

**DOUBLE CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$
AND ITS APPLICATION TO DNA CODES**



**A Thesis Submitted to the Graduate School of Naresuan University
in Partial Fulfillment of the Requirements
for the Doctor of Philosophy Degree in Mathematics
December 2024
Copyright 2024 by Naresuan University**

This thesis entitled “Double cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$
and its application to DNA codes”

by Arunothai Kanlaya

has been approved by the Graduate School as partial fulfillment of the
requirements for the Doctor of Philosophy Degree in Mathematics of
Naresuan University

Oral Defense Committee

..... *Manoj Siripitukdet* Chair
(Professor Manoj Siripitukdet, Ph.D.)

..... *Chakkrid Klin-eam* Advisor
(Associate Professor Chakkrid Klin-eam, Ph.D.)

..... *S. J. Itman* External Examiner
(Associate Professor Somphong Jitman, Ph.D.)

..... *N2* Internal Examiner
(Associate Professor Kijti Rodtes, Ph.D.)

..... *Ekkachai Laysirikul* Internal Examiner
(Assistant Professor Ekkachai Laysirikul, Ph.D.)

Approved

..... *Krongkarn Chootip*
(Associate Professor Krongkarn Chootip, Ph.D.)

Dean of the Graduate School

- 9 DEC 2024

ACKNOWLEDGEMENT

First and foremost, I am extremely grateful to my advisor, Associate Professor Chakkrid Klin-eam, for his invaluable advice, continuous support, and patience during my Ph.D. studies. His constant guidance and feedback helped me throughout the entire research and thesis writing process.

Furthermore, I would like to thank my thesis committees, Professor Manoj Siripitukdet, Associate Professor Somphong Jitman, Associate Professor Kijti Rodtes and Assistant Professor Ekkachai Laysirikul for their interest in my work and their valuable comments and suggestions.

I would like to extend my sincere thanks to the Royal Golden Jubilee (RGJ) Ph.D. Programme for their support in financing my doctoral studies and research at Universitat Autònoma de Barcelona, Barcelona, Spain. Additionally, I would like to thank the Department of Mathematics, Faculty of Science, Naresuan University for facilitating places and others that are useful to support this thesis.

Finally, I would like to express my heartfelt gratitude to my parents, professors, and friends for their unwavering encouragement and support throughout my studies. Whether in times of joy or difficulty, they have always been by my side, and their kindness has made my journey at university both enriching and wonderful. In addition, I would also like to take a moment to acknowledge myself for the determination, perseverance, and hard work that I have put into completing this thesis.

Arunothai Kanlaya

Title DOUBLE CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$
AND ITS APPLICATION TO DNA CODES

Author Arunothai Kanlaya

Advisor Associate Professor Chakkrid Klin-eam, Ph.D.

Academic Paper Ph.D. Dissertation in Mathematics,
Naresuan University, 2024.

Keywords Cyclic codes, Double cyclic codes, Reversible codes,
Reversible-Complement codes, DNA codes.

ABSTRACT

This thesis investigates the algebraic structure of double cyclic codes of length (α, β) over the finite commutative chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and examines related theories for generating DNA codes from these codes. The study of the algebraic structure of double cyclic codes is divided into 2 parts, based on the types of lengths α and β , as follows:

1. α and β are both odd positive integers.
2. α is an odd positive integer and β is an even positive integer.

Additionally, the theory for these codes for application to DNA codes is also divided into 2 parts, corresponding to their algebraic structures.

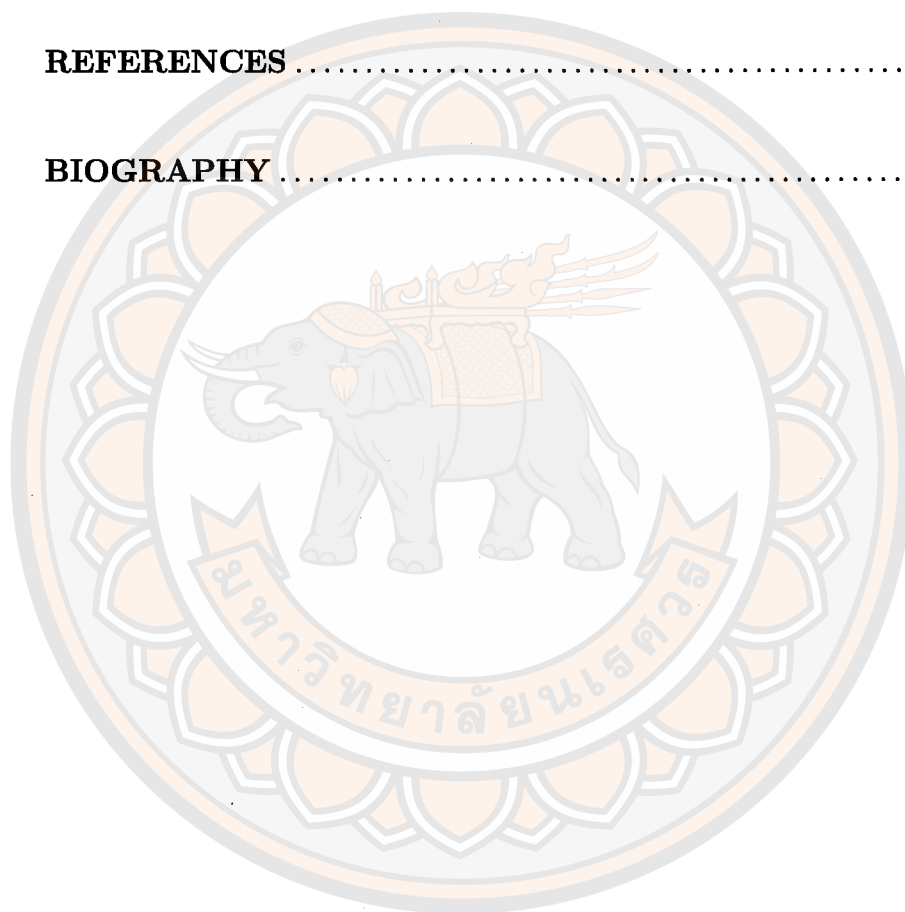
Furthermore, we introduce key notations relevant to DNA codes for double cyclic codes, such as reversibility, complementarity, and reversible-complementarity, and investigate the necessary and sufficient conditions for double cyclic codes to be suitable for DNA coding. Finally, we present the process for generating DNA codes based on our results, accompanied by illustrative examples.

LIST OF CONTENTS

Chapter	Page
I INTRODUCTION	1
II PRELIMINARIES	7
Rings and Fields	7
Polynomial rings	15
Modules	23
Basic Concept of Coding Theory	26
Double cyclic codes	33
DNA codes	35
III DOUBLE CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$	42
Double cyclic codes of length (α, β) over $\mathbb{F}_2 + u\mathbb{F}_2$	42
The case α and β are both odd positive integers	46
The case α is an odd and β is an even positive integer	54
IV CONSTRUCTING DOUBLE CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$ FOR DNA CODES	60
Basic concept for lengths α and β	60
Reversible codes	63
Reversible-complement codes	69
The case α and β are both odd positive integers	71
Reversible codes	71
Reversible-complement codes	83
The case α is an odd and β is an even positive integer	85
Reversible codes	85
Reversible-complement codes	103

LIST OF CONTENTS (CONT.)

Chapter	Page
V CONCLUSION.....	105
APPENDIX.....	110
REFERENCES	125
BIOGRAPHY	130



LIST OF TABLES

Table		Page
1	Addition and Multiplication tables for the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$	2
2	Codewords from the cyclic code $\mathcal{C}_1$ in Example 2.4.14	32
3	Codewords from the cyclic code $\mathcal{C}_2$ in Example 2.4.14	32
4	A DNA code $\mathcal{D}$ of length 9 from $\mathcal{C}$ in Example 2.4.26	39
5	A DNA code $\mathcal{D}_1$ of length 6 from $\mathcal{C}_1$ in Example 2.4.27	40
6	A DNA code $\mathcal{D}_2$ of length 6 from $\mathcal{C}_2$ in Example 2.4.27	40
7	The structure of double cyclic codes of length (α, β) over R ..	105
8	The properties of polynomials $l(x)$, $l_1(x)$ and $l_2(x)$ derived from the structures of double cyclic code $\mathcal{C}$ in Table 7 ...	106
9	The conditions for a double cyclic code $\mathcal{C}$ suit for DNA codes	107
10	The conditions for a double cyclic code $\mathcal{C}$ type 1 suit for DNA codes	108
11	The conditions for a double cyclic code $\mathcal{C}$ type 2 suit for DNA codes	109
12	Codewords from double cyclic code $\mathcal{C}_1$ of length $(3, 5)$ in Example 3.2.8	111
13	Codewords from double cyclic code $\mathcal{C}_2$ of length $(3, 5)$ in Example 3.2.8	113
14	Codewords from double cyclic code $\mathcal{C}_1$ of length $(3, 3)$ in Example 3.2.9	114
15	Codewords from double cyclic code $\mathcal{C}_2$ of length $(3, 3)$ in Example 3.2.9	115
16	Codewords from double cyclic code $\mathcal{C}_1$ of length $(3, 6)$ in Example 3.3.4	116
17	Codewords from double cyclic code $\mathcal{C}_2$ of length $(3, 6)$ in Example 3.3.4	117
18	Codewords from double cyclic code $\mathcal{C}$ of length $(3, 3)$ in Example 4.2.7	119

LIST OF TABLES (CONT.)

Table		Page
19	Codewords from double cyclic code $\mathcal{C}$ of length $(3, 9)$ in Example 4.2.8	120
20	DNA code $\mathcal{D}$ of length 12 obtained from $\mathcal{C} \cup \hat{\mathcal{C}}$ in Example 4.2.12	121
21	Codewords from double cyclic code $\mathcal{C}$ of length $(3, 6)$ in Example 4.3.10	122
22	Codewords from double cyclic code $\mathcal{C}$ of length $(3, 6)$ in Example 4.3.11	123
23	DNA code $\mathcal{D}$ of length 9 obtained from $\mathcal{C} \cup \hat{\mathcal{C}}$ in Example 4.3.14	124
24	DNA code $\mathcal{D}$ of length 9 obtained from $\mathcal{C} \cup \hat{\mathcal{C}}$ in Example 4.3.15	124

LIST OF FIGURES

Figure		Page
1	A simple communication model	1
2	Complementarity of strands in the DNA double helix. The complementary and opposite DNA strands follow the Watson-Crick complement rules. They also differ in sequence when each chain is read in the 5' → 3' direction	4
3	The structure of DNA double helix in simple form	4
4	DNA hybridization diagram. (a.) When two DNA strands hybridize perfectly. (b.) When two mismatched DNA strands hybridize.	5
5	Lattice of ideals of $\mathbb{Z}_{p^n}$	13
6	A paring of two DNA strands in Example 2.4.19	35

CHAPTER I

INTRODUCTION

Information media, such as communication systems and data storage devices, have a fundamental issue: interference during communication or storage reduces data dependability. One of the aims of coding theory is to detect or correct errors. Coding theory is usually divided into two categories: source coding and channel coding. Source coding is the process of transforming a message source into a code suitable for transmission through a channel. Channel coding is referred to as algebraic coding since it is studied with algebraic tools. The purpose of channel coding is to create encoders and decoders that can detect and correct errors during data transmission. In situations where the code is unable to correct an error, it is essential that the system at least notifies the user of the error occurrence. In addition, Figure 1 illustrates a basic model of communication with noise in a channel.

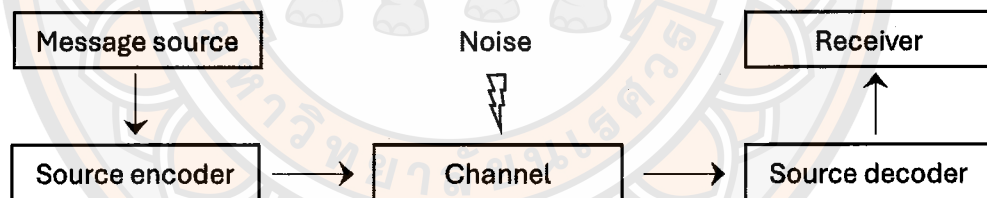


Figure 1 A simple communication model

Research on algebraic coding began with Shannon's work [1], who proposed that proper encoding can reduce errors occurring during the transmission of information through a communication channel. His contributions sparked significant interest in error detection and correction codes. Linear codes, a type of these codes, are used to detect and correct transmission errors. In [2], the authors developed linear codes and established a new type of linear code called cyclic codes. The study of cyclic codes has been continuously expanded and developed, leading to the development of well-known codes such as BCH codes and Reed-Solomon codes. [3–5]. Furthermore, these codes have been employed in satellite communications and digital data storage devices such as CDs, DVDs, Blu-ray discs and

QR codes. The study of algebraic structure of cyclic codes has been explored in various alphabets, including finite fields and finite rings [6–8]. Among the studies of cyclic codes over finite rings, this thesis focuses on the ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$. The ring $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}$ shared some properties of both finite field $\mathbb{F}_4$ and finite ring $\mathbb{Z}_4$. That is, the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with addition and multiplication tables correspond to $\mathbb{F}_4$ and $\mathbb{Z}_4$, respectively. The multiplication table coincides with that of $\mathbb{Z}_4$, when u and $1 + u$ are replaced by, respectively, 2 and 3. In this sense, the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is analogous to $\mathbb{Z}_4$ and u plays the role of 2. However, the addition table is different. The addition table is similar to that of the finite field $\mathbb{F}_4 = \{0, 1, \beta, \beta^2 = \beta + 1\}$, when u and $1 + u$ are replaced, respectively, by β^2 and β . The addition and multiplication tables for the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is given by Table 1.

Table 1 Addition and Multiplication tables for the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$

+	0	1	u	$1 + u$	*	0	1	u	$1 + u$
0	0	1	u	$1 + u$	0	0	0	0	0
1	1	0	$1 + u$	u	1	0	1	u	$1 + u$
u	u	$1 + u$	0	1	u	0	u	0	u
$1 + u$	$1 + u$	u	1	0	$1 + u$	0	$1 + u$	u	1

The algebraic structure of cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ was first investigated in [9], with a focus on codes of odd length. Later, the algebraic structures of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of both odd and even lengths were explored in [10]. However, as in prior studies, the focus remains on algebraic structures and specific properties using a single alphabet in both finite fields and finite rings.

Recently, a new type of error detection and correction codes was established, which is a generalization of binary linear codes and quaternary linear codes. This type of codes is called $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes [11, 12]. These codes are defined as a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta = \{(a; b) : a \in \mathbb{Z}_2^\alpha, b \in \mathbb{Z}_4^\beta\}$, where α is a positive integer and β is an odd positive integer; that is, the set of coordinates is parti-

tioned into two subsets, one of $\mathbb{Z}_2$ coordinates and the other of $\mathbb{Z}_4$ coordinates. Obvious that if $\alpha = 0$, $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes are linear codes over $\mathbb{Z}_4$ and if $\beta = 0$, then these codes are linear codes over $\mathbb{Z}_2$. In [13], the authors defined the simultaneous cyclic shift of subsets of coordinates of a codeword. They investigated $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes and identified these codes as $\mathbb{Z}_4[x]$ -modules of a certain group. Since then, these codes have been explored and developed, with an emphasis on the algebraic structure of the codes and their applications [14–20]. These codes are called cyclic codes over mixed alphabets since they require more than two sets of alphabets.

Shortly after, in [21], the author developed cyclic codes over mixed alphabets by employing a single alphabet while maintaining the concept of cyclic codes over mixed alphabets. These developed codes are known as double cyclic codes. The initial idea and research of double cyclic codes are investigated using the alphabet from $\mathbb{Z}_2$. They showed that double cyclic codes of length (α, β) over $\mathbb{Z}_2$ can be viewed as a submodule of the $\mathbb{Z}_2[x]$ -module $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^\beta - 1 \rangle}$, where α and β are positive integers. Furthermore, the polynomial representation of these codes and their duals were provided. Following this approach, the algebraic structure of these codes was examined, and the alphabet set was broadened to finite fields and finite rings [22–28]. Consequently, this inspired the study of double cyclic codes over the finite ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$, expanding knowledge of algebraic structures with direct applications to DNA codes.

DNA computing is a combination of computer science, chemical biology, and mathematics. The concept of DNA computing was first introduced in [29], where the author successfully used DNA molecules to solve the Hamiltonian path problem. This achievement demonstrated the potential of DNA as a computational tool by utilizing its chemical properties to arrange and match information. Since then, DNA computing has been applied in various fields, including DNA data storage, where its ability to store information at the molecular level has made it a promising solution for digital data storage [30–32]. DNA or Deoxyribonucleic acid is a linear molecule consisting of four different nucleotide bases: Adenine (*A*), Thymine (*T*), Guanine (*G*) and Cytosine (*C*). DNA has a double helix structure, consisting of two long strands twisting around each other. The Watson-Crick complement rule (WCC) states that the two DNA strands are bound together by

chemical connections between the bases, i.e. *A* bonds with *T* and *C* bonds with *G*. Furthermore, each strand of DNA has an ordered quaternary sequence of the letters *A*, *T*, *G* and *C*, with two different ends known as the 5' and 3' ends, as shown in Figure 2.

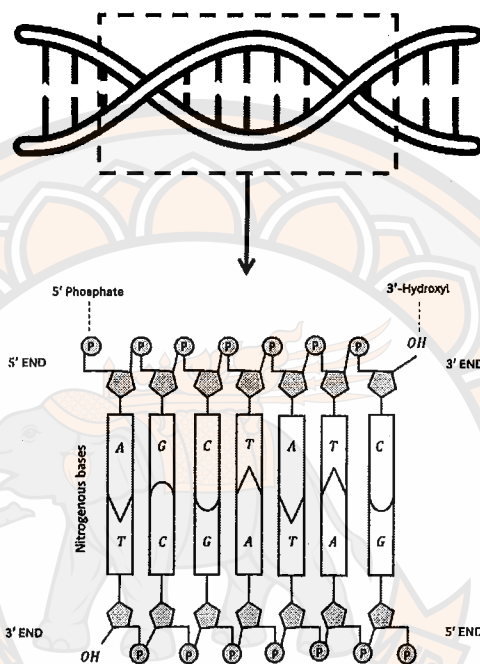


Figure 2 Complementarity of strands in the DNA double helix. The complementary and opposite DNA strands follow the Watson-Crick complement rules. They also differ in sequence when each chain is read in the 5' → 3' direction

For simplicity, in this thesis, the structure of the DNA double helix is presented in Figure 3.

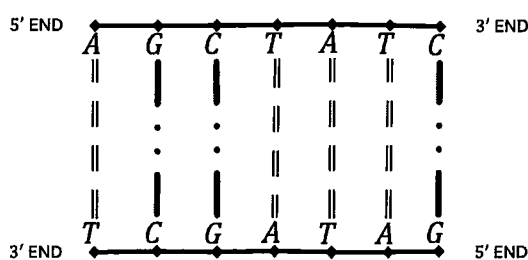


Figure 3 The structure of DNA double helix in simple form

In DNA computing, a significant task is developing a technique for designing DNA strands that can encode information securely and efficiently, considering the chemical and physical stability to avoid mismatched pairs or unwanted hybridization [33]. DNA hybridization is the process of pairing two single strands of DNA, thus forming a DNA double helix, as shown in the DNA hybridization diagram in Figure 4.

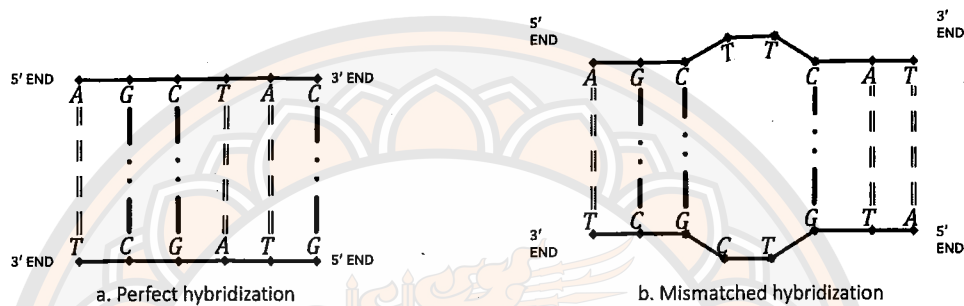


Figure 4 DNA hybridization diagram. (a.) When two DNA strands hybridize perfectly. (b.) When two mismatched DNA strands hybridize.

