CONSTRUCTION OF CYCLIC DNA CODES OVER FINITE RINGS

2024
MASTER THESIS
MATHEMATICS

Theyazzin Mamdooh Yousif YOUSIF

Thesis Advisor
Assist. Prof. Dr. Tülay YILDIRIM TURAN

CONSTRUCTION OF CYCLIC DNA CODES OVER FINITE RINGS

Theyazzin Mamdooh Yousif YOUSIF

Thesis Advisor
Assist. Prof. Dr. Tülay YILDRIM TURAN

T.C.
Karabuk University
Institute of Graduate Programs
Department of Mathematics
Prepared as
Master Thesis

KARABÜK
September 2024

I certify that in my opinion the thesis submitted by Theyazzin Mamdooh Yousif YOUSIF titled “CONSTRUCTION OF CYCLIC DNA CODES OVER FINITE RINGS” is fully adequate in scope and in quality as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Tülay YILDIRIM TURAN .....
Thesis Advisor, Department of Mathematics

This thesis is accepted by the examining committee with a unanimous vote in the Department of Mathematics as a Master of Science thesis. 03.09.2024

Examining Committee Members (Institutions)	Signature
Chairman: Assist. Prof. Dr. Eda TEKİN (KBU)	.....
Member: Assist. Prof. Dr. Tülay YILDIRIM TURAN (KBU)	.....
Member: Assist. Prof. Dr. Onur SALDIR (VAN YYU)	.....

The degree of Master of Science by the thesis submitted is approved by the Administrative Board of the Institute of Graduate Programs, Karabük University.

Assoc. Prof. Dr. Zeynep ÖZCAN .....
Director of the Institute of Graduate Programs

"I declare that all the information within this thesis has been gathered and presented in accordance with academic regulations and ethical principles and I have according to the requirements of these regulations and principles cited all those which do not originate in this work as well."

Theyazzin Mamdooh Yousif YOUSIF

ABSTRACT

M. Sc. Thesis

CONSTRUCTION OF CYCLIC DNA CODES OVER FINITE RINGS

Theyazzin Mamdooh Yousif YOUSIF

Karabük University
Institute of Graduate Programs
Department of Mathematics

Thesis Advisor:
Assist. Prof. Dr. Tülay YILDIRIM TURAN
September 2024, 44 pages

In this thesis we study cyclic DNA codes over various finite rings. These rings are $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$, $R_2 = \mathbb{Z}_4 + v\mathbb{Z}_4$ with $v^2 = v$ and $R_3 = F_4 + vF_4$ with $v^2 = v$, respectively. We first investigated the algebraic properties of these ring structures and then examined the structure of the gray maps defined on these rings. Also, we analyzed how the generator polynomials of each ring structure can be obtained. We observed that cyclic codes over these rings satisfy the reverse constraint and the reverse-complement constraint. The relationships between each ring element and DNA nucleotides were examined. We included examples from the literature. In this way, the research has been strengthened and gained meaning.

Key Words **:** Linear codes, Cyclic codes, DNA codes, Finite rings.

Science Code **:** 94B05, 94B15

ÖZET

Yüksek Lisans Tezi

DEVİRLİ DNA KODLARIN SONLU HALKALAR ÜZERİNDEKİ İNŞAASI

Theyazzin Mamdooh Yousif YOUSIF

Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Anabilim Dalı

Tez Danışmanı:
Dr. Öğr. Üyesi Tülay YILDIRIM TURAN
Eylül 2024, 44 sayfa

Bu tezde çeşitli sonlu halkalar üzerindeki döngüsel DNA kodlarını inceliyoruz. Bu halkalar sırasıyla $u^2 = 0$ olmak üzere $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$, $v^2 = v$ olmak üzere $R_2 = \mathbb{Z}_4 + v\mathbb{Z}_4$ ve $v^2 = v$ olmak üzere $R_3 = F_4 + vF_4$. Öncelikle bu halkaların yapılarının cebirsel özelliklerini araştırdık ve daha sonra bu halkalar üzerinde tanımlanmış gri haritaların inceledik. Ayrıca her bir halka yapısının üreteç polinomlarının nasıl elde edilebileceğini analiz ettik. Bu halkalar üzerindeki döngüsel kodların ters kısıtlayıcı ve ters tamamlayıcı filtrelerini gözlemledik. Her bir halka elemanı ile DNA nükleotidleri arasındaki ilişkiler incelendi. Literatürden örnekler ekledik. Bu sayede araştırma güçlendi ve anlam kazandı.

Anahtar Kelimeler : Lineer kodlar. Devirli kodlar, DNA kodları, Sonlu halkalar.

Bilim Kodu **:** 94B05, 94B15

ACKNOWLEDGMENT

My most profound appreciation goes to my advisor Assist. Prof. Dr. Tülay YILDIRIM TURAN. The completion of this thesis would not have been possible without the guidance and support of my advisor. I would like to thank Prof. Dr. Ayşe NALLI and all teachers in College of Science at Karabük University for their kinds and help, whose invaluable feedback and encouragement greatly influenced how I conducted my experiments and interpreted my findings. I'd like to express my gratitude my friends and lovers for their generosity and encouragement, my time spent studying and living in the Turkey has been truly rewarding. I'd also like to thank everyone who has been there for me emotionally and intellectually as I've worked on my thesis. This study was supported by Scientific and Technological Research Council of Türkiye (TUBITAK) under the Grant Number 123F286. I thank TUBITAK for their support. To conclude, I'd like to thank God and my parents and my brother and sisters and my wife for any helps they did to me, it would have been impossible to finish my studies without their unwavering support over the past few years.

CONTENTS

Page

Page

LIST OF TABLES

Page

SYMBOLS AND ABBREVIATIONS INDEX

F	: Field
F_q	: finite field with the q elements
G	: Group
S_n	: n-th symmetric group
K_n	: Set of all permutations
R	: Ring
I	: Ideal
M	: Maximal ideal
P	: Prime ideal
C	: Code
$C^{\perp}$	: Dual Code
C	: Codeword of a code C
N	: Length of a code C
M	: Number of codeword on a code C
$d(C)$	: Minimum distance of C
g	: An element of a group G
$\langle g \rangle$	: The cyclic supgroup generated by g
a^{-1}	: Inverse of the element a.
Char(R)	: Characteristic of a ring R
F_q^n	: Vector space on F_q with n-length, q-alphabet
$S^{\perp}$	: The orthogonal complement of S
I_k	: The identity matrix with size k
wt_H	: The Hamming weight
wt_L	: The Lee weight
wt_E	: The Euclidean weight
d_H	: The Hamming distance
d_L	: The Lee distance
d_E	: The Euclidean distance

d_G	: The Gray distance
$\oplus$, $\otimes$	: Addition and multiplication operations, respectively
A	: The nucleotide DNA bases Adenine
T	: The nucleotide DNA bases Thymine
G	: The nucleotide DNA bases Guanine
C	: The nucleotide DNA bases Cytosine
c^r	: Reversible code of c
c^c	: Complement code of c
c^{rc}	: Reversible-complement code of c

PART 1

INTRODUCTION

Over the past half-century, the algebraic coding theory of linear codes has garnered significant attention. Numerous studies have been conducted on linear codes over fields, particularly binary fields, because of their extensive practical applications. Cyclic codes, a significant class of linear codes, are valued for their complex algebraic structures and practical uses.

The emphasis on code construction has traditionally been on fields, but recent research, such as in [1], has shifted focus towards finite rings. A significant portion of the research now centers on codes defined over finite chain rings [2]. However, optimal codes can also be found over non-chain rings (e.g., see [3]), although dealing with non-chain structures is generally more complex [4]. In [5], the algebraic properties of cyclic codes over $F_2 + vF_2$ with $v^2 = v$, are examined. Zhu and Wang explored a particular class of constacyclic codes over F_p +vF_p in [6]. In [7] authors examined codes over $F_2 + vF_2$ with $v^2 = v$ and presented reversible codes, which offer a valuable source for developing DNA codes.

A single DNA strand comprises a sequence of four possible nucleotides: adenine (A), guanine (G), cytosine (C), and thymine (T). The ends of a DNA strand have chemical polarity, referred to as the 5' end and the 3' end. Because there are 4^n possible DNA strands of length n, and DNA strands can be synthesized quickly and inexpensively, DNA codewords can be utilized to encode information at the molecular scale, offering a basis for molecular computing.

DNA-based applications demand successful and precise hybridization between a DNA codeword and its Watson-Crick complement, while minimizing the occurrence of false-positive and false-negative signals. A single strand can pair with its

complementary strand to create a double helix. The Watson-Crick complement of a DNA strand is formed by substituting each A with T, each T with A, each C with G, and each G with C, while also reversing the 3' and 5' ends. For example, the Watson-Crick complement of 3'-CCATTGA-5' would be 5'-GGTAACT-3'.

DNA code constitutes the genetic material that transmits genetic information from one cell to another and across generations. It acts as a director, regulating and dictating the synthesis of proteins within a cell at specific times. The process of translation involves converting genetic information from a nucleotide polymer into a polymer of amino acids.

Changes in nucleic acids lead to alterations in the amino acids present in proteins, which prompted the development of a genetic code that directs the amino acid sequence during protein synthesis. A codon is a group of nucleotides that specifies a single amino acid. The genetic code defines the relationship between the sequence of amino acids in a polypeptide chain. DNA code consists of four types of nucleotides (A, T, G, C), while proteins are made from various amino acids. In a single-letter code, each base corresponds to one amino acid, but only four of the twenty amino acids can be encoded. The doublet code, involving two bases per amino acid, allows for more combinations. Gamow proposed the triplet code in 1954, where three bases or letters specify one amino acid. This results in 64 possible codons to encode twenty amino acids, meaning that each amino acid is represented by multiple codons.

