**T.R.**
**ONDOKUZ MAYIS UNIVERSITY**
**INSTITUTE OF GRADUATE STUDIES**
**DEPARTMENT OF MATHEMATICS**

# CONSTACYCLIC CODES OVER SOME FINITE RINGS

Master's Thesis

**Abdallah K. A. BALAHA**

Supervisor
**Asst. Prof. Dr. Abdullah DERTLİ**

**SAMSUN**
**2021**

**T.R.**
**ONDOKUZ MAYIS UNIVERSITY**
**INSTITUTE OF GRADUATE STUDIES**
**DEPARTMENT OF MATHEMATICS**

# CONSTACYCLIC CODES OVER SOME FINITE RINGS

Master's Thesis

**Abdallah K. A. BALAHA**

Supervisor
**Asst. Prof. Dr. Abdullah DERTLİ**

**SAMSUN**
**2021**

## THESIS ACCEPTANCE AND APPROVAL

This study, titled "**Constacyclic Codes over Some Finite Rings**", prepared by **Abdallah K. A. BALAHA** under the supervision of **Asst. Prof. Dr. Abdullah DERTLİ**, was accepted as a Master's Thesis after being unanimously approved by our jury as a result of the exam held on 14 /07 / 2021.

| | **Title Name Surname**<br>**University**<br>**Major Science/Department** | **Signature** | **Result** |
|---|---|---|---|
| **Chairman** | Asst. Prof. Dr. Ergin BAYRAM<br>Ondokuz Mayıs University<br>Mathematics Department | | ☒ Acceptance<br>☐ Rejection |
| **Member**<br>**(Supervisor)** | Asst. Prof. Dr. Abdullah DERTLİ<br>Ondokuz Mayıs University<br>Mathematics Department | | ☒ Acceptance<br>☐ Rejection |
| **Member** | Asst. Prof. Dr. Esra ÖZTÜRK SÖZEN<br>Sinop University<br>Mathematics Department | | ☒ Acceptance<br>☐ Rejection |

This thesis has been approved by the above-named jury members determined by the Institute Administrative Board.

Approval
… / … / 2021
Prof. Dr. Ali BOLAT
Institute Director

## DECLARATION OF CONFORMITY TO SCIENTIFIC ETHICS

I declare that I comply with scientific ethics and academic rules at all stages of my master's proficiency thesis, that I refer to every quotation I use directly or indirectly in the study, and that the works I benefit from are those shown in the References. I undertake and declare that every element is written in accordance with the institute writing guide and that the situations specified in third item, ninth section of the TÜBİTAK Research and Publication Ethics Board Regulation are not violated.

Signature

14 / 07 / 2021

Abdallah K. A. BALAHA

## THESIS STUDY AUTHENTICITY REPORT STATEMENT

**Thesis title:** Constacyclic Codes over Some Finite Rings

As a result of the originality report that I have received from the plagiarism detection program on 15 / 06 / 2021 for the thesis with the above title and the following results were obtained:
Similarity rate : % 12
Single reference rate : % 2

Signature

15 / 06 / 2021

Asst. Prof. Dr. Abdullah DERTLİ

# ÖZET

BAZI SONLU HALKALAR ÜZERİNDE TANIMLI SABİT DEVİRLİ KODLAR
Abdallah K. A. BALAHA
Ondokuz Mayıs Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Anabilim Dalı
Yüksek Lisans Tezi, Temmuz 2021
Danışman: Dr. Öğr. Üyesi Abdullah DERTLİ

Bu tezde, $p$ asal, $i = 1,2,3,4$ ve $j = 3,4, i \neq$ j için $v_i^2 = v_i, v_1v_2 = v_2v_1$, $v_iv_j = v_jv_i = 0$ olmak üzere $R = F_p + v_1F_p + v_2F_p + v_3F_p + v_4F_p + v_1v_2F_p$ halkası üzerinde $\alpha_0 + \alpha_1v_1 + \alpha_2v_2 + \alpha_3v_3 + \alpha_4v_4 + \alpha_5v_1v_2$-sabit devirli kodların yapısı incelenmiştir. $R^n$ den $F_p^{6n}$ ye bir Gray dönüşümü tanımlanarak, $n$ uzunluğundaki $\alpha_0 + \alpha_1v_1 + \alpha_2v_2 + \alpha_3v_3 + \alpha_4v_4 + \alpha_5v_1v_2$-sabit devirli kodların Gray görüntüsünün $6n$ uzunluğunda $(\alpha_0, \alpha_0 + \alpha_1, \alpha_0 + \alpha_2, \alpha_0 + \alpha_3, \alpha_0 + \alpha_4, \alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)$-multi-twisted kod olduğu gösterilmiştir. Ayrıca keyfi bir uzunluğa sahip sabit devirli kodların üreteçleri belirlenmiştir. Son olarak, $p = 3$ alınarak $R$ halkası üzerinde tanımlı sabit devirli bir kodun Gray görüntüsü kullanılarak yapılan bir kod çözme yöntemi verilmiştir.

Anahtar Sözcükler: Sabit devirli kodlar, multi-twisted kodlar, dual kodlar, Gray dönüşümü.

## ABSTRACT

CONSTACYCLIC CODES OVER SOME FINITE RINGS
Abdallah K. A. BALAHA
Ondokuz Mayıs University
Institute of Graduate Studies
Department of Mathematics
Master's Thesis, July 2021
Supervisor: Asst. Prof. Dr. Abdullah DERTLİ

We study the structures of $\alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 + \alpha_5 v_1 v_2$-constacyclic codes over the family of rings $R = F_p + v_1 F_p + v_2 F_p + v_3 F_p + v_4 F_p + v_1 v_2 F_p$, where $p$ is a prime and $v_i^2 = v_i,\ v_1 v_2 = v_2 v_1,\ v_i v_j = v_j v_i = 0$, for $i = 1,2,3,4$ and $j = 3,4, i \neq j$. A Gray map from $R^n$ to $F_p^{6n}$ is introduced and it is shown that the images of $\alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 + \alpha_5 v_1 v_2$-constacyclic codes of length $n$ are $(\alpha_0, \alpha_0 + \alpha_1, \alpha_0 + \alpha_2, \alpha_0 + \alpha_3, \alpha_0 + \alpha_4, \alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)$-multi-twisted codes of length $6n$. The generators of such constacyclic codes for an arbitrary length are determined are also discussed. And finally, we describe the decoding procedure using the Gray image of constacyclic codes over $R$, where $p = 3$.



Keywords: Constacyclic codes, multi-twisted codes, dual codes, Gray map.

## ACKNOWLEDGMENTS

Here, I would like to show my sincere gratitude to my supervisor Asst. Prof. Dr. Abdullah DERTLİ “Thank you for sharing your knowledge and resources”.

I would like to thank Prof. Dr. Yasemin ÇENGELLENMİŞ for her valuable comments.

Finally, I would like also to thank my committee for their evaluation and the Turkey government scholarship administration for their support and fund.

**Abdallah K. A. BALAHA**
**SAMSUN 2021**

## TABLE OF CONTENTS

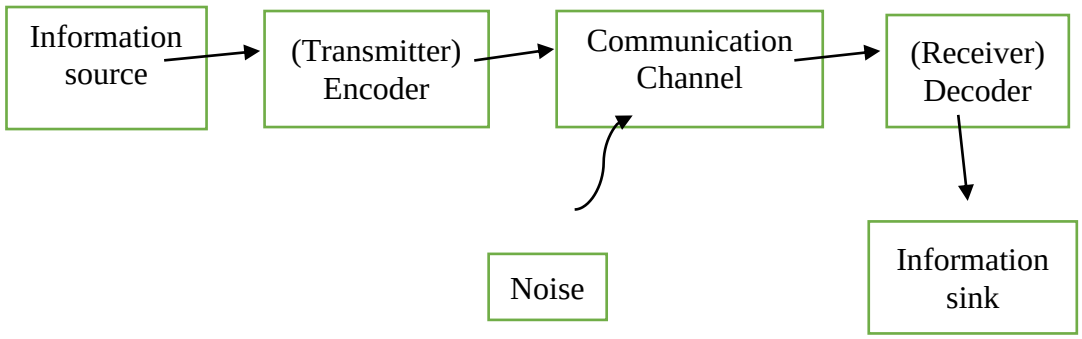
## LIST OF SYMBOLS

| | |
|---|---|
| $\oplus$ | : Direct sum |
| $\otimes$ | : Direct product |
| $\boldsymbol{R}$ | : The ring $F_p + v_1F_p + v_2F_p + v_3F_p + v_4F_p + v_1v_2F_p$ |
| $\boldsymbol{F_p}$ | : Field with $p$ elements, where $p$ is a prime |
| $\boldsymbol{F_q^n}$ | : $n$-dimensional vector space over $F_q$ |
| $\boldsymbol{\pi(a)}$ | : The polynomial representation of $a \in R^n$ |
| $\boldsymbol{R[x]}$ | : The ring of all polynomials with $R$ coefficients |
| $\boldsymbol{\langle I \rangle}$ | : Principal ideal generated by $I$ |
| $\boldsymbol{C}$ | : Usually, to denote a code |
| $\boldsymbol{C^{\perp}}$ | : The dual of the code $C$ |
| $\boldsymbol{d_H(x,y)}$ | : Hamming distance between $x$ and $y$ |
| $\boldsymbol{d_H(C)}$ | : Minimum Hamming distance of a code $C$ |
| $\boldsymbol{w_H(x)}$ | : Hamming weight of codeword $x$ |
| $\boldsymbol{d_L(x,y)}$ | : Lee distance between $x$ and $y$ |
| $\boldsymbol{d_L(C)}$ | : Minimum Lee distance of a code $C$ |
| $\boldsymbol{w_L(x)}$ | : Lee weight of codeword $x$ |
| $\boldsymbol{G}$ | : Usually, to denote a generator matrix of a code |
| $\boldsymbol{H}$ | : Usually, to denote a parity-check matrix of a code |
| $\boldsymbol{g(x)}$ | : Usually, to denote the generator polynomial of a code |
| $\boldsymbol{\phi(c)}$ | : Gray image of a $c \in R^n$ |
| $\boldsymbol{\sigma(c)}$ | : The cyclic shift of $c$ |
| $\boldsymbol{\varphi_s(c)}$ | : The quasi-cyclic shift of $c$. |
| $\boldsymbol{\gamma_\alpha(c)}$ | : The constacyclic shift of $c$. |
| $\boldsymbol{\varphi_{\Omega,s}(c)}$ | : The multi-twisted shift of $c$. |
| $\boldsymbol{(n,M,d)}$ | : A code of length $n$ with $M$ codewords and distance $d$ |
| $\boldsymbol{[n,k,d]}$ | : A linear code of length $n$, dimension $k$ and distance $d$ |

## LIST OF TABLES

## 1. INTRODUCTION

In 1948, Claude Shannon's 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. Shannon's colleague Richard Hamming had been laboring on error-correction for early computers even before Shannon's paper in 1948, and he made some of the first breakthroughs of coding theory. The following diagram shows the communication system for transmitting information from a source to a destination through a channel.




The most important part of the above 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 $G$ (Dahrouj, 2008).

In this thesis we are concerned about constacyclic codes over the finite rings, constacyclic codes are an important class of linear codes and have a great interest in coding theory. It was first introduced by Wolfman in (Wolfman, 1999). Since then, constacyclic codes have been studied by many authors. Zheng and Kong in (Zheng and Kong, 2017) studied cyclic and $\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$-constacyclic codes over $F_p + uF_p + vF_p + uvF_p$ with $u^2 = u$, $v^2 = v$ and $uv = vu$. Zhu and Wang in (Zhu and Wang, 2011) studied a class of constacyclic codes over $F_p + vF_p$ with $v^2 = v$. Dertli and Cengellenmis in (Dertli and Cengellenmis, 2020), obtained quantum codes from some constacyclic codes over a family of finite rings $F_p + uF_p + vF_p$, where $p$ is an odd prime and $u^2 = u$, $v^2 = v$ and $uv = vu$. The remainder of this thesis is organized as follows; in chapter 2, we discussed the preliminaries that we will use; in chapter 3, we define a Gray map from $R$ to $F_p^6$, then we gave the structures of $\alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 + \alpha_5 v_1 v_2$-constacyclic codes of arbitrary length over the ring $R$; in the last section of chapter 3, we give an example to describe how to apply the decoding algorithms by using the Gray image of such a constacyclic code.

## 2. PRELIMINARIES

### 2.1. General Definitions on Algebra

In this section, we introduce some elementary algebraic structures, such as groups, subgroups, rings, polynomial rings, ideals, maximal ideals, principal ideals, irreducible polynomial idempotent, locality of a ring and chain ring.

**Definition 2.1.1.** 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 $" \cdot "$ such that

i. For any $a, b \in G$ implies that $a \cdot b \in G$ (closed).

ii. For any $a, b, c \in G$ implies that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associative law).

iii. There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$ (the existence of an identity element in $G$).

iv. For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1}.a = e$ (the existence of inverses in $G$).

A group $G$ is said to be abelian or commutative if the binary operation is commutative (Hungerford, 2003).

***Example 2.1.1.*** The set of integer numbers $\mathbb{Z}$ is an abelian group under the ordinary addition, where $0$ is identity of this group.

***Example 2.1.2.*** Let $\mathbb{Z}_m$ denote the set of equivalence classes of $\mathbb{Z}$ under congruence modulo $m$, $\mathbb{Z}_m$ is an abelian group under the modular addition.

**Definition 2.1.2.** 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 (Hungerford, 2003).

**Definition 2.1.3.** A nonempty set $R$ is said to be a ring if in $R$, there are defined two operations, denoted by $" + "$ and $" \cdot "$ respectively, such that for all $a, b, c, \in R$ :

i. $R$ is an abelian group with respect to $" + "$;

ii. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ;

iii. left and right distributive laws:

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a$$

In addition:

iv. if $a \cdot b = b \cdot a$ for every $a, b \in R$, then $R$ is said to be a commutative ring.

v. if $R$ contains an element $1_R$ such that $1_R \cdot a = a \cdot 1_R = a$ for all $a \in R$, then R is said to be a ring with identity (Çallıalp, 2018).

**Definition 2.1.4.** An element $a$ in a ring $R$ with identity is said to be left (resp. right) invertible if there exists $c \in R$ (resp. $b \in R$) such that $c.a = 1_R$ (resp. $a.b = 1_R$). The element $c$ (resp. $b$) is called a left inverse (resp. right) inverse in $a$. An element $a \in R$ that is both left and right invertible is said to be invertible or to be a unit (Hungerford, 2003).

***Example 2.1.3.*** The set of $2 \times 2$ matrices with real number entries with the operations of matrix addition and matrix multiplication, this set satisfies the above ring axioms. The element

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

is the multiplicative identity of the ring. The ring is noncommutative.

**Definition 2.1.5.** A ring homomorphism $\phi$ from a ring $R$ to a ring $S$ is a mapping from $R$ to $S$ such that for all $a, b \in R$:

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

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

(Hungerford, 2003).

**Definition 2.1.6.** A ring homomorphism that is both one-to-one and onto is called an isomorphism (Hungerford, 2003).

**Definition 2.1.7.** Let $R$ be a ring. A nonempty subset $I$ of $R$ is called an ideal if

i. $a - b$ belong to $I$, for all $a, b \in I$,

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

(Ling and Xing, 2004).

***Example 2.1.4.*** For any ring, $\langle 0 \rangle$ and $R$ are trivial ideals of $R$.

**Definition 2.1.8.** 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

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

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 $g$ (Ling and Xing, 2004).

***Example 2.1.5.*** The ring $\mathbb{Z}$ is a principal ideal ring.

**Definition 2.1.9.** An ideal $I \neq R$ in a ring $R$ is said to be a maximal ideal of $R$ if for any ideal $J$ with $I \subseteq J$, either $J = I$ or $J = R$ (Herstein, 1975).

**Definition 2.1.10.** A zero-divisor is a nonzero element $a$ of a commutative ring $R$ such that there is a nonzero element $b \in R$ with $ab = 0$ (Herstein, 1975).

***Example 2.1.6.*** In the ring of integers $\mathbb{Z}$, the maximal ideals are the principal ideals generated by a prime number.

**Definition 2.1.11.** Let $I$ be an ideal of the ring $R$, the set of all equivalence classes of $R$ with respect to $I$ (denoted as $R/I$) is a ring under the two operation $\oplus$ and $\odot$ defined as

$$(a + I) \oplus (b + I) = (a + b) + I$$

$$(a + I) \odot (b + I) = (ab) + I$$

$R/I$ is called the quotient ring (Çallıalp, 2018).

**Definition 2.1.12.** A field is a nonempty set $F$ of elements with two operations '$+$' (called addition) and '$\cdot$' (called multiplication) satisfying the following conditions:

i. $F$ is a group under the addition operation.

ii. $F^*$ is also a group under the multiplication operation (Çallıalp, 2018).

**Remark.** A field of order $q$ is often called a Galois field of order $q$ and is denoted $GF(q)$ or $\boldsymbol{F}_q$.

**Theorem 2.1.1.** There exists a field of order $q$ if and only if $q$ is a prime power (i.e., $q = p^h$, where $p$ is prime and $h$ is a positive integer) (Hungerford, 1974).

**Definitions 2.1.13.** Let $\boldsymbol{F}$ be a field. The set

$$\boldsymbol{F}[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in \boldsymbol{F}, n \geq 0 \right\}$$

is called a polynomial ring over $\boldsymbol{F}$. An element of $\boldsymbol{F}[x]$ is called a polynomial over $\boldsymbol{F}$ (Herstein, 1975).

