. *[12] The annihilator $A(C)$ of the ideal C in $S=R_4(u,m)$ is of the following form :*

Case	C	$A(C)$
1	$\langle 0\rangle$	$\langle 1\rangle$
2	$\langle 1\rangle$	$\langle 0\rangle$
3	$\langle 2\rangle$	$\langle 2\rangle$
4	$\langle 2(u-1)^i\rangle$ $(1\le i\le 2^k-1)$	$\langle 2,(u-1)^{2^k-i}\rangle$
5	$\langle (u-1)^i\rangle$ $(1\le i\le 2^{k-1})$	$\langle (u-1)^{2^k-i}+2(u-1)^{2^{k-1}-i}\rangle$
6	$\langle (u-1)^i\rangle$ $(2^{k-1}+1\le i\le 2^k-1)$	$\langle 2(u-1)^{2^k-i},(u-1)^{2^{k-1}}+2\rangle$
7	$\langle (u-1)^i+2(u-1)^{i-2^{k-1}}\rangle$ $(2^{k-1}\le i\le 2^k-1)$	$\langle (u-1)^{2^k-i}\rangle$
8	$\langle (u-1)^i+2(u-1)^{i-2^{k-1}}(1+(u-1)^\tau\tilde{h}(u))\rangle$ $(2^{k-1}\le i\le 2^{k-1}+\tau,\ \tau\ge 1)$	$\langle (u-1)^{2^k-i}+2(u-1)^{2^{k-1}+\tau-i\tilde{h}(u)}\rangle$
9	$\langle (u-1)^i+2(u-1)^{i-2^{k-1}}(1+(u-1)^\tau\tilde{h}(u))\rangle$ $(2^{k-1}+\tau\le i\le 2^k-1,\ \tau\ge 1)$	$\langle 2(u-1)^{2^k-i},(u-1)^{2^{k-1}-\tau}+2\tilde{h}(u)\rangle$
10	$\langle (u-1)^{2^{k-1}}+2h(u)\rangle$ $(h_0\ne 0,1)$	$\langle (u-1)^{2^{k-1}}+2(1+h(u))\rangle$
11	$\langle (u-1)^i+2(u-1)^{i-2^{k-1}}h(u)\rangle$ $(2^{k-1}+1\le i\le 2^k-1,\ h_0\ne 0,1)$	$\langle 2(u-1)^{2^k-i},(u-1)^{2^{k-1}}+2(1+h(u))\rangle$
12	$\langle (u-1)^i+2(u-1)^th(u)\rangle$ $(2^{k-1}-i+t\ne 0, i\le 2^{k-1},\ h(u)\ne 0)$	$\langle (u-1)^{2^k-i}+2(u-1)^{2^{k-1}-i}$ $(1+(u-1)^{2^{k-1}-i+t}h(u))\rangle$
13	$\langle (u-1)^i+2(u-1)^th(u)\rangle$ $(2^{k-1}-i+t\ne 0,$ $2^{k-1}<i<2^{k-1}+t,\ h(u)\ne 0)$	$\langle 2(u-1)^{2^k-i},(u-1)^{2^{k-1}}$ $+2(1+(u-1)^{2^{k-1}-i+t}h(u))\rangle$
14	$\langle (u-1)^i+2(u-1)^th(u)\rangle$ $(2^{k-1}-i+t\ne 0, 2^{k-1}+t<i,$ $t>0\ h(u)\ne 0)$	$\langle 2(u-1)^{2^k-i},(u-1)^{i-t}$ $+2(h(u)+(u-1)^{i-t-2^{k-1}})\rangle$
15	$\langle (u-1)^i+2h(u)\rangle$ $(2^{k-1}<i,\ h(u)\ne 0)$	$\langle (u-1)^i+2(h(u)+(u-1)^{i-2^{k-1}})\rangle$
16	$\langle 2,(u-1)^i\rangle$ $(1\le i\le 2^k-1)$	$\langle 2(u-1)^{2^k-i}\rangle$

Case	C	$A(C)$
17	$\langle 2(u-1)^l, (u-1)^{2^{k-1}}+2\rangle$ $(1\le l\le 2^{k-1}-1)$	$\langle (u-1)^{2^k-l}\rangle$
18	$\langle 2(u-1)^l, (u-1)^{2^{k-1}}+2(1+(u-1)^\tau\tilde{h}(u))\rangle$ $(1\le l\le 2^{k-1}-1, 1\le\ l-1)$	$\langle (u-1)^{2^k-l}+2(u-1)^{2^{k-1}-l+\tau}\tilde{h}(u)\rangle$
19	$\langle 2(u-1)^l, (u-1)^{2^{k-1}}+2h(u)\rangle$ $(1\le l\le 2^{k-1}-1, h_0\neq\ 0,1)$	$\langle (u-1)^{2^k-l}+2(u-1)^{2^{k-1}-l}+(1+h(u))\rangle$
20	$\langle 2(u-1)^l, (u-1)^i+2h(u)\rangle$ $(2^{k-1}+1\le i\le 2^k-1, h(u)\neq 0$ $1\le l<2^k-i-1)$	$\langle (u-1)^{2^k-l}+2(u-1)^{2^k-l-i}(h(u)$ $+(u-1)^{i-2^{k-1}})\rangle$
21	$\langle 2(u-1)^l, (u-1)^i+2h(u)\rangle$ $(1\le i\le 2^{k-1}-1, h(u)\neq 0$ $1\le l<i-1)$	$\langle (u-1)^{2^k-l}+2(u-1)^{2^{k-1}-l}(1$ $+(u-1)^{2^{k-1}-i}h(u))\rangle$
22	$\langle 2(u-1)^l, (u-1)^i\rangle$ $(1\le i\le 2^k-1,$ $i-2^{k-1}+1\le l\le \min\{i,2^{k-1}\}-1)$	$\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l}$ $+2(u-1)^{2^{k-1}-l})\rangle$
23	$\langle 2(u-1)^l, (u-1)^i\rangle$ $(2^{k-1}+1\le i\le 2^k-1\ ,$ $1\le l\le i-2^{k-1})$	$\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l}\rangle$
24	$\langle 2(u-1)^l, (u-1)^i+2(u-1)^{i-2^{k-1}}\rangle$ $(2^{k-1}+1\le i\le 2^k-1\ ,$ $i-2^{k-1}<l<i)$	$\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l}\rangle$
25	$\langle 2(u-1)^l,$ $(u-1)^i+2(u-1)^{i-2^{k-1}}(1+(u-1)^\tau\tilde{h}(u))\rangle$ $(2^{k-1}+1\le i\le 2^k-1\ ,$ $i-2^{k-1}<l<\min\{i,2^{k-1}+\tau\})$	$\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l}$ $+2(u-1)^{2^{k-1}-l+\tau}\tilde{h}(u)\rangle$
26	$\langle 2(u-1)^l, (u-1)^i$ $+2(u-1)^{i-2^{k-1}}h(u)\rangle$ $(2^{k-1}+1\le i\le 2^k-1\ ,$ $i-2^{k-1}<l<2^{k-1}, h_0\neq 0,1)$	$\langle 2(u-1)^{2^{k-i}}, (u-1)^{2^k-l}$ $+2(u-1)^{2^{k-1}-l}(1+h(u))\rangle$
27	$\langle 2(u-1)^l, (u-1)^i$ $+2(u-1)^t h(u)\rangle$ $(2^{k-1}+t\le i\le 2^{k-1}+l, h(u)\neq 0,$ $0<t<l<2^k-i+t)$	$\langle 2(u-1)^{2^{k-i}}, (u-1)^{2^k-l}$ $+2(u-1)^{2^{k-1}-l}(1+h(u))\rangle$
28	$\langle 2(u-1)^l, (u-1)^i$ $+2(u-1)^t h(u)\rangle$ $(2^{k-1}+l\le i, h(u)\neq 0,$ $0<t<l<2^k-i+t)$	$\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l}$ $+2(u-1)^{2^k-l-i+t}h(u)\rangle$
29	$\langle 2(u-1)^l, (u-1)^i$ $+2(u-1)^t h(u)\rangle$ $(1\le i\le 2^{k-1}+t-1, h(u)\neq 0,$ $0<t<l<\min\{\ 2^{k-1}, i, 2^k-i+t\})$	$\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l}$ $+2(u-1)^{2^{k-1}-l}(1+(u-1)^{2^{k-1}-i+t})h(u)\rangle$

Proof. For each C, Let D denote the corresponding ideal in the right-most column.

A simple verification shows that $D \subseteq A(C)$ and that $|D| = (4^m)^{2^k}/|C|$. An argument similar to one for Lemma 5.2 in reference [12] proves that $\overline{A(C)} \subseteq C^{\perp}$

$$\Rightarrow (4^m)^{2^k}/|C| = |D| \leq |A(C)| = |\overline{A(C)}| \leq |C^{\perp}| = (4^m)^{2^k}/|C|.$$

Therefore, $D = A(C)$ and $\overline{A(C)} = C^{\perp}$. $\square$

Corollary 2.4.2. [*12*] *Let C be a cyclic code over Z_4 of length $2^k n$ and let $C = \bigoplus_{\alpha \in J} C_\alpha$. Then*

$$C^{\perp} = \bigoplus_{\alpha \in J} \overline{A(C_{\alpha'})},$$

where α' denote the representative in J of the coset containing $n - \alpha$, $\forall \alpha \in J$.

Therefore to understand self-dual codes, it is first necessary to identify the ideals $C \subseteq R_4(u, m)$ such that $C = \overline{A(C)}$.

Proposition 2.4.3. [*12*] *With notation as in Theorem 2.4.1, if $C = \overline{A(C)}$, then C must belong to one of the following types:*

- $\langle 2 \rangle$ *(case 3);*
- $\langle (u-1)^i + 2h(u) \rangle$, $(2^{k-1} < i,\ h(u) \neq 0)$ *(case 15);*
- $\langle 2(u-1)^{2^k - i}, (u-1)^i \rangle$ $, 3.2^{k-2} \leq i \leq 2^k - 1$ *(case 23);*
- $\langle 2(u-1)^{2^k-i}, (u-1)^i + 2(u-1)^t h(u) \rangle$, $2^{k-1} + t < i$, $h(u) \neq 0, 0 < t < 2^k - i$ *(case 27,28).*

Proof. First we eliminate the other cases. It is clear that C in cases 1 and 2 cannot satisfy $C = \overline{A(C)}$. For cases 4,6,7,9,11,13,14,16-21, C and $\overline{A(C)}$ are clearly of different types (e.g., in all cases except for case 7, one ideal is principal while the other is not). Some other cases are eliminated by showing an element is in C, if we assume $C = \overline{A(C)}$, while it really should not. This approach works for cases 5,8,10 and 12. We illustrate with case 8(one of the more involved among these cases). Note that Res(C)=Res($\overline{A(C)}$) implies that $i = 2^{k-1}$. Now write $h(u) = \sum h_j (u-1)^j$. So, Tor(C) $= \langle (u-1)^{2^{k-1}} \rangle$ in this case (cf. [12, Proposition 2.5]). The assumption $C = \overline{A(C)}$ implies that

$$C = \langle (u-1)^{2^{k-1}} + 2(1 + \sum h_j (u-1)^{j+\tau} \rangle$$

$$= \left\langle (u-1)^{2^{k-1}} + 2(u-1)^{\tau}\left(\sum h_j (u-1)^j u^{2^{k-1}-\tau-j}\right)\right\rangle,$$

which implies that

$$2\left(1+\sum h_j(u-1)^{j+\tau}\right) + 2(u-1)^{\tau}\left(\sum h_j(u-1)^j u^{2^{k-1}-\tau-j}\right) \in C.$$

This means that

$$\left(1+\sum h_j(u-1)^{j+\tau} + (u-1)^{\tau}\left(\sum h_j(u-1)^j u^{2^{k-1}-\tau-j}\right) \in \mathrm{Tor}(C) = \left\langle (u-1)^{2^{k-1}}\right\rangle,$$

which cannot be true since $\tau \geq 1$. Cases 5,10 and 12 can be eliminated in a similar fashion. The remaining cases to eliminate, i.e., cases 22,24, 25, 26 and 29, can proved by showing that the assumption $C = \overline{A(C)}$ leads to a contradiction to some of the conditions on i, l and t. E.g., consider Case 25. With $\tilde{h}(u) = \sum \tilde{h}_j(u-1)^j$, The assumption $C = \overline{A(C)}$ means that

$$\left\langle 2(u-1)^l, (u-1)^i + 2(u-1)^{i-2^{k-1}}(1+(u-1)^{\tau}\sum \tilde{h}_j(u-1)^j\right\rangle$$

$$= \left\langle 2(u-1)^{2^k-i}, (u-1)^{2^k-l} + 2(u-1)^{2^{k-1}-l+\tau}\left(\sum \tilde{h}_j(u-1)^j u^{2^{k-1}-\tau-j}\right)\right\rangle,$$

which implies that $i+l = 2^k$ and (hence)
$2(u-1)^{i-2^{k-1}}\left(1+(u-1)^{\tau}\sum \tilde{h}_j(u-1)^j\right) + 2(u-1)^{i-2^{k-1}+\tau}\left(\sum \tilde{h}_j(u-1)^j u^{2^{k-1}-\tau-j}\right) \in C,$
so
$(u-1)^{i-2^{k-1}}\left(1+(u-1)^{\tau}\sum \tilde{h}_j(u-1)^j\right) + (u-1)^{\tau}\left(\sum \tilde{h}_j(u-1)^j u^{2^{k-1}-\tau-j}\right) \in \mathrm{Tor(C)} = \left\langle (u-1)^l\right\rangle$. This means that $i - 2^{k-1} \geq l$, but this case assume that $i - 2^{k-1} < l$. Cases 22, 24. 26 and 29 may be dealt with in a similar way.

Consequently, only cases 3, 15, 23, 27 and 28 remain plausible for C. The additional constraint for case 23 in the statement of the proposition follows because $i + l = 2^k$ and $l \leq i - 2^{k-1}$. □

Corollary 2.4.4. [12] *For integer k such that $1 \leq k \leq 4$, the number of ideals $C \subseteq R_4(u,m)$ such that $C = \overline{A(C)}$ is : (i) 1 (where $k=1$)*
(ii) $2^m + 1$ (where $k = 2$;)
(iii) $2.(2^m)^2 + 2^m + 1$ (where $k = 3$); and

(iv) $(2^m)^4 + 2.(2^m)^3 + (2^m)^2 + 2$ *(where* $k = 4$*)*

For $\alpha \in J$*, recall that* N_α *denotes the number of ideals in* $R_4(u, m_\alpha)$*. Let* M_α *denote the number of ideals* C *in* $R_4(u, m_\alpha)$*, such that* $C = \overline{A(C)}$*.*

Let $\tilde{J}$ *denote the subset of* J *consisting of those* α *such that* $\alpha = \overline{\alpha}$ *where* $\overline{\alpha} \in J$ *is the representative of the cyclotomic coset containing* $n - \alpha$*. We also further partition* $J \setminus \tilde{J}$ *into two parts* K*,* K' *of equal size such that* $\alpha \in K$ *if and only if* $\overline{\alpha} \in K'$*.*

Proposition 2.4.5. [*12*] *The number of self-dual cyclic codes over* Z_4 *of length* $2^k n$ *is given by*

$$\prod_{\alpha \in K} N_\alpha \prod_{\alpha \in \tilde{J}} M_\alpha.$$

Corollary 2.4.6. [*12*] *If there exist* e *such that* $-1 \equiv 2^e \mod n$*, then there is only one cyclic self-dual code of length* $2n$*, where* n *is odd, namely* $2(Z_4)^{2n}$

Proof. If $N = 2n$, then as $N = 2^k n$, we have $k = 1$. We have that $Z_4[X]/\langle X^N - 1\rangle \cong \bigoplus_{\alpha \in J} R_4(u, m_\alpha)$. The condition that $-1 \equiv 2^e \mod n$, for some e implies that $\alpha = \alpha'$ for all $\alpha \in J$, i.e., $J = \tilde{J}$. Since $k = 1$, the only self-dual ideal in each $R_4(u, m)$ is $\langle 2\rangle$. Therefore there is only one cyclic self-dual code and it is $\bigoplus_{\alpha \in J} \langle 2\rangle = 2(Z_4)^{2n}$. $\square$

2.5 Examples

Example 2.5.1. *If* $N = 2$*, then* $n = 1$*,* $k = 1$*,* $J = \{0\}$*,* $m_0 = 1$*.*

There are $\prod_{\alpha \in J} 5 + 2^{m_\alpha} = 5 + 2^1 = 7$ *ideal of this case. We can list them by using Corollary 2.3.4, and Lemma 2.2.1 as:*

$\langle 0\rangle$, $\langle 1\rangle$,

$\langle 2(u-1)^i\rangle$, $0 \le i \le 2^k - 1 \Rightarrow 0 \le i \le 2^1 - 1 \Rightarrow 0 \le i \le 1$

$\Rightarrow \langle 2(u-1)^0\rangle, \langle 2(u-1)^1\rangle \Rightarrow \langle 2\rangle$, $\langle 2(u-1)\rangle$.

$\langle (u-1)^i + 2\sum_{j=0}^{i-1} s_j (u-1)^j\rangle$, $1 \le i \le 2^k - 1 \Rightarrow 1 \le i \le 1 \Rightarrow i = 1 \Rightarrow \langle (u-1)\rangle$.

$\langle 2(u-1)^l, (u-1)^i + 2\sum_{j=0}^{l-1} s_j (u-1)^j\rangle$, $l < i \Rightarrow \langle (u-1) + 2\rangle$, $\langle (u-1), 2\rangle$.

By Corollary 2.4.6, there is only one cyclic self-dual code of length 2, namely $\langle 2\rangle = 2(Z_4)^2$*.*

Example 2.5.2. *If* $N = 4$*, then* $n = 1$*,* $k = 2$*,* $J = \{0\}$*, and* $m_0 = 1$*. There are* $10.2^2 - 4.2^1 - 9 = 23$ *ideals for this case. There are* $2^m + 1 = 2^1 + 1 = 3$ *cyclic self-dual codes of this length. We list them:*
$\left\langle 2 \right\rangle$, $\left\langle (u-1)^3 + 2 \right\rangle$, $\left\langle 2(u-1), (u-1)^3 \right\rangle$.

Example 2.5.3. [12] *If* $N = 6$*, then* $n = 3$*,* $k = 1$*. The two cyclotomic coset* $\bmod 3$ *are* $c_0 = \{0\}$*,* $c_1 = \{1, 2\} \Rightarrow J = \{0, 1\}$*,* $m_0 = 1$*,* $m_1 = 2$
$\Rightarrow$ *There are* $\prod_{\alpha \in J} 5 + 2^{m_\alpha} = (5 + 2^1)(5 + 2^2) = (7)(9) = 63$ *ideals in this case. By Corollary 2.4.6 , there is only 1 cyclic self-dual code, namely* $\left\langle 2 \right\rangle \bigoplus \left\langle 2 \right\rangle = 2(Z_4)^6$.

Example 2.5.4. [12] *If* $N = 8$*, then* $n = 1$*,* $k = 3$*,* $J = \{0\}$*, and* $m_0 = 1$*. There are* $10(2^4) - 4(2^2) - 9 = 135$ *ideals in this case. There are* $2.(2^m)^2 + 2^m + 1 = 2(2^1)^2 + 2^1 + 1 = 11$ *cyclic self-dual codes of length 8. They are:*
$\left\langle 2 \right\rangle$, $\left\langle (u-1)^5 + 2 \right\rangle$, $\left\langle (u-1)^5 + 2(1 + (u-1)) \right\rangle$, $\left\langle (u-1)^5 + 2(1 + (u-1)^2) \right\rangle$, $\left\langle (u-1)^5 + 2(1 + (u-1) + (u-1)^2) \right\rangle$, $\left\langle (u-1)^6 + 2 \right\rangle$, $\left\langle (u-1)^6 + 2(1 + (u-1)) \right\rangle$, $\left\langle (u-1)^7 + 2 \right\rangle$, $\left\langle 2(u-1)^2, (u-1)^6 \right\rangle$, $\left\langle 2(u-1), (u-1)^7 \right\rangle$ *and* $\left\langle 2(u-1)^2, (u-1)^6 + 2(u-1) \right\rangle$.

Example 2.5.5. *If* $N = 10$*, then* $n = 5$*,* $k = 1$*,* $c_0 = \{0\}$*,* $c_1 = \{1, 2, 4, 3\} \bmod 5 \Rightarrow m_0 = 1$*,* $m_1 = 4$*,* $J = \{0, 1\}$*. There are* $\prod_{\alpha \in J}(5 + 2^{m_\alpha}) = (5 + 2^1)(5 + 2^4) = (7)(21) = 84$ *ideals in this case. There is only 1 cyclic self-dual code, namely* $\left\langle 2 \right\rangle \bigoplus \left\langle 2 \right\rangle = 2(Z_4)^{10}$.

Chapter 3

Negacyclic Codes of Even Length over Z_{2^a}

In this chapter, we determine the structure of negacyclic codes of even length over the ring Z_{2^a} and their dual codes. Furthermore we study self-dual negacyclic code of even length over Z_{2^a}. A necessary and sufficient condition for the existence of nontrivial self-dual negacyclic codes is given, and the number of the self-dual negacyclic codes for a given even lengh is determined.

3.1 A ring Construction

During this chapter, we will focus on dual and self-dual negacyclic codes over Z_{2^a} of length $N = 2^k n,$ where n is odd and $k,\ a \geq 1$ are positive integers.

Definition 3.1.1. [23] Negacyclic codes over Z_{2^a} of length $N = 2^k n,$ (n odd) are precisely ideals of the quotient ring $R_N = Z_{2^a}[x]/\langle x^N + 1 \rangle$.