In 1994, Adleman [12] pioneered DNA computing by solving an instance of an NP-complete problem using DNA molecules, leveraging the WCC property of DNA strands. This breakthrough laid the foundation for further research, which has since expanded the application of DNA computing to various mathematical problems. For example, Benenson et al. [13] tackled the Boolean satisfiability problem, while Kari et al. [14] addressed the bounded post correspondence problem, another NP-complete issue. Additionally, Marathe et al. [15] introduced four key constraints for studying DNA codes: the Hamming constraint, the reverse constraint, the reverse-complement constraint, and the fixed GC-content constraint. The fixed GC-content constraint ensures that all codewords have uniform thermodynamic properties, while the other

three constraints help prevent inadmissible hybridization between different DNA strands.

Given its promising theoretical efficiency and early implementations, DNA computing is expected to generate significant interest in the near future. One key research goal is to understand and apply this capability to algebraic codes used in communication systems. DNA codes hold considerable potential because DNA computing offers faster processing and greater memory storage compared to traditional silicon-based systems. Due to the biological characteristics of DNA, cyclic and reversible codes are seen as analogous to DNA codes. As the understanding of cyclic and reversible codes has advanced, researchers have increasingly focused on exploring cyclic DNA codes.
This thesis is organized as follows:

In part 2, we reviewed the studies in the literature. First, we reviewed the research on linear codes and cyclic codes. Then, we included cyclic DNA codes and their important results.

In part 3, we have examined the basic concepts and theories required for our thesis. First, we introduced ring theory and field theories. In the rest of this section, we mentioned about the basic concepts and theories of linear codes and cyclic codes.

In part 4, we investigated the algebraic structure of linear codes over the rings R_1, R_2 and R_3 examined their basic definitions and theories. In this section, we pay particular attention to how Gray maps, which are important for each ring structure, are defined.

In part 5, we investigate the construction and properties of cyclic DNA codes over different finite rings. Our primary objective is to examine the new structures and characteristics of these codes within these rings. In our research, we have observed how these codes can attain desirable features, such as error correction capabilities. Additionally, we have incorporated key theories and examples from existing literature, and provided tables that illustrate the relationships between DNA nucleotides and various ring elements.

In part 6, We summarize all the studies in the thesis. We also commented on possible topics that could be studied on in the future.

PART 2

LITERATURE REVIEW

Cyclic codes are among the most significant and extensively examined types of linear codes, renowned for their rich algebraic structure due to their representation as ideals in a polynomial ring. Recently, codes over rings have also garnered considerable research interest. Many authors have explored the structure of cyclic codes across various rings [23, 24, 25].

In [26], Adleman conducted a groundbreaking experiment in DNA computing. His approach utilized DNA, known for its dense and self-replicating properties, as an ideal medium for solving mathematical problems. Following this successful experiment, the field of DNA computing saw a surge of innovation, including developments in DNA tile assembly, the creation of DNA nanostructures, DNA-based data storage systems, and investigations into the error-correcting capabilities of DNA.

To explore DNA computing through algebraic coding theory, researchers have examined error-correcting codes over finite fields and finite rings of cardinality 4^n, mapping DNA nucleotides to elements of these structures. This approach led to rapid advancements in the study of cyclic DNA codes and their generalizations [8]. Abualrub et al. [9] focused on DNA codes over a field with four elements, developing a theory for constructing linear and cyclic codes of specific lengths over GF(4) to advance DNA computing. Siap et al. [10] investigated cyclic DNA codes over the finite ring $F_2 + uF_2$ with $u^2 = 1$. Guenda et al. [11] constructed DNA codes over the finite ring $F_2[u]/< u^2 >$ and developed an infinite family of BCH DNA codes. Liang et al. [12] also explored cyclic DNA codes over the same ring, providing necessary and sufficient conditions for reversible and reverse-complement codes. Yildiz et al. [13] examined cyclic DNA codes of odd length over the ring $F_2 +$

uF_2 with $u^4 = 1$, matching 16 elements of this ring with paired DNA nucleotides and studying the algebraic properties of these codes. Bayram et al. [14] discussed DNA codes and their applications over the ring $F_4[v]/< v^2 = v >$. Zhu et al. [15] considered cyclic codes of arbitrary length over the finite non-chain ring $\frac{F_2[u,v]}{<u^2}$, $v^2 - v, uv - vu >$, addressing codes that meet the reverse and reverse-complement constraints. Oztas et al. [16] introduced a new family of polynomials over GF(16) that generates reversible codes within this field. Additional studies on cyclic DNA codes across various rings are detailed in [17–22].

PART 3

PRELIMINARIES

In this section, we firstly give the necessary background of the ring theory and field theory. For more details, we refer reader to [28,29,30,31,32,33,34]. The chapter then continues by giving basic information about linear codes and a special class of them, cyclic codes. The main references for these codes are [27,35,36].

3.1. RING THEORY

Coding theory is related to algebra, a branch of mathematics. Therefore, in this part of the thesis, basic definitions, theorems, and results taken from many algebra books related to the subjects within the scope of the thesis is included [28,29,30,31].

Definition 3.1.1. [28]. Let $X \neq \emptyset$ be a set. $X \times X$ a defined from the Cartesian set to the set

$\Delta: X \times X \rightarrow X$

such that $(a, b) \mapsto a \Delta b$. The function is called a “binary operation” defined on X. The set defined by this operation is called "algebraic structure".

Definition 3.1.2.[28]. Let $G \neq \emptyset$ be a set and Δ a binary operation on the set G. Then

(i) For all $a, b, c \in G$, $a \Delta (b \Delta c) = (a \Delta b) \Delta c$.

(ii) There exists an element $e \in G$ such that for every $a \in G$, $a \Delta e = e \Delta a = a$.

(iii) For every $a \in G$, there exists $a^{-1} \in G$ such that $a \Delta a^{-1} = a^{-1} \Delta a = e$.

If these conditions hold on G, then (G, Δ) is called a group.

If for all a, b ∈ G, a Δ b = b Δ a then (G, Δ) is called a commutative group.

Definition 3.1.3.[28]. Let K be a non-empty set and $f: K \to K$ be a function. If the function f is injective and onto, the f is called a " permutation " on the set K. In particular, the set of all permutations on the set $K_n = [1,2,\dots.,n]$ is denoted by S_n , and the set S_n is called the " n – th symmetric group ". Any α in S_n is defined as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots\dots\dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots\dots\dots & \alpha(n) \end{pmatrix}.$$

Definition 3.1.4. Let H be a non-empty subset of the group (G, Δ). If (H, Δ) is a group, then H is called a subgroup of G.

Definition 3.1.5. Let g be an element in a group G. If the subgroup of G consists of all its integer powers, then it is called the cyclic subgroup generated by g, defined as $< g >=\{g^k: k \in Z\}$. The order of g is the number of element in $< g >$ and denoted by $| < g > |$.

Definition 3.1.6.[29]. Let R≠ ∅ be a set and "+" and "." two binary operations. Then,

(i) (R, +) is an abelian group,

(ii) (a. b). c = a. (b. c), for each a, b, c ∈ R,

(iii) (a + b). c = a. c + b .c and a. (b + c) = a.b + a .c for each a, b, c ∈ R,

If these conditions hold, then (R, +,.) is called ring.

If for all a, b ∈ R, a. b = b. a, then (R, +,.) is called a commutative ring.

If for all $a \in R$, $1_R \,.\, a = a \,.\, 1_R = a$, then (R, +,.) is called a unit ring.

Definition 3.1.7. If R is a unitary ring and there is an inverse of r ∈ R, then r is called a unitary element of R.

Definition 3.1.8.[29]. Let a be a nonzero element of R. If there exists a nonzero b ∈ R such that a. b = 0_R (b.a = 0_R) then a is called the left (right) divisor element of the ring R.

Definition 3.1.9.[29]. Let R be a unitary and commutative ring such that $1_R \neq 0_R$. If the ring R has no zero divisors, the ring R is called an integral domain. If every nonzero element of the ring R ring, which has a unit element, is reversible, then R is called a division ring.

Definition 3.1.10. Let R and S be two rings, then a ring homomorphism is a function $f: R \to S$ and it is closed under addition, multiplication and multiplicative identity such that for all $a, b \in R$,

(i) $f(a+b) = f(a) + f(b)$,

(ii) $f(a.b) = f(a).f(b)$,

(iii) $f(1_R) = 1_S$

Definition 3.1.11. Let R and S be two rings and $f: R \to S$ be a given ring homomorphism. The kernel of f, denoted by ker (f) and defined as $\{r \in R: f(r) = 0_S\}$, where 0_S is the zero element of S.

Definition 3.1.12. Let R be a ring. If there is a positive integer n such that $n.r = 0_R$ for all $r \in R$, then the smallest such positive integer is called the characteristic of R and denoted by Char(R). If there is no such positive integer, then R is said to be characteristic zero.

Definition 3.1.13. [29]. Let R be a ring and $\emptyset \neq I$ a subset of R. If the followings hold, I is called an ideal of R

(i) $a - b \in I$ for all $a, b \in I$,

(ii) $ra \in I \; or \; ar \in I$ for $all \; a \in I \; and \; r \in R$.

Definition 3.1.14. Let R be a commutative ring with unity. An ideal M in a ring R is called a maximal ideal if $M \neq R$ and the only ideals containing M are M and R.

In a ring with unity, every proper ideal is contained in a maximal ideal.

Definition 3.1.15. Let R be a commutative ring with unity. Then an ideal P is called a prime ideal if

(i) $P \neq R$,

(ii) If $a.b \in P$, then at least one of the a a or b in P.

Definition 3.1.16. Let $f: R \to S$ be a ring homomorphism with $\ker(f) = I$. The cosets of ker (f) are of the form $r + I$. In particular, if $f(\mathrm{r}) = b$, then $f^{-1}(b) = r + I$. The cosets defined by a ring isomorphic image of f such that

(i) $(r + I) + (s + I) = (r + s) + I$,

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

The corresponding ring of cosets is called the quotient ring of R by $\ker(f) = I$, denoted by R/I.

Definition 3.1.17. Let R be a ring, and $a_0, a_1, a_2, \ldots\ldots, a_n$ $(n \geq 0)$ are the elements of R. A polynomial $f(x)$ over R is of the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

If $a_n \neq 0$, then the degree of $f(x)$ is n. If $f(x) = 0$, then the degree of $f(x)$ is undefined. If degree of $f(x)$ is n, it is written as $\deg f(x) = n$. The set of all polynomials in the indeterminate x with coefficients in R is denoted by R[x].

