Negacyclic and Constacyclic codes over finite chain rings

June 29, 2008

THE ISLAMIC UNIVERSITY OF GAZA
DEANERY OF HIGHER STUDIES
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Negacyclic and Constacyclic codes over finite chain rings

PRESENTED BY
FAISAL MOHAMMED ABU DAHROUJ

SUPERVISED BY
Dr. MOHAMMED MAHMOUD AL-ASHKER

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

Dedication

To the spirit of my father...

To my mother

To my wife

To my sons nour, sundus, hla and lma

To all knowledge seekers...

Contents

Acknowledgments

I would like to express my sincere thanks and gratitude to Almighty for his blessings.

I would like to express my sincere appreciation and thanks to my supervisor Dr. Mohammed Mahmoud Al-ashker for his ceaseless help and supervision during the preparation of this project.

I would like to express my sincere thanks to all the staff members of mathematics department and all my teachers who taught me to come to this stage of learning.

I am extremely and sincerely thankful to my parents whose love, care and sacrifice enabled me to reach this level of learning.

Abstract

The negashift ν of Z_4^n is defined as the permeation of Z_4^n such that

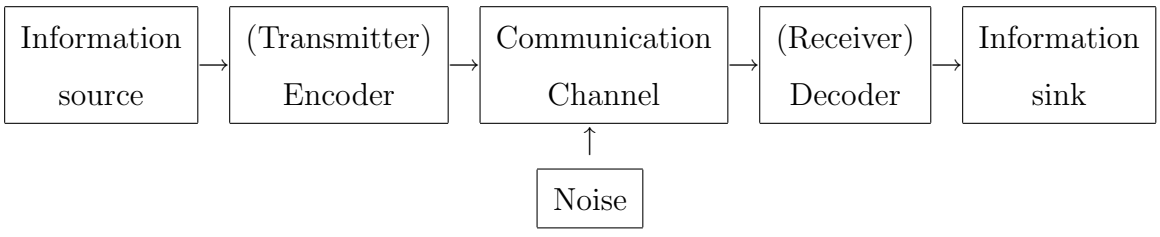
$$\nu(a_0, a_1, ..., a_i, ..., a_{n-1}) = (-a_{n-1}, a_0, ..., a_i, ...a_{n-2})$$

and negacyclic code of length n over Z_4 is defined as a subset C of Z_4^n such that $\nu(C) = C$. We prove that the Gray image of a linear negacyclic code over Z_4 of length n is a binary distance invariant cyclic code. We introduce $(1 + u)$-constacyclic and cyclic codes over the ring $R_2 = F_2 + uF_2$, and study them by analogy with the Z_4 case. We prove that the Gray image of a linear $(1 + u)$-constacyclic code over R_2 of length n is a binary distance invariant cyclic code. Also we define a Gray map between codes over $R_3 = F_2 + uF_2 + u^2F_2$ and codes over F_2. We prove that the Gray image of a linear $(1 - u^2)$-constacyclic code over R_3 of length n is a binary distance invariant linear quasi-cyclic code. Finally we define a new Gray map between $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ and $F_2^{2(k-1)}$. We prove that the Gray image of a linear $(1 - u^{k-1})$-constacyclic code over R_k of length n is a binary distance invariant quasi-cyclic code of order $k - 1$.

Keywords:- cyclic odes, negacyclic code, constacyclic code, quasi-cyclic code, Hpocyclic code, Gray map.

Introduction

Claude Shannons 1948 paper "A Mathematical Theory of Communication" gave birth to the twin disciplines of information theory and coding theory. The basic goal is efficient and reliable communication in an uncooperative (and possibly hostile) environment. To be efficient, the transfer of information must not require a prohibitive amount of time and effort. To be reliable, the received data stream must resemble the transmitted stream to within narrow tolerances. These two desires will always be at odds, and our fundamental problem is to reconcile them as best we can. At an early stage the mathematical study of such questions broke into the two broad areas. Information theory is the study of achievable bounds for communication and is largely probabilistic and analytic in nature. Coding theory then attempts to realize the promise of these bounds by models which are constructed through mainly algebraic means. Shannon was primarily interested in the information theory. Shannons colleague Richard Hamming had been laboring on error-correction for early computers even before Shannons 1948 paper, and he made some of the first breakthroughs of coding theory. The following diagram shows the system communication system for transmitting information from a source to a destination through a channel.



the most important part of the diagram, as far as we are concerned is the noise, for without it there would be no need for the theory.

A code of length n and size M consists of a set of M vectors each with n components, the components being taken from some alphabet set S. In classical coding theory S is a field of order $|S|$. Later more general alphabets are used such as rings. A code C is a set of n-tuples subset of S^n. A linear code C can be specified by a generator matrix G over a set S, such that C is the row space of G.

In an important paper, Hammons, there are another [2] show how to construct well known binary nonlinear like Kerdock codes and Delsarte-Goethals codes by applying the Gray map to linear code over Z_4. Another important alphabet of size 4 besides Z_4 is R_2 introduced in [3] for construct lattices. Codes over R_2 have been discussed by a number of authors [10], [11].

In [9], Wolfmann showed that the Gray image of a linear negacyclic code over Z_4 of length n is a distance-invariant cyclic code. In [12] he also determined all linear cyclic codes over Z_4 of odd length whose Gray images are linear codes.

In [11], Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu showed that the Gray image of a linear constacyclic code over R_3 of length n is a distance-invariant linear quasi- cyclic code of order 2. But no work has been done on the Gray image of a linear constacyclic code over R_k.

In this thesis, we generalize the main result of [11] to the ring R_k. We define a distance preserving map from R_k to $F_2^{2(k-1)}$, and characterize codes over $F_2^{2(k-1)}$ which are the Gray images of $(1-u^{k-1})$-constacyclic codes over R_k.

This thesis consists of four chapters. In the first chapter we give general definitions on rings and cods. Also we define the Generator matrix and parity-check matrix.

In chapter two we study Negacyclic codes over Z_4 and Negacyclic codes of length 2^t over Z_{2^m}.

In third chapter we study Constacyclic codes over the finite chain rings R_2 and R_3 and more over we study Constacyclic codes over Z_{2^k} , binary quasi-cyclic codes and Hpo-cyclic codes.

In chapter four we generalized our study in chapter three, to include Constacyclic codes

over R_k. As a new result, we constructed a new Gray map and we have proved that "The Gray image of a linear $(1-u^{k-1})$-constacyclic code over R_k is binary distance invariant linear quasi-cyclic code of order $k-1$."

Chapter 1

Preliminaries

1.1 General definitions on rings

In this section, we introduce fundamental algebra structures, namely groups, subgroups, rings, the polynomial rings, ideals, maximal ideals, principal ideals, irreducible polynomial and idempotent.

Definition 1.1.1. [8] A nonempty set of elements G is said to form a **group** if in G there is defined a binary operation, called the product and denoted by(.) such that

1. $a, b \in G$ implies that $a.b \in G$ (closed).
2. $a, b, c \in G$ implies that $a.(b.c) = (a.b).c$ (associative).
3. There exists an element $e \in G$ such that $a.e = e.a = a$ for all $a \in G$(the existence of an identity element in G).
4. For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a.a^{-1} = a^{-1}.a = e$ (the existence of inverse in G).

Definition 1.1.2. [8] A nonempty subset H of a group G is said to be a **subgroup** of G if, under the product in G, H itself forms a group.

Definition 1.1.3. [8] A nonempty set R is said to be an **associative ring** if in R, there are defined two operations, denoted by (+) and (.) respectively, such that for all a, b, c, in R :

1) $a + b$ is in R.

2) $a + b = b + a$

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

4) There is a unique element 0 in R such that $a + 0 = a$ (for every a in R).

5) There exists a unique element $-a$ in R such that $a + (-a) = 0$.

6) $a \,.\, b$ in R.

7) $a \,.\, (\, b \,.\, c\,) \;=\; (\, a \,.\, b\,) \,.\, c$.

8) $a \,.\, (\, b \;+\; c\,) \;=\; a \,.\, b \;+\; a \,.\, c$ and $(\, b \;+\; c\,).\; a \;=\; b \,.\, a \;+\; c \,.\, a$ (the two distributive laws hold).

If the multiplication in R is such that $a.b = b.a$ for every a, b in R, then we call R a **commutative ring**

Definition 1.1.4. [8] A **ring homomorphism** ϕ from a ring R to a ring S is a mapping from R to S such that for all a, b in R:

1. $\phi(a + b) = \phi(a) + \phi(b)$.

2. $\phi(ab) = \phi(a)\phi(b)$.

Example 1.1.1. *Let $R[x]$denote the ring of all polynomials with real coefficients. The mapping $f(x) \longrightarrow f(1)$ is a ring homomorphism from $R[x]$ onto R.*

Definition 1.1.5. [8] A ring homomorphism that is both one-to-one and onto is called an **isomorphism**.

Definition 1.1.6. [16] Let R be a ring. A nonempty subset I of R is called an **ideal** if

1. both $a + b$ and $a - b$ belong to I, for all $a, b \in I$.

2. $r.a \in I$, for all $r \in R$ and $a \in I$.

Example 1.1.2. *For any ring R , $\{0\}$ and R are ideals of R.*

Definition 1.1.7. [16] An ideal I of a ring R is called a **principle ideal** if it is generated by an element $g \in I$ such that $I = \langle g \rangle$, where

$$I = \langle g \rangle := \{gr : r \in R\} \quad .$$

A ring R is a **principal ideal ring** if every ideal of R is principal. The element g is called a **generator** of I and I is said to be generated by g.

Definition 1.1.8. [16] Let R be a ring and let A be ideal of R. The set of cosets $\{r + A | \ r \in R\}$ is called **factor ring**.

Example 1.1.3. *In the ring $F_2[x]/(x^3 - 1)$, the subset $I = \{0, 1+x, x+x^2, 1+x^2\}$ is an ideal.*

Definition 1.1.9. [8] An ideal $M \neq R$ in a ring R is said to be a **maximal ideal** of R if whenever U is an ideal of R such that $MU \subset R$, then either $R = U$ or $M = U$.

Example 1.1.4. *The maximal ideals of Z_{36} ,are $\langle 2 \rangle$ and $\langle 3 \rangle$.*

Example 1.1.5. *In the ring $F_2[x]/(x^3 - 1)$, the subset*

$$I := \{0, 1+x, x+x^2, 1+x^2\},$$

is principal (i.e.$I = \langle 1+x \rangle$). Now, note that;

$$0.(1+x) = 1 + x^3 = 0 = (1 + x + x^2)(1+x)$$
$$1.(1+x) = 1 + x = (x + x^2)(1+x)$$
$$x.(1+x) = x + x^2 = (1 + x^2)(1+x)$$
$$x^2.(1+x) = 1 + x^2 = (1+x)(1+x)$$

Definition 1.1.10. [8] A **zero-divisor** is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition 1.1.11. [8] Two polynomials $f_1, f_2 \in R[x]$ are called **coprime** if $< f_1 > + < f_2 >= R[x]$, or equivalently , if there exist $g_1, g_2 \in R[x]$ such that $f_1 g_1 + f_2 g_2 = 1$. A polynomial $f \in R[x]$ is **called regular** if it is not a zero divisor.

Definition 1.1.12. [8] A polynomial $f(x) \in F[x]$ is said to be **irreducible** over a field F if whenever $f(x) = a(x)\ b(x)$ with $a(x),\ b(x) \in F[x]$ then one of $a(x)$ or $b(x)$ has degree 0(constant), otherwise $f(x)$ is **reducible** .

Example 1.1.6. *The polynomial* $g(x) = 1+x+x^2 \in Z_2[x]$ *is of degree 2. It is irreducible, otherwise, it would have a linear factor* x *or* $x+1$ *; i.e., 0 or 1 would be a root of g(x), but* $g(0) = g(1) = 1 \in Z_2$.

Example 1.1.7. *The polynomial* $f(x) = x^4 + 2x^6 \in Z_3[x]$ *is of degree 6. It is reducible as* $f(x) = x^4(1 + 2x^2)$.

Definition 1.1.13. [16] We denote by $F_q[x]/(1 + x^n)$, the ring of all polynomial, modulo $(1 + x^n)$ over the field F_q.
A polynomials $I(x) \in R_n$ is called **idempotent**, if $I(x)^2 = I(x)\ \ mod\ (1 + x^2)$.

Example 1.1.8. $x^3 + x^6 \in Z_2[x]/(x^9 + 1)$, $(x^3 + x^6) mod\ \ (1 + x^9)$ *is an idempotent, because*
$(x^3 + x^6)^2 = (x^6 + 2x^9 + x^{12})\ \ mod\ \ (1 + x^9) = (x^3 + x^6)\ mod\ (1 + x^9)$ *over* Z_2.

Definition 1.1.14. [16] A **field** is a nonempty set F of elements with two operations "+" and "." satisfying the following axioms. For all $a, b, c \in F$:

1. F is closed under + and . ; i.e, $a + b$ and $a\ .\ b$ are in F.
2. Commutative laws: $a + b = b + a,\ \ a.b = b.a$.
3. Associative:$(a + b) + c = a + (b + c),\ \ (a.b).c = a.(b.c)$.
4. Distributive law: $a.(b + c) = a.b + a.c$.

Furthermore, two distinct identity elements 0 and 1 must exist in F satisfying the following:

1. $a + 0 = a$ for all $a \in F$.
2. $a.1 = a$ and $a.0 = 0$ for all $a \in F$.

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

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

Definition 1.1.15. [8] A nonempty set V is said to be a **vector space** over a field F if V is an abelian group under an operation which we denote by $(+)$, and if for every $\alpha \in F$, $v \in V$ there is defined an element, written αv subject to

1. $\alpha(v + w) = \alpha v + \alpha w$;

2. $(\alpha + \beta)v = \alpha v + \beta v$;

3. $\alpha(\beta v) = (\alpha\beta)v$;

4. $1v = v$;

   for all $\alpha, \beta \in F$, $v, w \in V$ where (the 1 represent the unit element of F under multiplication).

Definition 1.1.16. [8] If V is a vector space over F and if $W \subset U$, then W is a **subspace** of V whenever $w_1, w_2 \in W$, $\alpha, \beta \in F$ implies that $\alpha w_1 + \alpha w_2 \in W$.

1.2 General definitions on codes

In this section, we define alphabet, codes, codewords, or strings, codes over fields, Hamming weights and Hamming distances.

Definition 1.2.1. [16] Let $A = \{a_1, a_2.....a_q\}$ be a set of size q , which we refer to as a **code alphabet** and whose elements are called **code symbols**. A q-ary word of length n over A is a sequence $W = w_1w_2.....w_n$ with each $w_i \in A$ for all i. A **q-ary block code** of length n over A is a nonempty set C of q-ary words having the same length n on $C \subset A^n$.

Definition 1.2.2. [16] An element of C is called **codeword** in C. The number of codewords in C, denoted by $\mid C \mid$, is called **the size** of C. A code of length n and size M is called an (n, M)-code.

Example 1.2.1. *Let* $C = \{00, 10, 01, 11\}$,
01 is codeword and $\mid C \mid = 4$.

Definition 1.2.3. [16] Z_4 is a ring of integers modulo 4 contains four elements which are $\{0, 1, 2, 3\}$ or $\{0, 1, 2, -1\}$.

Definition 1.2.4. [18] ${F_q}^n$ denotes the vector space of all n-tuples over the finite field F_q.

Definition 1.2.5. [14] $R_2 = F_2 + uF_2$ 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

·	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 1.2.6. [15] $R_3 = F_2 + uF_2 + u^2F_2$ is a commutative ring of 8 elements which are $\{0, 1, u, u^2, v, v^2, uv, v^3\}$, where $u^3 = 0$, $v = 1+u$, $v^2 = 1+u^2$, $v^3 = 1+u+u^2$, $uv = u+u^2$. The element of R are the polynomials over F_2 modulo the ideal (u^3) of $F_2[u]$, where F_2 is the binary field $\{0, 1\}$. 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

·	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 1.2.7. [16] Let **x** and **y** be words of length n over an alphabet A. **The Hamming distance** from **x** and **y**, denoted by $d(x, y)$, is defined to be the number of places at which **x** and **y** differ . If $\mathbf{x} = x_1.....x_n$ and $\mathbf{y} = y_1.....y_n$, then

$$d(\mathbf{x}, \mathbf{y}) = d(x_1, y_1) + ... + d(x_n, y_n) \tag{1.2.1}$$

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

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

Example 1.2.2. *Let* $A = \{0, 1\}$ *and let* $\boldsymbol{x} = 01010$, $\boldsymbol{y} = 11101$

$$d(\boldsymbol{x}, \boldsymbol{y}) = 4$$

Example 1.2.3. *Let* $A = \{0, 1, 2, 3\} = Z_4$ *and let* $\boldsymbol{x} = 1234, \boldsymbol{y} = 1423$

$$\textit{then} \quad d(\boldsymbol{x}, \boldsymbol{y}) = 3$$

Proposition 1.2.1. *[16] Let* $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ *be words of length* n *over* A *. Then we have*

1) $0 \leq d(\boldsymbol{x}, \boldsymbol{y}) \leq n.$

2) $d(\boldsymbol{x}, \boldsymbol{y}) = 0$ *if and only if* $\boldsymbol{x} = \boldsymbol{y}$.

3) $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$ *for all* $x, y \in A$.

4) (Triangl inquality.) $d(\boldsymbol{x}, \boldsymbol{z}) \leq (\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{y}, \boldsymbol{z})$ *for all* $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in A$.

Proof. see [16]

□

Definition 1.2.8. [16] For a code C that containing at least two words, the **(minimum) distance** of C , denoted by $d(C)$, is

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

Example 1.2.4. *Let* $C = \{00000, 00111, 11111\}$ *be a binary code. Then* $d(C) = 2$ *because,*

$$d(00000, 00111) = 3$$
$$d(00000, 11111) = 5$$
$$d(00111, 11111) = 2$$

Hence, C is a binary $[5, 3, 2] - code$.

Example 1.2.5. *Let* $C = \{000000, 000111, 111222\}$ *be a ternary code (i.e. with code alphabet* $\{0, 1, 2\}$*). Then* $d(C) = 3$ *since*

$$d(000000, 000111) = 3$$
$$d(00000, 111222) = 6$$
$$d(000111, 111222) = 6$$

Hence, C is a ternary $(6, 3, 3) - code$.

Definition 1.2.9. [4] A code C is called a **linear code** if $\mathbf{x} + \mathbf{y}$ is a word in C whenever $\mathbf{x}$ and $\mathbf{y}$ are in C. That is, a linear code is a code which is closed under addition of words.

Example 1.2.6. $C = \{000, 111\}$ *is a linear code over* F_2, *since all four of the sums*

$$000 + 000 = 000$$
$$111 + 000 = 111$$
$$000 + 111 = 111$$
$$111 + 111 = 000$$

are in C. A linear code C must contain the zero word.

Definition 1.2.10. [16] A linear code C of length n over F_q is a subspace of ${F_q}^n$.

Example 1.2.7. *$C = \{(\lambda, \lambda, ..., \lambda) \quad : \quad \lambda \in F_q\}$ is a linear code. This code is often called a* ***repetition code.***

Definition 1.2.11. [16] Let $\mathbf{x}$ be a word in ${F_q}^n$. The **Hamming weight** of $\mathbf{x}$, denoted by $wt(\mathbf{x})$, is defined to be the number of nonzero coordinates in $\mathbf{x}$;i.e.,

$$wt(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$$

where $\mathbf{0}$ is the zero word.

Example 1.2.8. *If $\boldsymbol{x}$=(1010111)$\in F_2^7$ and $\boldsymbol{y}$=(00111010111)$\in F_2^{11}$, then wt($\boldsymbol{x}$)=5, wt($\boldsymbol{y}$)=7.*

Notation 1.2.2. *The Lee weight of an element $\boldsymbol{x} \in Z_4$ is defined by:*

$w_L(0)=0$

$w_L(1)=1$

$w_L(2)=2$

$w_L(3)=1$

Definition 1.2.12. [18] The **Lee weight** of $\mathbf{x}\in Z_4^n$ is $w_L = n_1(\mathbf{x})+2n_2(\mathbf{x})+n_3(\mathbf{x})$, where $n_a(\mathbf{x})$ denote the number of components of $\mathbf{x}$ equal to a for all $a \in Z_4$.

Remark 1.2.1. Z_4^n is a modulo over Z_4. A linear code C of length n over Z_4 is a Z_4-modulo subset of Z_4^n.

Example 1.2.9. *Let $\boldsymbol{x}$=(13201322)$\in Z_4^8$ then $w_L = n_1(\boldsymbol{x})+2n_2(\boldsymbol{x})+n_3(\boldsymbol{x}) = 2+2.3+2 =$* 10.

Definition 1.2.13. [18] The **Lee distance** d_L, is defined as $d_L = wt_L(\mathbf{x} - \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in Z_4^n$.

Remark 1.2.2. [16] For every element $\mathbf{x}$ of F_q, we can define the Hamming weight as follows:

$$wt(\mathbf{x}) = d(\mathbf{x}, 0) = \begin{cases} 1 & \text{if } \mathbf{x} \neq 0, \\ 0 & \text{if } \mathbf{x} = 0. \end{cases}$$

$\mathbf{x}$	$\mathbf{y}$	$\mathbf{x} \star \mathbf{y}$	$wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} \star \mathbf{y})$	$wt(\mathbf{x} + \mathbf{y})$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

Table (1)

Then writing $\mathbf{x} \in {F_q}^n$ as $\mathbf{x} = (x_1, x_2, ..., x_n)$, the Hamming weight of $\mathbf{x}$ can also be equivalently defined as

$$wt(\mathbf{x}) = wt(x_1) + wt(x_2) + ... + wt(x_n) \tag{1.2.2}$$

Proposition 1.2.3. *[4] We now list a number of facts concerning weight and distance, Let $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{z}$ be words of the same length n and $\boldsymbol{a}$ is a digit then,*

1) $0 \leq wt(\boldsymbol{x}) \leq n$.

2) $wt(\boldsymbol{x}) = 0 \ iff \ \boldsymbol{x} = 0$.

3) $0 \leq d(\boldsymbol{x}, \boldsymbol{y}) \leq n$.

4) *If* $d(\boldsymbol{x}, \boldsymbol{y}) = 0$ *if and only if* $\boldsymbol{x} = \boldsymbol{y}$.

5) $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$.

6) $wt(\boldsymbol{x} + \boldsymbol{y}) \leq wt(\boldsymbol{x}) + wt(\boldsymbol{y})$.

7) $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$.

8) $wt(\boldsymbol{ax}) = \boldsymbol{a}.wt(\boldsymbol{x})$, *where* $\boldsymbol{a} \neq 0$ *and* $\boldsymbol{a} \in F_q$.

9) $d(\boldsymbol{ax}, \boldsymbol{az}) = \boldsymbol{a}.d(\boldsymbol{x}, \boldsymbol{z})$, *where* $\boldsymbol{a} \neq 0$ *and* $\boldsymbol{a} \in F_q$.

Lemma 1.2.4. *[4] If* $\boldsymbol{x}, \boldsymbol{y} \in {F_q}^n$, *then* $d(\boldsymbol{x}, \boldsymbol{y}) = wt(\boldsymbol{x} - \boldsymbol{y})$.

Proof. For $\mathbf{x}, \mathbf{y} \in F_q$, $d(\mathbf{x}, \mathbf{y}) = 0$ if and only if $\mathbf{x} = \mathbf{y}$, which is true if and only if $\mathbf{x} - \mathbf{y} = 0$ or, equivalently $wt(\mathbf{x} - \mathbf{y}) = 0$.
Now from Equation 1.2.1 and 1.2.2, we have

$$d(\mathbf{x}, \mathbf{y}) = d(x_1, y_1) + d(x_2, y_2), ... + d(x_n, y_n), \tag{1.2.3}$$

$$wt(\mathbf{x}) = wt(x_1) + wt(x_2) + ... + wt(x_n). \tag{1.2.4}$$

And similarly

$$wt(\mathbf{x} - \mathbf{y}) = wt(x_1 - y_1) + wt(x_2 - y_2) + ... + wt(x_n - y_n) \tag{1.2.5}$$

$$wt(\mathbf{x} - \mathbf{y}) = d(x_1, y_1) + d(x_2, y_2) + ... + d(x_n, y_n). \tag{1.2.6}$$

From Equation 1.2.3 and 1.2.6 we have

$$d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$$

.

□

Lemma 1.2.5. *[16] Let $\boldsymbol{x}, \boldsymbol{y} \in {F_2}^n$, then*

$$wt(\boldsymbol{x} + \boldsymbol{y}) = wt(\boldsymbol{x}) + wt(\boldsymbol{y}) - 2wt(\boldsymbol{x} \star \boldsymbol{y}) \tag{1.2.7}$$

where $\boldsymbol{x} \star \boldsymbol{y} = (x_1 y_1, x_2 y_2, ..., x_n y_n)$, for
$\boldsymbol{x} = (x_1, x_2, ..., x_n)$ and $\boldsymbol{y} = (y_1, y_2, ..., y_n)$

Proof. From equation 1.2.2, it is enough to show that 1.2.7 is true for $\mathbf{x}, \mathbf{y} \in {F_2}^n$. This can be easily verified as, in the table (1). □

Definition 1.2.14. [16] Let C be a code. The **minimum(Hamming)weight** of C , denoted by wt(C), is the smallest of the weights of the nonzero codeword of C.

Theorem 1.2.6. *[16] Let C be a linear code over F_q. Then $d(C) = wt(C)$.*

Proof. From Lemma 1.2.4 we have $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. From Definition 1.2.14, there exist $\acute{\mathbf{x}}$, $\acute{\mathbf{y}} \in C$ such that $d(\acute{\mathbf{x}}, \acute{\mathbf{y}}) = d(C)$, so

$$d(C) = d(\acute{\mathbf{x}}, \acute{\mathbf{y}}) = wt(\acute{\mathbf{x}} - \acute{\mathbf{y}}) \geq wt(C) \tag{1.2.8}$$

since $\acute{\mathbf{x}} - \acute{\mathbf{y}} \in C$.

Conversely, there is a $\mathbf{z} \in C \setminus \{\mathbf{0}\}$ such that $wt(C) = wt(\mathbf{z})$. So

$$wt(C) = wt(\mathbf{z}) = d(\mathbf{z}, \mathbf{0}) \geq d(C) \tag{1.2.9}$$

Now from 1.2.8 and 1.2.9 we have

$$d(C) = wt(C).$$

□

Example 1.2.10. *Let the binary linear code* $C = \{0000, 1000, 0100, 1100\}$.

Now

$$wt(1000) = 1$$
$$wt(0100) = 1$$
$$wt(1100) = 2$$

Hence, $d(C) = 1$.