Definition 3.1.2. [23] Define the Galois ring $GR(2^a, m) = Z_{2^a}[x]/\langle h_m(x) \rangle$ where $h_m(x)$ is a monic basis irreducible polynomial in $Z_{2^a}[x]$ of degree m. Note that if $a = 1$, then $GR(2^a, m) = GF(2^m)$ and if $m = 1$, then $GR(2^a, m) = Z_{2^a}$. The Galois ring $GR(2^a, m)$ is local ring with maximal ideal $\langle 2 \rangle$ and residue field $GF(2^m)$.

The polynomial $h_m(x)$ has a root ξ in $GR(2^a, m)$, which is also a primitive $(2^m - 1)$th root of unity.

Let $R = Z_{2^a}[u]/\langle u^{2^k} + 1\rangle$. There exists a natural Z_{2^a}-module isomorphism $\phi : R^n \rightarrow Z_{2^a}^N$, where $N = 2^k n, (n$ odd) defined by

$$\psi\big(a_{0,0} + a_{0,1}u + \ldots + a_{0,2^k-1}u^{2^k-1}, \ldots, a_{n-1,0} + a_{n-1,1}u + \ldots + a_{n-1,2^k-1}u^{2^k-1}\big)$$

$$= \big(a_{0,0}, a_{1,0}, \ldots, a_{n-1,0}, a_{0,1}, a_{1,1}, \ldots, a_{n-1,1}, \ldots, a_{0,2^k-1}, a_{1,2^k-1}, \ldots, a_{n-1,2^k-1}\big)$$

This gives that constacyclic shift by u in R^n corresponds to a negacyclic shift in $Z_{2^a}^N$. Thus we get the following theorem:

Theorem 3.1.1. [23] *Negacyclic codes over Z_{2^a} of length $N = 2^k n$ (n odd) correspond to u-constacyclic codes over $R = Z_{2^a}[u]/\langle u^{2^k} + 1\rangle$ of length n via the map ψ.*

Next we introduce the quotient ring $R_a(u, m) = GR(2^a, m)[u]/\langle u^{2^k} + 1\rangle$.

Lemma 3.1.2. [23] *For any positive integer b, there exist a polynomial $\alpha_b(u) \in Z[u]$ such that $(u-1)^{2^b} = u^{2^b} + 1 - 2\alpha_b(u)$, and $\alpha_b(u)$ is a unit in $R_a(u, m)$. In particular, $(u-1)^{2^k} = 2\alpha_k(u)$, where $\alpha_k(u)$ is a unit in $R_a(u, m)$.*

Proof. We prove by induction on b. For $b = 1$, $(u-1)^2 = u^2 + 1 - 2u$, $\alpha_b(u) = u$ and hence $\alpha_b(u) = u$ is a unit in $R_a(u, m)$. Assume $b > 1$ and the conclusion is true for all positive integers less than b. Then

$$\begin{aligned}
(u-1)^{2^b} &= \big[(u-1)^{2^{b-1}}\big]^2 \\
&= \big[u^{2^{(b-1)}} + 1 - 2\alpha_{b-1}(u)\big]^2 \\
&= u^{2^b} + 1 + 4\alpha_{b-1}^2(u) + 2u^{2^{(b-1)}} - 4\alpha_{b-1}(u) - 4(u)^{2^{(b-1)}}\alpha_{b-1}(u) \\
&= u^{2^b} + 1 - 2\alpha_b(u)
\end{aligned}$$

where $\alpha_b(x) = -2\alpha_{b-1}^2(u) - u^{2^{(b-1)}} + 2\alpha_{b-1}(u) + 2u^{2^{(b-1)}}\alpha_{b-1}(u)$.

To show $\alpha_b(u)$ is a unit in $R_a(u, m)$, we note that u is invertible, and so $u^{2^{(b-1)}}$ is also invertible in $R_a(u, m)$. As 2 is nilpotent in $R_a(u, m)$, it follows that $\alpha_b(u)$ has the form

$\alpha_b(u) = u^{2^{(b-1)}}(1+y),$ where y is nilpotent in $R_a(u,m)$. Choose r to be an odd integer such that $y^r = 0,$ we have $1 = 1+y^r = (1+y)(1-y+y^2-\ldots+y^{r-1})$ which means $1+y$ is invertible in $R_a(u,m)$, and therefore $\alpha_b(u) = u^{2^{(b-1)}}(1+y)$ is a unit in $R_a(u,m)$.

It remains to show that $(u-1)^{2^k} = 2\alpha_k(u)$. To see this, note that $(u-1)^{2^k} = u^{2^k}+1-2\alpha_k(u)$

$= 2\alpha_k(u)$ (since $u^{2^k}+1$ is the zero element in $R_a(u,m)$). $\square$

Lemma 3.1.3. [23] *The ring $R_a(u,m)$ is a chain ring with maximal ideal $\langle u-1\rangle$ and residue field $GF(2^m)$. The ideals of $R_a(u,m)$ are $\langle (u-1)^i\rangle,\ 0 \le i \le 2^k a$.*

Proof. Let I be the ideal of $R_a(u,m)$. The set β consisting of elements of I reduced modulo 2 is an ideal of $R_a(1,m)$. Since $R_a(1,m)$ is a chain ring with the maximal ideal $\langle u-1\rangle$, then $\beta = \langle (u-1)^i\rangle$ in $R_a(1,m)$, for some $i \in \{0,1,\ldots,2^k\}$. Hence, for each element $r(u) \in I$, there exist $\kappa(u),\ \gamma(u) \in R_a(u,m)$ such that $r(u) = (u-1)^i\kappa(u) + 2\gamma(u)$. By Lemma 3.1.2, $2\gamma(u) \in \langle (u-1)^{2^s}\rangle,$ whenece I is contained in some ideal $\langle (u-1)^j\rangle$ of $R_a(u,m)$, where $0 \le j \le 2^k a$. Choose s to be the largest among those $j \in \{0,1,\ldots,2^k a\}$ such that $I \subseteq \langle (u-1)^j\rangle$ of $R_a(u,m)$. Then $I = \langle (u-1)^s\rangle$. As I was chosen arbitrary among ideals of $R_a(u,m)$. It follows that the ideals of $R_a(u,m)$ are $\langle (u-1)^i\rangle,\ 0 \le i \le 2^k a$. Consequently, $R_a(u,m)$ is a chain ring with maximal ideal $\langle u-1\rangle$ and residue field $GF(2^m)$. $\square$

Remark 3.1.1. [23] (1) In $R_a(u,m)$, Lemma 3.1.2 implies $\langle (u-1)^{2^k}\rangle = \langle 2\rangle$. Thus, the ideals of $R_a(u,m)$ can be written as $\langle 2^j(u-1)^b\rangle,\ 0 \le j \le a-1,\ 0 \le b \le 2^k-1$.

(2) Since negacyclic codes of length 2^k over $GR(2^a,m)$ are the ideals of $R_a(u,m)$, then by Lemma 3.1.3, we have that negacyclic codes of length 2^k over $GR(2^a,m)$ are precisely $\langle (u-1)^i\rangle,\ 0 \le i \le 2^k a$.

Theorem 3.1.4. [23] *Let C be an ideal of $R_a(u,m)$, then we have the following:*

(i) $C = \langle (u-1)^i\rangle$ for some $i \in \{0,1,\ldots,2^k a\}$ and the number of codewords in C is $|C| = 2^{m(2^k a-i)}$.

(ii) The dual code of C is $C^\perp = \langle (u-1)^{2^k a-i}\rangle$ and the number of codewords in $C^\perp$ is $|C^\perp| = 2^{mi}$.

Proof. (i) Follows directly from Lemma 3.1.3.

(ii) Since $|C||C^{\perp}| = \left|R_a(u,m)\right| = 2^{2^k am}$, we have $|C^{\perp}| = \frac{2^{2^k am}}{2^{m(2^k a-i)}} = 2^{mi}$.

Because $C^{\perp}$ is also a negacyclic code, then there exists $j \in \{0, 1, \ldots, 2^k a\}$ such that $C^{\perp} = \left\langle (u-1)^j \right\rangle$ and $|C^{\perp}| = 2^{m(2^k a - j)}$. It follows that $i = 2^k a - j$, and hence $C^{\perp} = \left\langle (u-1)^{2^k a - i} \right\rangle$ □

3.2 The Ideals Construction

Let m be the order of 2 modulo n, and let I be a complete set of 2-cyclotomic coset representatives modulo n. Let m_i be the size of the 2-cyclotomic coset modulo n containing i, and let ξ be a primitive nth root of unity in $GR(2^a, m)$.

Definition 3.2.1. [23]

Let $c = \left(c_{0,0}, c_{1,0}, \ldots, c_{n-1,0}, c_{0,1}, c_{1,1}, \ldots, c_{n-1,1}, \ldots, c_{0,2^k-1}, \ldots, c_{n-1,2^k-1}\right) \in Z_{2^a}^N$, with $c(x) = \sum_{i=1}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} x^{i+jn} \in Z_{2^a}[x]$ the corresponding polynomial. The Discrete Fourier Transform of $c(x)$ is the vector $(\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{n-1}) \in R_a(u,m)^n$ with

$$\hat{c_h} = c(u^{n'}\xi^h) = \sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j} \xi^{hi}, \text{ for } 0 \le h \le n-1, \text{ where } nn' \equiv 1(\mod 2^{k+1}).$$

Lemma 3.2.1. [*23*](Inversion Formula) *Let $c \in Z_{2^a}^N$ with $\hat{c}(z)$ its Mattson-Solomn polynomial as defined in chapter 2, (see Defn 2.3.1). Then*

$$c = \phi\left[\left(1, u^{-n'}, u^{-2n'}, \ldots, u^{-(n-1)n'}\right) * \frac{1}{n}\left(\hat{c}(1), \hat{c}(\xi), \ldots, \hat{c}(\xi^{n-1})\right)\right]$$

where $*$ denotes componentwise multiplication.

Proof. Let $0 \le t \le n-1$, Then

$$\begin{aligned}
\hat{c}(\xi^t) \;= \sum_{h=0}^{n-1} \hat{c}_h \xi^{-ht} &= \sum_{h=0}^{n-1} \left(\sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j} \xi^{hi} \right) \xi^{-ht} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{2^k-1} c_{i,j} u^{n'i+j} \sum_{n=0}^{n-1} \xi^{h(i-t)} \\
&= (nu^{n't}) \sum_{j=0}^{2^k-1} c_{t,j} u^j.
\end{aligned}$$

Hence, $u^{-n't}(\frac{1}{n})\hat{c}_h(\xi^t) = \sum_{j=0}^{2^k-1} c_{t,j}u^j$. Noting that $u^{-i} = u^{2^{k+1}-i} \in R_a(u,m)$, we get the result. $\square$

Theorem 3.2.2. [23] *Let $N = 2^k n$, where n is odd. Then*

$$\gamma : R_N = Z_{2^a}[x]/\langle x^N + 1\rangle \longmapsto \bigoplus_{i\in I} R_a(u,m_i)$$

defined by $\gamma(c) = (\hat{c}_i)_{i\in I}$ is a ring isomorphisim.
In particular, if C is a negacyclic code of length N over Z_{2^a}, then C is isomorphic to $\oplus_{i\in I}C_i$ where C_i is the ideal $\{c(u^{n'}\xi^i) : c(x) \in C\} \subseteq R_a(u,m_i)$ and I is a complete set of 2-cyclotomic coset representatives modulo n.

Combining Lemma 3.1.3, Theorem 3.1.4, and Lemma 3.2.2, we immediately get the following enumeration result.

Corollary 3.2.3. [23]
The number of distinct negacyclic codes over Z_{2^a} of length $N = 2^k n$ (n odd) is $(2^k a+1)^{|I|}$, where I is a complete set of 2-cyclotomic coset representatives modulo n, and $|I|$ denotes its cardinality.

Example 3.2.1. *Consider the cyclic codes of length 28 over Z_4*
$\Rightarrow 28 = 2^2(7) \Rightarrow k = 2, n = 7$ *and* $Z_4 = Z_{2^2}$
$\Rightarrow a = 2 \Rightarrow c_0 = \{0\},\ c_1 = \{1,2,4\},\ c_6 = \{6,5,3\}$
$\Rightarrow\ I = \{0,1,6\} \Rightarrow$*the number of distinct negacyclic codes over Z_4 of length 28 is* $(2^2(2)+1)^3 = 729$.

Lemma 3.2.4. [23] *Let $f_s(x)$ be the minimal polynomial of ξ^s in Z_{2^a}, and let n' be a positive integer such that $nn' \equiv 1(\mod 2^{k+1})$ Then*
(i) $f_s(u^{n'}\xi^s)$ not equivalent to 0 mod 2;
(ii) $f_s(u^{n'}\xi^s) \in \langle u-1\rangle$ but $f_s(u^{n'}\xi^s)$ not in $\langle (u-1)^2\rangle$.

Now we describe a negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd) in term of its generator polynomials.

Theorem 3.2.5. *[23]*

Let C be a negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd), then $C = \langle g(x) \rangle$, where $g(x) = \prod_{j=0}^{2^k a} [g_j(x)]^j$, and $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $Z_{2^a}[x]$.

Proof. By Theorem 3.2.2, C is isomorphic to a direct sum $\bigoplus_{i \in I} C_i$, where C_i is the ideal $\{c(u^{n'}\xi^i) : c(x) \in C\} \in R_a(u, m_i)$, where n' be a positive integer such that $nn' \equiv 1($ mod $2^{k+1})$. For each j, we define $g_j(x)$ to be the product of all minimal polynomials of ξ^i such that $C_i = \langle (u-1)^j \rangle$. If $a(x) = r(x)[g_j(x)]^b$, where $r(x)$ is relatively prime to $g_j(x)$ and $0 \leq b \leq 2^k a$, then by Lemma 3.2.4, $a(u^{n'}\xi^i) = r(u^{n'}\xi^i)\left[g_j(u^{n'}\xi^i)\right]^b \in \langle (u-1)^b \rangle$, but not in $\langle (u-1)^{b+1} \rangle$. Hence if $c(x) = g(x)h(x) \in C$ for some polynomial $h(x) \in R_N$, then $c(u^{n'}\xi^i) = g(u^{n'}\xi^i)h(u^{n'}\xi^i) \in \langle (u-1)^j \rangle$, but not in $\langle (u-1)^{j-1} \rangle$. Thus, we can take $g(x) = \prod_{j=0}^{2^k a} [g_j(x)]^j$ as the generator polynomial of C. $\square$

Corollary 3.2.6. *[23] If C is a negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd), and $C = \left\langle \prod_{j=0}^{2^k a} [g_j(x)]^j \right\rangle$, where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $Z_{2^a}[x]$, then*

$$|C| = 2^q, \text{ where } q = \sum_{j=0}^{2^k a - 1} (2^k a - j) \deg(g_j(x))$$

Proof. By Theorem 3.2.2, the size of C is $\prod_{i \in I} |C_i|$, where C_i is the ideal of $R_a(u, m_i)$. Note that if $C_i = \langle (u-1)^j \rangle$, then $g_j(\xi^i) = 0$ and $|C_i| = 2^{m_i(2^k a - j)}$. Calculating the product, we obtain the result. $\square$

3.3 Dual and Self-dual

Definition 3.3.1. [23] Let $R = Z_{2^a}[u]/\langle u^{2^k} + 1 \rangle$, and let $- : R \longrightarrow R$ denote the conjugate map defined by $\overline{\sum_{i=0}^{2^k-1} a_i u^i} = \sum_{i=0}^{2^k-1} a_i u^{-i}$, where $u^{-i} = u^{2^{k+1}-i}$ in R. This map is also extended to $R_a(u, m)$ in the obvious way. We define the Hermitian inner product as fellows:

For $c' = (c_0, c_1, \ldots, c_{n-1}) \in R^n$ and $d' = (d_0, d_1, \ldots, d_{n-1}) \in R^n$, $\langle c', d' \rangle = \sum_{j=0}^{n-1} c_j \overline{d_j}$.

Again recall that ϕ is a map from R^n to $Z_{2^a}^N$ defined as before. Suppose that $0 \leq\ t \leq\ n-1$, $c_t = \sum_{j=0}^{2^k-1} c_{t,j}u^j$ and $d_t = \sum_{j=0}^{2^k-1} d_{t,j}u^j$, then $\phi(c') = c,\ \phi(d') = d$, where

$$c = \left(c_{0,0}, c_{1,0}, \ldots, c_{n-1,0}, c_{0,1}, c_{1,1}, \ldots, c_{n-1,1}, \ldots, c_{0,2^k-1}, c_{1,2^k-1}, \ldots, c_{n-1,2^k-1}\right) \in\ Z_{2^a}^N$$

and

$$d = \left(d_{0,0}, d_{1,0}, \ldots, d_{n-1,0}, d_{0,1}, d_{1,1}, \ldots, d_{n-1,1}, \ldots, d_{0,2^k-1}, d_{1,2^k-1}, \ldots, d_{n-1,2^k-1}\right) \in\ Z_{2^a}^N$$

Lemma 3.3.1. [23] *Let the notation as above. Let ρ denote the negacyclic shift in $Z_{2^a}^N$ and let . denote the Euclidean inner product in $Z_{p^a}^N$. Then $\langle c', d' \rangle = 0$ if and only if $\rho^{nj}\big(\phi(c')\big).\phi(d') = 0$ for all $0 \leq\ j \leq\ 2^k - 1$.*

Let φ denote the inverse map of ϕ. Then applying lemma 3.3.1, we obtain the following Theorem:

Theorem 3.3.2. [23] *Let C be a negacyclic code over Z_{2^a} of length $2^k n$ (n odd), and let $\varphi(C)$ be its image in R^n under φ. Then $\varphi(C)^\perp = \varphi(C^\perp)$, where the dual in $Z_{2^a}^N$ is taken with respect to the Euclidean inner product, while the dual in R^n is taken with respect to the Hermitian inner product.*

Lemma 3.3.3. [23] *Let $C = \langle 2^j(u-1)^b \rangle$ be an ideal of $R_a(u,m)$, for some integers $0 \leq j \leq a-1,\ 0 \leq b \leq 2^k - 1$. Then $\overline{C} = C$.*

Proof. Let $a(u) \in\ C$, then $a(u) = 2^j(u-1)^b g(u)$, for some polynomial $g(u) \in\ R_a(u,m)$.
Since $\overline{2^j(u-1)^b} = (-u)^{-b}2^j(u-1)^b$, then $\overline{a(u)} = (-u)^{-b}\overline{g(u)}2^j(u-1)^b$.
Hence, $\overline{C} \subseteq\ C$. Since the conjugation map is a bijection map, then $\overline{C} =\ C$. □

Theorem 3.3.4. [23] *Let C be a negacyclic code over Z_{2^a} of length $2^k n$ (n odd) such that $C = \bigoplus_{i\in\ I} C_i$ and $D_{i'} = C_i^\perp$, where i' is the representative of the cyclotomic coset containing $n-i$ for each $i \in\ I$, I is a complete set of $2-$cyclotomic coset mod n. Then $C^\perp = \bigoplus_{i\in\ I} D_i$.*

Proof. Let $D = \bigoplus_{i\in\ I} D_i$, and let $c \in\ C,\ d \in\ D$. Since $C_i C_i^{\perp} = 0$ for all $i \in\ I$, it follows from lemma 3.3.3 that $C_i\overline{D_{i'}} = 0$ for all i. Let $\hat{c}(z) = \sum_{h=0}^{n-1} \hat{c}_{n-h} z^h$ and $\hat{d}(z) = \sum_{h=0}^{n-1} \hat{d}_{n-h} z^h$ be the Mattson-Solomon polynomials of c and d respectively, then $\hat{c}_i\overline{\hat{d}_{n-i}} = 0$. Thus, by lemma 3.3.1 we get $D \subseteq\ C^{\perp}$. Also, $|C_i||D_{i'}| = 2^{2^k a m_i}$ for all $i \in\ I$, so that $|C||D| = 2^{2^k m}$. Hence, $D = C^{\perp}$. □

Theorem 3.3.5. [23] *If C is a negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd), and $C = \left\langle \prod_{j=0}^{2^k a} [g_j(x)]^j \right\rangle$, where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $Z_{2^a}[x]$, then $C^{\perp} = \left\langle \prod_{j=0}^{2^k a} [g_j^*(x)]^{2^k a - j} \right\rangle$ and $|C^{\perp}| = 2^t$, where $t = \sum_{j=1}^{2^k a} j \deg(g_j(x))$.*

Proof. Define $g_j(x)$ as in the proof of Theorem 3.2.5. Let a_j denote the constants of $g_j(x),\ 0 \le j \le 2^k a$. Since $g_0(x)g_1(x)\dots g_{2^k a}(x) = x^n - 1,\ a_0 a_1 \dots a_{2^k a} = -1$. Therefore, a_j's are invertible elements of Z_{2^a} and a_j's are leading coefficients of $g_j^*(x)'$s. Define $h_j(x) = u_j g_j^*(x)$, where u_j's are suitable invertible elements in Z_{2^a} such that $h_j(x)'$s are monic polynomials. Note that $u_j = a_j^{-1}$ and $u_0 u_1 \dots u_{2^k a} = a_0^{-1} a_1^{-1} \dots a_{2^k a}^{-1} = -1$. So

$$\begin{aligned} h_0(x)h_1(x)\dots h_{2^k a}(x) &= (u_0 u_1 \dots u_{2^k a}) g_0^*(x) g_1^*(x) \dots g_{2^k a}^*(x) \\ &= -x^{\sum_{j=1}^{(2^k a)} \deg(g_j(x))} g_0(x^{-1}) g_1(x^{-1}) \dots g_{2^k a}(x^{-1}) \\ &= -x^n(x^{-n} - 1) \\ &= \quad x^n - 1. \end{aligned}$$

Therefore, $h_j(x)'$s are monic coprime divisors of $x^n - 1$ in $Z_{2^a}[x]$.