3.2. FINITE FIELDS

Since the structures used in cyclic DNA codes are closely related to finite fields, we give the basic properties of finite fields elements in this section. Throughout this section, we follow [32,33,34].

Definition 3.2.1. Let F_q be a finite field with q elements. The set of vectors of length n is defined as

$F_q^n = \{(v_1, v_2, \dots, v_n) | v_i \in F_q, 0 \leq i \leq n\}$.

Let $v = (v_1, v_2, \dots, v_n), w = (w_1, w_2, \dots, w_n)$ be vectors in F_q^n and $\lambda \in F_q$, then addition and multiplication operations on F_q^n are defined as:

(i) $v + w = (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n) \in F_q$.

(ii) $\lambda v = (\lambda v_1, \lambda v_2, \dots, \lambda v_n) \in F_q$.

Thus, F_q^n is a vector space on F_q.

Definition 3.2.2. Let V be a vector space on F_q and $\emptyset \neq C \subseteq V$. Then

(i) $x + y \in C$ for all $x, y \in C$,

(ii) $\lambda x \in C$ for all $\lambda \in F_q$ and $x \in C$.

Thus, the set C is called a subvector space of V.

Definition 3.2.3.

(i) Let V be a vector space on F_q and $\lambda_1, \lambda_2, \dots, \lambda_n \in F_q$. A linear combination of vectors $v_1, v_2, \dots, v_n$ in V is written in the form of $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$.

(ii) If the only solution of the equation $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$ is $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$, the set $\{v_1, v_2, \dots, v_n\}$ is linearly independent .

(iii) Let $S = \{v_1, v_2, \dots, v_n\} \subseteq V$. The set of all linear combinations of S is denoted by $\langle S \rangle$ and

$\langle S \rangle = \{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n | \lambda_1, \lambda_2, \dots, \lambda_n \in F_q\}$. $\langle S \rangle$ is called the subvector space generated by S. Moreover, the set S is a generator set of $\langle S \rangle$.

Proposition 3.2.4. If S is a sub-vector space of V, then $\langle S \rangle = S$.

Definition 3.2.5. Let V be a vector space on F_q.

(i) If the set $A = \{v_1, v_2, \dots, v_n\}$ is linearly independent and $V = \langle A \rangle$, then the set A is called a basis of the vector space V.

(ii) The number of elements of the basis A is called the dimension of V and is denoted by $\dim(V)$. If A contains infinite elements, then $\dim(V) = \infty$.

Theorem 3.2.6. Let V be a vector space on F_q. If $\dim(V) = k$, then

(i) the number of vectors in V is exactly q^k,

(ii) V has exactly $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$ different basis.

Definition 3.2.7. Let $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in F_q^n$.

(i) The Euclidean inner product vectors x and y is defined as $\langle x, y\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n$.

(ii) If S is a subset of F_q^n, then the set $S^{\perp} = \{x \in F_q^n | \langle x, s\rangle = 0\ , \forall s \in S\}$ is called the orthogonal complement of S .

Let $S \subseteq F_q^n$, then the set $S^{\perp}$ is always a subspace of F_q^n and $\langle S\rangle^{\perp} = S^{\perp}$.

Theorem 3.2.8. Let $S \subseteq F_q^n$, then $dim(S) + dim(S^{\perp}) = n$.

3.3. LINEAR CODES

Coding theory starts from the coding of the message and covers all stages until it reaches the receiver (even until the detection and correction of errors, if any). Linear codes are mathematical objects that play an important role in error correction and data transmission. In this section, general definitions and theorems regarding coding theory are mentioned [27,35,36].

Definition 3.2.1. A subset *C* of the set F_q with M elements is called the (n, M)-code defined on the finite filed F_q. The vector $(a_1, a_2, \ldots\ldots, a_n) \in F_q^n$ can also be represented in the form $a_1, a_2, \ldots\ldots, a_n$ and the vectors in the C set are called codewords. If the set *C* is a k-dimensional subspace of the vector space $\boldsymbol{F_q}$, then the set C is called the [n, k] linear code on the finite field F_q. *A* linear code C over the finite field F_q has q^k codewords. Throughout the section, we follow [27].

Definition 3.2.2. A $k \times n$ matrix *G*, whose rows are formed by the components of a basis of the subspace *C*, is called the generator matrix of the linear code *C*. The generator matrix of the code is in the form of $[I_k|A]$, where the matrix I_k is the identity matrix.

Definition 3.2.3. An $(n-k) \times k$ matrix H defined by $C = \{x \in F_q^n | Hx^T = 0\}$ is called check matrix (parity-check matrix) for the linear code *C*.

Theorem 3.2.4: Let *R* be a finite ring and *n* be a positive integer. If the set ***C*** is an R-submodule of the set $R^n = \{(u_1, u_2, \dots, u_n): u_i \in R, i = 1,2, \dots., n\}$, then C is called linear code over the ring R.

The distance of a code is one of the most important subjects. The minimum distance of a code provides information about the ability of the code to detect and correct the errors.

Definition 3.2.5. Let $d: F_q^n \times F_q^n \to \mathbb{N} \cup \{0\}$, for each $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in F_q^n$,

$(x,y) \longmapsto d(x,y) = |\{i: x_i \neq y_i\}|$

is called Hamming distance [1]. The Hamming distance has the following properties:

(i) $0 \leq d(x,y) \leq n$, for each $x, y \in \mathbb{F}_q^n$,

(ii) $d(x,y) = 0$ if and only if $x=y$ for all $x, y \in \mathbb{F}_q^n$,

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

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

Definition 3.2.6. Let *C* be a code,

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

is called the minimum distance of *C*.

Definition 3.2.7. A code with length n, number of elements M and minimum distance d is called a (n,M,d) code.

Definition 3.2.8. Let $\boldsymbol{x}$ be any element of the vector space $\mathbb{F}_{\boldsymbol{q}}^{\boldsymbol{n}}$**.** The number of non-zero components of the *x* is called the Hamming weight of the $\boldsymbol{x}$ and is denoted by $wt(x)$.

Lemma 3.2.9. For any $x, y \in \mathbb{F}_q^n, d(x,y) = wt(x-y)$.

Definition 3.2.10. Let *C* be a linear code. The smallest weight of the codewords different from the zero vector of the code *C* is called the minimum (Hamming) weight of *C* and is denoted by *wt(C).*

Theorem 3.2.11. If *C* is a linear code, then $d(c) = wt(c)$.

Definition 3.2.12. The dual code of C is denoted by $C^{\perp}$ and defined as

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

where $x.y$ represents the Euclidean inner product of x and y over the ring R.

3.4. CYCLIC CODES

Cyclic codes were first studied by Eugene Prange (1957) [28]. This work has led to important developments in the field of error-correcting codes theory. Some important code families are cyclic codes, such as Golay codes, BCH codes, and Reed-Solomon codes. Cyclic codes are more advantageous in the field of application thanks to their algebraic structure [35,36].

Definition 3.4.1.[36] If *C* is a linear code and for each $C = (c_{0,}c_1, \ldots., c_{n-1}) \in C$, $\psi(c) = (c_{n-1}, c_0, \ldots., c_{n-2}) \in C$, then *C* is called a cyclic code. The ψ transformation is called cyclic shift.

Example 3.4.2. The binary linear code

C
$= \{0000000,1011100,0101110,0010111,1110010,0111001,1001011,1100101\}$ is a cyclic code of length 7.

Definition 3.4.3.[36] Codes can be expressed in terms of polynomials as

$$\pi: F_q^n \longrightarrow F_q[x]/\langle x^n - 1\rangle.$$

The function π is defined as a linear transformation such that $c = (c_0, c_1, \ldots\ldots, c_{n-1}) \longrightarrow c(x) = c_0 + c_1 x + \cdots \ldots + c_{n-1}x^{n-1}$. The cyclic translation of $c \epsilon C$ codeword corresponds to x.c(x). Thus, cyclic codes can be expressed in terms of ideals.

Theorem 3.4.4. [36] Let $\boldsymbol{C \subseteq F_q^n}$. The necessary and sufficient condition for the linear code to be a cyclic code is that $\pi(C)$ is an ideal of the ring $F_q[x]/\langle x^n - 1\rangle$.

Example 3.4.5. The code C = {000,110,101,011} is a binary cyclic code. The set of polynomials corresponding to the codewords of C is $\pi(C) = \{0,1 + x, 1 + x^2, x + x^2\}$, $F_2[x]/\langle x^3 - 1\rangle$ is an ideal of the ring $\pi(C)$.

Theorem 3.4.6 [36] The smallest non-zero-degree monic polynomial in any non-zero ideal of the ring $F_q\,[x]/\langle x^n - 1\rangle$ is odd.

Definition 3.4.7.[36] Let $F_{q,n} = F_q[x]/\langle x^n - 1\rangle$ be a cyclic code and $C \subseteq F_q^n$ corresponds to $\pi(C)$ ideal of non-zero monic polynomial g(x). In this case, the polynomial g(x) is called the generator polynomial of C and is defined by $C = \langle g(x)\rangle = \{f(x)g(x) | f(x) \in F_{q,n}$.

Example 3.4.8. Let C= {000,110,011,101} be a cyclic code and its corresponding ideal is $\pi(C) = \{0,1 + x, x + x^2, 1 + x^2\} \subseteq F_2[X]/\langle X^3 - 1\rangle$. The smallest degree monic polynomial in this ideal produces the ideal 1+x, and $\pi(C)$ is also the generator polynomial of the C code.

Theorem 3.4.9 [36] In the ring $F_q[x]$, each monic divisor of the polynomial $x^n - 1$ produces a cyclic code defined on F_q.

Now, we introduce prime factorization of the polynomial $x^n - 1$ in the ring $F_q[x]$.

Theorem 3.4.10 [36] Let $x^n - 1 = \prod_{i=1}^{r} p_i^{e_i}(x)$. The number of cyclic codes of length n on F_q is $\prod_{i=1}^{r}(e_i + 1)$.