Definition 1.2.15. [4] 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 $\mathbf{x.c}$ is the usual scalar product $x_1c_1 + x_2c_2 + ... + x_nc_n$ of the vectors $\mathbf{x}$ and $\mathbf{c}$. **Note** that $C^{\perp}$ is an $[n, n-k]$ code.

Definition 1.2.16. [16] If $\mathbf{x} = x_1x_2, ..., x_n$ and $\mathbf{y} = y_1y_2, ..., y_n$ are binary words, we define the intersection of $\mathbf{x}$ and $\mathbf{y}$ by

$$\mathbf{x} \cap \mathbf{y} = (x_1y_1, x_2y_2, ..., x_ny_n).$$

Thus $\mathbf{x} \cap \mathbf{y}$ has a 1 in the *ith* position if and only of both $\mathbf{x}$ and $\mathbf{y}$ have 1 in the *ith* position.

We define the dot product of $\mathbf{x}$ and $\mathbf{y}$ by :

$$\mathbf{x}.\mathbf{y} = x_1y_1 + x_2y_2 + ... + x_ny_n.$$

Theorem 1.2.7. ***[18]*** *The following hold*

1) *If* $\boldsymbol{x}, \boldsymbol{y} \in F_2^n$, *then*

$$wt(\boldsymbol{x} + \boldsymbol{y}) = wt(\boldsymbol{x}) + wt(\boldsymbol{y}) - 2wt(\boldsymbol{x} \cap \boldsymbol{y}).$$

2) *If* $\boldsymbol{x}, \ \boldsymbol{y} \in F_2^n$, *then* $wt(\boldsymbol{x} \cap \boldsymbol{y}) \equiv \boldsymbol{x}.\boldsymbol{y}(mod 2)$.

3) *If* $\boldsymbol{x} \in F_2^n$, *then* $wt(\boldsymbol{x}) \equiv \ \boldsymbol{x}.\boldsymbol{x}(mod 2)$.

4) *If* $\boldsymbol{x} \in F_3^n$, *then* $wt(\boldsymbol{x}) \equiv \boldsymbol{x}.\boldsymbol{x}$ $(mod 3)$.

5) *If* $\boldsymbol{x} \in F_4^n$, *then* $wt(\boldsymbol{x}) \equiv \langle \boldsymbol{x}.\boldsymbol{x} \rangle (mod 2)$.

Proof. See [18].

□

Definition 1.2.17. [14] Let $R_2 = F_2 + uF_2$. The **Lee weight** a_r of an element r of the ring R_2 is given by the following equations:

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

Then the Lee weight of an element $x = (x_1, x_2, \ldots, x_n)$ of R_2^n is

$$wt_L(x) = \textstyle\sum_{i=1}^{n} a_r.$$

Definition 1.2.18. [15] Let $R_3 = F_2 + uF_2 + u^2F_2$. The **Lee weight** a_r of an element r of the ring R_3 is given by the following equations:

$$a_r = \begin{cases} 0, & \text{if r= 0;} \\ 1, & \text{if r= 1, or } v^2; \\ 2, & \text{if r= u or uv;} \\ 3, & \text{if r= v or } v^3 \text{ ;} \\ 4, & \text{if r= } u^2. \end{cases}$$

Then the Lee weight of an element $x = (x_1, x_2, \ldots, x_n)$ of R_3^n is

$$wt_L(x) = \sum_{i=1}^{n} a_r.$$

Example 1.2.11. *Let* $x = (1, 0, 0, u, v, v^2, u^2, uv)$; *then* $wt_L(x) = 13$

Definition 1.2.19. The Lee distance between $\mathbf{x}$ and $\mathbf{y} \in R^n$ is denoted by $d_L(\mathbf{x}, \mathbf{y}) = wt_L(\mathbf{x} - \mathbf{y})$.

Definition 1.2.20. [16] Let X be a vector space over F_q. A set of vectors $\{\mathbf{x_1}, ..., \mathbf{x_r}\}$ in X are **linearly independent** if

$$\lambda_1\mathbf{x_1} + ... + \lambda_r\mathbf{x_r} = 0 \Rightarrow \lambda_1 = ... = \lambda_r = 0$$

Example 1.2.12. *For any* F_q, *the set* $\{(0, 0, 0, 1), (0, 0, 1, 0), (0, 1, 0, 0)\}$ *is linearly independent.*

Definition 1.2.21. [16] Let V be a vector space over F_q and let $S = \{v_1, v_2, ..., v_k\}$ be a nonempty subset of V. The **(linear) span** of S is defined as

$$< S >= \{\lambda_1 v_1 + ... + \lambda_k v_k : \lambda_i \in F_q\}.$$

Given a subspace C of V, a subset S of C is called spanning set of C if $C =< S >$.

Definition 1.2.22. [16] Let X be a vector space over F_q. A nonempty subset B=$\{\mathbf{x_1}, ..., \mathbf{x_r}\}$ of X is called a **basis** for X if $X =< B >$, B is a spanning set for X and linearly independent.

Definition 1.2.23. [16] A vector space X over a finite field F_q can have many basis; but all basis contain the same number of elements. This number is called the **dimension** of X over F_q, denoted by $dim(X)$.

Definition 1.2.24. [7] Let a be a fixed generator of the maximal ideal M. Then a is **nilpotent**. We denote its nilpotent index by t and $a^t = 0$. The ideals of R from a chain

$$R = \langle a^0 \rangle \supsetneq \langle a^1 \rangle \supsetneq ..... \supsetneq \langle a^{t-1} \rangle \supsetneq \langle a^t \rangle = \langle 0 \rangle.$$

Definition 1.2.25. [7]A ring R is called a **right(left) chain ring** if the set of all right(left) ideals of R is a chain under set-theoretic inclusion. If R is both a right and a left chain ring, we simply call R a **chain ring**.

Example 1.2.13. *The ring $R = F_2 + uF_2 + u^2F_2$ is a commutative chain ring with maximal ideal $uR = \{0, u, u^2, uv\}$. Since u is nilpotent of index 3, we have*

$$R \supset (uR) \supset (u^2R) \supset (u^3R) = 0.$$

1.3 Generator matrix and parity-check matrix

Knowing basis for a linear code enables us to describe its codewords explicitly. In coding theory, a basis for a linear code is often represented in the form of a matrix, called a generator matrix, while a matrix that represents a basis for the dual code is called a parity-check matrix. These matrices play an important role in coding theory. The rank of a matrix over K is the number of nonzero rows in any (row echelon form)REF of the matrix. The dimension k of the code C is the dimension of C.

Definition 1.3.1. [4] If C is a linear code of length n and dimension k, then any matrix whose rows form a basis for C is called a **generator matrix** for C. Note that a generator matrix for C must have k rows and n columns.

Definition 1.3.2. [4] A 1 in a matrix G over K is called a **leading** 1 if there are no 1s to its left in the same row, and a column of G is called a **leading column** if it contains a leading 1. G is in **row echelon form(REF)** if the zero rows of G are all at the bottom, and each leading 1 is to the right of the leading 1 in the rows above. If further, each leading column contains exactly one 1, G is in **reduced row echelon form(RREF)**.

Definition 1.3.3. [4] The **rank** of a matrix over k is the number of nonzero rows in any REF of the matrix.

Theorem 1.3.1. *[16] A matrix G is a generator matrix for some linear code C if and only if the rows of G are linearly independent; that is, if and only if the rank of G is equal to the number of rows of G.*

Proof. See [16].

□

Definition 1.3.4. [4] Any $k \times n$ matrix G with $k < n$ whose first k columns the $k \times k$ identity matrix $\mathbf{I}_k$ so

$$G = \left(\begin{array}{c|c} \boldsymbol{I}_k & X \end{array} \right)$$

has linearly independent rows and in RREF. Thus G is a generator matrix for some linear code of length n and dimension k. A generator matrix G is said to be **standard form**, and the code C generated by G is called a **systematic code.**

Theorem 1.3.2. *[16] If* $G = \left(\begin{array}{c|c} I_k & X \end{array} \right)$ *is a generator matrix for the* $[n, k]$ *code* C *in standard form then* $H = \left(\begin{array}{c|c} -X^{\perp} & I_{n-k} \end{array} \right)$ *is a parity-check matrix for* C*.*

Proof. see [16] □

Theorem 1.3.3. *[16] If* G *is a generator matrix for a linear code* C*, then any matrix row equivalent to* G *is also a generator matrix for* C*. In particular, any linear code has a generator matrix in RREF.*

Proof. See [16].

□

Example 1.3.1. *To find a a generator matrix for a linear code* $C = \langle S \rangle$ *, where* $S = \{11101, 10110, 01011, 11010\}$*.*

By elementary row operations we write

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

So, $G = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right) = (I_3|X)$ *is a standard form for* C.

Definition 1.3.5. [16] A matrix H is called **parity-check matrix** for a linear code C if the rows of H form a basis for dual code $C^{\perp}$, defined by

$$C^{\perp} = \{\mathbf{x} \in {F_q}^n | \quad H\mathbf{x}^{\perp} = 0\}$$

If C has length n and dimension k, then, since the sum of the dimension of C and $C^{\perp}$ is n, any parity-check matrix for C must have n rows, $n-k$ columns and rank $n-k$.

Example 1.3.2. *To find a parity-check matrix for a linear code* $C = \langle S \rangle$, *where* $S = \{11101, 10110, 01011, 11010\}$, *we have the following:*

by elementary row operations we write

$$A = \left(\begin{array}{ccccc} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccccc} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

So, $G = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right) = \left(\begin{array}{c|c} I & X \end{array}\right)$ *is a generator matrix for* C.

We have $H = \left(\begin{array}{ccccc} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array}\right)$ *is a parity-check matrix for* C.

Theorem 1.3.4. *[4] A matrix* H *is a parity-check matrix for some linear code* C *if and only if the columns of* H *are linearly independent.*

Proof. See [4].

□

Theorem 1.3.5. *[4] If H is a parity-check matrix for a linear code C of length n then C consists precisely of all words $\boldsymbol{x}$ in K^n such that $\boldsymbol{x}H^\top = 0$.*

Proof. See [4].

□

Example 1.3.3. *The matrix* $G = \left(\begin{array}{c|c} I_4 & X \end{array} \right)$ *, where*

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right)$$

is a generator matrix in standard form for [7,4] binary code by Theorem 1.3.2. A parity-check matrix is

$$H = \left(\begin{array}{c|c} X^\top & I_3 \end{array} \right) = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right).$$

Definition 1.3.6. [16] The linear code C of length n is a **cyclic code** over R if it is invariant under a cyclic shift :

$$c = (c_0, c_1, \cdots, c_{n-2}, c_{n-1}) \in C$$

if and only if

$$\tilde{c} = (c_{n-1}, c_0, c_1, \cdots, c_{n-3}, c_{n-2}) \in C$$

Example 1.3.4. *The set*

$\{11111, 00000\} \subset {F_2}^5$ *are cyclic code.*

Example 1.3.5. *The following codes are cyclic codes :*

- *Three trivial codes* $\{\boldsymbol{0}\}$,$\{\lambda \ . \ \boldsymbol{1} : \lambda \in F_q\}$ *and* ${F_q}^n$.
- *The binary* $[3, 2, 2] - linearcode$ $\{000, 110, 101, 011\}$.

Theorem 1.3.6. *[16] Let C be cyclic code with generator polynomial $g(x) = g_1 + g_2x + ... + g_kx^{k-1}$.*

Then the generator matrix for the code is given by:

$$G = \begin{pmatrix} g_1 & g_2 & g_3 & ... & g_k & 0 & 0 & ... & 0 \\ 0 & g_1 & g_2 & ... & g_{k-1} & g_k & 0 & ... & 0 \\ 0 & 0 & g_1 & ... & g_{k-2} & g_{k-2} & g_k & ... & 0 \\ : & : & : & & : & : & : & & : \\ 0 & 0 & ... & ... & g_1 & ... & ... & ... & g_k \end{pmatrix}$$

Proof. see [16]

□

Remark 1.3.1. The generator polynomial $g(x)$ of a cyclic code of length n over F_q is a divisor of the polynomial $x^n - 1$.

Definition 1.3.7. [8](**polynomial ring**) By the ring of polynomials in the indeterminate x written $F[x]$, we mean the set of all symbols $a_0 + a_1x + ... + a_nx^n$, where n can be any non-negative integer and the coefficients $a_0, a_1, ..., a_n$ are all in F.

Definition 1.3.8. [8] If $p(x) = a_0+a_1x+.....+a_mx^m$ and $q(x) = b_0+b_1x+.....+b_nx^n$ are in $F[x]$, then $p(x) = q(x)$ if and only if for every integer $i \geq 0$, $a_i = b_i$.

Definition 1.3.9. [8] If $p(x) = a_0+a_1x+.....+a_mx^m$ and $q(x) = b_0+b_1x+.....+b_nx^n$ are in $F[x]$, then $p(x) + q(x) = c_0 + c_1x + ... + c_tx^t$ where for each i, $c_i = a_i + b_i$.

Definition 1.3.10. [8] If $p(x) = a_0+a_1x+.....+a_mx^m$ and $q(x) = b_0+b_1x+.....+b_nx^n$ are in $F[x]$, then $p(x)q(x) = c_0 + c_1x + ... + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + ... + a_0b_t$.

Definition 1.3.11. [16] A nonzero polynomial $f(x) = \sum_{i=0}^{n} a_ix^i$ of degree n is said to be **monic** if $a_n = 1$.

Definition 1.3.12. [18] A polynomial $f(x) \in Z_4[x]$ is irreducible if whenever $f(x) = g(x)h(x)$ for two polynomials $g(x)$ and $h(x)$ in $Z_4[x]$, one of $g(x)$ or $h(x)$ is a unit.

Example 1.3.6. *The following factorization of* $x^4 - 1$ *into irreducible polynomials in* $Z_4[x] = (x-1)(x+1)(x^2+1)$.

Definition 1.3.13. [16] Define $\mu : Z_4[x] \longrightarrow F_2[x]$ by $\mu(f(x)) = f(x)$ $(mod\ 2)$, that is μ is determine by $\mu(0) = \mu(2) = 0$, $\mu(1) = \mu(3) = 1$, and $\mu(x) = x$. The map μ is called the **reduction homomorphism** with kernel $(2) = \{2s(x) : s(x) \in Z_4[x]\}$.
A polynomial $f(x) \in Z_4[x]$ is called **basic irreducible** if $\mu(f(x))$ is irreducible in $F_2[x]$.

Definition 1.3.14. [16] Let $f(x), g(x) \in Z_4[x]$ be two nonzero polynomials. The **greatest common divisor** of $f(x), g(x) \in Z_4[x]$, denoted by $gcd(f(x), g(x))$, is the monic polynomial of the highest degree which is a divisor of both $f(x)$and $g(x)$. We say that $f(x)$ is **co-prime** to $g(x)$ if $gcd(f(x), g(x)) = 1$.

Lemma 1.3.7. *[18] Let* $f(x)$ *and* $g(x)$ *be polynomials in* $Z_4[x]$. *Then* $f(x)$ *and* $g(x)$ *are co-prime if and if only* $\mu(f(x))$ *and* $\mu(g(x))$ *are co-prime polynomials in* $F_2[x]$.

Definition 1.3.15. [16] If C has length n, dimension k and distance d, then we refer to C as an $[n, k, d]$ linear code. These three parameters, length, dimension and distance, provide vital information about C.

Theorem 1.3.8. *[18](**Hensel's lemma**) Let* $f(x) \in Z_4[x]$. *Suppose* $\mu(f(x)) = h_1(x)h_2(x).....h_k(x)$, *where* $h_1(x)h_2(x).....h_k(x)$ *are pairwise coprime polynomials in* $F_2[x]$. *Then there exist* $g_1(x)g_2(x).....g_k(x)$ *in* $Z_4[x]$ *such that :*

1. $\mu(g_i(x)) = h_i(x)$
2. $g_1(x)g_2(x).....g_k(x)$ *are pairwise coprime, and*
3. $f(x) = g_1(x)g_2(x).....g_k(x)$

Proof. See [18] □

Graeffe's method[18] For factorization $(x^n - 1)$ in $Z_n[x]$.

1. Let $h(x)$ be an irreducible factor of $x^n + 1$ in $F_2[x]$. Write $h(x) = e(x) + o(x)$, $e(x)$ 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 $\mu(g(x)) = h(x)$, where $g(x^2) = \pm(e(x))^2 - (o(x))^2$.

Example 1.3.7. *Let $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ in F_2 be the factorization of $x^7 + 1$ into irreducible polynomials.*
Apply Graeffe's method to find the factorization of $x^7 - 1$ into monic irreducible polynomials in $Z_4[x]$.
solution:

- *If $h(x) = x + 1$, then $e(x) = 1 \quad and \quad o(x) = x$. So $g(x^2) = -(1 - x^2) = x^2 - 1$ and thus $g(x) = x - 1$.*

- *If $h(x) = x^3 + x + 1$, then $e(x) = 1$ and $o(x) = x^3 + 1$. So $g(x^2) = -(1 - (x^3 + x)^2) = x^6 + 2x^4 + x^2 - 1$ and thus $g(x) = x^3 + 2x^2 + 2x - 1$.*

- *If $h(x) = x^3 + x^2 + 1$, then $e(x) = x^2 + 1$ and $o(x) = x^3$. So $g(x^2) = -((x^2 + 1)^2 - (x^3)^2) = x^6 - x^4 - 2x^2 - 1$ and thus $g(x) = x^3 - x^2 - 2x - 1$.*
  Therefore $x^7 - 1 = (x - 1)(x^3 + 2x^2 + 2x - 1)(x^3 - x^2 + 2x - 1)$ is the factorization of $x^7 - 1$ into monic irreducible polynomials in $Z_4[x]$.

Example 1.3.8. *Let $x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$ in F_2 be the factorization of $x^9 + 1$ into irreducible polynomials.*
Apply Graeffe's method to find the factorization of $x^9 - 1$ into monic irreducible polynomials in $Z_4[x]$.
solution:

- *If $h(x) = x + 1$, then $e(x) = 1 \quad and \quad o(x) = x$. So $g(x^2) = -(1 - x^2) = x^2 - 1$ and thus $g(x) = x - 1$.*

- *If* $h(x) = x^2+x+1$, *then* $e(x) = x^2+1$ *and* $o(x) = x$. *So* $g(x^2) = -((x^2+1)^2-x^2) = -x^4 - x^2 - 1$ *and thus* $g(x) = -x^2 - x - 1$.

- *If* $h(x) = x^6 + x^3 + 1$, *then* $e(x) = x^6 + 1$ *and* $o(x) = x^3$. *So* $g(x^2) = -((x^6+1)^2 - (x^3)^2) = -x^{12} - x^6 - 1$ *and thus* $g(x) = -x^6 - x^3 - 1$.
  Therefore $x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1)$ *is the factorization of* $x^9 - 1$ *into monic irreducible polynomials in* $Z_4[x]$.

1.4 Polynomial Encoding and Decoding

One can find various generator matrices for linear cyclic codes, the simplest is the matrix in which the rows are the codewords corresponding to the the generator polynomial and its first $k-1$ cyclic shift.

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}$$

Example 1.4.1. *Let* C *be the linear cyclic code of length* $n = 7$ *with generator polynomial* $g(x) = 1 + x + x^3$ *of degree* $n - k = 3$. *Then* $k = 4$, *so a basis for* C *is,*

$$g(x) = 1 + x + x^3$$
$$xg(x) = x + x^2 + x^4$$
$$x^2g(x) = x^2 + x^3 + x^5$$
$$x^3g(x) = x^3 + x^4 + x^6$$

and, a generating matrix for C *is*

$$G = \begin{pmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{pmatrix}$$

Let C be a linear cyclic code of length n and dimension k. The k information digits $(a_0, a_1, ..., a_{k-1})$ to be encoding can be thought of as a polynomial $a(x) = a_0 + a_1x + ... + a_{k-1}x^{k-1}$ called the **information message polynomial**. Encoding consists of polynomial multiplication, that is, $a(x)$ is encoding as $a(x)g(x) = c(x)$. The inverse operation to polynomial multiplication is polynomial division. Hence finding the message corresponding to the closest codeword $c(x)$ to the received word consists of dividing $c(x)$ by $g(x)$, thus recovering the message polynomial $a(x)$.

Example 1.4.2. *Let $g(x) = 1+x+x^3$ and $n = 7$. Then $k = 7-3 = 4$. Let $a(x) = 1+x^2$ be the message polynomial corresponding to the word $a = 1010$. The message $a(x)$ is encoding as $c(x) = a(x)g(x)$, so*

$$c(x) = (1 + x^2)(1 + x + x^3) = 1 + x + x^2 + x^5$$

with $c = 1110010$ as the corresponding codeword.
If $c(x) = 1+x+x^4+x^6$ then the corresponding message polynomial is $c(x)/g(x) = a(x) = 1 + x^3$ corresponding to the message $a = 1001$.

Definition 1.4.1. The **syndrome polynomial**, $s(x)$, is defined by $s(x) = w(x) \ mod\, g(x)$, where $w(x)$ is received and $g(x)$ is generator polynomial.

If $c(x)$ is sent and $w(x)$ is received with $w(x) = c(x) + e(x)$ then one would like to compute the the syndrome and the most likely error polynomial $e(x)$. As suming $g(x)$ has degree $n - k$, then $s(x)$ will have degree less than $n - k$ and will correspond to a binary word s, of length $n - k$. Since $w(x) = c(x) + e(x)$ and $c(x) = a(x)\ g(x)$ we have that $s(x) = e(x)\ mod\ g(x)$.
We can define a matrix H in which the i^{th} row r_i is the word of length $n-k$ corresponding to $r_i(x) = x^i\ mod\ g(x)$. If w is received word then

$$w(x) = c(x) + e(x), \text{ so}$$
$$wH = (c + e)H = s(x).$$

Then $s(x) = 0$ if and only if $w(x)$ is a codeword, so H is a parity check matrix. Also, if $wH = s$ then s corresponds to $s(x) = w(x)\ mod\ g(x)$.

Example 1.4.3. *Let* $n = 7$, *and* $g(x) = 1 + x + x^2$. *Then* $n - k = 3$. *We produce* H *as follows.*

$$\begin{aligned}
r_0(x = 1) \quad & mod\ g(x) = 1 && \leftrightarrow \quad 100 \\
r_1(x) = x \quad & mod\ g(x) = x && \leftrightarrow \quad 010 \\
r_2(x) = x^2 \quad & mod\ g(x) = x^2 && \leftrightarrow \quad 001 \\
r_3(x) = x^3 \quad & mod\ g(x) = x^3 && \leftrightarrow \quad 110 \\
r_4(x) = x^4 \quad & mod\ g(x) = x^4 && \leftrightarrow \quad 011 \\
r_2(x) = x^5 \quad & mod\ g(x) = x^5 && \leftrightarrow \quad 111 \\
r_6(x) = x^6 \quad & mod\ g(x) = x^6 && \leftrightarrow \quad 101
\end{aligned}$$

$$so \quad H = \begin{pmatrix} 100 \\ 010 \\ 001 \\ 110 \\ 011 \\ 111 \\ 101 \end{pmatrix}.$$

If $w(x) = 1+x^5+x^6$ *is received,* $w = 1000011$, *then* $wH = s = 110$ *and* $s(x) = 1+x = 1 + x^5 + x^6 \ \ mod\ (1 + x + x^3)$.

Method for decoding linear cyclic code

1. Calculate the syndrome polynomial $s(x) = w(x)\ mod\ \ g(x)$, where w is the received word.

2. For each $i \geq 0$, calculate $s_i \leftrightarrow s_i(x) = x^i\ mod\ g(x)$ unite a syndrome s_j is found with $wt(s_j) \leq t$. Then the most polynomial is $e(x) = x^{n-j}s_j(x)\ mod\ (1 + x^n)$.

Remark 1.4.1.

This method decoding will only correct patterns $e(x)$ where, for some i, $x^i e(x)\ mod\ (1+x^n)$ has degree at most $n - k$.

Example 1.4.4. *Let $n = 7$, let $g(x) = 1 + x + x^3$ be the generator polynomial for the 1 error correcting (so t=1) linear cyclic code. If $w(x) = x^2 + x^3$ is received then $s(x) = w(x)\ mod\ \ g(x) = x^2 + x^3\ mod\ (1 + x + x^3) = 1 + x + x^3$ is the syndrome polynomial. We next compute*

$$s_1(x) = xs(x)\ mod\ g(x) = x(1 + x + x^2)\ mod\ g(x) = 1 + x^2$$

$$s_2(x) = x^2 s(x)\ mod\ g(x) = x(1 + x^2)\ mod\ g(x) = 1,$$

which has weight $1 \leq t$. So $j = 2$ and therefore

$$e(x) = x^{7-2}\ s_2(x)\ mod\ (1 + x^7) = x^5.$$

Thus $c(x) = w(x) + e(x) = (x^2 + x^3) + x^5$ is the most likely codeword.

Chapter 2

Negacyclic codes over The finite chain rings Z_4 and Z_{2^m}.

In 1968, Berkelamp started the study of negacyclic codes over finite fields. Recently, Wolfman [9] gave various interesting results about negacyclic codes of odd length over Z_4 and proposed question about such codes when the length is even.
In this chapter, we will study Negacyclic codes over Z_4 and Negacyclic code of odd length. Wolfman[9] proved that the Gray image of a linear negacyclic code over Z_4 of length n is a binary distance invariant cyclic code and also proved that if n is odd then every binary code which is the Gray image of a linear cyclic code over Z_4 of length n is equivalent to a cyclic code. Also in [5] H.tapia-Recills and G. vega discussed Negacyclic codes of length 2^t over Z_{2^m}, they used an approach different to obtain the structure of negacyclic codes of length $2^t (t > 1)$ over Z_{2^m} for any integer $m > 2$.

2.1 Negacyclic codes over Z_4

We first recall that a linear code of length n over Z_4 is a Z_4-submodule of Z_4^n and that the polynomial representation of Z_4^n is the map P into $Z_4[x]$ such that

$$P(a_0, a_1, ..., a_i, ..., a_{n-1}) = \sum_{i=0}^{n-1} a_i x^i.$$

If C is a subset of Z_4^n, its polynomial representation is $P(C)$. We now introduce less familiar definitions about codes over Z_4.

Definition 2.1.1. [9] The **negashift** ν of Z_4^n is the permutation of Z_4^n defined by

$$\nu(a_0, a_1, ..., a_i, ..., a_{n-1}) = (-a_{n-1}, a_0, ..., a_i, ...a_{n-2})$$

Definition 2.1.2. [9] A **negacyclic code** of length n over Z_4 is defined as a subset C of Z_4 such that $\nu(C) = C$.