**Definition 2.1.14.** If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $q(x) = b_0 + b_1 x + \cdots + b_n x^n$ are in $\boldsymbol{F}[x]$, then $p(x) = q(x)$ if and only if for every integer $i \geq 0, a_i = b_i$. Thus, two polynomials are declared to be equal if and only if their corresponding coefficients are equal (Herstein, 1975).

**Definition 2.1.15.** If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $q(x) = b_0 + b_1 x + \cdots + b_n x^n$ are in $\boldsymbol{F}[x]$, then $p(x) + q(x) = c_0 + c_1 x + \cdots + c_t x^t$, where for each $i, c_i = a_i + b_i$ and $t = \max\{m, n\}$ (Herstein, 1975).

**Definition 2.1.16.** If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $q(x) = b_0 + b_1 x + \cdots + b_n x^n$ are in $\boldsymbol{F}[x]$, then $p(x).q(x) = c_0 + c_1 x + \cdots + c_t x^t$, where $c_t = a_t b_0 + a_{t-1} b_1 + a_{t-2} b_2 + \cdots + a_0 b_t$ and $t = m + n$ (Herstein, 1975).

**Definition 2.1.17.** If $f(x) = \sum_{i=0}^{n} a_i x^i \neq 0$ and $a^n \neq 0$, then the integer $n$ is called the degree of $f(x)$, denoted by $\deg\big(f(x)\big)$, if (for convenience, we define $deg(0) = -\infty$) (Herstein, 1975).

**Definition 2.1.18.** A nonzero polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ of degree $n$ is said to be monic if $a_n = 1$ (Herstein, 1975).

**Definition 2.1.19.** 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 (Herstein, 1975).

***Example 2.1.6.*** The polynomial $g(x) = \bar{1} + x + x^2 \in \mathbb{Z}_2[x]$ is of degree 2. It is irreducible; otherwise, it would have a linear factor $x$ or $x + \bar{1}$ ; i.e., $\bar{0}$ or $\bar{1}$ would be a root of $g(x)$, but $g(\bar{0}) = g(\bar{1}) = \bar{1} \in \mathbb{Z}_2$.

***Example 2.1.7.*** The polynomial $f(x) = x^4 + \bar{2}x^6 \in \mathbb{Z}_3[x]$ is of degree 6. It is reducible as $f(x) = x^4(\bar{1} + \bar{2}x^2)$.

***Example 2.1.8.*** In the ring $F_2[x]/\langle x^3 - 1\rangle$, the subset $I = \{\bar{0}, \overline{1+x}, \overline{x+x^2}, \overline{1+x^2}\}$ is an ideal.

***Example 2.1.9.*** In the ring $F_2[x]/\langle x^3 - 1\rangle$, the subset $I = \{\bar{0}, \overline{1+x}, \overline{x+x^2}, \overline{1+x^2}\}$ is a principal ideal generated by $1 + x$.

**Definition 2.1.20.** Two polynomials $f_1(x), f_2(x) \in R[x]$ are called coprime if $\langle f_1(x)\rangle + \langle f_2(x)\rangle = R[x]$, or equivalently, if there exist $g_1(x), g_2(x) \in R[x]$ such that $f_1(x)g_1(x) + f_2(x)g_2(x) = 1$ (Herstein, 1975).

A polynomial $f(x) \in R[x]$ is called regular if it is not a zero divisor.

**Definition 2.1.21.** We denote by $R_n = F_q[x]/\langle 1 + x^n\rangle$, the ring of all polynomial, modulo $(1 + x^n)$ over the field $F_q$ (Ling and Xing, 2004).

A polynomial $I(x) \in R_n$ is called idempotent, if $I^2(x) \equiv I(x) mod(1 + x^n)$.

**Example 2.1.10.** Consider the polynomial $\overline{x^3 + x^6} \in \mathbb{Z}_2[x]/\langle x^9 + 1\rangle$, $(x^3 + x^6) mod(1 + x^9)$ is an idempotent, because:

$$(x^3 + x^6)^2 = (x^6 + 2x^9 + x^{12})\ mod(1 + x^9) \equiv (x^3 + x^6) mod(1 + x^9)$$

over $\mathbb{Z}_2$.

**Definition 2.1.22.** 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 $\alpha v$ subject to "$\cdot$"

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

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

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

iv. $1v = v$;

for all $\alpha, \beta \in F$ and $v, w \in V$, where (the 1 represents the identity element of $F$ under multiplication) (Herstein, 1975).

**Definition 2.1.23.** If $V$ is a vector space over $F$ and if $W \subset V$, then $W$ is a subspace of $V$ whenever $w_1, w_2 \in W$ and $\alpha, \beta \in F$ implies that $\alpha w_1 + \beta w_2 \in W$ (Herstein, 1975).

**Definition 2.1.24.** Let $R$ be a ring. If there is at least positive integer $n$ such that $na = 0$ for all $a \in R$, then $R$ is said to have characteristic $n$. If no such $n$ exists $R$ is said to have characteristic zero. (Notation: $char\ R = n$) (Çallıalp, 2018).

***Example 2.1.11.*** The ring $\mathbb{Z}_p$ of integers has a characteristic of $p$.

**Definition 2.1.25.** Two sets, $A$ and $B$, are said to be equipollent, if there exists a bijective map $A \rightarrow B$; in this case we write $A \sim B$. Equipollence is an equivalence relation on the class $S$ of all sets (Hungerford, 2003).

**Definition 2.1.26.** The cardinal number (or cardinality) of a set $A$, denoted $|A|$, is the equivalence class of $A$ under the equivalence relation of equipollence. $|A|$ is an infinite or finite cardinal according as $A$ is an infinite or finite set (Hungerford, 2003).

**Definition 2.1.27.** A local ring is a commutative ring with identity which has a unique maximal ideal. A semi-local ring is a ring with finitely many maximal ideals. A ring $R$ with identity $1_R \neq 0$ in which every nonzero element is a unit is called a division ring (Hungerford, 2003).

**Note.** All fields are local rings, since $\{0\}$ is the only maximal ideal in these rings.

**Definition 2.1.28.** Let $R$ be a ring. A (left) $R$-module is an additive abelian group $A$ together with a function $R \times A \rightarrow A$ (the image of $(r, a)$ being denoted by $ra$ such that for all $r, s \in R$ and $a, b \in A$ :

i. $r(a + b) = ra + r\,b$

ii. $(r + s)a = ra + sa$

iii. $r(sa) = (rs)a.$

If $R$ has an identity element $1_R$ and

iv. $1_R a = a$ for all $a \in A$,

then $A$ is said to be a unitary $R$-module. If $R$ is a division ring, then a unitary $R$-module is called a (left) vector space (Hungerford, 2003).

**Definition 2.1.29.** Let $R$ be a ring, $A$ be an $R$-module and $B$ be a nonempty subset of $A$. $B$ is a submodule of $A$ provided that $B$ is an additive subgroup of $A$ and $rb \in B$ for all $r \in R$, $b \in B$. A submodule of a vector space over a division ring is called a subspace (Hungerford, 2003).

**Definition 2.1.30.** Let $R$ be a ring (usually assumed to be associative with an identity element) in which the left ideals form a chain. In other words, $R$ is a left chain ring if $R$ is a left chain module over itself. Every left chain ring is local. Right chain rings are defined similarly (Hungerford, 2003).

**Note.** Any field is a chain ring, since it has two ideals related by enclosure $\{0\}$ and the field itself.

**Theorem 2.1.2.** The rings $\mathbb{Z}, \boldsymbol{F}_q[x]$ and $\boldsymbol{F}_q[x]/\langle x^n - 1\rangle$ are all principal ideal rings (Ling and Xing, 2004).

***Proof.*** Let $I$ be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then $I = \langle 0\rangle$ is a principal ideal. Assume that $I \neq \{0\}$ and let $m$ be the smallest positive integer in $\mathbb{Z}$. Let $a$ be any element of $\mathbb{Z}$. By the division algorithm, we have

$$a = qm + r \qquad (*)$$

for some integers $q$ and $0 \leq r \leq m - 1$. The equality $(*)$ implies that $r$ is also an element of $I$ since $r = a - qm$. This force $r = 0$ by the choice of $m$. Hence, $I = \langle m\rangle$. This shows that $\mathbb{Z}$ is a principal ideal ring. Using the same arguments, we can easily show that $\boldsymbol{F}_q[x]$ is also a principal ideal ring. Essentially the same method can be employed for the case $\boldsymbol{F}_q[x]/\langle x^n - 1\rangle$. The zero ideal is obviously principal. We choose a nonzero polynomial $g(x)$ of a nonzero ideal $J$ with the lowest degree. For any polynomial $f(x)$ of $J$, we have

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

for some polynomials $s(x), r(x) \in \boldsymbol{F}_q[x]$ with $deg(r(x)) < deg(g(x))$. This force $r(x) = 0$, since $r(x) = f(x) - s(x)g(x) \in J$ and $g(x)$ has the lowest degree among the nonzero polynomials of $J$. Hence, $J = \langle g(x) \rangle$, and the desired result follows.

### 2.2. General Definitions on Codes

In this section, we define alphabet, codes, codewords, or strings, codes over fields, Hamming weights, Hamming distances and other elementary topics in coding theory.

**Definition 2.2.1.** Let $A = \{a_1, a_2, \ldots, a_q\}$ be a set of size $q$, which we refer to as a code alphabet and whose elements are called code symbols.

i. A $q$-ary word of length $n$ over $A$ is a sequence $w = w_1 w_2 \ldots w_n$ with each $w_i \in A$ for all $i$. Equivalently, $w$ may also be regarded as the vector $(w_1, w_2, \ldots, w_n)$.

ii. 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 $C \subset A^n$.

iii. An element of $C$ is called codeword in $C$.

iv. The number of codewords in $C$, denoted by $|C|$, is called the size of $C$.

v. The information rate of a code $C$ of length $n$ is defined to be $(\log_q |C|)/n$.

vi. A code of length $n$ and size $M$ is called an $(n, M)$-code (Ling and Xing, 2004).

***Example 2.2.1.*** Let $C = \{(0,0), (1,0), (0,1), (1,1)\}$. Then $(0,1)$ is a codeword and $|C| = 4$.

**Definition 2.2.2.** Let $x$ and $y$ be words of length $n$ over an alphabet $A$. The (Hamming) distance from $x$ to $y$, denoted by $d_H(x, y)$, is defined to be the number of places at which $x$ and $y$ differ. If $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then

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

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

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

(Ling and Xing, 2004).

***Example 2.2.2.*** Let $A = \{0, 1, 2, 3, 4\}$ and $x = (1,2,3,4), y = (1,4,2,3), z = (3,2,1,4)$. Then

$$d_H(x, y) = 3,$$

$$d_H(y, z) = 4,$$

$$d_H(z, x) = 2.$$

**Proposition 2.2.1.** Let $x, y, z$ be words of length $n$ over $A$. Then we have

i. $0 \leq d_H(x, y) \leq n,$

ii. $d_H(x, y) = 0 \Leftrightarrow x = y,$

iii. $d_H(x, y) = d_H(y, x),$

iv. $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$ (Ling and Xing, 2004).

**Definition 2.2.3.** For a code $C$ that containing at least two words, the (minimum Hamming) distance of $C$, denoted by $d_H(C)$, is

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

(Ling and Xing, 2004).

***Example 2.2.3.*** Consider the code $C = \{(0,0,0), (0,1,0), (1,0,1), (1,1,1)\}$, then $d_H(C) = 1$.

Let $\boldsymbol{F}_q^n$ be the set of all vectors of length $n$ with entries in $\boldsymbol{F}_q$ :

$$\boldsymbol{F}_q^n = \{(a_1, a_2, \dots, a_n) : a_i \in \boldsymbol{F}_q, i = 1, \dots, n\}.$$

The set $\boldsymbol{F}_q^n$ is a vector space over $\boldsymbol{F}_q$.

**Definition 2.2.4.** A linear code $C$ of length $n$ over finite field $\boldsymbol{F}_q$ is a subspace of the vector space $\boldsymbol{F}_q^n$ (Ling and Xing, 2004).

***Example 2.2.4.*** The code in (Example 2.2.3.) is a linear code of length $n$ over $\boldsymbol{F}_2$.

**Definition 2.2.5.** Let $x$ be a word in $\boldsymbol{F}_q^n$. The Hamming weight of $x$, denoted by $w_H(x)$, is defined to be the number of nonzero coordinates in $x$; i.e.,

$$w_H(x) = d_H(x, 0),$$

where 0 is the zero word (Ling and Xing, 2004).

***Example 2.2.5.*** The Hamming weight of $x = (0,0,1,1,0,1,0,1)$ is $w_H(x) = 4$.

**Lemma 2.2.2.** If $x, y \in \boldsymbol{F}_q^n$, then

$$d_H(x, y) = w_H(x - y)$$

(Ling and Xing, 2004).

***Proof.*** For $x, y \in \boldsymbol{F}_q^n, d_H(x, y) = 0$ if and only if $x = y$, which is true if and only if $x - y = 0$ or equivalently $w_H(x - y) = 0$.

$$d_H(x, y) = d_H(x_1, y_1) + d_H(x_2, y_2) + \cdots + d_H(x_n, y_n),$$

$$w_H(x) = w_H(x_1) + w_H(x_2) + \cdots + w_H(x_n).$$

Similarly

$$w_H(x - y) = w_H(x_1 - y_1) + w_H(x_2 - y_2) + \cdots + w_H(x_n - y_n)$$

$$w_H(x - y) = d_H(x_1, y_1) + d_H(x_2, y_2) + \cdots + d_H(x_n, y_n).$$

Then $d_H(x, y) = w_H(x - y)$.

**Definition 2.2.6.** Let $C$ be a code. The minimum (Hamming) weight of $C$, denoted by $w_H(C)$, is the smallest of the weights of the nonzero codeword of $C$ (Ling and Xing, 2004).

**Theorem 2.2.3.** Let $C$ be a linear code over $\boldsymbol{F}_q$. Then $d_H(C) = w_H(C)$ (Ling and Xing, 2004).

***Proof.*** From Lemma 2.2.2 we have $d_H(x,y) = w_H(x-y)$. From the Definition 2.2.3, there exist $'x, 'y \in C$ such that $d_H('x,'y) = d_H(C)$, so

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

since $'x - 'y \in C$.

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

$$w_H(C) = w_H(z) = d_H(z,0) \geq d_H(C)$$

Then we have

$$d_H(C) = w_H(C).$$

**Definition 2.2.7.** If $C$ is a $k$-dimensional subspace of $\boldsymbol{F}_q^n$, then $C$ will be called a linear $[n,k]$-code over $\boldsymbol{F}_q$ (Ling and Xing, 2004).

**Definition 2.2.8.** Let $C$ be a linear $[n,k]$-code. The set

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

is called the dual code for $C$, where $x \cdot c$ is the usual scalar product $x_1c_1 + x_2c_2 + \cdots + x_nc_n$ of the vectors $x = (x_1, x_2, \ldots, x_n)$ and $c = (c_1, c_2, \ldots, c_n)$. Note that $C^{\perp}$ is a linear $[n, n-k]$-code (Ling and Xing, 2004).

**Theorem 2.2.4.** Let $C$ be a linear code of length $n$ over $\boldsymbol{F}_q$. Then

i. $|C| = q^{\dim(C)}$,

ii. $\dim(C) + \dim(C^{\perp}) = n$,

iii. $(C^{\perp})^{\perp} = C$ (Ling and Xing, 2004).

**Definition 2.2.9.** Let $C$ be a linear code. $C$ is called self-orthogonal if $C \subset C^{\perp}$ and self-dual if $C = C^{\perp}$ (Ling and Xing, 2004).

**Theorem 2.2.5.** A self-dual linear code must have even length (Ling and Xing, 2004).

***Proof.*** Suppose that $C$ is a linear code of length $n$. From Theorem 2.2.4 we have $\dim(C) + \dim(C^{\perp}) = 2\dim(C) = n$, then $\dim(C) = n/2$. Therefore $n$ must be even.

### 2.3. Generator Matrix, Parity-check Matrix and Special Types of Codes

Knowing a 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.

**Definition 2.3.1.** i. A matrix $\boldsymbol{G}$ whose rows form a basis for $C$ is called a generator matrix for a linear code $C$.

ii. A parity-check matrix $\boldsymbol{H}$ for a linear code $C$ is a generator matrix for the dual code $C^{\perp}$ (Ling and Xing, 2004).

**Definition 2.3.2.** Any $k \times n$ matrix $\boldsymbol{G}$ with $k < n$ whose first $k$ columns the $k \times k$ identity matrix $\boldsymbol{I}_k$, so

$$\boldsymbol{G} = (\boldsymbol{I}_k | \boldsymbol{X})$$

has linearly independent rows and in RREF. Thus, $\boldsymbol{G}$ is a generator matrix for some linear code of length $n$ and dimension $k$. A generator matrix $\boldsymbol{G}$ is said to be standard form, and the code $C$ generated by $\boldsymbol{G}$ is called a systematic code (Ling and Xing, 2004).

**Theorem 2.3.1.** If $\boldsymbol{G} = (\boldsymbol{I}_k | \boldsymbol{X})$ is a generator matrix for the $[n, k]$ code $C$ in standard form, then $\boldsymbol{H} = (-\boldsymbol{X}^{\perp} | \boldsymbol{I}_{n-k})$ is a parity-check matrix for $C$ (Ling and Xing, 2004).