Let $C = \bigoplus_{i\in I} C_i$, where C_i is an ideal of $R_a(u, m_i)$, then by Theorem 3.3.4 $C^{\perp} = \bigoplus_{i\in l} D_i'$, where, $D_i = C_i^{\perp}$. Since $C_i = \langle (u-1)^j \rangle$, we have $g_j(\xi^i) = 0$, which implies $g_j^*(\xi^{-i}) = 0$. It follows that $h_j(\xi^{-i}) = 0$. Therefore, $h_j(x)$ is the product of all minimal polynomials of $\xi^{i'}$ such that $D_i = \langle (u-1)^{2^k a - j} \rangle$. According to the proof of Theorem 3.2.5, we can get that $C^{\perp} = \left\langle \prod_{j=0}^{2^k a} [h_j(x)]^{2^k a - j} \right\rangle = \left\langle \prod_{j=0}^{2^k a} [g_j^*(x)]^{2^k a - j} \right\rangle$.

The second result follows from Corollary 3.2.5 and the fact that

$|C||C^{\perp}| = 2^{2^k an\cdot}(cf.[18, Theorem 3.10(iii)])$ □

We now determine self-dual negacyclic codes over Z_{2^a} of length $N = 2^k n$ (n odd). The following lemma is clear.

Lemma 3.3.6. [23] *If C is a negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd), and $C = \bigoplus_{i \in I} C_i$, then C is a self-dual negacyclic code if and only if $C_{i'} = C_i^{\perp}$, where i' is the representative of cyclotomic coset containing $n - i$ for each $i \in I$.*

Theorem 3.3.7. [23] *If C is a negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd) with $C = \langle \prod_{j=0}^{2^k a} [g_j(x)]^j \rangle$, where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $Z_{2^a}[x]$, then C is self-dual if and only if $g_j^*(x)$ is an associate of $g_{2^k a - j}(x)$.*

Proof. Let $C = \bigoplus_{i \in I} C_i$, where C_i is an ideal of $R_a(u, m_i)$. By Lemma 3.3.6, If C is self-dual, then $C_{i'} = C_i^{\perp}$ for each $i \in I$. Let $C_i = \langle (u-1)^j \rangle, 0 \leq j \leq 2^k a$, then $C_{i'} = \langle (u-1)^{2^k a - j} \rangle$. Define $h_j(x)$ as in Theorem 3.3.5. Since $g_j(x) = 0$, which implies that $g_j^*(\xi^{-i}) = 0$, we have $h_j(x) = u_j g_j^*(x) = g_{2^k a - j}(x)$. Hence, g_j* is an associate of $g_{2^k a - j}(x)$.
On the other hand, by Theorem 3.3.5, $C^{\perp} = \langle \prod_{j=0}^{2^k a} [g_j^*(x)]^{2^k a - j} \rangle$, hence, if $g_j^*(x)$ is an associate of $g_{2^k a - j}(x)$, then

$$C^{\perp} = \langle \prod_{j=0}^{2^k a} [g_j^*(x)]^{2^k a - j} \rangle = \langle \prod_{j=0}^{2^k a} [g_{2^k a - j}(x)]^{2^k a - j} \rangle = C,$$

i.e, C is self-dual. □

Corollary 3.3.8. [23] *If C is a self-dual negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd), and $C = \langle g(x) \rangle$, then $(x-1)^{2^{k-1} a}$ divides $g(x)$.*

Proof. Observing that $\langle (u-1)^{2^{k-1} a} \rangle$ is the unique ideal of $R_a(u, m)$ such that $C_0 = C_0^{\perp}$, we have the result. □

Corollary 3.3.9. [23] *If there exist b such that $2^b \equiv -1(\mod n)$, then the only self-dual negacyclic code over Z_{2^a} of length $N = 2^k n$ (n odd) is $\langle (x^n - 1)^{2^{k-1} a} \rangle$.*

Proof. Let $C = \bigoplus_{i \in I} C_i$, where C_i is an ideal of $R_a(u, m_i)$ and I is a complete set of $2-$cyclotomic coset representative modulo n. Since there exists b such that $2^b \equiv -1($

mod n), i and $n-i$ are contained in the same cyclotomic coset for all $i \in I$. Hence, $C_{i'} = C_i$. If C is self-dual, then $C_{i'} = C_i^{\perp}$ by Lemma 3.3.6. It follows that $C_i = C_i^{\perp}$. Therefor $C_i = \left\langle (u-1)^{2^{k-1}a} \right\rangle$ for all i. Note that the product of all minimal polynomials of ξ^i is equal to $x^n - 1$. Thus, $C = \left\langle (x^n-1)^{2^{k-1}a} \right\rangle$. □

Lemma 3.3.10. [23] *If a is even, then $\left\langle (x^n-1)^{2^{k-1}a} \right\rangle = \left\langle 2^{\frac{a}{2}} \right\rangle$ in R_N.*

Proof. Similarly to the result in Lemma 3.1.2, it follows easily that $(x^n-1)^{2^k} = x^{2^k n} + 1 + 2\alpha_k(x^n)$ in $R_N,$ where $\alpha_k(x^n)$ is an invertible element in R_N. Therefore, computing in $R_N,$ $(x^n-1)^{2^k} = 2\alpha_k(x^n)$. It follows that if a is even, then $\left\langle (x^n-1)^{2^{k-1}a} \right\rangle = \left\langle 2^{\frac{a}{2}} \right\rangle$. □

Now we consider the enumeration of self-dual negacyclic codes over Z_{2^a} of length $N = 2^k n$ (n odd).

Let i be an integer such that $0 \leq i < n,$ and let b be the the smallest positive integer such that $i.2^b \equiv i(\mod n),$ then $C_i^{(n)} = \{i, 2i, \ldots, 2^{b-1}i\}$ is the 2-cyclotomic coset modulo n containing i.

Definition 3.3.2. [23] A cyclotomic coset is called symmetric if $n-i \in C_i^{(n)}$ and asymmetric otherwise. The asymmetric cosets come in pairs $C_i^{(n)}, C_{n-i}^{(n)},$ and let $\delta(n)$ denote the number of such pairs.

Theorem 3.3.11. [23] *The number of distinct self-dual negacyclic codes over Z_{2^a} of length $N = 2^k n$ (n odd) is $(2^k a + 1)^{\delta(n)},$ where $\delta(n)$ is the number of pairs of a symmetric 2-cyclotomic cosets modulo n.*

3.4 Examples

Example 3.4.1. [23] *Consider self-dual negacyclic codes of length 28 over Z_4.*

$\Rightarrow\ 28 = 2^2(7) \Rightarrow k = 2, n = 7$

$Z_4 = Z_{2^2} \Rightarrow a = 2$. *Let* $i = 2 \Rightarrow 0 \leq 2 < 7 \iff 0 \leq i < 7$.

Since $C_i^{(n)} = \{i, 2i, 2^2 i, \ldots, 2^{b-1}i\}$ *where* b *as above, then* $22^b \equiv 2(\mod 7) \Rightarrow b = 3 \Rightarrow$ $C_2^{(7)} = \{2, 2(2), 2^{3-1}(2)\} = \{2, 4, 8\} \Rightarrow n - i = 7 - 2 = 5$ not in $C_2^{(7)}$.

$\Rightarrow$ *The 2-cyclotomic coset* $(\mod 7)$ *containing* $i = 2$ *is asymmetric coset* $\Rightarrow$ *The pairs* $C_2^{(7)},\ C_5^{(7)}$ *is asymmetric.*

For $i = 0, 1, 3, 4, 5, 6,$ *we compute* $C_i^{(n)}$ *as above to get symmetric cosets for these* $i's$*. Hence there is only one pair asymmetric coset* $\Rightarrow$ $\delta(n) = 1 \Rightarrow$ *There are* $(2^k a + 1)^{\delta(n)} = (2^2(2)+1) = 9$ *self-dual negacyclic codes of length 28 over* Z_4*, all of which have order* 2^{28}.

$x^7 - 1 = (x-1)(x^3+2x^2+x-1)(x^3-x^2+2x-1)$ *in* $Z_4[x]$*. Using Theorem 3.2.5, Corollary 3.2.6, and Corollary 3.3.8, we have the following self-dual negacyclic codes of length 28 over* Z_4*, where* $2^k a = 2^2(2) = 8$.

(1) $\langle (u-1)^{2^{k-1}a} \rangle = \langle (u-1)^4 \rangle = \langle 2^{\frac{a}{2}} \rangle = \langle 2^1 \rangle = \langle 2 \rangle,$

(2) $\langle (x-1)^4(x^3-x^2+2x-1)^8 \rangle \Rightarrow$ *the order equal* $2^{4+3(8)} = 2^{28}$ *and* $(x-1)^4 \big| (x-1)^4(x^3-x^2+2x-1)^8$.

(3) $\langle (x-1)^4(x^3+2x^2+x-1)^8 \rangle \Rightarrow$ *the order equal* $2^{4+3(8)} = 2^{28}$ *and* $(x-1)^4 \big| (x-1)^4(x^3+2x^2+x-1)^8$.

(4) $\langle (x^3+2x^2+x-1)(x-1)^4(x^3-x^2+2x-1)^7 \rangle \Rightarrow$ *the order equal* $2^{3+4+3(7)} = 2^{28}$ *and* $(x-1)^4 \big| (x^3+2x^2+x-1)(x-1)^4(x^3-x^2+2x-1)^7$.

(5) $\langle (x^3+2x^2+x-1)^7(x-1)^4(x^3-x^2+2x-1) \rangle$

(6) $\langle (x^3+2x^2+x-1)^2(x-1)^4(x^3-x^2+2x-1)^6 \rangle$

(7) $\langle (x^3+2x^2+x-1)^6(x-1)^4(x^3-x^2+2x-1)^2 \rangle$

(8) $\langle (x^3+2x^2+x-1)^3(x-1)^4(x^3-x^2+2x-1)^5 \rangle$

(9) $\langle (x^3+2x^2+x-1)^5(x-1)^4(x^3-x^2+2x-1)^3 \rangle$

Example 3.4.2. [23] *Consider self-dual negacyclic codes of length 14 over* Z_8.

$14 = 2^1(7) \Rightarrow k = 1, n = 7.$

$Z_8 = Z_{2^3} \Rightarrow a = 3.$ *Now there is only one pair asymmetric coset* $\Rightarrow \delta(n) = 1 \Rightarrow$ *There are* $(2^k a + 1) = [2^1(3) + 1] = 7$ *self-dual negacyclic codes of length 14 over* Z_8*, all of which have order* 2^{21}.

$2^{k-1}.a = 3 \Rightarrow (x-1)^{2^{k-1}.a} = (x-1)^3.$

$x^7 - 1 = (x-1)(x^3+3x^2+2x-1)(x^3+6x^2+5x-1)$ *in* $Z_8[x]$.

We list all such self-dual negacyclic codes as follows:

(1) $\langle (x^7-1)^3\rangle \Rightarrow$ *the order equal* $2^{7(3)} = 2^{21}$.

(2) $\langle (x-1)^3(x^3+3x^2+2x-1)^6\rangle$ *the order equal* $2^{3+3(6)} = 2^{21}$, *and* $(x-1)^3 \big| (x-1)^3(x^3+3x^2+2x-1)^6$.

(3) $\langle (x-1)^3(x^3+6x^2+5x-1)^6\rangle$ *the order equal* $2^{3+3(6)} = 2^{21}$, *and* $(x-1)^3 \big| (x-1)^3(x^3+6x^2+5x-1)^6$.

(4) $\langle (x^3+6x^2+5x-1)(x-1)^3(x^3+3x^2+2x-1)^5\rangle$

(5) $\langle (x^3+3x^2+2x-1)(x-1)^3(x^3+6x^2+5x-1)^5\rangle$

(6) $\langle (x^3+6x^2+5x-1)^2(x-1)^3(x^3+3x^2+2x-1)^4\rangle$

(7) $\langle (x^3+3x^2+2x-1)^2(x-1)^3(x^3+6x^2+5x-1)^6\rangle$

Example 3.4.3. *Consider self-dual negacyclic codes of length 12 over* $Z_{16} \Rightarrow 12 = 2^2(3) \Rightarrow k = 2,\ n = 3$.

$Z_{16} = Z_{2^4} \Rightarrow a = 4$. *According to Corollary 3.3.9, we find a constant b such that* $2^b \equiv -1(\mod n)$, *choose* $b = 1 \Leftrightarrow 2^1 \equiv -1(\mod 3) \Rightarrow$ *The only self-dual negacyclic code of length 12 over* Z_{16} *is* $\langle (x^n-1)^{2^{k-1}a}\rangle = \langle (x^3-1)^{2^{2-1}.4}\rangle = \langle (x^3-1)^8\rangle$.

Example 3.4.4. *Consider self-dual negacyclic codes of length 28 over* Z_{16}.

$\Rightarrow\ 28 = 2^2(7) \Rightarrow k = 2, n = 7, a = 4$. *There is only one pair asymmetric 2-cyclotomic coset (mod 7).* $\Rightarrow\ \delta(n) = 1 \Rightarrow$ *There are* $(2^k a+1)^{\delta(n)} = (2^2(4)+1)^1 = 17$ *self-dual negacyclic codes of length 28 over* Z_{16}*, all of which have order* 2^{56}. $\Rightarrow\ C_0 = \langle (u-1)^{2^{k-1}a}\rangle = \langle (u-1)^8\rangle$.

$x^7-1 = (x-1)(x^3+14x^2+13x+15)(x^3+11x^2+10x+15)$ *in* $Z_{16}[x]$.

The following table gives all self-dual negacyclic codes of length 28 over Z_{16}.

Non zero generator polynomial(s)
$\langle (u-1)^8 \rangle$.
$\langle (u-1)^8 (x^3+14x^2+13x+15)^{16} \rangle$
$\langle (u-1)^8 (x^3+11x^2+10x+15)^{16} \rangle$
$\langle (x^3+14x^2+13x+15)(u-1)^8 (x^3+11x^2+10x+15)^{15} \rangle$
$\langle (x^3+14x^2+13x+15)^{15}(u-1)^8 (x^3+11x^2+10x+15) \rangle$
$\langle (x^3+14x^2+13x+15)^{2}(u-1)^8 (x^3+11x^2+10x+15)^{14} \rangle$
$\langle (x^3+14x^2+13x+15)^{14}(u-1)^8 (x^3+11x^2+10x+15)^{2} \rangle$
$\langle (x^3+14x^2+13x+15)^{3}(u-1)^8 (x^3+11x^2+10x+15)^{13} \rangle$
$\langle (x^3+14x^2+13x+15)^{13}(u-1)^8 (x^3+11x^2+10x+15)^{3} \rangle$
$\langle (x^3+14x^2+13x+15)^{4}(u-1)^8 (x^3+11x^2+10x+15)^{12} \rangle$
$\langle (x^3+14x^2+13x+15)^{12}(u-1)^8 (x^3+11x^2+10x+15)^{4} \rangle$
$\langle (x^3+14x^2+13x+15)^{5}(u-1)^8 (x^3+11x^2+10x+15)^{11} \rangle$
$\langle (x^3+14x^2+13x+15)^{11}(u-1)^8 (x^3+11x^2+10x+15)^{5} \rangle$
$\langle (x^3+14x^2+13x+15)^{6}(u-1)^8 (x^3+11x^2+10x+15)^{10} \rangle$
$\langle (x^3+14x^2+13x+15)^{10}(u-1)^8 (x^3+11x^2+10x+15)^{6} \rangle$
$\langle (x^3+14x^2+13x+15)^{7}(u-1)^8 (x^3+11x^2+10x+15)^{9} \rangle$
$\langle (x^3+14x^2+13x+15)^{9}(u-1)^8 (x^3+11x^2+10x+15)^{7} \rangle$

Chapter 4

Cyclic Codes over the Ring $F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$

Among the four rings of four elements, the Galois field F_4 and more recently the ring of integers modulo four Z_4 are the most used in coding theory. Z_4 -codes are renowned for producing good nonlinear codes by the Gray map, namely Kerdok, preparata or Goethals codes. On the other hand, the ring Z_4 admits a linear Gray map which does not give good binary codes. Let R_k be the ring $F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0 \mod 2$, where $F_2 = \{0, 1\} = Z_2$.

In [3], Abualrub and Siap studied cyclic codes of an arbitrary length n over $F_2 + uF_2 = \{0, 1, u, u+1\}$ where $u^2 = 0 \mod 2$ and over $F_2 + uF_2 + u^2F_2 = \{0, 1, u, u+1, u^2, 1+u^2, 1+u+u^2, u+u^2\}$ where $u^3 = 0 \mod 2$. In this chapter, we extend these results to more general rings of the form $F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ where $u^k = 0 \mod 2$.

We give a unique set of generators for these codes as ideals in the ring
$R_{k,n} = R_k[x]/\langle x^n - 1\rangle$. Also we study the rank of these codes and give a minimal spanning set for them.

We show that the results of [3] concerning the codes over the rings $F_2 + uF_2$ with $u^2 = 0 \mod 2$ and $F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \mod 2$ are valid for $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0 \mod 2$.

4.1 Background

Definition 4.1.1. [3] A free module C is a module with a basis (a linearly independent spanning set for C).

Definition 4.1.2. The ring $R_k = F_2[u]/\langle u^k \rangle = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ is a commutative chain ring of 2^k elements with maximal ideal uR_k, where $u^k = 0$.
Since u is nilpotent with nilpotent index k, we have

$$R_k \supset\ uR_k \supset\ u^2R_k \supset \ldots \supset\ u^kR_k = 0.$$

Moreover $R_k/uR_k \cong\ Z_2$ is the residue field and $|u^iR_k| = 2|(u^{i+1}R_k)| = 2^{k-i}$, $i = 0, 1, 2, \ldots, k-1$.
Denote $R_1 = F_2 = \{0, 1\}$, $R_2 = F_2 + uF_2$, $R_3 = F_2 + uF_2 + u^2F_2, \ldots$ etc.

Definition 4.1.3. Let C_k be a code of length n over the ring $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0 \mod 2$, we mean an additive submodule of the $R-$module R_k^n. A cyclic code of length n over R_k is an ideal in the ring $R_{k,n} = R_k[x]/\langle x^n - 1 \rangle$.

Following Abualrub and Siap [3, p.p. 274], the parameters of an R_2-code C with $4^{k_1}2^{k_2}$ code words, where k_1 refers to the free part and k_2 refers to non free part ($u-$multiple generator of C), and minimum distance d is denoted by $(n, 4^{k_1}2^{k_2}, d)$. Such codes are often referred to as codes of type $\{k_1, k_2\}$. Similarly the parameters of an R_3-code C with $8^{k_1}4^{k_2}2^{k_3}$ code words, where k_1 refers to the free part and k_2, k_3 refer to non free part (u and u^2 multiple generators of C), and minimum distance d is denoted by $(n, 8^{k_1}4^{k_2}2^{k_3}, d)$. Such codes are often referred to as codes of type $\{k_1, k_2, k_3\}$.
We define the rank of a code C over R_2 of type $\{k_1, k_2\}$, denoted by rank(C), by the minimum number of generators of C, and define the free rank of C, denoted by f-rank(C), by the maximum of the ranks of R_2-free submodules of C. A code C of type $\{k_1, k_2\}$ has a rank $(k_1 + k_2)$ and a f-rank k_1.
We define the rank of a code C over R_3 of type $\{k_1, k_2, k_3\}$, denoted by rank(C), by the minimum number of generators of C, and define the free rank of C, denoted by f-rank(C),

by the maximum of the ranks of R_3-free submodules of C. A code C of type $\{k_1, k_2, k_3\}$ has a rank $(k_1 + k_2 + k_3)$ and a f-rank k_1.
Following the same procedure, we can define the ranks and free ranks of a code C over R_k $\forall$ $k \geq 4$.
Notation: We write a for $a(x)$, g for $g(x), \ldots$etc.

4.2 A generator Construction

The structure of cyclic codes over R_i depends on cyclic codes over R_{i-1} for $i = 2, 3, \ldots, k$ and the structure of cyclic codes over R_2 depends on cyclic codes over $R_1 = F_2$.
By following results in [3], let C_1 be a cyclic code in $R_{k,n} = R_k[x]/\langle x^n - 1\rangle$.
Define $\psi_1 : R_k \to R_{k-1}$ by $\psi_1(a) = a$. ψ_1 is a ring homomorphism that can be extended to a homomorphism $\phi_1 : C_1 \to \; R_{k-1,n} = R_{k-1}[x]/\langle x^n - 1\rangle$ defined by

$$\phi_1(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \psi_1(c_0) + \psi_1(c_1)x + \ldots + \psi_1(c_{n-1})x^{n-1}.$$

$$\ker \phi_1 = \{u^{k-1}r(x) : r(x) \in F_2[x]\}.$$

Let $J_1 = \{r(x) : u^{k-1}r(x) \in \ker \phi_1\}$, J_1 is an ideal in $R_{1,n} = R_1[x]/\langle x^n - 1\rangle = F_2[x]/\langle x^n - 1\rangle$ and hence a cyclic code in $F_2[x]/\langle x^n - 1\rangle$. So $J_1 = \langle a_{k-1}(x)\rangle$ and $\ker \phi_1 = \langle u^{k-1}a_{k-1}(x)\rangle$ with $a_{k-1}(x)|(x^n - 1) \mod 2$.
Let C_2 be a cyclic code in $R_{k-1,n} = R_{k-1}[x]/\langle x^n - 1\rangle$.
Define $\psi_2 : R_{k-1} \to R_{k-2}$ by $\psi_2(a) = a$. ψ_2 is a ring homomorphism that can be extended to a homomorphism $\phi_2 : C_2 \to R_{k-2}[x]/\langle x^n - 1\rangle$ defined by

$$\phi_2(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \psi_2(c_0) + \psi_2(c_1)x + \ldots + \psi_2(c_{n-1})x^{n-1}.$$

$$\ker \phi_2 = \{u^{k-2}r(x) : r(x) \in F_2[x]\}.$$

Let $J_2 = \{r(x) : u^{k-2}r(x) \in \ker \phi_2\}$ is an ideal in $R_{1,n} = F_2[x]/\langle x^n - 1\rangle$ and hence a cyclic code in $F_2[x]/\langle x^n - 1\rangle$. So $J_2 = \langle a_{k-2}(x)\rangle$ and hence $\ker(\phi_2) = \langle u^{k-2}a_{k-2}(x)\rangle$ with $a_{k-2}(x)|(x^n - 1) \mod 2$.