Theorem 3.4.11. Let g(x) $\in$ $F_q[x]$, $g(x)|x^n - 1$ and deg(g(x)) =k. Then the code corresponding to the ideal generated by g(x) is a cyclic code of length n and dimension is an n-k code.

Example 3.4.12 [36] $x^7 - 1 = (1 + x)(1 + x^2 + x^3)(1 + x + x^3) \in F_2[x]$ is the decomposition of irreducible factor. The number of cyclic codes with length 7 on F_2 is 8 where $g(x) = (1 + x)(1 + x^2 + x^3) = 1 + x + x^2 + x^4$ polynomial produces a cyclic code of length 7 and dimension 3 such that

$\langle g(x) \rangle$
$= 0000000,1110100,0111010,0011101,1001110,0100111,1010011,1101001.$

Theorem 3.4.13 [36] Let $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k} \in F_q[x]$ and g(x) be a divisor of $x^n - 1$. The generator polynomial of code C is

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

Definition 3.4.14.[36] Let $h(x) = \sum_{i=0}^{k} a_i x^i$ be a polynomial of degree k. The reciprocal polynomial of h(x) is defined as $h^*(x) \coloneqq x^k h(1/x) = \sum_{i=0}^{k} a_{k-i} x^i$ polynomial.

Theorem 3.4.15.[36] Let C be cyclic code with [n, k] parameters defined on F_q , and the polynomial g(x) be the generator polynomial of C such that $g(x) = h_0 + h_1x + \cdots + h_kx^k \; and \; h(x) = (x^n - 1)/g(x)$. The polynomial $h_0^{-1}h^*(x)$ is the generator polynomial of the dual code $C^\perp$ and the polynomial $h_0^{-1}h^*(x)$ is called the control polynomial of C. The check matrix of C is defined as

$$H = \begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \ldots & \cdots & h_0 \end{pmatrix}$$

Example 3.4.16 [36] By Example 3.4.12, the generator matrix for the cyclic code generated by $g(x) = 1 + x + x^2 + x^4$ on F_q is

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

In the form. $h(x) = (x^7 - 1)/g(x) = 1 + x + x^2 + x^3$ and $h^*(x) = 1 + x^2 + x^3$. So, the check matrix is

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

Thus, the polynomial $h_0^{-1}h^*(x) = 1 + x^2 + x^3$ is also the check polynomial of C.

PART 4

LINEAR CODES OVER THE FINITE RINGS

Linear codes on finite rings represent an increasingly important area of coding theory. While traditional linear codes are typically constructed over finite fields such as $\mathbb{F}_q$, investigating coding theory over finite rings expands the scope of potential applications and offers unique algebraic properties that can be used for error detection and correction. Finite rings, unlike finite fields, may contain zero divisors and lack a multiplicative inverse for every non-zero element. These characteristics pose both challenges and opportunities in the context of coding theory. The rich structure of finite rings allows for the construction of codes with properties that are not possible over fields.

In this section, we specifically examine linear codes on three different finite rings. These rings are $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$, $R_2 = \mathbb{Z}_4 + v\mathbb{Z}_4$ with $v^2 = v$ and $R_3 = F_4 + vF_4$ with $v^2 = v$. We discussed the properties of linear codes for these finite rings respectively.

4.1. ALGEBRAIC PROPERTIES OF THE RING R_1

Let $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ be a ring with $u^2 = 0$ [37]. There are four elements in the ring R_1 and its characteristic number is two. The set of elements of R_1 is $\{0,1,u,\bar{u} = u + 1\}$. This ring is a local ring that has several good qualities with Z_4 and its maximal ideals are 0 and u. An additive submodule of the R_1-module ${R_1}^n$ is defined as a linear code C of length n [4]. In the literarture, Dougherty et al. [40], Bonnecaze and Udaya [39], and Bachoc [38] examined codes over the ring R_1 in details.

The Hamming weight of a codeword $u = (u_1, u_2, \dots, u_n)$ is the number of nonzero entries in u, and denoted by $w(u)$. The Hamming distance of a linear code C is

$d(C) = \min\{w(u): u \in C, u \neq 0\}$.

Massy defined a linear code with a complementary-dual (LCD CODE) as a linear code C that satisfies $C \cap C^{\perp} = \{0\}$. Generally, any linear code C over the finite rings satisfies $(C^{\perp})^{\perp} \neq C$; however, over the ring R_1 one has $(C^{\perp})^{\perp} = C$ [41].

Theorem 4.1.1 [43] Let $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ be a ring with $u^2 = 0$. A generator matrix of an R_1-linear code C is defined as

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

where A and D are F_2-matrices, B is an R_1-matrix, and I_{k_1}, I_{k_2} indicate the $k_1 \times k_1$and $k_2 \times k_2$ identity matrices, respectively. C is a free R_1-module if and only if k_2 = 0 and C is an abelian group of type $4^{k_1}2^{k_2}$.

Theorem 4.1.2 [43] Let $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ be a ring with $u^2 = 0$ and n is an odd positive integer. Then every ideal of R_1 is a principal ideal.

Since the factorization of $x^n - 1$ over R_n is not unique. For an odd positive integer n, we can consider the following theorem.

Theorem 4.1.3 [39] Let n be an odd positive integer. The factorization

$$x^n - 1 = f_1(x)f_2(x) \dots \dots f_r(x)$$

is unique if f_i are basic irreducible and pairwise co-prime polynomial. This factorization is obtained from factorization of $x^n - 1$ over F_2.

Theorem 4.1.4 [39,41] Let C be a cyclic code of odd length n over R_1, then

$$C = < f(x)h(x), uf(x)g(x) >,$$

where $f(x), g(x), h(x)$ are unique monic polynomials such that where $x^n - 1 =$ f(x)g(x)h(x) and $|C| = 4^{\deg(g(x))}2^{\deg(h(x))}$.

Corollary 4.1.1 [41] Given a cyclic code C = (f(x)h(x), uf(x)g(x)) of odd length n over R_1, where f(x), g(x), and h(x) are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$, then

(i) if $h(x) = 1$, then $C =< f(x) >, |C| = 4^{n-deg\,(f(x))}$,

(ii) if $g(x) = 1$, then $C =< uF(x) >, |C| = 2^{n-\deg(f(x))}$.

Theorem 4.1.5 [41] Let $C =< f(x)h(x), uf(x)g(x) >$ be a cyclic code of odd length n over R_1, where $f(x), g(x), and\ h(x)$ are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$, and |C| = $4^{\deg(g(x))}2^{\deg(h(x))}$. Then the dual code of C is generated as

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

and $|C^{\perp}| = 4^{\deg(f(x))}2^{\deg(h(x))}$, where $f^*(x), h^*(x)$ and $g^*(x)$ are the reciprocal polynomials of $f(x), h(x), and\ g(x)$, respectively.

Corollary 4.1.2 [41] Let $C =< f(x)h(x), uf(x)g(x) >$ be a cyclic code of odd length n over R_1, where f(x), g(x), and h(x) are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$ and the dual code of C is generated as $C^{\perp} = (\ g^*(x)h^*(x), ug^*(x)\ f^*(x))$, then we have

(i) if $h(x) = 1$, then $C =< f(x) >$ and $C^{\perp} = g^*(x)$,

(ii) if $g(x) = 1$, then $C =< uf(x) >$ and $C^{\perp} = \left(h^*(x), uf^*(x)\right)$.

4.2. ALGEBRAIC PROPERTIES OF THE RING R_2

Let $R_2 = \mathbb{Z}_4 + v\mathbb{Z}_4$ be a ring with $v^2 = v$ and $\{0,1,2,3, v, 2v, 3v, 1+v, 2+v, 3+v, 1+2v, 2+2v, 3+2v, 1+3v, 2+3v, 3+3v\}$ is the set of elements in ring R_2. The ring R_2 is isomorphic to the polynomial ring $\frac{\mathbb{Z}_4[v]}{\langle v^2-v\rangle}$. The set {1,3,1+2v,3+2v} is a set of unit elements in R_2. Also, R_2 is a principal ideal ring with two maximal ideals $\langle 2+v\rangle$ and $\langle 1+v\rangle$. Thus, R_2 is a semi-local ring. On the other hand, the rings $\frac{R_2}{\langle 2+v\rangle}$and $\frac{R_2}{\langle 1+v\rangle}$ are isomorphic to $\mathbb{Z}_2$. Throughout the section we follow [44,45].

Since maximal ideals of R_2 are $\langle 2+v\rangle$ and $\langle 1+v\rangle$, by Chineese Remainder Theorem R_2 can be expressed as $R_2 = \langle 2+v\rangle \oplus \langle 1+v\rangle$. Thus, for any element $a+vb$ in R_2,

$$a + vb = \alpha(2+v) + \beta(1+v)$$

where $a, b, \alpha, \beta \in \mathbb{Z}_4$. However, this expression is not unique and every element $a+vb$ of R_2 can be written as uniquely $\alpha(1+3v)+\beta v$, where $\alpha, \beta \in \mathbb{Z}_4$ so that

$$R_2 = \langle 1+3v\rangle \oplus \langle v\rangle$$

Therefore, $\alpha = a$ and $\beta = a+b$ and so $+vb = a(1+3v) + (a+b)v$.

Definition 4.2.1 Let $a+vb \in R$, the Gray map from R_2 to $\mathbb{Z}_4$ is defined as

$$\Psi: R_2 \longrightarrow \mathbb{Z}_4$$
$$\Psi(\mathrm{a}+\mathrm{vb}) = (\mathrm{a}, \mathrm{a}+\mathrm{b})$$

where $a+vb \in R_2$. This map can be extended by component wise as

$$\phi: {R_2}^n \longrightarrow \mathbb{Z}_4^{2n}$$
$$\phi(x_1, x_2, \dots, x_n) = (a_1, a_2, \dots, a_n, a_1+b_1, a_2+b_2, \dots, a_n+b_n)$$

where $x_i = a_i + vb_i$, $i = 1,2,\dots,n$. It is easy to check that ϕ is $\mathbb{Z}_4$ modules isomorphism.