**Remark.** If $C$ is an [$n$, $k$]-linear code, then a generator matrix for $C$ must be a $k \times n$ matrix and a parity-check matrix for $C$ must be an $(n - k) \times n$ matrix.

**Theorem 2.3.2.** If $\boldsymbol{G}$ is a generator matrix for a linear code $C$, then any matrix row equivalent to $\boldsymbol{G}$ is also a generator matrix for $C$. In particular, any linear code has a generator matrix in RREF (Ling and Xing, 2004).

***Example 2.3.1.*** A generator matrix and a parity-check matrix for the binary linear code $C = \langle S \rangle$, where $S = \{(1,1,1,0,1), (1,0,1,1,0), (0,1,0,1,1), (1,1,0,1,0)\}$ are obtained as follows:

$$\boldsymbol{A} = \begin{pmatrix} 1\,1\,1\,0\,1 \\ 1\,0\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 1\,1\,0\,1\,0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1\,1\,1\,0\,1 \\ 0\,1\,0\,1\,1 \\ 0\,0\,1\,1\,1 \\ 0\,0\,0\,0\,0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1\,0\,0\,0\,1 \\ 0\,1\,0\,1\,1 \\ 0\,0\,1\,1\,1 \\ 0\,0\,0\,0\,0 \end{pmatrix}$$

which is in RREF. By Theorem 2.3.1, we have

$$\boldsymbol{G} = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right) \Longrightarrow \boldsymbol{H} = \begin{pmatrix} 0\,1\,1\,1\,0 \\ 1\,1\,1\,0\,1 \end{pmatrix}.$$

**Theorem 2.3.3.** Let $C$ be a linear code and let $\boldsymbol{H}$ be a parity-check matrix for $C$. Then

i. $C$ has distance $\geq d$ if and only if any $d-1$ columns of $\boldsymbol{H}$ are linearly independent; and

ii. $C$ has distance $\leq d$ if and only if $\boldsymbol{H}$ has $d$ columns that are linearly dependent (Ling and Xing, 2004).

**Corollary 2.3.4.** Let $C$ be a linear code and let $\boldsymbol{H}$ be a parity-check matrix for $C$. Then the following statements are equivalent:

i. $C$ has distance $d$;

ii. Any $d-1$ columns of $\boldsymbol{H}$ are linearly independent and $\boldsymbol{H}$ has $d$ columns that are linearly dependent (Ling and Xing, 2004).

***Example 2.3.2.*** Let $C$ be a linear code over $\boldsymbol{F}_2$ with parity-check matrix

$$\boldsymbol{H} = \begin{pmatrix} 1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0 \\ 0\,1\,0\,0\,1 \end{pmatrix}$$

By inspection, it is seen that there are no zero columns and no two columns of $\boldsymbol{H}$ sum to $\mathbf{0}$, so any two columns of $\boldsymbol{H}$ are linearly independent. However, columns 1, 3 and 4 sums to $\mathbf{0}$, and hence are linearly dependent. Therefore, the distance of $C$ is $d = 3$.

**Theorem 2.3.5.** If $\boldsymbol{H}$ is a parity-check matrix for a linear code $C$ of length $n$, then $C$ consists precisely of all words $x$ in $\boldsymbol{F}_q^n$ such that $\boldsymbol{x}\boldsymbol{H}^T = \mathbf{0}$. "And this is why it is called parity-check" (Ling and Xing, 2004).

**Definition 2.3.3.** A linear code is said to be cyclic of length $n$ over $R$ if it is invariant under the cyclic shift acting on $R$ defined by $\sigma(r_0, r_1, \dots, r_{n-1}) = (r_{n-1}, r_0, \dots, r_{n-2})$ (Ling and Xing, 2004).

***Example 2.3.3.*** Let $C = \{(0,0,0), (0,1,1), (1,1,0), (1,0,1)\}$ be a $[3,2,2]$-linear code over $\boldsymbol{F}_2$, then $C$ is a cyclic code.

**Remark:** In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following correspondence:

$$\pi : \boldsymbol{F}_q^n \longrightarrow \boldsymbol{F}_q\,[x]/\langle x^n - 1\rangle$$

$$(a_0, a_1, \dots, a_{n-1}) \longrightarrow a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

Then $\pi$ is an $\boldsymbol{F}_q$-linear transformation of vector spaces over $\boldsymbol{F}_q$. We know that $\boldsymbol{F}_q\,[x]/\langle x^n - 1\rangle$ is a ring (but not a field unless $n = 1$).

***Example 2.3.4.*** Consider the cyclic code

$$C = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\},$$

then

$$\pi(C) = \{\bar{0}, \overline{1+x}, \overline{1+x^2}, \overline{x+x^2}\} \subset \boldsymbol{F}_2[x]/\langle x^3 - 1\rangle.$$

**Theorem 2.3.6.** Let $\pi$ be as defined earlier. Then a nonempty subset $C$ of $\boldsymbol{F}_q^n$ is a cyclic code if and only if $\pi(C)$ is an ideal of $\boldsymbol{F}_q[x]/\langle x^n - 1\rangle$ (Ling and Xing, 2004).

**Theorem 2.3.7.** Let $I$ be a nonzero ideal in $\boldsymbol{F}_q[x]/\langle x^n - 1\rangle$ and let $g(x)$ be a nonzero monic polynomial of the least degree in $I$. Then $g(x)$ is a generator of $I$ and divides $x^n - 1$ (Ling and Xing, 2004).

**Theorem 2.3.8.** There is a unique monic polynomial of the least degree in every nonzero ideal $I$ of $\boldsymbol{F}_q[x]/\langle x^n - 1\rangle$ (Ling and Xing, 2004).

**Definition 2.3.4.** The unique monic polynomial of the least degree of a nonzero ideal $I$ of $\boldsymbol{F}_q[x]/\langle x^n - 1\rangle$ is called the generator polynomial of $I$. For a cyclic code $C$, the generator polynomial of $\pi(C)$ is also called the generator polynomial of $C$ (Ling and Xing, 2004).

**Definition 2.3.5.** For a given unit $\omega \in R$, a linear code is said to be $\omega$-constacyclic of length $n$ over $R$ if it is invariant under the $\gamma_\omega$-constacyclic shift acting on $R$ defined by

$$\gamma_\omega : R^n \to R^n$$

$$\gamma_\omega(r_0, r_1, \dots, r_{n-1}) = (\omega r_{n-1}, r_0, \dots, r_{n-2}).$$

Moreover, if $R = \boldsymbol{F}_q$, then $C$ is an ideal in the ring $\boldsymbol{F}_q[x]/\langle x^n - \omega \rangle$ (Zhu and Wang, 2011).

**Note.** When $\omega = 1$, $C$ is said to be a cyclic code. When $\omega = -1$, $C$ is said to be a negacyclic code.

**Definition 2.3.6.** A linear code is said to be quasi-cyclic of length $n = ms$ and order $s$ over $\boldsymbol{F}_p$ if it is invariant under the $\varphi_s$-quasi-cyclic shift acting on $\boldsymbol{F}_p^n$ defined by

$$\varphi_s : \boldsymbol{F}_p^n \to \boldsymbol{F}_p^n$$

$$\varphi_s(a^1|a^2|\dots|a^s) = (\sigma(a^1)|\sigma(a^2)|\dots|\sigma(a^s))$$

where $a^i \in \boldsymbol{F}_p^m$ (Zheng and Kong, 2017)**.**

**Definition 2.3.7.** For a given vector $\Omega = (\omega_i | \omega_i \in \boldsymbol{F}_p^*, 1 \le i \le s)$, a linear code is said to be $\Omega$-multi-twisted of length $n = ms$ and order $s$ over $\boldsymbol{F}_p$ if it is invariant under the $\varphi_{\Omega,s}$-multi-twisted shift acting on $\boldsymbol{F}_p^n$ defined by

$$\varphi_{\Omega,s} : \boldsymbol{F}_p^n \to \boldsymbol{F}_p^n$$

$$\varphi_{\Omega,s}(a^1|a^2|\dots|a^s) = (\gamma_{\omega_1}(a^1)|\gamma_{\omega_1}(a^2)|\dots|\gamma_{\omega_s}(a^s))$$

where $a^i \in \boldsymbol{F}_p^m$ (Aydin and Halilović, 2017)**.**

***Example 2.3.5.*** Let $v = (1,0,2,0,3,1), u = (1,2,0,1,2,1)$ and $w = (3,2,1,1,2,3)$ be codewords in $\boldsymbol{F}_5^6$:

i. $\gamma_2(v) = (2,1,0,2,0,3)$,

ii. $\varphi_2(u) = (0,1,2,1,1,2)$,

iii. $\varphi_{\Omega,2}(w) = (3,3,2,1,1,2),\ \Omega = (3,2)$.

### 2.4. Encoding and Decoding with Linear Codes

Let $C$ be an $[n, k, d]$-linear code over the finite field $\boldsymbol{F}_q$. Each codeword of $C$ can represent one piece of information, so $C$ can represent $q^k$ distinct pieces of information. Once a basis $\{r_1, \dots, r_k\}$ is fixed for $C$, each codeword $v$, or, equivalently, each of the $q^k$ pieces of information, can be uniquely written as a linear combination,

$$v = u_1 r_1 + \cdots + u_k r_k$$

where $u_1, \dots, u_k \in \boldsymbol{F}_q$.

Equivalently, we may set $\boldsymbol{G}$ to be the generator matrix of $C$ whose $i$th row is the vector $r_i$ in the chosen basis. Given a vector $u = (u_1, \dots, u_k) \in \boldsymbol{F}_q^k$, it is clear that

$$\boldsymbol{v} = \boldsymbol{uG} \leftrightarrow v = u_1 r_1 + \cdots + u_k r_k$$

is a codeword in $C$. Conversely, any $v \in C$ can be written uniquely as $\boldsymbol{v} = \boldsymbol{uG} \leftrightarrow v$, where $u = (u_1, \dots, u_k) \in \boldsymbol{F}_q^k$. Hence, every word $u \in \boldsymbol{F}_q^k$ can be encoded as $\boldsymbol{v} = \boldsymbol{uG}$.

The process of representing the elements $u$ of $\boldsymbol{F}_q^k$ as codewords $\boldsymbol{v} = \boldsymbol{uG} \leftrightarrow v$ in $C$ is called encoding.

***Example 2.4.1.*** Let $C$ be the binary [5, 3]-linear code with the generator matrix

$$\boldsymbol{G} = \begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1 \end{pmatrix}$$

$u = (0, 0, 1)$ is encoded as:

$$\boldsymbol{v} = \boldsymbol{uG} = (0\ 0\ 1) \begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1 \end{pmatrix} = (0\ 0\ 1\ 1) \leftrightarrow (0, 0, 1, 1)$$

**Remarks.** If an $[n, k, d]$-linear code $C$ has a generator matrix $\boldsymbol{G}$ in standard form, $\boldsymbol{G} = (\boldsymbol{I} \,|\boldsymbol{X})$, then it is trivial to recover the message $u$ from the codeword $\boldsymbol{v} = \boldsymbol{uG}$ since $\boldsymbol{v} = \boldsymbol{uG} = \boldsymbol{u}(\boldsymbol{I} \,|\boldsymbol{X}) = (\boldsymbol{u}, \boldsymbol{uX})$; i.e., the first $k$ digits in the codeword $\boldsymbol{v} = \boldsymbol{uG}$ give the message $u$ and they are called the message digits. The remaining

$n-k$ digits are called check digits. The check digits represent the redundancy which has been added to the message for protection against noise.

But when it comes to cyclic or constacyclic codes, it is more preferable to use the polynomial form for encoding and decoding processes. Here, the encoding process is simply a polynomial multiplication between the message polynomial and the generator polynomial of that code, while the decoding process tends to be more sophisticated (but still simple) in order to retrieve the original message.

***Example 2.4.2.*** Let $g(x) = 1 + x + x^2 + x^3 + x^6 \in \boldsymbol{F}_2[x]$ be the generator polynomial for a [15,9]-linear code and $m(x) = 1 + x$ be the message polynomial, then the corresponding codeword of that message is

$$c(x) = (1 + x)(1 + x + x^2 + x^3 + x^6) = 1 + x^4 + x^6 + x^7$$

or it can be rewritten as $m = (1,1,0,0,0,0,0,0,0)$ and

$$c = (1,0,0,0,1,0,1,1,0,0,0,0,0,0,0).$$

**Definition 2.4.1.** (Ling and Xing, 2004) Let $C$ be an $[n, k, d]$-linear code over $\boldsymbol{F}_q$ and let $H$ be a parity-check matrix for $C$. For any $\in \boldsymbol{F}_q^n$, the syndrome of $w$ is the word

$$S(w) = \boldsymbol{w}\boldsymbol{H}^T = \boldsymbol{z} \leftrightarrow z \in \boldsymbol{F}_q^{n-k}.$$

**Steps to construct a syndrome look-up table assuming complete nearest neighbor decoding**

*Step* 1: List all the cosets for the code, choose from each coset a word of least weight as coset leader $u$.

*Step* 2: Find a parity-check matrix $\boldsymbol{H}$ for the code, then for each coset leader $u$, calculate its syndrome $S(u) = \boldsymbol{u}\boldsymbol{H}^T$.

**Decoding procedure for syndrome decoding**

*Step* 1: For the received word $w$, compute the syndrome $S(w)$.

*Step* 2: Find the coset leader $u$ next to the syndrome $S(w) = S(u)$ in the syndrome look-up table.

*Step* 3: Decode $w$ as $v = w - u$.

***Example 2.4.3.*** Let $q = 2$ and $C = \{(0,0,0,0), (1,0,1,1), (0,1,0,1), (1,1,1,0)\}$. Decode $w = (1,1,0,1)$.

First, we need to find the parity-check matrix $\boldsymbol{H}$

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

then, we need to construct a syndrome look-up table

| Coset leader | Syndrome |
|---|---|
| $(0,0,0,0)$ | $(0,0)$ |
| $(0,0,0,1)$ | $(0,1)$ |
| $(0,0,1,0)$ | $(1,0)$ |
| $(1,0,0,0)$ | $(1,1)$ |

Then we compute

$$S(w) = \boldsymbol{w}\boldsymbol{H}^T = (1\ 1\ 0\ 1)\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} = (1\ 1) \leftrightarrow (1,1).$$

From the table above, the coset leader is $(1,0,0,0)$. Therefore, $(1,1,0,1) - (1,0,0,0) = (0,1,0,1)$ was the most likely codeword sent.

The same procedures can be carried upon polynomials with a simple modification.

**Theorem 2.4.1.** Let $\boldsymbol{H} = (\boldsymbol{I}_{n-k} | \boldsymbol{A})$ be a parity-check matrix of a $q$-ary cyclic code $C$. Let $g(x)$ be the generator polynomial of $C$. Then the syndrome of a vector $w \in \boldsymbol{F}_q^n$ is equal to $w(x)\ mod\ g(x)$; i.e., the principal remainder of $w(x)$ divided by $g(x)$ (note that here we identify a vector of $\boldsymbol{F}_q^n$ with a polynomial of $\boldsymbol{F}_q[x]/(x^n - 1)$, and thus $w(x)$ is the corresponding polynomial of $w$ (Ling and Xing, 2004).

**Definition 2.4.2.** A cyclic run of 0 of length l of an $n$-tuple is a succession of $l$ cyclically consecutive zero components (Ling and Xing, 2004).

***Example 2.4.4.*** $c = (0,0,0,1,1,0,1,0,0,1,0)$ has a cyclic run of 4 consecutive zero components.

**Decoding algorithm for cyclic codes:**

Let $C$ be a $q$-ary $[n, k, d]$-cyclic code with generator polynomial $g(x)$. Let $w(x)$ be a received word with an error pattern $e(x)$, where $w_H(e(x)) \leq \lfloor (d-1)/2 \rfloor$ and $e(x)$ has a cyclic run of 0 of length at least $k$. The goal is to determine $e(x)$.

*Step 1*: Compute the syndromes of $x^i w(x)$, for $i = 0, 1, 2, \ldots$, and denote by $s_i(x)$ the syndrome $(x^i w(x) \ (mod\ g(x)))$.

*Step 2*: Find $m$ such that the weight of the syndrome $s_m(x)$ for $x^m w(x)$ is less than or equal to $\lfloor (d-1)/2 \rfloor$.

*Step 3*: Compute the remainder $e(x)$ of $x^{n-m} s_m(x)$ divided by $x^n - 1$. Decode $w(x)$ to $w(x) - e(x)$.

***Example 2.4.5.*** Consider the binary [15,7,5]-cyclic code generated by $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, by following the above algorithm, we can correct up to 2 bits by an error pattern with a cyclic run of zeros of length at least 7.

Consider the received word

$$w(x) = (1,1,0,0,1,1,1,0,1,1,0,0,0,1,0) = 1 + x + x^4 + x^5 + x^6 + x^8 + x^9 + x^{13}$$

By Computing the syndromes $s_i(x)$ of $x^i w(x)$ until $w_H(s_i(x)) \leq 2$, we see that it is only true for $s_7(x) = 1 + x^5$, thus $w(x)$ decoded to

$$w(x) - x^8 s_7(x) = w(x) - x^8 - x^{13} = 1 + x + x^4 + x^5 + x^6 + x^9$$

$$= (1,1,0,0,1,1,1,0,0,1,0,0,0,0,0).$$

## 3. CONSTACYCLIC CODES OVER $R$

In this chapter, we discussed some details about the ring $R$ in theorem/proof manner. We also discussed some results describing the general structure of $\omega$-constacyclic code over the same ring in the same manner, where $\omega = \alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 + \alpha_5 v_1 v_2$. It is fair to mention that most of the theorems in this chapter were proved under the light of (Zhu et al., 2010), (Qian et al., 2006), (Zhu and Wang, 2011) and (Zheng and Kong, 2017).