Let C_3 be a cyclic code in $R_{k-2,n} = R_{k-2}[x]/\langle x^n - 1\rangle$.

Define $\psi_3 : R_{k-2} \to R_{k-3}$ by $\psi_3(a) = a$. ψ_3 is a ring homomorphism that can be extended to a homomorphism $\phi_3 : C_3 \to R_{k-3}[x]/\langle x^n - 1\rangle$. Continue in the same way as above until we define $\psi_k : R_2 \to R_1 = F_2$ by $\psi_k(a) = a^2 \; mod \; 2$. ψ_k is a ring homomorphism because $(a+b)^2 = a^2 + b^2$ in R_2 and in F_2.

Extend ψ_k to a homomorphism $\phi_k : C_k \to F_2[x]/\langle x^n - 1\rangle = R_{1,n}$ defined by

$$\phi_k(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \psi_k(c_0) + \psi_k(c_1)x + \ldots + \psi_k(c_{n-1})x^{n-1}$$

$$= c_0^2 + c_1^2x + \ldots + c_{n-1}^2x^{n-1} \mod 2,$$

where C_k be a cyclic code in $R_{2,n} = R_2[x]/\langle x^n - 1\rangle$, where $R_2 = F_2 + uF_2$ with $u^2 = 0 \mod 2$.

$$\begin{aligned} \ker \phi_k &= \{ur(x) : r(x) \text{ is a binary polynomial in } F_2[x]/\langle x^n - 1\rangle\} \\ &= \langle ua_1(x)\rangle \text{ with } a_1(x) \big| (x^n - 1) \mod 2. \end{aligned}$$

The image of ϕ_k is also an ideal and hence a binary cyclic code generated by $g(x)$ with $g(x)\big|(x^n - 1)$. So the cyclic code over $R_2 = F_2 + uF_2$ would be in the form:

$C_k = \langle g(x) + up(x), ua_1(x)\rangle$ for some binary polynomial $p(x)$. Note that $a_1\big|(p\frac{x^n-1}{g})$ because

$$\phi_k\Big(\frac{x^n-1}{g}[g + up]\Big) = \phi_k\Big(up\frac{x^n-1}{g}\Big) = 0$$

$\Rightarrow \big(up\frac{x^n-1}{g}\big) \in \ker \phi_k = \langle ua_1\rangle$. Also $ug \in \ker \phi_k$ implies $a_1(x)\big|g(x)$.

Lemma 4.2.1. [3] *If $C_k = \langle g(x) + up(x), ua_1(x)\rangle$ over $R_2 = F_2 + uF_2$ with ($u^2 = 0 \mod 2$), and $g(x) = a_1(x)$ with $\deg g(x) = r$, then*
$C_k = \langle g(x) + up(x)\rangle$ and $(g + up)\big|(x^n - 1)$ in R_2.

Proof. Since $u(g + up) = ug$ and $g = a_1$, then $C_k \subseteq \langle g(x) + up(x)\rangle$.

Also as $C_k = \langle g(x)+up(x), ua_1(x)\rangle$, then $\langle g(x)+up(x)\rangle \subseteq C_k$, hence $C_k = \langle g(x)+up(x)\rangle$.

Now, by applying the division algorithm,

$x^n - 1 = (g(x) + up(x))q(x) + t(x)$, where $t(x) = 0$ or $\deg t(x) < \deg g(x) = r$. Since

$t(x) \in C_k$, then $t(x) = 0$. Thus $x^n - 1 = \big(g(x) + up(x)\big)q(x)$, and hence $(g + up)\big|\langle x^n - 1\rangle$ in R_2. □

Now since the image of ϕ_{k-1} is an ideal in $R_{2,n} = R_2[x]/\langle x^n - 1\rangle$ (where $R_2 = F_2 + uF_2$ with $u^2 = 0 \mod 2$), then $Im(\phi_{k-1}) = \langle g(x) + up_1(x), ua_1(x)\rangle$ with $a_1(x)\big|g(x)|(x^n - 1)$ and $a_1(x)\big|p_1(x)\big(\frac{x^n-1}{g(x)}\big)$. Also, $\ker(\phi_{k-1}) = \langle u^2 a_2(x)\rangle$ with $a_2(x)\big|(x^n - 1) \mod 2$. Since $u^2 a_1 \in \ker(\phi_{k-1}) = \langle u^2 a_2\rangle$, then the cyclic code C_{k-1} over $R_3 = F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \mod 2$ is

$C_{k-1} = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2\rangle$ with $a_2|a_1|g|(x^n - 1)$, $a_1(x)\big|p_1(x)\big(\frac{x^n-1}{g(x)}\big) \mod 2$, $a_2|q_1\big(\frac{x^n-1}{a_1}\big)$, $a_2|p_1\big(\frac{x^n-1}{g}\big)$ and $a_2\big|p_2\big(\frac{x^n-1}{g}\big)\big(\frac{x^n-1}{a_1}\big)$. We may assume that $\deg p_2 < \deg a_2$, $\deg q_1 < \deg a_2$, $\deg p_1 < \deg a_1$ (This is true since if $e = (a, b)$, then $e = (a, b + de)$ for any d).

Lemma 4.2.2. [3] *If $C_{k-1} = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2\rangle$ over $R_3 = F_2 + uF_2 + u^2F_2$ with ($u^3 = 0 \mod 2$), and $a_2 = g$, then $C_{k-1} = \langle g + up_1 + u^2p_2\rangle$ and $\big(g + up_1 + u^2p_2\big)\big|(x^n - 1)$ in R_3.*

Proof. Since $a_2 = g$, then $a_1 = a_2 = g$. From Lemma 4.2.1. we get that $\big(g + up\big)\big|(x^n - 1)$ in R_2 and $C_{k-1} = \langle g + up_1 + u^2p_2, u^2a_2\rangle$. The rest of the proof is similar to Lemma 4.2.1. □

Lemma 4.2.3. [3] *If n is odd, then $C_{k-1} = \langle g, ua_1, u^2a_2\rangle = \langle g + ua_1 + u^2a_2\rangle$ over R_3.*

Proof. See Lemma 8 in [3] □

Following the same process we find the cyclic code C_{k-2} over $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ with ($u^4 = 0 \mod 2$). So, since the image of ϕ_{k-2} is an ideal in $R_{3,n} = R_3[x]/\langle x^n - 1\rangle$ (where $R_3 = F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \mod 2$), then $Im(\phi_{k-2}) = \langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x)\rangle$ with $a_2|a_1|g|(x^n - 1)$, $a_1(x)\big|p_1(x)\big(\frac{x^n-1}{g(x)}\big) \mod 2$, $a_2|q_1(x)\bigg(\frac{(x^n-1)}{a_1(x)}\bigg)$ and $a_2\big|p_2(x)\big(\frac{x^n-1}{g(x)}\big)\big(\frac{x^n-1}{a_1(x)}\big)$. Also $\ker(\phi_{k-2}) = \langle u^3a_3(x)\rangle$ with $a_3(x)\big|(x^n - 1) \mod 2$.

Since $u^3a_2 \in \ker(\phi_{k-2}) = \langle u^3a_3(x)\rangle$, then the cyclic code C_{k-2} over

$R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ with $(u^4 = 0 \mod 2)$ is

$C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$ with

$$a_3 \big| a_2 \big| a_1 \big| g \big| (x^n - 1) \mod 2,\ a_1(x) \big| p_1(x) \big(\frac{x^n - 1}{g(x)} \big)\ mod\ 2,$$

$$a_2 \big| q_1(x) \Big(\frac{(x^n - 1)}{a_1(x)} \Big),\ a_2 \big| p_2(x) \big(\frac{x^n - 1}{g(x)} \big) \big(\frac{x^n - 1}{a_1(x)} \big),$$

$$a_3 \big| l_1(x) \Big(\frac{(x^n - 1)}{a_2(x)} \Big),\ a_3 \big| q_2(x) \big(\frac{x^n - 1}{q_1(x)} \big) \big(\frac{x^n - 1}{a_1(x)} \big)$$

and $a_3(x) \big| p_3(x) \big(\frac{x^n-1}{g(x)} \big) \big(\frac{x^n-1}{a_2(x)} \big) \big(\frac{x^n-1}{a_1(x)} \big)$. Moreover

$\deg p_3 < dega_3,\ \deg q_2 < dega_3,\ \deg l_1 < dega_3,\ \deg p_2 < dega_2,\ \deg q_1 < dega_2,\ \deg p_1 < dega_1$.

Lemma 4.2.4. *If $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$ over $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ with $(u^4 = 0 \mod 2)$, and $a_3 = g$, then $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3 \rangle$ and $\big(g + up_1 + u^2p_2 + u^3p_3 \big) \big| (x^n - 1)$ in R_4.*

Proof. Since $a_3 = g$, then $a_1 = a_2 = a_3 = g$. From Lemma 3.2 we get that $(g + up_1 + u^2p_2) \big| (x^n - 1)$ in R_3 and $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^3a_3 \rangle$. The rest of the proof is similar to Lemma 4.2.2. □

Lemma 4.2.5. *If n is odd, then the cyclic code C_{k-2} over R_4 can be written as*

$$C_{k-2} = \langle g, ua_1, u^2a_2, u^3a_3 \rangle = \langle g + ua_1 + u^2a_2 + u^3a_3 \rangle.$$

Proof. Since n is odd, then $(x^n - 1)$ factors uniquely into a product of distinct irreducible polynomials. So, $\gcd \big(a_1, \frac{x^n-1}{g(x)} \big) = \gcd \big(a_2, \frac{x^n-1}{a_1(x)} \big) = \gcd \big(a_2, \frac{x^n-1}{g(x)} \big) = \gcd \big(a_3, \frac{x^n-1}{a_2(x)} \big) = \gcd \big(a_3, \frac{x^n-1}{g(x)} \big) = 1$.

Since $a_1 \big| p_1(x) \big(\frac{x^n-1}{g(x)} \big)$, then $a_1 \big| p_1$. But $\deg p_1 < \deg a_1$. Hence $p_1 = 0$, since $a_2 \big| q_1(x) \big(\frac{x^n-1}{a_1(x)} \big)$ and $a_2(x) \big| p_2(x) \big(\frac{x^n-1}{g(x)} \big) \big(\frac{x^n-1}{a_1(x)} \big)$, then $a_2 \big| q_1$ and $a_2 \big| p_2$. But $\deg q_1 < \deg a_2$ and $\deg p_2 < \deg a_2$.

Hence, $p_2 = q_1 = 0$. Similarly $p_3 = q_2 = l_1 = 0$. So $C_{k-2} = \langle g, ua_1, u^2a_2, u^3a_3 \rangle$.

Let $h = g + ua_1 + u^2a_2 + u^3a_3$.
Then, $u^3h = u^3g$, $\frac{x^n-1}{a_2}h = \frac{x^n-1}{a_2}u^3a_3$ and $u^2\frac{x^n-1}{g}h = \frac{x^n-1}{g}u^3a_2 \in \langle h \rangle$. Since n is odd, we have $\left(\frac{x^n-1}{g}, g\right) = \left(\frac{x^n-1}{a_2}, a_2\right) = 1$. Hence
$1 = f_1\frac{x^n-1}{g} + f_2g$ for some polynomials f_1 and f_2, and $1 = m_1\frac{x^n-1}{a_2} + m_2a_2$ for some polynomials m_1 and m_2.
$u^3a_2 = u^3a_2f_1\frac{x^n-1}{g} + u^3a_2f_2g \in \langle h \rangle$. Also

$$u^3a_3 = u^3a_3m_1\frac{x^n-1}{a_2} + u^3a_3m_2a_2 \in \langle h \rangle$$

and $u^2a_2 = u^3m_2a_2^3 \in C_{k-2}$ and hence $g \in \langle h \rangle$. Similarly $ua_1 \in \langle h \rangle$.
Therefore $C_{k-2} = \langle g, ua_1, u^2a_2, u^3a_3 \rangle = \langle g + ua_1 + u^2a_2 + u^3a_3 \rangle$. □

From all the above discussion, we can construct any cyclic code C_1 over R_k by using the same process and induction to get the following theorem:

Theorem 4.2.6. *Let C_1 be a cyclic code in $R_{k,n} = R_k[x]/\langle x^n - 1 \rangle$, $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0$ mod 2.*
(1) If n is odd, then $R_{k,n}$ is a principal ideal ring and
$C_1 = \langle g, ua_1, u^2a_2, \ldots, u^{k-1}a_{k-1} \rangle = \langle g + ua_1 + u^2a_2 + \ldots + u^{k-1}a_{k-1} \rangle$
where $g(x), a_1(x), a_2(x), \ldots, a_{k-1}(x)$ are binary polynomials with
$a_{k-1}(x)\big|a_{k-2}(x)\big|\ldots\big|a_2(x)\big|a_1(x)\big|g(x)\big|(x^n - 1) \mod 2$.
(2) If n is not odd, then
(a) $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1} \rangle$ where $g(x)$, $p_i(x)$ are binary polynomials $\forall i = 1, 2, \ldots, k-1$ with $g(x)\big|(x^n - 1) \mod 2$, $(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1})\big|(x^n - 1)$ in R_k and $\deg\ p_i < deg\ p_{i-1}$ for all $2 \le i \le k-1$. Or,
(b) $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, u^{k-1}a_{k-1} \rangle$ where $a_{k-1}|g|(x^n - 1)$ mod 2, $(g + up)|(x^n - 1)$ in R_2, $g(x)|p_1\left(\frac{x^n-1}{g(x)}\right)$ and $a_{k-1}|p_1\left(\frac{x^n-1}{g(x)}\right)$, $a_{k-1}|p_2\left(\frac{x^n-1}{g(x)}\right)\left(\frac{x^n-1}{g(x)}\right), \ldots$ and $a_{k-1}|p_{k-1}\left(\frac{x^n-1}{g(x)}\right)\ldots\left(\frac{x^n-1}{g(x)}\right)(k-1, times)$ and deg $p_{k-1} <$ deg a_{k-1}. Or,
(c) $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}a_{k-2} + u^{k-1}t_1, u^{k-1}a_{k-1} \rangle$ with $a_{k-1}\big|a_{k-2}\big|\ldots\big|a_2\big|a_1\big|g\big|(x^n - 1) \mod 2$, $a_{k-2}|p_1\left(\frac{x^n-1}{g}\right), \ldots, a_{k-1}|t_1\left(\frac{x^n-1}{a_{k-2}}\right), \ldots, a_{k-1}|p_{k-1}\left(\frac{x^n-1}{g}\right)\ldots\left(\frac{x^n-1}{a_{k-2}}\right)$.
Moreover deg $p_{k-1} <$ deg $a_{k-1}, \ldots,$ deg $t_1 <$ deg $a_{k-1}, \ldots$ and deg $p_1 <$ deg a_{k-2}.

4.3 Ranks and Minimal Spanning Sets for Cyclic Codes over R_k

Theorem 4.3.1. [3] *Let C be a cyclic code of even length n over $R_2 = F_2 + uF_2$ with $u^2 = 0$ mod 2.*

(1) If $C = \langle g(x) + up(x) \rangle$ with deg $g(x) = r$ *and $\big(g(x) + up(x)\big) \big| (x^n - 1)$, then C is a free module with* $\mathrm{rank}(C) = n - r$ *and basis*

$$\beta = \Big\{ g + up(x),\ xg(x) + up(x), \ldots, x^{n-r-1}(g(x) + up(x)) \Big\}\ ,\ \textit{and } |C| = 4^{n-r}.$$

(2) If $C = \langle g(x)+up(x), ua(x) \rangle$ with deg $g(x) = r$, deg $a(x) = t$, *then C has* $\mathrm{rank}(C) = n - t$ *and a minimal spanning set given by*

$$\chi = \Big\{ g(x) + up(x), x(g(x) + up(x)) + \ldots + x^{n-r-1}\big(g(x) + up(x)\big), ua(x), xua(x), \ldots, x^{r-t-1}ua(x) \Big\},\ \textit{and } |C| = 2^{2n-r-t}.$$

Proof. (1)Let C be a cyclic code of even length n over $R_2 = F_2 + uF_2$ with $u^2 = 0 \mod 2$. Suppose $x^n - 1 = (g + up)(h + up)$ over R_2. Let $c(x) \in C = \langle g(x) + up(x) \rangle$, then $c(x) = (g(x) + up(x))f(x)$ for some polynomial $f(x)$.

If $f(x)$ has a degree less than or equal $n - r - 1$, then we are done, otherwise by division algorithm there exist two polynomials $q(x)$, $s(x)$ such that $f(x) = \big(\frac{x^n - 1}{g + up}\big)q(x) + s(x)$, where $s(x) = 0$ or $\deg s(x) \leq n - r - 1$.

Now, $(g(x) + up(x))f(x) = (g(x) + up(x))\big(\frac{x^n-1}{g(x)+up(x)}q(x) + s(x)\big) = (g(x) + up(x))s(x)$.

Since $\deg s(x) \leq n - r - 1$, then β spans C. Now we only need to show that β is linearly independent. Let $g(x) = 1 + g_1x + \ldots + x^r$ and $p(x) = p_0 + p_1x + \ldots + p_lx^l$. Suppose $(g(x) + up(x))c_0 + x(g(x) + up(x))c_1 + \ldots + x^{n-r-1}(g(x) + up(x))c_{n-r-1} = 0$.

Comparing coefficients in the above equation we get that

$(1 + up_0)c_0 = 0$ (constant coefficient).

Since $(1 + up_0)$ is a unit, then $c_0 = 0$.

Hence $x(g(x) + up(x))c_1 + \ldots + x^{n-r-1}(g(x) + up(x))c_{n-r-1} = 0$.

Again comparing coefficient we get that

$(1 + up_0)c_1 = 0$ (coefficient of x).

This implies that $c_1 = 0$. Similarly we get that $c_i = 0$ for all $i = 0, 1, \ldots, n-r-1$. Therefore β is linearly independent and hence a basis for C.

(2) Suppose $C = \langle g(x) + up(x), ua(x) \rangle$ with $\deg g(x) = r,\ \deg a(x) = t$. Since the lowest degree polynomial in C is $ua(x)$, then it is suffices to show that

χ spans $\gamma = \Big\{ g(x) + up(x), x(g(x) + up(x)), \ldots, x^{n-r-1}\big(g(x) + up(x)\big), ua(x), xua(x), \ldots, x^{n-t-1}ua(x) \Big\}$.

Similarly it suffices to show that $ux^{r-t}a(x) \in \mathrm{span}(\gamma)$.

$ux^{r-t}a(x) = u(g(x) + up(x)) + um(x)$ where $um(x)$ is a polynomial in C of degree less than r. Since any polynomial in C must have degree greater than or equal to $\deg a(x) = t$, then $t \leq \deg m(x) < r$. Hence $um(x) = \alpha_0 ua(x) + \alpha_1 xua(x) + \ldots + \alpha_{r-t-1} x^{r-t-1} ua(x)$.

Hence, χ is a generating set. By comparing coefficients as in (1) there is no elements in χ is a linear combination of the others. Therefore χ is a minimal generating set. $\square$

By following the same process, we find the rank and the minimal spanning set for any cyclic code over the ring R_i for $i = 2, 3, \ldots, k$.

To do this, let us consider the cyclic code C_{k-2} of even length n over the ring

$R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ with $u^4 = 0 \mod 2$.

(1) If $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3 \rangle$ as in Lemma 4.2.4, $\deg\ g(x) = r$, then C_{k-2} is a free module with $\mathrm{rank}(C_{k-2}) = n - r$ and basis

$$\beta = \Big\{ (g+up_1+u^2p_2+u^3p_3),\ x(g+up_1+u^2p_2+u^3p_3), \ldots,\ x^{n-r-1}(g+up_1+u^2p_2+u^3p_3) \Big\}.$$

(2) If $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$,

where $a_3 \big| a_2 \big| a_1 \big| g \big| (x^n - 1) \mod 2$ with $\deg\ g(x) = r$,

$\deg\ a_1(x) = s,\ \deg\ a_2(x) = t\ \mathit{and}\ \deg\ a_3(x) = b$, then C_{k-2} has $\mathrm{rank}(C_{k-2}) = n - b\ \mathit{and}$ a minimal spanning set given by

$\chi = \Big\{ (g + up_1 + u^2p_2 + u^3p_3),\ x(g + up_1 + u^2p_2 + u^3p_3),\ \ldots,\ x^{n-r-1}(g + up_1 + u^2p_2 + u^3p_3),\ (ua_1 + u^2q_1 + u^3q_2),\ x(ua_1 + u^2q_1 + u^3q_2),\ \ldots,\ x^{r-s-1}(ua_1 + u^2q_1 + u^3q_2),\ (u^2a_2 + u^3l_1),\ x(u^2a_2+u^3l_1),\ \ldots,\ x^{s-t-1}(u^2a_2+u^3l_1),\ (u^3a_3(x)),\ x(u^3a_3(x)),\ \ldots,\ x^{t-b-1}(u^3a_3(x)) \Big\}$.