In [33], the authors established four constraints for designing a DNA codeword set suitable for DNA computing, i.e., The Hamming distance, the reverse constraint, the reverse-complement constraint and the fixed GC-constraint. The first three constraints are designed to reduce the possibility of unwanted hybridizations between DNA strands. The last constraint aims to create similar melting temperatures. Each species of DNA has characteristic melting temperatures: the higher its content of *G* and *C* base pairs, the higher the melting temperature of the DNA [34]. A code that satisfies some or all the constraints is called a good DNA code.

Since the DNA alphabet consists of four letters, early studies of designing DNA strands that employed algebraic coding theory techniques worked on an error-correcting code over four-element sets with an algebraic structure. The construction of DNA codes satisfying a reverse-complement constraint and a GC-content constraint using additive and linear codes over a finite field with four elements was studied in [35]. Subsequently, studies were conducted to design DNA codes that satisfy some of the four constraints using linear and cyclic codes

over various algebraic structures. For instance, in [36], the authors studied the theory of constructing linear and cyclic codes of odd length over finite field with 4 elements suited for DNA computing, with a focus on the reverse-complement constraint. Later, in [37], the authors investigated the construction of DNA codes using cyclic codes over $\frac{\mathbb{F}_2[u]}{\langle u^2-1 \rangle}$ based on *CG*-constraint. In the recent decade, the investigation of constructing cyclic codes of odd length and even length over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ that satisfy reverse and reverse-complement constraints was studied in [38] and [39]. Constructing DNA codes in the works mentioned above has been studied using a code over an alphabet derived from either fields or rings. Recently, in [40], the authors introduced a new concept for constructing DNA codes using cyclic codes over some mixed alphabets that satisfy reverse-complement constraints. However, the concept of this work is based on separable codes. By the motivation of construction of cyclic codes over finite rings and cyclic codes over mixed alphabets suitable for DNA codes, a main problem addressed in this thesis is to construct double cyclic codes of length (α, β) over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ suitable for DNA codes.

This thesis is organized as follows: Chapter II provides some necessary definitions and relevant theorems for this thesis. Chapter III investigates the algebraic structure of double cyclic codes of length (α, β) over $\mathbb{F}_2 + u\mathbb{F}_2$. This chapter is organized into 3 sections based on the types of lengths α and β : the first is the case α and β are non-negative integers; the second is the case both are odd positive integers; and the last is the case α is an odd positive integer and β is an even positive integer. Chapter IV explores the construction of double cyclic codes satisfying the reversible-complement constraint, suitable for generating DNA codes. This chapter is divided into three sections based on the results of Chapter III. Chapter V provides the conclusion of this thesis. Finally, the codewords and DNA codes generated from our results are presented in the appendix.

CHAPTER II

PRELIMINARIES

This chapter provides some necessary definitions and theorems for this thesis and is organized this chapter into 4 sections. In Section 2.1, Section 2.2 and Section 2.3, the concepts and useful theories of rings, fields, polynomial rings and module have been provided. Section 2.4 presents fundamental concepts and relevant theories of coding theory for our study. This section is divided into two parts: the first part covers the concept of double cyclic codes and the second part addresses DNA codes and relevant theories.

2.1 Rings and Fields

Let S be a nonempty set. We recall that $S \times S = \{(s_1, s_2) | s_1, s_2 \in S\}$ and a binary operation on a set S is a mapping from $S \times S$ into S .

Definition 2.1.1. [41] Let R be a nonempty set on which two binary operations are defined, called addition and multiplication, and denoted by $+$ and $\cdot$, respectively. Then, a mathematical system $(R, +, \cdot)$ is called a **ring** with respect to these operations if the following properties hold:

1. Associative laws: For all $a, b, c \in R$,

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

2. Commutative law: For all $a, b \in R$,

$$a + b = b + a.$$

3. Identity element: The set R contains an additive identity element 0 , such that for all $a \in R$,

$$a + 0 = a \text{ and } 0 + a = a.$$

4. Additive inverses: For each $a \in R$, the equations

$$a + x = 0 \text{ and } x + a = 0$$

have a unique solution x in R , called the additive inverse of a , and denoted by $-a$.

5. Distributive laws: For all $a, b, c \in R$,

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

The ring R is called a **finite ring** if R has only a finite number of elements; otherwise R is called an **infinite ring**. If $a \cdot b = b \cdot a$ for all $a, b \in R$, then the ring R is called a **commutative ring**. In addition, if R contains an element 1_R such that $1_R \cdot a = a = a \cdot 1_R$ for all $a \in R$, R is called a **ring with identity**.

From the above the definition, a mathematical system $(R, +)$ satisfies items 1 – 4 is called an **abelian group** and $(R, \cdot)$ satisfies item 1 is called a **semigroup**.

In this thesis, the following conventions will be used for convenience:

1. For any $a, b \in R$, ab denotes $a \cdot b$.
2. For any $a, b \in R$, $a + (-b)$ denotes $a - b$.
3. A ring R is referred to a commutative ring with identity $(R, +, \cdot)$.

Example 2.1.2. Let $\mathbb{Z}$ be the set of all integers and $n \in \mathbb{Z}$. Suppose that

$$n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}.$$

Then, $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity 1 and $(n\mathbb{Z}, +, \cdot)$ is a commutative ring without identity 1, whenever $n \neq 1$ and $n \neq -1$. The ring $(\mathbb{Z}, +, \cdot)$ is called the **ring of integers**.

Example 2.1.3. Let $M_2(\mathbb{Z})$ denote the set of all 2×2 matrices over the ring of integers. Let $+$ and $\cdot$ denote the usual matrix addition and multiplication, respectively. Then, $(M_2(\mathbb{Z}), +, \cdot)$ is a ring with identity. Let

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 4 & 0 \end{bmatrix} \in M_2(\mathbb{Z}).$$

Then,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 4 & 0 \end{bmatrix} = \begin{bmatrix} 10 & 3 \\ 22 & 9 \end{bmatrix} \neq \begin{bmatrix} 11 & 16 \\ 4 & 8 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 4 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

Therefore, $M_2(\mathbb{Z})$ is a ring with identity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ but is not commutative.

Definition 2.1.4. [41] Let R be a ring.

1. An element u in R is called a **unit** if there is $v \in R$ such that $uv = 1$.
2. If every nonzero element of R is a unit, then R is called a **field**.
3. A **finite field** is a field with a finite number of elements.

Example 2.1.5. [42] Let $\mathbb{F}_4 = \{0, 1, \beta, \beta + 1\}$. The addition and multiplication in $\mathbb{F}_4$ are defined as follows:

+	0	1	β	$\beta+1$	*	0	1	β	$\beta+1$
0	0	1	β	$\beta+1$	0	0	0	0	0
1	1	0	$\beta+1$	β	1	0	1	β	$\beta+1$
β	β	$\beta+1$	0	1	β	0	β	$\beta+1$	1
$\beta+1$	$\beta+1$	β	1	0	$\beta+1$	0	$\beta+1$	1	β

It can be verified that $\mathbb{F}_4$ is a finite field.

Definition 2.1.6. [43] Let R be a ring and $a, b \in R$. An element a is called a **divisor** of b or a **factor** of b , written as $a \mid b$, if there is an element $c \in R$ such that $b = ac$.

Definition 2.1.7. [41] A nonzero element a in a ring R is called a **zero divisor** if there is $b \in R$ such that $b \neq 0$ and $ab = 0$.

Note that 0 is not considered a zero divisor. Furthermore, a field has no zero divisors.

Example 2.1.8. [42] Let n be a fixed positive integer. For any $a \in \mathbb{Z}$, dividing a by n , by division algorithm, we have

$$a = qn + r, \text{ where } q, r \in \mathbb{Z} \text{ and } 0 \leq r < n.$$

For any $a \in \mathbb{Z}$, $0 \leq a \leq n - 1$, let $\bar{a}$ denote the set

$$\bar{a} = \{a + kn : k \in \mathbb{Z}\} = \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}.$$

Hence, we introduce the notation

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Define binary operations $+_n$ and $\cdot_n$ on $\mathbb{Z}_n$ by

$$\bar{a} +_n \bar{b} = \overline{a + b} \text{ and } \bar{a} \cdot_n \bar{b} = \overline{ab}$$

for all $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Then, we obtain that $(\mathbb{Z}_n, +_n, \cdot_n)$ is a finite commutative ring with identity $\bar{1}$.

For example, when $n = 4$, we have

$$\bar{0} = \{\dots, -8, -4, 0, 4, 8, \dots\},$$

$$\bar{1} = \{\dots, -7, -3, 1, 3, 7, \dots\},$$

$$\bar{2} = \{\dots, -6, -2, 2, 6, 10, \dots\},$$

$$\bar{3} = \{\dots, -5, -1, 3, 7, 11, \dots\}.$$

Note that $\bar{0} = \bar{4} = \overline{-4} = \bar{8}$, etc. Hence, $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Since $\bar{2} \cdot_4 \bar{2} = \bar{0}$, $\bar{2}$ is zero divisor and not unit. Therefore, $\mathbb{Z}_4$ is not a field.

Sometimes, for simplicity, we identify $\bar{a} \in \mathbb{Z}_n$ with $a \in \{0, 1, 2, \dots, n - 1\}$. Then, we have $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$.

Corollary 2.1.9. [41] Let n be a positive integer. Then, $\mathbb{Z}_n$ is a field if and only if n is prime.

Definition 2.1.10. [41] If there is a positive integer n such that for all $a \in R$, $na = \underbrace{a + a + \dots + a}_{n \text{ copies}} = 0$, then the smallest such positive integer is called the **characteristic** of R . If no such positive integer exists, then R is said to be of **characteristic zero**.

Example 2.1.11. 1. The ring $(\mathbb{Z}, +, \cdot)$ has characteristic 0.

2. The ring $(\mathbb{Z}_n, +, \cdot)$ has characteristic n , where n is a positive integer.

3. From Example 2.1.8, we have that $2(\bar{2}) = \bar{2} + \bar{2} = \bar{4} = \bar{0}$. However, 4 is the smallest positive integer such that $4(\bar{a}) = \bar{a} + \bar{a} + \bar{a} + \bar{a} = \bar{0}$ for all $\bar{a} \in \mathbb{Z}_4$. Hence, $\mathbb{Z}_4$ has characteristic 4.

Definition 2.1.12. [41] A subset S of a ring $(R, +, \cdot)$ is called a **subring** of R if $(S, +, \cdot)$ is a ring. Similarly, when S and R are fields, S is called a **subfield** of R .

The following theorem gives a necessary and sufficient condition for a subset to be a subring.

Theorem 2.1.13. *Let R be a ring. A nonempty subset S of R is a subring of R if and only if $a - b \in S$ and $ab \in S$ for all $a, b \in S$.*

Example 2.1.14. From Example 2.1.2, we have $n\mathbb{Z} \subseteq \mathbb{Z}$ for all $n \in \mathbb{Z}$ and $(n\mathbb{Z}, +, \cdot)$ is a commutative ring. Therefore, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Definition 2.1.15. [41] A nonempty subset I of a ring R is called a **ideal** of R if for all $a, b \in I$ and for all $r \in R$, $a - b \in I$, $ra \in I$.

By Theorem 2.1.13, we obtain that a nonempty subset I of a ring R is an ideal if and only if $(I, +)$ is a subgroup of $(R, +)$ and $ar, ra \in I$ for all $a \in I$ and for all $r \in R$.

Example 2.1.16. From Examples 2.1.2 and 2.1.14, we have that $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ for all $n \in \mathbb{Z}$. Let $r \in \mathbb{Z}$ and $a \in n\mathbb{Z}$. Then, $a = nk$ for some $k \in \mathbb{Z}$. Hence,

$$ra = r(nk) = n(rk) \in n\mathbb{Z}.$$

Therefore, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Definition 2.1.17. [41] Let R be a ring and M be an ideal of R . Then, M is called a **maximal ideal** of R if $M \neq R$ and there does not exist any ideal I of R such that $M \subset I \subset R$.

Corollary 2.1.18. [41] *Let R be a ring and $a \in R$. Then, a is in a maximal ideal of R if and only if a is not a unit.*

Definition 2.1.19. A ring R is called a **local ring** if R has unique maximal ideal.

Theorem 2.1.20. [45] *A ring R is a local ring if and only if the set of all nonunits in R is an ideal.*

Example 2.1.21. 1. From Example 2.1.16, we have that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, where p is prime number. Moreover, $\mathbb{Z}$ is not local ring.

2. From Example 2.1.8, we have $\mathbb{Z}_4$ is a commutative ring with identity 1. We can show that $\{0\}$ and $\{0, 2\}$ are all ideals of $\mathbb{Z}_4$. Then, $\{0, 2\}$ is the unique maximal ideal. Therefore, $\mathbb{Z}_4$ is a local ring.

Definition 2.1.22. [41] Let R be a ring. Then, an ideal I is called a **principal ideal** of R if there is an element $a \in I$ such that

$$I = \langle a \rangle = \{ar : r \in R\}.$$

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

Note that generators of a principal ideal may not be unique.

Example 2.1.23. 1. From Example 2.1.21(2), we have that $\{0, 2\}$ is an ideal of $\mathbb{Z}_4$. Let $\langle 2 \rangle = \{2 \cdot_4 r : r \in \mathbb{Z}_4\} = \{0, 2\}$. Hence, the ideal $\{0, 2\}$ can be rewritten as $\langle 2 \rangle$ and 2 is called a generator of $\langle 2 \rangle$.

2. In $\mathbb{Z}$, we have $\langle m \rangle = \{rm : r \in \mathbb{Z}\} = m\mathbb{Z}$ for any m in $\mathbb{Z}$. From Example 2.1.16, we have that $\langle m \rangle$ is a principal ideal.

Definition 2.1.24. [8] A ring R is called a **principal ideal ring** if every ideal of R is principal.

Example 2.1.25. 1. From Example 2.1.21, we have that $\langle 0 \rangle$ and $\langle 2 \rangle$ are all ideals of $\mathbb{Z}_4$. Therefore, $\mathbb{Z}_4$ is a principal ideal ring.

2. Since every ideal I of the ring $\mathbb{Z}$ is a principal ideal and $I = \langle m \rangle$, where $m \in \mathbb{Z}$, we have $\mathbb{Z}$ is a principal ideal.

Definition 2.1.26. [8] A ring R is called a **chain ring** if all its ideals form a chain under inclusion.

Proposition 2.1.27. [8] Let R be a finite ring. Then, the following conditions are equivalent:

1. R is a local ring and the maximal ideal M of R is principal, i.e., $M = \langle m \rangle$ for some $m \in R$;
2. R is a local principal ideal ring;
3. R is a chain ring whose ideals are $\langle m^i \rangle, 0 \leq i \leq t$, where t is the smallest positive integer such that $m^t = 0$.

Example 2.1.28. 1. From Examples 2.1.21(2) and 2.1.25, we have that $\mathbb{Z}_4$ is a local principal ideal ring. Therefore, $\mathbb{Z}_4$ is a chain ring. Moreover, we can see that the ideals of $\mathbb{Z}_4$ are of the form $\langle 0 \rangle \subseteq \langle 2 \rangle$.

2. By Theorem 2.1.20, the ring $\mathbb{Z}_{p^n}$ is a local ring with maximal ideal $\langle p \rangle$, where p is a prime and n is a positive number. The ideals of $\mathbb{Z}_{p^n}$ are of the form

$$\langle 0 \rangle = \langle p^n \rangle \subset \langle p^{n-1} \rangle \subset \cdots \subset \langle p \rangle \subset \langle 1 \rangle = \mathbb{Z}_{p^n}.$$

A diagram of the lattice of ideals of $\mathbb{Z}_{p^n}$ is given in Figure 5.

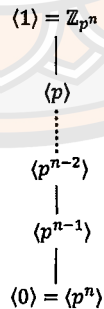


Figure 5 Lattice of ideals of $\mathbb{Z}_{p^n}$

Definition 2.1.29. [41] Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be rings and φ be a mapping from R to R' . Then, φ is called a **homomorphism** of R into R' if

$$\varphi(a + b) = \varphi(a) +' \varphi(b),$$

$$\varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$$

for all $a, b \in R$.

Definition 2.1.30. [41] Let φ be a homomorphism of a ring R into a ring R' . Then, φ is called an **isomorphism** if the following conditions are satisfied.

1. φ is one-one, that is, if $\varphi(a) = \varphi(b)$ then $a = b$ for all $a, b \in R$.
2. φ is onto, that is, if $b' \in R'$, there is $a \in R$ such that $\varphi(a) = b'$.

Definition 2.1.31. [41] Two rings R and R' are called **isomorphic** if there is an isomorphism of R onto R' . We write $R \cong R'$ when R and R' are isomorphic.

Theorem 2.1.32. [42] *Any two finite fields containing the same number of elements are isomorphic.*

Example 2.1.33. [41] Let φ be a mapping from $\mathbb{Z}$ onto $\mathbb{Z}_n$ defined by $\varphi(a) = \bar{a}$ for all $a \in \mathbb{Z}$. Then,

$$\varphi(a + b) = \bar{a} +_n \bar{b} \text{ for all } a, b \in \mathbb{Z}$$

and

$$\varphi(a \cdot b) = \bar{a}\bar{b} = \bar{a} \cdot_n \bar{b} = \varphi(a) \cdot_n \varphi(b) \text{ for all } a, b \in \mathbb{Z}.$$

Thus, φ is a homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}_n$.

Let R be a ring and I be an ideal of R . Suppose that

$$r + I = \{r + a : a \in I\}$$

for all $r \in R$. Remember that $a + I = b + I$ if and only if $a - b \in I$.

Definition 2.1.34. [41] Let R be a ring and I be an ideal of R and

$$R/I = \{r + I : r \in R\}.$$

Define an addition and a multiplication on R/I as follows:

$$(r + I) + (r' + I) = (r + r') + I \text{ and } (r + I) \cdot (r' + I) = rr' + I \quad (2.1.1)$$

for all $(r + I), (r' + I) \in R/I$. Then, $(R/I, +, \cdot)$ forms a ring. Moreover, the ring R/I is called the **quotient ring** of R by I .

Example 2.1.35. Let n be a fixed positive integer in $\mathbb{Z}$. Suppose that

$$\langle n \rangle = \{nq : q \in \mathbb{Z}\} \text{ and } a + \langle n \rangle = \{a + nq : q \in \mathbb{Z}\}.$$

Let $\mathbb{Z}/\langle n \rangle = \{a + \langle n \rangle : a \in \mathbb{Z}\}$. Then, $\mathbb{Z}/\langle n \rangle$ with addition and multiplication which are defined as 2.1.1 is a ring. Define $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}/\langle n \rangle$ by $\varphi(\bar{a}) = a + \langle n \rangle$ for all $\bar{a} \in \mathbb{Z}_n$. Recall that

$$\bar{a} = \bar{b} \text{ if and only if } a - b = nq \text{ for some } q \in \mathbb{Z}.$$

Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$ with $\varphi(\bar{a}) = \varphi(\bar{b})$. Then, $a + \langle n \rangle = b + \langle n \rangle$ and so $a - b \in \langle n \rangle$. This implies that $\bar{a} = \bar{b}$. Since $\mathbb{Z}_n$ and $\mathbb{Z}/\langle n \rangle$ have the same number of elements, φ is a one-one and onto. Consider, for any $\bar{a}, \bar{b} \in \mathbb{Z}_n$,

$$\varphi(\bar{a} +_n \bar{b}) = \varphi(\overline{a+b}) = (a+b) + \langle n \rangle = (a + \langle n \rangle) + (b + \langle n \rangle) = \varphi(\bar{a}) + \varphi(\bar{b})$$

and

$$\varphi(\bar{a} \cdot_n \bar{b}) = \varphi(\overline{ab}) = ab + \langle n \rangle = (a + \langle n \rangle)(b + \langle n \rangle) = \varphi(\bar{a})\varphi(\bar{b}).$$

Hence, φ is a homomorphism of $\mathbb{Z}_n$ into $\mathbb{Z}/\langle n \rangle$. Therefore, we can conclude that $\mathbb{Z}_n$ and $\mathbb{Z}/\langle n \rangle$ are isomorphic.

From the above example, we obtain that, for any prime number p , $\mathbb{Z}/\langle p \rangle \cong \mathbb{Z}_p$ is a field with p elements.

2.2 Polynomial rings

This section introduces an important class of rings known as the polynomial rings. In this section, we denote R as a commutative ring with identity, F as a field and x as an indeterminate. Assume that i is a non-negative integer, then expressions of the form

$$a_i x^i, a_i \in R,$$

are called **monomials** of **degree** i in the **indeterminate** x with coefficients in R . A formal sum

$$a_0x^0 + a_1x^1 + \cdots + a_nx^n \quad (2.2.1)$$

of a finite number of monomials

$$a_0x^0, a_1x^1, \dots, a_nx^n$$

with coefficients $a_0, a_1, \dots, a_n$ in R , where n is any non-negative integer, is called a **polynomial** in the indeterminate x with coefficients in R or simply, a **polynomial over the ring** R . In polynomial (2.2.1), a_ix^i is called its **i -th degree term** and a_i is called **coefficient** of the term. We define $x^0 = 1, x^1 = x$ and write a_0x^0 as a_0 , a_1x^1 as a_1x , then the polynomial (2.2.1) becomes

$$a_0 + a_1x + \cdots + a_nx^n.$$

The simple notations $a(x), b(x), f(x), g(x)$, etc. are used for polynomials. From now on, we let $R[x]$ be the set of all polynomials over a ring R and $F[x]$ be the set of all polynomial over a field F .