### 3.1. The Algebraic Structure of $R$

Consider the polynomial quotient ring

$$R^{\sim} = \boldsymbol{F}_p[v_i]/\langle v_i^2 - v_i, v_i v_j = v_j v_i, v_1 v_2 - v_2 v_1\rangle$$
$$= \left\{ \begin{matrix} a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2 + \langle v_i^2 - v_i\,, v_i v_j = v_j v_i, v_1 v_2 - v_2 v_1\rangle : \\ a_s \in \boldsymbol{F}_p\,, 0 \le s \le 5, i = 1,2,3,4,\ \ j = 3,4, i \ne \mathrm{j} \end{matrix} \right\}$$

Since

$$a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2 + \langle 0\rangle$$
$$= \left\{ \begin{matrix} a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2 + 0 \cdot k : a_s \in \boldsymbol{F}_p, \\ k \in \boldsymbol{F}_p[v_i]\,, 0 \le s \le 5, i = 1,2,3,4 \end{matrix} \right\}$$
$$= \{a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2\}$$

we have

$$R^{\sim} = \left\{ \{a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2\} : a_s \in \boldsymbol{F}_p\,, 0 \le s \le 5 \right\}.$$

So $R \coloneqq \boldsymbol{F}_p + v_1 \boldsymbol{F}_p + v_2 \boldsymbol{F}_p + v_3 \boldsymbol{F}_p + v_4 \boldsymbol{F}_p + v_1 v_2 \boldsymbol{F}_p$ is a commutative finite ring.

**Theorem 3.1.1.** $R \cong R^{\sim}$.

***Proof.*** Let us define a mapping from $R$ to $R^{\sim}$ as follows:

$$f : R \to R^{\sim}$$

$$a = a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2 \longmapsto f(a) = \zeta$$

where $\zeta = \{a_0 + a_1 v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4 + a_5 v_1 v_2\}$.

Let $a$ and $b$ be two arbitrary elements in $R$, where

$$a = a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2,$$

$$b = b_0 + b_1v_1 + b_2v_2 + b_3v_3 + b_4v_4 + b_5v_1v_2.$$

$$a = b \Leftrightarrow a_i = b_i, 0 \leq i \leq 5 \Leftrightarrow \{a\} = \{b\} \Leftrightarrow f(a) = f(b)$$

from the last statement, the mapping $f$ is well-defined and one-to-one.

It is clear to see that $|R| = |R^{\sim}| = p^6$, and since $f$ is one-to-one, $f$ is also surjective.

$$\begin{aligned} f(a+b) = f(&a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2 + b_0 + b_1v_1 + b_2v_2 \\ &+ b_3v_3 + b_4v_4 + b_5v_1v_2) \\ &= f((a_0 + b_0) + (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + (a_3 + b_3)v_3 + (a_4 \\ &+ b_4)v_4 + (a_5 + b_5)v_1v_2) \\ &= \{(a_0 + b_0) + (a_1 + b_1)v_1 + (a_2 + b_2)v_2 + (a_3 + b_3)v_3 + (a_4 \\ &+ b_4)v_4 + (a_5 + b_5)v_1v_2\} \\ &= \{a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2\} + \{b_0 + b_1v_1 \\ &+ b_2v_2 + b_3v_3 + b_4v_4 + b_5v_1v_2\} = f(a) + f(b) \end{aligned}$$

$$\begin{aligned} f(a \cdot b) = f(&a_0b_0 + (a_0b_1 + a_1b_0 + a_1b_1)v_1 + (a_0b_2 + a_2b_0 + a_2b_2)v_2 \\ &+ (a_0b_3 + a_3b_0 + a_3b_3)v_3 + (a_0b_4 + a_4b_0 + a_4b_4)v_4 \\ &+ (a_0b_5 + a_1b_2 + a_1b_5 + a_2b_1 + a_2b_5 + a_5b_0 + a_5b_1 + a_5b_2 \\ &+ a_5b_5)v_1v_2) \\ &= \{a_0b_0 + (a_0b_1 + a_1b_0 + a_1b_1)v_1 + (a_0b_2 + a_2b_0 + a_2b_2)v_2 \\ &+ (a_0b_3 + a_3b_0 + a_3b_3)v_3 + (a_0b_4 + a_4b_0 + a_4b_4)v_4 \\ &+ (a_0b_5 + a_1b_2 + a_1b_5 + a_2b_1 + a_2b_5 + a_5b_0 + a_5b_1 + a_5b_2 \\ &+ a_5b_5)v_1v_2\} \end{aligned}$$

$$\begin{aligned} f(a) \cdot f(b) = &\{a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2\} \cdot \{b_0 + b_1v_1 + b_2v_2 \\ &+ b_3v_3 + b_4v_4 + b_5v_1v_2\} = f(a \cdot b) \end{aligned}$$

from the last two equalities, we showed that $f$ is a ring homomorphism. Therefore, $f$ is a ring isomorphism from $R$ to $R^{\sim}$. ■

We define $R$ to be the ring with all the elements of the form

$$a = a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2$$

where $a_s \in \boldsymbol{F}_p, 0 \leq s \leq 5$ and $v_i^2 = v_i, 1 \leq i \leq 4$ ; $v_1v_2 = v_2v_1$ ; $v_2v_4 = v_1v_3 = v_3v_4 = v_2v_3 = v_1v_4 = 0$.

Every element $a \in R$ can be rewritten as

$$a = a_0\lambda_1 + (a_0 + a_1)\lambda_2 + (a_0 + a_2)\lambda_3 + (a_0 + a_3)\lambda_4 + (a_0 + a_4)\lambda_5 + (a_0 + a_1 + a_2 + a_5)\lambda_6$$

where

$$\lambda_1 = 1 - v_1 - v_2 - v_3 - v_4 + v_1v_2,$$

$$\lambda_2 = v_1 - v_1v_2,$$

$$\lambda_3 = v_2 - v_1v_2 ,$$

$$\lambda_4 = v_3,$$

$$\lambda_5 = v_4 ,$$

$$\lambda_6 = v_1v_2.$$

It is easy to show that the following formulas are true:

$$\lambda_i^2 = \lambda_i, 1 \leq i \leq 6;\ \lambda_i\lambda_j = 0, i \neq j;\ \sum_{i=1}^{6} \lambda_i = 1.$$

**Theorem 3.1.2.** The characteristic of $R$ is $p$. Moreover, every element $a$ in $R^*$ is a zero divisor unless $(a^{p-1} - 1) = 0$ , where $p$ is prime.

***Proof.*** Consider the ring $R = \boldsymbol{F}_p + v_1\boldsymbol{F}_p + v_2\boldsymbol{F}_p + v_3\boldsymbol{F}_p + v_4\boldsymbol{F}_p + v_1v_2\boldsymbol{F}_p$, let $a \in R$ such that $a = a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_1v_2$, then $pa = pa_0 + pa_1v_1 + pa_2v_2 + pa_3v_3 + pa_4v_4 + pa_5v_1v_2 = 0$, since $char\boldsymbol{F}_p = p$. Thus $charR = p$.

Moreover, according to Fermat's theorem, which states that: If $p$ is prime, then $a^p = a$ for all $a \in \boldsymbol{F}_p$ or equivalently, $a^p = a(mod\ p)$ for all $p$. In $R$, $a^p = a_0^p\lambda_1 + (a_0 + a_1)^p\lambda_2 + (a_0 + a_2)^p\lambda_3 + (a_0 + a_3)^p\lambda_4 + (a_0 + a_4)^p\ \lambda_5 + (a_0 + a_1 + a_2 + a_5)^p\lambda_6 = a_0\lambda_1 + (a_0 + a_1)\lambda_2 + (a_0 + a_2)\lambda_3 + (a_0 + a_3)\lambda_4 + (a_0 + a_4)\lambda_5 +$

$(a_0 + a_1 + a_2 + a_5)\lambda_6 = a$, then $a(a^{p-1} - 1) = 0$, which gives that every element in $R^*$ is a zero divisor unless $(a^{p-1} - 1) = 0$. ■

The previous theorem gives us a condition which is satisfied by every element in $R$ except $1_R$. But we already know that $\lambda_i\lambda_j = 0, i \neq j$, which also makes these zero divisors too. By this fact we deduce that $R$ is not an integral domain ring.

**Remark:** When $p = 2$, there is no unit in $R$ except $1_R$.

**Theorem 3.1.3.** For all $a \in R$, $a$ is a unit in $R$ if and only if $\alpha_i \neq 0$, where $a = \sum_{i=1}^{6} \alpha_i\lambda_i$.

***Proof.*** Assume that $a$ be a unit in $R$ such that $a = \sum_{i=1}^{6} \alpha_i\lambda_i$, where $\alpha_j = 0$ for some $j$ and let $a^{-1}$ be the inverse of $a$ in $R$ such that $a \cdot a^{-1} = (\sum_{i=1}^{6} \alpha_i\lambda_i)(\sum_{i=1}^{6} \alpha_i^{-1}\lambda_i) = \sum_{i=1}^{6} \alpha_i\alpha_i^{-1}\lambda_i = \sum_{i=1}^{6} \lambda_i = 1$. But, in order to make the last equality true, $\alpha_i\alpha_i^{-1}$ must equal 1, where $1 \leq i \leq 6$. Since $\alpha_j = 0$ for some $j$, there is no element in the field $\boldsymbol{F}_p$ satisfy the equality of $\alpha_j\alpha_i^{-1} = 0\alpha_i^{-1} = 1$, and this contradict with the first assumption. Hence, $a$ is a unit in $R$ if $\alpha_i \neq 0$, where $a = \sum_{i=1}^{6} \alpha_i\lambda_i$.

Assume that $a \in R$ and $\alpha_i \neq 0$, where $a = \sum_{i=1}^{6} \alpha_i\lambda_i$. Since $\alpha_i \in \boldsymbol{F}_p$, there exist $\alpha_i^{-1} \in \boldsymbol{F}_p$ such that $\alpha_i\alpha_i^{-1} = 1$. Now let $a^{-1}$ be in $R$ such that $a^{-1} = \sum_{i=1}^{6} \alpha_i^{-1}\lambda_i$, then $a \cdot a^{-1} = (\sum_{i=1}^{6} \alpha_i\lambda_i)(\sum_{i=1}^{6} \alpha_i^{-1}\lambda_i) = \sum_{i=1}^{6} \alpha_i\alpha_i^{-1}\lambda_i = \sum_{i=1}^{6} \lambda_i = 1$, which implies that $a^{-1}$ is the inverse of $a$ and $a$ is unit in $R$. Therefore, for all $a \in R$, $a$ is a unit in $R$ if and only if $\alpha_i \neq 0$, where $a = \sum_{i=1}^{6} \alpha_i\lambda_i$. ■

**Theorem 3.1.4.** $R$ is a non-chain ring.

***Proof.*** The proof is trivial since $\langle\lambda_i\rangle$s are ideals in $R$ and $\langle\lambda_i\rangle \cap \langle\lambda_j\rangle = \{0\}$, where $i \neq j$. ■

**Theorem 3.1.5.** $R$ is a local ring with a unique maximal ideal generated by $\langle\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5, \lambda_6\rangle$, where $p = 3$.

***Proof.*** In order to prove this theorem, the following algorithm has been written to find the non-unit set, then check whether it is an ideal or not, then finding its generating elements.

**Start:**

Step 1: List $R$ elements in $\sum_{i=1}^{6} a_i\lambda_i$ form;

Step 2: Construct a multiplication table for $R$ as $T$;

Step 3: For each column $c$ in $T$

If $1 = \sum_{i=1}^{6} \lambda_i$ is not a member of $c$, then

Add the first element in column $c$ to the set of non-units $U$;

Else Continue;

Step 4: For each $u$ in $U$

If $u \cdot R$ is in $U$ and

If $u + U$ is in $U$ and

If $\big(u + (p-1)\big) \cdot U$ is in $U$, then

$U$ is the maximal ideal;

Else $U$ is not an ideal;

Step 5: if $U$ is the maximal ideal, then

Select $i$ elements from $U$ as $\{u_1, \dots, u_i\}$, where $i = 1$;

For each $\{u_1, \dots, u_i\}$ combination in $U$

If $u_1 \cdot R + \cdots + u_i \cdot R$ is equal to $U$, then

$U$ generated by $\langle u_1, \dots, u_i \rangle$;

Else $i = i + 1$;

Else **End.**

By implementing the previous algorithm using MATLAB, the theorem proved. ■

**Theorem 3.1.6.** $R \cong \bigotimes_{1 \le i \le 6} \langle \lambda_i \rangle$.

***Proof.*** Since $R = \bigoplus_{1 \le i \le 6} \langle \lambda_i \rangle$ already, has a multiplication identity 1, and the intersection of each $\langle \lambda_i \rangle$ is equal to $\{0\}$, then $\langle \lambda_i \rangle$ form a partition for $R$. By applying the Chinese Reminder Theorem,

$$R/\big(\bigoplus_{2 \le i \le 6} \langle \lambda_i \rangle \cap \langle \lambda_1 \rangle\big) = R/\{0\} = R \cong R/\big(\bigoplus_{2 \le i \le 6} \langle \lambda_i \rangle \otimes R/\langle \lambda_1 \rangle = \langle \lambda_1 \rangle \otimes R/\langle \lambda_1 \rangle.$$

Since $R' = R/\langle \lambda_1 \rangle = \bigoplus_{2 \le i \le 6} \langle \lambda_i \rangle$, then

$R'/(\bigoplus_{3\le i\le 6}\langle\lambda_i\rangle \cap \langle\lambda_2\rangle) = R'/\{0\} = R' \cong R'/\bigoplus_{3\le i\le 6}\langle\lambda_i\rangle \otimes R'/\langle\lambda_2\rangle = \langle\lambda_1\rangle \otimes \langle\lambda_2\rangle \otimes R'/\langle\lambda_2\rangle$, and so on until $R \cong \langle\lambda_1\rangle \otimes \langle\lambda_2\rangle \otimes \langle\lambda_3\rangle \otimes \langle\lambda_4\rangle \otimes \langle\lambda_5\rangle \otimes \langle\lambda_6\rangle$. ■

**Proposition 3.1.1.** A subset $C$ of $R^n$ is a linear $\omega$-constacyclic code of length $n$ over $R$ if and only if its polynomial representation is an ideal of $R[x]/\langle x^n - \omega\rangle$.

***Proof.*** Suppose that $\pi(C)$ is an ideal of $R[x]/\langle x^n - \omega\rangle$, where $\pi$ be as mentioned in page 15. From the definition of the ideal, we can deduce easily that $C$ is a linear code.

Let $c = (c_0, c_1, \dots, c_{n-1})$ be a codeword of $C$, the polynomial representation of $c$ is $\pi(c) = \sum_{i=0}^{n-1} c_i x^i \in \pi(C)$, but since $\pi(C)$ is an ideal of $R[x]/\langle x^n - \omega\rangle$, we have $x\pi(c) = \omega c_{n-1} + \sum_{i=0}^{n-2} c_i x^{i+1} \in \pi(C)$, then $(\omega c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ which means that $C$ is a linear $\omega$-constacyclic code of length $n$ over $R$.

Conversely, let $C$ be a linear $\omega$-constacyclic code of length $n$ over $R$ and $f = (f_0, f_1, \dots, f_{n-1})$ be a codeword of $C$. It is easy to show that $\pi\big(\gamma_\omega(f)\big) = xf(x)$, where $f(x) = \pi(f)$.

Then $\forall i \ge 0$, we have $x^i f(x) \in \pi(C)$. Since $C$ is a linear code, $\forall a, b \in R, \forall\, i, j \in \mathbb{N}^+$,

$$a\left(x^i f(x)\right) + b\left(x^j f(x)\right) \in \pi(C)$$

which implies that

$$g(x) = \sum_{i=0}^{n-1} g_i x^i \in R[x]/(x^n - \omega), g(x)f(x) = \sum_{i=0}^{n-1} g_i(x^i f(x)) \in \pi(C)$$

Therefore, $\pi(C)$ is an ideal of $R[x]/\langle x^n - \omega\rangle$. ■

**Proposition 3.1.2.** Let $\mu$ be a mapping from $R[x]/\langle x^n - 1\rangle$ to $R[x]/\langle x^n - \omega\rangle$ defined by:

$$\mu\big(f(x)\big) = f(\omega x).$$

If $n = (k+1)(p-1) - 1, k \in \mathbb{N}$, $p$ is an odd prime and $p \nmid n$, where $p$ is the characteristic of $R$, then $\mu$ is a ring isomorphism.

***Proof.*** Now, we need to show that $\mu$ is one-to-one mapping.

For $f(x), g(x) \in R[x]/\langle x^n - 1\rangle$, $f(x) \equiv g(x) mod(x^n - 1)$ if and only if there exists at least one polynomial $\overline{h(x)} \in R[x]/\langle x^n - 1\rangle$ such that $\overline{f(x)} - \overline{g(x)} = \overline{h(x)(x^n - 1)}$ if and only if

$$\overline{f(\omega x)} - \overline{g(\omega x)} = \overline{h(\omega x)((\omega x)^n - 1))}$$

if and only if

$$\overline{f(\omega x)} - \overline{g(\omega x)} = \overline{h(\omega x)(\omega^n x^n - \omega^{p-1})}$$

if and only if

$$\overline{f(\omega x)} - \overline{g(\omega x)} = \overline{h(\omega x)\omega^{p-2}(\omega^{n-p+2}x^n - \omega)}$$

if and only if

$$\overline{f(\omega x)} - \overline{g(\omega x)} = \overline{h(\omega x)\omega^{p-2}}\ \overline{(x^n - \omega)}$$

if and only if

$$\mu\big(f(x)\big) \equiv \mu\big(g(x)\big) mod(x^n - \omega).$$

Therefore, $\mu$ is also one-to-one.