Example 2.1.1. *Let* $D = (000, 133, 222, 020, 333, 331, 111, 002, 200, 311, 113, 131, 022, 202, 220, 313)$.
Clearly $D \subset {Z_4}^3$ *and* D *is linear code since any* $c_1, c_2 \in D$ *then* $c_1 + c_2 \in D$.
D *is negacyclic code since for any* $c \in D$ *we have* $\nu(c) \in D$ *where* ν *is negashift.*

Definition 2.1.3. [16] We consider the following correspondence :
$\pi : F_q^n \to F_q[x]/(x^n - 1), \quad (a_0, a_1, ..., a_{n-1}) \mapsto a_0 + a_1 x + ... + a_{n-1}x^{n-1}$
then π is an F_q-linear transformation of vector spaces over F_q.

Proposition 2.1.1. *[9] A subset* C *of* Z_4^n *is a linear negacyclic code of length* n *over* Z_4 *if and only if its polynomial representation is an ideal of the factor ring* $Z_4[x]/(x^n + 1)$.

Proof. Suppose that $\pi(C)$ is an ideal of $Z_4[x]/(x^n+1)$. Then for any $\alpha, \beta \in Z_4[x]/(x^n+1)$ and $a, b \in C$. We have $\alpha\pi(a), \beta\pi(b) \in \pi(C)$ by Definition 1.1.6 part (2). Thus by Definition 1.1.6 part(1) $\alpha\pi(a) + \beta\pi(b)$ is an element of $\pi(C)$, i.e; $\alpha\pi(a) + \beta\pi(b) = \pi(\alpha(a) + \beta(b)) \in \pi(C)$, hence $\alpha(a) + \beta(b)$ is codeword of C. This shows that C is a linear code. Now let $c = (c_0, c_1, \ldots, c_{n-1})$ be a codeword of C then The polynomial representation of C is

$$\pi(c) = (c_0 + c_1 x + \ldots + c_{n-1}x^{n-1})$$

is an element of $\pi(C)$. Since $\pi(C)$ is an ideal of $Z_4[x]/(x^n + 1)$ then the element

$$x\pi(c) = c_0 x + c_1 x^2 + \ldots + c_{n-1}x^n \in \pi(C).$$

But $\pi(C)$ is ideal in $Z_4[x]/(x^n + 1)$ is ideal and since $x^n + 1 = 0 \Rightarrow x^n = -1$.

$$\text{then } x\pi(c) = c_0 x + c_1 x^2 + \ldots + c_{n-2}x^{n-1} + c_{n-1}(-1)$$

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

is in $\pi(C)$, i.e; $(-c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is codeword of C. This mean that C is negacyclic code.

Conversely, suppose that C is negacyclic code . Then part(1) of the Definition 1.1.6 is satisfied for $\pi(C)$. For any polynomial

$$f(x) = f_0 + f_1 x + \ldots + f_{n-2} x^{n-1} + f_{n-1} x^{n-1} = \pi(f_0, f_1, \ldots, f_{n-2}, f_{n-1})$$

of $\pi(C)$ with $(f_0, f_1, \ldots, f_{n-1}) \in C$, the polynomial

$$xf(x) = -f_{n-1} + f_0 x + f_1 x^2 + \ldots + f_{n-2} x^{n-2} = -f_{n-1} + f_0 x + f_1 x^2 + ... + x^{n-1} f_{n-2}$$

is also an element of $\pi(C)$ since C is negacyclic. Thus, $x^2 f(x) = x(xf(x))$ is an element of $\pi(C)$. By induction, suppose that $x^j f(x)$ belong to $\pi(C)$ for all $j \geq 0$.

Since C is a linear code and π is a linear transformation, $\pi(C)$ is a linear space over Z_4. Hence, for any $g(x) = g_0 + g_1 x + \ldots + g_{n-1} x^{n-1} \in Z_4[x]/(x^n + 1)$, the polynomial

$$g(x)f(x) = \textstyle\sum_{i=0}^{n-1} g_i (x^i f(x))$$

is an element of $\pi(C)$. Therefore, $\pi(C)$ is an ideal of $Z_4[x]/(x^n + 1)$ since part (2) of the Definition 1.1.6 is also satisfied.

□

2.1.1 Negacyclic Codes of Odd Length

In this subsection, We will study some definitions and theorems that study negacyclic code of odd length.

Proposition 2.1.2. *[9] Let μ be the map of $Z_4[x]/(x^n - 1)$ into $Z_4[x]/(x^n + 1)$ defined by*

$$\mu(f(x)) = f(-x).$$

If n is odd then μ is a ring isomorphism.

Proof. First we will show μ is a ring homomorphism.

For the polynomials $f(x), g(x) \in Z_4[x]/(x^n - 1)$, $\mu(f(x) + g(x)) = \mu((f + g)(x)) = (f + g)(-x)) = f(-x)) + g(-x))$

$$= \mu(f(x)) + \mu(g(x)).$$

And $\mu(f(x)g(x)) = \mu((fg)(x)) = (fg)(-x)) = f(-x)g(-x)$.

$= \mu(f(x))\mu(g(x))$.

Therefore μ is a ring homomorphism.

Now we will show μ is a one to one. For the polynomials $f(x), g(x) \in Z_4[x]$, $f(x) \equiv g(x) mod\ \ (x^n - 1)$ if and only if there exists a polynomial $h(x) \in Z_4[x]$ such that $f(x) - g(x) = h(x)(x^n - 1)$ if and only if n is odd and $f(-x) - g(-x) = h(-x)((-x)^n - 1)$, if and only if

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

if and only if

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

if and only if

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

if and only if

$$\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (-1)).$$

That means, for $f, g \in Z_4[x]/(x^n - 1)$, $\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (-1))$ if and only if $f(x) \equiv g(x)(\text{mod } (x^n - 1))$. This implies that μ is a one to one homomorphism.

To show μ is onto, let $f(x) \in Z_4[x]/(x^n - (-1))$. Then there exists $f(-x) \in Z_4[x]/(x^n - 1)$ such that $\mu(f(-x)) = f((-1)^2 x) = f(x)$. Thus μ is onto.

Therefore, μ is a ring isomorphism. □

Corollary 2.1.3. *[9] If I is a subset of $Z_4[x]/(x^n - 1)$ and $\mu(I)$ is a subset of $Z_4[x]/(x^n + 1)$ with n odd, then I is an ideal of $Z_4[x]/(x^n - 1)$ if and only if $\mu(I)$ is an ideal of $Z_4[x]/(x^n + 1)$.*

Proof. Suppose I is ideal of $Z_4[x]/(x^n - 1)$. Now $f(x) + g(x) \in I$ for all $f(x)$, $g(x) \in I$ where I is ideal. So by definition of μ we have, $\mu(f(x)+g(x)) \in \mu(I)$, but $\mu(f(x)+g(x)) = \mu((f + g))(x) = (f + g)(-x) = f(-x) + g(-x) \in \mu(I)$, implies

$$f(-x) + g(-x) \in \mu(I), \quad \forall f(-x), g(-x) \in \mu(I) \tag{2.1.1}$$

And let $f(x).l(x) \in I$ for all $f(x) \in I$, $l(x) \in Z_4[x]$, by definition of μ we have

$\mu(f(x).l(x)) \in \mu(I)$, but $\mu(f(x).l(x)) = \mu((f.l)(x)) = (f.l)(-x) = f(-x).l(-x) \in \mu(I)$, implies

$$f(-x).l(-x) \in \mu(I). \tag{2.1.2}$$

From Equation 2.1.1 and Equation 2.1.2 we have $\mu(I)$ is ideal of $Z_4[x]/(x^n + 1)$.

Conversely suppose $\mu(I)$ is an ideal of $Z_4[x]/(x^n - 1)$.

Now $f(-x) + g(-x) \in \mu(I)$ for all $f(-x), g(-x) \in \mu(I)$ where $\mu(I)$ is ideal. So by definition of μ $\exists$ $f(x), g(x) \in I$ such that

$f(-x) + g(-x) = (f + g)(-x) = \mu((f + g)(x)) \in \mu(I)$.

Since μ is is a ring isomorphism then $\mu^{-1}\mu((f+g)(x)) \in \mu^{-1}\mu(I)$, therefore $(f+g)(x) \in I$, i.e;

$$f(x) + g(x) \in I \forall f(x), g(x) \in I. \tag{2.1.3}$$

Let $f(x) \in I$ and $l(x) \in Z_4[x]$, then $f(-x) \in \mu(I)$ and $l(-x) \in Z_4[x]$

now $f(-x).l(-x) \in \mu(I)$ for all $f(-x) \in \mu(I)$, $l(-x) \in Z_4[x]$ because $\mu(I)$ is an ideal $Z_4[x]/(x^n - 1)$. So by definition of μ $\exists$ $f(x) \in I$ and $l(x) \in Z_4$ s.t.

$f(-x).l(-x) = (f.l)(-x) = \mu((f.l)(x)) \in \mu(I)$.

Since μ is is a ring isomorphism then $\mu^{-1}\mu((f.l)(x)) \in \mu^{-1}\mu(I) = I$, therefore $(f.l)(x) \in I$, i.e;

$$f(x).l(x) \in I. \tag{2.1.4}$$

From Equations 2.1.3 and 2.1.4 we have I is an ideal of $Z_4[x]/(x^n - 1)$.

□

Corollary 2.1.4. *[9] Let $\tilde{\mu}$ be the permutation of Z_4 with n odd, such that*
$\tilde{\mu}(a_0, a_1, ..., a_i, ..., a_{n-1}) = (a_0, -a_1, a_2, ..., (-1)^i a_i, ..., (-1)^{n-1} a_{n-1})$.
Let D be a subset of Z_4^n. D is a linear cyclic code if and only if $\tilde{\mu}(D)$ is a linear negacyclic code.

Proof. The proof is obvious if we remark that the action of $\tilde{\mu}$ on vectors is the translation of the action of μ on polynomials, that is, $\tilde{\mu} = P^{-1}\mu P$.

If D is cyclic code over Z_4, then $D(x)$ is an ideal of $Z_4[x]/(x^n-1)$.

If $a = (a_0, a_1, ..., a_{n-1}) \in D$, then $a(x), xa(x), ..., x^{n-1}a(x) \in D(x)$. The polynomial representation of the corespondents D are

$$a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$$
$$xa(x) = xa_0 + a_1x^2 + ... + a_{n-2}x^{n-1} + a_{n-1}x^n$$
$$xa(x) = a_{n-1}x^n + xa_0 + a_1x^2 + ... + a_{n-2}x^{n-1}$$

implies

$$\mu(a(x)) = a_0 - a_1x + a_2x^2 + ... + a_{n-1}(-1)^{n-1}x^{n-1}$$
$$\mu(xa(x)) = a_{n-1}(-x)^n + a_0(-x) + a_1(-x)^2 + ... + a_{n-2}(-1)^{n-1}x^{n-1}$$

The vector representation of $\mu(a(x))$ and $\mu(xa(x))$ are

$P^{-1}\mu(a(x)) = (a_0, -a_1, a_2, ..., (-1)^{n-1}a_{n-1})$ and $P^{-1}\mu(xa(x)) = (-a_{n-1}, -a_0, a_1, -a_2, ...$ $...., (-1)^{n-1}a_{n-2})$. Implies $\tilde{\mu} = P^{-1}\mu P$.

So $(a_0, -a_1, a_2, ..., (-1)^{n-1}a_{n-1}) \in \tilde{\mu}(D)$, $(-a_{n-1}, -a_0, a_1, -a_2, ..., (-1)^{n-1}a_{n-2}) \in \tilde{\mu}(D)$. So $\tilde{\mu}(D)$ is negacyclic code over Z_4.

□

Definition 2.1.4. [9] Let R be a commutative ring and let n be a positive integer .

The quotient ring $A(n) = R[x]/(x^n-1)$ is the set of polynomial

$$\sum_{i=0}^{n-1} r_i x^i$$

of $R[x]$ and calculations are made modulo (x^n-1) with the laws of $R[x]$. We will denote $A(n)$ by $A_2(n)$ if $R = F_2$ and by $A_4(n)$ if $R = Z_4$.

Definition 2.1.5. [9] (**Binary reduction**) If

$$a(x) = \sum_{i=0}^{n-1} a_i x^i \in Z_4[x] \tag{2.1.5}$$

and $a_i = r_i + 2q_i$ with r_i and q_i in F_2, then the F_2-reduction of $a(x)$ is

$$\tilde{a}(x) = \sum_{i=0}^{n-1} r_i x^i. \tag{2.1.6}$$

Remark 2.1.1.

- The $(x^n+1)-$ reduction of $a(x)$ is the image of $a(x)$ by the canonical map of $Z_4[x]$ into $Z_4[x]/(x^n+1)$ by

$$a(x) = \sum_{i=1}^{n} a_i x^i \in Z_4[x] \to a(x) \ \ mod \ \ (x^n+1).$$

- The map $a(x) \longrightarrow \tilde{a}(x)$ and the $(x^n+1)-$reduction are both ring homomorphism.

Corollary 2.1.5. *[9] Let n be odd.*

Every ideal in the ring $Z_4[x]/x^n+1$ is a principle.

Proof.

Let I be an ideal of $Z_4[x]/(x^n+1)$. If $I=0$, then $I=\langle 0\rangle$ is principal. Assume that $I \neq 0$ and we choose a nonzero polynomial $g(x)$ of a nonzero ideal I with the lowest degree. For any polynomial $f(x)$ of I, we have

$$f(x) = s(x)g(x) + r(x)$$

for some polynomial $s(x), r(x) \in Z_4[x]$ with $deg(r(x)) < deg(g(x))$. This forces $r(x) = 0$, since $r(x) = f(x) - s(x)g(x) \in I$ and $g(x)$ has the lowest degree among the nonzero polynomial of I. Hence, $I = \langle g(x)\rangle$. Therefore I is an ideal principle . □

Proposition 2.1.6. *[7] Let Z_4 be a finite commutative ring and*

$$a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$$
$$b(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1} \in Z_4[x].$$

Then $a(x)b(x) = 0$ in $Z_4[x]/(x^n+1)$ if and only if $(a_0, a_1, ..., a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, ..., b_0)$ and all it is negacyclic shifts.

Proof. Let ν denote the negacyclic shift for codewords of length n, i.e., for each $(x_0, x_1, ..., x_{n-1} \in Z_4^n)$

$$\nu(x_0, x_1, ..., x_{n-1}) = (-x_{n-1}, x_0, ..., x_{n-2}) \quad .$$

Thus $\nu^i((b_{n-1}, b_{n-2}, ..., b_0)$, $i = 1, 2, ...2n$, are all negacyclic shift of $(b_{n-1}, b_{n-2}, ..., b_0)$, and

$$(b_{n-1}, b_{n-2}, ..., b_0) = -\nu^{n+j}(b_{n-1}, b_{n-2}, ..., b_0) \quad ,$$

for $j = 0, 1, ..., n$. Let

$c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} = a(x)b(x) \in Z_4[x]/(x^n + 1)$ Then

$c(x) = (a_0 + a_1x + ... + a_{n-1}x^{n-1})(b_0 + b_1x + ... + b_{n-1}x^{n-1})$. Therefore

$c(x) = a_0b_0 + a_0b_1x + ... + a_0b_{n-1}x^{n-1} + a_1b_0x + a_1b_1x^2 + ... + a_1b_{n-1}x^n + a_2b_0x^2 +$

$a_2b_1x^3 + ... + a_2b_{n-1}x^{n+1} + a_{n-1}b_0x^{n-1} + a_{n-1}b_1x^n + ... + a_{n-1}b_{n-1}x^{2n-2}$.

Since $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ then

$c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$,.....,$c_{n-1} = a_0b_{n-1} + a_1b_{n-2} + ... + a_{n-1}b_0$.

Now since $(a_0, a_1, ..., a_{n-1})$ is orthogonal to $(b_{n-1}, b_{n-2}, ..., b_0)$ and all it is negacyclic shifts then

$a_0b_{n-1} + a_1b_{n-2} + ... + a_{n-1}b_0 = 0$. So $c_k = 0$ for all $k = 0, 1, 2, ..., n - 1$.

Therefore, $c(x) = 0$ if and only if $c_k = 0$ for $k = 0, 1, 2, ..., n - 1$ if and only if $(a_0, a_1, ..., a_{n-1}).\nu^{k+1}(b_{n-1}, b_{n-2}, ..., b_0) = 0$ for $k = 0, 1, 2, ..., n - 1$. □

Lemma 2.1.7. *[7] Consider the finite commutative ring Z_4 and C a negacyclic code of length n over Z_4. Then the dual code $C^\perp$ is also a negacyclic code.*

Proof. Let $(x_0, x_1, \ldots, x_{n-1})$ be a codeword of $C^\perp$. For any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ where C is a negacyclic, $(-c_1, -c_2, \ldots, -c_{n-1}, c_0) \in C$. Therefore,

$$(x_0, x_1, \ldots, x_{n-2}, x_{n-1}).(-c_1, -c_2. \ldots, -c_{n-1}, c_0) = 0 \quad .$$

That means

$$-x_0c_1 - x_1c_2 - \ldots - x_{n-2}c_{n-1} + x_{n-1}c_0 = 0 \quad .$$

Whence

$$-x_{n-1}c_0 + x_0c_1 + x_1c_2 + \ldots + x_{n-2}c_{n-1} = 0.$$

Thus,

$$(-x_{n-1}, x_0, x_1, \ldots, x_{n-2}).(c_0.c_1, \ldots, c_{n-1}) = 0.$$

Hence $(-x_{n-1}, x_0, x_1, \ldots, x_{n-2}) \in C^\perp$, and consequently, $C^\perp$ is negacyclic.

□

2.1.2 Gray map and Negacyclic codes

We introduce the fundamental starting point of this subsection which is the fact that, roughly speaking , the Gray map of the negashift is the shift of the Gray map. We denote additions in $F_2, {F_2}^n, {F_2}^{2n}$ and $F_2[x]$ by $\oplus$, while additions in $Z_4, {Z_4}^n$ and $Z_4[x]$ are denote by $+$. We consider ${F_2}^n$ as the subset $\{0,1\}^n$ of ${Z_4}^n$ where 0 or 1 are in Z_4.

Definition 2.1.6. [18] The **Gray map** ϕ from Z_4 to F_2^2

$$\phi : Z_4 \longrightarrow F_2^2$$

is defined by

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

This map is then extended componentwise from Z_4^n to F_2^{2n}

as $$\phi(x_0, x_1, ..., x_{n-1}) = (\phi(x_0), \phi(x_1), ..., \phi(x_{n-1}))$$

We note that ϕ is nonlinear, since $\phi(1+1) \neq \phi(1) + \phi(1)$, because $\phi(2) = 11, \ \ \phi(1) = 01$ and $\phi(1) + \phi(1) = 00$.

If C is a Z_4-linear code, its Gray image will be the binary code denoted by $\phi(C)$.

Example 2.1.2. *Let* $c_1 = 1113$ *then* $\phi(c_1) = \phi(1113) = 01010110$.

And $c_2 = 2002$ *then* $\phi(c_2) = \phi(2002) = 11000011$.

Also, the Gray map can be defined as follows:

Definition 2.1.7. [6] The Gray map ϕ of ${Z_4}^n$ into ${F_2}^{2n}$ is defined by

$$\phi(Z) = (q(Z), q(Z) \oplus r(Z))$$

for all $Z = (z_1, z_2, ..., z_n) \in {Z_4}^n$ and

$$r(Z) = (r(z_1), r(z_2), ..., r(z_n))$$
$$q(Z) = (q(z_1), q(z_2), ..., q(z_n)).$$

That is

$$\phi(Z) = ((q(z_1), ..., q(z_n), q(z_1) \oplus r(z_1), ..., q(z_n) \oplus r(z_n)),$$

where q and r are two maps from Z_4 into F_2 such that if $z \in Z_4$, then the 2-adic expansion of z is $z = r(z) + 2q(z)$.

Remark 2.1.2. we notice that

1. $r(-z) = r(z)$.

2. $q(-z) = r(z) \oplus q(z)$.

Proof. 1. $-z = 4 - z$ where $z \in Z_4 \Rightarrow -z = 4 - (r(z) + 2q(z)) = 4 - r(z) - 2q(z) = -r(z) + 4 - 2q(z) = -r(z) + 2(2 - q(z))$ consequently $r(-z) = -r(z)$.

2. $-z = 4 - z$ where $z \in Z_4 \Rightarrow -z = 4 - (r(z) + 2q(z)) = 4 - r(z) - 2q(z) = -r(z) + 4 - 2q(z) = -r(z) + 2r(z) - 2r(z) + 4 - 2q(z) = r(z) + 4 - 2r(z) - 2q(z) = r(z) + 4 - 2(r(z) + q(z)) = r(z) + 2(r(z) + q(z)$ where $4 - 2(r(z) + q(z)) \in Z_4$, consequently $q(-z) = r(z) \oplus q(z)$.

□

Example 2.1.3. *Let $z = 3$, i.e; $z = 1 + 2.1$, $r(3) = 1$, $q(3) = 1$.*
Now $1 = r(-3) = r(1) = r(3) = 1$ where $1 = 1 + 2.0$, $r(1) = 1$ and $q(1) = 0$.
$0 = q(1) = q(-3) = r(3) \oplus q(3) = 1 + 1 = 0$.

Proposition 2.1.8. *[9] If ν is a negashift of Z_4^n, σ is a cyclic shift of F_2^{2n}, and ϕ is the Gray map of Z_4^n into F_2^{2n}, then*

$$\phi\nu = \sigma\phi.$$

Proof. Let $a = (a_0, a_1, ..., a_i, ..., a_{n-1})$ in Z_4^n. Let r_i and q_i in F_2 such that $a_i = 2q_i + r_i$ where $q_i = q(a_i)$ and $r_i = r(a_i)$. From definiens we obtain that

$$\phi(a) = (q_0, q_1, ..., q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-1} \oplus r_{n-1})$$

and

$$\sigma(\phi(a)) = (q_{n-1} \oplus r_{n-1}, q_0, q_1, ..., q_{n-2}, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-2} \oplus r_{n-2}.) \quad (2.1.7)$$

On the other hand

$$\nu(a) = (-a_{n-1}, a_0, ..., a_i, ...a_{n-2}).$$

We deduce $\phi(\nu(a))$ as

$$\phi(\nu(a)) = (q(-a_{n-1}), q_0, q_1, ..., q_{n-2}, r(-a_{n-1}) \oplus q(-a_{n-1}), q_0 \oplus r_0, ..., q_{n-2} \oplus r_{n-2}) \quad (2.1.8)$$

From Remark 2.1.2 we have

$$q(-a_{n-1}) = q(a_{n-1}) \oplus r(a_{n-1}) = q_{n-1} \oplus r_{n-1} \tag{2.1.9}$$

$$r(-a_{n-1}) \oplus q(-a_{n-1}) = q(a_{n-1}) = q_{n-1}. \tag{2.1.10}$$

Now from Equations 2.1.8 , 2.1.9 and 2.1.10 we have

$$\phi(\nu(a)) = (q_{n-1} \oplus r_{n-1}, q_0, q_1, ..., q_{n-2}, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-2} \oplus r_{n-2}) \tag{2.1.11}$$

Now, from Equations 2.1.7 and 2.1.11 we have

$$\phi\nu = \sigma\phi.$$

□

Definition 2.1.8. [16] A code is **distance invariant** if for any pair of codewords c_1 and c_2, the number of codewords distance i from c_1 equals the number of codewords distance i from c_2 for $1 \leq i \leq n$.

Theorem 2.1.9. *[9] The Gray map of a linear negacyclic code over Z_4 is a binary-distance-invariant cyclic code.*

Proof. Let C be a linear negacyclic code over Z_4. Then $\nu(C) = C$ and, therefore, $(\phi\nu)(C) = \phi(C)$. It follows from Proposition 2.1.8 that $\sigma(\phi(C)) = \phi(C)$ which means that $\phi(C)$ is acyclic code. On the other hand, this code is binary-distance-invariant from Proposition 2.1.8. □

Definition 2.1.9. [9] Let τ be the following permutation of $\{0, 1, \ldots, 2n-1\}$:

$$\tau = (1, n+1)(3, n+3)\ldots(2i+1, n+2i+1)\ldots(n-2, 2n-2).$$

The **Nechaev permutation** is the permutation τ of F_2^2 defined by:

$$\tau(a_0, a_1, \ldots, a_i, \ldots, a_{i-1}) = (a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{\tau(i)}, \ldots, a_{\tau(i-1)}).$$

Proposition 2.1.10. *[9] Assume n is odd number. Let μ be the map of $Z_4[x]/(x^n - 1)$ into $Z_4[x]/(x^n + 1)$ defined by*

$$\mu(a(x)) = a(-x).$$

Let $\tilde{\mu}$ be the permutation of Z_4^n such that

$$\tilde{\mu}(a_0, a_1, \ldots, a_i, \ldots, a_{n-1}) = (a_0, -a_1, \ldots, (-1)^i a_i, \ldots, (-1)^{n-1} a_{n-1}).$$

If π is the Necheav permutation and if ϕ is the Gray map Z_4^n into F_2^{2n} then

$$\phi\tilde{\mu} = \pi\phi.$$

Proof. Let $a = (a_0, a_1, \ldots, a_i, \ldots, a_{n-1})$ be in Z_4^n. From the definition of the permutation $\tilde{\mu}$ we have

$$(\tilde{\mu})(a) = (a_0, -a_1, \ldots, (-1)^i a_i, \ldots, (-1)^{n-1} a_{n-1})$$

and by Remark 2.1.2, it follows that, if

$$(\phi\tilde{\mu})(a) = (s_0, s_1, \ldots, s_{n-1}, s_n, \ldots, s_{2n-1}) \tag{2.1.12}$$

then for $0 \leq j \leq n-1$:

$$if \quad j \quad even : s_j = q_j, s_{n+j} = q_j \oplus r_j \tag{2.1.13}$$

$$if \quad j \quad odd : s_j = q_j \oplus r_j, s_{n+j} = q_j. \tag{2.1.14}$$

Now from Equations 2.1.12, 2.1.13 and 2.1.14 we have

$$(\phi\tilde{\mu})(a) = (q(a_0), q(-a_1) \oplus r(-a_1), q(a_2), q(-a_3) \oplus r(-a_3), \ldots, q(a_{n-1}), q(-a_n) \oplus r(-a_n)).$$

By Remake 2.1.2 we have

$$(\phi\tilde{\mu})(a) = (q_0, q_1, q_2, q_3, \ldots, q_{n-1}, q_n) \tag{2.1.15}$$

On the other hand

$$\phi(a) = (q_0, q_1, ..., q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-1} \oplus r_{n-1}).$$

By the Nechaev permutation π we have

$$\pi(\phi(a)) = (q_{\tau(0)}, q_{\tau(1)}, \ldots, q_{\tau(n-1)}, q_{\tau(0)} \oplus r_{\tau(0)}, q_{\tau(1)} \oplus r_{\tau(1)}, \ldots, q_{\tau(n-1)} \oplus r_{\tau(n-1)}).$$

□

2.2 Negacyclic codes of length 2^t over Z_{2^m}

In this section, we will use an approach different from the one in last subsection to obtain the structure of negacyclic codes of length $2^t (t \leq 1)$ over Z_{2^m} for any integer $m \geq 2$. We start our discussion with a couple of observations.