Let $a(x)$ and $b(x)$ be polynomials over a ring R such that

$$a(x) = \sum_{i=0}^s a_ix^i \text{ and } b(x) = \sum_{i=0}^t b_ix^i, \quad (2.2.2)$$

where s and t are non-negative integers. Let $M = \max\{s, t\}$. Set

$$a_{s+1} = a_{s+2} = \cdots = a_M = 0 \text{ if } s < M,$$

$$b_{t+1} = b_{t+2} = \cdots = b_M = 0 \text{ if } t < M,$$

then $a(x)$ and $b(x)$ can be written as

$$a(x) = \sum_{i=0}^M a_ix^i \text{ and } b(x) = \sum_{i=0}^M b_ix^i.$$

The addition (+) and multiplication ($\cdot$) on $R[x]$ are defined as follows:

$$a(x) + b(x) = \sum_{i=0}^M (a_i + b_i)x^i \text{ and } a(x) \cdot b(x) = \sum_{i=0}^{s+t} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i,$$

where

$$a_{s+1} = a_{s+2} = \cdots = a_{s+t} = 0 \text{ if } t \geq 1,$$

$$b_{t+1} = b_{t+2} = \cdots = b_{s+t} = 0 \text{ if } s \geq 1.$$

Furthermore, for any $a(x), b(x), c(x) \in R[x]$,

$$\begin{aligned} a(x) \cdot (b(x) + c(x)) &= a(x) \cdot b(x) + a(x) \cdot c(x) \text{ and} \\ (a(x) + b(x)) \cdot c(x) &= a(x) \cdot c(x) + b(x) \cdot c(x). \end{aligned}$$

Therefore, $(R[x], +, \cdot)$ is a ring. The ring $R[x]$ is called a **polynomial ring** over R . The zero 0 of R is the zero of $R[x]$. If R has an identity 1_R , then $R[x]$ has an identity. Moreover, if R is commutative, $R[x]$ is also commutative. Sometimes, for simplicity, we will write $a(x)b(x)$ for $a(x) \cdot b(x)$ for all $a(x), b(x) \in R[x]$.

Definition 2.2.1. [41] Let R be a ring and $a(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ such that $a_n \neq 0$ and n is a non-negative integer. Then,

1. The number n is called the **degree** of $a(x)$, written $\deg(a(x))$.
2. The coefficient a_n is called the **leading coefficient** of $a(x)$.
3. If $a_n = 1_R$, the $a(x)$ is called a **monic polynomial**.
4. The polynomials of degree 0 in $R[x]$ are exactly those elements from $R - \{0\}$ and $0 \in R[x]$ has no degree.

Theorem 2.2.2. [41] Let $R[x]$ be a polynomial ring and $a(x), b(x)$ be non-zero polynomials in $R[x]$.

1. If $a(x)b(x) \neq 0$, then $\deg(a(x)b(x)) \leq \deg(a(x)) + \deg(b(x))$.
2. If $a(x) + b(x) \neq 0$, then $\deg(a(x) + b(x)) \leq \max\{\deg(a(x)), \deg(b(x))\}$.

Example 2.2.3. Let $a(x) = 1 + 2x^2$ and $b(x) = 3 + 2x^2$ be polynomials in the polynomial ring $\mathbb{Z}_4[x]$. Then, $a(x)b(x) = 3$ and $a(x) + b(x) = 0$. Hence, $\deg(a(x)b(x)) = 0 < 4 = \deg(a(x)) + \deg(b(x))$ and $a(x) + b(x)$ has no degree.

Theorem 2.2.4. [41] (*Division Algorithm*) Let R be a ring and $a(x), b(x)$ be polynomials in $R[x]$ with the leading coefficient of $a(x)$ is a unit in R . Then, there exist unique polynomials $q(x), r(x) \in R[x]$ such that

$$b(x) = a(x)q(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) \leq \deg(a(x)) - 1$.

The polynomials $q(x)$ and $r(x)$ in Theorem 2.2.4 are called the **quotient** and **remainder**, respectively, on division of $b(x)$ by $a(x)$.

Definition 2.2.5. [41] Let R be a ring and $a(x), b(x) \in R[x]$ such that $a(x) \neq 0$. We say that $a(x)$ divides $b(x)$, and write $a(x) \mid b(x)$ if there exists $q(x) \in R[x]$ such that $b(x) = a(x)q(x)$.

Example 2.2.6. Let $R = \mathbb{Z}_4$,

$$a(x) = x^3 + x + 1 \text{ and } b(x) = x^5 + x^4 + x^2 + 1.$$

By Division Algorithm, we obtain the quotient and the remainder on division of $a(x)$ by $b(x)$ as $q(x) = x^2 + x + 3$ and $r(x) = 3x^2 + 2$, respectively, and the result can be written as

$$x^5 + x^4 + x^2 + 1 = (x^3 + x + 1)(x^2 + x + 3) + (3x^2 + 2).$$

Example 2.2.7. Let $R = \mathbb{Z}_4$,

$$a(x) = 2x^3 + x + 1 \text{ and } b(x) = x^5 + x^4 + x^2 + 1.$$

Since there is no element k in R such that $2k = 1$, there are no polynomials $q(x)$ and $r(x)$ in $R[x]$ such that $b(x) = a(x)q(x) + r(x)$, where $\deg(r(x)) < \deg(a(x))$.

Definition 2.2.8. [43] Let R be a ring. For elements $a, b \in R$, an element d is called a **greatest common divisor** of a and b if

1. $d \mid a$ and $d \mid b$ and
2. if $c \mid a$ and $c \mid b$, for some $c \in R$, then $c \mid d$.

We write a greatest common divisor of a and b by $\gcd(a, b)$.

Lemma 2.2.9. [42] *Let $a(x), b(x)$ and $c(x)$ be polynomials over field F and assume that $a(x) \neq 0$. If $a(x) \mid b(x)c(x)$ and $\gcd(a(x), b(x)) = 1$, then $a(x) \mid c(x)$.*

Definition 2.2.10. [8] Let R be a finite commutative chain ring and $a(x) \in R[x]$ with degree k such that $a(x) = a_0 + a_1x + \cdots + a_kx^k$. Then, the **reciprocal polynomial** of $a(x)$ is defined as

$$a^*(x) = x^k a\left(\frac{1}{x}\right) = a_k + a_{k-1}x + \cdots + a_0x^k.$$

Then, if $a_0 \neq 0$, then $\deg(a^*(x)) = \deg(a(x))$ otherwise $\deg(a^*(x)) \leq \deg(a(x))$. Furthermore, $a(x)$ is called **self-reciprocal** if $a^*(x) = a(x)$.

Lemma 2.2.11. [8] *Let R be a finite commutative chain ring and $a(x), b(x) \in R[x]$.*

1. *If $\deg(a(x)) \geq \deg(b(x))$, then $(a(x) + b(x))^* = a^*(x) + x^i b^*(x)$, where $i = \deg(a(x)) - \deg(b(x))$.*
2. *$(a(x)b(x))^* = a^*(x)b^*(x)$.*

Example 2.2.12. Let $R = \mathbb{Z}_4$ and

$$a(x) = x^3 + 3x^2 + x + 2 \text{ and } b(x) = x^2 + 2x$$

be polynomials in $R[x]$. Then,

$$\begin{aligned} a^*(x) &= x^3 a\left(\frac{1}{x}\right) = x^3 \left(\frac{1}{x^3} + \frac{3}{x^2} + \frac{1}{x} + 2\right) = 1 + 3x + x^2 + 2x^3 \text{ and} \\ b^*(x) &= x^2 b\left(\frac{1}{x}\right) = x^2 \left(\frac{1}{x^2} + \frac{2}{x}\right) = 1 + 2x. \end{aligned}$$

Consider,

$$\begin{aligned} a^*(x) + x^{3-2}b^*(x) &= (1 + 3x + x^2 + 2x^3) + x(1 + 2x) \\ &= 1 + 3x + x^2 + 2x^3 + x + 2x^2 \\ &= 1 + 3x^2 + 2x^3 \\ &= (a(x) + b(x))^*. \end{aligned}$$

Consider,

$$\begin{aligned} a^*(x)b^*(x) &= (1 + 3x + x^2 + 2x^3)(1 + 2x) = 1 + x + 3x^2 \text{ and} \\ (a(x)b(x))^* &= (x^5 + x^4 + 3x^3)^* = 1 + x + 3x^2. \end{aligned}$$

Hence, $(a(x)b(x))^* = a^*(x)b^*(x)$.

Definition 2.2.13. [42] Let R be a ring and m be a fixed element of R . For any $a, b \in R$, define

$$a \equiv b \pmod{m} \text{ if and only if } m \mid (a - b).$$

We read $a \equiv b \pmod{m}$ as a is congruent to b modulo m .

Example 2.2.14. Let $m(x) = x^2 + 1 \in \mathbb{Z}_4[x]$ be fixed element. Suppose that

$$a(x) = x^4 + 2x + 1 \text{ and } b(x) = 2x + 2$$

are polynomials in $\mathbb{Z}_4[x]$. By Division Algorithm, we have

$$\begin{aligned} a(x) - b(x) &= x^4 + 2x + 1 - 2x - 2 \\ &= x^4 + 3 \\ &= m(x)(x^2 + 3). \end{aligned}$$

Hence, $m(x)$ divides $a(x) - b(x)$. Therefore, $a(x) \equiv b(x) \pmod{x^2 + 1}$.

Definition 2.2.15. [42] Let m be fixed element in a ring R . Then,

1. $\bar{a} = \{a + mq : q \in R\}$ for all $a \in R$,
2. for any $a \in R$, $\bar{a}$ is called the **residue class mod m** ,
3. for any $a \in R$, the set of all multiples of a is denoted by $\langle a \rangle$, that is,
 $\langle a \rangle = \{ra : r \in R\}$,
4. the set of residue classes mod m in R will be denoted by $\frac{R}{\langle m \rangle}$.

Remark 2.2.16. For any $a, b \in R$, $\bar{a} = \bar{b}$ if and only if $a \equiv b \pmod{m}$.

Example 2.2.17. From Example 2.2.14, we let $m(x) = x^2 + 1 \in \mathbb{Z}_4[x]$ be fixed element. For any polynomial $a(x) \in \mathbb{Z}_4[x]$, by Division Algorithm, we have that

$$a(x) = (x^2 + 1)q(x) + r(x),$$

where $q(x), r(x) \in \mathbb{Z}_4[x]$ with $\deg(r(x)) \leq \deg(m(x)) - 1 = 1$. Hence, for all $a(x) \in \mathbb{Z}_4[x]$, the residue class mod $x^2 + 1$ containing $a(x)$ is of the form

$$\overline{r(x)} = \overline{r_0 + r_1x} = \{r_0 + r_1x + (x^2 + 1)q(x) : q(x) \in \mathbb{Z}_4[x]\},$$

where $r_0, r_1 \in \mathbb{Z}_4$. Therefore, the set of residue classes mod $x^2 + 1$ in $\mathbb{Z}_4[x]$ is

$$\frac{\mathbb{Z}_4[x]}{\langle x^2 + 1 \rangle} = \{\overline{r_0 + r_1x} : r_0, r_1 \in \mathbb{Z}_4\}.$$

Theorem 2.2.18. [42] Let R be a ring and m be a fixed element of R . Define binary operations $+$ and $\cdot$ on $\frac{R}{\langle m \rangle}$ by

$$\overline{a} + \overline{b} = \overline{a + b} \text{ and } \overline{a} \cdot \overline{b} = \overline{ab}$$

for all $\overline{a}, \overline{b} \in \frac{R}{\langle m \rangle}$. Then, $(\frac{R}{\langle m \rangle}, +, \cdot)$ is a ring.

Definition 2.2.19. [42] Let R be a ring and m be a fixed element of R . The ring $\frac{R}{\langle m \rangle}$ is called the **residue class ring** of R modulo m .

Example 2.2.20. Let $m(x) = x^2 + 1$ be a fixed polynomial in $\mathbb{Z}_4[x]$. From Example 2.2.17, we have

$$\frac{\mathbb{Z}_4[x]}{\langle x^2 + 1 \rangle} = \{\overline{r_0 + r_1x} : r_0, r_1 \in \mathbb{Z}_4\}.$$

By Theorem 2.2.18, we obtain that $(\frac{\mathbb{Z}_4[x]}{\langle x^2 + 1 \rangle}, +, \cdot)$ is a ring.

Let R be a ring and $m(x)$ be a fixed polynomial of degree $n > 0$. For each $r \in R$, there is a residue class

$$\overline{r} = \{r + m(x)q(x) : q(x) \in R[x]\}.$$

Then, we will identify the residue class $\bar{r}$ of $r \in R$ modulo $m(x)$ by r . More generally, the residue class of $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \pmod{m(x)}$, where $a_0, a_1, \dots, a_{n-1} \in R$ will be denoted by

$$\begin{aligned} \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} &= \overline{a_0} + \overline{a_1x} + \cdots + \overline{a_{n-1}x^{n-1}} \\ &= \overline{a_0} + \overline{a_1} \bar{x} + \cdots + \overline{a_{n-1}} \bar{x}^{n-1} \\ &= a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1}. \end{aligned}$$

For simplicity, we usually delete the bar and write the polynomial

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

for $a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1}$. Thus, the residue class ring of $R[x]$ modulo $m(x)$ can be rewritten as

$$\frac{R[x]}{\langle m(x) \rangle} = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} : a_0, a_1, \dots, a_{n-1} \in R\}.$$

For any $b(x) \in R[x]$, we also use the notation

$$b(x) \pmod{m(x)}$$

to denote the unique polynomial of degree less than n , which is congruent to $b(x)$ modulo by $m(x)$.

Example 2.2.21. From Example 2.2.17, we can rewrite $\frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle}$ as

$$\frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle} = \{r_0 + r_1x : r_0, r_1 \in \mathbb{Z}_4\}.$$

The addition $+$ and multiplication $\cdot$ on $\frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle}$ are rewritten as

$$\begin{aligned} (a_0 + a_1x) + (b_0 + b_1x) &= (a_0 + b_0) + (a_1 + b_1)x \text{ and} \\ (a_0 + a_1x) \cdot (b_0 + b_1x) &= (a_0 + a_1x)(b_0 + b_1x) \pmod{x^2 + 1}, \end{aligned}$$

for all $a_0 + a_1x, b_0 + b_1x \in \frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle}$.

Let $a(x) = 2 + x$ and $b(x) = 1 + 3x$ be polynomials in $\frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle}$. Then, we have $a(x) + b(x) = 3$ in $\frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle}$ and

$$\begin{aligned} a(x) \cdot b(x) &= (2 + x)(1 + 3x) \pmod{x^2 + 1} \\ &= 2 + 3x + 3x^2 \pmod{x^2 + 1} \\ &\equiv 3 + 3x \pmod{x^2 + 1}. \end{aligned}$$

Hence, $a(x) \cdot b(x) = 3 + 3x$ in $\frac{\mathbb{Z}_4[x]}{\langle x^2+1 \rangle}$.

Example 2.2.22. Let $m(x) = x^2 + x + 1$ be a fixed polynomial in $\mathbb{Z}_4[x]$.

$$\frac{\mathbb{Z}_4[x]}{\langle x^2 + x + 1 \rangle} = \{r_0 + r_1x + r_2x^2 : r_0, r_1, r_2 \in \mathbb{Z}_4\}.$$

The addition $+$ and multiplication $\cdot$ on $\frac{\mathbb{Z}_4[x]}{\langle x^2+x+1 \rangle}$ are rewritten as

$$a(x) + b(x) = a(x) + b(x) \text{ and } a(x) \cdot b(x) = a(x)b(x) \pmod{x^2 + x + 1},$$

for all $a(x), b(x) \in \frac{\mathbb{Z}_4[x]}{\langle x^2+x+1 \rangle}$. Given polynomials $a(x) = 2 + x$ and $b(x) = 1 + 3x$ in $\frac{\mathbb{Z}_4[x]}{\langle x^2+x+1 \rangle}$.

Then, $a(x) + b(x) = 3$ in $\frac{\mathbb{Z}_4[x]}{\langle x^2+x+1 \rangle}$ and

$$\begin{aligned} a(x) \cdot b(x) &= (2 + x)(1 + 3x) \pmod{x^2 + x + 1} \\ &= 2 + 3x + 3x^2 \pmod{x^2 + x + 1} \\ &\equiv 3 \pmod{x^2 + x + 1}. \end{aligned}$$

Hence, $a(x) \cdot b(x) = 3$ in $\frac{\mathbb{Z}_4[x]}{\langle x^2+x+1 \rangle}$.

The above examples demonstrate that multiplying the same polynomials $a(x)$ and $b(x)$ in different residue class rings has different results; that is, it depends on a fixed polynomial $m(x)$.

2.3 Modules

In this section, we will give some important definitions and theorems of modules for the thesis.

Definition 2.3.1. [41] Let $(R, +, \cdot)$ be a ring and $(M, +')$ be an abelian group. Then, M is called a **left R-module** with respect to a mapping $\mu : R \times M \rightarrow M$ denoted by $\mu(r, m) = rm$, for all $r \in R$ and $m \in M$, if for all $r_1, r_2 \in R$ and $m_1, m_2 \in M$,

1. $r_1(m_1 +' m_2) = r_1m_1 +' r_1m_2$,
2. $(r_1 + r_2)m_1 = r_1m_1 +' r_2m_1$,
3. $r_1(r_2m_1) = (r_1 \cdot r_2)m_1$,

4. $1_R m = m$ for all $m \in M$, where 1_R is an identity element of R .

In addition, a **right R -module** can be defined similarly.

Example 2.3.2. 1. A vector space V over a field F is an F -module.

2. In a ring R , every left (right) ideal of R is a left (right) R -module. In particular, R is a left and right R -module.
3. Let $R = \mathbb{Z}$. Then, any abelian group $(M, +)$ can be considered as $\mathbb{Z}$ -module by defining

$$nm = \underbrace{m + m + \cdots + m}_{n \text{ times, } n > 0} \text{ or}$$

$$nm = \underbrace{(-m) + (-m) + \cdots + (-m)}_{-n \text{ times, } n < 0} \text{ and}$$

$$0m = 0,$$

for any $m \in M$.

Since we use the results of the left R -module, from now on, unless stated otherwise, we refer to a left R -module as an R -module.

Definition 2.3.3. [41] Let M be an R -module and S be a nonempty subset of M . Then, S is called a **submodule** of M if S is a subgroup of M and for all $r \in R, a \in S$, we have $ra \in S$.

Example 2.3.4. Consider a ring $\mathbb{Z}$ and an abelian group $(\mathbb{Z}[x], +)$. Then, we can obtain that $\mathbb{Z}[x]$ is an $\mathbb{Z}$ -module by defining as Example 2.3.2(3). Let

$$2\mathbb{Z}[x] = \{2f(x) : f(x) \in \mathbb{Z}[x]\} \subseteq \mathbb{Z}[x].$$

Since $2f_1(x) - 2f_2(x) = 2(f_1(x) - f_2(x)) \in 2\mathbb{Z}[x]$, for all $2f_1(x), 2f_2(x) \in 2\mathbb{Z}[x]$, we have $2\mathbb{Z}[x]$ is a subgroup of $\mathbb{Z}[x]$. For any $n \in \mathbb{Z}$ and $2f(x) \in 2\mathbb{Z}[x]$, we have $n2f(x) = 2nf(x) = 2(nf(x)) \in 2\mathbb{Z}[x]$. Therefore, $2\mathbb{Z}[x]$ is a submodule of $\mathbb{Z}[x]$.

Definition 2.3.5. [44] Let S be a nonempty subset of an R -module M . Then, the submodule of M **generated** by S is defined to be the intersection of all submodules of M which contain S and is denoted by $\langle S \rangle$.

Theorem 2.3.6. [41] Let R be a ring and M be R -module. Suppose that X is a nonempty subset of M . Then,

$$\langle X \rangle = \left\{ \sum_{i=1}^k r_i x_i : r_i \in R, x_i \in X, 1 \leq i \leq k, k \in \mathbb{N} \right\}.$$

Example 2.3.7. Let $R = \mathbb{Z}_4$ and $R^3 = \{(r_1, r_2, r_3) : r_1, r_2, r_3 \in R\}$. Recall that $(R, +, \cdot)$ is a commutative ring with the operations defined as Example 2.1.8.