From the definition of $\mu$, it is clear to see that for all $\overline{f(x)} \in R[x]/\langle x^n - \omega\rangle$, there exist $\overline{f(\omega x)} \in R[x]/\langle x^n - 1\rangle$ such that $\overline{\mu\big(f(\omega x)\big)} = \overline{f(\omega^{-1}\omega x)} = \overline{f(x)}$,which implies that $\mu$ is onto too.

Therefore, $\mu$ is a ring isomorphism. ■

**Corollary 3.1.1.** $I$ is an ideal of $R[x]/\langle x^n - 1\rangle$ if and only if $\mu(I)$ is an ideal of $R[x]/\langle x^n - \omega\rangle$, where $n = (k+1)(p-1) - 1, k \in \mathbb{N}$, $p$ is an odd prime and $p \nmid n$, where $p$ is the characteristic of $R$.

***Proof.*** Suppose that $I$ is an ideal of $R[x]/\langle x^n - 1\rangle$. Let $\overline{f(\omega x)}, \overline{g(\omega x)} \in \mu(I)$, where $\overline{f(x)}, \overline{g(x)} \in I$.

$\overline{\mu\big(f(x) + g(x)\big)} \in \mu(I)$, but $\overline{\mu\big(f(x) + g(x)\big)} = \overline{\mu\big((f+g)(x)\big)} = \overline{(f+g)(\omega x)}$

$$= \overline{f(\omega x)} + \overline{g(\omega x)} \in \mu(I).$$

Let $\overline{h(x)} \in R[x]/\langle x^n - \omega\rangle$. $\overline{\mu\big(f(x)h(x)\big)} \in \mu(I)$, but $\overline{\mu\big(f(x)h(x)\big)} = \overline{\mu\big((f \cdot h)(x)\big)}$

$$= \overline{(f \cdot h)(\omega x)} = \overline{f(\omega x)h(\omega x)} \in \mu(I).$$

Which implies that $\mu(I)$ is an ideal of $R[x]/\langle x^n - \omega\rangle$.

Conversely, suppose that $\mu(I)$ is an ideal of $R[x]/\langle x^n-\omega\rangle$. Let $\overline{f(x)}, \overline{g(x)} \in I$, then $\overline{f(\omega x)} + \overline{g(\omega x)} = \overline{(f+g)(\omega x)} = \overline{\mu\big((f+g)(x)\big)} \in \mu(I)$.

Since $\mu$ is a ring isomorphism, there exist $\mu^{-1}$ such that $\overline{\mu^{-1}\left(\mu\big((f+g)(x)\big)\right)} = \overline{(f+g)(x)} = \overline{f(x)} + \overline{g(x)} \in I$.

Let $\overline{h(x)} \in R[x]/\langle x^n-1\rangle$. $\overline{f(\omega x)h(\omega x)} = \overline{(f\cdot h)(\omega x)} = \overline{\mu\big((f\cdot h)(x)\big)} \in \mu(I)$, then $\overline{\mu^{-1}\left(\mu\big((f\cdot h)(x)\big)\right)} = \overline{(f\cdot h)(x)} = \overline{f(x)h(x)} \in I$.

Which implies that $I$ is an ideal of $R[x]/\langle x^n-1\rangle$. ■

**Corollary 3.1.2.** Let $\bar{\mu}$ be the permutation of $R^n$ with $n=(k+1)(p-1)-1, k \in \mathbb{N}$, $p$ is an odd prime and $p \nmid n$, where $p$ is the characteristic of $R$, such that $\bar{\mu}(c_0, c_1, c_2, \dots, c_{n-1}) = (c_0, \omega c_1, \omega^2 c_2, \dots, \omega^{n-1}c_{n-1})$, and $D$ be a subset of $R^n$, then $D$ is a linear cyclic code if and only if $\bar{\mu}(D)$ is a linear $\omega$-constacyclic code.

***Proof.*** The proof is a direct result from Proposition 3.1.2 and Corollary 3.1.1. ■

### 3.2. Gray Map

Every element $r$ of $R$ can be represented as $r = a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f$, where $a, b, c, d, e, f \in \boldsymbol{F}_p$. We define the Gray map as follows:

$$\phi : R \to \boldsymbol{F}_p^6$$

$$r = a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \longmapsto \phi(r) = \varrho$$

where $a, b, c, d, e, f \in \boldsymbol{F}_p$, $\varrho = (a, a+b, a+c, a+d, a+e, a+b+c+f)$.

The Gray map naturally extends to $R^n$ as follows:

$$\phi(r_0, r_1, \dots, r_{n-1}) = \varsigma$$

where $\varsigma = (a_0, a_1, \dots, a_{n-1}, a_0+b_0, a_1+b_1, \dots, a_{n-1}+b_{n-1}, a_0+c_0, a_1+c_1, \dots, a_{n-1}+c_{n-1}, a_0+d_0, a_1+d_1, \dots, a_{n-1}+d_{n-1}, a_0+e_0, a_1+e_1, \dots, a_{n-1}+e_{n-1}, a_0+b_0+c_0+f_0, a_1+b_1+c_1+f_1, \dots, a_{n-1}+b_{n-1}+c_{n-1}+f_{n-1})$.

**Definition 3.2.1.** We define the Lee weight as follows,

$$w_L : R \to \mathbb{N}$$

$$r = a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \longmapsto w_L(r) = \kappa$$

where $a, b, c, d, e, f \in \boldsymbol{F}_p$, $\kappa = w_H(a, a+b, a+c, a+d, a+e, a+b+c+f)$.

The Lee weight of a codeword $a = (a_0, a_1, \dots, a_{n-1}) \in R^n$ is defined by

$$w_L(a) = \sum_{i=0}^{n-1} w_L(a_i)$$

and the Lee distance between $a, b \in R^n$ is defined by

$$d_L : R^n \times R^n \to \mathbb{N}$$

$$d_L(a, b) = w_L(a - b) = \textstyle\sum_{i=0}^{n-1} w_L(a_i - b_i).$$

The minimum Lee distance of $C$ is the smallest nonzero Lee distance between all pairs of distinct codewords. The minimum Lee distance over a linear code $C$ over $R$ is denoted by $d_L(C)$.

***Example 3.2.1.*** Let $c = 3 + 4v_1 + 2(v_2 + v_3) + v_4 + v_1 v_2$, where $c \in R$. Then the Lee weight of $c$ is $w_L(c) = w_H(3, 2, 0, 0, 4, 0) = 3$.

By the definition of the Gray map, we can get the following theorem easily:

**Theorem 3.2.1.** $\phi$ is a linear and distance preserving map from $(R^n, d_L)$ to $(\boldsymbol{F}_p^{6n}, d_H)$.

***Proof.*** It is easy to show that $\phi(x - y) = \phi(x) - \phi(y)$ for $x, y \in R^n$ since it inherits this property from $\boldsymbol{F}_p$

$$d_L(x, y) = w_L(x - y) = w_H\big(\phi(x - y)\big) = w_H\big(\phi(x) - \phi(y)\big) = d_H(\phi(x), \phi(y))$$

which means that $\phi$ is indeed a distance preserving map from $(R^n, d_L)$ to $(\boldsymbol{F}_p^{6n}, d_H)$.

Now, to prove that $\phi$ is a linear map from $(R^n, d_L)$ to $(\boldsymbol{F}_p^{6n}, d_H)$, let $r_i = a_i + v_1 b_i + v_2 c_i + v_3 d_i + v_4 e_i + v_1 v_2 f_i$ for $i = 1, 2$ and $s \in \boldsymbol{F}_p$, then

$$\phi(r_1 + r_2) = \phi\big(a_1 + a_2 + v_1(b_1 + b_2) + v_2(c_1 + c_2) + v_3(d_1 + d_2) +$$
$$v_4(e_1 + e_2) + v_1 v_2(f_1 + f_2)\big) = (a_1 + a_2, a_1 + b_1 + a_2 + b_2, a_1 + c_1 + a_2 +$$

$$c_2, a_1 + d_1 + a_2 + d_2, a_1 + e_1 + a_2 + e_2, a_1 + b_1 + c_1 + f_1 + a_2 + b_2 + c_2 + f_2) = (a_1, a_1 + b_1, a_1 + c_1, a_1 + d_1, a_1 + e_1, a_1 + b_1 + c_1 + f_1) + (a_2, a_2 + b_2, a_2 + c_2, a_2 + d_2, a_2 + e_2, a_2 + b_2 + c_2 + f_2) = \phi(r_1) + \phi(r_2).$$

$$\phi(sr_1) = \phi(sa_1 + v_1 sb_1 + v_2 sc_1 + v_3 sd_1 + v_4 se_1 + v_1 v_2 sf_1) = (sa_1, sa_1 + sb_1, sa_1 + sc_1, sa_1 + sd_1, sa_1 + se_1, sa_1 + sb_1 + sc_1 + sf_1) = s\phi(r_1).$$

Therefore, $\phi$ is linear. As $\phi$ is a bijective, then $|C| = |\phi(C)|$ and since $\phi$ is a distance preserving map, we have $d_L = d_H$.

Hence, $\phi(C)$ is a linear $(6n, M, d_H)$-code over $\boldsymbol{F}_p$. ■

**Proposition 3.2.1.** Let $\phi$ be the Gray map from $R^n$ to $\boldsymbol{F}_p^{6n}$, let $\sigma$ be the cyclic shift operator on $R^n$ and let $\varphi_6$ be the quasi-cyclic shift operator on $\boldsymbol{F}_p^{6n}$. Then $\phi\sigma = \varphi_6\phi$.

***Proof.*** Let $r_i = a_i + v_1 b_i + v_2 c_i + v_3 d_i + v_4 e_i + v_1 v_2 f_i \in R, 0 \le i \le n-1$. Then we have

$$\sigma(r_0, r_1, \dots, r_{n-1}) = (r_{n-1}, r_0, \dots, r_{n-2}).$$

By applying the $\phi$, we have

$$\phi\big(\sigma(r_0, r_1, \dots, r_{n-1})\big) = \phi(r_{n-1}, r_0, \dots, r_{n-2}) = (a_{n-1}, a_0, \dots, a_{n-2}, a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1} + c_{n-1}, a_0 + c_0, \dots, a_{n-2} + c_{n-2}, a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2}, a_{n-1} + e_{n-1}, a_0 + e_0, \dots, a_{n-2} + e_{n-2}, a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}, a_0 + b_0 + c_0 + f_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + f_{n-2}).$$

On the other hand,

$$\varphi_6\big(\phi(r_0, r_1, \dots, r_{n-1})\big) = (a_{n-1}, a_0, \dots, a_{n-2}, a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1} + c_{n-1}, a_0 + c_0, \dots, a_{n-2} + c_{n-2}, a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2}, a_{n-1} + e_{n-1}, a_0 + e_0, \dots, a_{n-2} + e_{n-2}, a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}, a_0 + b_0 + c_0 + f_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + f_{n-2}).$$

Thus $\phi\sigma = \varphi_6\phi$. ■

**Theorem 3.2.2.** Let $\sigma$ and $\varphi_6$ be as defined above. A code $C$ of length $n$ over $R$ is a cyclic code if and only if $\phi(C)$ is a quasi-cyclic code of index 6 and length $6n$ over $\boldsymbol{F}_p$.

***Proof.*** Suppose $C$ is a cyclic code. Then $\sigma(C) = C$. If we apply $\phi$, we have $\phi(\sigma(C)) = \phi(C)$. From Proposition 3.2.1, $\phi(\sigma(C)) = \varphi_6(\phi(C)) = \phi(C)$. So, $\phi(C)$ is a quasi-cyclic code of index 6.

Conversely, if $\phi(C)$ is a quasi-cyclic code of index 6, then $\varphi_6(\phi(C)) = \phi(C)$. Again, from Proposition 3.2.1, $\varphi_6(\phi(C)) = \phi(\sigma(C)) = \phi(C)$. Since $\phi$ is injective, it follows that $\sigma(C) = C$. ■

**Proposition 3.2.2.** Let $\phi$ be the Gray map from $R^n$ to $\boldsymbol{F}_p^{6n}$, $\gamma_\omega$ be the $\omega$-constacyclic shift operator on $R^n$ and $\varphi_{\Omega,6}$ be the Ω-multi-twisted shift operator on $\boldsymbol{F}_p^{6n}$, where $\Omega = (\alpha_0, \alpha_0 + \alpha_1, \alpha_0 + \alpha_2, \alpha_0 + \alpha_3, \alpha_0 + \alpha_4, \alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)$ and $\omega = \alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 + \alpha_5 v_1 v_2$. Then $\phi\gamma_\omega = \varphi_{\Omega,6}\phi$.

***Proof.*** Let $r_i = a_i + v_1 b_i + v_2 c_i + v_3 d_i + v_4 e_i + v_1 v_2 f_i \in R$, where $0 \le i \le n-1$ and $\phi$ be the Gray map that we defined earlier. It is easy to show that

$$\omega v_1 = (\alpha_0 + \alpha_1)v_1 + (\alpha_2 + \alpha_5)v_1 v_2,$$

$$\omega v_2 = (\alpha_0 + \alpha_2)v_2 + (\alpha_1 + \alpha_5)v_1 v_2,$$

$$\omega v_3 = (\alpha_0 + \alpha_3)v_3,$$

$$\omega v_4 = (\alpha_0 + \alpha_4)v_4,$$

$$\omega v_1 v_2 = (\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)v_1 v_2,$$

then $\omega r_{n-1} = \alpha_0 a_{n-1} + v_1(\alpha_1 a_{n-1} + (\alpha_0 + \alpha_1)b_{n-1}) + v_2(\alpha_2 a_{n-1} + (\alpha_0 + \alpha_2)c_{n-1}) + v_3(\alpha_3 a_{n-1} + (\alpha_0 + \alpha_3)d_{n-1}) + v_4(\alpha_4 a_{n-1} + (\alpha_0 + \alpha_4)e_{n-1}) + v_1 v_2(\alpha_5 a_{n-1} + (\alpha_2 + \alpha_5)b_{n-1} + (\alpha_1 + \alpha_5)c_{n-1} + (\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)f_{n-1})$.

We have

$\phi(\gamma_\omega(r_0, r_1, \dots, r_{n-1})) = \phi(\omega r_{n-1}, r_0, \dots, r_{n-2}) = (\alpha_0 a_{n-1}, a_0, \dots, a_{n-2}, (\alpha_0 + \alpha_1)(a_{n-1} + b_{n-1}), a_0 + b_0, \dots, a_{n-2} + b_{n-2}, (\alpha_0 + \alpha_2)(a_{n-1} + c_{n-1}), a_0 + c_0, \dots, a_{n-2} + c_{n-2}, (\alpha_0 + \alpha_3)(a_{n-1} + d_{n-1}), a_0 + d_0, \dots, a_{n-2} + d_{n-2}, (\alpha_0 + \alpha_4)(a_{n-1} + e_{n-1}), a_0 + e_0, \dots, a_{n-2} + e_{n-2}, (\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)(a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}), a_0 + b_0 + c_0 + f_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + f_{n-2})$.

On the other hand

$$\begin{aligned}\phi(r_0,\dots,r_{n-1}) = (&a_0,a_1,\dots,a_{n-1},a_0+b_0,a_1+b_1,\dots,a_{n-1}+b_{n-1},a_0+c_0,a_1\\&+c_1,\dots,a_{n-1}+c_{n-1},a_0+d_0,a_1+d_1,\dots,a_{n-1}+d_{n-1},a_0+e_0,a_1\\&+e_1,\dots,a_{n-1}+e_{n-1},a_0+b_0+c_0+f_0,a_1+b_1+c_1+f_1,\dots,a_{n-1}\\&+b_{n-1}+c_{n-1}+f_{n-1}).\end{aligned}$$

By applying the $\varphi_{\Omega,6}$, we have

$$\begin{aligned}&\varphi_{\Omega,6}\big(\phi(r_0,r_1,\dots,r_{n-1})\big) = \varphi_{\Omega,6}(a_0,a_1,\dots,a_{n-1},a_0+b_0,a_1+b_1,\dots,a_{n-1}+\\&b_{n-1},a_0+c_0,a_1+c_1,\dots,a_{n-1}+c_{n-1},a_0+d_0,a_1+d_1,\dots,a_{n-1}+d_{n-1},a_0+\\&e_0,a_1+e_1,\dots,a_{n-1}+e_{n-1},a_0+b_0+c_0+f_0,a_1+b_1+c_1+f_1,\dots,a_{n-1}+b_{n-1}+\\&c_{n-1}+f_{n-1}) = \big(\gamma_{\alpha_0}(a_0,a_1,\dots,a_{n-1}),\gamma_{\alpha_0+\alpha_1}(a_0+b_0,a_1+b_1,\dots,a_{n-1}+\\&b_{n-1}),\gamma_{\alpha_0+\alpha_2}(a_0+c_0,a_1+c_1,\dots,a_{n-1}+c_{n-1}),\gamma_{\alpha_0+\alpha_3}(a_0+d_0,a_1+\\&d_1,\dots,a_{n-1}+d_{n-1}),\gamma_{\alpha_0+\alpha_4}(a_0+e_0,a_1+e_1,\dots,a_{n-1}+e_{n-1}),\gamma_{\alpha_0+\alpha_1+\alpha_2+\alpha_5}(a_0+\\&b_0+c_0+f_0,a_1+b_1+c_1+f_1,\dots,a_{n-1}+b_{n-1}+c_{n-1}+f_{n-1})\big).\end{aligned}$$

Thus $\phi\gamma_\omega = \varphi_{\Omega,6}\phi$. ■

From Proposition 3.2.2, the following theorem can be easily verified:

**Theorem 3.2.3.** Let $\gamma_\omega$ and $\varphi_{\Omega,6}$ be as defined above. A code $C$ of length $n$ over $R$ is a $\omega$-constacyclic code if and only if $\phi(C)$ is a $\Omega$-multi-twisted code of index 6 and length $6n$ over $\boldsymbol{F}_p$, where $\Omega = (\alpha_0, \alpha_0+\alpha_1, \alpha_0+\alpha_2, \alpha_0+\alpha_3, \alpha_0+\alpha_4, \alpha_0+\alpha_1+\alpha_2+\alpha_5)$ and $\omega = \alpha_0+\alpha_1 v_1+\alpha_2 v_2+\alpha_3 v_3+\alpha_4 v_4+\alpha_5 v_1 v_2$.