Definition 2.2.1. [7] A polynomial $f \in R[x]$ is called **invertible** if it is not a zero divisor.

Lemma 2.2.1. *[7] For any positive integer n, there exists a polynomial $\alpha_n(x) \in Z[x]$ such that $(x+1)^{2^n} = x^{2^n} + 1 - 2\alpha_n(x)$, and $2 \nmid \alpha_n[x]$ in $Z[x]$. Furthermore, $\alpha_n[x]$ is invertible in $Z_{2^m}[x]/(x^{2^t}+1)$.*

Proof. We will show that by induction on n.

1. For $n = 1$,
   $(x+1)^2 = x^2 + 1 - 2\alpha_1(x)$, $\alpha_1(x) = -x$ and does not divides $\alpha_1(x)$ in $Z[x]$.

2. Now assume $n > 1$ and suppose the statement is true for all positive integer less than n. i.e,
   $(x+1)^{2^{n-1}} = x^{2^{n-1}} + 1 - 2\alpha_{n-1}(x)$, and $2 \nmid \alpha_{n-1}(x)$ in $Z[x]$.

3. Now we show that the statement is true for n
   $$\begin{aligned}(x+1)^{2^n} &= (x+1)^{22^{n-1}} = [(x+1)^{2^{n-1}}]^2 = [x^{2^{n-1}} + 1 - 2\alpha_{n-1}(x)]^2 \\ &= (x^{2^{n-1}})^2 + 2x^{2^{n-1}} + 1 + 4\alpha_{n-1}^2(x) - 2(x^{2^{n-1}}+1)2\alpha_{n-1}(x). \\ &= x^{2^n} + 2x^{2^{n-1}} + 1 + 4\alpha_{n-1}^2(x) - 4\alpha_{n-1}(x)(x^{2^{n-1}}+1) \\ &= x^{2^n} + 2x^{2^{n-1}} + 1 + 4\alpha_{n-1}^2(x) - 4\alpha_{n-1}(x)x^{2^{n-1}} + 4\alpha_{n-1}(x) \\ &= x^{2^n} + 1 - 2(x^{2^{n-1}} - 2\alpha_{n-1}^2(x) + 2\alpha_{n-1}(x)x^{2^{n-1}} + 2\alpha_{n-1}(x)).\end{aligned}$$
   and $2 \nmid \alpha_n(x)$. Since x invertible in $Z_{2^m}[x]/(x^{2^t}+1)$, $x^{2^{n-1}}$ is also invertible in $Z_{2^m}[x]/(x^{2^t}+1)$, .
   Therefore, as 2 is nilpotent in $Z_{2^m}[x]/(x^{2^t}+1)$, we can write $\alpha_n(x)$ as
   $x^{2^{n-1}}(1+z)$, where z is a nilpotent element in $Z_{2^m}[x]/(x^{2^t}+1)$.

   Now let ξ be an odd integer such that $z^\xi = 0$. We have

$$1 = 1 + z^{\xi} = (1 + z)(1 - z + z^2 - \ldots + z^{\xi-1}).$$

That means, $(1 + z)$ is invertible in $Z_{2^m}[x]/(x^{2^t} + 1)$.

Hence $\alpha_n(x)$ is invertible in $Z_{2^m}[x]/(x^{2^t} + 1)$.

□

Lemma 2.2.2. *[7] Let P be a prime number, and n, k be positive integers with $k \geq 2$, and $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z_{P^k}[x]$, $(a_0, a_1, \ldots, \ a_n \in \{0, 1, \ldots, P^k - 1\}, a_n \neq 0)$.*

If in Z, $P|a_0, P|a_1, \ldots, P|a_{n-1}, P \nmid a_n, P^2 \nmid a_0$, then $f(x)$ is irreducible in $Z_{P^k}[x]$.

Proof. Suppose, on the contrary, that $f(x)$ is reducible, i.e.,

$$f(x) = (b_0 + b_1x + \ldots + b_rx^r)(c_0 + c_1x + \ldots + c_sx^s),$$

where $(b_0+b_1x+\ldots+b_rx^r)$ and $(c_0+c_1x+\ldots+c_sx^s)$ are both non invertible polynomials in $Z_{P^k}[x]$. Since $(b_0 + b_1x + \ldots + b_rx^r)$ and $(c_0 + c_1x + \ldots + c_sx^s)$ are proper divisors of $f(x)$ in $Z_{P^k}[x]$, the redaction modulo P of $(b_0+b_1x+\ldots+b_rx^r)$ and $(c_0+c_1x+\ldots+c_sx^s)$ must be proper divisor of the reduction modulo P of $f(x)$ over $Z_{P^k}[x]$. It follows that $P|b_i$ and $P|c_i$ for every $i \geq n$. On the other hand,

$a_0 \equiv b_0c_0(mod \ \ P^k)$ and

$$a_n \equiv \sum_{i+j=n} b_ic_j(mod \ \ P^k).$$

By hypothesis, $P|b_0c_0$ and $P^2 \nmid b_0a_0$. It follows that either $P|b_0$ and $P \nmid c_0$ or $P \nmid b_0$ and $P|c_0$.

Without loss of generality, assume that $P|b_0$ and $P \nmid c_0$. Since $P \nmid a_n$, we have $P \nmid \sum_{i+j=n} b_ic_j$.

Hence, there exists L, necessarily less that n, such that $P \nmid b_L$. Let b_d be the first coefficient in $b_0 + b_1x + \ldots + b_rx^r$ such that $P \nmid b_d$. As $a_d \equiv b_dc_0 + b_{d-1}c_1 + \ldots + b_0c_d \ \ (\ \ mod \ \ p^k)$. We have $P \nmid b_d$. Thus, $d = n$, which is a contradiction. Therefore $f(x)$ is irreducible in $Z_{P^k}[x]$. □

2.2.1 Galois rings

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 if its reduction modulo p is irreducible.

Definition 2.2.2. 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 2.2.1.

- $GR(p, m) = F_{p^m}, \quad GR(p^s, 1) = Z_{p^s}$.
- *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 $GR(2^2, 3) = Z_4[x]/\langle g(x)$.*

Notation 2.2.3. *Every element $f(x) \in Z_{2^m}[x]/(x^{2^t} + 1)$ can be viewed as a polynomial with degree less than or equal to 2^t-1 in $Z_{2^m}[x]$. In words, there exist $b_0, b_1x, \ldots, b_{2^t-1}x^{2^t-1}x^{2t-1}-$ such that*

$$f(x) = b_0 + b_1x + \ldots + b_{2^t-1}$$

For $i = 0, \ldots, 2^t - 1$, each b_i has a unique binary representation

$$b_i = b_{i0} + 2b_{i1} + \ldots + 2^{m-1}b_{i(m-1)}$$

where $b_{ik} \in \{0, 1\}$ $(k = 0, 1, \ldots, m - 1)$. Hence, $f(x)$ can be written as

$$f(x) = f_0(x) + 2f_1(x) + \ldots + 2^{m-1}f_{m-1}(x)$$

where $f_j(x) \in Z_2[x]$, $0 \le j \le m - 1$. Furthermore, x can be represented as

$$x = (x + 1) + (2^m - 1) = (x + 1) + (1 + 2 + 2^2 + \ldots + 2^{m-1}).$$

Consequently, $f(x)$ can be written(uniquely) as

$$f(x) = \sum_{j=0}^{2^t-1} a_{0j}(x + 1)^j + 2\sum_{j=0}^{2^t-1} a_{1j}(x + 1)^j + \ldots + 2^{m-1}\sum_{j=0}^{2^t-1} a_{(m-1)j}(x + 1)^j$$

where $a_{ij} \in Z_2$, $0 \le j \le m - 1$, $0 \le j \le 2^t - 1$.

Example 2.2.2. *Let $t = 1$, $m = 2$ in Notation 2.2.3 for all polynomials $f(x) \in Z_4[x]/(x^2+1)$,*

$$f(x) = \sum_{j=0}^{1} a_{0j}(x+1)^j + 2\sum_{j=0}^{1} a_{1j}(x+1)^j.$$

So

$f(x) = a_{00}(x+1)^0 + a_{01}(x+1) + 2[a_{10}(x+1)^0 + a_{11}(x+1)]$,

$f(x) = a_{00} + a_{01}(x+1) + 2[a_{10} + a_{11}(x+1)]$, *where* $a_{00}, a_{01}, a_{10}, a_{11} \in Z_2[x]$,

$f(x) = f_0(x) + 2f_1(x)$ *where* $f_0(x) = a_{00} + a_{01}(x+1)$, $f_1(x) = a_{10} + a_{11}(x+1)$.

Now we will write all polynomials $f(x) \in Z_4[x]/(x^2+1)$ in the following table

$f(x)$	$f_0(x)$	$f_1(x)$	$f(x) = f_0(x) + 2f_1(x)$
0	*0*	*0*	*[0]+2[0]*
1	*1*	*0*	*[1]+2[0]*
2	*0*	*1*	*[0]+2[1]*
3	*1*	*1*	*[1]+2[1]*
x	*1+(x+1)*	*1*	*[1+(x+1)]+2[1]*
x+1	*x+1*	*0*	*[x+1]+2[0]*
x+2	*1+(x+1)*	*0*	*[1+(x+1)]+2[0]*
x+3	*x+1*	*1*	*[x+1]+2[0]*
2x	*0*	*1+(x+1)*	*[0]+2[1+(x+1)]*
2x+1	*1*	*1+(x+1)*	*[1]+2[1+(x+1)]*
2x+2	*0*	*x+1*	*[0]+2[x+1]*
2x+3	*1*	*x+1*	*[1]+2[x+1]*
3x	*1+(x+1)*	*x+1*	*[1+(x+1)]+2[x+1]*
3x+1	*x+1*	*1+(x+1)*	*[x+1]+2[1+(x+1)]*
3x+2	*1+(x+1)*	*1+(x+1)*	*[1+(x+1)]+2[1+(x+1)]*
3x+3	*x+1*	*x+1*	*[x+1]+2[x+1]*

Theorem 2.2.4. *[7] The negacyclic codes of length 2^t over Z_{2^m} (i.e, the ideals of $f(x) \in Z_{2^m}[x]/(x^{2^t}+1)$), are precisely*

$$\langle 1\rangle = \langle (x+1)^0\rangle, \langle (x+1)\rangle, \langle (x+1)^2\rangle, \ldots, \langle (x+1)^{m_0-1}\rangle, \langle (x+1)^{m_0}\rangle = \langle 0\rangle$$

where $m_0 = m2^t$ is the nilpotency of $(x+1)$ in $f(x) \in Z_{2^m}[x]/(x^{2^t}+1)$.

Proof. See [7]

□

Proposition 2.2.5. *[7] The number of codewords in any linear code C of length n over Z_{p^m} is p^k, for some integer $k \in \{0, 1, 2, \ldots, mn\}$. Moreover, the dual code $C^\perp$ has p^l codewords, where $k + l = mn$.*

Proof. See [7]

□

Proposition 2.2.6. *[7] For $i \in \{0, 1, \ldots, 2^t m\}$, there are $2^{2^t m - i}$ codewords in the negacyclic code $\langle (x+1)^i\rangle$.*

Proof. The chain of $(2^t m + 1)$ ideals $\langle (x+1)^i\rangle$ $(i = 0, 1, \ldots, 2^t m)$ of $Z_{2^m}[x]/\langle x^{2^t}+1\rangle$ is a strictly decreasing chain

$$\langle 1\rangle = \langle (x+1)^0\rangle \supsetneq \langle (x+1)\rangle \supsetneq \langle (x+1)^2\rangle \supsetneq \ldots \supsetneq \langle (x+1)^{m_0-1}\rangle \supsetneq \langle (x+1)^{m_0}\rangle = \langle 0\rangle$$

by Proposition 2.2.5, each of these ideals has order 2^k for some integer $k \in \{0, 1, \ldots, 2^t m\}$. Now there are precisely $(2^t m + 1)$ such that orders and furthermore

$$2^{2^t m} > 2^{2^t m - 1} > \ldots > 2^1 > 2^0.$$

Therefore, for $i \in \{0, 1, \ldots, 2^t m\}$,

$$| \langle (x+1)^i\rangle | = 2^{2^t m - i}.$$

□

Example 2.2.3. *Consider negacyclic codes of length 4 over Z_4(t=2, m=2).*
Now by Theorem 2.2.4, $m_0 = m2^t = 2.2^2 = 8$. Hence the negacyclic codes of length 4 over Z_4 are

$$\langle 0\rangle, \langle 1\rangle, \langle (x+1)\rangle, \ldots, \langle (x+1)^7\rangle$$

Let $i = 0$. Then the generator is $\langle (x+1)^0 \rangle$. By Proposition 2.2.6, the order of the code equal $2^{2^t m-0} = 2^{2^2 2-0} = 2^{8-0} = 2^8$. Similarly for $i = 1$, the generator is $\langle (x+1) \rangle$ and the order of the code equal $2^{2^t m-1} = 2^{2^2 2-1} = 2^{8-1} = 2^7$.

Now this table contain on all generators of the codes of length 4 over Z_4 and their orders.

i	generator of the code	order of the code
0	$(x+1)^0$	$2^8 = 256$
1	$(x+1)^1 = x+1$	$2^7 = 128$
2	$(x+1)^2 = x^2+2x+1$	$2^6 = 64$
3	$(x+1)^3 = x^3+3x^2+3x+1$	$2^5 = 32$
4	$(x+1)^4 = 2x^2$	$2^4 = 16$
5	$(x+1)^5 = 2x^3+2x^2$	$2^3 = 8$
6	$(x+1)^6 = 2x^2+2$	$2^2 = 4$
7	$(x+1)^7 = 2x^3+2x^2+2x+2$	$2^1 = 2$
8	$(x+1)^8 = 0$	$2^0 = 1$

Theorem 2.2.7. *[7] Let C be a negacyclic code of length 2^t over Z_{2^m}. Then for some $i \in \{0, 1, \ldots, 2^t m\}$ and $(x+1)^i$ is calculated modulo $(x^{2^t}+1)$, the followings hold:*

1. *$C = \langle (x+1)^i \rangle$, $\mid C \mid = 2^{2^t m-i}$.*
2. *$C^\perp = \langle (x+1)^{2^t m-i} \rangle$, $\mid C^\perp \mid = 2^i$.*

Proof. 1. By Theorem 2.2.4 and Proposition 2.2.6 we get on the result.

2. By Proposition 2.2.5 the dual $C^\perp$ is p^l when $k+l = mn$, k order of C and length of C is 2^t by (1)we see $\mid C \mid = 2^{2^t m-i}$ implies $k = 2^t m - i$

   $\therefore k + l = mn \rightarrow 2^t m - i + l = 2^t m \rightarrow l = i$. so,

   $$\mid C^\perp \mid = 2^l = 2^i.$$

   Moreover by Lemma 2.1.7, $C^\perp$ is also negacyclic code, and so Proposition 2.2.6 implies that

   $$C^\perp = \langle (x+1)^{2^t m-i} \rangle.$$

□

Corollary 2.2.8. *[7]* $C = \langle (x+1)^{2^{t-1}m} \rangle$ *is the only self-dual negacyclic code of length* 2^t *over* Z_2^m.

Proof. Let C be a self-dual negacyclic code of length 2^t over Z_2^m. Then, by Theorem 2.2.7, $C = \langle (x+1)^i \rangle$ and $C^\perp = \langle (x+1)^{2^t m - i} \rangle$ for some $i \in \{0, 1, \ldots, 2^t m\}$. Self-duality of C forces $i = 2^t m - i$, i.e, $i = 2^{t-1} m$, as desired.

□

Chapter 3

Constacyclic codes over the finite chain rings $F_2 + uF_2$ and $F_2 + uF_2 + u^2F_2$

In this chapter We study constacyclic code over $R_2 = F_2 + uF_2$ and $R_3 = F_2 + uF_2 + u^2F_2$, we study some definitions and propositions about constacyclic codes, some constacyclic codes over Z_{2^k}, binary quasi-cyclic codes and Hpo-cyclic codes.

3.1 Introduction

In this section we will study some definitions and notes about $\beta - constacyclic$ and t-quasi-cyclic codes.

Definition 3.1.1. [13] A code is **β-constacyclic** if for every code word $(a_0, a_1, \ldots, a_{n-1})$, the constacyclic shifted vector by positions, $(\beta a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also a codeword, where β is an element of $F_q^* \backslash \{0\}$. These are the ideals in the ring $F_q[x]/(x^n - \beta)$.

Notation 3.1.1. *When $\beta = 1$, the code is called cyclic code.*

Notation 3.1.2. *When $\beta = -1$, the code is called negacyclic code.*

Definition 3.1.2. [13] A code is **t-quasi-cyclic** if for every codeword $(a_0, a_1, \ldots, a_{n-1})$, the cyclically shifted vector by t position, $(a_{n-t}, \ldots, a_{n-1}, a_0, a_1, \ldots, a_{n-t-1})$ is also a codeword.

Let σ be the usual shift on F_2^{2n} and $Z_{2^{k+1}}^n$. For any positive t, let ψ_t be the quasi-shift on $(F_2^{2n})^t$ and δ_t be the quasi-negashift on (Z_4^n) given by:

$$\psi_t(a^{(1)}|a^{(2)}|\ldots|a^{(t)}) = \sigma(a^{(1)})|\sigma(a^{(2)})|\ldots|\sigma(a^{(t)})),$$
$$\delta_t(\tilde{a}^{(1)}|\tilde{a}^{(2)}|\ldots|\tilde{a}^{(t)}) = \nu(\tilde{a}^{(1)})|\nu(\tilde{a}^{(2)})|\ldots|\nu(\tilde{a}^{(t)})),$$

where $a^{(i)} \in F_2^{2n}$, $\tilde{a}^{(i)} \in Z_4^n$, for $i = 1, 2, \ldots, t$ and "|" denotes the usual vector concatenation.

Notation 3.1.3. *When $t = 1$, this is code called cyclic code.*

3.2 $(1+u)-$Constacyclic codes over $F_2 + uF_2$

In this subsection we will prove that a subset C of R_3^n is a linear $(1+u)$- constacyclic of length n if and only if its polynomial representation is an ideal of $R_2[x]/(x^n - (1+u))$ and we will prove the Gray image of a linear $(1+u)$-constacyclic code over $F_2 + uF_2$ of length n is a binary distance invariant linear cyclic code.

Definition 3.2.1. [10] Let $R_2 = F_2 + uF_2$. A code of length n over R_2 is $(1+u)$-constacyclic if the code is invariant under Automorphism ν which has

$$\nu(a_0, a_1, \ldots, a_{n-1}) = ((1+u)a_{n-1}, a_0, \ldots, a_{n-2})$$

Proposition 3.2.1. *[10] A subset C of R^n is a linear $(1+u)$ constacyclic of length n if and only if its polynomial representation is an ideal of $R_2[x]/(x^n - (1+u))$.*

Proof. $\leftarrow$ Suppose that $\pi(C)$ is an ideal of $R_2[x]/(x^n - (1+u))$. Then for any $\alpha, \beta \in R_2^n \subset R_2[x]/(x^n - (1 - (1+u))$ and $a, b \in C$, we have $\alpha\pi(a), \beta\pi(b) \in \pi(C)$ by definition 1.1.6 part (2). Thus by Definition 1.1.6 part (1), $\alpha\pi(a) + \beta\pi(b)$ is an element of $\pi(C)$, i.e; $\alpha\pi(a) + \beta\pi(b) = \pi(\alpha a + \beta b) \in \pi(C)$, hence $\alpha(a) + \beta(b)$ is codeword of C. This shows that C is a linear code. Now let $c = (c_0, c_1, \ldots, c_{n-1})$ be a codeword of C then The polynomial representation of C is

$$\pi(c) = (c_0 + c_1x + \ldots + c_{n-1}x^{n-1})$$

is an element of $\pi(C)$. Since $\pi(C)$ is an ideal of $R_2[x]/(x^n - (1+u))$ then the element

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

But $\pi(C)$ is ideal in $R_2[x]/(x^n - (1+u))$ and since $x^n - (1+u) = 0 \Rightarrow x^n = (1+u)$,

$$\begin{aligned} then \;\; x\pi(c) &= c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1} + c_{n-1}(1 - (1+u)) \\ &= (1+u)c_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1} \end{aligned}$$

is in $\pi(C)$, i.e; $((1+u)c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is codeword of C. This mean that C is $(1+u)$-constacyclic codes.

Conversely, suppose that C is $(1+u)$-constacyclic code over R . Then part (1) of Definition 1.1.6 is satisfied for $\pi(C)$. For any polynomial

$$f(x) = f_0 + f_1x + \ldots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1} = \pi(f_0, f_1, \ldots, f_{n-2}, f_{n-1})$$

of $\pi(C)$ with $(f_0, f_1, \ldots, f_{n-1}) \in C$, the polynomial

$$xf(x) = x^nf_{n-1} + f_0x + f_1x^2 + \ldots + f_{n-2}x^{n-1} = (1+u)f_{n-1} + f_0x + f_1x^2 + \ldots\ldots + x^{n-1}f_{n-2}$$

is also an element of $\pi(C)$ since C is $(1+u)-$constacyclic. Thus, $x^2f(x) = x(xf(x))$ is an element of $\pi(C)$. By induction, suppose that $x^jf(x)$ belongs to $\pi(C)$ for all $j \geq 0$. Since C is a linear code and π is a linear transformation, $\pi(C)$ is a module over R_2. Hence, for any $g(x) = g_0 + g_1x + \ldots + g_{n-1}x^{n-1} \in R_2[x]/(x^n - (1+u))$, the polynomial

$$g(x)f(x) = \textstyle\sum_{i=0}^{n-1} g_i(x^if(x))$$

is an element of $\pi(C)$. Therefore, $\pi(C)$ is an ideal of $R_2[x]/(x^n - (1+u))$ since part (2) of the Definition 1.1.6 is also satisfied.

□

Definition 3.2.2. [10] Let R_2 be the commutative ring $F_2 + uF_2$. Any element $z \in R_2$ can be expressed as $z = r + uq$, where r, q are in F_2. The Gray map $\phi : R_2 \longrightarrow F_2$ is given by

$$\phi(z) = (q, q + r).$$

This map can be extended to R_2^n in a natural way. For $z = (z_1, z_2, \ldots, z_n) \in R_2^n$, ϕ is extended to R_2^n as follows:

$$\phi : R_2^n \longrightarrow F_2^{2n}$$

$$(z_1, z_2, \ldots, z_n) \longrightarrow (q_1, q_2, \ldots, q_n, q_1 \oplus r_1, \ldots, q_n \oplus r_n)$$

where $z_i = r_i + uq_i$, for $1 \leq i \leq n$ and where $\oplus$ is the binary addition.

Example 3.2.1. $\phi(1) = 01 \qquad q = 0, r = 1$

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

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

$\phi(1+u) = 10 \qquad q = 1, r = 1$

Notation 3.2.2. $(1+u)^n = 1 + u \qquad$ *if n is odd.*

$(1+u)^n = 1 \qquad$ *if n is even.*

3.2.1 $(1+u)-$Constacyclic codes of odd length

In this subsection, we will study some propositions that study $(1+u)-$Constacyclic codes of odd length.

Proposition 3.2.3. *[10] Let μ be the map of $R_2[x]/(x^n - 1)$ into $R_2[x]/(x^n - (1+u))$ defined by:*

$$\mu(f(x)) = f((1+u)x).$$

If n is odd, then μ is ring isomorphism.

Proof. First we will show that μ is a ring homomorphism.

For the polynomials $f(x), g(x) \in R_2[x]/(x^n - 1)$, $\mu(f(x) + g(x)) = \mu((f+g)(x)) = (f+g)((1+u)x)) = f((1+u)x)) + g((1+u)x))$

$$= \mu(f(x)) + \mu(g(x)).$$

And $\mu(f(x)g(x)) = \mu((fg)(x)) = (fg)((1+u)x) = f((1+u)x)g((1+u)x).$

$$= \mu(f(x))\mu(g(x)).$$

Therefore μ is a ring homomorphism.

Now we will show μ is one to one. For the polynomials $f(x), g(x) \in R_2[x]$, $f(x) \equiv g(x) mod\ \ (x^n - 1)$ if and only if there exists a polynomial $h(x) \in R_2[x]$ such that $f(x) - g(x) = h(x)(x^n - 1)$ if and only if n is odd and $f((1+u)x) - g((1+u)x) = h((1+u)x)((1+u)x)^n - 1)$, if and only if

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

$$= h((1+u)x)(x^n - (1+u))$$

if and only if

$$(1+u)(\mu(f(x)) - \mu(g(x))) = h((1+u)x)(x^n - (1+u))$$

if and only if

$$(\mu(f(x)) - \mu(g(x))) = (1+u)h((1+u)x)(x^n - (1+u))$$

if and only if

$$\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (1+u))).$$

That means, for $f, g \in R_2[x]/(x^n - 1)$, $\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (1+u)))$ if and only if $f(x) \equiv g(x)(\text{mod } (x^n - 1))$. This implies that μ is a one to one homomorphism.
To show μ is onto, let $f(x) \in R_2[x]/(x^n - (1+u))$. Then there exists $f((1+u)x) \in R_2[x]/(x^n - 1)$ such that $\mu(f((1+u)x)) = f((1+u)^2 x) = f(x)$. Thus μ is onto.