Then, R^3 is an R -module under the following definitions:

For all $(r_1, r_2, r_3), (s_1, s_2, s_3) \in R^3$ and $a \in R$,

$$\begin{aligned} (r_1, r_2, r_3) + (s_1, s_2, s_3) &= (r_1 + s_1, r_2 + s_2, r_3 + s_3), \\ a(r_1, r_2, r_3) &= (ar_1, ar_2, ar_3). \end{aligned}$$

Let $S = \{(\bar{1}, 0, 0), (0, \bar{1}, 0), (0, 0, \bar{1})\} = \{s_1, s_2, s_3\} \subseteq R^3$. Then,

$$\langle S \rangle = \{a_1 s_1 + a_2 s_2 + a_3 s_3 : a_1, a_2, a_3 \in R\}.$$

Since $(a_1, a_2, a_3) = a_1 s_1 + a_2 s_2 + a_3 s_3$ for all $(a_1, a_2, a_3) \in R^3$, we have $R^3 = \langle S \rangle$.

Definition 2.3.8. [43] Let M and N be R -modules.

1. A mapping $\varphi : M \rightarrow N$ is called an **R -homomorphism** if

$$\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) \text{ and } \varphi(rm) = r\varphi(m)$$

for all $r \in R$ and $m, m_1, m_2 \in M$. The set of all R -homomorphisms from M into N is denoted by

$$\text{hom}_R(M, N).$$

2. For an R -homomorphism $\varphi \in \text{hom}_R(M, N)$, we define its kernel as

$$\ker(\varphi) = \{m \in M : \varphi(m) = 0\} \subseteq M.$$

3. For an R -homomorphism $\varphi \in \text{hom}_R(M, N)$, we define its image as

$$\varphi(M) = \{\varphi(m) \in N : m \in M\} \subseteq N.$$

Furthermore, we obtain that $\ker(\varphi)$ is a submodule of M and $\varphi(M)$ is a submodule of N .

Definition 2.3.9. [43] Let $\varphi \in \text{hom}_R(M, N)$. Then, φ is called an **isomorphism** if the following conditions are satisfied.

1. φ is one-one, that is, if $\varphi(a) = \varphi(b)$ then $a = b$ for all $a, b \in M$.
2. φ is onto, that is, if $b' \in N$, there is $a \in M$ such that $\varphi(a) = b'$.

Two R -modules M and N are called **isomorphic** if there is an isomorphism of M into N . We write $M \cong N$ when M and N are isomorphic. Let S be a submodule of R -module M . Recall that

$$M/S = \{m + S : m \in M\}$$

is an abelian group under an addition $+$ which is defined by

$$(m_1 + S) + (m_2 + S) = (m_1 + m_2) + S$$

for all $(m_1 + S), (m_2 + S) \in M/S$. Therefore, M/S is an R -module by defining the operation of R on M/S as

$$r(m + S) = rm + S$$

for all $r \in R$ and $m \in M$ and M/S is called the **quotient module** of M by S .

Theorem 2.3.10. [43] (*Fundamental homomorphism theorem*) Let M and N be R -modules. If $\varphi : M \rightarrow N$ is any R -homomorphism, then

$$M/\ker(\varphi) \cong \varphi(M).$$

2.4 Basic Concepts of Coding Theory

This section provides the necessary definitions and theorems for our study of the algebraic coding theorem. We will start with the following definitions.

Definition 2.4.1. [46] Let $V = \{v_1, v_2, \dots, v_q\}$ be a set with q elements, which we refer to as a **code alphabet** and whose elements are called **code symbols**.

1. A q -ary word of length n over V is a sequence $\mathbf{a} = a_0a_1\cdots a_{n-1}$ with each $a_i \in V$ for all i . Equivalently, $\mathbf{a}$ may also be regarded as the vector $(a_0, a_1, \dots, a_{n-1})$.
2. A q -ary block code of length n over V is a nonempty set $\mathcal{C}$ of q -ary word having the same length n , i.e.,

$$\mathcal{C} \subseteq V^n = \{\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) : a_i \in V, i \in \{0, 1, \dots, n-1\}\}.$$

3. An element of $\mathcal{C}$ is called a **codeword** in $\mathcal{C}$.
4. The number of codewords in $\mathcal{C}$, denoted by $|\mathcal{C}|$, is called the **size** of $\mathcal{C}$.

Example 2.4.2. [46] A code over the code alphabet $\mathbb{F}_2 = \{0, 1\}$ is called a **binary code**, i.e, the code symbols for a binary code are 0 and 1. Some examples of binary codes are:

1. $\mathcal{C}_1 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ is a code of length 2 with $|\mathcal{C}_1| = 4$.
2. $\mathcal{C}_2 = \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$ is a code of length 3 with $|\mathcal{C}_2| = 4$.
3. $\mathcal{C}_3 = \{(0, 0, 1, 1), (0, 1, 0, 1), (1, 0, 1, 0), (1, 1, 0, 0), (1, 0, 0, 1), (0, 1, 1, 0)\}$ is a code of length 4 with $|\mathcal{C}_3| = 6$.

Definition 2.4.3. [46] Let $\mathbf{a}$ and $\mathbf{b}$ be words of length n over an alphabet V . The Hamming distance from $\mathbf{a}$ to $\mathbf{b}$, denoted by $d_H(\mathbf{a}, \mathbf{b})$, is defined to be the number of places at which $\mathbf{a}$ and $\mathbf{b}$ differ. If $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ and $\mathbf{b} = (b_0, b_1, \dots, b_{n-1})$, then

$$d_H(\mathbf{a}, \mathbf{b}) = d(a_0, b_0) + d(a_1, b_1) + \cdots + d(a_{n-1}, b_{n-1}),$$

where, for all $i \in \{0, 1, \dots, n-1\}$,

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

Example 2.4.4. Let $V = \{0, 1, 2, 3, 4\}$ and $\mathbf{a} = (1, 2, 3, 4)$, $\mathbf{b} = (1, 4, 2, 3)$ and $\mathbf{c} = (3, 2, 4, 1)$ be words of length 4 over V . Then,

$$d_H(\mathbf{a}, \mathbf{b}) = d(1, 1) + d(2, 4) + d(3, 2) + d(4, 3) = 0 + 1 + 1 + 1 = 3,$$

$$d_H(\mathbf{b}, \mathbf{c}) = d(1, 3) + d(4, 2) + d(2, 4) + d(3, 1) = 1 + 1 + 1 + 1 = 4,$$

$$d_H(\mathbf{a}, \mathbf{c}) = d(1, 3) + d(2, 2) + d(3, 4) + d(4, 1) = 1 + 0 + 1 + 1 = 3.$$

Definition 2.4.5. [46] For a code $\mathcal{C}$ containing at least two codewords, the minimum distance of $\mathcal{C}$, denoted by $d(\mathcal{C})$, is

$$d(\mathcal{C}) = \min\{d_H(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathcal{C}, \mathbf{a} \neq \mathbf{b}\}.$$

Example 2.4.6. Let $V = \mathbb{Z}_3$ and

$$\mathcal{C} = \{(0, 0, 0, 0, 0, 0), (0, 0, 0, 1, 1, 1), (1, 1, 1, 2, 2, 2)\}$$

be a code of length 6 over V . Then,

$$d_H((0, 0, 0, 0, 0, 0), (0, 0, 0, 1, 1, 1)) = 3$$

$$d_H((0, 0, 0, 0, 0, 0), (1, 1, 1, 2, 2, 2)) = 6$$

$$d_H((0, 0, 0, 1, 1, 1), (1, 1, 1, 2, 2, 2)) = 6.$$

Hence, $d(\mathcal{C}) = 3$.

From Definition 2.4.1, the code alphabet V is a finite set. Then, the study of coding theory will concentrate on the code alphabet, which is a finite ring or a finite field. Next, we will provide some definitions of linear and cyclic codes over a finite ring.

For a finite ring R , let R^n be a set of n -tuples of elements from R . Let $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$, $\mathbf{b} = (b_0, b_1, \dots, b_{n-1}) \in R^n$. The binary operation $+$ on R^n is defined by

$$\mathbf{a} + \mathbf{b} = (a_0, a_1, \dots, a_{n-1}) + (b_0, b_1, \dots, b_{n-1}) = (a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}).$$

Then, we obtain that $(R^n, +)$ is an abelian group.

For any $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in R^n$ and $r \in R$, the operation between the ring R and the group R^n is defined by

$$r\mathbf{a} = r(a_0, a_1, \dots, a_{n-1}) = (ra_0, ra_1, \dots, ra_{n-1}).$$

Therefore, we can obtain that R^n is an R -module.

Let $\mathcal{C}$ be a code of length n over R . Then, $\mathcal{C}$ is a collection of codewords $(a_0, a_1, \dots, a_{n-1})$, where $a_i \in R$ for all $i \in \{0, 1, \dots, n-1\}$. We also write $\mathcal{C} \subseteq R^n$.

Definition 2.4.7. [8] A nonempty subset $\mathcal{C}$ of R^n is called a **linear code** of length n over R if $\mathcal{C}$ is an R -submodule of R^n .

Definition 2.4.8. [8] A linear code $\mathcal{C}$ of length n over R is called **cyclic code** if for any $(a_0, a_1, \dots, a_{n-1}) \in \mathcal{C}$, its cyclic shift $(a_{n-1}, a_0, \dots, a_{n-2})$ is also in $\mathcal{C}$.

Example 2.4.9. The following are cyclic codes:

1. $\mathcal{C}_1 = \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\} \subseteq \mathbb{F}_2^4$.
2. $\mathcal{C}_2 = \{(0, 0, 0), (1, 1, 1), (2, 2, 2), (3, 3, 3)\} \subseteq \mathbb{Z}_4^3$.
3. $\mathcal{C}_3 = \{(0, 0, 0), (0, 0, 2), (0, 2, 0), (0, 2, 2), (1, 1, 1), (1, 1, 3), (1, 3, 1), (1, 3, 3), (2, 2, 2), (2, 0, 0), (2, 0, 2), (2, 2, 0), (3, 3, 3), (3, 1, 3), (3, 1, 1), (3, 3, 1)\} \subseteq \mathbb{Z}_4^3$.

Next, we will represent the codewords in polynomial forms. These forms simplify the study of cyclic codes. In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following mapping:

$$\tau : R^n \rightarrow \frac{R[x]}{\langle x^n - 1 \rangle}, (a_0, a_1, \dots, a_{n-1}) \mapsto a_0 + a_1x + \dots + a_{n-1}x^{n-1}.$$

Hence, τ is an R -homomorphism. For any $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ in R^n , the polynomial $a(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ in the residue class ring $\frac{R[x]}{\langle x^n - 1 \rangle}$ is called **polynomial representation** of $\mathbf{a}$. Notice that if

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

then

$$xa(x) = a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} \pmod{x^n - 1}$$

which would represent the codeword $\mathbf{a}$ cyclically shifted one to the right.

Example 2.4.10. Consider the cyclic code

$$\mathcal{C} = \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\} \text{ over } \mathbb{F}_2,$$

$$\text{then } \tau(\mathcal{C}) = \{0, 1 + x^2, x + x^3, 1 + x + x^2 + x^3\} \subseteq \frac{\mathbb{F}_2[x]}{\langle x^4 - 1 \rangle}.$$

More formally, the fact that a cyclic code $\mathcal{C}$ is invariant under a cyclic shift implies that if $a(x)$ is in $\tau(\mathcal{C})$, then so is $xa(x) \pmod{x^n - 1}$. This means that the studying of cyclic codes of length n over R is the residue class ring $\frac{R[x]}{\langle x^n - 1 \rangle}$. Under the correspondence of vectors with polynomials as given above, cyclic codes are ideals of $\frac{R[x]}{\langle x^n - 1 \rangle}$ and ideals of $\frac{R[x]}{\langle x^n - 1 \rangle}$ are cyclic codes. Thus, the study of cyclic codes in R^n is equivalent to the study of ideal in $\frac{R[x]}{\langle x^n - 1 \rangle}$. From now on, we replace $\tau(\mathcal{C})$ of the cyclic code $\mathcal{C}$ with $\mathcal{C}$.

Proposition 2.4.11. [8] *A linear code $\mathcal{C}$ of length n over R is a cyclic code if and only if $\mathcal{C}$ is an ideal of the ring $\frac{R[x]}{\langle x^n - 1 \rangle}$.*

Since this thesis investigates and focuses on a code over the alphabet $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$, we will provide some of the necessary theories for a cyclic code over this alphabet. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ is a residue class ring

$$\frac{\mathbb{F}_2[u]}{\langle u^2 \rangle} = \{0, 1, u, 1 + u\}.$$

Moreover, by Section 2.1, we obtain that the ring $\mathbb{F}_2 + u\mathbb{F}_2$ is a finite commutative chain ring with maximal ideal $\langle u \rangle$ and has characteristic 2. The field $\mathbb{F}_2$ can be view as a subring of $\mathbb{F}_2 + u\mathbb{F}_2$. By Theorem 2.1.32, we have that the finite field $\mathbb{F}_2$ and $\mathbb{Z}_2$ are isomorphic. This implies that the ring $\mathbb{F}_2 + u\mathbb{F}_2 \cong \mathbb{Z}_2 + u\mathbb{Z}_2$ with $u^2 = 0$. Hence, we can apply the result in [10] to the ring $\mathbb{F}_2 + u\mathbb{F}_2$ directly. For simplicity, we use R instead of the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$.

The structure of cyclic codes of length n over R is as follows:

Theorem 2.4.12. [10] *Let n be a positive integer and $\mathcal{C}$ be a cyclic code of length n over R . Then,*

1. *If n is odd, then $\frac{R[x]}{\langle x^n - 1 \rangle}$ is a principal ideal ring and $\mathcal{C} = \langle f_0(x), uf_1(x) \rangle = \langle f_0(x) + uf_1(x) \rangle$, for some $f_0(x), f_1(x) \in \mathbb{F}_2[x]$ with $f_1(x) \mid f_0(x) \mid (x^n - 1)$.*

2. *If n is even, then*

$$(a) \mathcal{C} = \langle g(x) + up(x) \rangle, \text{ for some } g(x), p(x) \in \mathbb{F}_2[x] \text{ with } g(x) \mid (x^n - 1), \\ (g(x) + up(x)) \mid (x^n - 1) \text{ and } g(x) \mid p(x)\left(\frac{x^n - 1}{g(x)}\right). \text{ Or,}$$

(b) $\mathcal{C} = \langle g(x) + up(x), ua(x) \rangle$, for some $g(x), p(x), a(x) \in \mathbb{F}_2[x]$ with $a(x) \mid g(x)(x^n - 1)$, $a(x) \mid p(x)\left(\frac{x^n - 1}{g(x)}\right)$ and $\deg(a(x)) > \deg(p(x))$.

The following examples are cyclic codes over the ring R derived from the above theorems:

Example 2.4.13. Let $n = 5$. Consider,

$$x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1) \in \mathbb{F}_2[x].$$

Suppose that $\mathcal{C} = \langle (x^5 - 1) + u(x + 1) \rangle$. By Theorem 2.4.12, we obtain that $\mathcal{C}$ is a cyclic code of length 5 over R with 16 codewords. Furthermore,

$$\begin{aligned} \mathcal{C} = \{ & 0, ux^2 + ux, ux^3 + ux, ux^3 + ux^2, ux^4 + ux^2, ux^4 + ux^3, ux^4 + ux, \\ & ux^4 + ux^3 + ux^2 + ux, ux + u, ux^2 + u, ux^3 + u, ux^4 + u, \\ & ux^3 + ux^2 + ux + u, ux^4 + ux^2 + ux + u, ux^4 + ux^3 + ux + u, \\ & ux^4 + ux^3 + ux^2 + u \} \text{ which is} \\ \mathcal{C} = \{ & (0, 0, 0, 0, 0), (0, u, u, 0, 0), (0, u, 0, u, 0), (0, 0, u, u, 0), (0, 0, u, 0, u), \\ & (0, 0, 0, u, u), (0, u, 0, 0, u), (0, u, u, u, u), (u, u, 0, 0, 0), (u, 0, u, 0, 0), \\ & (u, 0, 0, u, 0), (u, 0, 0, 0, u), (u, u, u, u, 0), (u, u, u, 0, u), (u, u, 0, u, u), \\ & (u, 0, u, u, u) \}. \end{aligned}$$

Example 2.4.14. [39] Let $n = 6$. Consider,

$$x^6 - 1 = (x + 1)^2(x^2 + x + 1)^2 = g_1(x)^2 g_2(x)^2 \in \mathbb{F}_2[x].$$

Suppose

$$\mathcal{C}_1 = \langle g_1(x)g_2(x)^2 + ug_2(x)^2 \rangle \text{ and } \mathcal{C}_2 = \langle g_1(x)g_2(x)^2 + ug_2(x), ug_1(x)g_2(x) \rangle.$$

By Theorem 2.4.12, we obtain that $\mathcal{C}_1$ and $\mathcal{C}_2$ are cyclic codes of length 6 over R with 4 and 64 codewords.

We have generated the codewords from Example 2.4.14 and presented them in Tables 2 and 3, respectively.

Table 2 Codewords from the cyclic code C_1 in Example 2.4.14

$(0, 0, 0, 0, 0, 0)$	$(1 + u, 1, 1 + u, 1, 1 + u, 1)$
(u, u, u, u, u, u)	$(1, 1 + u, 1, 1 + u, 1, 1 + u)$

Table 3 Codewords from the cyclic code C_2 in Example 2.4.14

$(0, 0, 0, 0, 0, 0)$	$(1 + u, 1, 1 + u, 1 + u, 1, 1)$
$(1 + u, 1, 1, 1 + u, 1, 1 + u)$	$(1 + u, 1 + u, 1, 1 + u, 1, 1)$
$(1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(1 + u, 1, 1, 1 + u, 1 + u, 1)$
$(1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(1 + u, 1 + u, 1, 1, 1, 1 + u)$
$(1 + u, 1, 1, 1, 1 + u, 1 + u)$	$(1 + u, 1 + u, 1, 1, 1 + u, 1)$
$(1 + u, 1, 1 + u, 1, 1, 1 + u)$	$(1 + u, 1 + u, 1 + u, 1 + u, 1, 1 + u)$
$(1 + u, 1, 1 + u, 1 + u, 1 + u, 1 + u)$	$(1 + u, 1 + u, 1 + u, 1 + u, 1 + u, 1)$
$(1 + u, 1 + u, 1, 1 + u, 1 + u, 1 + u)$	$(1 + u, 1 + u, 1 + u, 1, 1 + u, 1 + u)$
$(1, 1, 1, 1 + u, 1, 1)$	$(1, 1, 1 + u, 1, 1, 1)$
$(1, 1, 1, 1, 1, 1 + u)$	$(1, 1 + u, 1, 1, 1, 1)$
$(1, 1, 1, 1, 1 + u, 1)$	(u, u, u, u, u, u)
$(0, u, u, u, u, 0)$	$(0, u, u, u, 0, u)$
$(0, u, u, 0, u, u)$	$(0, u, 0, u, u, u)$
$(0, 0, u, u, u, u)$	$(1, 1, 1 + u, 1 + u, 1, 1 + u)$
$(1, 1 + u, 1 + u, 1 + u, 1, 1)$	$(1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(1, 1 + u, 1, 1 + u, 1, 1 + u)$	$(1, 1 + u, 1, 1 + u, 1 + u, 1)$
$(1, 1, 1, 1 + u, 1 + u, 1 + u)$	$(1, 1, 1 + u, 1, 1 + u, 1 + u)$
$(1, 1 + u, 1 + u, 1, 1 + u, 1)$	$(1, 1 + u, 1, 1, 1 + u, 1 + u)$
$(1, 1 + u, 1 + u, 1, 1, 1 + u)$	$(u, u, u, u, 0, 0)$
$(u, u, u, 0, u, 0)$	$(u, u, u, 0, 0, u)$
$(u, u, 0, u, 0, u)$	$(u, u, 0, 0, u, u)$
$(u, 0, u, 0, u, u)$	$(u, 0, 0, u, u, u)$
$(u, u, 0, u, u, 0)$	$(0, u, u, 0, 0, 0)$
$(0, u, 0, u, 0, 0)$	$(u, 0, u, u, u, 0)$
$(u, 0, u, u, 0, u)$	$(0, 0, u, u, 0, 0)$
$(0, 0, u, 0, u, 0)$	$(0, 0, 0, u, u, 0)$
$(0, u, 0, 0, u, 0)$	$(0, 0, 0, 0, u, u)$
$(0, 0, 0, u, 0, u)$	$(0, 0, u, 0, 0, u)$
$(0, u, 0, 0, 0, u)$	$(1 + u, 1, 1, 1, 1, 1)$
$(1, 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(u, u, 0, 0, 0, 0)$
$(u, 0, u, 0, 0, 0)$	$(u, 0, 0, u, 0, 0)$
$(u, 0, 0, 0, u, 0)$	$(u, 0, 0, 0, 0, u)$

2.4.1 Double cyclic codes

In this section, we present new classes of error-correcting code known as double cyclic codes. The concept of double cyclic codes was introduced in [21]. The authors provided the concept of double cyclic codes over $\mathbb{Z}_2$. Since $\mathbb{Z}_2$ and $\mathbb{F}_2$ are isomorphic, we will use $\mathbb{F}_2$ instead of $\mathbb{Z}_2$.