(3) If $C_{k-2} = \langle g + up_1 + u^2p_2 + u^3p_3, u^3a_3 \rangle$ where $\deg\ g(x) = r$, $\deg\ a_3(x) = t$, then C_{k-2} has $\mathrm{rank}(C_{k-2}) = n - t$ and a minimal spanning set given by

$\Gamma = \Big\{(g + up_1 + u^2p_2 + u^3p_3),\ x(g + up_1 + u^2p_2 + u^3p_3), \ldots,\ x^{n-r-1}(g + up_1 + u^2p_2 + u^3p_3), u^3a_3,\ xu^3a_3, \ldots, x^{r-t-1}u^3a_3\Big\}$.

Continue in the same way as above to get the following Theorem which is a generalization of the results in [3].

Theorem 4.3.2. *Let C_1 be a cyclic code of even length n over $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0 \mod 2$.*

The constraints on the generator polynomials as in Theorem 4.2.6.

(1) *If $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}\rangle$, $\deg\ g(x) = r$, then C_1 is a free module with $\mathrm{rank}(C_1) = n - r$ and basis*

$\beta = \Big\{(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}),\ x(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}),\ \ldots,\ x^{n-r-1}(g+up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1})\Big\}$.

(2) *If $C_1 = \langle g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}, ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}, u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}, \ldots, u^{k-2}a_{k-2}+u^{k-1}t_1, u^{k-1}a_{k-1}\rangle$ with $\deg\ g(x) = r_1$, $\deg\ a_1(x) = r_2$, $\deg\ a_2(x) = r_3, \ldots$, $\deg\ a_{k-1} = r_k$, then C_1 has $\mathrm{rank}(C_1) = n - r_k$ and a minimal spanning set given by*

$\chi = \Big\{\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ x\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \ldots,\ x^{n-r_1-1}\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ x\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ \ldots,\ x^{r_1-r_2-1}\big(ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}\big),\ (u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}),\ x(u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}),\ \ldots,\ x^{r_2-r_3-1}(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ u^{k-1}a_{k-1}(x),\ xu^{k-1}a_{k-1}(x),\ \ldots,\ x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)\Big\}$.

(3) *If $C_1 = \langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, u^{k-1}a_{k-1}\rangle$ with deg $g(x) = r$,deg $a_{k-1} = t$ then C_1 has $\mathrm{rank}(C_1) = n - t$ and a minimal spanning set given by*

$\Gamma = \Big\{(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}),\ x(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}),\ \ldots,\ x^{n-r-1}(g+up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}),\ u^{k-1}a_{k-1},\ xu^{k-1}a_{k-1}, \ldots, x^{r-t-1}u^{k-1}a_{k-1}\Big\}$.

Proof. (1) Let C_1 be a cyclic code of even length over $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0 \mod 2$. Suppose

$$x^n - 1 = \big(g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}\big)\big(h + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}\big) \text{ over} R_k.$$

Let $c(x) \in\ C_1 = \big\langle g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big\rangle$, then $c(x) = \big(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big)f(x)$ for some polynomial $f(x)$. If $\deg(f(x) \leq n-r-1,$ then we are done, otherwise by division algorithm there exist two polynomials $q(x), s(x)$ such that

$$f(x) = \left(\frac{x^n - 1}{g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}}\right)q(x) + s(x)$$

where $s(x) = 0$ or $\deg(s(x)) \leq n-r-1$.
Now, $\Bigg(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\Bigg)f(x)$
$= \Bigg(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\Bigg)\Bigg(\frac{x^n-1}{g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}}q(x) + s(x)\Bigg)$
$= \Bigg(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\Bigg)s(x)$. Since $\deg(s(x)) \leq n-r-1,$ then β spans C_1. Now we only need to show that β is linearly independent. Let $g(x) = 1 + g_1x + \ldots + x^r,\ p_1(x) = p_{1,0} + p_{1,1}x + \ldots + p_{1,l}x^l,\ p_2(x) = p_{2,0} + p_{2,1}x + \ldots + p_{2,b}x^b, \ldots,\ p_{k-1}(x) = p_{k-1,0} + p_{k-1,1}x + \ldots + p_{k-1,d}x^d$. Suppose $\big(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big)c_0 + x\big(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big)c_1 + \ldots + x^{n-r-1}\big(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big)c_{n-r-1} = 0$. Comparing coefficients in the above equation we get that $\big(1 + up_{1,0} + u^2p_{2,0} + \ldots + u^{k-1}p_{k-1,0}\big)c_0 = 0$ (constant coefficient).
Since $\big(1 + up_{1,0} + u^2p_{2,0} + \ldots + u^{k-1}p_{k-1,0}\big)$ is a unit, then $c_0 = 0$.
Hence, $x\big(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big)c_1 + \ldots + x^{n-r-1}\big(g(x) + up_1(x) + u^2p_2(x) + \ldots + u^{k-1}p_{k-1}(x)\big)c_{n-r-1} = 0$.
Again comparing coefficients we get that
$\big(1 + up_{1,0} + u^2p_{2,0} + \ldots + u^{k-1}p_{k-1,0}\big)c_1 = 0$. (coefficient of x)
This implies that $c_1 = 0$. Similarly we get that $c_i = 0$ for all $i = 0, 1, \ldots, n-r-1$. Therefore, β is linearly independent and hence a basis for C_k.
(2) Suppose $C_1 = \big\langle g + up_1 + u^2p_2 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-1}a_{k-1}\big\rangle$ with $\deg(g + up_1 + \ldots + u^{k-1}p_{k-1}) = r_1,\ \deg(ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}) = r_2,\ \deg(u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}) = r_3, \ldots,\ \deg(u^{k-1}a_{k-1}) = r_k$.
Since the lowest degree polynomial in C_1 is $u^{k-1}a_{k-1}(x)$, then it's suffices to show that χ spans

$\gamma = \Big\{\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ x\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \ldots,\ x^{n-r_1-1}\big(g+up_1+u^2p_2+\ldots+u^{k-1}p_{k-1}\big),\ \big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ x\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ldots,\ x^{r_1-r_2-1}\big(ua_1+u^2q_1+\ldots+u^{k-1}q_{k-2}\big),\ (u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ x(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ x^{r_2-r_3-1}(u^2a_2+u^3l_1+\ldots+u^{k-1}l_{k-3}),\ \ldots,\ u^{k-1}a_{k-1}(x),\ xu^{k-1}a_{k-1}(x),\ldots,\ x^{n-r_k-1}u^{k-1}a_{k-1}(x)\Big\}.$

Similarly, it suffices to show that $u^{k-1}x^{r_{k-1}-r_k}a_{k-1} \in \text{span}\gamma$.

$u^{k-1}x^{r_{k-1}-r_k}a_{k-1}(x) = u^{k-1}\big(g(x)+up_1(x)+u^2p_2(x)+\ldots+u^{k-1}p_{k-1}(x)\big)+u^{k-1}m(x)$, where $u^{k-1}m(x)$ is a polynomial in C_1 of degree less than r_{k-1}.

Since any polynomial in C_1 must have degree greater or equal to

$\deg(u^{k-1}a_{k-1}(x)) = r_k$, then $r_k \le \deg(m(x)) < r_{k-1}$.

Hence $u^{k-1}m(x) = \alpha_0 u^{k-1}a_{k-1}(x)+\alpha_1 xu^{k-1}a_{k-1}(x)+\ldots+\alpha_{r_{k-1}-r_k-1}x^{r_{k-1}-r_k-1}u^{k-1}a_{k-1}(x)$.

Hence, χ is a generating set.

By comparing coefficients as in (1) we get that non of elements in χ is a linear combination of the others. Therefore χ is a minimal generating set.

(3) this case is a special case of case (2). So the proof is similar to case (2). □

Definition 4.3.1. [3] Let $C = \big\langle g + up(x), ua(x)\big\rangle$ be a cyclic code of even length n over $R_2 = F_2 + uF_2$. We define $C_u = \big\{k(x) : uk(x) \in C\big\}$ in $R_{2,n} = R_2[x]/\big\langle x^n - 1\big\rangle$.

Remark 4.3.1. [3] C_u is a cyclic code over $F_2 = \{0, 1\} = R_1$.

Proof. Let $k(x) \in C_u$, we need to show that $xk(x) \in C_u$.

Now since $k(x) \in C_u \Rightarrow uk(x) \in C$, but C is cyclic code over $R_2 \Rightarrow xuk(x) \in C \Rightarrow xk(x) \in C_u$. □

Definition 4.3.2. [3] Let $C = \big\langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2\big\rangle$ be a cyclic code of even length over $R_3 = F_2 + uF_2 + u^2F_2$ with ($u^3 = 0 \mod 2$). We define $C_{u^2} = \big\{k(x) : u^2k(x) \in C\big\}$ in $R_{3,n} = R_3[x]/\big\langle x^n - 1\big\rangle$.

Remark 4.3.2. [3] C_{u^2} is a cyclic code over $R_1 = \{0, 1\} = F_2$.

Proof. Let $k(x) \in C_{u^2}$, we need to show that $xk(x) \in C_{u^2}$.

Now, since $k(x) \in C_{u^2} \Rightarrow u^2k(x) \in C,$ but C is cyclic code over $R_3 \Rightarrow xu^2k(x) \in C \Rightarrow xk(x) \in C_{u^2}$. $\square$

By following the same process, we define $C_{u^{i-1}}$ over the ring R_i for $i = 2, 3, \ldots, k$. So, if $i = 4$, then we let $C = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$ be a cyclic code of even length over $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ with $(u^4 = 0 \mod 2) \Rightarrow C_{u^3} = \{R(x) : u^3k(x) \in C\}$ is a cyclic code over F_2.
Hence, we generalize these definitions to more general ring R_k as follows:

Definition 4.3.3. Let $C = \langle g + up_1 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}a_{k-2} + u^{k-1}t_1, u^{k-1}a_{k-1} \rangle$
be a cyclic code of even length n over $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ with $u^k = 0\, mod\, 2$. We define $C_{u^{k-1}} = \{k(x) : u^{k-1}k(x) \in C\}$ in $R_{k,n}$.

Remark 4.3.3. $C_{u^{k-1}}$ is a cyclic code over $F_2 = \{0, 1\}$.

Proof. Let $k(x) \in C_{u^{k-1}},$ we need to show that $xk(x) \in C_{u^{k-1}}$.
Now, since $k(x) \in C_{u^{k-1}} \Rightarrow u^{k-1}k(x) \in C,$ but C is cyclic code over $R_k \Rightarrow xu^{k-1}k(x) \in C \Rightarrow xk(x) \in C_{u^{k-1}}$. $\square$

Theorem 4.3.3. *[3] Let $C = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2 \rangle$.*
Then $C_{u^2} = \langle a_2(x) \rangle$ and $w_H(C) = w_H(C_{u^2})$.

Proof. Since $u^2a_2 \in C$, then $\langle a_2(x) \rangle \subseteq C_{u^2}$. Now given an $b(x) \in C_{u^2}$, then $u^2b(x) \in C$ and hence there exist polynomials $c(x),\ e(x),\ k(x) \in F_2[x]$ such that
$u^2b(x) = c(x)u^2g(x) + e(x)u^2a_1(x) + k(x)u^2a_2(x)$. Since $a_2(x)\big|g(x)$ and $a_2(x)\big|a_1(x),$ we have $u^2b(x) = u^2l(x)a_2(x)$ for some $l(x)$. So $C_{u^2} \subseteq \langle a_2(x) \rangle$ and hence $C_{u^2} = \langle a(x) \rangle$.
Furthermore, given a codeword $l(x) = l_0(x) + ul_1(x) + u^2l_2(x) \in C$ where
$l_0(x), l_1(x), l_2(x) \in F_2[x],$ since $u^2l(x) = u^2l_0(x) \in C$ and $w_H(u^2l(x)) \leq w_H(l(x))$ and u^2C is a subcode of C with $w_H(u^2C) \leq w_H(C)$ it is sufficient to focus on the subcode u^2C in order to compute the Hamming weight of C. Since $u^2C = \langle u^2a_2(x) \rangle,$ thus $w_H(C) = w_H(C_{u^2})$. $\square$

According to Theorem 4.3.3,

if $C = \langle g + up_1 + u^2p_2 + u^3p_3, ua_1 + u^2q_1 + u^3q_2, u^2a_2 + u^3l_1, u^3a_3 \rangle$ over $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ with ($u^4 = 0 \mod 2$).

Then $C_{u^3} = \langle a_3(x) \rangle$ and $w_H(C) = w_H(C_{u^3})$.

Continue in the same way as above we have the following theorem:

Theorem 4.3.4. *If* $C = \langle g + up_1 + \ldots + u^{k-1}p_{k-1}, ua_1 + u^2q_1 + \ldots + u^{k-1}q_{k-2}, u^2a_2 + u^3l_1 + \ldots + u^{k-1}l_{k-3}, \ldots, u^{k-2}a_{k-2} + u^{k-1}t_1, u^{k-1}a_{k-1} \rangle$ *is a cyclic code of even length over* $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ *with* $u^k = 0 \mod 2$. *Then* $C_{u^{k-1}} = \langle a_{k-1} \rangle$ *and* $w_H(C) = w_H(C_{u^{k-1}})$.

Proof. Since $u^{k-1}a_{k-1} \in C$, then $\langle a_{k-1}(x) \rangle \subseteq C_{u^{k-1}}$. Now given an $b(x) \in C_{u^{k-1}}$, then $u^{k-1}b(x) \in C$ and hence there exist polynomials $c_1(x), c_2(x), \ldots, c_t(x) \in F_2[x]$ such that $u^{k-1}b(x) = c_1(x)u^{k-1}g(x) + c_2(x)u^{k-1}a_1(x) + c_3(x)u^{k-1}a_2(x) + \ldots + c_t(x)u^{k-1}a_{k-1}(x)$. Since $a_{k-1}(x) \big| a_{k-2}(x) \big| \ldots \big| a_2(x) \big| a_1(x) \big| g(x)$, we have $u^{k-1}b(x) = u^{k-1}m(x)a_{k-1}(x)$ for some $m(x)$. So $C_{u^{k-1}} \subseteq \langle a_{k-1}(x) \rangle$ and hence $C_{u^{k-1}} = \langle a_{k-1}(x) \rangle$.

Further, given a codeword $m(x) = m_0(x_0) + um_1(x) + u^2m_2(x) + \ldots + u^{k-1}m_{k-1}(x) \in C$, where $m_0(x), m_1(x), m_2(x), \ldots, m_{k-1}(x) \in F_2[x]$, since $u^{k-1}m(x) = u^{k-1}m_0(x) \in C$ and $w_H(u^{k-1}m(x)) \leq w_H(m(x))$ and $u^{k-1}C$ is a subcode of C with $w_H(u^{k-1}C) \leq w_H(C)$ it is sufficient to focus on the subcode $u^{k-1}C$ in order to compute the Hamming weight of C. Since $u^{k-1}C = \langle u^{k-1}a_{k-1}(x) \rangle$, thus $w_H(C) = w_H(C_{u^{k-1}})$. □

4.4 Examples

Example 4.4.1. *Cyclic codes of length 5 over* $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$ *with* $u^4 = 0 \mod 2$.

Now, $x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1) = g_1g_2$

$\Rightarrow$*The Nonzero cyclic codes of length 5 over* R_4 *with generator polynomials are on the following table:*

Non zero generator polynomials
$\langle 1\rangle,\ \langle g_1\rangle,\ \langle g_2\rangle$
$\langle u\rangle,\ \langle ug_1\rangle,\ \langle ug_2\rangle$
$\langle u^2\rangle,\ \langle u^2g_1\rangle,\ \langle u^2g_2\rangle$
$\langle u^3\rangle,\ \langle u^3g_1\rangle,\ \langle u^3g_2\rangle$
$\langle g_1,u\rangle,\ \langle g_2,u\rangle,\ \langle g_1,u^2\rangle,\ \langle g_2,u^2\rangle$
$\langle g_1,u^3\rangle,\ \langle g_2,u^3\rangle$
$\langle ug_1,u^2\rangle,\ \langle ug_2,u^2\rangle$
$\langle u^2g_1,u^3\rangle,\ \langle u^2g_2,u^3\rangle$

Table 1 : Cyclic codes of length 5 over $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$

Example 4.4.2. [3] *If* $k = 2 \Rightarrow R_2 = F_2 + uF_2$, *let* $n = 8$, *then* $x^8 - 1 = (x-1)^8 = [g(x)]^8$ *over* Z_2.

We will list all free module cyclic codes and all non free module of length 8 *over* $R_2 = F_2 + uF_2$.

In the case for free module cyclic codes, and due to the classification theorems, we have the following tables that give all such codes:

Non zero generator polynomial(s) =g=x+1
1
$\langle g\rangle, \langle g+u\rangle$
$\langle g + u(c_0 + c_1x)\rangle$
$\langle g^3 + u(c_0 + c_1x + c_2x^2)\rangle$
$\langle g^4 + u(c_0 + c_1x + c_2x^2 + c_3x^3)\rangle$
$\langle g^5 + u(x^2+1)(c_0 + c_1x + c_2x^2)\rangle$
$\langle g^6 + u(x+1)^4(c_0 + c_1x)\rangle$
$\langle g^7 + uc_0\rangle$

Table 2 : Free module cyclic code of length 8 over $R_2 = F_2 + uF_2$

To illustrate the cyclic code $\langle g^3 + u(c_0 + c_1x + c_2x^2)\rangle$
$C = \langle g(x) + up(x)\rangle \Rightarrow g(x) = g^3 = (x+1)^3 \mod 2$,

$p(x) = c_0 + c_1x + c_2x^2 \mod 2 \Rightarrow \deg p(x) < \deg g(x)$,
$g(x)\big|(x^8-1)$ *since* $(x+1)^3\big|(x^8-1)$,
$g(x)\big|p(x)\big(\frac{x^8-1}{g(x)}\big)$ *since* $\frac{x^8-1}{g(x)} = \frac{x^8-1}{(x+1)^3} = (x+1)^5$
$\Rightarrow (x+1)^3\Big|(c_0+c_1x+c_2x^2)(x+1)^5$.
According to Theorem 4.3.1
$deg\big(g(x)+up(x)\big) = 3 \Rightarrow$ *f-rank*$(C) = n - r = 8 - 3 = 5$ *and* C *has a basis given by*
$\beta = \Big\{g^3+u(c_0+c_1x+c_2x^2),\ x\big(g^3+u(c_0+c_1x+c_2x^2)\big),\ \cdots\ x^4\big(g^3+u(c_0+c_1x+c_2x^2)\big)\Big\}$
and $|C| = 4^{n-r} = 4^5$ *codewords.*

Non zero generator polynomial(s) :g=x+1
$\langle u\rangle$
$\langle ug^i\rangle,\ i=1,2,3,4,5,6$
$\langle ug^7\rangle$
$\langle g^i,u\rangle,\ i=1,2,3,4,5,6,7$
$\langle g^2+uc_0,ug)\rangle$
$\langle g^3+uc_0,ug)\rangle$
$\langle g^3+u(c_0+c_1x),ug^2\rangle$
$\langle g^4+uc_0,ug\rangle$
$\langle g^4+u(c_0+c_1x),ug^2\rangle$
$\langle g^4+u(c_0+c_1x+c_2x^2),ug^3\rangle$
$\langle g^5+uc_0,ug\rangle$
$\langle g^5+u(c_0+c_1x),ug^2\rangle$
$\langle g^5+u(c_0+c_1x+c_2x^2),ug^3\rangle$
$\langle g^5+u(x+1)(c_0+c_1x+c_2x^2),ug^4\rangle$
$\langle g^6+uc_0,ug\rangle$
$\langle g^6+u(c_0+c_1x),ug^2\rangle$
$\langle g^6+ug(c_0+c_1x),ug^3\rangle$
$\langle g^6+ug^2(c_0+c_1x),ug^4\rangle$
$\langle g^6+ug^3(c_0+c_1x),ug^5\rangle$
$\langle g^7+uc_0,ug\rangle$
$\langle g^7+ugc_0,ug^2\rangle,\langle g^7+ug^2c_0,ug^3\rangle,\langle g^7+ug^3c_0,ug^4\rangle$
$\langle g^7+ug^4c_0,ug^5\rangle,\langle g^7+ug^5c_0,ug^6\rangle$

Table 3 : Non Free module cyclic code of length 8 over $R_2 = F_2 + uF_2$

To illustrate the generator polynomial $\big\langle g^5+uc_0,ug\big\rangle$:

$C = \big\langle g(x)+up(x),ua(x)\big\rangle \Rightarrow g(x) = g^5 = (x+1)^5 \mod 2,\ p(x) = c_0 \mod 2$,

$a(x) = g = x+1 \mod 2 \Rightarrow \deg a(x) > \deg p(x)$,

$a(x)\big|g(x)\big|x^8-1 \mod 2$, *since* $(x+1)\big|(x+1)^5\big|(x^8-1)$,

$a(x)\big|p(x)\big(\frac{x^8-1}{g(x)}\big)$ *since* $\frac{x^8-1}{g(x)} = \frac{x^8-1}{(x+1)^5} = (x+1)^3 \mod 2$

$\Rightarrow x+1\big|c_0(x+1)^3$.