Therefore, μ is a ring isomorphism. □

Example 3.2.2. *Let $n = 7$.*

$$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } R_2[x] \quad ,$$

by the ring isomorphism μ

$(1+u)^7 x^7 + 1 = ((1+u)x + 1)((1+u)^3 x^3 + (1+u)x + 1)((1+u)^3 x^3 + (1+u)^2 x^2 + 1)$

by Notation 3.2.2 we have

$(1+u)x^7 + 1 = ((1+u)x + 1)((1+u)x^3 + (1+u)x + 1)((1+u)x^3 + x^2 + 1)$

$(1+u)(x^7 + (1+u)) = (1+u)(x + (1+u))(1+u)(x^3 + x + (1+u))(1+u)(x^3 + (1+u)x^2 + (1+u))$

$(1+u)(x^7 + (1+u)) = (1+u)^3(x + (1+u))(x^3 + x + (1+u))(x^3 + (1+u)x^2 + (1+u))$

$(1+u)(x^7 + (1+u)) = (1+u)(x + (1+u))(x^3 + x + (1+u))(x^3 + (1+u)x^2 + (1+u))$

dividing by $(1+u)$, we have

$$x^7 + (1+u) = (x + (1+u))(x^3 + x + (1+u))(x^3 + (1+u)x^2 + (1+u))$$

Example 3.2.3. *Let $n = 9$.*

$$x^9 + 1 = (x+1)(x^2 + x + 1)(x^6 + x^3 + 1) \text{ in } R_2[x] \quad ,$$

by the ring isomorphism μ,

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

by Notation 3.2.2 we have

$(1+u)x^9+1 = ((1+u)x+1)(x^2+(1+u)x+1)(x^6+(1+u)x^3+1)\ (1+u)(x^9+(1+u)) =$
$(1+u)(x+(1+u))(x^2+(1+u)x+1)(x^6+(1+u)x^3+1)$

dividing by $(1+u)$, *we have*

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

Corollary 3.2.4. *[10] I is an ideal of $R_2[x]/(x^n-1)$ if and only if $\mu(I)$ is an ideal of $R_2[x]/(x^n-(1+u))$.*

Proof. Suppose I is an ideal of $R_2[x]/(x^n-1)$. Let $f((1+u)x), g((1+u)x) \in \mu(I)$.
Now $f(x)+g(x) \in I$ for all $f(x)$, $g(x) \in I$ since I is ideal. So, by the definition of μ we have, $\mu(f(x)+g(x)) \in \mu(I)$, but $\mu(f(x)+g(x)) = \mu((f+g))(x) = (f+g)((1+u)x) = f((1+u)x)+g((1+u)x) \in \mu(I)$, this implies that

$$f((1+u)x)+g((1+u)x) \in \mu(I) \tag{3.2.1}$$

Now let $f((1+u)x), l((1+u)x) \in \mu(I)$. Since $f(x).l(x) \in I$ for all $f(x) \in I$, $l(x) \in R_2[x]$, by the definition of μ we have

$\mu(f(x).l(x)) \in \mu(I)$. But $\mu(f(x).l(x)) = \mu((f.l)(x)) = (f.l)((1+u)x) = f((1+u)x).l((1+u)x) \in \mu(I)$. So

$$f((1+u)x).l((1+u)x) \in \mu(I). \tag{3.2.2}$$

From Equation 3.2.1 and Equation 3.2.2 we have $\mu(I)$ is an ideal of $R_2[x]/(x^n-(1+u))$.
Conversely suppose $\mu(I)$ is an ideal of $R_2[x]/(x^n-(1+u))$. Let $f(x), g(x) \in I$.
Now $f((1+u)x)+g((1+u)x) \in \mu(I)$ for all $f((1+u)x), g((1+u)x) \in \mu(I)$ because $\mu(I)$ is an ideal of $R_2[x]/(x^n-(1+u))$. So by the definition of μ we have

$f((1+u)x)+g((1+u)x) = (f+g)((1+u)x) = \mu((f+g)x) \in \mu(I)$.

Since μ is a ring isomorphism, then $\mu^{-1}\mu((f+g)x) \in \mu^{-1}\mu(I)$. Therefore $(f+g)(x) \in I$, i.e;

$$f(x)+g(x) \in I \tag{3.2.3}$$

Let $f(x) \in I$ and $l(x) \in R[x]$.

Now $f((1+u)x).l((1+u)x) \in \mu(I)$ for all $f((1+u)x), l((1+u)x) \in \mu(I)$ where $\mu(I)$ is ideal. So by the definition of μ we have

$f((1+u)x).l((1+u)x) = (f.l)((1+u)x) = \mu((f.l)x) \in \mu(I)$.

Since μ is a ring isomorphism then $\mu^{-1}\mu((f.l)x) \in \mu^{-1}\mu(I)$. Therefore $(f.l)(x) \in I$, i.e;

$$f(x).l(x) \in I. \tag{3.2.4}$$

From Equations 3.2.3 and 3.2.4 we have I is an ideal of $R_2[x]/(x^n - 1)$.

□

Corollary 3.2.5. *[10] Let $\tilde{\mu}$ be the permutation of R_2^n with n odd, such that*

$\tilde{\mu}(a_0, a_1, \ldots, a_{n-1}) = (a_0, (1+u)a_1, (1+u)^2 a_2, \ldots, (1+u)^i a_i, \ldots, (1+u)^{n-1} a_{n-1})$,

and let D be a subset of R_2^n. Then D is a linear cyclic code if and only if $\tilde{\mu}(D)$ is a linear (1+u)-constacyclic code.

Proof. Let $R_2 = F_2 + uF_2$, the proof is obvious if we remark that the action of $\tilde{\mu}$ on vectors is the translation of the action of μ on polynomials, that is, $\tilde{\mu} = P^{-1}\mu P$.

If D is a cyclic code over $R_2[x]$, then $D(x)$ is an ideal of $R_2[x]/(x^n - (1+u))$.

If $a = (a_0, a_1, ..., a_{n-1}) \in D$, then $a(x), xa(x), ..., x^{n-1}a(x) \in D(x)$. The polynomial representation of the corespondents D are

$$a(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1}$$
$$xa(x) = xa_0 + a_1 x^2 + ... + a_{n-2}x^{n-1} + a_{n-1}x^n$$
$$xa(x) = a_{n-1}x^n + xa_0 + a_1 x^2 + ... + a_{n-2}x^{n-1}$$

implies

$$\mu(a(x)) = a_0 + (1+u)a_1 x + (1+u)^2 a_2 x^2 + ... + a_{n-1}(1+u)^{n-1}x^{n-1}$$
$$\mu(xa(x)) = a_{n-1}((1+u)x)^n + a_0((1+u)x) + a_1((1+u)x)^2 + ... + a_{n-2}(1+u)^{n-1}x^{n-2}$$
$$\mu(xa(x)) = a_{n-1}(1+u)^n x^n + a_0((1+u)x) + a_1 x^2 + ... + a_{n-2}x^{n-1}$$

If P is a map from $R_2^n \longrightarrow R_2[x]$ such that $P(a_0, a_1, ..., a_{n-1}) = \sum_{i=0}^{n-1} a_i x^i$ then the vectors representation of $\mu(a(x))$ and $\mu(xa(x))$ are

$P^{-1}\mu(a(x)) = (a_0, (1+u)a_1, a_2, ..., a_{n-1})$ and $P^{-1}\mu(xa(x)) = ((1+u)a_{n-1}, a_0, (1+u)a_1, a_2, ...$

$...., a_{n-2})$. Implies $\tilde{\mu} = P^{-1}\mu P$.

So $(a_0, (1+u)a_1, a_2, ..., a_{n-1}) \in \tilde{\mu}(D)$, $((1+u)a_{n-1}, (1+u)a_0, a_1, (1+u)a_2, ..., a_{n-2}) \in \tilde{\mu}(D)$. So $\tilde{\mu}(D)$ is $(1+u)$-constacyclic code over $F_2 + uF_2$.

□

3.2.2 Gray map and $(1+u)$-constacyclic

We introduce the fundamental starting point of this subsection which is the fact that, roughly speaking , the Gray map of the $(1+u)$-constacyclic is the shift of the Gray map.

Remark 3.2.1. Following Definition 3.2.2 we notice that

1. $r((1+u)z) = r(z)$.
2. $q((1+u)z) = r(z) \oplus q(z)$.

Proposition 3.2.6. *[10] If ν is the $(1+u)-$constacyclic of R_2^n, σ is the shift of F_2^{2n}, and ϕ is the Gray map of R_2^n into F_2^{2n}, then*

$$\phi\nu = \sigma\phi.$$

Proof. Let $a = (a_0, a_1, ..., a_i, ..., a_{n-1})$ in R_2^n and let r_i and q_i in F_2 such that $a_i = uq_i + r_i$ where $q_i = q(a_i)$ and $r_i = r(a_i)$. From Definition 3.2.2 we obtain that

$$\phi(a) = (q_0, q_1, ..., q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-1} \oplus r_{n-1})$$

Thus

$$\sigma(\phi(a)) = (q_{n-1} \oplus r_{n-1}, q_0, q_1, ..., q_{n-2}, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-2} \oplus r_{n-2}.) \quad (3.2.5)$$

On the other hand, since

$$\nu(a) = ((1+u)a_{n-1}, a_0, ..., a_i, ...a_{n-2}),$$

then we have

$$\phi(\nu(a)) = (q((1+u)a_{n-1}), q_0, q_1, ..., q_{n-2}, r((1+u)a_{n-1}) \oplus q((1+u)a_{n-1}), q_0 \oplus r_0, ..., q_{n-2} \oplus r_{n-2}) \quad (3.2.6)$$

From Remark 3.2.1 we have

$$q((1+u)a_{n-1}) = q(a_{n-1}) \oplus r(a_{n-1}) = q_{n-1} \oplus r_{n-1} \tag{3.2.7}$$

$$r((1+u)a_{n-1}) \oplus q((1+u)a_{n-1}) = q(a_{n-1}) = q_{n-1}. \tag{3.2.8}$$

Also from Equations 3.2.6 , 3.2.7 and 3.2.8 we have

$$\phi(\nu(a)) = (q_{n-1} \oplus r_{n-1}, q_0, q_1, ..., q_{n-2}, q_{n-1}, q_0 \oplus r_0, q_1 \oplus r_1, ..., q_{n-2} \oplus r_{n-2}) \tag{3.2.9}$$

Now, from Equations 3.2.5 and 3.2.9 we have

$$\phi\nu = \sigma\phi.$$

□

Theorem 3.2.7. *[10] The Gray image of a linear $(1+u)-$constacyclic code over R_2 is a binary distance invariant linear cyclic code.*

Proof. Let C be a linear $(1+u)-$constacyclic code over R_2. Then $\nu(c) = c$, and therefore $\phi(\nu(c)) = \phi(c)$. By Proposition 3.2.6 we have $\sigma(\phi(c)) = \phi(c)$, which means that $\phi(c)$ is a linear cyclic code.

Example 3.2.4. *From Example 3.2.2 we have,*
$x^7 + (1+u) = (x + (1+u))(x^3 + x + (1+u))(x^3 + (1+u)x^2 + (1+u))$
Let $C = (x + (1+u))(x^3 + x + (1+u)) = 1 + x^2 + (1+u)x^3 + x^4$, *i.e;*
The code C has length 7, and 14 is the number of basis codewords

i	c_i	$\phi(c_i)$
1	$(1,0,1,(1+u),1,0,0)$	$(0,0,0,1,0,0,0,1,0,1,0,1,0,0)$
2	$(0,1,0,1,(1+u),1,0)$	$(0,0,0,0,1,0,0,0,1,0,1,0,1,0)$
3	$(0,0,1,0,1,(1+u),1)$	$(0,0,0,0,0,1,0,0,0,1,0,1,0,1)$
4	$((1+u),0,0,1,0,1,(1+u))$	$(1,0,0,0,0,0,1,0,0,0,1,0,1,0)$
5	$(1,(1+u),0,0,1,0,1)$	$(0,1,0,0,0,0,0,1,0,0,0,1,0,1)$
6	$((1+u),1,(1+u),0,0,1,0)$	$(1,0,1,0,0,0,0,0,1,0,0,0,1,0)$

7	$(0,(1+u),1,(1+u),0,0,1)$	$(0,1,0,1,0,0,0,0,0,1,0,0,0,1)$
8	$((1+u),0,(1+u),1,(1+u),0,0)$	$(1,0,1,0,1,0,0,0,0,0,1,0,0,0)$
9	$(0,(1+u),0,(1+u),1,(1+u),0)$	$(0,1,0,1,0,1,0,0,0,0,0,1,0,0)$
10	$(0,0,(1+u),0,(1+u),1,(1+u))$	$(0,0,1,0,1,0,1,0,0,0,0,0,1,0)$
11	$(1,0,0,(1+u),0,(1+u),1)$	$(0,0,0,1,0,1,0,1,0,0,0,0,0,1)$
12	$((1+u),1,0,0,(1+u),0,(1+u))$	$(1,0,0,0,1,0,1,0,1,0,0,0,0,0)$
13	$(1,(1+u),1,0,0,(1+u),0)$	$(0,1,0,0,0,1,0,1,0,1,0,0,0,0)$
14	$(0,1,(1+u),1,0,0,(1+u))$	$(0,0,1,0,0,0,1,0,1,0,1,0,0,0)$

From the above table we have $\phi(C) = \{\phi(c_i), \quad i = 1 \quad to \quad 14\}$ *is binary cyclic code* $[14,4,4]$*.(by Definitions 1.2.17 and 1.2.19).*

□

3.3 $(1-u^2)-$Constacyclic codes Over $F_2 + uF_2 + u^2F_2$

Let $R_3 = F_2+uF_2+u^2F_2$ be a commutative chain of 8 elements which are $\{0,1,u,u^2,v,v^2,uv,v^3\}$, where $u^3 = 0, \quad v = 1+u, \quad v^2 = 1+u^2, \quad v^3 = 1+u+u^2, \quad uv = u+u^2$.

Definition 3.3.1. [11] A code of length n is $(1-u^2)$-constacyclic if the code is invariant under Automorphism ν which has

$$\nu(a_0,a_1,\ldots,a_{n-1}) = ((1-u^2)a_{n-1},a_0,\ldots,a_{n-2})$$

Proposition 3.3.1. *[11] A subset* C *of* R_3^n *is a linear* $(1-u^2)$*-constacyclic of length* n *if and only if its polynomial representation is an ideal of* $R_3[x]/(x^n-(1-u^2))$.

Proof. Similar to the proof of Proposition 3.2.1

□

3.3.1 $(1-u^2)-$constacyclic codes of odd length

In this section we will study same propositions over $(1-u^2)-$constacyclic, and we study the properties of $(1-u^2)-$constacyclic codes of odd length.

Remark 3.3.1.
- $(1-u^2)^n = 1-u^2$ if n is odd.
- $(1-u^2)^n = 1$ if n is even.

Proposition 3.3.2. *[11] Let μ be the map of $R_3[x]/(x^n-1)$ into $R_3[x]/(x^n-(1-u^2))$ defined by:*

$$\mu(f(x)) = f((1-u^2)x)$$

If n is odd, then μ is ring isomorphism.

Proof. First we will show that μ is a ring homomorphism.

For the polynomials $f(x), g(x) \in R_3[x]/(x^n-1)$, $\mu(f(x)+g(x)) = \mu((f+g)(x)) = (f+g)((1-u^2)x)) = f((1-u^2)x)) + g((1-u^2)x))$

$$= \mu(f(x)) + \mu(g(x)).$$

And $\mu(f(x)g(x)) = \mu((fg)(x)) = (fg)((1-u^2)x) = f((1-u^2)x)g((1-u^2)x)$.

$$= \mu(f(x))\mu(g(x)).$$

Therefore μ is a ring homomorphism.

Now we will show μ is one to one. For the polynomials $f(x), g(x) \in R_3[x]$, $f(x) \equiv g(x) mod\ \ (x^n-1)$ if and only if there exists a polynomial $h(x) \in R_3[x]$ such that $f(x) - g(x) = h(x)(x^n-1)$ if and only if n is odd and $f((1-u^2)x) - g((1-u^2)x) = h((1-u^2)x)((1-u^2)x^n-1)$, if and only if

$$(1-u^2)f((1-u^2)x) - (1-u^2)g((1-u^2)x) = (1-u^2)h((1-u^2)x)((1-u^2)^n x^n - 1)$$
$$= h((1-u^2)x)(x^n-(1-u^2))$$

if and only if

$$(1-u^2)(\mu(f(x)) - \mu(g(x))) = h((1-u^2)x)(x^n-(1-u^2))$$

if and only if

$$(\mu(f(x)) - \mu(g(x))) = (1-u^2)h((1-u^2)x)(x^n-(1-u^2))$$

if and only if

$$\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (1-u^2))).$$

That means, for $f, g \in R_3[x]/(x^n - 1)$, $\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (1-u^2)))$ if and only if $f(x) \equiv g(x)(\text{mod } (x^n - 1))$. This implies that μ is a one to one homomorphism. To show μ is onto, let $f(x) \in R_3[x]/(x^n - (1-u^2))$. Then there exists $f((1-u^2)x) \in R_3[x]/(x^n - 1)$ such that $\mu(f((1-u^2)x)) = f((1-u^2)^2 x) = f(x)$. Thus μ is onto.

Therefore, μ is a ring isomorphism. □

Example 3.3.1. *Let $n = 7$.*

$$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } R_3[x] \quad ,$$

by the ring isomorphism

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

by Remark 3.3.1 we have

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

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

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

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

dividing by $(1-u^2)$, we have

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

Corollary 3.3.3. *[11] Let $\tilde{\mu}$ be the permutation of R_3^n with n odd, such that*

$$\tilde{\mu}(a_0, a_1, \ldots, a_{n-1}) = (a_0, (1-u^2)a_1, (1-u^2)^2 a_2, \ldots, (1-u^2)^i a_i, \ldots, (1-u^2)^{n-1} a_{n-1}),$$

and let D be a subset of R_3^n, Then D is a linear cyclic code if and only if $\tilde{\mu}(D)$ is a linear $(1-u^2)-$constacyclic code.

Proof. Let $R_3 = F_2 + uF_2 + u^2F_2$, the proof is obvious if we remark that the action of $\tilde{\mu}$ on vectors is the translation of the action of μ on polynomials, that is, $\tilde{\mu} = P^{-1}\mu P$.
If D is a cyclic code over $R_3[x]$, then $D(x)$ is an ideal of $R_3[x]/(x^n - (1-u^2))$.
If $a = (a_0, a_1, ..., a_{n-1}) \in D$, then $a(x), xa(x), ..., x^{n-1}a(x) \in D(x)$. The polynomial representation of the corespondents D are

$$a(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$$
$$xa(x) = xa_0 + a_1x^2 + ... + a_{n-2}x^{n-1} + a_{n-1}x^n$$
$$xa(x) = a_{n-1}x^n + xa_0 + a_1x^2 + ... + a_{n-2}x^{n-1}$$

implies

$$\mu(a(x)) = a_0 + (1-u^2)a_1x + (1-u^2)^2a_2x^2 + ... + a_{n-1}(1-u^2)^{n-1}x^{n-1}$$
$$\mu(xa(x)) = a_{n-1}((1-u^2)x)^n + a_0((1-u^2)x) + a_1((1-u^2)x)^2 + ... + a_{n-2}(1-u^2)^{n-1}x^{n-2}$$
$$\mu(xa(x)) = a_{n-1}(1-u^2)x^n + a_0((1-u^2)x) + a_1x^2 + ... + a_{n-2}x^{n-2}$$

The vector representation of $\mu(a(x))$ and $\mu(xa(x))$ are

$P^{-1}\mu(a(x)) = (a_0, (1-u^2)a_1, a_2, ..., (1-u^2)^{n-1}a_{n-1})$ and $P^{-1}\mu(xa(x)) = ((1-u^2)a_{n-1}, (1-u^2)a_0, a_1, (1-u^2)a_2, ..., (1-u^2)^{n-1}a_{n-2})$. Implies $\tilde{\mu} = P^{-1}\mu P$.
So $(a_0, (1-u^2)a_1, a_2, ..., a_{n-1}) \in \tilde{\mu}(D)$, $((1-u^2)a_{n-1}, (1-u^2)a_0, a_1, (1-u^2)a_2, ..., a_{n-2}) \in \tilde{\mu}(D)$. So $\tilde{\mu}(D)$ is $(1-u^2)$-constacyclic code over R_3.

□

3.3.2 Gray map and $(1-u^2)-$constacyclic codes

In this subsection,we prove that the Gray image of a linear$(1-u^2)-$constacyclic codes over R_3 of length n is a binary distance invariant linear quasi-cyclic code. We generalize the Gray map of $(1+u)-$constacyclic codes on R_2 . Now, every element $c \in R_3$ can be written uniquely as $c = \beta_0(c) + u\beta_1(c) + u^2\beta_2(c)$, where $\beta_i(c) \in F_2$. We define the Gray map $\phi : R_3 \longrightarrow F_2^4$ as follows :

$$\phi(c) = (\beta_2(c), \beta_2(c) + \beta_0(c), \beta_2(c) + \beta_1(c), \beta_2(c) + \beta_1(c) + \beta_0(c)).$$

Claim: ϕ is linear.

Proof. Let $c, c_1 \in F_2 + uF_2 + u^2F_2$. Then $\phi(c+c_1) = (\beta_2(c+c_1), \beta_2(c+c_1) + \beta_0(c+c_1), \beta_2(c+c_1) + \beta_1(c+c_1), \beta_2(c+c_1) + \beta_1(c+c_1) + \beta_0(c+c_1))$, since β_i is linear in F_2 for each $i - 0, 1$ *and* 2, then

$\phi(c+c_1) = (\beta_2(c), \beta_2(c) + \beta_0(c), \beta_2(c) + \beta_1(c), \beta_2(c) + \beta_1(c) + \beta_0(c_1)) \oplus (\beta_2(c_1), \beta_2(c_1) + \beta_0(c_1), \beta_2(c_1) + \beta_1(c_1), \beta_2(c_1) + \beta_1(c_1) + \beta_0(c_1)) = \phi(c) + \phi(c_1)$. □

The Gray map ϕ can be extended to R_3^n in an obvious way. For $c = (c_0, c_1, \ldots, c_{n-1}) \in$

R_3^n, define $\beta_i(c) = (\beta_i(c_0), \beta_i(c_1), \ldots, \beta_i(c_n))$, $0 \leq i \leq 2$. Then ϕ is extended to R_3^n as follows :

$$\phi(c) = (\beta_2(c), \beta_2(c) + \beta_0(c), \beta_2(c) + \beta_1(c), \beta_2(c) + \beta_1(c) + \beta_0(c))$$

for all $c \in R_3^n$.

Clearly, the extended ϕ is a bijection from R_3^n to F_2^{4n}. $\phi(c)$ is called the binary image of c under ϕ.

Proposition 3.3.4. *[11] Let ν be as in Definition 3.3.1 and ψ_t be as Definition 3.1.2. Then $\phi\nu = \psi_2\phi$.*

Proof. Let $c = (c_0, c_1, \ldots, c_{n-1})$ be in R_3^n, $c_i = \beta_0(c_i) + u\beta_1(c_i) + u^2\beta_2(c_i)$, where $\beta_i(c_i) \in F_2$. From the definition of ϕ, we obtain

$\phi(c) = (\beta_2(c_0), \beta_2(c_1), \ldots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_1(c_0), \ldots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}))$.
and

$\psi_2\phi(c) = \sigma(\beta_2(c_0), \beta_2(c_1), \ldots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-1}) + \beta_0(c_{n-1}))|, \sigma(\beta_2(c_0) + \beta_1(c_0), \ldots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}))$.

$\psi_2\phi(c) = (\beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0), \beta_2(c_1), \ldots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-2}) + \beta_0(c_{n-2}), \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_1(c_0), \ldots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$.

$\psi_2\phi(c) = (\beta_2(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0), \beta_2(c_1), \ldots, \beta_2(c_{n-1}), \beta_2(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-2}) + \beta_0(c_{n-2}), \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), \beta_2(c_0) + \beta_1(c_0), \ldots, \beta_2(c_{n-1}) + \beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), \ldots, \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$.
On the other hand

$$\nu(c) = ((1 - u^2)c_{n-1}, c_0, ..., cn - 2).$$

Note that

$$(1 - u^2)c_{n-1} = \beta_0(c_{n-1}) + \beta_1(c_{n-1})u + (\beta_2(c_{n-1}) + \beta_0(c_{n-1}))u^2.$$

From definition, we obtain

$\phi(\nu(c)) = (\beta_2(c_{n-1})+\beta_0(c_{n-1}), \beta_2(c_0), ..., \beta_2(c_{n-2})|, \beta_2(c_{n-1})+\beta_0(c_{n-1})+\beta_0(c_{n-1}), ..., \beta_2(c_{n-2})+$
$\beta_0(c_{n-2})|, \beta_2(c_{n-1}) + \beta_1(c_{n-1}) + \beta_0(c_{n-1}), ..., \beta_2(c_{n-2}) + \beta_1(c_{n-2})|, \beta_2(c_{n-1}) + \beta_0(c_{n-1}) +$
$\beta_1(c_{n-1}) + \beta_0(c_{n-1}), ..., \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$.

Now

$\phi(\nu(c)) = (\beta_2(c_{n-1})+\beta_0(c_{n-1}), \beta_2(c_0), ..., \beta_2(c_{n-2})|, \beta_2(c_{n-1}), \beta_2(c_0)+\beta_0(c_0), ..., \beta_2(c_{n-2})+$
$\beta_0(c_{n-2})|, \beta_2(c_{n-1})+\beta_1(c_{n-1})+\beta_0(c_{n-1}), \beta_2(c_0)+\beta_1(c_0), ..., \beta_2(c_{n-2})+\beta_1(c_{n-2})|, \beta_2(c_{n-1})+$
$\beta_1(c_{n-1}), \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), ..., \beta_2(c_{n-2}) + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$

Thus

$$\phi(\nu(c)) = (\psi_2\phi(c)).$$

□

Theorem 3.3.5. *[11] The Gray image of a linear $(1-u^2)$-constacyclic code over R_3 is binary distance invariant linear quasi-cyclic code of order 2.*

Proof. Let C be a linear $(1-u^2)$-constacyclic code over R_3. Then $\nu(C) = C$, and therefore, $(\phi\nu)C = \phi(C)$. It follows from Proposition 3.3.4 that $\psi_2(\phi(C)) = \phi(C)$, which means that $\phi(C)$ is a linear quasi-cyclic code of order 2. □

Example 3.3.2. *From Example 3.3.1 we have,*
$x^7 + (1-u^2) = (x + (1-u^2))(x^3 + x + (1-u^2))(x^3 + (1-u^2)x^2 + (1-u^2))$
Let $C = (x + (1-u^2))(x^3 + x + (1-u^2)) = 1 + x^2 + (1-u^2)x^3 + x^4$, *i.e;*
The code C has length 7, and 14 is the number of basis codewords.
By definition of ϕ in Proposition 3.3.4 we have this table:

i	c_i	$\phi(c_i)$
1	$(1,0,1,(1-u^2),1,0,0)$	$(0,0,0,1,0,0,0,1,0,1,0,1,0,0$ $,0,0,0,1,0,0,0,1,0,1,0,1,0,0)$
2	$(0,1,0,1,(1-u^2),1,0)$	$(0,0,0,0,1,0,0,0,1,0,1,0,1,0$ $,0,0,0,0,1,0,0,0,1,0,1,0,1,0)$

3	$(0,0,1,0,1,(1-u^2),1)$	$(0,0,0,0,0,1,0,0,0,1,0,1,0,1$ $,0,0,0,0,0,1,0,0,0,1,0,1,0,1)$
4	$((1-u^2),0,0,1,0,1,(1-u^2))$	$(1,0,0,0,0,0,1,0,0,0,1,0,1,0$ $,1,0,0,0,0,0,1,0,0,0,1,0,1,0)$
5	$(1,(1-u^2),0,0,1,0,1)$	$(0,1,0,0,0,0,0,1,0,0,0,1,0,1$ $,0,1,0,0,0,0,0,1,0,0,0,1,0,1)$
6	$((1-u^2),1,(1-u^2),0,0,1,0)$	$(1,0,1,0,0,0,0,0,1,0,0,0,1,0$ $,1,0,1,0,0,0,0,0,1,0,0,0,1,0)$
7	$(0,(1-u^2),1,(1-u^2),0,0,1)$	$(0,1,0,1,0,0,0,0,0,1,0,0,0,1$ $,0,1,0,1,0,0,0,0,0,1,0,0,0,1)$
8	$((1-u^2),0,(1-u^2),1,(1-u^2),0,0)$	$(1,0,1,0,1,0,0,0,0,0,1,0,0,0$ $,1,0,1,0,1,0,0,0,0,0,1,0,0,0)$
9	$(0,(1-u^2),0,(1-u^2),1,(1-u^2),0)$	$(0,1,0,1,0,1,0,0,0,0,0,1,0,0$ $,0,1,0,1,0,1,0,0,0,0,0,1,0,0)$
10	$(0,0,(1-u^2),0,(1-u^2),1,(1-u^2))$	$(0,0,1,0,1,0,1,0,0,0,0,0,1,0$ $,0,0,1,0,1,0,1,0,0,0,0,0,1,0)$
11	$(1,0,0,(1-u^2),0,(1-u^2),1)$	$(0,0,0,1,0,1,0,1,0,0,0,0,0,1$ $,0,0,0,1,0,1,0,1,0,0,0,0,0,1)$
12	$((1-u^2),1,0,0,(1-u^2),0,(1-u^2))$	$(1,0,0,0,1,0,1,0,1,0,0,0,0,0$ $,1,0,0,0,1,0,1,0,1,0,0,0,0,0)$
13	$(1,(1-u^2),1,0,0,(1-u^2),0)$	$(0,1,0,0,0,1,0,1,0,1,0,0,0,0$ $,0,1,0,0,0,1,0,1,0,1,0,0,0,0)$
14	$(0,1,(1-u^2),1,0,0,(1-u^2))$	$(0,0,1,0,0,0,1,0,1,0,1,0,0,0$ $,0,0,1,0,0,0,1,0,1,0,1,0,0,0)$

From above table we have $\phi(C) = \{\phi(c_i), \quad i = 1 \quad to \quad 14\}$ *is 2-quasicyclic code* $[28, 8, 8]$.