Definition 2.4.15. [21] Let $\mathcal{C}$ be a linear code of length $n = \alpha + \beta$ over $\mathbb{F}_2$. The code $\mathcal{C}$ is called a **double cyclic code** of length (α, β) if any

$$(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathcal{C}$$

implies the cyclic shift

$$(a_{\alpha-1}, a_0, \dots, a_{\alpha-2}; b_{\beta-1}, b_0, \dots, b_{\beta-2}) \in \mathcal{C}.$$

The code $\mathcal{C}$ is called **separable** if $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$, where $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ are the coordinate projections of $\mathcal{C}$ on the first α and the last β coordinates, respectively.

From the above definition, we can see that the double cyclic code $\mathcal{C}$ can be viewed as an $\mathbb{F}_2$ -submodule of $\mathbb{F}_2^\alpha \times \mathbb{F}_2^\beta$.

The double cyclic code seems to be similar to the cyclic code. But there is a difference and this distinction is interesting. One difference is a linear code over $\mathbb{F}_2$, which is not a cyclic code over $\mathbb{F}_2$ but a double cyclic code over $\mathbb{F}_2$.

Example 2.4.16. Let $\mathcal{C} = \{(0, 0, 0), (0, 1, 0), (0, 0, 1), (0, 1, 1)\}$ be a linear code of length 3 over $\mathbb{F}_2$. We can see that a shift of codeword $(0, 0, 1)$ is not an element in $\mathcal{C}$. Then, $\mathcal{C}$ is not a cyclic code of length 3 over $\mathbb{F}_2$.

If we partition the length of the code $\mathcal{C}$ into 2 parts, that is, $\alpha = 1$ and $\beta = 2$, we get the new code

$$\mathcal{C}' = \{(0; 0, 0), (0; 1, 0), (0; 0, 1), (0; 1, 1)\}.$$

Hence, we see that both parts of codewords in $\mathcal{C}'$ are invariant under cyclic shift. Therefore, $\mathcal{C}'$ is a double cyclic code of length $(1, 2)$ over $\mathbb{F}_2$.

Example 2.4.17. The following are double cyclic codes over $\mathbb{F}_2$:

1. $\mathcal{C}_1 = \{(0, 0; 0, 0, 0), (1, 1; 0, 0, 0), (1, 0; 1, 1, 1), (0, 1; 1, 1, 1)\}$ is a double cyclic code of length $(2, 3)$;
2. $\mathcal{C}_2 = \{(0, 0, 0; 0, 0, 0), (0, 1, 1; 1, 0, 1), (1, 0, 1; 1, 1, 0), (1, 1, 1; 0, 0, 0), (0, 1, 0; 1, 1, 0), (0, 0, 1; 0, 1, 1), (1, 0, 0; 1, 0, 1), (1, 1, 0; 0, 1, 1)\}$ is a double cyclic code of length $(3, 3)$.

Similar to the study of the algebraic structure of cyclic codes in Section 2.4, for any element $\mathbf{v} = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathbb{F}_2^\alpha \times \mathbb{F}_2^\beta$, we obtain that $\mathbf{v}$ can be identified with an element in $\frac{\mathbb{F}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^\beta - 1 \rangle}$ as follows:

$$\mathbf{v}(x) = (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1}) = (a(x); b(x)).$$

The polynomial $\mathbf{v}(x)$ is called **polynomial representation** of $\mathbf{v}$. This identification provides a one-to-one correspondence between $\mathbb{F}_2^\alpha \times \mathbb{F}_2^\beta$ and $\frac{\mathbb{F}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^\beta - 1 \rangle}$.

Definition 2.4.18. [21] Let $R_{\alpha, \beta} = \frac{\mathbb{F}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^\beta - 1 \rangle}$. Then, the operation $*$ between $\mathbb{F}_2[x]$ and $R_{\alpha, \beta}$ is defined as follows

$$k(x) * (a(x); b(x)) = (k(x)a(x) \pmod{x^\alpha - 1}; k(x)b(x) \pmod{x^\beta - 1}),$$

where $k(x) \in \mathbb{F}_2[x]$ and $\mathbf{v}(x) = (a(x); b(x)) \in R_{\alpha, \beta}$.

Therefore, the additive abelian group $\frac{\mathbb{F}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^\beta - 1 \rangle}$ is an $\mathbb{F}_2[x]$ -module with respect to the usual addition and multiplication $*$.

Moreover, let $\mathbf{v} = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1})$ be an element in $\mathbb{F}_2^\alpha \times \mathbb{F}_2^\beta$ and $\mathbf{v}(x) = (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1})$ be the polynomial representation of $\mathbf{v}$ in $\frac{\mathbb{F}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^\beta - 1 \rangle}$. Consider,

$$\begin{aligned} x * \mathbf{v}(x) &= x * (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1}) \\ &= (a_{\alpha-1} + a_0x + \dots + a_{\alpha-2}x^{\alpha-1}; b_{\beta-1} + b_0x + \dots + b_{\beta-2}x^{\beta-1}). \end{aligned}$$

We can see that $x * \mathbf{v}(x)$ represents the element $(a_{\alpha-1}, a_0, \dots, a_{\alpha-2}; b_{\beta-1}, b_0, \dots, b_{\beta-2})$ in $\mathbb{F}_2^\alpha \times \mathbb{F}_2^\beta$. This implies that $x * \mathbf{v}(x)$ is a polynomial representation of a shift of codeword $\mathbf{v}$. Therefore, the double cyclic code $\mathcal{C}$ of length (α, β) over $\mathbb{F}_2$ can be viewed as an $\mathbb{F}_2[x]$ -submodule of $\frac{\mathbb{F}_2[x]}{\langle x^\alpha - 1 \rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^\beta - 1 \rangle}$.

Since then, many researchers have used the concept to study the algebraic

structure of double cyclic codes by expanding the code alphabet into finite fields or finite rings [22–26]. In this thesis, we will apply the concept of double cyclic codes by using the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ as the code alphabet.

2.4.2 DNA codes

DNA is a linear molecule consisting of four different nucleotide bases: Adenine (A), Thymine (T), Guanine (G) and Cytosine (C). DNA has a double helix structure, consisting of two long strands twisting around each other. The **Watson-Crick complement rule (WCC)** states that the two DNA strands are bound together by chemical connections between the bases, i.e. A bonds with T and C bonds with G . Furthermore, each strand of DNA has an ordered quaternary sequence of the letters A, T, G and C , with two different ends known as the 5' and 3' ends, as shown in Figure 2.

Example 2.4.19. For instance, the strand of $5' - AGCTATC - 3'$ is paired with $3' - TCGATAG - 5'$ as shown in Figure 6.

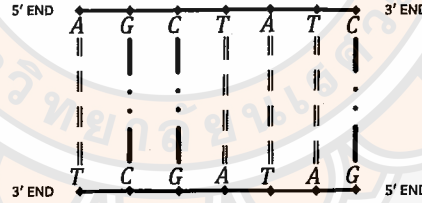


Figure 6 A paring of two DNA strands in Example 2.4.19

Let $S_{\mathcal{D}_4} = \{A, T, G, C\}$ be a set of DNA alphabets. For any $y \in S_{\mathcal{D}_4}$, we denote the complement of y as $\bar{y}$, i.e.,

$$\bar{A} = T, \bar{T} = A, \bar{G} = C \text{ and } \bar{C} = G.$$

A DNA code $\mathcal{D}$ of length n is a set of sequences $\mathbf{a} = a_0 a_1 \cdots a_{n-1}$, where $a_i \in S_{\mathcal{D}_4}$ for $i \in \{0, 1, \dots, n-1\}$ and have the same direction ($5' \rightarrow 3'$).

Example 2.4.20. From the Example 2.4.19, the words

AGCTATC and GATAGCT

represent the DNA strands

$$5' - AGCTATC - 3' \text{ and } 5' - GATAGCT - 3',$$

respectively. Then, we can rewrite the DNA double helix in the form of a DNA code $\mathcal{D}$ as

$$\mathcal{D} = \{AGCTATC, GATAGCT\}.$$

By the basic concept of coding theory in Section 2.4, the DNA code $\mathcal{D}$ can be viewed as a code of length 7 over the alphabet $S_{\mathcal{D}_4}$. More generally, let $\mathcal{D}$ be a DNA code of length n over $S_{\mathcal{D}_4}$. Then, for each word $\mathbf{a} = a_0a_1 \cdots a_{n-1} \in S_{\mathcal{D}_4}^n$,

- the **reverse** of $\mathbf{a}$ is $\mathbf{a}^r = a_{n-1}a_{n-2} \cdots a_0$,
- the **complement** of $\mathbf{a}$ is $\mathbf{a}^c = \bar{a}_0\bar{a}_1 \cdots \bar{a}_{n-1}$, where the complement of each element a_i corresponds to WCC and
- the **reverse-complement** of $\mathbf{a}$ is $\mathbf{a}^{rc} = \bar{a}_{n-1}\bar{a}_{n-2} \cdots \bar{a}_0$.

Example 2.4.21. From the Example 2.4.20, we have a DNA code

$$\mathcal{D} = \{AGCTATC, GATAGCT\}.$$

Suppose that $\mathbf{a} = AGCTATC$. Hence,

$$\mathbf{a}^r = CTATCGA$$

$$\mathbf{a}^{rc} = \overline{CTATCGA} = GATAGCT.$$

Therefore, we observe that $\mathbf{a}, \mathbf{a}^{rc} \in \mathcal{D}$.

Recall that the Hamming distance between words $\mathbf{a}$ and $\mathbf{b}$, denoted by $d_H(\mathbf{a}, \mathbf{b})$, is simply the number of coordinates in which these two words differ. In [33], the authors provided four combinatorial constraints of a good DNA code $\mathcal{D}$ and a code that satisfies some or all of the conditions below is said to be a DNA code:

1. **Hamming distance constraint:** For any $\mathbf{a}, \mathbf{b} \in \mathcal{D}$ with $\mathbf{a} \neq \mathbf{b}$, $d_H(\mathbf{a}, \mathbf{b}) \geq d$ for some prescribed minimum distance d .
2. **Reverse constraint:** For any $\mathbf{a}, \mathbf{b} \in \mathcal{D}$ (including $\mathbf{a} = \mathbf{b}$), $d_H(\mathbf{a}, \mathbf{b}^r) \geq d$ for some prescribed minimum distance d . For example, let $\mathbf{a} = \mathbf{b} = ATCCG$, $\mathbf{b}^r = GCCTA$. Then, $d_H(\mathbf{a}, \mathbf{b}^r) = 4$.
3. **Reverse-complement constraint:** For any $\mathbf{a}, \mathbf{b} \in \mathcal{D}$ (including $\mathbf{a} = \mathbf{b}$), $d_H(\mathbf{a}, \mathbf{b}^{rc}) \geq d$ for some prescribed minimum distance d . For example, let $\mathbf{a} = \mathbf{b} = ATCCG$, $\mathbf{b}^{rc} = CGGAT$. Then, $d_H(\mathbf{a}, \mathbf{b}^{rc}) = 5$.
4. **Fixed GC-content constraint:** This constraint means that each codeword in $\mathcal{D}$ has the same number of G or C entries. For example,

$$\mathcal{D} = \{TGTG, CACA, GTTG, CAAC\}.$$

Then, the same number of G and C in $\mathcal{D}$ is 2.

This thesis focuses on a special constraint of a DNA code $\mathcal{D}$, which is reverse-complement constraint. It means that for every $\mathbf{a}, \mathbf{b} \in \mathcal{D}$, $d_H(\mathbf{a}, \mathbf{b}^{rc}) \geq d$, including $\mathbf{a} = \mathbf{b}$, where d is a specified minimum distance.

In [38] and [39], the authors gave a one-to-one correspondence ϕ between the elements of $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and $S_{\mathcal{D}_4}$ as

$$\phi(0) = A, \phi(1) = G, \phi(u) = T \text{ and } \phi(1+u) = C.$$

According to the linking in the DNA bases, we obtain that

$$\bar{0} = u, \bar{1} = 1 + u, \bar{u} = 0 \text{ and } \overline{1+u} = 1.$$

In [38] and [39], the authors expanded the map ϕ so that $\phi(\mathcal{C})$ can be viewed as a DNA code for a code $\mathcal{C}$ of length n over $\mathbb{F}_2 + u\mathbb{F}_2$.

Example 2.4.22. Let

$$\mathcal{C} = \{(0, 1, 1+u, u, 0, u, 1+u), (1, 0, u, 0, 1, 1+u, u)\} = \{\mathbf{a}, \mathbf{b}\}$$

be a code of length 7 over $\mathbb{F}_2 + u\mathbb{F}_2$. Then,

$$\phi(\mathbf{a}) = AGCTATC \text{ and } \phi(\mathbf{b}) = GATAGCT.$$

Let $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ be a codeword in a code C of length n over $\mathbb{F}_2 + u\mathbb{F}_2$. The reverse (respectively, complement, reverse-complement) of $\mathbf{a}$ is denoted by

$$\mathbf{a}^r = (a_{n-1}, a_{n-2}, \dots, a_0)$$

(respectively, $\mathbf{a}^c = (\bar{a}_0, \bar{a}_1, \dots, \bar{a}_{n-1})$, $\mathbf{a}^{rc} = (\bar{a}_{n-1}, \bar{a}_{n-2}, \dots, \bar{a}_0)$). From Example 2.4.22, we observe that $\mathbf{a}^{rc} = \mathbf{b}$.

Definition 2.4.23. [38] A linear code C of length n over $\mathbb{F}_2 + u\mathbb{F}_2$ is called **reversible** (respectively, **complement**, **reversible-complement**) if $\mathbf{a}^r \in C$ ($\mathbf{a}^c \in C$, $\mathbf{a}^{rc} \in C$) for all $\mathbf{a} \in C$.

Next, we will provide theorems for cyclic codes to be reversible and reversible-complement codes. In [38] and [39], the authors have investigated the necessary and sufficient conditions for reversible cyclic codes of length n over $\mathbb{F}_2 + u\mathbb{F}_2$ as follows:

Theorem 2.4.24. Let n be a positive integer and C be a cyclic code of length n over $\mathbb{F}_2 + u\mathbb{F}_2$.

1. Suppose that n is odd. Then,

$C = \langle f_0(x) + uf_1(x) \rangle$ is reversible if and only if $f_0(x)$ and $f_1(x)$ are self-reciprocal.

2. Suppose that n is even and $i = \deg(g(x)) - \deg(p(x))$. Then,

(a) $C = \langle g(x) + up(x) \rangle$ is reversible if and only if

i. $g(x)$ is self-reciprocal,

ii. $x^i p^*(x) = p(x)$ or $g(x) = x^i p^*(x) + p(x)$.

(b) $C = \langle g(x) + up(x), ua(x) \rangle$ is reversible if and only if

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

ii. $a(x) \mid (x^i p^*(x) + p(x))$.

Theorem 2.4.25. Let n be a positive integer, $u\mathbb{I}(x) = u + ux + \dots + ux^{n-1}$ and C be a cyclic code of length n over $\mathbb{F}_2 + u\mathbb{F}_2$. Then,

1. Suppose that n is odd. Then,

$\mathcal{C} = \langle f_0(x) + u f_1(x) \rangle$ is reversible-complement if and only if $u\mathbb{I}(x) \in \mathcal{C}$, $f_0(x)$ and $f_1(x)$ are self-reciprocal.

2. Suppose that n is even and $i = \deg(g(x)) - \deg(p(x))$. Then,

(a) $\mathcal{C} = \langle g(x) + up(x) \rangle$ is reversible-complement if and only if

- i. $u\mathbb{I}(x) \in \mathcal{C}$ and $g(x)$ is self-reciprocal,
- ii. $x^i p^*(x) = p(x)$ or $g(x) = x^i p^*(x) + p(x)$.

(b) $\mathcal{C} = \langle g(x) + up(x), ua(x) \rangle$ is reversible-complement if and only if

- i. $u\mathbb{I}(x) \in \mathcal{C}$, $g(x)$ and $a(x)$ are self-reciprocal,
- ii. $a(x) \mid (x^i p^*(x) + p(x))$.

The following examples are cyclic codes over the ring R , which are reversible-complement codes derived from the above theorems:

Example 2.4.26. Let $n = 9$. Consider,

$$x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1) \in \mathbb{F}_2[x].$$

Suppose that

$$\mathcal{C} = \langle (x^2 + x + 1)(x^6 + x^3 + 1) + u(x^6 + x^3 + 1) \rangle$$

is a cyclic code of length 9 over $\mathbb{F}_2 + u\mathbb{F}_2$. By Theorem 2.4.24, we obtain that $\mathcal{C}$ is a reversible code. Since

$$u\mathbb{I}(x) = u((x^2 + x + 1)(x^6 + x^3 + 1) + u(x^6 + x^3 + 1)) \in \mathcal{C},$$

by Theorem 2.4.25, $\mathcal{C}$ is reversible-complement. Then, a DNA code $\mathcal{D}$ of length 9 with $d(\mathcal{D}) = 3$ from $\mathcal{C}$ has 16 codewords, which is given in Table 4.

Table 4 A DNA code $\mathcal{D}$ of length 9 from $\mathcal{C}$ in Example 2.4.26

AATAATAAT	TAATAATAA	ATTATTATT	CGCCGCCGC
TTTTTTTTT	AAAAAAAAA	CGGCGGCGG	TTATTATTA
ATAATAATA	CCCCCCCCC	GGCGGCGGC	GCCGCCGCC
GCGGCGGCG	TATTATTAT	CCGCCGCCG	GGGGGGGGG

Example 2.4.27. From Example 2.4.14,

$$\mathcal{C}_1 = \langle (x+1)(x^2+x+1)^2 + u(x^2+x+1)^2 \rangle$$

and

$$\mathcal{C}_2 = \langle (x+1)(x^2+x+1)^2 + u(x^2+x+1), u(x+1)(x^2+x+1) \rangle$$

are a cyclic code of length 6 over $\mathbb{F}_2 + u\mathbb{F}_2$. By Theorem 2.4.24 and 2.4.25, we obtain that $\mathcal{C}_1$ and $\mathcal{C}_2$ are reversible-complement codes. Then, DNA codes $\mathcal{D}_1$ and $\mathcal{D}_2$ of length 6 from $\mathcal{C}_1$ and $\mathcal{C}_2$ have 4 and 64 codewords, which are given in Tables 5 and 6, respectively. Moreover, $d(\mathcal{D}_1) = 6$, $d(\mathcal{D}_2) = 2$.