***Proof.*** Suppose $C$ is a $\omega$-constacyclic code. Then $\gamma_\omega(C) = C$. If we apply $\phi$, we have $\phi\big(\gamma_\omega(C)\big) = \phi(C)$. From Proposition 3.2.2, $\phi\big(\gamma_\omega(C)\big) = \varphi_{\Omega,6}\big(\phi(C)\big) = \phi(C)$. So, $\phi(C)$ is a $\Omega$-multi-twisted code of index 6.

Conversely, if $\phi(C)$ is a $\Omega$-multi-twisted code of index 6, then $\varphi_{\Omega,6}\big(\phi(C)\big) = \phi(C)$. From Proposition 3.2.2, $\varphi_{\Omega,6}\big(\phi(C)\big) = \phi\big(\gamma_\omega(C)\big) = \phi(C)$. Since $\phi$ is injective, it follows that $\gamma_\omega(C) = C$. ■

### 3.3. $\omega$-constacyclic Code over $R$

We denote that

$$\bigoplus_{1\le i\le 6} A_i = \{a_1 + a_2 + a_3 + a_4 + a_5 + a_6, a_i \in A_i, 1 \le i \le 6\},$$

$$\bigotimes_{1\le i\le 6} A_i = \{(a_1, a_2, a_3, a_4, a_5, a_6), a_i \in A_i, 1 \le i \le 6\}.$$

Let $C$ be a linear code of length $n$ over $R$ and

$$C_1 = \{a \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C, \exists b, c, d, e, f \in \boldsymbol{F}_p^n\},$$

$$C_2 = \{a + b \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C, \exists c, d, e, f \in \boldsymbol{F}_p^n\},$$

$$C_3 = \{a + c \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C, \exists b, d, e, f \in \boldsymbol{F}_p^n\},$$

$$C_4 = \{a + d \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C, \exists b, c, e, f \in \boldsymbol{F}_p^n\},$$

$$C_5 = \{a + e \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C, \exists b, c, d, f \in \boldsymbol{F}_p^n\},$$

$$C_6 = \{a + b + c + f \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C, \exists d, e \in \boldsymbol{F}_p^n\}.$$

Obviously, $C_i$ , $1 \le i \le 6$ are linear codes over $\boldsymbol{F}_p$. Moreover, the linear code $C$ can be written as $C = \bigoplus_{1\le i\le 6} \lambda_i C_i$, where $d_H(C) = \min\{d_H(C_i), 1 \le i \le 6\}$.

**Theorem 3.3.1.** Let $C$ be a linear code of length $n$ over $R$, then $\phi(C) = \bigotimes_{1\le i\le 6} C_i$ and $|C| = \prod_{i=1}^{6} |C_i|$ .

***Proof.*** Let $\begin{pmatrix} a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1}, c_0, c_1, \dots, c_{n-1}, \\ d_0, d_1, \dots, d_{n-1}, e_0, e_1, \dots, e_{n-1}, f_0, f_1, \dots, f_{n-1} \end{pmatrix} \in \phi(C)$.

Let $(r_0, r, \dots, r_{n-1}) \in C$, where $r_i = a_i + v_1(b_i - a_i) + v_2(c_i - a_i) + v_3(d_i - a_i) + v_4(e_i - a_i) + v_1 v_2(a_i - b_i - c_i + f_i) \in R$.

From the definition of $C_i$, we obtain that

$$(a_0, a_1, \dots, a_{n-1}) \in C_1, (b_0, b_1, \dots, b_{n-1}) \in C_2,$$
$$(c_0, c_1, \dots, c_{n-1}) \in C_3, (d_0, d_1, \dots, d_{n-1}) \in C_4,$$
$$(e_0, e_1, \dots, e_{n-1}) \in C_5, (f_0, f_1, \dots, f_{n-1}) \in C_6 .$$

So,

$$\begin{pmatrix} a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1}, c_0, c_1, \dots, c_{n-1}, \\ d_0, d_1, \dots, d_{n-1}, e_0, e_1, \dots, e_{n-1}, f_0, f_1, \dots, f_{n-1} \end{pmatrix} \in \bigotimes_{1\le i\le 6} C_i$$

Hence, $\phi(C) \subseteq \bigotimes_{1\le i\le 6} C_i$ .

On the other hand, for any

$$\begin{pmatrix} a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1}, c_0, c_1, \dots, c_{n-1}, \\ d_0, d_1, \dots, d_{n-1}, e_0, e_1, \dots, e_{n-1}, f_0, f_1, \dots, f_{n-1} \end{pmatrix} \in \bigotimes_{1\le i\le 6} C_i$$

where

$$a = (a_0, a_1, \dots, a_{n-1}) \in C_1, b = (b_0, b_1, \dots, b_{n-1}) \in C_2,$$

$$c = (c_0, c_1, \dots, c_{n-1}) \in C_3, d = (d_0, d_1, \dots, d_{n-1}) \in C_4,$$

$$e = (e_0, e_1, \dots, e_{n-1}) \in C_5, f = (f_0, f_1, \dots, f_{n-1}) \in C_6.$$

From the definition of $C$, we have

$c^{\sim} = a + v_1(b-a) + v_2(c-a) + v_3(d-a) + v_4(e-a) + v_1v_2(a-b-c+f) \in C$. So,

$$\phi(c^{\sim}) = \begin{pmatrix} a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1}, c_0, c_1, \dots, c_{n-1}, \\ d_0, d_1, \dots, d_{n-1}, e_0, e_1, \dots, e_{n-1}, f_0, f_1, \dots, f_{n-1} \end{pmatrix},$$

which gives $\bigotimes_{1\le i\le 6} C_i \subseteq \phi(C)$. Hence, $\phi(C) = \bigotimes_{1\le i\le 6} C_i$.

Since $\phi$ is bijective from $C$ to $\bigotimes_{1\le i\le 6} C_i$, $|C| = \left|\bigotimes_{1\le i\le 6} C_i\right| = \prod_{i=1}^{6} |C_i|$. ■

From Theorem 3.3.1, we get that $|C| = p^{6n-\sum_{i=1}^{6}\deg(g_i(x))}$, where $g_i(x)$ are the generator polynomial of $C_i$.

**Theorem 3.3.2.** Let $C$ be a linear code of length $n$ over $R$, then $\phi(C^{\perp}) = \phi(C)^{\perp}$. Moreover if $C$ is self-dual, so is $\phi(C)$.

***Proof.*** For all $x \in C$ and $y \in C^{\perp}$, let $x_i = a_i + v_1b_i + v_2c_i + v_3d_i + v_4e_i + v_1v_2f_i$ and $y_i = a_i' + v_1b_i' + v_2c_i' + v_3d_i' + v_4e_i' + v_1v_2f_i'$ such that $x = (x_0, x_1, \dots, x_{n-1})$ and $y = (y_0, y_1, \dots, y_{n-1})$. If

$$\begin{aligned} x \cdot y = \sum_{i=0}^{n-1} [&a_ia_i' + v_1(a_ib_i' + b_ia_i' + b_ib_i') + v_2(a_ic_i' + c_ia_i' + c_ic_i') \\ &+ v_3(a_id_i' + d_ia_i' + d_id_i') + v_4(a_ie_i' + b_ie_i' + e_ie_i') + v_1v_2(a_if_i' \\ &+ b_if_i' + b_ic_i' + c_ib_i' + c_if_i' + f_ia_i' + f_ib_i' + f_ic_i' + f_if_i')] = 0. \end{aligned}$$

Then

$$\sum_{i=0}^{n-1} a_i a_i' = \sum_{i=0}^{n-1} (a_i b_i' + b_i a_i' + b_i b_i') = \sum_{i=0}^{n-1} (a_i c_i' + c_i a_i' + c_i c_i')$$
$$= \sum_{i=0}^{n-1} (a_i e_i' + b_i e_i' + e_i e_i') = \sum_{i=0}^{n-1} (a_i d_i' + d_i a_i' + d_i d_i')$$
$$= \sum_{i=0}^{n-1} (a_i f_i' + b_i f_i' + b_i c_i' + c_i b_i' + c_i f_i' + f_i a_i' + f_i b_i' + f_i c_i'$$
$$+ f_i f_i') = 0.$$

Therefore

$$\phi(x) \cdot \phi(y) = 6 \sum_{i=0}^{n-1} a_i a_i'$$
$$+ 2\left(\sum_{i=0}^{n-1} (a_i b_i' + b_i a_i' + b_i b_i') + \sum_{i=0}^{n-1} (a_i c_i' + c_i a_i' + c_i c_i')\right)$$
$$+ \sum_{i=0}^{n-1} (a_i e_i' + b_i e_i' + e_i e_i') + \sum_{i=0}^{n-1} (a_i d_i' + d_i a_i' + d_i d_i')$$
$$+ \sum_{i=0}^{n-1} (a_i f_i' + b_i f_i' + b_i c_i' + c_i b_i' + c_i f_i' + f_i a_i' + f_i b_i' + f_i c_i'$$
$$+ f_i f_i') = 0.$$

Thus $\phi(C^{\perp}) \subseteq \phi(C)^{\perp}$.

By Theorem 3.2.2, we can verify that $|\phi(C^{\perp})| = |\phi(C)^{\perp}|$ which implies that $\phi(C^{\perp}) = \phi(C)^{\perp}$. If $C$ is a self-dual code, so $\phi(C) = \phi(C^{\perp}) = \phi(C)^{\perp}$ which implies that $\phi(C)$ is self-dual. ■

**Theorem 3.3.3.** Let $C$ be a linear code over $R$, then $C^{\perp} = \bigoplus_{1 \le i \le 6} \lambda_i C_i^{\perp}$. Moreover, $C$ is self-dual if and only if $C_i$ is self-dual over $\boldsymbol{F}_p$ where $1 \le i \le 6$.

***Proof.*** Define

$$C_1^{\sim} = \{a \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C^{\perp}, \exists b, c, d, e, f \in \boldsymbol{F}_p^n\},$$

$$C_2^{\sim} = \{a + b \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C^{\perp}, \exists c, d, e, f \in \boldsymbol{F}_p^n\},$$

$$C_3^{\sim} = \{a + c \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C^{\perp}, \exists b, d, e, f \in \boldsymbol{F}_p^n\},$$

$$C_4^{\sim} = \{a + d \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C^{\perp}, \exists b, c, e, f \in \boldsymbol{F}_p^n\},$$

$$C_5^{\sim} = \{a + e \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C^{\perp}, \exists b, c, d, f \in \boldsymbol{F}_p^n\},$$

$$C_6^{\sim} = \{a + b + c + f \in \boldsymbol{F}_p^n | a + v_1 b + v_2 c + v_3 d + v_4 e + v_1 v_2 f \in C^{\perp}, \exists d, e \in \boldsymbol{F}_p^n\}.$$

Then $C^{\perp} = \bigoplus_{1\le i\le 6} \lambda_i C_i^{\sim}$ and this expression is unique. Clearly $C_i^{\sim} \subseteq C_i^{\perp}$. Let $r \in C_1^{\perp}$ and $s = a\lambda_1 + b\lambda_2 + c\lambda_3 + d\lambda_4 + e\lambda_5 + f\lambda_6 \in C$ where $a, b, c, d, e, f \in \boldsymbol{F}_p^n$, then $\lambda_1 r \cdot s = \lambda_1 \cdot a = 0$, so $\lambda_1 r \in C^{\perp}$, by the unique expression of $C^{\perp}$, $r \in C_1^{\sim}$, which implies $C_1^{\perp} \subseteq C_1^{\sim}$ and $C_1^{\perp} = C_1^{\sim}$.

Similarly, we can prove that $C_i^{\perp} = C_i^{\sim}$, for $2 \le i \le 6$. Therefore $C^{\perp} = \bigoplus_{1\le i\le 6} \lambda_i C_i^{\perp}$.

If $C$ is self-dual, then $\phi(C) = \phi(C^{\perp})$, by Theorem 3.3.1, $\phi(C) = \bigotimes_{1\le i\le 6} C_i^{\perp} = \phi(C^{\perp}) = \bigotimes_{1\le i\le 6} C_i^{\perp}$, which implies $C_i = C_i^{\perp}$ for $1 \le i \le 6$. Clearly, if $C_i$ is self-dual over $F_p$ for $1 \le i \le 6$, so is $C$. ■

**Theorem 3.3.4.** Let $C = \bigoplus_{1\le i\le 6} \lambda_i C_i$ be a linear code over $R$. $C$ is a $\omega$-constacyclic code over $R$ if and only if $C_i, 1 \le i \le 6$ are $\alpha_0$-constacyclic code, $\alpha_0 + \alpha_1$-constacyclic code, $\alpha_0 + \alpha_2$-constacyclic code, $\alpha_0 + \alpha_3$-constacyclic code, $\alpha_0 + \alpha_4$-constacyclic code, $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5$-constacyclic code over $\boldsymbol{F}_p$, respectively, where $\omega = \alpha_0 + \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 + \alpha_5 v_1 v_2$ is a unit over $R$.

***Proof.*** For any $r = (r_0, r_1, \dots, r_{n-1}) \in C$, we write its components in this form $r_i = a_i\lambda_1 + b_i\lambda_2 + c_i\lambda_3 + d_i\lambda_4 + e_i\lambda_5 + f_i\lambda_6$, where $a_i, b_i, c_i, d_i, e_i, f_i \in \boldsymbol{F}_p$ and $0 \le i \le n-1$.

Let $a = (a_0, a_1, \dots, a_{n-1}), b = (b_0, b_1, \dots, b_{n-1}), c = (c_0, c_1, \dots, c_{n-1})$, $d = (d_0, d_1, \dots, d_{n-1}), e = (e_0, e_1, \dots, e_{n-1}), f = (f_0, f_1, \dots, f_{n-1})$, then $a \in C_1, b \in C_2, c \in C_3, d \in C_4, e \in C_5, f \in C_6$ .

If $C_i, 1 \le i \le 6$ are $\alpha_0$-constacyclic code, $\alpha_0 + \alpha_1$-constacyclic code, $\alpha_0 + \alpha_2$-constacyclic code, $\alpha_0 + \alpha_3$-constacyclic code, $\alpha_0 + \alpha_4$-constacyclic code, $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5$-constacyclic code over $\boldsymbol{F}_p$, respectively, then $\gamma_{\alpha_0}(a) \in C_1, \gamma_{\alpha_0+\alpha_1}(b) \in C_2, \gamma_{\alpha_0+\alpha_2}(c) \in C_3, \gamma_{\alpha_0+\alpha_3}(d) \in C_4, \gamma_{\alpha_0+\alpha_4}(e) \in C_5$ , $\gamma_{\alpha_0+\alpha_1+\alpha_2+\alpha_5}(f) \in C_6$. Then we have

$$\gamma_\omega(r) = (\omega(a_{n-1}\,\lambda_1 + b_{n-1}\,\lambda_2 + c_{n-1}\,\lambda_3 + d_{n-1}\,\lambda_4 + e_{n-1}\,\lambda_5 + f_{n-1}\,\lambda_6), a_0\,\lambda_1 + b_0\,\lambda_2 + c_0\,\lambda_3 + d_0\,\lambda_4 + e_0\,\lambda_5 + f_0\,\lambda_6, \dots, a_{n-2}\,\lambda_1 + b_{n-2}\,\lambda_2 + c_{n-2}\,\lambda_3 + d_{n-2}\,\lambda_4 + e_{n-2}\,\lambda_5 + f_{n-2}\,\lambda_6)$$

$$= (\alpha_0 a_{n-1}\lambda_1 + (\alpha_0+\alpha_1)b_{n-1}\lambda_2 + (\alpha_0+\alpha_2)c_{n-1}\lambda_3 + (\alpha_0+\alpha_3)d_{n-1}\lambda_4 + (\alpha_0+\alpha_4)e_{n-1}\lambda_5 + (\alpha_0+\alpha_1+\alpha_2+\alpha_5)f_{n-1}\lambda_6, a_0\lambda_1 + b_0\lambda_2 + c_0\lambda_3 + d_0\lambda_4 + e_0\lambda_5 + f_0\lambda_6, \dots, a_{n-2}\lambda_1 + b_{n-2}\lambda_2 + c_{n-2}\lambda_3 + d_{n-2}\lambda_4 + e_{n-2}\lambda_5 + f_{n-2}\lambda_6)$$

$$= (\alpha_0 a_{n-1}, a_0, \dots, a_{n-2})\lambda_1 + \big((\alpha_0+\alpha_1)b_{n-1}, b_0, \dots, b_{n-2}\big)\lambda_2 + \big((\alpha_0+\alpha_2)c_{n-1}, c_0, \dots, c_{n-2}\big)\lambda_3 + \big((\alpha_0+\alpha_3)d_{n-1}, d_0, \dots, d_{n-2}\big)\lambda_4 + \big((\alpha_0+\alpha_4)e_{n-1}, e_0, \dots, e_{n-2}\big)\lambda_5 + \big((\alpha_0+\alpha_1+\alpha_2+\alpha_5)f_{n-1}, f_0, \dots, f_{n-2}\big)\lambda_6$$

$= \gamma_{\alpha_0}(a)\lambda_1 + \gamma_{\alpha_0+\alpha_1}(b)\lambda_2 + \gamma_{\alpha_0+\alpha_2}(c)\lambda_3 + \gamma_{\alpha_0+\alpha_3}(d)\lambda_4 + \gamma_{\alpha_0+\alpha_4}(e)\lambda_5 + \gamma_{\alpha_0+\alpha_1+\alpha_2+\alpha_5}(f)\lambda_6 \in C.$

This proves that $C$ is a $\omega$-constacyclic code over $R$.