3.4 Constacyclic codes over Z_{2^k} and binary quasi-cyclic codes

In this section we'll study an important isometry ϕ^k, $k \geq 1$ between codes over Z_{2^k+1} and codes over Z_4. Also, we'll study, by some definitions , the Hpo-cyclic, negacyclic and quasi-cyclic codes. Later in this section, we'll introduce the linear Hpo-cyclic code to the end, we have the following definitions and notations.

3.4.1 Definitions and notation

Recall the definition of the Gray map ϕ of ${Z_4}^n$ and ${F_2}^{2n}$ as follows:

$$\phi(Z) = (q(Z), q(Z) \oplus r(Z))$$

for all $Z = (z_1, z_2, ..., z_n) \in {Z_4}^n$ and

$$r(Z) = (r(z_1), r(z_2), ..., r(z_n))$$
$$q(Z) = (q(z_1), q(z_2), ..., q(z_n)).$$

That is

$$\phi(Z) = ((q(z_1), ..., q(z_n), q(z_1) \oplus r(z_1), ..., q(z_n) \oplus r(z_n)),$$

where q and r are two maps from Z_4 into F_2 such that if $z \in Z_4$, then the 2-adic expansion of z is $z = r(z) + 2q(z)$.

For easy writing , if we replace r by r_0 and q by r_1 we get:

$$\phi(Z) = ((r_1(z_1), ..., r_1(z_n), r_1(z_1) \oplus r_0(z_1), ..., r_1(z_n) \oplus r_0(z_n)),$$

and $z = r_0(z) + 2r_1(z)$.

Definition 3.4.1. [5] For $k \geq 1$, $k+1$ mappings r_i, $i = 0, 1, \ldots, k$, from $Z_{2^{k+1}}$ in to F_2 such that if $a, b \in Z_{2^{k+1}}$, the 2-adic expansion of a and b are

$$a = r_0(a) + 2r_1(a) + \ldots + 2^k r_k(a).$$
$$b = r_0(b) + 2r_1(b) + \ldots + 2^k r_k(b).$$

Using the 2-adic expansions of any element in $Z_{2^{k+1}}$, the operation " $\odot$ " on $Z_{2^{k+1}}$ is introduced as follows: if $a, b \in Z_{2^{k+1}}$, then

$$a \odot b = (r_0(a)r_0(b)) + 2(r_1(a)r_1(b)) + \ldots + 2^k(r_k(a)r_k(b)).$$

This operation is extended to $Z_{2^{k+1}}^n$ in the following natural way: if $A = (a_0, a_1, \ldots, a_{n-1})$, $B = (b_0, b_1, \ldots, b_{n-1}) \in Z_{2^{k+1}}^n$ then define

$$A \odot B = (a_0 \odot b_0, a_1 \odot b_1, \ldots, a_{n-1} \odot b_{n-1}).$$

Definition 3.4.2. [5] For $k \leq 2$, define $\rho_k : Z_{2^{k+1}} \longrightarrow F_2^{k-1}$ by

$$\rho_k(a) = (r_{k-1}(a), r_{k-2}(a), \ldots, r_2(a), r_1(a))$$

For all $i \in \{0, 1, \ldots, (2^{k-1} - 1)\}$, let $\alpha_i^k \in F_2^{k-1}$ be the binary expression of i using $k-1$ bits, where the most significant bit is on left.

Example 3.4.1. *If $k = 5$ and $i = 13$ in the above definition then the binary expression is (1011) but the most significant bit is on left is(1101), therefor α_{13}^5 =(1101).*

Definition 3.4.3. [5] By means of ρ_k and α_i^k, the following function $\varphi_i^k : Z_{2^{k+1}}^n \longrightarrow Z_4^{2^{k-1}n}$ given by:

$$\varphi_i^k(a) = 2(r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k)) + r_0(a), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$$

where " $\cdot$ " denote the usual dot product in F_2^{k-1}.

Definition 3.4.4. [5] The action of the functions φ_i^k are extended to $Z_{2^{k+1}}^n$ as follows: if $A = (a_0, a_1, \ldots, a_{n-1}) \in Z_{2^{k+1}}^n$, then $\varphi_i^k(A) = (\varphi_i^k(a_0), \varphi_i^k(a_1), \ldots, \varphi_i^k(a_{n-1}))$. Thus, the map $\varphi^k : Z_{2^{k+1}}^n \longrightarrow Z_4^{2^{k-1}n}$ defined by:

$$\varphi^k(A) = (\varphi_0^k(A), \varphi_1^k(A), \ldots, \varphi_{2^{k-1}-1}^k(A)), \qquad \forall A \in Z_{2^{k+1}}^n.$$

Notation 3.4.1. *$\varphi^1 : Z_4^n \longrightarrow Z_4^n$ is defined as the identity map, that is $\varphi^1(A) = A$.*

Proof. Let $A = (a_0, a_1, \ldots, a_{n-1})$,

$\varphi^1(A) = \varphi_0^1(A)$ (from Definition 3.4.4)

$\varphi^1(A) = \varphi_0^1(A) = (\varphi_0^1(a_0), \varphi_0^1(a_1), \ldots, \varphi_0^1(a_{n-1}))$ (from Definition 3.4.4).

Now $\varphi_0^1(a_0) = \varphi_0^1(a) = 2(r_1(a) \oplus (\rho_1(a) \cdot \alpha_0^1)) + r_0(a)$, $i = 0$ (from Definition 3.4.3).

From definition 3.4.2 and Definition 3.4.3 we have $\rho_1(a) = r_0(a_0)$ and $\alpha_0^1 = 0$.

Therefore $\varphi_0^1(a_0) = 2(r_1(a_0)) + r_0(a_0) = a_0$. Similarly $\varphi_0^1(a_1) = a_1$.....$\varphi_0^1(a_{n-1}) = a_{n-1}$.

Finally $\varphi^1(A) = \varphi_0^1(A) = (\varphi_0^1(a_0), \varphi_0^1(a_1), \ldots, \varphi_0^1(a_{n-1})) = (a_0, a_1, \ldots, a_{n-1}) = A$.

□

Definition 3.4.5. [5] Using the map ϕ^k we will define the **generalized Gray map** $\phi : Z_{2^{k+1}}^n \longrightarrow F_2^{2^k n}$, by

$$\phi(A) = (\phi\varphi_0^k(A), \phi\varphi_1^k(A), \ldots, \phi\varphi_{2^{k-1}-1}^k(A)), \qquad \forall A \in Z_{2^{k+1}}^n.$$

Definition 3.4.6. For $k \geq 1$ the **homogeneous weight,** wt_{hom}, on $Z_{2^{k+1}}$ is defined by:

$$wt_{hom}(a) = \begin{cases} 0, & \text{if a= 0;} \\ 2^k, & \text{if } a = 2^k; \\ 2^{k-1}, & \text{otherwise.} \end{cases} \qquad \forall a \in Z_{2^{k+1}}$$

3.4.2 Hpo-cyclic, negacyclic and quasi-cyclic codes

In this subsection, we'll study the characterization of the Hpo-cyclic codes in terms of their images under the isometry ϕ^k. Also the proof of the following two propositions, given after definition of Hpo-cyclic code, allows us to establish the connection between negacyclic and Hpo-cyclic codes.

Definition 3.4.7. [5] For any positive integer k, if the unit λ in $Z_{2^{k+1}}$ is equal to $2^k + 1$ (half of 2^{k+1} plus one), then the set $C \subseteq Z_{2^{k+1}}^n$ such that $\nu_\lambda(C) = C$ will be called an **Hpo-cyclic code**.

Proposition 3.4.2. *[5] Let $r_i, i = 0, 1, 2, \ldots, k$, be the mappings as defined in Definition 3.4.1 and let $\lambda = 2^k + 1$ be a unit of $Z_{2^{k+1}}$. Then for all $a \in Z_{2^{k+1}}$:*

$$r_i(\lambda a) = \begin{cases} r_i(a), & \textit{if i= 0, 1, \ldots, k-1;} \\ r_k(a) \oplus r_0(a), & \textit{if i=k.} \end{cases}$$

Proof. let $a = \sum_{i=0}^k 2^i r_i(a)$, then $\lambda a = (2^k + 1)(\sum_{i=0}^k 2^i r_i(a))$,

now $\lambda a = 2^k \sum_{i=0}^k 2^i r_i(a) + \sum_{i=0}^k 2^i r_i(a) = 2^k \sum_{i=0}^k 2^i r_i(a) + \sum_{i=0}^{k-1} 2^i r_i(a) + 2^k r_k(a)$

$= \sum_{i=0}^{k-1} 2^i r_i(a) + 2^k(\sum_{i=0}^k 2^i r_i(a) + r_k(a))$

$= \sum_{i=0}^{k-1} 2^i r_i(a) + 2^k(r_0(a) + \sum_{i=1}^k 2^i r_i(a) + r_k(a))$

$= \sum_{i=0}^{k-1} 2^i r_i(a) + 2^k(r_0(a) \oplus r_k(a))$ □

Proposition 3.4.3. *[5] Let φ_i^k, $r_i, i = 0, 1, 2, \ldots, 2^{k-1} - 1$ be the mapping as defined in definition 3.4.3 and let $\lambda = 2^k + 1$. Then for all $a \in Z_{2^{k+1}}$:*

$$\varphi_i^k(\lambda a) = -\varphi_i^k(a).$$

Proof. By Definition 3.4.3 we have,

$\varphi_i^k(\lambda a) = 2(r_k(\lambda a) \oplus (\rho_k(\lambda a) \cdot \alpha_i^k)) + r_0(\lambda a), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,,$

also, from Definition 3.4.2 we have $r_k(\lambda a) = r_k(a) \oplus r_0(a)$, $\rho_k(\lambda a) = \rho_k(a)$ and $r_0(\lambda a) = r_0(a)$.

therefore,

$\varphi_i^k(\lambda a) = 2(r_k(a) \oplus r_0(a) \oplus (\rho_k(a) \cdot \alpha_i^k)) + r_0(a), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$

$\phi_i^k(\lambda a) = 2r_0(a) \oplus 2(r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k)) + r_0(a), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$

$\phi_i^k(\lambda a) = 3r_0(a) \oplus 2(r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k)), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$

since $\varphi_i^k : Z_{2^{k+1}}^n \longrightarrow Z_4^{2^{k-1}n}$, then 3= -1 and 2= -2,i.e;

$\varphi_i^k(\lambda a) = -r_0(a) \oplus -2(r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k)), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$

$\phi_i^k(\lambda a) = -(r_0(a) \oplus 2(r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k))), \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$

$\phi_i^k(\lambda a) = -\phi_i^k(a) \qquad \forall i = 0, 1, \ldots, 2^{k-1} - 1,$ □

Theorem 3.4.4. *[5] Let C be a code over $Z_{2^{k+1}}$ of length n. Then C is an Hpo-cyclic code if and only if $\varphi^k(C)$ is a quasi-negacyclic code of order 2^{k-1} and length $2^{k-1}n$.*

Proof. Suppose $C = (c_0, c_1, \ldots, c_{n-1})$ is Hpo-cyclic code, then $\nu_\lambda(C) = C$ where $\lambda = 2^k+1$.

Now $\varphi^k(C) = \varphi^k(\nu_\lambda(C)) = (\varphi_0^k(\nu(c_0)), \varphi_1^k(\nu(c_1)), \ldots, \varphi_{2^{k-1}-1}^k(\nu(c_{n-1}))), \ \forall \nu_\lambda(C) \in Z_{2^{k+1}}^n$.

By Proposition 3.4.3 we have :

$\varphi^k(\nu_\lambda(C)) = (\nu(\varphi_0^k(c_0)), \nu(\varphi_1^k(c_1)), \ldots, \nu(\varphi_{2^{k-1}-1}^k(c_{n-1}))) \qquad \forall \nu_\lambda(C) \in Z_{2^{k+1}}^n.$

$\varphi^k(\nu_\lambda(C)) = \nu(\varphi_0^k(c_0))|\nu(\varphi_1^k(c_1))| \ldots |\nu(\varphi_{2^{k-1}-1}^k(c_{n-1})) \qquad \forall \nu_\lambda(C) \in Z_{2^{k+1}}^n.$

$\varphi^k(\nu_\lambda(C)) = \delta_{2^{k-1}}(\varphi_0^k|\varphi_1^k| \ldots |\varphi_{2^{k-1}-1}^k) \qquad \forall \nu_\lambda(C) \in Z_{2^{k+1}}^n.$

$\varphi^k(\nu_\lambda(C)) = \delta_{2^{k-1}}(\varphi^k(C))$ where δ_t be the quasi-negacyclic on $Z_{2^{k+1}}$ of order 2^{k-1} and length $2^{k-1}n$.

The converse is proved in a similar way.

□

Remark 3.4.1. 1. In the previous theorem when $k = 1$, the concept of an Hpo-cyclic code and a negacyclic code are the same.

2. Recall (1) above shows that the Hpo-cyclic code is natural generalization of the negacyclic code.

Proposition 3.4.5. *[5] If ν is the negashift on Z_4^n, σ is the shift on F_2^{2n}, and if ϕ is the Gray map from Z_4^n into F_2^{2n}, then*

$$\phi\nu = \sigma\phi$$

.

Proof. Let $A = (a_0, a_1, \ldots, a_n) \in Z_4^n$. Since $k = 1$, then $i = 0$ and $\lambda = 3 = -1$.

From definition 3.4.5 we have,

$$\begin{aligned}\phi(\nu_{-1}(A)) = \phi\varphi_0^1(\nu_{-1}(A)) &= \phi\varphi_0^1(-a_n, a_0, \ldots, a_{n-1}) \\ &= \phi(\varphi_0^1(-a_n), \varphi_0^1(a_0), \ldots, \varphi_0^1(a_{n-1})) \text{ (by Definition 3.4.4).} \\ &= \phi(\varphi_0^1(a_n), \varphi_0^1(a_0), \ldots, \varphi_0^1(a_{n-1})) \text{ (by Proposition 3.4.3)}\end{aligned}$$

Therefore,

$$\phi(\nu_{-1}(A)) = \phi(\varphi_0^1(a_n), \varphi_0^1(a_0), \ldots, \varphi_0^1(a_{n-1})). \tag{3.4.1}$$

In the other hand

$$\begin{aligned}\phi(A) = \phi\varphi_0^1(A) &= \phi\varphi_0^1(a_0, a_1, \ldots, a_n) \text{ (by Definition 3.4.5)} \\ &= \phi(\varphi_0^1(a_0), \varphi_0^1(a_1), \ldots, \varphi_0^1(a_n)) \text{ (by Definition 3.4.4)} \\ \sigma(\phi(A)) &= \sigma\phi(\varphi_0^1(a_0), \varphi_0^1(a_1), \ldots, \varphi_0^1(a_n)) \\ \sigma(\phi(A)) &= \phi\sigma(\varphi_0^1(a_0), \varphi_0^1(a_1), \ldots, \varphi_0^1(a_n)).\end{aligned}$$

Since σ is normal shift then

$$\sigma(\phi(A)) = \phi(\varphi_0^1(a_n), \varphi_0^1(a_0), \ldots, \varphi_0^1(a_{n-1})). \tag{3.4.2}$$

From Equation 3.4.1 and Equation 3.4.2 we are done.

□

Proposition 3.4.6. *[5] If $\lambda = 2^k + 1 \in Z_{2^{k+1}}$ then, $\phi\nu_\lambda = \psi_{2^{k-1}}\phi$.*

Proof. Let $A \in Z_{2^{k+1}}$, then

$$\begin{aligned}\phi(\nu_\lambda(A)) &= (\phi\varphi_0^k(\nu_\lambda(A)), \phi\varphi_1^k(\nu_\lambda(A)), \ldots, \phi\varphi_{2^{k-1}-1}^k(\nu_\lambda(A)) \text{ (by Definition 3.4.5).} \\ &= \phi\nu\varphi_0^k(A), \phi\nu\varphi_1^k(A), \ldots, \phi\nu\varphi_{2^{k-1}-1}^k(A) \text{ (bt Theorem 3.4.4).}\end{aligned}$$

$= (\sigma\phi\varphi_0^k(A)|\sigma\phi\varphi_1^k(A)|\ldots|\sigma\phi\varphi_{2^{k-1}-1}^k(A))$ (by Proposition 3.4.5).

$= \psi_{2^k-1}(\phi\varphi_0^k(A)|\phi\varphi_1^k(A)|\ldots|\phi\varphi_{2^{k-1}-1}^k(A))$ (from Definition ψ).

$= \psi_{2^k-1}\phi(A)$.

□

3.4.3 Linear Hpo-cyclic codes

In this section we will represent the elements of $Z_{2^{k+1}}^n$ as polynomials in the ring $Z_{2^{k+1}}[x]/(x^n-1)$. This is achieved via the polynomial representation map given by:

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1x + \ldots + a_{n-1}x^{n-1}.$$

The operation $\odot$ in Definition 3.4.1 can be extended to $Z_{2^{k+1}}[x]/(x^n-1)$ as follows: if $A(x) = \sum_{j=0}^{n-1} a_jx^j$ and $B(x) = \sum_{j=0}^{n-1} b_jx^j$ are elements of $A(x) = \sum_{j=0}^{n-1} a_jx^j$ then

$$A(x) \odot B(x) = \textstyle\sum_{j=0}^{n-1}(a_j \odot b_j)x^j.$$

The action of the mappings φ_i^k in Definition 3.4.4 is extended to $Z_{2^{k+1}}[x]/(x^n-1)$ as follows:
if $A(x) = \sum_{j=0}^{n-1} a_jx^j \in Z_{2^{k+1}}[x]/(x^n-1)$ then,

$$\varphi_i^k A(x) = \textstyle\sum_{j=0}^{n-1} \varphi_i^k(a_j)x^j, \quad i = 0, 1, \ldots, 2^{k-1}-1$$

and the action of the map φ^k on $Z_{2^{k+1}}[x]/(x^n-1)$ is

$$\varphi^k A(x) = (\varphi_0^k(A(x)), \ldots, \varphi_{2^{k-1}-1}^k(A(x))) \qquad \forall A(x) \in Z_{2^{k+1}}[x]/(x^n-1).$$

Proposition 3.4.7. *[5] Let $\lambda = 2^k + 1 \in Z_{2^{k+1}}$. Then a subset C of $Z_{2^{k+1}}^n$ is a linear Hpo-cyclic code of length n if and only if its polynomial representation is an ideal of the ring $Z_{2^{k+1}}[x]/(x^n-\lambda)$.*

Proof. $\leftarrow$ Suppose that $\pi(C)$ is an ideal of $Z_{2^{k+1}}/(x^n-\lambda)$. Then for any $\alpha, \beta \in Z_{2^{k+1}}/(x^n-\lambda)$ and $a, b \in C$. We have $\alpha\pi(a), \beta\pi(b) \in \pi(C)$ by definition 1.1.6 part (2). Thus by definition 1.1.6 part(1) $\alpha\pi(a) + \beta\pi(b)$ is element of $\pi(C)$, i.e; $\alpha\pi(a) + \beta\pi(b) = \pi(\alpha(a) + \beta(b)) \in \pi(C)$, hence $\alpha(a) + \beta(b)$ is codeword of C. This shows that C is a linear code.

Now let $c = (c_0, c_1, \ldots, c_{n-1})$ be a codeword of C then The polynomial representation of C is

$$\pi(c) = (c_0 + c_1x + \ldots + c_{n-1}x^{n-1})$$

is an element of $\pi(C)$. Since $\pi(C)$ is an ideal of $Z_{2^{k+1}}/(x^n - \lambda)$ then the element

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

But $\pi(C)$ is ideal in $Z_{2^{k+1}}/(x^n - \lambda)$ and since $x^n - \lambda = 0 \Rightarrow x^n = \lambda$.

$$\text{then } x\pi(c) = c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1} + c_{n-1}\lambda$$
$$= \lambda c_{n-1} + c_0x + c_1x^2 + \ldots + c_{n-2}x^{n-1}$$

is in $\pi(C)$, i.e; $(\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is codeword of C. This mean that C is Hpo-cyclic codes.

Conversely, suppose that C is Hpo-cyclic code . Then part(1) of the Definition 1.1.6 is satisfied for $\pi(C)$. For any polynomial

$$f(x) = f_0 + f_1x + \ldots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1} = \pi(f_0, f_1, \ldots, f_{n-2}, f_{n-1})$$

of $\pi(C)$ with $(f_0, f_1, \ldots, f_{n-1}) \in C$, the polynomial

$$xf(x) = \lambda f_{n-1} + f_0x + f_1x^2 + \ldots + f_{n-2}x^{n-2} = \lambda f_{n-1} + f_0x + f_1x^2 + ... + x^{n-1}f_{n-2}$$

is also an element of $\pi(C)$ since C is hpo-cyclic code. Thus, $x^2f(x) = x(xf(x))$ is an element of $\pi(C)$. By induction, suppose that $x^jf(x)$ belong to $\pi(C)$ for all $j \geq 0$.

Since C is a linear code and π is a linear transformation, $\pi(C)$ is a linear space over $Z_{2^{k+1}}$. Hence, for any $g(x) = g_0 + g_1x + \ldots + g_{n-1}x^{n-1} \in Z_{2^{k+1}}/(x^n - \lambda)$, the polynomial

$$g(x)f(x) = \textstyle\sum_{i=0}^{n-1} g_i(x^if(x))$$

is an element of $\pi(C)$. Therefore, $\pi(C)$ is an ideal of $Z_{2^{k+1}}/(x^n - \lambda)$ since part (2) of the Definition 1.1.6 is also satisfied.

□

Remark 3.4.2. If $\lambda = 2^k + 1 \in Z_{2^{k+1}}$, then

1. $(2^k + 1)^n \equiv (2^k + 1) \mod(2^{k+1})$ if n is odd.
2. $(2^k + 1)^n \equiv 1 \mod(2^{k+1})$ if n is even.

Proposition 3.4.8. *[5] Let n be an odd positive integer and $\lambda = 2^k + 1 \in Z_{2^{k+1}}$. Then the map μ_λ from $Z_{2^{k+1}}[x]/(x^n - 1)$, into $Z_{2^{k+1}}[x]/(x^n - \lambda)$ given by*

$$\mu_\lambda(f(x)) = f(\lambda x)$$

is a ring isomorphism.

Proof. First we will show μ is a ring homomorphism.

For the polynomials $f(x), g(x) \in Z_{2^{k+1}}[x]/(x^n - 1)$, $\mu(f(x) + g(x)) = \mu((f + g)(x)) = (f + g)(\lambda x)) = f(\lambda x)) + g(\lambda x))$

$$= \mu(f(x)) + \mu(g(x)).$$

And $\mu(f(x)g(x)) = \mu((fg)(x)) = (fg)(\lambda x) = f(\lambda x)g(\lambda x)$.

$$= \mu(f(x))\mu(g(x)).$$

Therefore μ is a ring homomorphism.

Now we will show that μ is a one to one. For the polynomials $f(x), g(x) \in Z_{2^{k+1}}[x]$, $f(x) \equiv g(x) mod \ \ (x^n - 1)$ if and only if there exists a polynomial $h(x) \in Z_{2^{k+1}}[x]$ such that $f(x) - g(x) = h(x)(x^n - 1)$ if and only if n is odd and $f(\lambda x) - g(\lambda x) = h(\lambda x)((\lambda x)^n - 1)$, if and only if

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

$$= h(\lambda x)(x^n - \lambda)$$

if and only if

$$\lambda(\mu(f(x)) - \mu(g(x))) = h(\lambda x)(x^n - \lambda)$$

if and only if

$$(\mu(f(x)) - \mu(g(x))) = \lambda h(\lambda x)(x^n - \lambda)$$

if and only if

$$\mu(f(x)) \equiv \mu(g(x)) (\text{mod } (x^n - \lambda)).$$

That means, for $f, g \in Z_{2^{k+1}}[x]/(x^n - 1)$, $\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - \lambda))$ if and only if $f(x) \equiv g(x)(\text{mod } (x^n - 1))$. This implies that μ is a one to one homomorphism.

To show μ is onto, let $f(x) \in Z_{2^{k+1}}[x]/(x^n - \lambda)$. Then there exists $f(\lambda x) \in Z_{2^{k+1}}[x]/(x^n - 1)$ such that $\mu(f(\lambda x)) = f(\lambda^2 x) = f(x)$. Thus μ is onto.