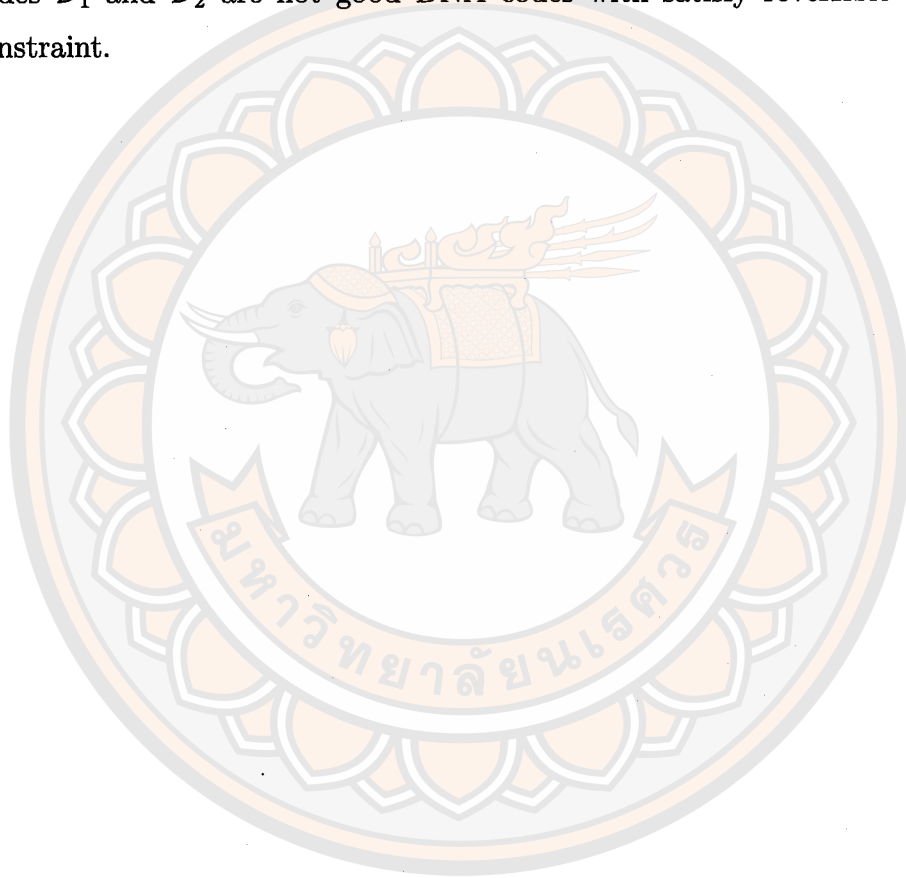
Table 5 A DNA code $\mathcal{D}_1$ of length 6 from $\mathcal{C}_1$ in Example 2.4.27

AAAAA	CGCGCG	TTTTTT	GCGCGC
-------	--------	--------	--------

Table 6 A DNA code $\mathcal{D}_2$ of length 6 from $\mathcal{C}_2$ in Example 2.4.27

AAAAAA	CGCCGG	CGGCGC	CCGCGG
CCCGGG	CGGCCG	CGCGCG	CCGGGG
CGGGCC	CCGGCG	CGCGGC	CCCCGC
CGCCCC	CCCCCG	CCGCCC	CCCGCC
GGGCGG	GGCGGG	GGGGGC	GCGGGG
GGGGCG	TTTTTT	ATTTTA	ATTTAT
ATTATT	ATATTT	AATTTT	GGCCCG
GCCCGG	GGCCCG	GCGCGC	GCGCCG
GGGCCC	GGCGCC	GCCGCG	GCGGCC
GCCGGC	TTTTAA	TTTATA	TTTAAT
TTATAT	TTAATT	TATATT	TAATTT
TTATTA	ATTAAA	ATATAA	TATTTA
TATTAT	AATTAA	AATATA	AAATTA
ATAATA	AAAATT	AAATAT	AATAAT
ATAAAT	CGGGGG	GCCCCC	TTAAAA
TATAAA	TAATAA	TAAATA	TAAAAT

Let n be a positive integer, $\mathcal{D}$ be a DNA code of length n and $\mathbf{a} \in \mathcal{D}$. From the above examples, we observe that $\mathbf{a}^{rc} \neq \mathbf{a}$ when n is odd. If n is even, $\mathbf{a}^{rc} = \mathbf{a}$ may occur. Therefore, a cyclic code $\mathcal{C}$ of odd length n can generate a good DNA code. However, for even length n , a cyclic code $\mathcal{C}$ can generate a suitable DNA code by considering the condition in which no strand in the code equals its reverse-complement. In addition, in Example 2.4.27, since a codeword $\mathbf{a} = CGCGCG = \mathbf{a}^{rc} \in \mathcal{D}_1$ and a codeword $\mathbf{b} = GGGCCC = \mathbf{b}^{rc} \in \mathcal{D}_2$, the DNA codes $\mathcal{D}_1$ and $\mathcal{D}_2$ are not good DNA codes with satisfy reversible-complement constraint.



CHAPTER III

DOUBLE CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$

Let R be the ring $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$. This chapter investigates the algebraic structure of double cyclic codes of length (α, β) over R , organized into 3 sections based on the types of lengths α and β .

In the first section, we have provided the concept of double cyclic codes over R , where α and β are non-negative integers. We introduce the concept of double cyclic codes over R , where α and β are non-negative integers. The second section investigates the algebraic structure of double cyclic codes over R for odd positive integers α and β . The last section examines the case where α is an odd positive integer and β is an even positive integer. Additionally, examples of double cyclic DNA codes are provided in Sections 3.2 and 3.3, with the corresponding codewords included in the appendix.

3.1 Double cyclic codes of length (α, β) over $\mathbb{F}_2 + u\mathbb{F}_2$

In this section, we will give the concept of double cyclic codes of length (α, β) over R , where both α, β are non-negative integers. Let α and β be two non-negative integers and $n = \alpha + \beta$. Define $\psi : R^n \rightarrow R^\alpha \times R^\beta$ by

$$\psi(a_0, a_1, \dots, a_{n-1}) = (a_0, a_1, \dots, a_{\alpha-1}; a_\alpha, a_{\alpha+1}, \dots, a_\beta)$$

for all $(a_0, a_1, \dots, a_{n-1}) \in R^n$. Hence, ψ is an R -homomorphism. Then, R^n and $R^\alpha \times R^\beta$ are isomorphism. Then, for any linear code $\mathcal{C}$ of length n over R , $\psi(\mathcal{C}) \subseteq R^\alpha \times R^\beta$. Since ψ is an R -homomorphism and $\mathcal{C}$ is linear code, $\psi(\mathcal{C})$ is an R -submodule of $R^\alpha \times R^\beta$. Similarly to the definition of double cyclic codes over $\mathbb{Z}_2$ in Section 2.4.1, the double cyclic codes of length (α, β) over the ring R is defined as follows:

Definition 3.1.1. A linear code $\mathcal{C}$ of length $n = \alpha + \beta$ over R is called a **double cyclic code** of length (α, β) over R if

$$(a_{\alpha-1}, a_0, \dots, a_{\alpha-2}; b_{\beta-1}, b_0, \dots, b_{\beta-2}) \in \mathcal{C}$$

for all $(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathcal{C}$.

The code $\mathcal{C}$ is called **separable** if $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$, where $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ are the coordinate projections of $\mathcal{C}$ on the first α and the last β coordinates, respectively.

Example 3.1.2. Let

$$\begin{aligned} \mathcal{C} = \{ & (0, 0, 0; 0, 0, 0), (0, u, u; 0, 0, 0), (u, 0, u; 0, 0, 0), (u, u, 0; 0, 0, 0), \\ & (0, 0, u; u, u, u), (u, 0, 0; u, u, u), (0, u, 0; u, u, u), (u, u, u; u, u, u) \} \end{aligned}$$

be a subset of $R^3 \times R^3$. It is easy to see that $\mathcal{C}$ is a double cyclic code of length $(3, 3)$ over R . Furthermore, we obtain that

$$\begin{aligned} \mathcal{C}_\alpha &= \{(0, 0, 0), (0, u, u), (u, 0, u), (u, u, 0), (0, 0, u), (u, 0, 0), (0, u, 0), (u, u, u)\}, \\ \mathcal{C}_\beta &= \{(0, 0, 0), (u, u, u)\}. \end{aligned}$$

Consider,

$$\begin{aligned} \mathcal{C}_\alpha \times \mathcal{C}_\beta = \{ & (0, 0, 0; 0, 0, 0), (0, u, u; 0, 0, 0), (u, 0, u; 0, 0, 0), (u, u, 0; 0, 0, 0), \\ & (0, 0, u; 0, 0, 0), (u, 0, 0; 0, 0, 0), (0, u, 0; 0, 0, 0), (u, u, u; 0, 0, 0), \\ & (0, 0, 0; u, u, u), (u, u, u; u, u, u), (u, 0, u; u, u, u), (u, u, 0; u, u, u), \\ & (0, 0, u; u, u, u), (u, 0, 0; u, u, u), (0, u, 0; u, u, u), (u, u, u; u, u, u) \}. \end{aligned}$$

We obtain that $\mathcal{C} \neq \mathcal{C}_\alpha \times \mathcal{C}_\beta$. Therefore, $\mathcal{C}$ is not separable.

Example 3.1.3. Let

$$\begin{aligned} \mathcal{C} = \{ & (0, 0, 0; 0, 0, 0, 0), (0, 0, 0; u, u, u, u), (0, 0, 0; 1, 1 + u, 1, 1 + u), \\ & (0, 0, 0; 1 + u, 1, 1 + u, 1), (u, u, u; 0, 0, 0, 0), (u, u, u; u, u, u, u), \\ & (u, u, u; 1, 1 + u, 1, 1 + u), (u, u, u; 1 + u, 1, 1 + u, 1) \} \end{aligned}$$

be a subset of $R^3 \times R^4$. It is easy to see that $\mathcal{C}$ is a double cyclic code of length $(3, 4)$ over R . Furthermore, we obtain that

$$\begin{aligned} \mathcal{C}_\alpha &= \{(0, 0, 0), (u, u, u)\}, \\ \mathcal{C}_\beta &= \{(0, 0, 0, 0), (u, u, u, u), (1, 1 + u, 1, 1 + u), (1 + u, 1, 1 + u, 1)\}. \end{aligned}$$

Consider,

$$\mathcal{C}_\alpha \times \mathcal{C}_\beta = \{(0, 0, 0; 0, 0, 0, 0), (0, 0, 0; u, u, u, u), (0, 0, 0; 1, 1 + u, 1, 1 + u),$$

$$(0, 0, 0; 1 + u, 1, 1 + u, 1), (u, u, u; 0, 0, 0, 0), (u, u, u; u, u, u, u), \\ (u, u, u; 1, 1 + u, 1, 1 + u), (u, u, u; 1 + u, 1, 1 + u, 1)\}.$$

Hence, $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$. Therefore, $\mathcal{C}$ is a separable code.

In order to convert the combinatorial structure of double cyclic codes into an algebraic one, we consider the following mapping:

$$\tau : R^\alpha \times R^\beta \rightarrow \frac{R[x]}{\langle x^\alpha - 1 \rangle} \times \frac{R[x]}{\langle x^\beta - 1 \rangle},$$

$$(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \mapsto (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1}).$$

Hence, τ is an R -homomorphism. For simplicity, we let

$$\mathbf{v}(x) = (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1}) = (a(x); b(x)).$$

For any $\mathbf{v} = (\mathbf{a}, \mathbf{b}) = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1})$ in $R^\alpha \times R^\beta$, the polynomial $\mathbf{v}(x) = (a(x); b(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle} \times \frac{R[x]}{\langle x^\beta - 1 \rangle}$ is called **polynomial representation** of $\mathbf{v}$. We denote the additive abelian group $\frac{R[x]}{\langle x^\alpha - 1 \rangle} \times \frac{R[x]}{\langle x^\beta - 1 \rangle}$ by $R_{\alpha, \beta}$.

Similarly to the Definition 2.4.18, for any polynomial $k(x)$ in $R[x]$ and polynomial $\mathbf{v}(x) = (a(x); b(x))$ in $R_{\alpha, \beta}$, the multiplication of $k(x)$ and $\mathbf{v}(x)$ is defined as follows:

$$k(x) * \mathbf{v}(x) = (k(x)a(x) \pmod{x^\alpha - 1}; k(x)b(x) \pmod{x^\beta - 1}).$$

Therefore, the additive abelian group $R_{\alpha, \beta}$ is an $R[x]$ -module with respect to the usual addition and multiplication $*$. Throughout this thesis, we will use

$$k(x) * \mathbf{v}(x) = (k(x)a(x); k(x)b(x))$$

instead of $k(x) * \mathbf{v}(x) = (k(x)a(x) \pmod{x^\alpha - 1}; k(x)b(x) \pmod{x^\beta - 1})$.

Moreover, for any $\mathbf{v} = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1})$ in $R^\alpha \times R^\beta$ with polynomial representation $\mathbf{v}(x) = (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1})$ of $\mathbf{v}$, we obtain that

$$x * \mathbf{v}(x) = (a_{\alpha-1} + a_0x + \dots + a_{\alpha-2}x^{\alpha-1}; b_{\beta-1} + b_0x + \dots + b_{\beta-2}x^{\beta-1}).$$

Hence, $x * \mathbf{v}(x)$ is the polynomial representation of $(a_{\alpha-1}, a_0, \dots, a_{\alpha-2}; b_{\beta-1}, b_0, \dots, b_{\beta-2})$.

Theorem 3.1.4. *A linear code $\mathcal{C}$ of length $n = \alpha + \beta$ over R is a double cyclic code of length (α, β) over R if and only if $\tau(\mathcal{C})$ is an $R[x]$ -submodule of $R_{\alpha, \beta}$.*

Proof. Suppose that $\mathcal{C}$ is a double cyclic code of length (α, β) over R . Then, $\mathcal{C}$ is an R -submodule of $R^\alpha \times R^\beta$ and so $\tau(\mathcal{C})$ is a subgroup of $R_{\alpha, \beta}$. Let

$$\begin{aligned} v(x) &= (a(x); b(x)) \\ &= (a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1}) \text{ in } \tau(\mathcal{C}). \end{aligned}$$

By setting $v = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathcal{C}$ then $\tau(v) = v(x)$. Since $\mathcal{C}$ is a double cyclic code, the polynomial $x * v(x)$ is also an element of $\tau(\mathcal{C})$. Thus, $x^2 * v(x) = x * (x * v(x))$ is an element of $\tau(\mathcal{C})$. By induction, we have $x^i * v(x) \in \tau(\mathcal{C})$ for all $i \geq 0$. Hence, for any polynomial $r(x) = r_0 + r_1x + \cdots + r_kx^k \in R[x]$ with non-negative integer k , we consider

$$\begin{aligned} r(x) * v(x) &= (r_0 + r_1x + \cdots + r_kx^k) * v(x) \\ &= (r_0 * v(x)) + (r_1x * v(x)) + \cdots + (r_kx^k * v(x)). \end{aligned}$$

Since $\mathcal{C}$ is a linear code, we have $r * v \in \mathcal{C}$ for all $r \in R$ and $v \in \mathcal{C}$. This implies that $r(x) * v(x) \in \tau(\mathcal{C})$. Therefore, $\tau(\mathcal{C})$ is an $R[x]$ -submodule of $R_{\alpha, \beta}$.

On the other hand, we suppose that $\tau(\mathcal{C})$ is an $R[x]$ -submodule of $R_{\alpha, \beta}$. Let $v = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1})$ be a codeword in $\mathcal{C}$. Then,

$$\tau(v) = (a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1}) \in \tau(\mathcal{C}).$$

By assumption,

$$x * \tau(v) = (a_{\alpha-1} + a_0x + \cdots + a_{\alpha-2}x^{\alpha-1}; b_{\beta-1} + b_0x + \cdots + b_{\beta-2}x^{\beta-1}) \in \tau(\mathcal{C}).$$

Hence, $(a_{\alpha-1}, a_0, \dots, a_{\alpha-2}; b_{\beta-1}, b_0, \dots, b_{\beta-2}) \in \mathcal{C}$. Therefore, $\mathcal{C}$ is a double cyclic code of length (α, β) over R . $\square$

By the above theorem, a double cyclic code $\mathcal{C}$ of length (α, β) over R can be viewed as an $R[x]$ -submodule of $R_{\alpha, \beta}$. From now on, we replace $\tau(\mathcal{C})$ of the double cyclic code $\mathcal{C}$ with $\mathcal{C}$.

Let $\mathcal{C}$ be an $R[x]$ -submodule of $R_{\alpha, \beta}$. We define $\tau_\alpha : \mathcal{C} \rightarrow \frac{R[x]}{\langle x^\alpha - 1 \rangle}$ by

$$\tau_\alpha(a(x); b(x)) = a(x) \pmod{x^\alpha - 1} \quad (3.1.1)$$

for each $(a(x); b(x)) \in \mathcal{C} \subseteq R_{\alpha, \beta}$ and define $\tau_\beta : \mathcal{C} \rightarrow \frac{R[x]}{\langle x^\beta - 1 \rangle}$ by

$$\tau_\beta(a(x); b(x)) = b(x) \pmod{x^\beta - 1} \quad (3.1.2)$$

for each $(a(x); b(x)) \in \mathcal{C} \subseteq R_{\alpha, \beta}$. Therefore, τ_α and τ_β are $R[x]$ -homomorphism. The next sections will investigate the generator polynomials of a double cyclic code $\mathcal{C}$ of length (α, β) over R , by separating the study by the types of lengths α, β . Note that, for any $f(x)$ in $R[x]$, the polynomial $f(x)$ can be written as $f(x) = f_0(x) + uf_1(x)$, where $f_0(x), f_1(x) \in \mathbb{F}_2[x]$.

3.2 The case α and β are both odd positive integers

In this section, we will study the algebraic structure of double cyclic codes of length (α, β) over R , where both α and β are odd positive integers. Throughout this section, we let α, β be both odd positive integers.

The following theorem is used to determine the generator polynomials for double cyclic codes of length (α, β) over R :

Theorem 3.2.1. *Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . Then,*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle,$$

for some polynomials $f_0(x), f_1(x), g_0(x), g_1(x) \in \mathbb{F}_2[x]$ with $f_1(x) \mid f_0(x) \mid (x^\alpha - 1)$, $g_1(x) \mid g_0(x) \mid (x^\beta - 1)$ and for some $l(x) \in R[x]$ with $(l(x); g_0(x) + ug_1(x)) \in \mathcal{C}$.

Proof. Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . By Theorem 3.1.4, we have $\mathcal{C}$ is an $R[x]$ -submodule of $R_{\alpha, \beta}$. We claim that $\tau_\beta(\mathcal{C})$, which is defined as (3.1.2), is an ideal of $\frac{R[x]}{\langle x^\beta - 1 \rangle}$. Let $b(x), b'(x) \in \tau_\beta(\mathcal{C})$. Then, there exist $(a(x); b(x)), (a'(x); b'(x)) \in \mathcal{C}$ such that $b(x) = \tau_\beta(a(x); b(x))$ and $b'(x) = \tau_\beta(a'(x); b'(x))$. Consider

$$b(x) - b'(x) = \tau_\beta(a(x); b(x)) - \tau_\beta(a'(x); b'(x)) = \tau_\beta((a(x); b(x)) - (a'(x); b'(x))).$$

Since $\mathcal{C}$ is an $R[x]$ -submodule of $R_{\alpha, \beta}$, $(a(x); b(x)) - (a'(x); b'(x)) \in \mathcal{C}$ and so $b(x) - b'(x) \in \tau_\beta(\mathcal{C})$. Hence, $\tau_\beta(\mathcal{C})$ is an additive subgroup of $\frac{R[x]}{\langle x^\beta - 1 \rangle}$.