Conversely, for all $a = (a_0, a_1, \dots, a_{n-1}) \in C_1, b = (b_0, b_1, \dots, b_{n-1}) \in C_2, c = (c_0, c_1, \dots, c_{n-1}) \in C_3, d = (d_0, d_1, \dots, d_{n-1}) \in C_4, e = (e_0, e_1, \dots, e_{n-1}) \in C_5, f = (f_0, f_1, \dots, f_{n-1}) \in C_6$, let $r_i = a_i\lambda_1 + b_i\lambda_2 + c_i\lambda_3 + d_i\lambda_4 + e_i\lambda_5 + f_i\lambda_6, 0 \le i \le n-1$, then $r = (r_0, r_1, \dots, r_{n-1}) \in C$. If $C$ is a $\omega$-constacyclic code over $R$, then $\gamma_\omega(r) = \gamma_{\alpha_0}(a)\lambda_1 + \gamma_{\alpha_0+\alpha_1}(b)\lambda_2 + \gamma_{\alpha_0+\alpha_2}(c)\lambda_3 + \gamma_{\alpha_0+\alpha_3}(d)\lambda_4 + \gamma_{\alpha_0+\alpha_4}(e)\lambda_5 + \gamma_{\alpha_0+\alpha_1+\alpha_2+\alpha_5}(f)\lambda_6 \in C$.

Thus $\gamma_{\alpha_0}(a) \in C_1, \gamma_{\alpha_0+\alpha_1}(b) \in C_2, \gamma_{\alpha_0+\alpha_2}(c) \in C_3, \gamma_{\alpha_0+\alpha_3}(d) \in C_4, \gamma_{\alpha_0+\alpha_4}(e) \in C_5, \gamma_{\alpha_0+\alpha_1+\alpha_2+\alpha_5}(f) \in C_6$. Therefore, $C_i, 1 \le i \le 6$ are $\alpha_0$-constacyclic code, $\alpha_0+\alpha_1$-constacyclic code, $\alpha_0+\alpha_2$-constacyclic code, $\alpha_0+\alpha_3$-constacyclic code, $\alpha_0+\alpha_4$-constacyclic code, $\alpha_0+\alpha_1+\alpha_2+\alpha_5$-constacyclic code over $\boldsymbol{F}_p$, respectively. ■

**Theorem 3.3.5.** If $C = \bigoplus_{1\le i\le 6} \lambda_i C_i$ is a $\omega$-constacyclic code of length $n$ over $R$, then there exists a polynomial $g(x) = \sum_{i=1}^{6} \lambda_i\, g_i(x)$ in $R[x]$ that divides $x^n - \omega$ that generates the code, where $g_i(x)$ is the generator polynomial of $C_i$ in $\boldsymbol{F}_p[x]$ for each $1 \le i \le 6$.

***Proof.*** Let $C = \bigoplus_{1\le i\le 6} \lambda_i C_i$ is a $\omega$-constacyclic code of length $n$ over $R$. Let $g_i(x)$ be the generator polynomial of $C_i$, $1 \le i \le 6$. It follows that $C$ has the form

$$C = \langle \lambda_1\, g_1(x\,), \lambda_2\, g_2(x\,), \lambda_3\, g_3(x\,), \lambda_4\, g_4(x\,), \lambda_5\, g_5(x\,), \lambda_6\, g_6(x\,)\rangle.$$

Let $C' = \langle \sum_{i=1}^{6} \lambda_i\, g_i(x)\rangle$. We can have that $C' \subseteq C$. Note that

$$\lambda_j \left(\sum_{i=1}^{6} \lambda_i\, g_i(x)\right) = \lambda_j\, g_j(x\,), 1 \le j \le 6.$$

we can get that $C \subseteq C'$. So $C' = C$ and $C$ is generated by a single element. It is known that the generator $g_1(x\,)$ divides $x^n - \alpha_0, g_2(x\,)$ divides $x^n - (\alpha_0 + \alpha_1)$, $g_3(x\,)$ divides $x^n - (\alpha_0 + \alpha_2)$, $g_4(x\,)$ divides $x^n - (\alpha_0 + \alpha_3)$, $g_5(x\,)$ divides $x^n - (\alpha_0 + \alpha_4)$ and $g_6(x\,)$ divides $x^n - (\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)$ since $C_i, 1 \le i \le 6$ are $\alpha_0$-constacyclic code, $\alpha_0 + \alpha_1$-constacyclic code, $\alpha_0 + \alpha_2$-constacyclic code, $\alpha_0 + \alpha_3$-constacyclic code, $\alpha_0 + \alpha_4$-constacyclic code, $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5$-constacyclic code over $\boldsymbol{F}_p$, respectively. Let $f_i(x)$ be the polynomial such that $g_1(x)f_1(x) = x^n - \alpha_0$, $g_2(x)f_2(x) = x^n - (\alpha_0 + \alpha_1)$, $g_3(x)f_3(x) = x^n - (\alpha_0 + \alpha_2)$, $g_4(x)f_4(x) = x^n - (\alpha_0 + \alpha_3)$, $g_5(x)f_5(x) = x^n - (\alpha_0 + \alpha_4)$, $g_6(x)f_6(x) = x^n - (\alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)$. Then we have $x^n - \omega = [\sum_{i=1}^{6} \lambda_i\, g_i(x)][\sum_{i=1}^{6} \lambda_i\, f_i(x)]$. So, we have that $x^n - \omega = g(x)[\sum_{i=1}^{6} \lambda_i\, f_i(x)]$. ■

**Theorem 3.3.6.** Let $C = \bigoplus_{1\le i\le 6} \lambda_i C_i$ be a $\omega$-constacyclic code of length $n$ over $R$ and $C = \langle \sum_{i=1}^{6} \lambda_i\, g_i(x)\rangle$, where $g_i(x)$ is the generator polynomial of $C_i$, for $1 \le i \le 6$. Then

$$\phi(C) = \langle \prod_{i=1}^{6} g_i(x)\rangle.$$

***Proof.*** We showed earlier that $\phi(C) = \bigotimes_{1\le i\le 6} C_i$, let $c(x) \in \bigotimes_{1\le i\le 6} C_i$ such that $c(x) = \prod_{i=1}^{6} f_i(x)$ for any $f_i(x) \in C_i$, since $f_i(x)$ can be generated by $g_i(x)$, then there exist $r_i(x)$ such that $f_i(x) = r_i(x)g_i(x)$, then

$$c(x) = \prod_{i=1}^{6} r_i(x)g_i(x) = \prod_{i=1}^{6} r_i(x) \cdot \prod_{i=1}^{6} g_i(x)$$

which means $c(x) \in \langle \prod_{i=1}^{6} g_i(x)\rangle$ which implying that $C \subseteq \langle \prod_{i=1}^{6} g_i(x)\rangle$. It is easy to show that,

$$|\phi(C)| = |C| = p^{6n-\sum_{i=1}^{6}\deg(g_i)} = |\langle\prod_{i=1}^{6} g_i(x)\rangle|.$$

Therefore $\phi(C) = \langle\prod_{i=1}^{6} g_i(x)\rangle$. ■

### 3.4. Special Case: $\beta$-constacyclic Codes over $R$

Here we give an example of this class of constacyclic codes where $\alpha_i = 1$ for $0 \le i \le 5$. One condition is necessary here $1 + v_1 + v_2 + v_3 + v_4 + v_1v_2$ is a unit in $R$ if $p$ is an odd prime only. In this section, we shall denote $1 + v_1 + v_2 + v_3 + v_4 + v_1v_2$ by $\beta$.

**Proposition 3.4.1.** $\beta$ is a unit in $R$ if $p$ is an odd prime.

***Proof.*** In order to prove that $\beta$ is a unit, we need to find $\beta^{-1} \in R$ such that $\beta\beta^{-1} = 1$. Let $\beta^{-1} = \beta_0^{-1} + \beta_1^{-1}v_1 + \beta_2^{-1}v_2 + \beta_3^{-1}v_3 + \beta_4^{-1}v_4 + \beta_5^{-1}v_1v_2$.

When $p = 2$:

$\beta\beta^{-1} = \beta_0^{-1} + (\beta_0^{-1} + 2\beta_1^{-1})v_1 + (\beta_0^{-1} + 2\beta_2^{-1})v_2 + (\beta_0^{-1} + 2\beta_3^{-1})v_3 + (\beta_0^{-1} + 2\beta_4^{-1})v_4 + (\beta_0^{-1} + 2\beta_1^{-1} + 2\beta_2^{-1} + 4\beta_5^{-1})v_1v_2 = \beta_0^{-1} + \beta_0^{-1}v_1 + \beta_0^{-1}v_2 + \beta_0^{-1}v_3 + \beta_0^{-1}v_4 + \beta_0^{-1}v_1v_2$ and this implies that $\beta$ is not a unit in $R$ when $p = 2$.

For $p$ is an odd prime: $\beta\beta^{-1} = \beta_0^{-1} + (\beta_0^{-1} + 2\beta_1^{-1})v_1 + (\beta_0^{-1} + 2\beta_2^{-1})v_2 + (\beta_0^{-1} + 2\beta_3^{-1})v_3 + (\beta_0^{-1} + 2\beta_4^{-1})v_4 + (\beta_0^{-1} + 2\beta_1^{-1} + 2\beta_2^{-1} + 4\beta_5^{-1})v_1v_2$. So, in order to prove that $\beta\beta^{-1} = 1$, all equations below must have solutions in $\boldsymbol{F}_p$ :

$\beta_0^{-1} = 1$, $\beta_0^{-1} + 2\beta_1^{-1} = 0$, $\beta_0^{-1} + 2\beta_2^{-1} = 0$, $\beta_0^{-1} + 2\beta_3^{-1} = 0$, $\beta_0^{-1} + 2\beta_4^{-1} = 0$, $\beta_0^{-1} + 2\beta_1^{-1} + 2\beta_2^{-1} + 4\beta_5^{-1} = 0$ and the solutions are: $\beta_0^{-1} = 1$, $\beta_1^{-1} = \beta_2^{-1} = \beta_3^{-1} = \beta_4^{-1} = (p-1)(2^{-1})$, $\beta_5^{-1} = 4^{-1}$. Therefore, $\beta$ is a unit in $R$ if $p$ is an odd prime. ■

**Proposition 3.4.2.** Let $\phi$ be the Gray map from $R^n$ to $\boldsymbol{F}_p^{6n}$, $\gamma_\beta$ be the $\beta$-constacyclic shift operator on $R^n$ and $\varphi_{\Omega,6}$ be the Ω-multi-twisted shift operator on $\boldsymbol{F}_p^{6n}$, where $\Omega = (1,2,2,2,2,4)$, then $\phi\gamma_\beta = \varphi_{\Omega,6}\phi$.

***Proof.*** Let $r_i = a_i + v_1b_i + v_2c_i + v_3d_i + v_4e_i + v_1v_2f_i \in R$ for $0 \le i \le n-1$ and $\phi$ be the Gray map that we defined earlier. It is easy to show that

$$\beta v_1 = 2v_1 + 2v_1v_2, \beta v_2 = 2v_2 + 2v_1v_2, \beta v_3 = 2v_3, \beta v_4 = 2v_4, \beta v_1v_2 = 4v_1v_2,$$

$$\beta r_{n-1} = a_{n-1} + v_1(a_{n-1} + 2b_{n-1}) + v_2(a_{n-1} + 2c_{n-1}) + v_3(a_{n-1} + 2d_{n-1}) + v_4(a_{n-1} + 2e_{n-1}) + v_1v_2(a_{n-1} + 2b_{n-1} + 2c_{n-1} + 4f_{n-1}).$$

We have

$$\phi\left(\gamma_\beta(r_0, \dots, r_{n-1})\right) = \phi(\beta r_{n-1}, r_0, \dots, r_{n-2}) = (a_{n-1}, a_0, \dots, a_{n-2}, 2(a_{n-1} + b_{n-1}), a_0 + b_0, \dots, a_{n-2} + b_{n-2}, 2(a_{n-1} + c_{n-1}), a_0 + c_0, \dots, a_{n-2} + c_{n-2}, 2(a_{n-1} + d_{n-1}), a_0 + d_0, \dots, a_{n-2} + d_{n-2}, 2(a_{n-1} + e_{n-1}), a_0 + e_0, \dots, a_{n-2} + e_{n-2}, 4(a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}), a_0 + b_0 + c_0 + f_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + f_{n-2}).$$

On the other hand,

$$\phi(r_0, \dots, r_{n-1}) = (a_0, a_1, \dots, a_{n-1}, a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}, a_0 + c_0, a_1 + c_1, \dots, a_{n-1} + c_{n-1}, a_0 + d_0, a_1 + d_1, \dots, a_{n-1} + d_{n-1}, a_0 + e_0, a_1 + e_1, \dots, a_{n-1} + e_{n-1}, a_0 + b_0 + c_0 + f_0, a_1 + b_1 + c_1 + f_1, \dots, a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}).$$

By applying $\varphi_{\Omega,6}$, we have

$$\varphi_{\Omega,6}\big(\phi(r_0, \dots, r_{n-1})\big) = \varphi_{\Omega,6}(a_0, a_1, \dots, a_{n-1}, a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}, a_0 + c_0, a_1 + c_1, \dots, a_{n-1} + c_{n-1}, a_0 + d_0, a_1 + d_1, \dots, a_{n-1} + d_{n-1}, a_0 + e_0, a_1 + e_1, \dots, a_{n-1} + e_{n-1}, a_0 + b_0 + c_0 + f_0, a_1 + b_1 + c_1 + f_1, \dots, a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}). = (a_{n-1}, a_0, \dots, a_{n-2}, 2(a_{n-1} + b_{n-1}), a_0 + b_0, \dots, a_{n-2} + b_{n-2}, 2(a_{n-1} + c_{n-1}), a_0 + c_0, \dots, a_{n-2} + c_{n-2}, 2(a_{n-1} + d_{n-1}), a_0 + d_0, \dots, a_{n-2} + d_{n-2}, 2(a_{n-1} + e_{n-1}), a_0 + e_0, \dots, a_{n-2} + e_{n-2}, 4(a_{n-1} + b_{n-1} + c_{n-1} + f_{n-1}), a_0 + b_0 + c_0 + f_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + f_{n-2}).$$

Thus $\phi\gamma_\beta = \varphi_{\Omega,6}\phi$. ■

From Proposition 3.4.2 the following theorem can be easily verified:

**Theorem 3.4.1.** Let $\gamma_\beta$ and $\varphi_{\Omega,6}$ be as defined above. A code $C$ of length $n$ over $R$ is a $\beta$-constacyclic code if and only if $\phi(C)$ is a Ω-multi-twisted code of index 6 and length $6n$ over $\boldsymbol{F}_p$, where $\Omega = (1,2,2,2,2,4)$.

**Theorem 3.4.2.** Let $C = \bigoplus_{1 \le i \le 6} \lambda_i C_i$ be a linear code over $R$, $C$ is a $\beta$-constacyclic code over $R$ if and only if $C_i$ are cyclic code, 2-constacyclic code, 2-constacyclic code, 2-constacyclic code, 2-constacyclic code, 4-constacyclic code over $\boldsymbol{F}_p$, respectively, for $1 \le i \le 6$, where $\beta$ is a unit over $R$.

***Proof.*** For any $r = (r_0, r_1, \dots, r_{n-1}) \in C$, we can write its components as $r_i = a_i\lambda_1 + b_i\lambda_2 + c_i\lambda_3 + d_i\lambda_4 + e_i\lambda_5 + f_i\lambda_6$, where $a_i, b_i, c_i, d_i, e_i, f_i \in \boldsymbol{F}_p$, $0 \leq i \leq n-1$.

Let $a = (a_0, a_1, \dots, a_{n-1}), b = (b_0, b_1, \dots, b_{n-1}), c = (c_0, c_1, \dots, c_{n-1})$, $d = (d_0, d_1, \dots, d_{n-1}), e = (e_0, e_1, \dots, e_{n-1}), f = (f_0, f_1, \dots, f_{n-1})$, where $a \in C_1, b \in C_2, c \in C_3, d \in C_4, e \in C_5, f \in C_6$.