Therefore, μ is a ring isomorphism. □

Corollary 3.4.9. *[5] A subset I of $Z_{2^{k+1}}[x]/(x^n-1)$ is an ideal of $Z_{2^{k+1}}[x]/(x^n-1)$ if and only if $\mu_\lambda(I)$ is an ideal of $Z_{2^{k+1}}[x]/(x^n-\lambda)$.*

Proof. Suppose I is ideal of $Z_{2^{k+1}}/(x^n-1)$. Let $f(\lambda x), g(\lambda x) \in \mu(I)$.
Now $f(x)+g(x) \in I$ for all $f(x)$, $g(x) \in I$ where I is ideal. So by the definition of μ_λ we have, $\mu_\lambda(f(x)+g(x)) \in \mu_\lambda(I)$. But $\mu_\lambda(f(x)+g(x)) = \mu_\lambda((f+g))(x) = (f+g)(\lambda x) = f(\lambda x)+g(\lambda x) \in \mu_\lambda(I)$, implies

$$f(\lambda x)+g(\lambda x) \in \mu_\lambda(I) \tag{3.4.3}$$

Let $f(\lambda x), l(\lambda x) \in \mu_\lambda(I)$. Now $f(x).l(x) \in I$ for all $f(x) \in I$, $l(x) \in Z_{2^{k+1}}$. By definition of μ_λ we have

$\mu_\lambda(f(x).l(x)) \in \mu_\lambda(I)$. But $\mu_\lambda(f(x).l(x)) = \mu_\lambda((f.l)(x)) = (f.l)(\lambda x) = f(\lambda x).l(\lambda x) \in \mu_\lambda(I)$, implies

$$f(\lambda x).l(\lambda x) \in \mu_\lambda(I). \tag{3.4.4}$$

From Equation 3.4.3 and Equation 3.4.4 we have $\mu_\lambda(I)$ is an ideal of $Z_{2^{k+1}}/(x^n-\lambda)$.
Conversely suppose $\mu_\lambda(I)$ is ideal. Let $f(x), g(x) \in I$.
Now $f(\lambda x)+g(\lambda x) \in \mu_\lambda(I)$ for all $f(\lambda x), g(\lambda x) \in \mu_\lambda(I)$ where $\mu_\lambda(I)$ is ideal. So by definition μ_λ we have

$f(\lambda x)+g(\lambda x) = (f+g)(\lambda x) = \mu_\lambda((f+g)x) \in \mu_\lambda(I)$.
Since μ_λ is a ring isomorphism then $\mu_\lambda^{-1}\mu_\lambda((f+g)x) \in \mu_\lambda^{-1}\mu_\lambda(I)$. Therefore $(f+g)(x) \in I$, i.e;

$$f(x)+g(x) \in I \tag{3.4.5}$$

Let $f(x) \in I$ and $l(x) \in Z_{2^{k+1}}$ now $f(\lambda x).l(\lambda x) \in \mu_\lambda(I)$ for all $f(\lambda x).l(\lambda x) \in \mu_\lambda(I)$ where $\mu(I)$ is ideal. So by definition μ_λ we have

$f(\lambda x).l(\lambda x) = (f.l)(\lambda x) = \mu_\lambda((f.l)x) \in \mu_\lambda(I)$.
Since μ_λ is a ring isomorphism then $\mu_\lambda^{-1}\mu_\lambda((f.l)x) \in \mu_\lambda^{-1}\mu_\lambda(I)$. Thus $(f.l)(x) \in I$, i.e;

$$f(x).l(x) \in I. \tag{3.4.6}$$

From Equation 3.4.5 and 3.4.6 we have I is an ideal of $Z_{2^{k+1}}/(x^n-1)$. □

Example 3.4.2. *Let $n = 7$ and $k = 2$.*

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } F_2[x].$$

By Hensel lemma over Z_8 we find

$$x^7 + 1 = (x + 1)(x^3 + 6x^2 + 5x - 1)(x^3 + 3x^2 + 2x - 1) \text{ in } Z_8[x].$$

Applying the ring isomorphism, μ_λ, $\lambda = 5$, over Z_8 we have,

$(5x)^7 + 1 = ((5x) + 1)((5x)^3 + 6(5x)^2 + 5(5x) - 1)((5x)^3 + 3(5x)^2 + 2(5x) - 1)$.

So

$$x^7 - 5 = (x - 5)(x^3 + 6x^2 + 5x + 3)(x^3 - x^2 + 2x + 3).$$

Theorem 3.4.10. *The generalized Gray map image of a linear Hpo-cyclic code over Z_2^{k+1} of length n, is a binary-distance-invariant quasi-cyclic code of order 2^{k-1} and length $2^k n$.*

Proof. Let C be a linear Hpo-cyclic code over Z_2^{k+1} and let $\lambda = 2^k + 1$. Then $\nu_\lambda(C) = C$, and therefore $\phi(\nu_\lambda(C)) = \phi(C)$. By Proposition 3.4.6 we have $\phi\nu_\lambda(C) = \psi_{2^{k-1}}\phi(C)$. Which means that $\phi_\lambda(C) = \psi_{2^{k-1}}\phi(C)$, i.e; $\phi(C)$ is a quasi-cyclic code of order 2^{k-1}. By theorem 3.4.4 we have code length of $2^{k-1}n$. □

Example 3.4.3. *In above example we have $n = 7$, $k = 2$ and*

$$x^7 - 5 = (x - 5)(x^3 + 6x^2 + 5x + 3)(x^3 - x^2 + 2x + 3).$$

in $Z_8[x]$.

Let C be the Hpo-cyclic code generated by the polynomial

$G(x) = x^7 - 5 = (x - 5)(x^3 + 6x^2 + 5x + 3) = x^4 + x^3 - x^2 + 2x + 1.$*,i.e;*

The code C has length 7, and 14 the number of basis codewords

By definition of ϕ in Proposition 3.4.10 we did complicated and very long maths processes and we finally had those results shown in this table :

i	c_i	$\phi(c_i)$
1	$(1, 2, 7, 1, 1, 0, 0)$	$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0,$ $0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$
2	$(0, 1, 2, 7, 1, 1, 0)$	$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0,$ $0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$

i	c_i	$\phi(c_i)$
3	$(0,0,1,2,7,1,1)$	$(0,0,0,0,1,0,0,0,0,1,1,0,1,1,$ $0,0,0,1,0,0,0,0,0,1,0,1,1,1)$
4	$(5,0,0,1,2,7,1))$	$(1,0,0,0,0,1,0,0,0,0,1,1,0,1,$ $1,0,0,0,1,0,0,0,0,0,1,0,1,1)$
5	$(5,5,0,0,1,2,7)$	$(1,1,0,0,0,0,1,0,0,0,0,1,1,0,$ $1,1,0,0,0,1,0,0,0,0,0,1,0,1)$
6	$(3,5,5,0,0,1,2)$	$(0,1,1,0,0,0,0,1,0,0,0,0,1,1,$ $1,1,1,0,0,0,1,0,0,0,0,0,1,0)$
7	$(2,3,5,5,0,0,1)$	$(0,0,1,1,0,0,0,1,1,0,0,0,0,1,$ $1,1,1,1,0,0,0,0,0,0,0,0,0,1)$
8	$(5,2,3,5,5,0,0)$	$(1,0,0,1,1,0,0,0,1,1,0,0,0,0,$ $1,1,1,1,1,0,0,0,0,0,0,0,0,0)$
9	$(0,5,2,3,5,5,0)$	$(0,1,0,0,1,1,0,0,0,1,1,0,0,0,$ $0,1,1,1,1,1,0,0,0,0,0,0,0,0)$
10	$(0,0,5,2,3,5,5,)$	$(0,0,1,0,0,1,1,0,0,0,1,1,0,0,$ $0,0,1,1,1,1,1,0,0,0,0,0,0,0)$
11	$(1,0,0,5,2,3,5,)$	$(0,0,0,1,0,0,1,1,0,0,0,1,1,0,$ $0,0,0,1,1,1,1,1,0,0,0,0,0,0)$
12	$(1,1,0,0,5,2,3,)$	$(0,0,0,0,1,0,0,1,1,0,0,0,1,1,$ $0,0,0,0,1,1,1,1,1,0,0,0,0,0)$
13	$(7,1,1,0,0,5,2)$	$(1,0,0,0,0,1,0,0,1,1,0,0,0,1,$ $0,0,0,0,0,1,1,1,1,1,0,0,0,0)$
14	$(2,7,1,1,0,0,5)$	$(0,1,0,0,0,0,1,1,0,1,1,0,0,0,$ $0,0,0,0,0,0,1,1,1,1,1,0,0,0)$

From last table we have $\phi(C) = \{\phi(c_i), \quad i = 1 \quad to \quad 14\}$ *is 2-quasicyclic code* $[28, 512, 10]$.

Chapter 4

$(1-u^{k-1})-$ Constacyclic codes over $F_2+uF_2+u^2F_2+\ldots+u^{k-1}F_2$

In [11], Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu showed that the Gray image of a linear constacyclic code over $R_3 = F_2 + uF_2 + u^2F_2$ of length n is a distance-invariant linear quasi- cyclic code of order 2. But not much work has been done on the Gray image of a linear constacyclic code over $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$.
In this chapter, we generalize the main result of [11] to the ring R_k. We define a distance preserving map from R_k to $F_2^{2^{(k-1)}}$, and characterize codes over $F_2^{2^{(k-1)}}$ which are the Gray images of $(1-u^{k-1})$-constacyclic codes over R_k.

4.1 Introduction

In this section, We will study some definitions and notes that study $(1-u^{k-1})-$constacyclic code of odd length.

Definition 4.1.1. The ring $R_k = F_2[u]/(u^k)$ is a commutative chain ring of 2^k elements, every element $c \in F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ can be written uniquely as $c = \beta_0(c) + u\beta_1(c) + u^2\beta_2(c) + \ldots + u^{k-1}\beta_{k-1}(c)$,with $u^k = 0$, where $\beta_i(c) \in F_2$.

Notation 4.1.1. *Let C be a code of length n over a ring R_k, we mean an additive submod-*

ule of the $R_k -$ module R_k^n. Let $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1}) \in R_k^n$ and $\boldsymbol{y} = (y_0, y_1, \ldots, y_{n-1}) \in R_;^n$, their scalar product is defined by

$$\boldsymbol{x}.\boldsymbol{y} = x_0y_0 + x_1y_1 + \ldots + x_{n-1}y_{n-1}.$$

Definition 4.1.2. A code of length n is $(1 - u^{k-1})-$constacyclic if the code is invariant under the Automorphism ν which has

$$\nu(a_0, a_1, \ldots, a_{n-1}) = ((1 - u^{k-1})a_{n-1}, a_0, \ldots, a_{n-2})$$

Proposition 4.1.2. *A subset C of R_k^n is a linear $(1 - u^{k-1})$ constacyclic of length n if and only if its polynomial representation is an ideal of $R_k[x]/x^n - (1 - u^{k-1})$.*

Proof. Similarly proof Proposition 3.2.1

□

4.2 A mapping construction

In [7] a linear isometry Gray map ϕ from $F_2 + uF_2$ into F_2^2 is defined and in [11], Gray linear map from $F_2 + uF_2 + u^2F_2$ into F_2^4 is also defined which extends the result in [7]. In this section we extend the result in [7] and [11], to define a linear Gray map from $R_k = F_2 + uF_2 + u^2F_2 + \ldots + u^{k-1}F_2$ into $F_2^{2^{(k-1)}}$.

Every element $c \in R$ can be written uniquely as $c = \beta_0(c) + u\beta_1(c) + u^2\beta_2(c) + \ldots + u^{k-1}\beta_{k-1}(c)$. We range the coefficients in the set $\{\beta_0, \beta_1, \beta_2, \ldots\ldots, \beta_{k-1}\}$ in the following ordering (we call it the $B-$ ordering): :

$\{0, \beta_0, \beta_1, (\beta_0 + \beta_1), \beta_2, \beta_2 + \beta_0, \beta_2 + \beta_1, (\beta_2 + \beta_1 + \beta_0), \beta_3, \beta_3 + \beta_0, \beta_3 + \beta_1, \beta_3 + \beta_1 + \beta_0, \beta_3 + \beta_2 + \beta_0, (\beta_3 + \beta_2 + \beta_1 + \beta_0), \beta_4, \beta_4 + \beta_0, \ldots\ldots, (\beta_4 + \beta_3 + \beta_2 + \beta_1 + \beta_0), \ldots\ldots, \beta_{k-3}, \beta_{k-3} + \beta_0, \beta_{k-3} + \beta_1, \ldots\ldots, (\beta_{k-3} + \beta_{k-4} + \beta_{k-3} + \ldots\ldots + \beta_0), \beta_{k-2}, \beta_{k-2} + \beta_0, \ldots\ldots, (\beta_{k-2} + \beta_{k-3} + \beta_{k-4} + \ldots\ldots \beta_0), \beta_{k-1}, \beta_{k-1} + \beta_0, ..., (\beta_{k-1} + \beta_{k-2} + ... + \beta_0)\}$.

Definition 4.2.1. We define the gray map $\phi : R_k \longrightarrow F_2^{2^{(k-1)}}$ as follows:-

$\phi(c) = (\beta_{k-1}(c), \beta_{k-1}(c) + \beta_0(c), \beta_{k-1}(c) + \beta_1(c), (\beta_{k-1}(c) + \beta_0(c) + \beta_1(c)), \beta_{k-1}(c) + \beta_2(c), \beta_{k-1}(c) + \beta_2(c) + \beta_0(c), \beta_{k-1}(c) + \beta_2(c) + \beta_1(c), (\beta_{k-1}(c) + \beta_2(c) + \beta_1(c) + \beta_0(c)), \beta_{k-1}(c) +$

$\beta_3(c), \beta_{k-1}(c)+\beta_3(c)+\beta_0(c), \beta_{k-1}(c)+\beta_3(c)+\beta_1(c), \beta_{k-1}(c)+\beta_3(c)+\beta_1(c)+\beta_0(c), \beta_{k-1}(c)+$
$\beta_3(c)+\beta_2(c)+\beta_0(c), (\beta_{k-1}(c)+\beta_3(c)+\beta_2(c)+\beta_1(c)+\beta_0(c)), \beta_{k-1}(c)+\beta_4(c), \beta_{k-1}(c)+$
$\beta_4(c)+\beta_0(c), \ldots\ldots, (\beta_{k-1}(c)+\beta_4(c)+\beta_3(c)+\beta_2(c)+\beta_1(c)+\beta_0(c)), \ldots\ldots, \beta_{k-1}(c)+$
$\beta_{k-3}(c), \beta_{k-1}(c)+\beta_{k-3}(c)+\beta_0(c), \beta_{k-1}(c)+\beta_{k-3}(c)+\beta_1(c), \ldots\ldots, (\beta_{k-1}(c)+\beta_{k-3}(c)+$
$\beta_{k-4}(c)+\beta_{k-3}(c)+\ldots\ldots+\beta_0(c)), \beta_{k-1}(c)+\beta_{k-2}(c), \beta_{k-1}(c)+\beta_{k-2}(c)+\beta_0(c), \ldots\ldots, (\beta_{k-1}(c)+$
$\beta_{k-2}(c)+\beta_{k-1}(c)+\beta_{k-3}(c)+\beta_{k-4}(c)+\ldots\ldots+\beta_0(c))).$

Claim ϕ is linear.

Proof: $\phi(c+c_1) = \phi(\beta_0(c)+\beta_0(c_1)+u(\beta_1(c)+\beta_1(c_1)+\ldots\ldots+u^{k-1}(\beta_{k-1}(c)+\beta_{k-1}(c_1))).$

$= \{\beta_{k-1}(c)+\beta_{k-1}(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_0(c)+\beta_0(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_1(c)+$
$\beta_1(c_1), (\beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_0(c)+\beta_0(c_1)+\beta_1(c)+\beta_1(c_1)), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_2(c)+$
$\beta_2(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_2(c)+\beta_2(c_1)+\beta_0(c)+\beta_0(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_2(c)+\beta_2(c_1)+$
$\beta_1(c)+\beta_1(c_1), (\beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_2(c)+\beta_2(c_1)+\beta_1(c)+\beta_1(c_1)+\beta_0(c)+\beta_0(c_1)), \beta_{k-1}(c)+$
$\beta_{k-1}(c_1)+\beta_3(c)+\beta_3(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_3(c)+\beta_3(c_1)+\beta_0(c)+\beta_0(c_1), \beta_{k-1}(c)+$
$\beta_{k-1}(c_1)+\beta_3(c)+\beta_3(c_1)+\beta_1(c)+\beta_1(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_3(c)+\beta_3(c_1)+\beta_1(c+c_1)+$
$\beta_0(c+c_1), \beta_{k-1}(c+c_1)+\beta_3(c+c_1)+\beta_2(c)+\beta_2(c_1)+\beta_0(c)+\beta_0(c_1), (\beta_{k-1}(c)+\beta_{k-1}(c_1)+$
$\beta_3(c)+\beta_3(c_1)+\beta_2(c)+\beta_2(c_1)+\beta_1(c)+\beta_1(c_1)+\beta_0(c)+\beta_0(c_1)), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_4(c)+$
$\beta_4(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_4(c)+\beta_4(c_1)+\beta_0(c)+\beta_0(c_1), \ldots\ldots, (\beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_4(c)+$
$\beta_4(c_1)+\beta_3(c)+\beta_3(c_1)+\beta_2(c)+\beta_2(c_1)+\beta_1(c)+\beta_1(c_1)+\beta_0(c)+\beta_0(c_1)), \ldots\ldots, \beta_{k-1}(c)+$
$\beta_{k-1}(c_1)+\beta_{k-3}(c)+\beta_{k-3}(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_{k-3}(c)+\beta_{k-3}(c_1)+\beta_0(c)+\beta_0(c_1), \beta_{k-1}(c)+$
$\beta_{k-1}(c_1)+\beta_{k-3}(c)+\beta_{k-3}(c_1)+\beta_1(c)+\beta_1(c_1), \ldots\ldots, (\beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_{k-3}(c)+\beta_{k-3}(c_1)+$
$\beta_{k-4}(c)+\beta_{k-4}(c_1)+\beta_{k-3}(c)+\beta_{k-3}(c_1)+\ldots\ldots+\beta_0(c)+\beta_0(c_1)), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_{k-2}(c)+$
$\beta_{k-2}(c_1), \beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_{k-2}(c)+\beta_{k-2}(c_1)+\beta_0(c)+\beta_0(c_1), \ldots\ldots, (\beta_{k-1}(c)+\beta_{k-1}(c_1)+$
$\beta_{k-2}(c)+\beta_{k-2}(c_1)+\beta_{k-1}(c)+\beta_{k-1}(c_1)+\beta_{k-3}(c)+\beta_{k-3}(c_1)+\beta_{k-4}(c)+\beta_{k-4}(c_1)+\ldots\ldots+$
$\beta_0(c)+\beta_0(c_1))\}$

so

$\phi(c+c_1) = \{\beta_{k-1}(c), \beta_{k-1}(c)+\beta_0(c), \beta_{k-1}(c)+\beta_1(c), (\beta_{k-1}(c)+\beta_0(c)+\beta_1(c)), \beta_{k-1}(c)+$
$\beta_2(c), \beta_{k-1}(c)+\beta_2(c)+\beta_0(c), \beta_{k-1}(c)+\beta_2(c)+\beta_1(c), (\beta_{k-1}(c)+\beta_2(c)+\beta_1(c)+\beta_0(c)), \beta_{k-1}(c)+$
$\beta_3(c), \beta_{k-1}(c)+\beta_3(c)+\beta_0(c), \beta_{k-1}(c)+\beta_3(c)+\beta_1(c), \beta_{k-1}(c)+\beta_3(c)+\beta_1(c)+\beta_0(c), \beta_{k-1}(c)+$
$\beta_3(c)+\beta_2(c)+\beta_0(c), (\beta_{k-1}(c)+\beta_3(c)+\beta_2(c)+\beta_1(c)+\beta_0(c)), \beta_{k-1}(c)+\beta_4(c), \beta_{k-1}(c)+$

$\beta_4(c)+\beta_0(c),\ldots\ldots,(\beta_{k-1}(c)+\beta_4(c)+\beta_3(c)+\beta_2(c)+\beta_1(c)+\beta_0(c)),\ldots\ldots,\beta_{k-1}(c)+$
$\beta_{k-3}(c),\beta_{k-1}(c)+\beta_{k-3}(c)+\beta_0(c),\beta_{k-1}(c)+\beta_{k-3}(c)+\beta_1(c),\ldots\ldots,(\beta_{k-1}(c)+\beta_{k-3}(c)+$
$\beta_{k-4}(c)+\beta_{k-3}(c)+\ldots\ldots+\beta_0(c)),\beta_{k-1}(c)+\beta_{k-2}(c),\beta_{k-1}(c)+\beta_{k-2}(c)+\beta_0(c),\ldots\ldots,(\beta_{k-1}(c)+$
$\beta_{k-2}(c)+\beta_{k-1}(c)+\beta_{k-3}(c)+\beta_{k-4}(c)+\ldots\ldots+\beta_0(c))\}\oplus\{\beta_{k-1}(c_1),\beta_{k-1}(c_1)+\beta_0(c_1),\beta_{k-1}(c_1)+$
$\beta_1(c_1),(\beta_{k-1}(c_1)+\beta_0(c_1)+\beta_1(c_1)),\beta_{k-1}(c_1)+\beta_2(c_1),\beta_{k-1}(c_1)+\beta_2(c_1)+\beta_0(c_1),\beta_{k-1}(c_1)+$
$\beta_2(c_1)+\beta_1(c_1),(\beta_{k-1}(c_1)+\beta_2(c_1)+\beta_1(c_1)+\beta_0(c_1)),\beta_{k-1}(c_1)+\beta_3(c_1),\beta_{k-1}(c_1)+\beta_3(c_1)+$
$\beta_0(c_1),\beta_{k-1}(c_1)+\beta_3(c_1)+\beta_1(c_1),\beta_{k-1}(c_1)+\beta_3(c_1)+\beta_1(c_1)+\beta_0(c_1),\beta_{k-1}(c_1)+\beta_3(c_1)+$
$\beta_2(c_1)+\beta_0(c_1),(\beta_{k-1}(c_1)+\beta_3(c_1)+\beta_2(c_1)+\beta_1(c_1)+\beta_0(c_1)),\beta_{k-1}(c_1)+\beta_4(c_1),\beta_{k-1}(c_1)+$
$\beta_4(c_1)+\beta_0(c_1),\ldots\ldots,(\beta_{k-1}(c_1)+\beta_4(c_1)+\beta_3(c_1)+\beta_2(c_1)+\beta_1(c_1)+\beta_0(c_1)),\ldots\ldots,\beta_{k-1}(c_1)+$
$\beta_{k-3}(c_1),\beta_{k-1}(c_1)+\beta_{k-3}(c_1)+\beta_0(c_1),\beta_{k-1}(c_1)+\beta_{k-3}(c_1)+\beta_1(c_1),\ldots\ldots,(\beta_{k-1}(c_1)+\beta_{k-3}(c_1)+$
$\beta_{k-4}(c_1)+\beta_{k-3}(c_1)+\ldots\ldots+\beta_0(c_1)),\beta_{k-1}(c_1)+\beta_{k-2}(c_1),\beta_{k-1}(c_1)+\beta_{k-2}(c_1)+\beta_0(c_1),\ldots\ldots,(\beta_{k-1}(c_1)+$
$\beta_{k-2}(c_1)+\beta_{k-1}(c_1)+\beta_{k-3}(c_1)+\beta_{k-4}(c_1)+\ldots\ldots+\beta_0(c_1))\}$.

Therefore $\phi(c+c_1)=\phi(c)+\phi(c_1)$.

The Gray map ϕ can be extended to R_k^n. For $c=(c_0,c_1,\ldots\ldots\ldots,c_{n-1})\in R_k^n$ define $\beta_i(C)=(\beta_i(c_0),\beta_i(c_1),\ldots\ldots,\beta_i(c_n))$, for $0\leq i\leq k-1$. Then ϕ is extended to R^n as follows:

$\phi(c)=(\beta_{k-1}(c),\beta_{k-1}(c)+\beta_0(c),\ldots\ldots\ldots,\beta_{k-1}(c)+\beta_{k-2}(c)+\ldots\ldots\ldots+\beta_0(c))$, for any $c\in R_k^n$.

The extended ϕ is bijection from R_k^n to $(F_2^{2^{(k-1)}})^n$.

The Generalized lee weights of the element $c\in R_k$ are defined by:

$$wt_{Gl}(C)=wt_H(\phi(C))=\begin{cases}2^{k-2}, & \text{if } C\neq u^{k-1};\\ 2^{k-1}, & \text{if C= } u^{k-1}.\end{cases}$$

and the generalized lee weight of 0 is 0.

The Generalized lee weight of a codeword in R_k^n is the rational integer sum of the Generalized lee weights of its coordinates.

The Generalized distance between two codewords c and c_1 is the generalized lee weight of $c-c_1$.

Proposition 4.2.1. *ϕ is distance-preserving map or isometry from (R_k^n, Generalized lee distance) to ($(F_2^{2^{(k-1)}})^n$, Hamming distance).*

For any $c \in R_k^n$, $\phi(c)$ is called binary image of c under ϕ.

Remark 4.2.1.
- $(1-u^{k-1})^n = 1-u^{k-1}$ if n is odd.
- $(1-u^{k-1})^n = 1$ if n is even.

4.3 $(1-u^{k-1})-$Constacyclic codes of odd length

Proposition 4.3.1. *Let μ be the map of $R_k[x]/(x^n-1)$ into $R_k[x]/(x^n-(1-u^{k-1}))$ defined by:*

$$\mu(f(x)) = f((1-u^{k-1})x)$$

If n is odd, then μ is a ring isomorphism.

Proof. First we will show that μ is a ring homomorphism.

For the polynomials $f(x), g(x) \in R_k[x]/(x^n-1)$, $\mu(f(x)+g(x)) = \mu((f+g)(x)) = (f+g)((1-u^{k-1})x)) = f((1-u^{k-1})x)) + g((1-u^{k-1})x))$

$$= \mu(f(x)) + \mu(g(x)).$$

And $\mu(f(x)g(x)) = \mu((fg)(x)) = (fg)((1-u^{k-1})x)) = f((1-u^{k-1})x)g((1-u^{k-1})x)$.

$$= \mu(f(x))\mu(g(x)).$$

Therefore μ is a ring homomorphism.