Definition 4.2.2 Let x be an element in $\mathbb{Z}_4^n$, then

(i) The Hamming weight is defined as

$$wt_H(x) = n_1(x) + n_2(x) + n_3(x)$$

(ii) The Lee weight is defined as

$$wt_L(x) = n_1(x) + 2n_2 + n_3$$

(iii) (The Euclidean weight is defined as

$$wt_E(x) = n_1(x) + 4n_2(x) + n_3(x)$$

where $n_i(x)$ indicates the number of coordinates of x equal to i.

Definition 4.2.3. The Gray weight of any element x in R_2 can be defined as the Hamming weight

$$wt_G(x) = wt_H(a, a + b)$$

The Lee weight of x in R_2 is defined as

$$wt_L(x) = wt_L(a, a + b)$$

The Euclidean weight x in R_2 is defined as

$$wt_E(x) = wt_E(a, a + b)$$

Let $x, y \in R_2^n$, then the Hamming distance, the Lee distance, the Gray distance and the Euclidean distance are denoted by $d_H(x, y), d_L(x, y), d_G(x, y)$ and $d_E(x, y)$, respectively. The distance between x and y is always weights of $x - y$.

A linear code C of length n over R_2 is an R_2-submodule of R_2^n.

Lemma 4.2.4. The Gray map $\phi: {R_2}^n \longrightarrow \mathbb{Z}_4^{2n}$ is a distance-preserving and linear map.

Proof: Let $x, y \in {R_2}^n$ and $r \in Z_4$, then we have $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(rx) = r\phi(x)$. So, ϕ is a linear map. Thus,

$$d_L(x,y) = wt_L(x-y) = wt_L\left(\phi(x-y) = wt_L\big(\phi(x)\big) - \phi(y)\right)$$
$$= d_L\big(\phi(x), \phi(y)\big).$$

By the same routine,

$d_E(x,y) = d_E\big(\phi(x), \phi(y)\big)$ and $d_G(x,y) = d_H\big(\phi(X), \phi(Y)\big)$.

By the linearity of the Gray map, if C is a linear code over r of length n then $\phi(C)$ is also a linear code over $\mathbb{Z}_4$ with length 2n.

Definition 4.2.5. Let

$$C_1 = \{a \in \mathbb{Z}_4^n : a + bv \in C \ for\ some\ b \in \mathbb{Z}_4^n\}$$

And

$$C_2 = \{a + b \in \mathbb{Z}_4^n : a + bv \in C \ for\ some\ a \in \mathbb{Z}_4^n\}$$

be two linear codes over $\mathbb{Z}_4$. Since R_2 is a Frobenius ring [45], we have $|C||C^{\perp}| = 16^n$.

Theorem 4.2.6. Let C be a linear code over R_2 with length n. Then $\phi(C) = C_1 \otimes C_2\ and\ |C| = |C_1||C_2|$.

Proof: Since ϕ is a bijective map, for any $C' = (a_1, a_2, \ldots, a_n, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \in \phi(C)$ there exists a $c = (C_1, C_2, \ldots, C_n)$ in C there exists a $C = (C_1, C_2, \ldots, C_n) \in$ C such that $\phi(C) = C'$ where $c_i = a_i + b_i v$.

By the construction of C_1 and C_2, one has $(a_1, a_2, \ldots, a_n) \in C_1$ and $(a_1 + b_1, a_2 + b_2, \ldots, a_n b_n) \in C_2$. So, $(a_1, a_2, \ldots, a_n, a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \in C_1 \otimes C_2$. Hence $\phi(C) \subseteq C_1 \otimes C_2$.

Let $a = (a_1, a_2, \ldots, a_n) \in C_1$, and $b = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \in C_2$ and for every $(a, b) \in C_1 \otimes C_2$, there exists $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in C such that $x = a + vs$ and $y = b + (1 + 3v)t$ where $s, t \in \mathbb{Z}_4^n$. By the linearity of C, we have

$$x(1 + 3v) + yv = a + (3a + b)v \in C.$$

Thus, $\phi(a + (3a + b)v) = (a, b) \in \phi(C)$. This shows that $C_1 \otimes C_2 \subseteq \phi(C)$. Therefore,

$$|\phi(C)| = |C_1 \otimes C_2| = |C_1||C_2|.$$

ϕ is a bijective map and so we have

$$|C| = |\phi(C)| = |C_1||C_2|.$$

Corollary 4.2.7. Let C be a linear code over R_2, then $C = (1 + 3v)C_1 \otimes vC_2$.

Proof: Assume that $c = (c_1, c_2, \ldots, c_n) \in C$ where $c_i = a_i + b_i v$. So, $\phi(c) = (a, \ a + b)$, where $b = (b_1, b_2, \ldots, b_n)$ and $a = (a_1, a_2, \ldots, a_n)$. $a \in C_1$, $a + b \in C_2$ since $\phi(C) = C_1 \otimes C_2$. Therefore,

$$(1 + 3v)a + v(a + b) = a + bv = c \in (1 + 3v)C_1 \oplus vC_2$$

as a result. As a result, $C \subseteq (1 + 3v)C_1 \oplus vC_2$.

Let $a \in C_1$ and $b \in C_2$, such that $x = (1+3v)a + vb \in (1+3v)C_1 \oplus vC_2$. So,

$\phi(x) = (a, b) \in C_1 \otimes C_2 = \phi(C)$.

Since ϕ is a bijective map $x \in C$ and so that $(1+3v)C_1 \oplus vC_2 \subseteq C$. As a result

$C = (1+3v)C_1 \oplus C_2$.

Theorem 4.2.8. Let C be a linear code over R_2 with length n. Then $\phi(C^{\perp}) = \phi(C)^{\perp}$

Proof: Let $c_1 = a_1 + vb_2 \in C^{\perp}$ such that $\phi(c_1) \in \phi C^{\perp}$. Then for all $c_2 = a_2 + vb_2 \in C$, we have $c_1.c_2 = 0$. This shows that $a_1.b_2 + a_2.b_1 + b_1.b_2 = 0$ and $a_1.a_2 = 0$. For any element $c_2 \in C$, one gets $\phi(c_2) \in \phi(C)$ and

$$\phi(c_1).\phi(c_2) = (a_1, a_1 + b_1).(a_2, a_2 + b_2) = 2a_1.a_2 + (a_1.b_2 + a_2.b_1 + b_1.b_2) = 0$$

Thus, $\phi(c_1) \in \phi(C)^{\perp}$ and this implies that $\phi(C^{\perp}) \subseteq \phi(C)^{\perp}$

For the converse inclusion, we have module isomorphic map ϕ and $\mathbb{Z}_4$ −code $\phi(C)$ with length 2n. Thus, $|\phi(C)^{\perp}| = \frac{4^{2n}}{|\phi(C)|} = \frac{16^n}{|C|} = |C^{\perp}| = |\phi(C)^{\perp}|$. Consequently $\phi(C^{\perp}) = \phi(C)^{\perp}$.

Theorem 4.2.9. Let C be a linear code and $C^{\perp}$ a dual code of C over R_2 with length n such that $\phi(C) = C_1 \otimes C_2$. Then $\phi(C)^{\perp} = C_1^{\perp} \otimes C_2^{\perp}$ where for i=1, 2, $C_i^{\perp}{}'s$ are duals of $C_i{}'s$, respectively.

Proof: It is easy to show that $(C_1 \otimes C_2)^{\perp} = C_1^{\perp} \otimes C_2^{\perp}$. Thus, the result follows from Theorem 4.

Theorem 4.2.10. Let C be a linear code over R_2 and the minimum Lee, Gray, and Euclidean distances of C is denoted by d_L, d_G and d_E, respectively. Then $d_L = \min\{d_L(C_1, d_L(C_2)\}$, $d_G = \min\{d_H(C_1), d_H(C_2)\}$ where C_1, C_2 are $\mathbb{Z}_4$ −linear codes.

Proof: Since ϕ is a distance preserving map, we have

$d_L = d_L\big(\phi(C)\big) = d_L(C_1 \otimes C_2) = \min\{d_L(C_1), d_L(C_2)\}$.

In a similar manner, $d_E = \min\{d_E(C_1), d_E(C_2)\}$ and $d_G = \min\{d_H(C_1), d_H(C_2)\}$.

4.3. ALGEBRAIC PROPERTIES OF THE RING R_3

Let $R_3 = F_4 + vF_4 = \{a + vb | a, b \in F_4\}$ be a commutative ring with $v^2 = v$ and sixteen elements. The ring R_3 is a finite non-chain ring. Any element of R_3 is uniquely expressed as $c = a + vb$, where $a, b \in F_4$. The Gray map $\phi(c) = (a + b, a)$ gives the map from R_3 to $F_4 \times F_4$. R_3 is a finite semi-local Frobenius ring as it is usual to verify that ϕ is a ring isomorphism, which indicates that R_3 is isomorphic to the ring $F_4 \times F_4$. Throughout the section we follow [46].

The ideals of the ring R_3 are

(i) $R_3 = (1) = (w) = (w + 1) = (v + w) = (1 + v + w) = (1 + vw) = (1 + v + vw) = (1 + w + vw) = (v + w + vw)$,

(ii) $(v) = (vw) = \big(v(w + 1)\big) = \{0, v, vw, v(w + 1)\}$,

(iii) $(v + 1) = \big((v + 1)w\big) = \big((v + 1)(w + 1)\big) = \{0, v + 1, (v + 1)w, (v + 1)(w + 1)\}$,

(iv) $(0) = \{0\}$.

Moreover, there are two maximal ideals in the quotient ring R_3: (v) and $(v+1)$. Through the application of the Chinese Remainder Theorem, we obtain $R_3 \cong F_4[v]/(v-1) \oplus F_4[v]/(v) \cong F_4 \oplus F_4 \cong (v) \oplus (1+v)$. So, every element of R_3 can be uniquely rewritten as $a+bv = (a+b)v + a(v+1)$, for some $a, b \in F_4$. $U_4 = \{1, w, w+1, v+w, 1+v+w, 1+vw, 1+v+vw, 1+w+vw, v+w+vw\}$ is the unit group of R_3. The fact that $U_4 \cong Z_3 \times Z_3$ is readily apparent.