Example 4.4.3. *If $n = 8$ over $R_3 = F_2 + uF_2 + u^2F_2$ with $u^3 = 0 \mod 2$.*
$x^8 - 1 = (x-1)^8 = \big(g(x)\big)^8$ *over $F_2 = \{0, 1\}$.*
The nonzero free/non free module cyclic codes over R_3 are on the following tables:

Non zero generator polynomial(s): g=x+1
$\langle 1\rangle,\ \langle g\rangle,\ \langle g+u\rangle,\ \langle g+u^2\rangle$
$\langle g+u(c_0+c_1x)\rangle,\ \langle g+u^2(c_0+c_1x)\rangle$
$\langle g^3+u(c_0+c_1x+c_2x^2)\rangle,\ \langle g^3+u^2(c_0+c_1x+c_2x^2)\rangle$
$\langle g^4+u(c_0+c_1x+c_2x^2+c_3x^3)\rangle,\ \langle g^4+u^2(c_0+c_1x+c_2x^2+c_3x^3)\rangle$
$\langle g^5+u(x^2+1)(c_0+c_1x+c_2x^2)\rangle,\ \langle g^5+u^2(x^2+1)(c_0+c_1x+c_2x^2)\rangle$
$\langle g^6+u(x+1)^4(c_0+c_1x)\rangle,\ \langle g^6+u^2(x+1)^4(c_0+c_1x)\rangle$
$\langle g^7+uc_0\rangle,\ \langle g^7+u^2c_0\rangle$

Table 4 : Non zero Free module cyclic codes of length 8 over $R_3 = F_2 + uF_2 + u^2F_2$

Non zero generator polynomial(s): g=x+1
$\langle u\rangle,\ \langle u^2\rangle$
$\langle ug^i\rangle,\ i=1,\ldots,7,\ \langle u^2g^i\rangle,\ i=1,\ldots,7.$
$\langle g^i,u\rangle,\ i=1,2,\ldots,7,\ \langle g^i,u^2\rangle,\ i=1,\ldots,7.$
$\langle g^2+uc_0,ug\rangle,\ \langle g^2+u^2c_0,u^2g\rangle$
$\langle g^3+uc_0,ug)\rangle,\ \langle g^3+u^2c_0,u^2g)\rangle$
$\langle g^3+u(c_0+c_1x),ug^2\rangle,\ \langle g^3+u^2(c_0+c_1x),u^2g^2\rangle$
$\langle g^4+uc_0,ug\rangle,\ \langle g^4+u^2c_0,u^2g\rangle$
$\langle g^4+u(c_0+c_1x),ug^2\rangle,\ \langle g^4+u^2(c_0+c_1x),u^2g^2\rangle$
$\langle g^4+u(c_0+c_1x+c_2x^2),ug^3\rangle,\ \langle g^4+u^2(c_0+c_1x+c_2x^2),u^2g^3\rangle$
$\langle g^5+uc_0,ug\rangle,\ \langle g^5+u^2c_0,u^2g\rangle$
$\langle g^5+u(c_0+c_1x),ug^2\rangle,\ \langle g^5+u^2(c_0+c_1x),u^2g^2\rangle$
$\langle g^5+u(c_0+c_1x+c_2x^2),ug^3\rangle,\ \langle g^5+u^2(c_0+c_1x+c_2x^2),u^2g^3\rangle$
$\langle g^5+u(x+1)(c_0+c_1x+c_2x^2),ug^4\rangle,\ \langle g^5+u^2(x+1)(c_0+c_1x+c_2x^2),u^2g^4\rangle$
$\langle g^6+uc_0,ug\rangle,\ \langle g^6+u^2c_0,u^2g\rangle$
$\langle g^6+u(c_0+c_1x),ug^2\rangle,\ \langle g^6+u^2(c_0+c_1x),u^2g^2\rangle$
$\langle g^6+ug(c_0+c_1x),ug^3\rangle,\ \langle g^6+u^2g(c_0+c_1x),u^2g^3\rangle$
$\langle g^6+ug^2(c_0+c_1x),ug^4\rangle,\ \langle g^6+u^2g^2(c_0+c_1x),u^2g^4\rangle$
$\langle g^6+ug^3(c_0+c_1x),ug^5\rangle\ \langle g^6+u^2g^3(c_0+c_1x),u^2g^5\rangle$
$\langle g^7+uc_0,ug\rangle,\ \langle g^7+u^2c_0,u^2g\rangle$
$\langle g^7+ugc_0,ug^2\rangle,\ \langle g^7+u^2gc_0,u^2g^2\rangle$
$\langle g^7+ug^2c_0,ug^3\rangle,\ \langle g^7+u^2g^2c_0,u^2g^3\rangle$
$\langle g^7+ug^3c_0,ug^4\rangle,\ \langle g^7+u^2g^3c_0,u^2g^4\rangle$
$\langle g^7+ug^4c_0,ug^5\rangle,\ \langle g^7+u^2g^4c_0,u^2g^5\rangle$
$\langle g^7+ug^5c_0,ug^6\rangle,\ \langle g^7+u^2g^5c_0,u^2g^6\rangle$

Table 5 : Non Free module cyclic codes of length 8 over $R_3 = F_2 + uF_2 + u^2F_2$

Chapter 5

Constacyclic Codes over the Rings $F_2 + uF_2$ and $F_2 + uF_2 + u^2F_2$

In this chapter, we study the structure of $(1+u)-$constacyclic codes of even length n over the ring $F_2 + uF_2, with\ u^2 = 0\ mod\ 2$. We find a set of generators for each $(1+u)$-constacyclic code and its dual. We study the rank of cyclic codes and find their minimal spanning sets. We prove that the Gray image of a $(1+u)$-constacyclic code is a binary cyclic code of length $2n$. We extend these results that was proved in [2] to the ring $F_2 + uF_2 + u^2F_2, with\ u^3 = 0\ mod\ 2$. Examples of $(1+u)$, $(1-u^2)$-constacyclic codes of even lengths are also studied.

5.1 Classification of $(1+u)$, $(1-u^2)$-Constacyclic Codes

Definition 5.1.1. [2] Consider the ring $R = F_2 + uF_2 = \{0, 1, u, u+1\}$, where $u^2 = 0$ mod 2 and $S = F_2 + uF_2 + u^2F_2 = \{0, 1, u, u+1, u^2, 1+u^2, 1+u+u^2, u+u^2\}$, where $u^3 = 0 \mod 2$.

A linear code of length n is a $(1+u)-$constacyclic if it is invariant under the automorphism v which is given by $v(c_0, c_1, \ldots, c_{n-1}) = \big((1+u)c_{n-1}, c_0, \ldots, c_{n-2}\big)$,where $1+u$ is a unit in R.

A linear code of length n is a $(1-u^2)-$constacyclic if it is invariant under the automorphism σ which is given by $\sigma(c_0, c_1, \ldots, c_{n-1}) = \big((1-u^2)c_{n-1}, c_0, \ldots, c_{n-2}\big)$, where $1-u^2$ is a unit in S.

A subset C of R^n is a linear cyclic code if its polynomial representation is an ideal in $M_n = S[x]/\big\langle x^n - 1\big\rangle$.

A subset C of R^n is a linear $(1+u)-$Constacyclic code if its polynomial representation is an ideal in $R_n = S[x]/\big\langle x^n - (1+u)\big\rangle$.

A subset C of S^n is a linear cyclic code if its polynomial representation is an ideal in $T_n = S[x]/\big\langle x^n - 1\big\rangle$.

A subset C of S^n is a linear $(1-u^2)-$Constacyclic code if its polynomial representation is an ideal in $S_n = S[x]/\big\langle x^n - (1-u^2)\big\rangle$.

Definition 5.1.2. [4] Let $S = F_2 + uF_2 + u^2F_2 = \{0, 1, u, 1+u, u^2, 1+u^2, 1+u+u^2, u+u^2\}$ where $u^3 = 0 \mod 2$. We define the Generalized Lee weight of any non zero element t in S by

$$wt_{GL}(t) = \begin{cases} 2, & \text{if } t \neq u^2 \\ 4, & \text{if } t = u^2 \end{cases}$$

and the Generalized Lee weight of 0 is 0.

Further the Generalized Lee weight of any non zero $n-$ tuple in S^n is the sum of Generalized Lee weights of its components.

Example 5.1.1. *If* $n = 8$*, let* $x = (1, 0, u^2, 1+u, 1, u+u^2, u^2, 0) \in S^8$.
$\Rightarrow wt_{GL}(x) = 16$.

Definition 5.1.3. [4] The Generalized Lee distance between x and $y \in R^n$ is defined by $d_{GL}(x, y) = wt_{GL}(x-y)$.

Example 5.1.2. *If* $n = 4$*, let* $x = (0, u, 1+u, u^2)$ *and* $y = (0, 1, u, 0)$ *be two vectors in* S^4
$\Rightarrow d_{GL}(x, y) = wt_{GL}(x-y) = wt_{GL}(0, 1+u, 1, u^2) = 8$.

Notation: We write a for $a(x)$ and $(a)_2$ represents a binary cyclic codes in $F_2[x]$ with generator a.

Following results in [3], let $R = F_2 + uF_2 = \{0, 1, u, 1 + u\}$ with $u^2 = 0$ mod 2, and $S = F_2 + uF_2 + u^2F_2$ with $u^3 = 0$ mod 2. Let C be a constacyclic code in $S_n = S[x]/\langle x^n - (1 - u^2)\rangle$. Define $\Psi_1 : S \to R$ by $\Psi_1(a) = a$. Ψ_1 is a ring homomorphism that can be extended to a homomorphism $\Phi : C \to R_n = R[x]/\langle x^n - (1 + u)\rangle$ defined by $\Phi(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \Psi_1(c_0) + \Psi_1(c_1)x + \ldots + \Psi_1(c_{n-1})x^{n-1}$.
Ker$\Phi = \{u^2r(x) : r(x) \in Z_2[x]\}$. Let $J = \{r(x) : u^2r(x) \in ker\Phi\} \Rightarrow$ J is an ideal in $Z_2[x]/\langle x^n - 1\rangle$ and hence a cyclic code in $Z_2[x]/\langle x^n - 1\rangle$. So $J = \langle a_2(x)\rangle$ and $ker\Phi = \langle u^2a_2(x)\rangle$ with $a_2(x)|(x^n - 1)$ mod 2. In order to determine the generators of a cyclic code in S_n, we need to know the image Φ which is a constacyclic code in R_n. Let D be a constacyclic code in R_n as above, we define $\Psi_2 : R \to Z_2$ by $\Psi_2(a) = a^2 \; mod \; 2$. Ψ_2 is a ring homomorphism because $(a + b)^2 = a^2 + b^2$ in R and in $Z_2 = \{0, 1\}$. Extend Ψ_2 to a homomorphism $\varphi : D \to Z_2[x]/\langle x^n - 1\rangle$ defined by $\varphi(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) = \Psi_2(c_0) + \Psi_2(c_1)x + \ldots + \Psi_2(c_{n-1})x^{n-1} = c_0^2 + c_1^2x + \ldots + c_{n-1}^2x^{n-1}$ mod 2.
$Ker\varphi = \{ur(x) : r(x) \; is \; a \; binary \; polynomial \; in \; Z_2[x]/\langle x^n - 1\rangle\} = \langle ua_1(x)\rangle$ with $a_1(x)|(x^n - 1)$ mod 2. The image of φ is also an ideal and hence a binary cyclic code generated by $g(x)$ with $g(x)|(x^n - 1)$. So, $C = \langle g(x) + up(x), ua_1(x)\rangle$ for some binary polynomial $p(x)$. Note that $a_1|\left(p\frac{x^n-1}{g}\right)$ because $\varphi\left(\frac{x^n-1}{g}[g + up]\right) = \varphi\left(up\frac{x^n-1}{g}\right) = 0$ which implies $\left(up\frac{x^n-1}{g}\right) \in \; ker\varphi = \langle ua_1\rangle$. Also $ug \in \; ker\varphi$ implies $a_1(x)|g(x)$. Now since the image of Φ is an ideal in R_n, then $Im(\Phi) = \langle g(x) + up_1(x) \; , \; ua_1(x)\rangle$ with$a_1(x)|g(x)|\left(x^n - 1\right)$ and $a_1(x)|p_1(x)\left(\frac{x^n-1}{g(x)}\right)$. Also $ker\Phi = \langle u^2a_2(x)\rangle$ with $a_2(x)|\left(x^n - 1\right)$ mod 2. Since $u^2a_1 \; \in \; ker\Phi = \langle u^2a_2\rangle$, then we get the following lemma.

Lemma 5.1.1. [3] *If $C = \langle g(x) + up(x), ua_1(x)\rangle$ is a linear-cyclic code in R_n and $g(x) = a_1(x)$ with $deg\left(g(x)\right) = r$, then $C = \langle g(x) + up(x)\rangle$ and $(g + up)|(x^n - 1)$ in R.*

Proof. Since $u(g + up) = ug$ and$g = a_1$, then $C \subseteq \langle g(x) + up(x)\rangle$,
hence $C = \langle g(x) + up(x)\rangle$. By the division algorithim, $x^n - 1 = \left(g(x) + up(x)q(x)\right) + t(x)$, where $t(x) = 0$ or $deg \; t(x) < r$. Since $t(x) \in \; C$ then $t(x) = 0$ and hence $(g + up)|(x^n - 1)$ in R . □

Lemma 5.1.2. [3] *If* $C = \langle g + up_1 + u^2p_2, ua_1 + u^2q_1, u^2a_2\rangle$ *is a linear-cyclic code in* S_n *and if* $a_2 = g$*, then* $C = \langle g + up_1 + u^2p_2\rangle$ *and* $\big(g + up_1 + u^2p_2\big)|\big(x^n - 1\big)$ *in* S*.*

Proof. Since $a_2 = g$, then $a_1 = a_2 = g$. From Lemma 5.1.1, we get that $(g + up)|(x^n - 1)$ in R and $C = \langle g+up_1+u^2p_2, u^2a_2\rangle$. The rest of the proof is similar to Lemma 5.1.1 . □

Lemma 5.1.3. *Let* C *be a linear-constacyclic code in* $S_n = S[x]/\langle x^n - (1 - u^2\rangle$*, then* C *can be written uniquely as* $C = \big\langle g(x)+up_1(x)+u^2p_2(x), ua_1(x)+u^2q_1(x), u^2a_2(x)\big\rangle$*, where* $a_1(x),\ a_2(x),\ p_1(x),\ p_2(x),\ q_1(x)$ *and* $g(x)$ *are binary polynomials with* $a_2|a_1|g|\langle x^n - 1\rangle$ mod 2, $a_1(x)|p_1(x)\big(\frac{x^n-1}{g(x)}\big)$ *and* a_2 *divides* $q_1(x)\big(\frac{x^n-1}{a_1(x)}\big)$ *and* $p_2(x)\big(\frac{x^n-1}{g(x)}\big)\big(\frac{x^n-1}{a_1(x)}\big)$*. Moreover* $\deg p_2 < \deg a_2,\ \ \deg q_1 < \deg a_2$ *and* $\deg p_1 < \deg a_1$*.*

Proof. Assume that $C = \big\langle g(x) + up_1(x) + u^2p_2(x), ua_1(x) + u^2q_1(x), u^2a_2(x)\big\rangle = \big\langle h(x) + um_1(x) + u^2m_2(x), ub_1(x) + u^2l_1(x), u^2b_2(x)\big\rangle$. Since $ker\Phi = \big\langle u^2a_2(x)\big\rangle = \big\langle u^2b_2(x)\big\rangle$, then $a_2(x) = b_2(x)$ and similarly $ker\varphi = \big\langle ua_1(x)\big\rangle = \big\langle ub_1(x)\big\rangle$ implies $a_1(x) = b_1(x)$.
Also $\varphi\big(\Phi(C)\big) = \big\langle g(x)\big\rangle = \big\langle h(x)\big\rangle$ and hence $g(x) = h(x)$. Since $g+up_1+u^2p_2 \in\ C = \big\langle g+um_1+u^2m_2, ua_1+u^2l_1, u^2a_2\big\rangle$, then $g+up_1+u^2p_2 = g+um_1+u^2m_2+(ua_1+u^2l_1)\alpha_1+u^2a_2\alpha_2$ ……………………… (1).
Multiplying by u we get $u^2(p_1 - m_1) = u^2a_1\alpha_1$. Since $deg(p_1 - m_1) < deg(p_1)$, then $p_1 = m_1$. So equation (1) becomes $u^2p_2 = u^2m_2+(ua_1+u^2l_1)\alpha_1+u^2a_2\alpha_2$ and $u^2(p_2-m_2) = (ua_1 + u^2l_1)\alpha_1 + u^2a_2\alpha_2$. So $u^2(p_2 - m_2) \in\ C$ and hence $\in\ ker\Phi = \big\langle u^2a_2(x)\big\rangle$.
But again $deg(p_2 - m_2) < deg\big(a_2(x)\big)$. Thus $p_2 = m_2$. Similarly, we can show that $q_1 = l_1$ and hence we are done. □

Remark 5.1.1. The above generators $a_1(x)$, $a_2(x)$ and $g(x)$ of C are divisors of $(x^n - 1)mod\ 2$ and they are not divisors of $\big(x^n - (1 - u^2)\big)$, so for this fact makes the study of $(1 - u^2)-$constacyclic codes easier to understand.

Lemma 5.1.4. [2] $\big(x + (1 + u)\big)^{2L} = \big(x + 1\big)^{2L}$ *for any integer* L*.*

Proof.
$$\begin{aligned}\big(x + (1 + u)\big)^{2L} &= \Big[\big(x + (1 + u)\big)^2\Big]^L \\ &= \big[x^2 + (1 + u)^2\big]^L\end{aligned}$$

$$= \left(x^2 + 1 + u^2 + 2u\right)^L$$
$$= \left(x^2 + 1\right)^L = \left[(x+1)^2\right]^L = \left(x+1\right)^{2L}. \qquad \square$$

Lemma 5.1.5. *$\left(x + (1-u^2)\right)^{2L} = \left(x+1\right)^{2L}$ for any integer L.*

Proof.
$$\left(x + (1-u^2)\right)^{2L} = \left[\left(x + (1-u^2)\right)^2\right]^L$$
$$= \left[x^2 + (1-u^2)^2 + 2x(1-u^2)\right]^L$$
$$= \left(x^2 + 1 + u^4 - 2u^2\right)^L$$
$$= \left(x^2 + 1 + uu^3\right)^L$$
$$= \left(x^2 + 1\right)^L = \left[(x+1)^2\right]^L = \left(x+1\right)^{2L}. \qquad \square$$

Lemma 5.1.6. [2] *Let $n = 2^e m$ where $\gcd(2,m) = 1$. Then u belongs to both ideals $\langle x^m + 1\rangle$ and $\left\langle \left(x+1\right)^{2^e}\right\rangle$ in R_n.*

Proof. In the ring $R_n = R[x]/\langle x^n - (1+u)\rangle$, we have $x^n - (1+u)$ is the zero element, so $u = x^n + 1 = x^{2^e m} + 1 = \left(x^m + 1\right)^{2^e} = \left[\left(x+1\right)f(x)\right]^{2^e}$,
$\big($ since $x^m + 1 = \left(x+1\right)f(x)$ for some $f(x) \in \ f_2(x)\big)$
so $u = \left(x+1\right)^{2^e}\left[f(x)\right]^{2^e} = \left(x^{2^e} + 1\right)\left[f(x)\right]^{2^e}$.
Therefore u belongs to both ideals $\langle x^m + 1\rangle$ and $\left\langle \left(x+1\right)^{2^e}\right\rangle$ in R_n. $\square$

Lemma 5.1.7. *Let $n = 2^e m$ where $\gcd(2,m) = 1$. Then u^2 belongs to both ideals $\big((x^m + 1)\big)$ and $\big((x+1)^{2^e}\big)$ in S_n.*

Proof. Similar to the proof of Lemma 5.1.6 $\square$

Lemma 5.1.8. [2] *If $n = 2^e$, then $\big(1 + (x+1)^i p\big)$ is a unit in R_n and in S_n for any polynomial p and $e > 0$.*

Proof. Let $k = 2n$, then $\left[1 + (x+1)^i p\right]^k = 1 + \left(x+1\right)^{ik} p^k = 1 + \left(x+1\right)^{2ni} p^k = 1.$ $\square$

Theorem 5.1.9. [2] *Let $C = \langle g(x) + up(x), ua_1(x)\rangle$ be a $\big(1+u\big)-$constacyclic code in R_n for $n = 2^e$. Then $C = \langle d(x+1)^i\rangle$, where $d = 1$ or u and $i < n$.*

Proof. If $g(x) + up(x) = 0,$ then

$$C = \langle ua_1(x)\rangle \text{ with } a_1(x) | \left(x^n - 1\right).$$

Hence $a_1(x) = (x-1)^i,\ i < n$ and $C = \big\langle u(x+1)^i \big\rangle$. If $g(x) + up(x) \neq 0$, then

$$\begin{aligned} g(x) + up(x) &= (x+1)^i + (x+1)^n p(x) \\ &= (x+1)^i \big[1 + (x+1)^{n-i} p(x)\big] \\ &= (x+1)v \text{ for some unit } v. \end{aligned}$$

Hence we may assume that $C = \big\langle (x+1)^i, u(x+1)^j \big\rangle$. Since $u = (x+1)^n$, then $u(x+1)^j \in \big\langle (x+1)^i \big\rangle$. Therefor $C = \big\langle (x+1)^i \big\rangle$. □

Theorem 5.1.10. *Let $C = \big\langle g(x) + up_1(x) + u^2 p_2(x), u^2 a_2(x) \big\rangle$ be a $\big(1-u^2\big)-$constacyclic code in S_n for $n = 2^e$. Then $C = \big\langle d(x+1)^i \big\rangle$ where $d = 1$ or u^2 and $i < \frac{n}{2}$.*

Proof. If $g(x) + up_1(x) + u^2 p_1(x) + u^2 p_2(x) = 0$, then

$$C = \big\langle u^2 a_2(x) \big\rangle \text{ with } a(x) | \big(x^n - 1\big).$$