Next, let $k(x) \in \frac{R[x]}{\langle x^\beta - 1 \rangle}$ and $b(x) \in \tau_\beta(\mathcal{C})$. Then, there is $a(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle}$ such that $(a(x); b(x)) \in \mathcal{C}$. Since $k(x)$ is a residue class modulo $x^\beta - 1$, $k(x)$ can be viewed as a polynomial over R with $\deg(k(x)) < \beta$. Consider,

$$k(x) * (a(x); b(x)) = (k(x)a(x); k(x)b(x)) \in \mathcal{C}.$$

Hence, $k(x)b(x) \in \tau_\beta(\mathcal{C})$ and we get the claim. Since $\tau_\beta(\mathcal{C})$ is an ideal of $\frac{R[x]}{\langle x^\beta - 1 \rangle}$ and β is odd, by Theorem 2.4.12 (1), we obtain that

$$\tau_\beta(\mathcal{C}) = \langle g_0(x) + ug_1(x) \rangle$$

for some $g_0(x), g_1(x) \in \mathbb{F}_2[x]$ with $g_1(x) \mid g_0(x) \mid (x^\beta - 1)$. Hence, there is $l(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle}$ such that $(l(x); g_0(x) + ug_1(x)) \in \mathcal{C}$. Note that

$$\ker(\tau_\beta) = \{(a(x); 0) \in \mathcal{C} : a(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle}\}.$$

Define a set $I = \{a(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle} : (a(x); 0) \in \ker(\tau_\beta)\} \subseteq \frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Let $a(x), a'(x) \in I$. Then, $(a(x); 0), (a'(x); 0) \in \ker(\tau_\beta)$. Since $\ker(\tau_\beta)$ is a $R[x]$ -submodule of $\mathcal{C}$, we have $(a(x) - a'(x); 0) = (a(x); 0) - (a'(x); 0) \in \ker(\tau_\beta)$ and so $a(x) - a'(x) \in I$. Hence, I is an additive subgroup of $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Next, let $k'(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle}$ and $a(x) \in I$. Then, $(a(x); 0) \in \ker(\tau_\beta)$. Since $k'(x)$ is a residue class modulo $x^\alpha - 1$, $k'(x)$ can be viewed as a polynomial over R with $\deg(k'(x)) < \alpha$. Since $\ker(\tau_\beta)$ is a $R[x]$ -submodule of $\mathcal{C}$, we obtain that

$$k'(x) * (a(x); 0) = (k'(x)a(x); 0) \in \ker(\tau_\beta).$$

Hence, $k'(x)a(x) \in I$ and so I is an ideal of $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. By Theorem 2.4.12 (1), $I = \langle f_0(x) + uf_1(x) \rangle$ for some $f_0(x), f_1(x) \in \mathbb{F}_2[x]$ with $f_1(x) \mid f_0(x) \mid (x^\alpha - 1)$. For any $(a(x); 0) \in \ker(\tau_\beta)$, we have $a(x) \in I$ and then there exists $k(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle}$ such that $a(x) = k(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}$. Hence,

$$\begin{aligned} (a(x); 0) &= (k(x)(f_0(x) + uf_1(x)); 0) \\ &= k(x) * (f_0(x) + uf_1(x); 0) \in \langle (f_0(x) + uf_1(x); 0) \rangle. \end{aligned}$$

Thus, $\ker(\tau_\beta) \subseteq \langle (f_0(x) + uf_1(x); 0) \rangle$. This implies that

$$\ker(\tau_\beta) = \langle (f_0(x) + uf_1(x); 0) \rangle.$$

By Fundamental homomorphism theorem,

$$\mathcal{C}/\ker(\tau_\beta) \cong \tau_\beta(\mathcal{C}) = \langle g_0(x) + ug_1(x) \rangle.$$

Next, we will show that $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$. For any $v(x) = (a(x); b(x)) \in \mathcal{C}$, we have $b(x) = \tau_\beta(v(x)) \in \tau_\beta(\mathcal{C})$. Then, we have $b(x) = k_1(x)(g_0(x) + ug_1(x)) \pmod{x^\beta - 1}$ for some $k_1(x) \in \frac{R[x]}{\langle x^\beta - 1 \rangle}$. Consider,

$$\begin{aligned} (a(x); b(x)) - [k_1(x) * (l(x); g_0(x) + ug_1(x))] \\ = (a(x) - k_1(x)l(x); b(x) - k_1(x)(g_0(x) + ug_1(x))) \\ = (a(x) - k_1(x)l(x); 0) \in \ker(\tau_\beta). \end{aligned}$$

Then, there exists $k_2(x) \in R[x]$ such that

$$(a(x) - k_1(x)l(x); 0) = k_2(x) * (f_0(x) + uf_1(x); 0).$$

So, $a(x) - k_1(x)l(x) \pmod{x^\alpha - 1} = k_2(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}$ and thus

$$\begin{aligned} v(x) &= (a(x); b(x)) \\ &= (k_2(x)(f_0(x) + uf_1(x)) + k_1(x)l(x); k_1(x)(g_0(x) + ug_1(x))) \\ &= k_2(x) * (f_0(x) + uf_1(x); 0) + k_1(x) * (l(x); g_0(x) + ug_1(x)). \end{aligned}$$

Therefore, $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$. □

Next, we will investigate a condition of the polynomial $l(x)$ derived from Theorem 3.2.1.

Lemma 3.2.2. *If $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ is a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g_0(x), g_1(x)$ satisfy Theorem 3.2.1, then we can assume that*

$$\deg(l(x)) < \deg(f_0(x) + uf_1(x)).$$

Proof. Assume that $\deg(l(x)) \geq \deg(f_0(x) + uf_1(x))$. Let $i = \deg(l(x)) - \deg(f_0(x) + uf_1(x))$ and $\mathcal{C}'$ be a double cyclic code of length (α, β) over R generated by

$$\{(f_0(x) + uf_1(x); 0(x)), (l(x) + ax^i(f_0(x) + uf_1(x)); g_0(x) + ug_1(x))\},$$

where a is the leading coefficient of $l(x)$. Obvious that $\deg(l(x) + ax^i(f_0(x) + uf_1(x)) + uf_1(x)) < \deg(l(x))$. Consider,

$$(l(x); g_0(x) + ug_1(x)) = (l(x) + ax^i(f_0(x) + uf_1(x)); g_0(x) + ug_1(x)) \\ - ax^i * (f_0(x) + uf_1(x); 0).$$

Then, $(l(x); g_0(x) + ug_1(x)) \in \mathcal{C}'$. Hence, $\mathcal{C} \subseteq \mathcal{C}'$.

On the other hand,

$$(l(x) + ax^i(f_0(x) + uf_1(x)); g_0(x) + ug_1(x)) = ax^i * (f_0(x) + uf_1(x); 0) \\ + (l(x); g_0(x) + ug_1(x)).$$

Then, $(l(x) + ax^i(f_0(x) + uf_1(x)); g_0(x) + ug_1(x)) \in \mathcal{C}$ and so $\mathcal{C}' \subseteq \mathcal{C}$. Hence, $\mathcal{C} = \mathcal{C}'$. This implies that the degree of $l(x)$ can be reduced in $\mathcal{C}$ and so we can assume that $\deg(l(x)) < \deg(f_0(x) + uf_1(x))$. $\square$

Lemma 3.2.3. *If $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ is a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g_0(x), g_1(x)$ satisfy Theorem 3.2.1, then*

$$(f_0(x) + uf_1(x)) \mid \left(\frac{x^\beta - 1}{g_1(x)}\right)l(x) \text{ in } \frac{R[x]}{\langle x^\alpha - 1 \rangle} \text{ and} \\ (f_0(x) + uf_1(x)) \mid \left(u\frac{x^\beta - 1}{g_0(x)}\right)l(x) \text{ in } \frac{R[x]}{\langle x^\alpha - 1 \rangle}.$$

Proof. We consider

$$\frac{x^\beta - 1}{g_1(x)} * (l(x); g_0(x) + ug_1(x)) = \left(\frac{x^\beta - 1}{g_1(x)}l(x); \right. \\ \left. \frac{x^\beta - 1}{g_1(x)}g_0(x) + u\frac{x^\beta - 1}{g_1(x)}g_1(x)\right) \\ = \left(\frac{x^\beta - 1}{g_1(x)}l(x); 0\right).$$

From the proof of Theorem 3.2.1, we have that

$$\ker(\tau_\beta) = \langle (f_0(x) + uf_1(x); 0) \rangle.$$

Then,

$$\left(\frac{x^\beta - 1}{g_1(x)}l(x); 0\right) \in \langle (f_0(x) + uf_1(x); 0) \rangle.$$

Hence, there is $q_1(x) \in R[x]$ such that $(\frac{x^\beta-1}{g_1(x)}l(x); 0) = q_1(x) * (f_0(x) + uf_1(x); 0)$.

So,

$$\frac{x^\beta-1}{g_1(x)}l(x) \equiv q_1(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha-1}.$$

Therefore, $(f_0(x) + uf_1(x)) \mid \frac{x^\beta-1}{g_1(x)}l(x)$ in $\frac{R[x]}{\langle x^\alpha-1 \rangle}$. In a similar process, we consider

$$\begin{aligned} u \frac{x^\beta-1}{g_0(x)} * (l(x); g_0(x) + ug_1(x)) &= (u \frac{x^\beta-1}{g_0(x)}l(x); \\ &\quad u \frac{x^\beta-1}{g_0(x)}g_0(x) + u^2 \frac{x^\beta-1}{g_0(x)}g_1(x)) \\ &= (u \frac{x^\beta-1}{g_0(x)}l(x); 0) \in \ker(\tau_\beta). \end{aligned}$$

Then, there is $q_2(x) \in R[x]$ such that $(u \frac{x^\beta-1}{g_0(x)}l(x); 0) = q_2(x) * (f_0(x) + uf_1(x); 0)$.

So,

$$u \frac{x^\beta-1}{g_0(x)}l(x) \equiv q_2(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha-1}.$$

Therefore, $(f_0(x) + uf_1(x)) \mid u \frac{x^\beta-1}{g_0(x)}l(x)$ in $\frac{R[x]}{\langle x^\alpha-1 \rangle}$. □

Recall that two polynomials $f(x), g(x) \in R[x]$ are called **coprime** if there exist $a(x), b(x) \in R[x]$ such that $f(x)a(x) + g(x)b(x) = 1$.

Corollary 3.2.4. *Suppose that $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ is a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g_0(x), g_1(x)$ satisfy Theorem 3.2.1. If $f_0(x) + uf_1(x)$ and $\frac{x^\beta-1}{g_1(x)}$ are coprime over $R[x]$, then we may assume that $l(x) = 0$.*

Proof. By Lemma 3.2.3, we obtain that

$$(\frac{x^\beta-1}{g_1(x)})l(x) = (x^\alpha-1)q_1(x) + q_2(x)(f_0(x) + uf_1(x))$$

for some $q_1(x), q_2(x) \in R[x]$. Since $f_0(x) + uf_1(x)$ and $\frac{x^\beta-1}{g_1(x)}$ are coprime, there are $a(x), b(x) \in R[x]$ such that

$$1 = (f_0(x) + uf_1(x))a(x) + \frac{x^\beta-1}{g_1(x)}b(x).$$

Multiplying both sides by $l(x)$, we have

$$l(x) = l(x)(f_0(x) + uf_1(x))a(x) + l(x)\frac{x^\beta-1}{g_1(x)}b(x)$$

$$\begin{aligned}
&= l(x)(f_0(x) + uf_1(x))a(x) + (x^\alpha - 1)q_1(x)b(x) + q_2(x)(f_0(x) + uf_1(x))b(x) \\
&\equiv \left(l(x)a(x) + q_2(x)b(x) \right) (f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.
\end{aligned}$$

This implies that

$$\begin{aligned}
(l(x); g_0(x) + ug_1(x)) &= \left(l(x)a(x) + q_2(x)b(x) \right) * (f_0(x) + uf_1(x); 0) \\
&\quad + (0; g_0(x) + ug_1(x)).
\end{aligned}$$

Since

$$\begin{aligned}
(0; g_0(x) + ug_1(x)) &= \left(l(x)a(x) + q_2(x)b(x) \right) * (f_0(x) + uf_1(x); 0) \\
&\quad + (l(x); g_0(x) + ug_1(x)),
\end{aligned}$$

we obtain that

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (0; g_0(x) + ug_1(x)) \rangle.$$

Hence, $l(x)$ can be reduced to be 0. □

Let $f(x)$ be a non-zero polynomial over R and n be a positive integer. Then, by Theorem 2.2.4, there exist polynomials $q(x), r(x)$ in $R[x]$ such that

$$f(x) = (x^n - 1)q(x) + r(x),$$

where $\deg(r(x)) \leq n - 1$. We denote the remainder $r(x)$ by $[f(x)]_{(x^n-1)}$.

Remark 3.2.5. Let $g_0(x) + ug_1(x)$ and $q_0(x) + uq_1(x)$ be polynomials in $R[x]$ such that $q_0(x), q_1(x), g_0(x), g_1(x) \in \mathbb{F}_2[x]$, $g_1(x) \mid g_0(x) \mid (x^n - 1)$ and n be an odd positive integer.

$$\text{If } (q_0(x) + uq_1(x))(g_0(x) + ug_1(x)) \equiv 0 \pmod{x^n - 1},$$

then $q_0(x) + uq_1(x) = \frac{x^n-1}{g_1(x)}h_0(x) + u\frac{x^n-1}{g_0(x)}h_1(x)$, where $h_0(x), h_1(x) \in \mathbb{F}_2[x]$.

Proof. Suppose that $(q_0(x) + uq_1(x))(g_0(x) + ug_1(x)) \equiv 0 \pmod{x^n - 1}$. Then, there exists $r_0(x) + ur_1(x) \in R[x]$ such that

$$q_0(x)g_0(x) + u(q_1(x)g_0(x) + q_0(x)g_1(x)) = (x^n - 1)r_0(x) + u(x^n - 1)r_1(x).$$

Hence,

$$q_0(x)g_0(x) = (x^n - 1)r_0(x) \text{ and} \tag{3.2.1}$$

$$q_1(x)g_0(x) + q_0(x)g_1(x) = (x^n - 1)r_1(x). \quad (3.2.2)$$

Multiplying $g_1(x)$ and $g_0(x)$ to both side of equations (3.2.1) and (3.2.2), respectively, we have

$$q_0(x)g_0(x)g_1(x) = (x^n - 1)r_0(x)g_1(x) \text{ and} \quad (3.2.3)$$

$$q_1(x)g_0(x)g_0(x) + q_0(x)g_1(x)g_0(x) = (x^n - 1)r_1(x)g_0(x). \quad (3.2.4)$$

Hence, $q_1(x)g_0(x)g_0(x) = (x^n - 1)r_0(x)g_1(x) + (x^n - 1)r_1(x)g_0(x)$. This implies that $q_1(x)g_0(x) = \frac{x^n - 1}{g_0(x)}(r_0(x)g_1(x) + r_1(x)g_0(x))$. Since $\gcd(\frac{x^n - 1}{g_0(x)}, g_0(x)) = 1$, by Lemma 2.2.9, $q_1(x) = \frac{x^n - 1}{g_0(x)}h_1(x)$ for some $h_1(x) \in \mathbb{F}_2[x]$. Substitute $q_1(x)$ in equation (3.2.2), we obtain that $q_0(x)g_1(x) = (x^n - 1)r_1(x) + (x^n - 1)h_1(x)$. Thus,

$$q_0(x) = \frac{x^n - 1}{g_1(x)}(r_1(x) + h_1(x)) = \frac{x^n - 1}{g_1(x)}h_0(x),$$

where $h_0(x) = r_1(x) + h_1(x) \in \mathbb{F}_2[x]$. Therefore,

$$q_0(x) + uq_1(x) = \frac{x^n - 1}{g_1(x)}h_0(x) + \frac{x^n - 1}{g_0(x)}h_1(x),$$

where $h_0(x), h_1(x) \in \mathbb{F}_2[x]$. □

The above remark helps in proving several theorems in this and next chapters. The following propositions show some results of separable codes over R .

Proposition 3.2.6. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g_0(x), g_1(x)$ satisfy Theorem 3.2.1. Then, $\mathcal{C}$ is separable if and only if $l(x)$ is divisible by $f_0(x) + uf_1(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.*

Proof. Suppose that $l(x) = 0$. Then, $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (0; g_0(x) + ug_1(x)) \rangle$. Hence, $\tau_\alpha(\mathcal{C}) = \langle f_0(x) + uf_1(x) \rangle$ and $\tau_\beta(\mathcal{C}) = \langle g_0(x) + ug_1(x) \rangle$. Thus, we can see that $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$, where $\mathcal{C}_\alpha$ is a cyclic code of length α over R with associated ideal generated by $f_0(x) + uf_1(x)$ and $\mathcal{C}_\beta$ is a cyclic code of length β over R with associated ideal generated by $g_0(x) + ug_1(x)$. This means that $\mathcal{C}$ is a separable code.

On the other hand, we let $\mathcal{C}' = \langle (f_0(x) + uf_1(x); 0), (0; g_0(x) + ug_1(x)) \rangle$

and suppose that $\mathcal{C}$ is a separable code. Then, there exist $\mathcal{C}_\alpha \subseteq R^\alpha$ and $\mathcal{C}_\beta \subseteq R^\beta$ such that $\mathcal{C} = \mathcal{C}_\alpha \times \mathcal{C}_\beta$. Thus, the code $\mathcal{C}$ can be viewed as $\tau_\alpha(\mathcal{C}) \times \tau_\beta(\mathcal{C})$, where $\tau_\alpha(\mathcal{C})$ and $\tau_\beta(\mathcal{C})$ are images of $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$, respectively. Since $l(x) \in \tau_\alpha(\mathcal{C})$ and $0 \in \tau_\beta(\mathcal{C})$, $(l(x); 0) \in \tau_\alpha(\mathcal{C}) \times \tau_\beta(\mathcal{C}) = \mathcal{C}$. Since $(0; g_0(x) + ug_1(x)) = (l(x); 0) + (l(x); g_0(x) + ug_1(x)) \in \mathcal{C}$, we obtain that $\mathcal{C}' \subseteq \mathcal{C}$. Thus,

$$(l(x); 0) = \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g_0(x) + ug_1(x)),$$

where $\lambda_1(x), \lambda_2(x) \in R[x]$. So,

$$l(x) = [\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x)]_{(x^\alpha-1)} \text{ and} \quad (3.2.5)$$

$$0 = [\lambda_2(x)(g_0(x) + ug_1(x))]_{(x^\beta-1)}. \quad (3.2.6)$$

By (3.2.6), we have $0 \equiv \lambda_2(x)(g_0(x) + ug_1(x)) \pmod{x^\beta - 1}$. By Remark 3.2.5, we obtain that $\lambda_2(x) = \frac{x^\beta-1}{g_1(x)}\gamma_1(x) + u\frac{x^\beta-1}{g_0(x)}\gamma_2(x)$ for some $\gamma_1(x), \gamma_2(x) \in \mathbb{F}_2[x]$. Then, by (3.2.5),

$$l(x) = \left[\lambda_1(x)(f_0(x) + uf_1(x)) + \left(\frac{x^\beta-1}{g_1(x)}\gamma_1(x)\right)l(x) + \left(u\frac{x^\beta-1}{g_0(x)}\gamma_2(x)\right)l(x) \right]_{(x^\alpha-1)}.$$

By Lemma 3.2.3, we obtain that $(f_0(x) + uf_1(x)) \mid l(x)$ in $\frac{R[x]}{(x^\alpha-1)}$. $\square$

By using Corollary 3.2.4 and Proposition 3.2.6, we obtain the next proposition directly.

Proposition 3.2.7. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g_0(x), g_1(x)$ satisfy Theorem 3.2.1. If $f_0(x) + uf_1(x)$ and $\frac{x^\beta-1}{g_1(x)}$ are coprime in $R[x]$, then $\mathcal{C}$ is separable.*

Proof. Suppose that $f_0(x) + uf_1(x)$ and $\frac{x^\beta-1}{g_1(x)}$ are coprime. By Corollary 3.2.4, then we can assume $l(x) = 0$. Then, by Proposition 3.2.6, $\mathcal{C}$ is separable. $\square$

The following examples are double cyclic codes of length (α, β) over the ring R derived from the theorems presented in this section:

Example 3.2.8. Let $\alpha = 3$ and $\beta = 5$. Consider,

$$x^3 - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and}$$

$$x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1) = m_1(x)m_3(x) \in \mathbb{F}_2[x].$$

1. Suppose $\mathcal{C}_1 = \langle (m_1(x)m_2(x) + um_1(x); 0), (0; m_3(x) + u) \rangle$. Then, by Theorem 3.2.1, we can obtain that $\mathcal{C}_1$ is a double cyclic code of length $(3, 5)$ over R . Moreover, $\mathcal{C}_1$ is separable and $|\mathcal{C}_1| = 256$.
2. Suppose $\mathcal{C}_2 = \langle ((1 + u)m_1(x); 0), (u; (1 + u)m_3(x)) \rangle$. Then, by Theorem 3.2.1, we can obtain that $\mathcal{C}_2$ is a double cyclic code of length $(3, 5)$ over R and $|\mathcal{C}_2| = 64$.

In addition, double cyclic codes generated from $\mathcal{C}_1$ and $\mathcal{C}_2$ are given in Tables 12 and 13.

Example 3.2.9. Let $\alpha = 3$ and $\beta = 3$. Consider,

$$x^3 - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x].$$

1. Suppose $\mathcal{C}_1 = \langle ((1 + u)m_2(x); 0), (x + 1 + u; (1 + u)m_1(x)) \rangle$. Then, by Theorem 3.2.1, we can obtain that $\mathcal{C}_1$ is a double cyclic code of length $(3, 3)$ over R and $|\mathcal{C}_1| = 64$.
2. Suppose $\mathcal{C}_2 = \langle ((1 + u)m_2(x); 0), (x + u; (1 + u)m_1(x)) \rangle$. Then, by Theorem 3.2.1, we can obtain that $\mathcal{C}_2$ is a double cyclic code of length $(3, 3)$ over R and $|\mathcal{C}_2| = 64$. Since $(x + 1 + u; (1 + u)m_1(x)) \notin \mathcal{C}_2$, we obtain that $\mathcal{C}_1 \neq \mathcal{C}_2$.

In addition, double cyclic codes generated from $\mathcal{C}_1$ and $\mathcal{C}_2$ are given in Tables 14 and 15.

3.3 The case α is an odd and β is an even positive integer

In this section, we will give a structure of double cyclic codes of length (α, β) over R , where α is an odd positive integer and β is an even positive integer.

Throughout this section, α is an odd positive integer and β is an even positive integer.