The units U_4 have the following subgroups:

(i) $(1) = \{1\}$,

(ii) $(w) = (w+1) = \{1, w, w+1\}$,

(iii) $(v+w) = (v+w+1) = \{1, v+w, v+w+1\}$,

(iv) $(1+vw) = (1+v+vw) = \{1, 1+vw, 1+v+vw\}$,

(v) $(v+w+vw) = (1+w+vw) = \{1, v+w+vw, 1+w+vw\}$.

An R_3 submodule of R_3^n is a linear code C over R_3 of length n.

The Hamming weight of an element a in R_3 is equal to the sum of the Hamming weights of its components such that $w(a) = \sum_{i=1}^{n} w(a_i)$, where $a = (a_1, a_2, \dots, a_n) \in {R_3}^n$. In R_3, the Hamming distance of a and b is defined as $d(a,b) = w(a-b)$. The gray map from $R_3 \; to \; F_4^2$ is defined as

$$\phi: R_3 \longrightarrow F_4^2$$
$$a + vb \longrightarrow (a+b, a).$$

The Hamming weight of an element is its Gray image or $w_L(c) = w_H(\phi(c))$ is the Lee weight of any element in R_3.

Consider two linear codes A and B. The definition of the operations $\oplus$ and $\otimes$ is given by

$A \oplus B = \{a + b | a \in A\, , b \in B\}$,

$A \otimes B = \{(a, b) | a \in A\, , b \in B\}$.

It is easy to see that a generator matrix for a nonzero linear code C over R_3 can be expressed in the following form by permitting coordinate permutations:

$$G = \begin{pmatrix} I_{k_1} & (1+v)B_1 & vA_1 & (1+v)A_2 & (1+v)A_3 + vB_3 \\ 0 & vI_{k_2} & 0 & vA_4 & 0 \\ 0 & 0 & (1+v)I_{k_3} & 0 & (1+v)B_4 \end{pmatrix}.$$

For every $1 \leq i, j \leq 4$, A_i and B_j are the F_4-matrices. Let

$$C_1 = \{x + y \in F_4^n | (x+y)v + x(v+1) \in C\, , for\ some\ x, y \in F_4^n\}$$
$$C_2 = \{x \in F_4^n | (x+y)v + x(v+1) \in C\, , for\ some\ y \in F_4^n\}$$

where $C_1$and $C_2$are linear codes. Consequently, $C = vC_1 \oplus (1+v)C_2$ and $|C| = 16^{k_1}4^{k_2}4^{k_3}$.

Lemma 4.3.1 Let C_i be the $[n, k_i, d(C_i)]$ linear codes for $i = 1,2$ and let $C = (v)C_1 \oplus (1+v)C_2$ be a linear code of length n over R. Therefore, over F_4, $\phi(C)$ is a $[2n\, , k_1 + k_2\, , \min\{d(C_1), d(C_2)\}]$ code.

PART 5

CYCLIC DNA CODES OVER THE FINITE RINGS

In this chapter, we explore the construction and properties of cyclic DNA codes over various finite rings. Our main goal is to analyze new structures and properties of cyclic DNA codes on these rings. During our studies, we observed how these codes can achieve desired features such as error correction capability. We have also included important theories and examples from the literature and presented the relationships between DNA nucleotides and different ring elements in tables. Throughout our study we follow [22,47,48,49].

5.1. CYCLIC DNA CODES OVER THE RING R_1

The nucleotide DNA bases $A, T, C,$ and G correspond exactly to the elements $0, 1, u,$ and $1 + u$ of R_1 such that $0 \longrightarrow A$, $u \longrightarrow T$, $1 \longrightarrow G$ and $1 + u \longrightarrow C$. Assume that $x = x_0 x_1 \dots x_{n-1} \in {R_1}^n$, the reverse, complement and reverse-complement of x are defined as $x^r = x_{n-1} \dots . x_1 x_0$, $x^c = \overline{x_0}\,\overline{x_1} \dots . \overline{x_{n-1}}$ and $x^{rc} = \overline{x_{n-1}} \dots . \overline{x_1}\,\overline{x_0}$, respectively. We followed throughout our study unless otherwise stated [47,48,49].

A code is called a DNA code if it meets some or all of the followings:

(i) For any two distinct codewords $c_1, c_2 \in C, H(c_1, c_2) \geq d$ is the Hamming constraint.

(ii) Reverse constraint: $H(c_1, c_2^r) \geq d$ for any two codewords $c_1, c_2 \in C$.

(iii) Reverse-complement constraint: $H(c_1, c_2^{rc}) \geq d$ for any pair of codewords $c_1, c_2 \in C$.

(iv) The fixed constraint on GC content, there are exactly the same number of G and C elements in any codeword $c \in C$.

Definition 5.1.1. Let C be a cyclic code of length n over R_1. Then C is called

(i) reversible code if $x^r \in C$ for every $x \in C$,

(ii) complement code if $x^c \in C$ for every $x \in C$,

(iii) reversible-complement code if $x^{rc} \in C$ for every $x \in C$.

Lemma 5.1.2. Let $f(x)$ and $g(x)$ be two polynomials in R_1 with $\deg f(x) \geq \deg g(x)$. Then

(i) $[f(x)g(x)]^* = f^*(x)g^*(x)$,

(ii) $[f(x) + g(x)]^* = f^*(x) + x^{\deg f - \deg g} g^*(x)$.

(iii) **Theorem 5.1.3.** Let C be cyclic code in $R_n = R[x]/(x^n - 1)$. Then

(i) If n is odd then R_n is a principal ideal ring and $C = < \big(g(x) + ua(x)\big) >$, where $g(x)$ and $a(x)$ are binary polynomials with $a(x)|g(x)|(x^n - 1)\ (mod\ 2)$.

(ii) If n is not odd then, then one of the followings holds:

(a) C $= <\big(g(x) + up(x)\big)>$ where $g(x)|(x^n - 1)\ (mod\ 2)$ and $\big(g(x) + up(x)\big)|(x^n - 1)$ in R_1 and $g(x)|p(x)\left(\frac{x^n-1}{g(x)}\right)$

(b) C $=<(g(x)+up(x), ua(x))>$ where $g(x), a(x)\ and\ p(x)$ are binary polynomials with $a(x)|g(x)|(x^n-1)\ (mod\ 2)$, $a(x)|p(x)\left(\frac{x^n-1}{g(x)}\right)$ and $\deg a(x) > \deg p(x)$.

Lemma 5.1.4. Let $C =< f(x) >$ be a cyclic code over $\mathbb{F}_2$. Then C is reversible if and only if $f(x)$ is a self-reciprocal polynomial.

Theorem 5.1.5. Let $C =< g(x)+up(x) >$ be a cyclic code of even-length over R_1, Then C is reversible code if and only if

(i) $g(x)$ is a self -reciprocal polynomial,

(ii) one of the followings holds:

(a) $x^i p^*(x) = p(x)$,

(b) $g(x) = x^i p^* + p(x)$, where $i = \deg\big(g(x)\big) - \deg\big(p(x)\big)$.

Theorem 5.1.6. Let $C = \big(g(x)+up(x), ua(x)\big)$ be a cyclic code of length n over R_1 with $(x)\left|g(x)\right|(x^n-1)$, $a(x)\left|p(x)\left(\frac{x^n-1}{g(x)}\right)\right.$ $\deg a(x) > \deg p(x)$. Then C is a reversible code if and only if

(i) $g(x)$ and $a(x)$ are self-reciprocal polynomials,

(ii) $a(x)\ \left|\left(x^i p^*(x) + p(x)\right)\right.$, where $i = \deg\big(g(x)\big) - \deg\big(p(x)\big)$.

Lemma 5.1.7. Let c in R_1, then $c + \bar{c} = u$.

Lemma 5.1.8. If a, b are in R_1, then $\overline{a+b} = \bar{a} + \bar{b} + u$.

Lemma 5.1.9. If $c \in \mathbb{F}_2$, then $u + \overline{uc} = uc$.

Theorem 5.1.10. Let $C = \big(g(x) + up(x)\big)$ be a cyclic code of even length n over R_1. Then C is a reverse-complement code if and only if

(i) $g(x)$ is self-reciprocal and $u((1-x^n)/(1-x)) \in C$,

(ii) one of the followings holds:

(a) $x^i p^*(x) = p(x)$.

(b) $g(x) = x^i p^*(x) + p(x)$, where $i = \deg\big(g(x)\big) - \deg\big(p(x)\big)$.

Example 5.1.1. Let $x^{10} - 1 = (x+1)^2(x^4 + x^3 + x^2 + x + 1)^2 \in \mathbb{F}_2[x]$.

Assume that $C =< g(x) + up(x) >$ and that g(x)=$g_1 g_2^2$ and $p(x) = g_2^2$. Let $g_1 = (x+1)$ and $g_2 = (x^4 + x^3 + x^2 + x + 1)$. Verifying $g(x) = x^i p^*(x) + p(x)$, where $i = \deg g(x) - \deg p(x)$ is a simple process. C is a ten-length cyclic DNA code with a minimum Hamming distance of ten. There are four codewords:

$$AAAAAAAAAA\ TTTTTTTTTT\ CGCGCGCGCG\ GCGCGCGCGC$$

5.2. CYCLIC DNA CODES OVER THE RING R_2

We follow [50,51] throughout our study unless otherwise stated.

Lemma 5.2.1. If $C = \langle f(x) \rangle$ is a cyclic code over $\mathbb{Z}_4$, then $f(x)$ is a self-reciprocal polynomial if and only if C is a reversible code.

Lemma 5.2.2. Let C be a cyclic code of length n over $\mathbb{Z}_4$, then $C = \langle f(x)[h(x) + 2] \rangle$ where $x^n - 1 = f(x)g(x)h(x)$ in $\mathbb{Z}_4[x]$ and the polynomials $f(x), g(x), h(x)$ are pairwise coprime. Also, $|C| = 2^{2\deg(g(x)) + \deg(h(x))}$.