Hence $a_2(x) = (x-1)^i,\ i < n$ and $C = \big\langle u^2(x+1)^i \big\rangle$. If $g(x) + up_1(x) + u^2 p_2(x) \neq 0$, then

$$\begin{aligned} g(x) + up_1(x) + u^2 p_2(x) &= (x+1)^i + (x+1)^{\frac{n}{2}} p_1(x) + (x+1)^n p_2(x) \\ &= (x+1)^i \big[1 + (x+1)^{\frac{n}{2}-i} p_1(x) + (x+1)^{n-i} p_2(x)\big] \\ &= (x+1)^i \big[1 + (x+1)^{\frac{n}{2}-i} \big(p_1(x) + (x+1)^{\frac{n}{2}} p_2(x)\big)\big] \\ &= (x+1)v \text{ for some unit } v. \end{aligned}$$

Hence we may assume that $C = \big\langle (x+1)^i, u^2(x+1)^j \big\rangle$. Since $u^2 = (x+1)^n$, then $u^2(x+1)^j \in \big\langle (x+1)^i \big\rangle$. Therefor $C = \big\langle (x+1)^i \big\rangle$. □

Theorem 5.1.11. [2] *Let $C = \big\langle g(x) + up(x), ua_1(x) \big\rangle$ be a $\big(1+u\big)-$constacyclic code in R_n for $n = 2^e m$ and $\gcd(2, m) = 1$. If $p(x) = 0$, then $C = \big\langle g(x) \big\rangle$ or $\big\langle ug(x) \big\rangle$.*

Proof. Let $C = \big\langle g(x) + up(x), ua_1(x) \big\rangle$ be a $(1+u)-$constacyclic code in R_n. Assume that $p(x) = 0$, then $C = \big\langle g(x), ua_1(x) \big\rangle$, where $ua_1(x) = (x^n - 1)a_1(x)$.
Since $g(x) | \big\langle x^n - 1 \big\rangle$, then $ua_1(x) \in \big\langle g(x) \big\rangle$. Hence $C = \big\langle g(x) \big\rangle$ or $\big\langle ug(x) \big\rangle$. □

Theorem 5.1.12. *Let $C = \big\langle g(x) + up_1(x) + u^2 p_2(x), u^2 a_2(x) \big\rangle$ be a $\big(1-u^2\big)-$constacyclic code in S_n for $n = 2^e m$ and $\gcd(2, m) = 1$. If $p_1(x) = p_2(x) = 0$, then $C = \big\langle g(x) \big\rangle$ or $\big\langle u^2 g(x) \big\rangle$.*

Proof. Let $C = \langle g(x) + up_1(x) + u^2p_2(x), u^2a_2(x)\rangle$ be a $(1-u^2)-$constacyclic code in S_n. Assume that $p_1(x) = p_2(x) = 0,$ then $C = \langle g(x), u^2g(x)\rangle,$ where $u^2a_2(x) = (x^n - 1)a_2(x)$. Since $g(x)|\langle x^n-1\rangle$, then $u^2a_2(x) \in \langle g(x)\rangle$. Hence $C = \langle g(x)\rangle$ or $\langle u^2g(x)\rangle$. □

Lemma 5.1.13. [2] *Suppose that* $C = \langle f^k\rangle$ *is a* $(1+u)-$*constacyclic code in* R_n *for* $n = 2^e m$, $\gcd(2,m) = 1$ *and* $f|(x^m-1)$. *Then we may assume that* $k \leq 2^{e+1}$.

Proof. Since $g.c.d.\left(\frac{x^n-1}{f^{2^e}}, f^{2^e}\right) = 1$, then
$s_1(x^n-1)f^{2^e} + s_2f^{2^e} = 1,$
$s_1(x^n-1) + s_2f^{2^{e+1}} = f^{2^e},$
$s_1u + s_2f^{2^{e+1}} = f^{2^e}$. (squaring both sides),
$s_2^2f^{2^{e+2}} = f^{2^{e+1}}$.
This implies $\langle f^{2^{e+2}}\rangle = (f^{2^{e+1}})$ and hence
$\langle f^{2^{e+1}}\rangle = (f^k)$ if $2^{e+2} \leq\ k\ \leq 2^{e+1}$.
If $k = 2^{e+2} + t$, then
$\langle f^k\rangle = \langle f^{2^{e+2}+t}\rangle = \langle f^{2^{e+1}+t}\rangle = \langle f^{2^{e+1}}\rangle$. □

Lemma 5.1.14. *Suppose that* $C = \langle f^k\rangle$ *is a* $(1-u^2)-$*constacyclic code in* S_n *for* $n = 2^e m$, $\gcd(2,m) = 1$ *and* $f|(x^m-1)$. *Then we may assume that* $k \leq 2^{e+1}$.

Proof. Since $\left(\frac{x^n-1}{f^{2^e}}, f^{2^e}\right) = 1$, then
$s_1(x^n-1)f^{2^e} + s_2f^{2^e} = 1,$
$s_1(x^n-1) + s_2f^{2^{e+1}} = f^{2^e},$
$s_1u^2 + s_2f^{2^{e+1}} = f^{2^e}$. (squaring both sides),
$s_2^2f^{2^{e+2}} = f^{2^{e+1}}$.
This implies $\langle f^{2^{e+2}}\rangle = (f^{2^{e+1}})$ and hence
$\langle f^{2^{e+1}}\rangle = (f^k)$ if $2^{e+2} \leq\ k\ \leq 2^{e+1}$.
If $k = 2^{e+2} + t$, then
$\langle f^k\rangle = \langle f^{2^{e+2}+t}\rangle = \langle f^{2^{e+1}+t}\rangle = \langle f^{2^{e+1}}\rangle$. □

Lemma 5.1.15. [2] *Suppose* $C = \langle f^i, ug^k\rangle$ *is a* $(1+u)-$*constacyclic code in* R_n *for* $n = 2^e m$, *where* $e > 0$, f *and* g *divides* (x^m+1) *and* $\gcd(2,m) = 1$, *then* $C = \langle h\rangle$, *where* $h = \gcd(f^i, (x^n+1)g^k)$.

Proof. First, note that $u = x^n + 1$ in R_n. Also note that f^i and $(x^n+1)g^k$ are polynomials in $Z_2[x]$ and hence $h = \gcd(f^i, (x^n+1)g^k)$ exists. Second, let $h = \gcd(f^i, (x^n+1)g^k)$ which implies $h|f^i$ and $h|(x^n+1)g^k$, then f^i and $(x^n+1)g^k \in \langle h \rangle$. Hence $C \subseteq \langle h \rangle$.
On the other hand $h = \alpha f^i + \beta(x^n+1)g^k$ (properties of gcd) for some $\alpha, \beta \in \ R[x]$.
$\Rightarrow \ h \in C \ \Rightarrow \langle h \rangle \subseteq C$.
Therefor, $C = \langle h \rangle$. □

Lemma 5.1.16. *Suppose $C = \langle f^i, u^2 g^k \rangle$ is a $(1-u^2)-$constacyclic code in S_n for $n = 2^e m$, where $e > 0$, f and g divides (x^m+1) and $\gcd(2,m) = 1$, then $C = \langle h \rangle$, where $h = \gcd(f^i, (x^n+1)g^k)$.*

Proof. First, note that $u^2 = x^n + 1$ in S_n. Also note that f^i and $(x^n+1)g^k$ are polynomials in $Z_2[x]$ and hence $h = \gcd(f^i, (x^n+1)g^k)$ exists. Second, let $h = \gcd(f^i, (x^n+1)g^k)$ which implies $h|f^i$ and $h|(x^n+1)g^k$, then f^i and $(x^n+1)g^k \in \langle h \rangle$. Hence $C \subseteq \langle h \rangle$.
On the other hand $h = \alpha f^i + \beta(x^n+1)g^k$ (properties of gcd) for some $\alpha, \beta \in \ S[x]$
$\Rightarrow \ h \in C \ \Rightarrow \langle h \rangle \subseteq C$.
Therefor, $C = \langle h \rangle$. □

Theorem 5.1.17. [2] *Let $C = \langle g(x) + up(x), ua_1(x) \rangle$ be a $(1+u)-$constacyclic code in R_n for $n = 2^e m$ and $\gcd(2,m) = 1$. Suppose $p(x) \neq 0$, then $C = \langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle$, where $f_1, f_2, \dots, f_r$ are the monic binary divisors of $(x^m - 1) \mod 2$, and $i_1, i_2, \dots, i_r \leq 2^{e+1}$.*

Proof. Suppose $p \neq 0$. Consider

$$\begin{aligned}
&\Phi\left[\left(\tfrac{x^n-1}{g(x)}\right)\left(g(x) + up(x)\right)\right] \\
&\quad = \Phi\left[(x^n - 1) + u\tfrac{x^n-1}{g(x)}p(x)\right] \\
&\quad = \Phi\left[u + u\tfrac{x^n-1}{g(x)}p(x)\right] \\
&\quad = \Phi\left[u\left(1 + \tfrac{x^n-1}{g(x)}p(x)\right)\right] = 0
\end{aligned}$$

Hence $u\left(1 + \frac{x^n-1}{g(x)}p(x)\right) \in \ ker\Phi = \langle ua_1(x) \rangle$.
So $1 + \frac{x^n-1}{g(x)}p(x) = a_1(x)k(x)$,
$g(x) + \left(x^n - 1\right)p(x) = g(x)a_1(x)k(x)$.
$\Rightarrow g(x) + up(x) = g(x)a1(x)k(x) \ \left(Since\ u = x^n - 1\right)$ in R.

Hence $C = \langle g(x)a_1(x)k(x), ua_1(x)\rangle$. But $1 + \frac{x^n-1}{g(x)}p(x) = a_1(x)k(x)$.
$\Rightarrow 1 = \frac{x^n-1}{g(x)}p(x) + a_1(x)k(x)$.
$\Rightarrow g(x)a_1(x) = ua_1(x)p(x) + g(x){a_1}^2(x)k(x)$.
This implies that $g(x)a_1(x) \in\ C$and $C = \langle g(x)a_1(x), ua_1(x)\rangle$.
So we may assume that $C = \langle g_1^{l_1}(x)g_2^{l_2}(x)\ldots\ g_r^{l_r}(x), ua_1(x)\rangle$, where $g_i(x)|\big(x^n-1\big)$. Since $\big(x^n-1\big) = \big(x^m-1\big)^{2^e}$, then each $g_i(x) = f_i^{l_i}(x)$, where f_i is a monic divisor of x^m+1 mod 2 and $l_i \leq 2^e$.
So $C = \langle f_1^{m_1}f_2^{m_2}\ldots\ f_r^{m_r}, uf_t^{l_t}\rangle$, where $\{f_i\}$ are monic coprime divisors of $\big(x^m+1\big)$ mod 2. By Lemma 5.1.15, we get that $C = \langle f_1^{i_1}f_2^{i_2}\ldots f_r^{i_r}\rangle$, where $f_s|\big(x^m-1\big)$ mod 2 and $i_1, i_2, \ldots\ i_r \leq 2^{e+1}$. □

Theorem 5.1.18. *Let $C = \langle g(x)+up_1(x)+u^2p_2(x), u^2a_2(x)\rangle$ be a $(1-u^2)-$constacyclic code in S_n for $n = 2^em$ and $\gcd(2, m) = 1$. Suppose $p_1(x)$ and $p_2(x) \neq 0$, then $C = \langle f_1^{i_1}f_2^{i_2}\ldots f_r^{i_r}\rangle$, where $f_1, f_2, \ldots, f_r$ are the monic binary divisors of (x^m-1) mod 2 and $i_1, i_2, \ldots, i_r \leq 2^{e+1}$.*

Proof. Suppose $p_1(x),\ p_2(x) \neq 0$. Concider

$$\begin{aligned}
&\Phi\big[\big(\tfrac{x^n-1}{g(x)}\big)\big(g(x)+up_1(x)+u^2p_2(x)\big)\big]\\
&\quad = \Phi\big[x^n-1+u\tfrac{x^n-1}{g(x)}p_1(x)+u^2\tfrac{x^n-1}{g(x)}p_2(x)\big]\\
&\quad = \Phi\big[u^2+u\tfrac{x^n-1}{g(x)}p_1(x)+u^2\tfrac{x^n-1}{g(x)}p_2(x)\big]\\
&\quad = \Phi\big[u\big(u+\tfrac{x^n-1}{g(x)}p_1(x)+u\tfrac{x^n-1}{g(x)}p_2(x)\big)\big] = 0.
\end{aligned}$$

Hence $u\big(u+\frac{x^n-1}{g(x)}p_1(x)+u\frac{x^n-1}{g(x)}p_2(x)\big) \in\ ker\Phi = \langle u^2a_2(x)\rangle$.
So $u+\frac{x^n-1}{g(x)}p_1(x)+u\frac{x^n-1}{g(x)}p_2(x) = a_2(x)k(x)$,
$ug(x)+\big(x^n-1\big)p_1(x)+u\big(x^n-1\big)p_2(x) = g(x)a_2(x)k(x)$.
$\Rightarrow ug(x)+u^2p_1(x) = g(x)a_2(x)k(x)\ \big(Since\ u^2 = x^n-1\ \Rightarrow\ u(x^n-1) = 0\big)$.
Hence $C = \langle g(x)a_2(x)k(x), u^2a_2(x)\rangle$. But $u+\frac{x^n-1}{g(x)}p_1(x)+u\frac{x^n-1}{g(x)}p_2(x) = a_2(x)k(x)$.
$\Rightarrow u = \frac{x^n-1}{g(x)}p_1(x)+u\frac{x^n-1}{g(x)}p_2(x)+a_2(x)k(x)$.
$\Rightarrow ug(x)a_2(x) = u^2a_2(x)p_1(x)+g(x){a_2}^2(x)k(x)$.
This implies that $g(x)a_2(x) \in\ C$ and $C = \langle g(x)a_2(x), u^2a_2(x)\rangle$.
So we may assume that $C = \langle g_1^{l_1}(x)g_2^{l_2}(x)\ldots\ g_r^{l_r}(x), u^2a_2(x)\rangle$, where $g_i(x)|\big(x^n-1\big)$. Since

$\big(x^n - 1\big) = \big(x^m - 1\big)^{2^e}$, then each $g_i(x) = f_i^{l_i}(x)$, where f_i is a monic divisor of $x^m + 1$ mod 2 and $l_i \leq 2^e$.

So $C = \big\langle f_1^{m_1} f_2^{m_2} \dots\ f_r^{m_r}, u^2 f_t^{l_t} \big\rangle$, where $\big\{f_i\big\}$ are monic coprime divisors of $\big(x^m + 1\big)$ mod 2. By lemma 5.1.16, we get that $C = \big\langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \big\rangle$, where $f_s \big| \big(x^m - 1\big)$ mod 2 and $i_1, i_2, \dots\ i_r \leq 2^{e+1}$. □

5.2 The Dual and the Minimal Spanning Sets of $(1+u)$, $(1-u^2)$-Constacyclic Codes

Lemma 5.2.1. [2] *Let $C = \big\langle g \big\rangle$ be a $(1+u)-$constacyclic code of length $n = 2^e m$ and $\gcd(2, m) = 1$ in R_n, where $g \big| \big(x^n - 1\big)$ mod 2 and $\deg\ g = r$. Then C has a minimal spanning set over R given by*

$$\beta = \{g, xg, \dots, x^{n-r-1}g, u, xu, \dots, x^{r-1}u\},$$

and $\big|C\big| = 4^{n-r}2^r$.

Proof. Since $u = x^n - 1$ in R_n, and $g \big| \big(x^n - 1\big)$ in R_n, then $u \in\ C$.

The rest of the proof is similar to the proof of Theorem 4.2.1 in the previous chapter. □

Lemma 5.2.2. *Let $C = \big\langle g \big\rangle$ be a $(1 - u^2)-$constacyclic code of length $n = 2^e m$ and $\gcd(2, m) = 1$ in S_n, where $g \big| \big(x^n - 1\big)$ mod 2 and $\deg\ g = r$. Then C has a minimal spanning set over S given by*

$$\beta = \{g, xg, \dots, x^{n-r-1}g, u, xu, \dots, x^{r-1}u, u^2, xu^2, \dots, x^{r-1}u^2\},$$

and $|C| = 8^{n-r}4^r 2^r$.

Proof. Since $u^2 = x^n - 1$ in S_n, and $g \big| \big(x^n - 1\big)$ in S_n, then $u^2 \in\ C$.

Let $g(x) = 1 + g_1(x) + \dots\ x^r$ and $gc_0 + xgc_1 + \dots + x^{n-r-1}gc_{n-r-1} = 0 \Rightarrow\ c_i = 0$ for every $i = 0, 1, \dots\ , n - r - 1$.

Now, we show that β spans

$$\gamma = \{g, xg, \ldots, x^{n-r-1}g, u, xu, \ldots, x^{n-1}u, u^2, xu^2, \ldots, x^{n-1}u^2\}.$$

So we only show that $u^i x^r \in \ span(\gamma)$, for $i = 1, 2$.

$u^i x^r = u^i g(x) + u^i m(x)$ where $m(x)$ is a polynomial in C of degree less than r, since any polynomial in C must have degree greater or equal to zero, then $0 \leq \ deg\ m(x) < \ r$. Hence $u^i m(x) = \alpha_0 u^i + \alpha_1 x u^i + \ldots + \alpha_{r-1} x^{r-1} u^i$. Hence β is a generating set.

By comparing coefficient as above, we have that non of the elements in β is a linear combination of the others. Therefore β is a minimal generating set for C and $|C| = 8^{n-r}4^r2^r$. $\square$

Lemma 5.2.3. [2] *Let $C = \langle ug \rangle$ be a $(1+u)-$constacyclic code of length $n = 2^e m$ and* $\gcd(2, m) = 1$ *in R_n, where $g|(x^n - 1)$ mod 2 and* $\deg\ g = r$. *Then C has a minimal spanning set over R given by*

$$\beta = \{ug, uxg, \ldots, ux^{n-r-1}g\},$$

and $|C| = 2^{n-r}$.

Proof. Since the binary code generated by $g(x)$ has basis $\{g, xg, \ldots, x^{n-r-1}g\}$, then the code $C = \langle ug \rangle$ has a minimal spanning set $\beta = \{ug, uxg, \ldots, ux^{n-r-1}g\}$, and hence $|C| = 2^{n-r}$. $\square$

Lemma 5.2.4. *Let $C = \langle ug \rangle$ be a $(1-u^2)-$constacyclic code of length $n = 2^e m$ and* $\gcd(2, m) = 1$ *in S_n, where $g|(x^n - 1)$ mod 2 and* $\deg\ g = r$. *Then C has a minimal spanning set over S given by*

$$\beta = \{ug, uxg, \ldots, ux^{n-r-1}g, u^2g, u^2xg, \ldots, u^2x^{r-1}g\},$$

and $|C| = 4^{n-r}2^r$.

Proof. Since the binary code generated by $g(x)$ has basis $\{g, xg, \ldots, x^{n-r-1}g, ug, uxg, \ldots, ux^{r-1}g\}$, then the code $C = \langle ug \rangle$ has a minimal spanning set $\beta = \{ug, uxg, \ldots, ux^{n-r-1}g, u^2g, u^2xg, \ldots, u^2x^{r-1}g\}$, and hence $|C| = 4^{n-r}2^r$. $\square$

Lemma 5.2.5. *Let $C = \langle u^2 g \rangle$ be a $(1-u^2)-$constacyclic code of length $n = 2^e m$ and $\gcd(2, m) = 1$ in S_n, where $g|(x^n - 1)$ mod 2 and $\deg\ g = r$. Then C has a minimal spanning set over S given by*

$$\beta = \{u^2g, u^2xg, \ldots, u^2x^{n-r-1}g\}.$$

and $|C| = 2^{n-r}$.

Proof. Since the binary code generated by $g(x)$ has basis $\{g, xg, \ldots, x^{n-r-1}g\}$, then the code $C = \langle u^2g \rangle$ has a minimal spanning set $\beta = \{u^2g, u^2xg, \ldots, u^2x^{n-r-1}g\}$. $\square$

Lemma 5.2.6. [2] *Let $C = \langle f_1^{i_1} f_2^{i_2} \ldots f_r^{i_r} \rangle$ be a $(1+u)-$constacyclic code of length $n = 2^e m$ and $\gcd(2, m) = 1$ in R_n. Suppose for some i_j we have $2^e < i_j \leq 2^{e+1}$. Let $C = \langle fg \rangle$, where g is a polynomial of largest degree such that $\deg g = r$, $\deg f = t$ and $f|g|\langle x^n - 1 \rangle \mod 2$. Then C has a minimal spanning set over R spanned by*

$$\beta = \{fg, xfg, \ldots, x^{n-r-1}fg, uf, xuf, \ldots, x^{r-t-1}uf\}$$

and $|C| = 4^{n-r}2^{r-t}$.

Proof. Since $C = \langle fg \rangle$ and $f|g|(x^n - 1)$ mod 2, then the lowest degree polynomial in C is uf. Let $c(x) \in C$, then $c(x) = fgh$, for some polynomial $h \in R_n$. Applying the division algorithm, we get $h = \frac{x^n-1}{g}q + d$, where $deg\ q \leq r - 1$, and $d = 0$ or $deg\ d < n - r - 1$. This implies that $fgh = fg\left(\frac{x^n-1}{g}q + d\right) = fuq + fgd$. Note that $fgd \in span(\beta)$. If $deg\ q \leq r - t - 1$, then $fuq \in span(\beta)$ and hence $c(x) = fgh \in span(\beta)$. If $deg\ q > r - t$, then $r < deg(fuq) \leq r + t - 1 < n + t - 1 = deg(x^{n-r-1}fg)$.
Hence $fuq \in span(\beta)$. Therefore β spans C. From the construction of C, we have β is a minimal spanning set and hence $|C| = 4^{n-r}2^{r-t}$. $\square$

Lemma 5.2.7. *Let $C = \langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle$ be a $(1-u^2)-$constacyclic code of length $n = 2^e m$ and* $\gcd(2, m) = 1$ *in S_n. Suppose for some i_j we have $2^e < i_j \leq 2^{e+1}$. Let $C = \langle fg \rangle$ where g is a polynomial of largest degree such that* $\deg g = r$, $\deg f = t$ *and* $f|g|(x^n - 1) \mod 2$. *Then C has a minimal spanning set over S spanned by*

$$\beta = \{fg, xfg, \dots, x^{n-r-1}fg, uf, xuf, \dots, x^{r-t-1}uf, u^2 f, xu^2 f, \dots, x^{r-t-1}u^2 f\}.$$

and $|C| = 8^{n-r} 4^{r-t} 2^{r-t}$.