If $C_i$ are cyclic code, 2-constacyclic code, 2-constacyclic code, 2-constacyclic code, 2-constacyclic code, 4-constacyclic code over $\boldsymbol{F}_p$, respectively, for $1 \leq i \leq 6$, then $\gamma_1(a) \in C_1, \gamma_2(b) \in C_2, \gamma_2(c) \in C_3, \gamma_2(d) \in C_4, \gamma_2(e) \in C_5, \gamma_4(f) \in C_6$. Then we have

$$\begin{aligned}
\gamma_\beta(r) = (&\beta(a_{n-1}\lambda_1 + b_{n-1}\lambda_2 + c_{n-1}\lambda_3 + d_{n-1}\lambda_4 + e_{n-1}\lambda_5 + f_{n-1}\lambda_6), a_0\lambda_1 \\
&+ b_0\lambda_2 + c_0\lambda_3 + d_0\lambda_4 + e_0\lambda_5 + f_0\lambda_6, \dots, a_{n-2}\lambda_1 + b_{n-2}\lambda_2 + c_{n-2}\lambda_3 \\
&+ d_{n-2}\lambda_4 + e_{n-2}\lambda_5 + f_{n-2}\lambda_6) \\
= (&a_{n-1}\lambda_1 + 2b_{n-1}\lambda_2 + 2c_{n-1}\lambda_3 + 2d_{n-1}\lambda_4 + 2e_{n-1}\lambda_5 + 4f_{n-1}\lambda_6, a_0\lambda_1 + b_0\lambda_2 \\
&+ c_0\lambda_3 + d_0\lambda_4 + e_0\lambda_5 + f_0\lambda_6, \dots, a_{n-2}\lambda_1 + b_{n-2}\lambda_2 + c_{n-2}\lambda_3 \\
&+ d_{n-2}\lambda_4 + e_{n-2}\lambda_5 + f_{n-2}\lambda_6) \\
= (&a_{n-1}, a_0, \dots, a_{n-2})\lambda_1 + (2b_{n-1}, b_0, \dots, b_{n-2})\lambda_2 + (2c_{n-1}, c_0, \dots, c_{n-2})\lambda_3 \\
&+ (2d_{n-1}, d_0, \dots, d_{n-2})\lambda_4 + (2e_{n-1}, e_0, \dots, e_{n-2})\lambda_5 \\
&+ (4f_{n-1}, f_0, \dots, f_{n-2})\lambda_6 \\
= &\gamma_1(a)\lambda_1 + \gamma_2(b)\lambda_2 + \gamma_2(c)\lambda_3 + \gamma_2(d)\lambda_4 + \gamma_2(e)\lambda_5 + \gamma_4(f)\lambda_6 \in C.
\end{aligned}$$

This proves that $C$ is a $\beta$-constacyclic code over $R$.

Conversely, for all $a = (a_0, a_1, \dots, a_{n-1}) \in C_1, b = (b_0, b_1, \dots, b_{n-1}) \in C_2, c = (c_0, c_1, \dots, c_{n-1}) \in C_3, d = (d_0, d_1, \dots, d_{n-1}) \in C_4, e = (e_0, e_1, \dots, e_{n-1}) \in C_5, f = (f_0, f_1, \dots, f_{n-1}) \in C_6$, let $r_i = a_i\lambda_1 + b_i\lambda_2 + c_i\lambda_3 + d_i\lambda_4 + e_i\lambda_5 + f_i\lambda_6, 0 \leq i \leq n-1$, then $r = (r_0, r_1, \dots, r_{n-1}) \in C$. If $C$ is a $\beta$-constacyclic code over $R$, then $\gamma_\beta(r) = \gamma_1(a)\lambda_1 + \gamma_2(b)\lambda_2 + \gamma_2(c)\lambda_3 + \gamma_2(d)\lambda_4 + \gamma_2(e)\lambda_5 + \gamma_4(f)\lambda_6 \in C$. Thus $\gamma_1(a) \in C_1, \gamma_2(b) \in C_2, \gamma_2(c) \in C_3, \gamma_2(d) \in C_4, \gamma_2(e) \in C_5, \gamma_4(f) \in C_6$. So $C_i, 1 \leq i \leq 6$ are cyclic code, 2-constacyclic code, 2-constacyclic code, 2-constacyclic code, 2-constacyclic code, 4-constacyclic code over $\boldsymbol{F}_p$, respectively. ■

***Example 3.4.1.*** Let $n = 15$ and $R = \boldsymbol{F}_3 + v_1\boldsymbol{F}_3 + v_2\boldsymbol{F}_3 + v_3\boldsymbol{F}_3 + v_4\boldsymbol{F}_3 + v_1v_2\boldsymbol{F}_3$. We have $g_1(x) = g_6(x) = x^{12} + x^9 + x^6 + x^3 + 1$ as a factor of $x^{15} -$

1 and $g_2(x) = g_3(x) = g_4(x) = g_5(x) = x^6 + x^5 + x + 1$ as a factor of $x^{15} + 1$. Then, $C$ will be a $\beta$-constacyclic code of length 15 generated by $g(x) = \sum_{i=1}^{6} \lambda_i g_i(x)$ and $\phi(C)$ is a [90,42,4] Ω-multi-twisted code of index 6 and length 90 over $\boldsymbol{F}_3$, where

$$\Omega = (1, -1, -1, -1, -1, 1)$$

and

$$\beta = 1 + v_1 + v_2 + v_3 + v_4 + v_1 v_2.$$

Here, we managed to find the distance of the code above by using the properties in Theorem 2.3.3 and Corollary 2.3.4 and rewrote it in algorithmic form as below:

Input: generator polynomial $g(x)$

**Start**: $i = 2$

Step 1: find the parity-check matrix $H$

Step 2: select all $i$ combinations of columns of $H$ as $H_i$

Step 3: check every $i$ columns of $H_i$ for linearly-dependency

Step 4: if true, then $d = i$ and **End**;

else $i = i + 1$ and repeat Step2-4 until $i =$# of $H$'s columns $-1$

Output: $d$

By implementing the above algorithm using MATLAB, we calculated the following results:

Table 3.1. Generator polynomial of $C_i$ over $\boldsymbol{F}_3$ of length 15

| $g_i(x)$ | $x^n - \alpha$ | $[n, k, d]$ |
|---|---|---|
| $x^8 + 2x^7 + x^5 + 2x^4 + x^3 + 2x + 1$ | $x^{15} - 1$ | [15,7,3] |
| $x^{12} + x^9 + x^6 + x^3 + 1$ | $x^{15} - 1$ | [15,3,5] |
| $x^9 + x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2$ | $x^{15} - 1$ | [15,6,3] |
| $x^{10} + x^5 + 1$ | $x^{15} - 1$ | [15,5,3] |
| $x^6 + x^5 + x + 1$ | $x^{15} + 1$ | [15,9,4] |
| $x^7 + 2x^6 + x^5 + x^2 + 2x + 1$ | $x^{15} + 1$ | [15,8,4] |

Table 3.2. Generator polynomial of $C_i$ over $\boldsymbol{F}_5$ of length 12

| $g_i(x)$ | $x^n - \alpha$ | $[n, k, d]$ |
|---|---|---|
| $x^4 + 2x^3 + 4x^2 + 2$ | $x^{12} - 1$ | [12,8,4] |
| $x^4 + 2x^2 + 4x + 3$ | $x^{12} - 1$ | [12,8,4] |
| $x^5 + 3x^3 + x + 2$ | $x^{12} - 1$ | [12,7,4] |
| $x^7 + 2x^6 + 2x^5 + x^4 + 3x^3 + 4x^2 + 3x + 3$ | $x^{12} - 1$ | [12,5,4] |
| $x^4 + x^2 + 2$ | $x^{12} - 2$ | [12,8,3] |
| $x^4 + 4x^2 + 2$ | $x^{12} - 2$ | [12,8,3] |
| $x^4 + 3x^3 + 2x^2 + 2x + 1$ | $x^{12} - 4$ | [12,8,4] |
| $x^4 + 4x^3 + 3x^2 + 4x + 1$ | $x^{12} - 4$ | [12,8,4] |
| $x^4 + 2x^3 + 2x^2 + 3x + 1$ | $x^{12} - 4$ | [12,8,4] |
| $x^4 + x^3 + 3x^2 + x + 1$ | $x^{12} - 4$ | [12,8,4] |

By using the results in Table 1 and Table 2 above, we can find the parameters of the $\beta$-constacyclic code $C$ generated by $g(x) = \sum_{i=1}^{6} \lambda_i g_i(x)$ easily.

As a general rule, $\phi(C)$ is a $[6n, 6n - \sum_{i=1}^{6} \deg(g_i)\ , min\ \{d_H(C_i)\}]$-Ω-multi-twisted code of index 6 and length $6n$ over $\boldsymbol{F}_p$, where $\Omega = (1,2,2,2,2,4)$.

***Example 3.4.2.*** Let $C$ be a $\beta$-constacyclic code of length 12 over $R = \boldsymbol{F}_5 + v_1\boldsymbol{F}_5 + v_2\boldsymbol{F}_5 + v_3\boldsymbol{F}_5 + v_4\boldsymbol{F}_5 + v_1v_2\boldsymbol{F}_5$ generated by $g(x) = \sum_{i=1}^{6} \lambda_i g_i(x)$, we choose $g_1(x)$ as a factor of $x^{12} - 1$, $g_{i=2,3,4,5}(x)$ as a factor of $x^{12} - 2$ and $g_6(x)$ as a factor of $x^{12} - 4$ from the table above

$$g_1(x) = x^4 + 2x^3 + 4x^2 + 2$$

$$g_2(x) = g_3(x) = g_4(x) = g_5(x) = x^4 + x^2 + 2$$

$$g_6(x) = x^4 + x^3 + 3x^2 + x + 1$$

Then $\phi(C)$ is a [72,48,3]-Ω-multi-twisted code of index 6 and length 72 over $\boldsymbol{F}_5$, where $\Omega = (1,2,2,2,2,4)$.

### 3.5. Decoding of $\beta$-constacyclic Codes over $R$

Let $d_i$ be the Hamming distance of $C_i$ where $1 \leq i \leq 6$, since the Gray map is literally the concatenation of $C_i$, then we need to rethink about the Hamming distance of $\phi(C)$. For an instance, let $r_i \in C_i\ , 1 \leq i \leq 6$ , then $\exists\, r \in \phi(C)$ such that $r = (r_1|r_2|\ldots|r_6)$, we see that $r_i$'s segment differ from any matching codeword's segment in $r_i' \in C_i$ by at least $d_i$ where $r' = (r_1'|r_2'|\ldots|r_6') \in \phi(C)$, then instead of using $\phi(C)$'s syndromes in decoding, it is more efficient to apply the decoding process using $C_i$'s syndromes on the corresponding codeword's segment.

#### Example on $\boldsymbol{F_3 + v_1F_3 + v_2F_3 + v_3F_3 + v_4F_3 + v_1v_2F_3}$

Let us use the generating polynomial $g(x) = \sum_{i=1}^{6} \lambda_i g_i(x)$ as explained in the Example 3.4.1, we will generate the codeword $w$ as

$$w = (x + x^8 + x^{13})g(x) = (v_1 + v_2 + v_3 + v_4 + v_1v_2 + 1)x^{14} + 2x^{13} + (2v_1 + 2v_2 + 2v_3 + 2v_4 + 2v_1v_2 + 1)x^{11} + (v_1 + v_2 + v_3 + v_4 + v_1v_2 + 2)x^{10} + (v_1 + v_2 + v_3 + v_4 + v_1v_2)x^9 + x^8 + (2v_1 + 2v_2 + 2v_3 + 2v_4 + 2v_1v_2 + 2)x^7 + (v_1 + v_2 + v_3 + v_4 + v_1v_2)x^6 + (2v_1 + 2v_2 + 2v_3 + 2v_4 + 2v_1v_2 + 1)x^5 + (2v_1 + 2v_2 + 2v_3 + 2v_4 + 2v_1v_2 + 2)x^4 + (v_1 + v_2 + v_3 + v_4 + v_1v_2 + 1)x^3 + x^2 + (2v_1 + 2v_2 + 2v_3 + 2v_4 + 2v_1v_2 + 2)x.$$

We can clearly see that the first and the last segment (i.e., the length of every segment is 15 components) of the Gray image of $w$ were both generated by $(x + x^8 + x^{13})(x^{12} + x^9 + x^6 + x^3 + 1)$ as a $[15,3,5]$-cyclic codes. So, if we introduce an error polynomial $e(x) = x + x^{14}$ with Hamming weight equals 2 (which is exceeds the error correction capacity of the $[90,42,4]$-Ω-multi-twisted code mentioned in Example 3.4.1) to interfere with the first or the last segments, then we obliged to apply the syndrome decoding algorithm for both segments regarding to their parameters and not to the main code parameters. By Computing the syndromes $s_i(x)$ of $x^i w(x)$ until $w_H(s_i(x)) \leq 2$, we see that it is only true for $s_1(x) = 1 + x^2$, thus $w(x)$ decoded to

$$w(x) - x^{14}s_1(x) = w(x) - (x + x^{14})$$

Briefly, every $n$-segment of a codeword in $\phi(C)$ need to be decoded independently with respect to their parameters only (where $C$ is a $\beta$-constacyclic code of length $n$ over $R$).

## 4. CONCLUSION

In this thesis, we discuss the main properties of the ring $R$ in Section 3.1, we found $R$ to be a semi-local, non-chain and principal ring. In Section 3.2, we proved that the Gray map $\phi$ from $R$ to $\boldsymbol{F}_p^6$ is distance preserving and Gray the image of $\omega$-constacyclic code of length $n$ over $R$ is a $\Omega$-multi-twisted code of index 6 and length $6n$ over $\boldsymbol{F}_p$, where $\Omega = (\alpha_0, \alpha_0 + \alpha_1, \alpha_0 + \alpha_2, \alpha_0 + \alpha_3, \alpha_0 + \alpha_4, \alpha_0 + \alpha_1 + \alpha_2 + \alpha_5)$. In Section 3.3, we proved that the generator polynomial of $\omega$-constacyclic code of length $n$ over $R$ is $g(x) = \sum_{i=1}^{6} \lambda_i g_i(x)$ where $g_i(x)$ is nothing but the generator polynomial of $C_i$. In Section 3.4, we gave an example of such a code where $\alpha_i = 1, 0 \leq i \leq 5$. Finally, in Section 3.5, we describe the decoding procedure on the Gray image of these types of codes, and we found that every $n$-segment in a codeword of $\phi(C)$ need to be decoded (after being received) independently with respect to their parameters only (where $C$ is a $\beta$-constacyclic code of length $n$ over $R$).

## REFERENCES


Aydin, N., Cengellenmis, Y. and Dertli, A. (2018). On some constacyclic codes over $\mathrm{Z}_4[u]/\langle u^2-1\rangle$, their $\mathrm{Z}_4$ images, and new codes. *Designs, Codes and Cryptography*, 86(6), 1249-1255.

Aydin, N. and Halilović, A. (2017). A generalization of quasi-twisted codes: Multi-twisted codes. *Finite Fields and Their Applications*, 45, 96-106.

Çallıalp, F. (2018). *Abstract Algebra With Examples*. Birsen Yayin Dagitim Ltd.

Dahrouj, A. M. F., Negacyclic and constacyclic codes over finite chain rings, The Islamic University of Gaza, Master's Thesis, Palestine, 2008.

Dertli, A. and Cengellenmis, Y. (2020). Quantum Codes Obtained from Some Constacyclic Codes over a Family of Finite Rings $F_p + uF_p + vF_p + uvF_p$. *Mathematics in Computer Science*, 14(2), 437-441.

Herstein, I. N. (1975). *Topics in Algebra*. University of Chicago press.

Hungerford, T. W. (2003). *Algebra*. Springer New York.

Ling, S. and Xing, C. (2004). *Coding Theory A First Course*. Cambridge University Press.

Qian, J.F., Zhang, L.N. and Zhu, S.X. (2006). $(1+u)$-constacyclic and cyclic codes over $F_2 + uF_2$. *Applied Mathematics Letters*, 19(8), 820-823.

Wolfman, J. (1999). Negacyclic and cyclic codes over $\mathrm{Z}_4$. *IEEE Transactions on Information Theory*, 45(7), 2527-2532.

Zheng, X. and Kong, B. (2017). Cyclic codes and $\lambda_1 + \lambda_2 u + \lambda_3 v + \lambda_4 uv$-constacyclic codes over $F_p + uF_p + vF_p + uvF_p$. *Applied Mathematics and Computation*, 306, 86-91.

Zhu, S. and Wang, L. (2011). A class of constacyclic codes over $F_p + uF_p$ and its Gray image. *Discrete Mathematics*, 311, 2677–2682.

Zhu, S., Wang, Y. and Shi, M. (2010). Some Results on Cyclic Codes over $F_2 + uF_2$. *IEEE Transactions on Information Theory*, 56(4), 1680-1684.

## CURRICULUM VITAE

**Personal Details**


| | |
|---|---|
| Name and surname | Abdallah K. A. Balaha |
| Gender | Male |
| Citizenship | Palestine |
| E-mail | abdallah.balaha@gmail.com |
| Current profession | Student |


**EDUCATION**

| | |
|---|---|
| *2018-09 – 2021-07* | Ondokuz Mayıs University - M.Sc. Mathematics<br>M.Sc. Mathematics minor Abstract Algebra and Number Theory |
| *2013-09 – 2017-07* | Al-Azhar University - B.Sc. Mathematics Credits: 139 B.Sc. Mathematics Minor Computer |