Table 5.1. [22] Relation Between elements of the Ring R_2 and DNA Nucleotides

Elements x of R_2	**Gray images ρ**	**DNA pairs $\phi(x)$**
0	(0,0)	AA
1	(1,1)	TT
2	(2,2)	GG
3	(3,3)	CC
$\boldsymbol{v}$	(0,1)	AT
$\boldsymbol{2v}$	(0,2)	AG
$\boldsymbol{3v}$	(0,3)	AC
$\boldsymbol{1+v}$	(1,2)	TG
$\boldsymbol{1+2v}$	(1,3)	TC
$\boldsymbol{1+3v}$	(1,0)	TA
$\boldsymbol{2+v}$	(2,3)	GC
$\boldsymbol{2+2v}$	(2,0)	GA
$\boldsymbol{2+3v}$	(2,1)	GT
$\boldsymbol{3+v}$	(3,0)	CA
$\boldsymbol{3+2v}$	(3,1)	CT
$\boldsymbol{3+3v}$	(3,2)	CG

Definition 5.2.3 Given a codeword $a \in D$ with $a = (a_0, a_1, \dots, a_{n-1}) \in {R_2}^n$ and D code over R_2 of length n, we build a map as follows using Table 5.2.1,

$$\phi: D \longrightarrow M^n$$

$$(a_0, a_1, \dots, a_{n-1}) \longmapsto \big(\phi(a_0), \phi(a_1), \dots., \phi(a_{n-1})\big).$$

Four fundamental nucleotides $A, T, G \text{ and } C$ combine to 16 codons such as $M = \{AA, AT, AC, AG, TT, TA, TG, TC, CC, CG, GT, CA, CT, GG, GC, GA\}$. The elements of R_2 and the 16 codons over the alphabet D listed in Table 5.2.1 correspond exactly to one another. The complement of Watson-Crick is satisfied by the codons. The idea of

the Watson-Crick complement is naturally extended to the codon elements so that $(AA)^c = TT, \dots, (GA)^c = CT$ and so on.

If $\phi(b) = \phi(a)^c$, the complement $a \in R_2$ is defined as $a^c = b$. Consequently, for any $a, b \in R_2$, $a^c + a = 1$ and $(a+b)^c = a^c + b^c + 3$.

Definition 5.2.4 Assume that C is a linear code of length n over R_2.

(i) If $\phi(a)^r \in \phi(C)$ for all a$\in C$, then C or equivalently $\phi(C)$ is called a reversible DNA code.

(ii) If $\phi(a)^{rc} \in \phi(C)$ for all a$\in C$, then C or equivalently $\phi(C)$ is called a reversible-complement DNA code.

Lemma5.2.5. Let $C = vC_1 \oplus (1-v)C_2$ be a linear code over R_2. Then C_1 and C_2 are both cyclic codes over $\mathbb{Z}_4$ if and only if C is a cyclic code. Moreover,

$$C = \langle vf_1(x)g_1(x) + (1-v)f_2(x)g_2(x), 2vf_1(x)g_1(x) + 2(1-v)f_2(x)g_2(x)\rangle$$

where $C_1 = \langle f_1(x)g_1(x), 2f_1(x)h_1(x)\rangle$ and $C_2 = \langle f_2(x)g_2(x), 2f_2(x)h_2(x)\rangle$ over $\mathbb{Z}_4$ and $x^n - 1 = f_1(x)g_1(x)h_1(x) = f_2(x)g_2(x)h_2(x)$.

Theorem 5.2.6. Let $C = vC_1 \oplus (1-v)C_2$ be a linear code over R_2. Then

$$C = \langle vf_1(x)(h_1(x)+2) + (1-v)f_2(x)(h_2(x)+2)\rangle$$

where $x^n - 1 = f_1(x)g_1(x)h_1(x) = f_2(x)g_2(x)h_2(x)$and $C_1 = \langle f_1(x)(h_1(x)+2)\rangle$ and $C_2 = \langle f_2(x)(h_2(x)+2)\rangle$ over $\mathbb{Z}_4$. Moreover $|C| = 2^{2\deg(g_1(x))+\deg(h_1(x))+2\deg(g_2(x))+\deg(h_2(x))}$.

Lemma 5.2.7. Let $(a_0 + vb_0, \dots, a_{n-1} + vb_{n-1}) \in R^n$. Then

$$\big(\phi(a_0 + vb_0, \dots, a_{n-1} + vb_{n-1})\big)^r = \big(\phi(a_{n-1} + (1+3v)b_{n-1}), \dots, \phi(a_0 + (1+3v)b_0)\big).$$

Theorem 5.2.8 Let $g_1(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ be a self-reciprocal polynomial in $\mathbb{Z}_4[x]$. If $C = \langle vg_1(\mathrm{x}) + (1 - \mathrm{v})g_1(\mathrm{x}) \rangle$ is a cyclic code of odd length of n with minimum distance d and size K, then

(i) for the alphabet $\{A, T, G, C\}$ }, $\phi(C)$ yields a reversible DNA code of length $2n$, size K and minimum distance code of at least d,

(ii) if $r(x) = 1 + x + x^2 + \cdots + x^{n-1} \in C$, then $\phi(C)$ is a reversible-complement DNA code of length $2n$. size K with a minimum distance code of at least d over the alphabet $\{A, T, G, C\}$,

5.3. CYCLIC DNA CODES OVER THE RING R_3

We followed [7] throughout our study unless otherwise stated.

Theorem 5.3.1. Let$2 \leq \ell$ be an even integer and that $g_1(x)$ and $g_2(x)$ self-reciprocal polynomials with degrees t_1 and t_2, respectively and dividing $x^n - 1$ over F_4. Then

(i) $g(x) = vg_1(x) + (v + 1)g_2(x)$, $|\langle E(g)\rangle| = 16^{\ell}$ and $|\langle E(g)\rangle| = 4^{\ell}$ if $\deg g_1(x) = \deg g_2(x)$ or one of $g_1(x)$ or $g_2(x)$ is equal to zero.

(ii) $g(x) = vg_1(x) + (v + 1)x^{s/2}g_2(x)$ for $\deg g_1(x) > \deg g_2(x)$, $g(x) = vx^{s/2}g_1(x) + (v + 1)g_2(x)$ for $\deg g_1(x) < \deg g_2(x)$ and $|\langle E(g)\rangle| = 16^{\ell}$ if $\deg g_1(x) \neq \deg g_2(x)$ and $2 \leq s = |t_1 - t_2|$ is even.

Table 5.2 [7] Relation Between elements of the Ring R_3 and DNA Nucleotides

Elements a	**Gray images**	**DNA double pairs $\xi(a)$**
$\mathbf{0}$	$(0,0)$	AA
$\mathbf{1}$	$(1,1)$	TT
$\boldsymbol{w}$	(w,w)	CC
$\mathbf{1}+\boldsymbol{w}$	$(1+w,1+w)$	GG
$\boldsymbol{v}$	$(1,0)$	TA
$\mathbf{1}+\boldsymbol{v}$	$(0,1)$	AT
$\boldsymbol{v}+\boldsymbol{w}$	$(1+w,w)$	GC
$\mathbf{1}+\boldsymbol{v}+\boldsymbol{w}$	$(w,1+w)$	CG
$\boldsymbol{vw}$	$(w,0)$	CA
$\mathbf{1}+\boldsymbol{vw}$	$(1+w,1)$	GT
$\boldsymbol{w}+\boldsymbol{vw}$	$(0,w)$	AC
$\mathbf{1}+\boldsymbol{w}+\boldsymbol{vw}$	$(1,1+w)$	TG
$\boldsymbol{v}+\boldsymbol{vw}$	$(1+w,0)$	GA
$\mathbf{1}+\boldsymbol{v}+\boldsymbol{vw}$	$(w,1)$	CT
$\boldsymbol{w}+\boldsymbol{v}+\boldsymbol{vw}$	$(1,w)$	TC
$\mathbf{1}+\boldsymbol{w}+\boldsymbol{v}+\boldsymbol{vw}$	$(0,1+w)$	AG

Let $\Theta(c): C \longrightarrow S_{D_4}^{2n}$ be a map defined as $(c_0, c_1, \dots, c_{n-1}) \mapsto \big(\xi(c_0)\xi(c_1)\dots\xi(c_{n-1})\big)$

For example, $\big(\xi(1)\xi(v)\xi(w)\xi(v+w)\big) = (TTTACCGC)$ is defined as $(c_0, c_1, c_2, c_3) = (1, v, w, w+v)$.

Definition 5.3.2. Let $g_1(x)$and $g_2(x)$ be polynomials that divide $x^n - 1$ over F_4 and have $\deg g_1(x) = t_1$ and $\deg g_1(x) = t_2$. Suppose that $g(x) = vg_1(x) + (v+1)g_2(x)$ over R and $\ell = \min\{n - t_1, n - t_2\}$. $E(g)$ is called a $\psi - set$ and described as

$$E(g) = \{E_0, E_1, \dots, E_{\ell-1}\}$$

where

$$E_i = \begin{cases} x^i g(x) & if\ i\ is\ even \\ x^i \psi(g(x)) & if\ i\ is\ odd\ . \end{cases}$$

The linear code C over R generated by $E(g)$. Denoted by $C = \langle g(x) \rangle \psi$. $\langle E(g) \rangle$ or $\langle g(x) \rangle \psi$ represents R-module generated by $E(g)$.

PART 6

CONCLUSION

In this thesis, we have explored the construction of cyclic DNA codes over finite rings, focusing on the algebraic properties and implications of these structures. Through detailed analysis and theoretical development, we have demonstrated how different finite rings, such as $F_2 + uF_2$ with $u^2 = 0$, $Z_4 + vZ_4$ with $v^2 = v$ and $F_4 + vF_4$ with $v^2 = v$ can be utilized to generate cyclic DNA codes with desirable properties for various applications in bioinformatics and coding theory.