Proof. Since $C = \langle fg \rangle$ and $f|g|\big(x^n - 1\big) \mod 2$, then the lowest degree polynomial in C is $u^2 f$. Let $c(x) \in C$, then $c(x) = fgh$, for some polynomial $h \in S_n$. Applying the division algorithm, we get $h = \frac{x^n-1}{g}q + d$, where $deg\ q \leq r - 1$, and $d = 0$ or $deg\ d < n - r - 1$. This implies that $fgh = fg\big(\frac{x^n-1}{g}q + d\big) = fu^2 q + fgd$.
Note that $fgd \in span\big(\beta\big)$. If $deg\ q \leq r - t - 1$, then $fu^2 q \in span\big(\beta\big)$ and hence $c(x) = fgh \in span\big(\beta\big)$. If $deg\ q > r - t$, then $r < deg\big(fu^2 q\big) \leq r + t - 1 < n + t - 1 = deg\big(x^{n-r-1} fg\big)$.
Hence $fu^2 q \in span\big(\beta\big)$. Therefore β spans C. From the construction of C, we have β is a minimal spanning set and hence$|C| = 8^{n-r} 4^{r-t} 2^{r-t}$. □

Theorem 5.2.8. [2]

Let C be be a $(1 + u)-$constacyclic code in R_n, where $n = 2^e m$,
$\gcd(2, m) = 1$.

(1) If $C = \langle g(x) \rangle$, then
$A(C) = \big(u\frac{x^n-1}{g}\big)$ *and* $C^{\perp} = \big(u(\frac{x^n-1}{g})^*\big)$.

(2) If $C = \langle ug(x) \rangle$, then
$A(C) = \big(\frac{x^n-1}{g}\big)$ *and* $C^{\perp} = \big((\frac{x^n-1}{g})^*\big)$.

(3) If $C = \langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle$ then for some i_j and $2^e < i_j \leq 2^{e+1}$, then
$A(C) = \big(f_1^{2^{e+1}-i_1} f_2^{2^{e+1}-i_2} \dots f_r^{2^{e+1}-i_r}\big)$ *and*
$C^{\perp} = \Big(\big(f_1^{2^{e+1}-i_1}\big)^*, \big(f_2^{2^{e+1}-i_2}\big)^*, \dots, \big(f_r^{2^{e+1}-i_r}\big)^*\Big)$.

Proof. (1) Since $C = \langle g(x) \rangle$, then from Lemma 5.2.1 $\left(u\frac{x^n-1}{g}\right) \subseteq A(C)$ and $\left|\left(u\frac{x^n-1}{g}\right)\right| = 4^{n-deg\left(u\frac{x^n-1}{g}\right)}$, but $|C||C^\perp| = 4^n$, hence $C^\perp = \left(u(\frac{x^n-1}{g})^*\right)$.

(2) Similarly it follows directly from Lemma 5.2.3 .

(3) Similarly it follows directly from Lemma 5.2.6 .

$\square$

Theorem 5.2.9. *Let C be be a $(1-u^2)-$constacyclic code in S_n where $n = 2^e m$,* $\gcd(2, m) = 1$.

(1) If $C = \langle g(x) \rangle$, then
$A(C) = \left(u^2\frac{x^n-1}{g}\right)$ *and* $C^\perp = \left(u^2(\frac{x^n-1}{g})^*\right)$.

(2) If $C = \langle ug(x) \rangle$, then
$A(C) = \left(u\frac{x^n-1}{g}\right)$ *and* $C^\perp = \left(u(\frac{x^n-1}{g})^*\right)$.

(3) If $C = \langle u^2 g(x) \rangle$,then
$A(C) = \left(\frac{x^n-1}{g}\right)$ *and* $C^\perp = \left((\frac{x^n-1}{g})^*\right)$.

(4) If $C = \langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle$ where for some i_j and $2^e < i_j \leq 2^{e+1}$, then
$A(C) = \left(f_1^{2^{e+1}-i_1} f_2^{2^{e+1}-i_2} \dots f_r^{2^{e+1}-i_r}\right)$ *and*
$C^\perp = \left(\left(f_1^{2^{e+1}-i_1}\right)^*, \left(f_2^{2^{e+1}-i_2}\right)^*, \dots, \left(f_r^{2^{e+1}-i_r}\right)^*\right)$.

Proof. (1) Since $C = \langle g(x) \rangle$, then from Lemma 5.2.2 $\left(u^2\frac{x^n-1}{g}\right) \subseteq A(C)$ and $\left|\left(u^2\frac{x^n-1}{g}\right)\right| = 8^{n-deg\left(u^2\frac{x^n-1}{g}\right)}$, but $|C||C^\perp| = 8^n$, hence $C^\perp = \left(u^2(\frac{x^n-1}{g})^*\right)$.

(2) Since $C = \langle ug(x) \rangle$, then from Lemma 5.2.4 $\left(u\frac{x^n-1}{g}\right) \subseteq A(C)$ and $|C| = 4^{n-r}2^r$, but $|C||C^\perp| = 8^n$, hence $C^\perp = \left(u(\frac{x^n-1}{g})^*\right)$.

(3) Similarly it follows directly from Lemma 5.2.5 .

(4) Similarly it follows directly from Lemma 5.2.7 .

$\square$

5.3 The Gray Map and $(1+u)$, $(1-u^2)$-constacyclic Codes

An element $z \in S$ can expressed uniquely as

$$z = a + ur + u^2 q, \text{ where } a, r, q \in Z_2.$$

Following [4]; The Generalized Gray map $\psi : S^n \to Z_2^{4n}$ is defined by $\psi(z_1, z_2, \ldots, z_n) = \big(q_1, q_2, \ldots, q_n, q_1 \oplus a_1, q_2 \oplus a_2, \ldots, q_n \oplus a_n, q_1 \oplus r_1, q_2 \oplus r_2, \ldots, q_n \oplus r_n, q_1 \oplus r_1 \oplus a_1, q_2 \oplus r_2 \oplus a_2, \ldots, q_n \oplus r_n \oplus a_n\big)$, where $\oplus$ is componentwise addition in Z_2 and $z_i = a_i + ur_i + u^2 q_i, \quad 1 \leq i \leq n$.

ψ is an isometry from (S^n, Generalized Lee distance) to (Z_2^{4n}, Hamming distance). The polynomial representation of the Generalized Gray map was given in the following way: Every polynomial $z(x) \in S[x]$ of degree less than n can be expressed as $z(x) = b(x) + ut(x) + u^2 m(x)$, where $b(x)$, $t(x)$, and $m(x) \in Z_2[x]$ are polynomials of degree less than n. Recall that $S_n = S[x]/\big\langle x^n - (1-u^2)\big\rangle$.

Define the map $\psi_p : S_n \to Z_2[x]/\big\langle x^{4n} + 1\big\rangle$ by

$$\psi_p(z(x)) = b(x)x^n + t(x)(x^n + 1) + m(x)(x^{2n} + 1).$$

ψ_p is the polynomial representation of ψ where $\psi : S \to Z_2^4$ defined by

$$\psi(a + ur + u^2 q) = (q, q \oplus a, q \oplus r, q \oplus a \oplus r).$$

Similarly, as above an element $z \in R = F_2 + uF_2$ can be expressed as $z = r + uq$ where r and q are in $F_2 = \big\{0, 1\big\}$. The Gray map $\Psi : R \to F_2^2$ is defined by $\Psi\big(r + uq\big) = \big(q, q \oplus r\big)$. This map can be extended to $\psi : R^n \to F_2^{2n}$ defined by

$$\psi(z_1, z_2, \ldots\ z_n) = (q_1, q_2, \ldots\ q_n, q_1 \oplus r_1, q_2 \oplus r_2, \ldots, q_n \oplus r_n),$$

where $z = (z_1, z_2, \ldots, z_n)$, $z_i = r_i + uq_i$, $1 \leq\ i \leq\ n$, and $\oplus$ is a binary addition.

Example:-

$\Psi(1) = 01 \qquad q = 0\ ,\ r = 1$

$\Psi(0) = 00 \qquad q = 0\ ,\ r = 0$

$\Psi(u) = 11 \qquad q = 1\ ,\ r = 0$

$\Psi(1+u) = 01 \qquad q = 1\ ,\ r = 1.$

It well known that ψ is an isometry from (R^n, Lee distance) to (Z_2^{2n}, Hamming distance).

The polynomial representation of the Gray map was given in the following way:

Every polynomial $z(x) \in R[x]$ of degree less than n can be expressed as $z(x) = a(x) + ub(x)$, where $a(x),\ b(x) \in Z_2[x]$, are polynomials of degree less than n. Recall that $R_n = S[x]/\langle x^n - (1+u)\rangle$.

Define the map $\psi_p : R_n \to Z_2[x]/\langle x^{2n}+1\rangle$ by

$$\psi_p(z(x)) = a(x)x^n + b(x)(x^n+1).$$

ψ_p is the polynomial representation of ψ.

Lemma 5.3.1. [2] *Let $C = \langle g\rangle$ be a $(1+u)-$constacyclic code in R_n, where $g|(x^n-1)$* mod 2.

Then $\psi_p(C) = \langle g\rangle_2$ is a cyclic code of $Z_2^{2n}[x]$.

Proof. Let $C = \langle g\rangle$ be any $(1+u)-$constacyclic code in R_n where $g|(x^n-1) \mod 2$. From the definition of ψ_p we have

$$\psi_p(\langle g\rangle) = gx^n \in \langle g\rangle_2.$$

Hence $\psi_p(C) \subseteq \langle g\rangle_2$. We have $\psi_p(gx^n) = gx^{2n} = g$. Hence $\langle g\rangle_2 \subseteq \psi_p(C)$ and $\psi_p(C) = \langle g\rangle_2$. □

Lemma 5.3.2. *Let $C = \langle g\rangle$ be a $(1-u^2)-$constacyclic code in S_n, where $g|(x^n-1)$* mod 2.

Then $\psi_p(C) = \langle g\rangle_2$ is a cyclic code of $Z_2^{4n}[x]$.

Proof. Let $C = \langle g\rangle$ be any $(1-u^2)-$constacyclic code in S_n, where $g|(x^n-1) \mod 2$. From the definition of ψ_p we have

$$\psi_p(\langle g\rangle) = gx^n \in \langle g\rangle_2.$$

Hence $\psi_p(C) \subseteq \langle g \rangle_2$. We have $\psi_p(gx^n) = gx^{4n} = g$. Hence $\langle g \rangle_2 \subseteq \psi_p(C)$ and $\psi_p(C) = \langle g \rangle_2$. $\square$

Lemma 5.3.3. [2] *Let $C = \langle ug \rangle$ be a $(1+u)-$constacyclic code in R_n where $g|(x^n - 1)$* mod 2.

Then $\psi_p(C) = \langle g(x^n + 1) \rangle_2$ is a cyclic code of $Z_2^{2n}[x]$.

Proof. Similar to the proof of Lemma 5.3.1 . $\square$

Lemma 5.3.4. *Let $C = \langle ug \rangle$ be a $(1-u^2)-$constacyclic code in S_n where $g|(x^n - 1)$* mod 2.

Then $\psi_p(C) = \langle g(x^n + 1) \rangle_2$ is a cyclic code of $Z_2^{4n}[x]$.

Proof. Similar to the proof of Lemma 5.3.2 . $\square$

Lemma 5.3.5. *Let $C = \langle u^2 g \rangle$ be a $(1-u^2)-$constacyclic code in S_n where $g|(x^n - 1)$* mod 2.

Then $\psi_p(C) = \langle g(x^n + 1) \rangle_2$ is a cyclic code of $Z_2^{4n}[x]$.

Proof. Similar to the proof of Lemma 5.3.2 . $\square$

Lemma 5.3.6. [2] *Let $C = \langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle$ be a $(1+u)-$constacyclic code of length $n = 2^e m$ and $\gcd(2, m) = 1$ in R_n. Suppose for some i_j, we have $2^e < i_j \leq 2^{e+1}$. Then $\psi_p(C)$ is a binary cyclic code of length $2n$ with generator $\langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle_2$.*

Proof. Similar to the proof of Lemma 5.3.1 . $\square$

Lemma 5.3.7. *Let $C = \langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle$ be a $(1-u^2)-$constacyclic code of length $n = 2^e m$ and $\gcd(2, m) = 1$ in S_n. Suppose for some i_j, we have $2^e < i_j \leq 2^{e+1}$. Then $\psi_p(C)$ is a binary cyclic code of length $4n$ with generator $\langle f_1^{i_1} f_2^{i_2} \dots f_r^{i_r} \rangle_2$.*

Proof. Similar to the proof of Lemma 5.3.2 . $\square$

5.4 Examples

Example 5.4.1. [2] *Let* $C = \langle f_1^3 f_2 \rangle$ *where* $x^6 - 1 = f_1^2 f_2^2,\ f_1(x) = x + 1,$ *and* $f_2(x) = x^2 + x + 1$*. According to Lemma 5.2.6,* $f(x) = f_1(x)$ *and* $g(x) = f_1^2(x) f_2(x)$
$\Rightarrow C = \big\langle (x+1)^3(x^2+x+1) \big\rangle = \big\langle (x+1)(x+1)^2(x^2+x+1) \big\rangle = \big\langle f(x)g(x) \big\rangle$
$\Rightarrow$ *deg* $f = 1$ *, deg* $g = 4$ *i.e.r* $= 4$ *,* $t = 1$*. Hence the generating set of codewords of* C *over* R *is given by:* $\beta = \{f_1^3 f_2, x f_1^3 f_2, u f_1, x u f_1, x^2 u f_1\}$*, and* $|C| = 4^2.2^3$*.*

Example 5.4.2. $x^{10} - 1 = (x+1)^2(x^4 + x^3 + x^2 + x + 1)^2 = f_1^2(x) f_2^2(x)$
According to Lemma 5.2.7 , let $f(x) = x + 1 = f_1(x)$ *and* $g(x) = (x+1)^2(x^4 + x^3 + x^2 + x + 1) = f_1^2(x) f_2(x)$*.*
$\Rightarrow$ *deg*$\big(g(x)\big) = 6,$ *deg*$\big(f(x)\big) = 1 \Rightarrow r = 6,\ t = 1,\ n - r - 1 = 3,\ r - t - 1 = 4.$
Since $(x+1)|(x+1)^2(x^4 + x^3 + x^2 + x + 1)|(x^{10} - 1)$
$\Rightarrow f|g|(x^{10} - 1)$ *mod 2* $\Rightarrow C = \big\langle fg \big\rangle = \big\langle f_1^3 f_2 \big\rangle$*. Thus the generating set of code words of* C *over* S *is given by:*
$\beta = \big\{fg, xfg, x^2fg, x^3fg, uf, xuf, x^2uf, x^3uf, x^4uf, u^2f, xu^2f, x^2u^2f, x^3u^2f, x^4u^2f\big\}$*. Thus* $|C| = 8^4.4^5.2^5$*.*

Example 5.4.3. [2] *Let* $C = \big\langle u g_1^3 g_2^2 g_3^4 \big\rangle$ *where* $x^{28} - 1 = g_1^4 g_2^4 g_3^4,\ g_1(x) = x + 1,\ g_2(x) = x^3 + x + 1,$ *and* $g_3(x) = x^3 + x^2 + 1$*. According to Lemma 5.2.3,* $g(x) = g_1^3 g_2^2 g_3^4$ *and a generating set of codewords of* C *is given by* $\beta = \{ug, uxg, \dots, ux^6 g\}$*. Thus* $|C| = 2^7 = 128$*..*

Example 5.4.4. $x^8 - 1 = (x-1)^8$ *in* S*.*
Now, since $u^2 = x^n - 1 \Rightarrow u^2 = x^8 - 1$*. Let* $g(x) = (x-1)^4 \Rightarrow g(x)|(x^8 - 1)$ *mod 2* $\Rightarrow$ $u^2 g = (x^8 - 1)(x-1)^4 = x^{12} - 1 = x^4 - 1 \ \big(\text{mod } x^8 - 1\big) \Rightarrow C = \big\langle x^4 - 1 \big\rangle = \big\langle g(x) \big\rangle$*.*
According to Lemma 5.2.2, deg $g = 4 \Rightarrow r = 4,\ n - r - 1 = 3,\ r - 1 = 3$*. Thus* C *has a minimal spanning set over* S *given by:*
$\beta = \big\{x, xg, x^2g, x^3g, u, xu, x^2u, x^3u, u^2, xu^2, x^2u^2, x^3u^2\big\}$*. Thus* $|C| = 8^4.4^4.2^4$*.*

Conclusion

In this thesis, we studied cyclic codes of an arbitrary length n over the ring $F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2,$ with $u^k = 0 \; mod \; 2.$ The rank and minimum spanning of this family of codes are studied as well.

We also studied constacyclic codes of even length n over the ring $F_2 + uF_2 + u^2F_2,$ with $u^3 = 0 \; mod \; 2.$ The dual and Gray images of this family of codes are studies as well.

Open problems include the study of constacyclic codes of even length over the ring $F_p + uF_p + u^2F_p + \ldots + u^kF_p,$ where k is positive, $u^{k+1} = 0 \mod p$ and p is a prime integer. Also it will be interesting to construct a decoding algorithm for these codes that works for any length n.

Bibliography

[1] T. Abualrub and R. Oehmke, On the generators of Z_4 cyclic codes of length 2^e, IEEE Trans.Inf.Theory, vol.49, no.9, pp.2126-2133, 2003.

[2] T. Abualrub and I. Saip, Constacyclic codes over $F_2 + uF_2$, Journal of the Franklin Institute, vol.346, no.02, pp.520-529, 2009.

[3] T. Abualrub and I. Saip, Cyclic codes over the Rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$, Designs, Codes and Creptography vol.42, no.03, pp.273-287, 2007.

[4] M. Al-Ashker, Simplex codes over the Ring $\sum_{n=0}^{s} u^n F_2$, Turk .J.Math, vol.29, pp.221-233, 2005.

[5] G. Bini and F. Flamini, Finite commutative rings and their applications, University of Michigan, Universita degli Studi Roma Tre, U.S.A and Italy, 2002.

[6] T. Blackford, Cyclic codes over Z_4 of oddly even length, Discrete Applied Mathematics, vol.128, pp.83-92, 2001.

[7] A. Bonnecaze and P. Udaya, Cyclic codes and Self-dual codes over $F_2 + uF_2$, IEEE Trans.Inform.Theory, vol.45, no.04, pp.1250-1255, 1999.

[8] AR. Calderbank, EM. Rains, PW. Shor, J. Neil, NJA. Sloane, Quantum error corrections via codes over GF(4), LEEE Transactions on Information Theory, vol.4, no.4, pp.1369-1387, 1998.

[9] AR. Calderbank and NJA. Sloane, Modular and P-adic cyclic codes, Des Codes Crypt, vol.37, no.6, pp.21-35, 1995.

[10] H.Q. Dinh and S.R. Lopez, Cyclic and negacyclic codes over finite chain rings, IEEE Trans.Inform.Theory, vol.50, no.8, pp.1728-1744, 2004.

[11] S.T. Dougherty and K. Shiromoto, Maximum mistance codes over rings of order 4, IEEE Trans. Inform. Theory, vol.47, no.1, pp.400-404, 2001.

[12] S.T. Dougherty and S. Ling, Cyclic codes over Z_4 of even length, Designs, Codes and Creptography vol.34, no.2, pp.127-153, 2006.

[13] J.B Fraleigh, First course in abstract algebra, 5^{th} Edition, 1993.

[14] D. Hofman, Coding theory, 1990.

[15] W.C. Huffman and V. Pless, Fundementals of Error-Correcting Codes, Cambridge, U.K. Cambridge Univ. Press, 2003.

[16] V.K. Khanna, A course in abstract algebra, University of Delhi Second Rivisted Edition, 1998.

[17] C. Musiti, Introduction to Rings and Modules, University of Hyderabad, Second Rivisted Edition, 1994.

[18] G. Noton and A. Salagean, On the structure of linear and cyclic codes over a finite chain ring, Applicable Algebra Engineering Communication and Computing. Vol.10, No.6, pp.489-506, (2000).

[19] V. Pless and Z. Qian, Cyclic codes and quadratic residue codes over Z_4, IEEE Trans. Inform. Theory, vol.45, no.5, pp.1594-1600, 1996.

[20] J.F. Qian, L.N. Zhang, S.X. Zhu, $(1+u)-$constacyclic and cyclic codes over F_2+uF_2, Appl. Math. Lett, vol.19, pp.820-823, 2006.

[21] C. Shannon, Amathematical theory of communication, Bell System Tech.J.27, pp.379-423 and 623-656, 1948.

[22] J.H. Van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory, vol.37, no.2, pp.343-345, 1977.

[23] S.X. Zhu, X. Kai, Dual and self-dual negacyclic codes of even length over Z_{2^a}, Discrete Mathematics, vol.13, no.5, pp.7-10, 2008.