Now we will show μ is a one to one. For the polynomials $f(x), g(x) \in R_k[x]$, $f(x) \equiv g(x) mod\ (x^n-1)$ if and only if there exists a polynomial $h(x) \in R_k[x]$ such that $f(x) - g(x) = h(x)(x^n-1)$ if and only if n is odd and $f((1-u^{k-1})x) - g((1-u^{k-1})x) = h((1-u^{k-1})x)((1-u^{k-1})x)^n - 1)$, if and only if

$(1-u^{k-1})f((1-u^{k-1})x) - (1-u^{k-1})g((1-u^{k-1})x) = (1-u^{k-1})h((1-u^{k-1})x)((1-u^{k-1})^n x^n - 1)$

$$= h((1-u^{k-1})x)(x^n-(1-u^{k-1}))$$

if and only if

$$(1-u^{k-1})(\mu(f(x)) - \mu(g(x))) = h((1-u^{k-1})x)(x^n-(1-u^{k-1}))$$

if and only if

$$(\mu(f(x)) - \mu(g(x))) = (1 - u^{k-1})h((1 - u^{k-1})x)(x^n - (1 - u^{k-1}))$$

if and only if

$$\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (1 - u^{k-1}))).$$

That means, for $f, g \in R[x]/(x^n - 1)$, $\mu(f(x)) \equiv \mu(g(x))(\text{mod } (x^n - (1 - u^{k-1})))$ if and only if $f(x) \equiv g(x)(\text{mod } (x^n - 1))$. This implies that μ is a one to one homomorphism. To show μ is onto, let $f(x) \in R_k[x]/(x^n - (1 - u^{k-1}))$. Then there exists $f((1 - u^{k-1})x) \in R_k[x]/(x^n - 1)$ such that $\mu(f((1 - u^{k-1})x)) = f((1 - u^{k-1})^2 x) = f(x)$. Thus μ is onto.

Therefore, μ is a ring isomorphism. □

Here, we introduce the following example as an application of Proposition 4.3.1:

Example 4.3.1. *For $n = 7$.*

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \text{ in } R_k(x).$$

Applying the ring isomorphism μ, we have

$(1 - u^{k-1})^7 x^7 + 1 = ((1 - u^{k-1})x + 1)((1 - u^{k-1})^3 x^3 + (1 - u^{k-1})x + 1)((1 - u^{k-1})^3 x^3 + (1 - u^{k-1})^2 x^2 + 1)$.

By Remark 4.2.1 we have

$(1-u^{k-1})x^7+1 = ((1-u^{k-1})x+1)((1-u^{k-1})x^3+(1-u^{k-1})x+1)((1-u^{k-1})x^3+x^2+1)$

$(1-u^{k-1})(x^7+(1-u^{k-1})) = (1-u^{k-1})(x+(1-u^{k-1}))(1-u^{k-1})(x^3+x+(1-u^{k-1}))(1-u^{k-1})(x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$

$(1 - u^{k-1})(x^7 + (1 - u^{k-1})) = (1 - u^{k-1})^3(x + (1 - u^{k-1}))(x^3 + x + (1 - u^{k-1}))(x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$ $(1 - u^{k-1})(x^7 + (1 - u^{k-1})) = (1 - u^{k-1})(x + (1 - u^{k-1}))(x^3 + x + (1 - u^{k-1}))(x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$.

Multiplying by $(1 - u^{k-1})$we get

$x^7 + (1 - u^{k-1}) = (x + (1 - u^{k-1}))(x^3 + x + (1 - u^{k-1}))(x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$,

by Remark 4.2.1.

Now the following table explains the factorization of $x^n + (1 - u^{k-1})$ *into irreducible polynomials for* $1 \leq n \leq 31$, n *odd:*

n	*Factorization*
1	$(x + (1 - u^{k-1}))$
3	$(x + (1 - u^{k-1}))(x^2 + (1 - u^{k-1})x + 1)$
5	$(x + (1 - u^{k-1}))(x^4 + (1 - u^{k-1})x^3 + x^2 + (1 - u^{k-1})x + 1)$
7	$(x + (1 - u^{k-1}))(x^3 + x + (1 - u^{k-1}))(x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$
9	$(x + (1 - u^{k-1}))(x^2 + (1 - u^{k-1})x + 1)(x^6 + (1 - u^{k-1})x^3 + 1)$
11	$(x + (1 - u^{k-1}))(x^{10} + (1 - u^{k-1})x^9 + x^8 + (1 - u^{k-1})x^7 + \ldots\ldots + (1 - u^{k-1})x + 1)$
13	$(x + (1 - u^{k-1}))(x^{12} + (1 - u^{k-1})x^{11} + x^{10} + \ldots\ldots + (1 - u^{k-1})x + 1)$
15	$(x + (1 - u^{k-1}))(x^2 + (1 - u^{k-1})x + 1)(x^4 + (1 - u^{k-1})x^3 + x^2 + (1 - u^{k-1})x + 1)$ $(x^4 + (1 - u^{k-1})x + 1)(x^4 + (1 - u^{k-1})x^3 + 1)$
17	$(x + (1 - u^{k-1}))(x^8 + (1 - u^{k-1})x^7 + x^6 + x^4 + x^2 + (1 - u^{k-1})x + 1)$ $(x^8 + (1 - u^{k-1})x^5 + x^4 + (1 - u^{k-1})x^3 + 1)$
19	$(x + (1 - u^{k-1}))(x^{18} + (1 - u^{k-1})x^{17} + x^{16} + \ldots\ldots + x^2 + (1 - u^{k-1})x + 1)$
21	$(x + (1 - u^{k-1}))(x^2 + (1 - u^{k-1})x + 1)$ $(x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))(x^3 + x + (1 - u^{k-1}))$ $(x^6 + (1 - u^{k-1})x^5 + x^4 + x^2 + 1)(x^6 + x^4 + x^2 + (1 - u^{k-1})x + 1)$
23	$(x + (1 - u^{k-1}))(x^{11} + x^9 + x^7 + (1 - u^{k-1})x^6 + x^5 + x + (1 - u^{k-1}))$ $(x^{11} + (1 - u^{k-1})x^{10} + (1 - u^{k-1})x^6 + x^5 + (1 - u^{k-1})x^4 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$
25	$(x + (1 - u^{k-1}))(x^4 + (1 - u^{k-1})x^3 + x^2 + (1 - u^{k-1})x + 1)$ $(x^{20} + (1 - u^{k-1})x^{15} + x^{10} + (1 - u^{k-1})x^5 + 1)$
27	$(x + (1 - u^{k-1}))(x^2 + (1 - u^{k-1})(x^2 + (1 - u^{k-1})x + 1)$ $(x^6 + (1 - u^{k-1})x^3 + 1)(x^{18} + (1 - u^{k-1})x^9 + 1)$
29	$(x + (1 - u^{k-1}))$ $(x^{28} + (1 - u^{k-1})x^{27} + x^{26} + (1 - u^{k-1})x^{25} + \ldots\ldots + x^2 + (1 - u^{k-1})x + 1)$
31	$(x + (1 - u^{k-1}))(x^5 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))(x^5 + x^3 + (1 - u^{k-1}))$ $(x^5 + x^3 + (1 - u^{k-1})x^2 + x + (1 - u^{k-1}))$ $(x^5 + (1 - u^{k-1})x^4 + (1 - u^{k-1})x^2 + x + (1 - u^{k-1}))$ $(x^5 + (1 - u^{k-1})x^4 + x^3 + x + (1 - u^{k-1}))$ $(x^5 + (1 - u^{k-1})x^4 + x^3 + (1 - u^{k-1})x^2 + (1 - u^{k-1}))$

Corollary 4.3.2. *I is an ideal of $R_k[x]/(x^n - 1)$ if and only if $\mu(I)$ is an ideal of $R_k[x]/(x^n - (1 - u^{k-1}))$.*

Proof. similar to proof 3.2.4.

□

Corollary 4.3.3. *Let $\tilde{\mu}$ be the permutation of R_k^n with n odd, such that*
$\tilde{\mu}(a_0, a_1, \ldots, a_{n-1}) = (a_0, (1-u^{k-1})a_1, (1-u^{k-1})^2 a_2, \ldots, (1-u^{k-1})^i a_i, \ldots, (1-u^{k-1})^{n-1} a_{n-1})$,

and D be a subset of R_k^n; then D is a linear cyclic code over R_k if and only if $\tilde{\mu}(D)$ is a linear $(1-u^{k-1})$-constacyclic code.

Proof. We will show that the action of $\tilde{\mu}$ on vectors in D is the translation of the action of μ on polynomials in $\pi(D)$.

Let $D \subseteq R_k^n$ be linear cyclic code. If $a = (a_0, a_1, \cdots, a_{n-1}) \in D$ then all cyclic shifts of a are in D. This implies that the polynomial representation of a and its cyclic shift in $\pi(D)$ has the forms:

$a(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1}$ and

$xa(x) = xa_0 + a_1 x^2 + ... + a_{n-1}x^n$.

From the definition of μ we have

$\mu(a(x)) = a_0 + a_1(1-u^{k-1})x + \cdots + a_{n-1}(1-u^{k-1})^{n-1}x^{n-1}$ and $\mu(xa(x)) = (1-u^{k-1})xa_0 + (1-u^{k-1})^2 x^2 a_1 + \cdots + (1-u^{k-1})^n x^n a_{n-1} = a_{n-1} + (1-u^{k-1})xa_0 + (1-u^{k-1})^2 x^2 a_1 + \cdots + (1-u^{k-1})^{n-1}x^{n-1}a_{n-2}$ as $(1-u^{k-1})^n x^n = (1-u^{k-1})x^n = 1 \in R[x]/(x^n - (1-u^{k-1})$ *for* n odd.

This implies that

$$\tilde{\mu}(a_0, a_1, \ldots, a_{n-1}) = (a_0, (1-u^{k-1})a_1, (1-u^{k-1})^2 a_2, \ldots, (1-u^{k-1})^i a_i, \ldots, (1-u^{k-1})^{n-1} a_{n-1})$$

and $\tilde{\mu}(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) = (a_{n-1}, (1-u^{k-1})a_0, (1-u^{k-1})^2 a_1, \ldots, (1-u^{k-1})^i a_i, \ldots, (1-u^{k-1})^{n-1}a_{n-2}) \in \tilde{\mu}(D)$. Then $\tilde{\mu}(D)$ is a linear constacyclic code over R_k. The converse part is the same.

□

4.4 Gray map$(1-u^{k-1})-$Constacyclic codes

In this section, we generalize the results of [11].

Proposition 4.4.1. *Let ν be as Definition 4.1.2 and ψ_t be as Definition 3.1.2. Then $\phi\nu = \psi_{k-1}\phi$.*

Proof. Let $c = (c_0, c_1, \ldots, c_{n-1})$ be in R_k^n, $c_i = \beta_0(c_i) + u\beta_1(c_i) + u^2\beta_2(c_i) + \ldots + u^{k-1}\beta_{k-1}(c_i)$, where $\beta_k(c_i) \in F_2$. From definition of $\phi(c)$ we obtain

$\phi(c) = (\beta_{k-1}(c_0) \ldots\ldots, \beta_{k-1}(c_{n-1}), \beta_{k-1}(c_0)+\beta_0(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1}), ..., \beta_{k-1}(c_0)+\beta_0(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})|, \beta_{k-1}(c_0)+\beta_1(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_1(c_{n-1}), \beta_{k-1}(c_0)+\beta_2(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_2(c_{n-1}), ..., \beta_{k-1}(c_0)+\beta_{k-2}(c_0)+.....+\beta_1(c_0)+\beta_0(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_{k-2}(c_{n-1}) + ... + \beta_1(c_{n-1}) + \beta_0(c_{n-1}))$ and

$\psi_{k-1}\phi(c) = (\beta_{k-1}(c_{n-1})+\beta_0(c_{n-1}), \beta_{k-1}(c_0) \ldots\ldots, \beta_{k-1}(c_{n-1}), \beta_{k-1}(c_0)+\beta_0(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1}), ..., \beta_{k-1}(c_0)+\beta_0(c_0), ..., \beta_{k-1}(c_{n-2})+\beta_0(c_{n-2})|, \beta_{k-1}(c_{n-1})+\beta_{k-2}(c_{n-1})+.....+\beta_1(c_{n-1})+\beta_0(c_{n-1}), \beta_{k-1}(c_0)+\beta_1(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_1(c_{n-1}), \beta_{k-1}(c_0)+\beta_2(c_0), ..., \beta_{k-1}(c_{n-1})+\beta_2(c_{n-1}), ..., \beta_{k-1}(c_0)+\beta_{k-2}(c_0)+.....+\beta_1(c_0)+\beta_0(c_0), ..., \beta_{k-1}(c_{n-2})+\beta_{k-2}(c_{n-2})+ ..... + \beta_1(c_{n-2}) + \beta_0(c_{n-2}))$

On the other hand

$$\nu(c_0, c_1, \ldots, c_{n-1}) = ((1 - u^{k-1})c_{n-1}, c_0, \ldots, c_{n-2})$$

Note that

$$(1 - u^{k-1})c_{n-1} = \beta_0(c_{n-1}) + \beta_1(c_{n-1})u + ... + (\beta_{k-1}(c_{n-1}) + \beta_0(c_{n-1}))u^{k-1}$$

$\phi(\nu(c)) = \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1}), \beta_{k-1}(c_0), ..., \beta_{k-1}(c_{n-2}), \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_0(c_{n-1}), ..., \beta_{k-1}(c_{n-2})+\beta_0(c_{n-2}), ..., \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_0(c_{n-1}), ..., \beta_{k-1}(c_{n-2})+\beta_0(c_{n-2})|, \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_1(c_0), ..., \beta_{k-1}(c_{n-2})+\beta_1(c_{n-2}), \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_2(c_{n-1}), ..., \beta_{k-1}(c_{n-2})+\beta_2(c_{n-2}), ..., \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_{k-2}(c_{n-1})+.....+\beta_1(c_{n-1})+\beta_0(c_{n-1}), ..., \beta_{k-1}(c_{n-2})+\beta_{k-2}(c_{n-2}) + ... + \beta_1(c_{n-2}) + \beta_0(c_{n-2}).$

Now we have

$\phi(\nu(c)) = \beta_{k-1}(c_{n-1}) + \beta_0(c_{n-1}), \beta_{k-1}(c_0), ..., \beta_{k-1}(c_{n-2}), \beta_{k-1}(c_{n-1}), ..., \beta_{k-1}(c_{n-2}) + \beta_0(c_{n-2}), ..., \beta_{k-1}(c_{n-1}), ..., \beta_{k-1}(c_{n-2})+\beta_0(c_{n-2})|, \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_1(c_0), ..., \beta_{k-1}(c_{n-2})+\beta_1(c_{n-2}), \beta_{k-1}(c_{n-1})+\beta_0(c_{n-1})+\beta_2(c_{n-1}), ..., \beta_{k-1}(c_{n-2})+\beta_2(c_{n-2}), ..., \beta_{k-1}(c_{n-1})+\beta_{k-2}(c_{n-1}) + ... + \beta_1(c_{n-1}), ..., \beta_{k-1}(c_{n-2}) + \beta_{k-2}(c_{n-2}) + ... + \beta_1(c_{n-2}) + \beta_0(c_{n-2}).$

From above we have

$$\psi_{k-1}(\phi(c)) = \phi(\nu(c)).$$

□

Theorem 4.4.2. *The Gray image of a linear $(1-u^{k-1})$-constacyclic code over R_k is binary distance invariant linear quasi-cyclic code of order $k-1$.*

Proof. Let C be a linear $(1-u^{k-1})$-constacyclic code over R_k. Then $\nu(C) = C$, and therefore, $(\phi\nu)C = \phi(C)$. It follows from Proposition 4.4.1 that $\psi_{k-1}(\phi(C)) = \phi(C)$, which means that $\phi(C)$ is a linear quasi-cyclic code of order $k-1$. □

The following example represents a $(1-u^{k-1})-$constacyclic over R_1^7 where $R_4 = F_2 + uF_2 + u^2F_2 + u^3F_2$, $k = 4$ and its Gray image is $(F_2^{2^3})^7$.

Example 4.4.1. *From Example 4.3.1 we have,*
$x^7 + (1-u^{k-1}) = (x + (1-u^{k-1}))(x^3 + x + (1-u^{k-1}))(x^3 + (1-u^{k-1})x^2 + (1-u^{k-1}))$
Let $C = (x + (1-u^{k-1}))(x^3 + x + (1-u^{k-1})) = (1 + x^2 + (1-u^3)x^3 + x^4)$ *be a* $(1-u^3)$-*constacyclic code over* R_4 *generated be the polynomial* $(1 + x^2 + (1-u^3)x^3 + x^4)$
The code C *has length 7, and 14 the number of basis codewords.*
From Definition 4.2.1 of $\phi(c)$ *we have*
$\phi(c) = (\beta_3(c_0), ..., \beta_3(c_6), (\beta_3(c_0)+\beta_0(c_0), ..., \beta_3(c_6)+\beta_0(c_6), \beta_3(c_0)+\beta_1(c_0), ..., \beta_3(c_6)+$
$\beta_1(c_6), \beta_3(c_0) + \beta_2(c_0), ..., \beta_3(c_6) + \beta_2(c_6), \beta_3(c_0) + \beta_2(c_0) + \beta_0(c_0), ..., \beta_3(c_6) +$
$\beta_2(c_6) + \beta_0(c_6), \beta_3(c_0) + \beta_2(c_0) + \beta_1(c_0), ..., \beta_3(c_6) + \beta_2(c_6) + \beta_1(c_6), \beta_3(c_0) + \beta_1(c_0) +$
$\beta_0(c_0), ..., \beta_3(c_6) + \beta_1(c_6) + \beta_0(c_6) + \beta_3(c_0) + \beta_2(c_0) + \beta_1(c_0) + \beta_0(c_0), ..., \beta_3(c_6) +$
$\beta_2(c_6) + \beta_1(c_6) + \beta_0(c_6))$

and by Proposition 4.4.1 and Theorem 4.4.2 we have the following table:

i	c_i	$\phi(c_i)$
1	$(1,0,1,(1-u^3),1,0,0)$	$(0,0,0,1,0,0,0,1,0,1,0,1,0,0$
		$,0,0,0,1,0,0,0,0,0,0,1,0,0,0$
		$,1,0,1,0,1,0,0,0,0,0,1,0,0,0$
		$,1,0,1,0,1,0,0,1,0,1,0,1,0,0)$

2	$(0,1,0,1,(1-u^3),1,0)$	$(0,0,0,0,1,0,0,0,1,0,1,0,1,0$ $,0,0,0,0,1,0,0,0,0,0,0,1,0,0$ $,0,1,0,1,0,1,0,0,0,0,0,1,0,0$ $,0,1,0,1,0,1,0,0,1,0,1,0,1,0)$
3	$(0,0,1,0,1(1-u^3),1)$	$(0,0,0,0,0,1,0,0,0,1,0,1,0,1$ $,0,0,0,0,0,1,0,0,0,0,0,0,1,0$ $,0,0,1,0,1,0,1,0,0,0,0,0,1,0$ $,0,0,1,0,1,0,1,0,0,1,0,1,0,1)$
4	$((1-u^3),0,0,1,0,1,(1-u^3))$	$(1,0,0,0,0,0,1,0,0,0,1,0,1,0$ $,1,0,0,0,0,0,1,1,0,0,0,0,0,1$ $,0,0,0,1,0,1,0,1,0,0,0,0,0,1$ $,0,0,0,1,0,1,0,0,0,0,1,0,1,0)$
5	$(1,(1-u^3),0,0,1,0,1)$	$(0,1,0,0,0,0,0,1,0,0,0,1,0,1$ $,0,1,0,0,0,0,0,0,1,0,0,0,0,0$ $,1,0,0,0,1,0,1,0,1,0,0,0,0,0$ $,1,0,0,0,1,0,1,1,0,0,0,1,0,1)$
6	$((1-u^3),1,(1-u^3),0,0,1,0)$	$(1,0,1,0,0,0,0,0,1,0,0,0,1,0$ $,1,0,1,0,0,0,0,1,0,1,0,0,0,0$ $,0,1,0,0,0,1,0,1,0,1,0,0,0,0$ $,0,1,0,0,0,1,0,0,1,0,0,0,1,0)$
7	$(0,(1-u^3),1,(1-u^3),0,0,1)$	$(0,1,0,1,0,0,0,0,0,1,0,0,0,1$ $,0,1,0,1,0,0,0,0,1,0,1,0,0,0$ $,0,0,1,0,0,0,1,0,1,0,1,0,0,0$ $,0,0,1,0,0,0,1,0,0,1,0,0,0,1)$
8	$((1-u^3),0,(1-u^3),1,(1-u^3),0,0)$	$(1,0,1,0,1,0,0,0,0,0,1,0,0,0$ $,1,0,1,0,1,0,0,1,0,1,0,1,0,0$ $,0,0,0,1,0,0,0,1,0,1,0,1,0,0$ $,0,0,1,0,0,0,1,0,0,1,0,0,0,1)$

9	$(0,(1-u^3),0,(1-u^3),1,(1-u^3),0)$	$(0,1,0,1,0,1,0,0,0,0,0,1,0,0$ $,0,0,1,0,1,0,1,0,0,1,0,1,0,1$ $,0,0,0,0,0,1,0,0,0,1,0,1,0,1,0$ $,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0)$
10	$(0,0,(1-u^3),0,(1-u^3),1,(1-u^3))$	$(0,0,1,0,1,0,1,0,0,0,0,0,1,0$ $,0,0,1,0,1,0,1,0,0,1,0,1,0,1$ $,0,0,0,0,0,0,1,0,0,0,1,0,1,0,1$ $,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0)$
11	$(1,0,0,(1-u^3),0,(1-u^3),1)$	$(0,0,0,1,0,1,0,1,0,0,0,0,0,1$ $,0,0,0,1,0,1,0,0,0,0,1,0,1,0$ $,1,0,0,0,0,0,1,0,0,0,1,0,1,0$ $,1,0,0,0,0,0,0,1,1,0,0,0,0,0,1)$
12	$((1-u^3),1,0,0,(1-u^3),0,(1-u^3))$	$(1,0,0,0,1,0,1,0,1,0,0,0,0,0$ $,1,0,0,0,1,0,1,1,0,0,0,1,0,1$ $,0,1,0,0,0,0,0,1,0,0,0,1,0,1$ $,0,1,0,0,0,0,0,0,1,0,0,0,0,0)$
13	$(1,(1-u^3),1,0,0,(1-u^3),0)$	$(0,1,0,0,0,1,0,1,0,1,0,0,0,0$ $,0,1,0,0,0,1,0,0,1,0,0,0,1,0$ $,1,0,1,0,0,0,0,0,1,0,0,0,1,0$ $,1,0,1,0,0,0,0,1,0,1,0,0,0,0)$
14	$(0,1,(1-u^3),1,0,0,(1-u^3))$	$(0,0,1,0,0,0,1,0,1,0,1,0,0,0$ $,0,0,1,0,0,0,1,0,0,1,0,0,0,1$ $,0,1,0,1,0,0,00,0,1,0,0,0,1$ $,0,1,0,1,0,0,0,0,1,0,1,0,0,0)$

From the above table we deduce that $\phi(C)$, which has length=56, dimension=16 and distance=16, is a 3-quasi-cyclic binary linear code.

Conclusion

In this thesis, we have studied a new Gray map between codes over $R_k = \sum_{n=0}^{k-1} u^n F_2$ and codes over F_2 where $u^k = 0$ and also we proved that the Gray image of a linear $(1-u^{k-1})-$constacyclic codes over R_k of length n whenever n is odd is a binary distance invariant linear quasi-cyclic code of order $k-1$. It would be interesting to investigate $(1-u^{k-1})-$constacyclic codes over R_k of even length and investigates $(1-u^{k-1})-$constacyclic codes over more general rings $F_p + uF_p + ... + u^{k-1}F_p$ where p is prime of odd and even lengths.

Index

V

Z

Bibliography

[1] A. Bonnecazes and P. Udaya . "Cyclic codes and self-dual codes over $F_2 + uF2$." IEEE. IT, vol 45 , no . 4 pp 1250-1254 , 1999.

[2] A.R.Hammons Jr.,P.V.Kumar,A.R.Calderbank,N.J.A.Sloane and P.Sole,"The Z_4-linearty of Kerdock,Preparata,Goethals, and related codes," IEEE Trans Inform. Theory, vol.40, no.2, pp .301-319.1994.

[3] C. Bachoc, "Application of coding theory to the construction of modular lattices," J. Combin. Teory ser. A. vol.78, pp.92-119, 1997.

[4] D.G.Hoffman,D.A.Leonard,C.C.Lindner,K.T Phelps,C.A.Rodger,J.R.Wall,"Coding Theory." The Essentialsz Auburn University, 1991.

[5] H. Tapia-Recillas, G. vega"Some constacyclic codes over Z_{2^k} and binary quasi-cyclic codes". Discrete Applied Mathematics 128 (2003) 305-316.

[6] H. Tapia-Recillas and G. vega"On $Z_{2^k}-$linear and quaternary codes". Siam J. Discrete Math 2003 Society for Industrial and Applied Mathematics, vol. 17, no. 1, pp. 103-113.

[7] Hai Quang Dinh and Sergio R.López-Permouth"Cyclic and Negacyclic Codes Over Finite Chain Rings." IEEE transactions on information theory. vol, 50, no 8, august 2004, PP 1773-1741.

[8] I.N.Herstein" *Topics in Algebra*",University of Chicago.press1975.

[9] Jacques Wolfmann "Negacyclic and cyclic codes over Z_4" IEEE transactions on information theory, vOL.45, nO.7, november 1999. pp 2527-2532.

[10] Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu"$(1+u)$ constacyclic and cyclic over F_2+uF_2" Applied Mathematics Letters Volume 19, Issue 8, August 2006, pp 820-823.

[11] J . Qian, Li Zhang and Shi Zhu," Constacyclic and cyclic codes over $F_2+uF_2+u^2F_2$". Oxfored Journals Mathematics and Physical Sciences IEICE-Tran Fund Elec, Comm and Comp Sci volume E89-A, number 6, 2006 pp. 1863-1865.

[12] J . Wolfman "Binary Images of Cyclic Codes over Z_4" IEEE trans . inf . Th , vol . 47, no . 5 , July 2001 pp 1773-1779.

[13] Kiran. T and B. Sundar Rajan, Senior Member," Consta-Abelian codes Over Galois Rings IEEE Ttransactions on information theory, vOL.5O.nO, 2, februry 2004, 367-370.

[14] Mohammed M. Al-Ashker simplex codes over rhe ring F_2+uF_2, The Arabian Journal for Science and Engineering, volume 30, number 2A, 2005 pp 277-285.

[15] Mohammed M. Al-Ashker simplex codes over rhe ring $\sum_{n=0}^{s} u^n F_2$, Turk J Math, 29(2005), pp 221-233 TÜBİTAK.

[16] San ling and Chaoping xing "Coding Theory A first Course" Cambridge University press, 2004.

[17] V . Pless and Z . Qian , " Cyclic self-dual Z_4 codes". Finite fields and their applications 3. PP 48-69 , 1997.

[18] W.Cary Huffman, Vera Pless "*Fundemantal Of Error Correcting Codes*" printed in the United Kingdom Cambridge University Pres 2003.