Our study has shown that the interplay between ring theory and coding theory provides a rich framework for constructing DNA codes with specific characteristics, such as error correction capabilities and efficient encoding/decoding processes. By leveraging the unique properties of finite rings, we can design codes that are not only mathematically robust but also practically relevant for the storage and transmission of genetic information.

The theoretical results presented in this thesis, which include important theorems and structures existing in the literature, contribute to the broader understanding of cyclic DNA codes and their potential applications. Future research can build on these foundations, exploring new types of rings and their corresponding codes, as well as practical implementations in genetic engineering and data storage technologies.

In conclusion, the integration of finite ring theory into the study of cyclic DNA codes opens up new avenues for research and application, highlighting the importance of mathematical approaches in advancing the field of bioinformatics.

REFERENCES

[1] Hammons, A.R., Kumar, Jr.P.V., Calderbank, J.A., Sloane, N.J.A., Sole, p. "The Z_4- linearity of Kerdock, Preparata, Goethals, and related codes", IEEE Trans. Inf. Theory. 40, 301-319, (1994).

[2] Dinh, H., Lo´pez-Permouth, S.R., "Cyclic and negacyclic codes over finite chain rings", IEEE Trans. Inf. Theory. 50(8), 1728-1744, (2000).

[3] Yildiz, B., Karadeniz, S." Linear codes over F_2 + uF_2 + vF_2 + uvF_2. Des", Codes Cryptor. 54, 61-81 (2010).

[4] Bayram, A., Siap, I. "Cyclic and constacyclic codes over a non-chain ring", J. Algebra Comb. Discret. Struct. Appl. 1, 1-13 (2014).

[5] Zhu S., Wang L. "A class of constacyclic codes over F_p + vF_p and its Gray image", Discret. Math. Theory. 311(23), 2677-2682 (2011).

[6] Zhu S., Wang Y., Shi M. "Some result on cyclic codes over $F_2 + vF_2$", IEEE Trans. Inf. Theory. 56, 1680-1684 (2010).

[7] Aysegul Bayram[1] · Elif Segah Oztas[1] · Irfan Siap[1] Des. "Codes over F_4 + v F_4 and some DNA applications", Codes Cryptogr. 80:379–393 DOI 10.1007/s10623-015-0100-8, (2016).

[8] Gaborit, P.; King, O.D. "Linear construction for DNA codes", *Theory. Comput. Sci.*, *334*, 99–113, (2005).

[9] Abualrub, T.; Ghrayeb, A.; Zeng, X.N. "Construction of cyclic codes over *GF* (4) for DNA computing", *J. Frankl. Inst. 343*, 448–457, (2006).

[10] Siap, I.; Abualrub, T.; Ghrayeb, A. "Cyclic DNA codes over the ring $F_2[u]/\langle u^2 - 1\rangle$ based on deletion distance", *J. Frankl. Inst. 346*, 731–740, (2009).

[11] Guenda, K.; Gulliver, T.A. "Construction of cyclic codes over F_2 + *u*F_2 for DNA computing", *Appl. Algebra Engrg. Comm. Comput. 24*, 445–459,(2013).

[12] Liang, J.; Wang, L. "On cyclic DNA codes over F_2 + *u*F_2", *J. Appl. Math. Comput.51*, 81–91, (2016).

[13] Yildiz, B.; Siap, I. "Cyclic DNA codes over the ring $F_2[u]/\langle u^4 - 1\rangle$ and applications to DNA codes", *Comput. Math. Appl. 63*, 1169–1176, (2012).

[14] Bayram, A.; Oztas, E.; Siap, I. “Codes over $F_4 + vF_4$ and some DNA applications”, *Des. Codes Cryptogr. 80*, 379–393, (2016).

[15] Zhu, S.; Chen, X. “Cyclic DNA codes over $F_2 + uF_2 + vF_2 + uvF_2$”, *J. Appl. Math. Comput. 55*, 479–493, (2015).

[16] Oztas, E.S.; Siap, I. “Lifted polynomials over F_{16} and their applications to DNA codes”, *Filomat .27*, 459–466, (2013).

[17] Bennenni, N.; Guenda, K.; Mesnager, S. “DNA cyclic codes over rings”, *Adv. Math. Commun., 11*, 83–98, (2017).

[18] Dinh, H.Q.; Singh, A.K.; Pattanayak, S.; Sriboonchitta, S. “DNA cyclic codes over the ring $F_2[u,v]/\langle u^2 - 1, v^3 - v, uv - vu\rangle$”, *Int.J.Biomath.11*,1–19 ,(2018).

[19] Dinh, H.Q.; Singh, A.K.; Pattanayak, S.; Sriboonchitta, S. “Cyclic DNA codes over the ring $F_2 + uF_2 + vF_2 + uvF_2 + v^2F_2 + uv^2F_2$”, *Des. Codes Cryptogr. 86*, 1451–1467, (2018).

[20] Dinh, H.Q.; Singh, A.K.; Pattanayak, S.; Sriboonchitta, S. “Construction of cyclic DNA codes over the ring $Z_4[u]/\langle u^2-1\rangle$basedonthedeletiondistance”, *Theor.Comput.Sci.773*,27–42, (2019).

[21] Liu, J.; Liu, H. “DNA codes over the ring $F_4[u]/\langle u^3\rangle$”, *IEEE Access. 8*, 77528–77534, (2020).

[22] Liu, J.; Liu, H. “Construction of cyclic DNA codes over the ring $Z_4 + vZ_4$”, *IEEE Access, 8*, 111200–111207, (2020).

[23] Abualrub T, Siap I. “Cyclic codes over the rings $Z2 + uZ2$ and $Z2 + uZ2 + u^2Z2$”, Design Code Cryptogr, 42: 271-287, (2007).

[24] Al-Ashker M, Chen J. “Cyclic codes of arbitrary length over $Fq + uFq + ... + u^{k-1}Fq$”, Palestine J Math. 2: 72-80, (2013).

[25] Bonnecaze A, Udaya P. “Cyclic codes and self dual codes over $F2 +uF2$” . IEEE T Inform Theory . 45: 1250-1255, (1999).

[26] L. M. Adleman.“Molecular computation of solutions to combinatorial problems”, Science 266 1021–1024, (1994).

[27] Hill R.“A first course in coding theory”, Clarendon Press, Oxford, (1986).

[28] Karakaş, H. İ.“Cebir Dersleri”, Ankara: Tüba Yayınları , (2012).

[29] Hungerford, T. “Algebra”, New York: Springer-Verlag, (1973).

[30] Çallıalp, F. “Örneklerle Soyut Cebir”, İstanbul: Birsen yayinevi , (2013).

[31] Jitman, S., Udomkavanich, P. ve Ling, S. “Skew Constacyclic Codes over Finite Chain Rings, Advances Mathematics Communications”, 6, 29-63, (2012).

[32] ÇALLIALP, F. “Cebir”, Sakarya Üniversitesi Yay. No:16, Sakarya, (1995).

[33] MONTGOMERY, H.L., NIVEN, I., ZUCKERMAN, H.S. “An Introduction to the Theory of Numbers”, Wiley, (1991).

[34] ROMAN, S. “Coding and Information Theory”, Graduate Texts in Mathematics, Springer Verlag, (1992).

[35] Huffman, W.C., Cary, W. ve pless, V.(2003).”Fundamentals of Error-Correcting Codes”, Cambridge: Cambridge University Press, (2003).

[36] Ling, S. ve Xing, C. “Coding Theory a First Course”, New York: Cambridge University Press, (2004).

[37] B. Pashaei Rad, H.R. Maimani and A. Tehranian “on the complementary dual code over $\mathbb{F}_2 + u\mathbb{F}_2$”, Italian Journal of Pure and Applied Mathematics -N.45- (317-322), (2021).

[38] C. Bachoc. “Application of coding theory to the construction of modular lattices”, J. Combin. Theory Ser. A, 78 ,92-119, (1997).

[39] A. Bonnecaze and U. Parampalli. “Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$”, IEEE Trans. Inform. Theory, 45 ,1250-1255, (1999).

[40] S.T. Dougherty, Gaborit, P. Harada and M. “Sole Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$”, IEEE Trans. Inform. Theory, 45, 32-45, (1999).

[41] S.T. Dougherty, J.L. Kim, H. Kulosman and H. Liu. “self-dual codes over commutative frobenius ring”, Finite Fields Appl. 16 ,14-26, (2010).

[42] J.L Massey. ” Linear codes with complementary duals”, Discrete Math., 106/107, 337-342, (1992).

[43] Z. Xian Wan.“Quaternary codes”, Word Scientific Publishing Co. Pte. Ltd (series on applied mathematics; v.8), (1997).

[44] B. Yildiz and S. Karadeniz. “Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$”, Mac Williams identities, projections, and formally self-dual codes, Finite Fields Appl., 27, pp. 24-40, (2014).

[45] J. Wood. “Duality for modules over finite rings and applications to coding theory”, Amer. J. Math., 121, 555-575, (1999).

[46] Gursoy F., Siap I., Yildiz B. “Construction of skew cyclic codes over $F_q + vF_q$”. Adv. Math. Commun. 8,313-322 (2014).

[47] Abualrub, T., Siap, I. “Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$” . Des. Codes Cryyptogr. 42, 273-287 (2007).

[48] Guenda, K., Aaron Gulliver, T. “Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ for DNA computing”, AAECC 24(6), 445-459 (2013).

[49] Massey, J.L. “Reversible codes”, Inf. Control 7(3), 369-380 (1964).

[50] J. Gao, F. Fu, Y. Gao. “Some classes of linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and their applications to construct good and new $\mathbb{Z}_4$-linear codes”, Appl. Algebra Engyg. Comm. Comput, 28,131-153, (2017).

[51] Z. Wan. “Quaternary codes”, World Scientific Pub Co Inc, (1997).

RESUME

Theyyazin Mamdooh Yousif YOUSIF started studying mathematic at Tikrit University (Iraq) in 2016 and graduated by 2020. then, in 2021, he started the graduate program at Karabük Universjty (Türkiye) department of mathematics to get his master degree. his research intersts about DNA codes and finite rings.