The following theorem is used to determine the generator polynomials for double cyclic codes of length (α, β) over R :

Theorem 3.3.1. *Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . Then, we can classify $\mathcal{C}$ into two types:*

- Type 1:* $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$,
for some polynomials $f_0(x), f_1(x), g(x), p(x) \in \mathbb{F}_2[x]$ with
 $f_1(x) \mid f_0(x) \mid (x^\alpha - 1)$, $g(x) \mid (x^\beta - 1)$, $(g(x) + up(x)) \mid (x^\beta - 1)$,
 $g(x) \mid p(x)(\frac{x^\beta - 1}{g(x)})$ and for some $l(x) \in R[x]$ with
 $(l(x); g(x) + up(x)) \in \mathcal{C}$.
- Type 2:* $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$,
for some polynomials $f_0(x), f_1(x), g(x), p(x), a(x) \in \mathbb{F}_2[x]$ with
 $f_1(x) \mid f_0(x) \mid (x^\alpha - 1)$, $a(x) \mid g(x) \mid (x^\beta - 1)$, $a(x) \mid p(x)(\frac{x^\beta - 1}{g(x)})$
and for some $l_1(x), l_2(x) \in R[x]$ with $(l_1(x); g(x) + up(x)),$
 $(l_2(x); ua(x)) \in \mathcal{C}$.

Proof. Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . Proceeding with the proof as in Theorem 3.2.1, we obtain that $\tau_\beta(\mathcal{C})$ is an ideal of $\frac{R[x]}{\langle x^\beta - 1 \rangle}$, where τ_β is a mapping which is defined as (3.1.2). By Theorem 2.4.12(2), we obtain that $\tau_\beta(\mathcal{C})$ can be represented as 2 types:

1. $\tau_\beta(\mathcal{C}) = \langle g(x) + up(x) \rangle$, where the polynomials $g(x), p(x)$ are in $\mathbb{F}_2[x]$ with $g(x) \mid (x^\beta - 1)$, $(g(x) + up(x)) \mid (x^\beta - 1)$ and $g(x) \mid p(x)(\frac{x^\beta - 1}{g(x)})$. Or,
2. $\tau_\beta(\mathcal{C}) = \langle g(x) + up(x), ua(x) \rangle$, where the polynomials $g(x), p(x), a(x)$ are in $\mathbb{F}_2[x]$ with $a(x) \mid g(x) \mid (x^\beta - 1)$ and $a(x) \mid p(x)(\frac{x^\beta - 1}{g(x)})$.

Note that $\ker(\tau_\beta) = \{(a'(x); 0) : (a'(x); 0) \in \mathcal{C}\}$. Let $I = \{a'(x) \in \frac{R[x]}{\langle x^\alpha - 1 \rangle} : (a'(x); 0) \in \ker(\tau_\beta)\}$. By following the proof as in Theorem 3.2.1, it can be shown that I is an ideal of $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. By Theorem 2.4.12(1), we have $I = \langle f_0(x) + uf_1(x) \rangle$, where $f_0(x), f_1(x) \in \mathbb{F}_2[x]$ with $f_1(x) \mid f_0(x) \mid (x^\alpha - 1)$. Hence, $\ker(\tau_\beta) = \langle (f_0(x) + uf_1(x); 0) \rangle$. By Fundamental homomorphism theorem, $\mathcal{C}/\ker(\tau_\beta) \cong \tau_\beta(\mathcal{C})$. Since

$\tau_\beta(\mathcal{C})$ has two types, we will divide the consideration of the double cyclic code $\mathcal{C}$ into two parts.

Firstly, suppose that $\tau_\beta(\mathcal{C}) = \langle g(x) + up(x), ua(x) \rangle$. Then, there exist polynomials $l_1(x), l_2(x) \in R[x]$ such that $(l_1(x); g(x) + up(x))$ and $(l_2(x); ua(x))$ are in $\mathcal{C}$. Then, $\langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle \subseteq \mathcal{C}$. For any $v(x) = (b(x); d(x))$ in $\mathcal{C}$, we obtain that $d(x) \in \tau_\beta(\mathcal{C})$. Hence, there exist polynomials $k_1(x), k_2(x) \in R[x]$ such that $d(x) = k_1(x)(g(x) + up(x)) + uk_2(x)a(x)$. Consider,

$$\begin{aligned} (b(x); d(x)) &- [k_1(x) * (l_1(x); g(x) + up(x))] - [k_2(x) * (l_2(x); ua(x))] \\ &= (b(x) - k_1(x)l_1(x) - k_2(x)l_2(x); d(x) - k_1(x)(g(x) + up(x)) - uk_2(x)a(x)) \\ &= (b(x) - k_1(x)l_1(x) - k_2(x)l_2(x); 0) \in \ker(\tau_\beta). \end{aligned}$$

Then, $(b(x) - k_1(x)l_1(x) - k_2(x)l_2(x); 0) = k_3(x) * (f_0(x) + uf_1(x); 0)$, where $k_3(x) \in R[x]$. So, $[b(x) - k_1(x)l_1(x) - k_2(x)l_2(x)]_{(x^\alpha-1)} = [k_3(x)(f_0(x) + uf_1(x))]_{(x^\alpha-1)}$. This implies that

$$\begin{aligned} (b(x); d(x)) &= (k_3(x)(f_0(x) + uf_1(x)) + k_1(x)l_1(x) + k_2(x)l_2(x); \\ &\quad k_1(x)(g(x) + up(x)) + uk_2(x)a(x)) \\ &= k_3(x) * (f_0(x) + uf_1(x); 0) + k_1(x) * (l_1(x); g(x) + up(x)) \\ &\quad + k_2(x) * (l_2(x); ua(x)) \\ &\in \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle. \end{aligned}$$

Therefore, $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$.

Lastly, suppose that $\tau_\beta(\mathcal{C}) = \langle g(x) + up(x) \rangle$, there is a polynomial $l(x)$ in $R[x]$ such that $(l(x); g(x) + up(x)) \in \mathcal{C}$. Then, $\langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle \subseteq \mathcal{C}$. Similarly to the above case, $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$. $\square$

Next, we will investigate the conditions of the polynomials $l(x), l_1(x)$ and $l_2(x)$ derived from Theorem 3.3.1.

Lemma 3.3.2. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g(x), p(x)$*

satisfy Theorem 3.3.1 (Type 1). Then, we can assume that the degree of $l(x)$ is less than the degree of $f_0(x) + uf_1(x)$.

Furthermore, $f_0(x) + uf_1(x)$ divides $\frac{x^\beta - 1}{g(x) + up(x)}l(x)$ and $u\frac{x^\beta - 1}{g(x)}l(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Assume that $\deg(l(x)) \geq \deg(f_0(x) + uf_1(x))$. Let $i = \deg(l(x)) - \deg(f_0(x) + uf_1(x))$. Suppose that

$$C' = \langle (f_0(x) + uf_1(x); 0), (l(x) + ax^i(f_0(x) + uf_1(x)); g(x) + up(x)) \rangle$$

is a double cyclic code of length (α, β) over R , where a is the leading coefficient of $l(x)$. Hence, we have $C' \subseteq C$ and $\deg(l(x) + ax^i(f_0(x) + uf_1(x))) < \deg(l(x))$. Consider,

$$\begin{aligned} (l(x); g(x) + up(x)) &= (l(x) + ax^i(f_0(x) + uf_1(x)); g(x) + up(x)) \\ &\quad + ax^i * (f_0(x) + uf_1(x); 0). \end{aligned}$$

We obtain that $(l(x); g(x) + up(x))$ is in C' . Thus, $C \subseteq C'$. This implies that $C = C'$ and hence, the degree of $l(x)$ can be reduced in C and so we may assume that $\deg(l(x)) < \deg(f_0(x) + uf_1(x))$.

Furthermore, from the proof of Theorem 3.3.1, we have that

$$\ker(\tau_\beta) = \langle (f_0(x) + uf_1(x); 0) \rangle.$$

Consider,

$$\frac{x^\beta - 1}{g(x) + up(x)} * (l(x); g(x) + up(x)) = \left(\frac{x^\beta - 1}{g(x) + up(x)} l(x); 0 \right) \in \langle (f_0(x) + uf_1(x); 0) \rangle$$

and

$$u \frac{x^\beta - 1}{g(x)} * (l(x); g(x) + up(x)) = \left(u \frac{x^\beta - 1}{g(x)} l(x); 0 \right) \in \langle (f_0(x) + uf_1(x); 0) \rangle.$$

This implies that $f_0(x) + uf_1(x)$ divides $\frac{x^\beta - 1}{g(x) + up(x)}l(x)$ and $u\frac{x^\beta - 1}{g(x)}l(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. $\square$

Lemma 3.3.3. Let $C = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l_1(x), l_2(x), g(x), p(x), a(x)$ satisfy Theorem 3.3.1 (Type 2). Then, we can assume that the degrees of $l_1(x)$ and $l_2(x)$ are less than the degree of $f_0(x) + uf_1(x)$.

Furthermore, $f_0(x) + uf_1(x)$ divides $ul_2(x), u\frac{x^\beta - 1}{g(x)}l_1(x), \frac{x^\beta - 1}{a(x)}l_2(x), ul_1(x) + \frac{g(x)}{a(x)}l_2(x)$ and $\frac{x^\beta - 1}{g(x)}l_1(x) + p(x)\frac{x^\beta - 1}{g(x)a(x)}l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Assume that $\deg(l_1(x)) \geq \deg(f_0(x) + uf_1(x))$ and $\deg(l_2(x)) \geq \deg(f_0(x) + uf_1(x))$. Let $i = \deg(l_1(x)) - \deg(f_0(x) + uf_1(x))$ and $j = \deg(l_2(x)) - \deg(f_0(x) + uf_1(x))$. Suppose that

$$\begin{aligned} \mathcal{C}' = \langle (f_0(x) + uf_1(x); 0), (l_1(x) + ax^i(f_0(x) + uf_1(x)); g(x) + up(x)), \\ (l_2(x) + a'x^j(f_0(x) + uf_1(x)); ua(x)) \rangle \end{aligned}$$

is a double cyclic code of length (α, β) over R , where a and a' are the leading coefficients of $l_1(x)$ and $l_2(x)$, respectively. Hence, we have $\mathcal{C}' \subseteq \mathcal{C}$, $\deg(l_1(x) + ax^i(f_0(x) + uf_1(x))) < \deg(l_1(x))$ and $\deg(l_2(x) + a'x^j(f_0(x) + uf_1(x))) < \deg(l_2(x))$. Consider,

$$\begin{aligned} (l_1(x); g(x) + up(x)) &= (l_1(x) + ax^i(f_0(x) + uf_1(x)); g(x) + up(x)) \\ &\quad + ax^i * (f_0(x) + uf_1(x); 0) \\ (l_2(x); ua(x)) &= (l_2(x) + a'x^j(f_0(x) + uf_1(x)); ua(x)) \\ &\quad + a'x^j * (f_0(x) + uf_1(x); 0). \end{aligned}$$

We obtain that $(l_1(x); g(x) + up(x))$ and $(l_2(x); ua(x))$ are in $\mathcal{C}'$. Thus, $\mathcal{C} \subseteq \mathcal{C}'$. This implies that $\mathcal{C} = \mathcal{C}'$ and hence, the degree of $l_1(x)$ and $l_2(x)$ can be reduced in $\mathcal{C}$ and so we can assume that $\deg(l_1(x)) < \deg(f_0(x) + uf_1(x))$ and $\deg(l_2(x)) < \deg(f_0(x) + uf_1(x))$.

Furthermore, from the proof of Theorem 3.3.1, we have that

$$\ker(\tau_\beta) = \langle (f_0(x) + uf_1(x); 0) \rangle.$$

Consider,

$$\begin{aligned} u * (l_2(x); ua(x)) &= (ul_2(x); 0) \in \langle (f_0(x) + uf_1(x); 0) \rangle, \\ \frac{x^\beta - 1}{a(x)} * (l_2(x); ua(x)) &= \left(\frac{x^\beta - 1}{a(x)} l_2(x); 0 \right) \in \langle (f_0(x) + uf_1(x); 0) \rangle, \\ u \frac{x^\beta - 1}{g(x)} * (l_1(x); g(x) + up(x)) &= \left(u \frac{x^\beta - 1}{g(x)} l_1(x); 0 \right) \in \langle (f_0(x) + uf_1(x); 0) \rangle. \end{aligned}$$

This implies that $f_0(x) + uf_1(x)$ divides $ul_2(x)$, $\frac{x^\beta - 1}{a(x)} l_2(x)$ and $u \frac{x^\beta - 1}{g(x)} l_1(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Next, we consider

$$u * (l_1(x); g(x) + up(x)) + \frac{g(x)}{a(x)} * (l_2(x); ua(x))$$

$$\begin{aligned}
&= (ul_1(x) + \frac{g(x)}{a(x)}l_2(x); ug(x) + ug(x)) \\
&= (ul_1(x) + \frac{g(x)}{a(x)}l_2(x); 0) \in \langle (f_0(x) + uf_1(x); 0) \rangle
\end{aligned}$$

and

$$\begin{aligned}
&\frac{x^\beta - 1}{g(x)} * (l_1(x); g(x) + up(x)) + p(x) \frac{x^\beta - 1}{g(x)a(x)} * (l_2(x); ua(x)) \\
&= (\frac{x^\beta - 1}{g(x)}l_1(x); u\frac{x^\beta - 1}{g(x)}p(x)) + (p(x)\frac{x^\beta - 1}{g(x)a(x)}l_2(x); u\frac{x^\beta - 1}{g(x)}p(x)) \\
&= (\frac{x^\beta - 1}{g(x)}l_1(x) + p(x)\frac{x^\beta - 1}{g(x)a(x)}l_2(x); 0) \in \langle (f_0(x) + uf_1(x); 0) \rangle.
\end{aligned}$$

So, $f_0(x) + uf_1(x)$ divides $ul_1(x) + \frac{g(x)}{a(x)}l_2(x)$ and $\frac{x^\beta - 1}{g(x)}l_1(x) + p(x)\frac{x^\beta - 1}{g(x)a(x)}l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. $\square$

The following are double cyclic codes of length (α, β) over the ring R , derived from the theorems in this section:

Example 3.3.4. Let $\alpha = 3$ and $\beta = 6$. Consider,

$$\begin{aligned}
x^3 - 1 &= (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and} \\
x^6 - 1 &= (x + 1)^2(x^2 + x + 1)^2 = m_1(x)^2m_2(x)^2 \in \mathbb{F}_2[x].
\end{aligned}$$

1. Suppose $\mathcal{C}_1 = \langle ((1 + u)m_2(x); 0), (ux + u; m_1(x)^2m_2(x) + um_1(x)^2) \rangle$. Then, by Theorem 3.3.1 (Type 1), we can obtain that $\mathcal{C}_1$ is a double cyclic code of length $(3, 6)$ over R and $|\mathcal{C}_1| = 64$.
2. Suppose $\mathcal{C}_2 = \langle (m_1(x); 0), (u; m_1(x)m_2(x)^2 + um_2(x)), (0; um_1(x)m_2(x)) \rangle$. Then, by Theorem 3.3.1 (Type 2), we can obtain that $\mathcal{C}_2$ is a double cyclic code of length $(3, 6)$ over R and $|\mathcal{C}_2| = 256$.

In addition, double cyclic codes generated from $\mathcal{C}_1$ and $\mathcal{C}_2$ are given in Tables 16 and 17.

CHAPTER IV

CONSTRUCTING DOUBLE CYCLIC CODES OVER $\mathbb{F}_2 + u\mathbb{F}_2$ FOR DNA CODES

Let R be the ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and α, β be positive integers. From Chapter III, we have the algebraic structure of double cyclic codes of length (α, β) over R . Hence, this chapter applies that structure to develop the theory for constructing double cyclic codes suitable for DNA codes. Recall that this thesis focusses on a specific constraint of a good DNA code $\mathcal{D}$, which is a reverse-complement constraint. It means that for every $x, y \in \mathcal{D}$, $d_H(x, y^{rc}) \geq d$, including $x = y$, where d is a minimum distance of $\mathcal{D}$. We provide the necessary and sufficient conditions for the double cyclic codes to be reversible and reversible-complement codes. To correspond with the algebraic structure of a double cyclic code of length (α, β) over R , this chapter is organized into 3 sections based on the types of lengths α and β .

The first section introduces the basic concept of constructing double cyclic codes suitable for DNA codes, where α and β are non-negative integers. Additionally, a process for generating DNA codes from double cyclic codes is provided. The second and last sections present theorems for double cyclic codes to be reversible and reversible-complement codes when both α and β are odd integers, and when α is an odd integer and β is an even integer, respectively. Additionally, examples of double cyclic DNA codes are provided at the end of each section. The codewords generated from these examples are included in the appendix.

4.1 Basic concept for lengths α and β

By applying the idea of the study DNA codes employing cyclic codes [38–40], we will present the notions of reversible, complement and reversible-complement for double cyclic codes which are suitable for studying DNA codes.

Let $\mathfrak{R}$ be a finite commutative ring. Consider,

$$\mathbf{v} = (\mathbf{a}; \mathbf{b}) = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathfrak{R}^{\alpha, \beta}.$$

Then,

- the reverse of $\mathbf{v}$ is defined as $\mathbf{v}^r = (a_{\alpha-1}, a_{\alpha-2}, \dots, a_0; b_{\beta-1}, b_{\beta-2}, \dots, b_0)$, that is, $\mathbf{v}^r = (\mathbf{a}^r; \mathbf{b}^r)$,
- the complement of $\mathbf{v}$ is defined as $\mathbf{v}^c = (\overline{a_0}, \overline{a_1}, \dots, \overline{a_{\alpha-1}}; \overline{b_0}, \overline{b_1}, \dots, \overline{b_{\beta-1}})$, that is, $\mathbf{v}^c = (\mathbf{a}^c; \mathbf{b}^c)$ and
- the reverse-complement of $\mathbf{v}$ is defined as $\mathbf{v}^{rc} = (\overline{a_{\alpha-1}}, \overline{a_{\alpha-2}}, \dots, \overline{a_0}; \overline{b_{\beta-1}}, \overline{b_{\beta-2}}, \dots, \overline{b_0})$, that is, $\mathbf{v}^{rc} = (\mathbf{a}^{rc}; \mathbf{b}^{rc})$.

The double cyclic DNA codes of length (α, β) over $\mathfrak{R}$ is defined as follows:

Definition 4.1.1. Let $\mathcal{C}$ be a double cyclic code of length (α, β) over $\mathfrak{R}$. Then, $\mathcal{C}$ is called **reversible** (respectively, **complement** and **reversible-complement**) if $\mathbf{v}^r \in \mathcal{C}$ (respectively, $\mathbf{v}^c \in \mathcal{C}$ and $\mathbf{v}^{rc} \in \mathcal{C}$) for all $\mathbf{v} \in \mathcal{C}$.

Furthermore, if $\alpha = 0$, $\mathcal{C}$ is a reversible (complement, reversible-complement) cyclic code of length β over $\mathfrak{R}$. If $\beta = 0$, $\mathcal{C}$ is a reversible (complement, reversible-complement) cyclic code of length α over $\mathfrak{R}$.

Definition 4.1.2. Let $\mathcal{C}$ be a linear code of length $n = \alpha + \beta$ over $\mathfrak{R}$. Then, $\mathcal{C}$ is called a **double cyclic DNA code** of length (α, β) over $\mathfrak{R}$ if $\mathcal{C}$ is a double cyclic code of length (α, β) over $\mathfrak{R}$, and for any $\mathbf{v} \in \mathcal{C}$, $\mathbf{v} \neq \mathbf{v}^{rc}$, $\mathbf{v}^{rc} \in \mathcal{C}$.

Recall that for any element $a \in R = \mathbb{F}_2 + u\mathbb{F}$ with $u^2 = 0$, we have $\overline{a} = u + a$ and

$$\phi(0) = A, \phi(1) = G, \phi(u) = T \text{ and } \phi(1+u) = C.$$

Example 4.1.3. From Example 3.1.3, we have

$$\begin{aligned} \mathcal{C} = \{ & (0, 0, 0; 0, 0, 0, 0), (0, 0, 0; u, u, u, u), (0, 0, 0; 1, 1+u, 1, 1+u), \\ & (0, 0, 0; 1+u, 1, 1+u, 1), (u, u, u; 0, 0, 0, 0), (u, u, u; u, u, u, u), \\ & (u, u, u; 1, 1+u, 1, 1+u), (u, u, u; 1+u, 1, 1+u, 1) \} \end{aligned}$$

is a double cyclic code of length $(3, 4)$ over R . It is easy to check that $\mathcal{C}$ is a double cyclic DNA code.

To generate DNA codes from a double cyclic codes of length (α, β) over R , we have the process as follows:

Let $\mathcal{C}$ be a code of length $n = \alpha + \beta$ over R and $S_{\mathcal{D}_4} = \{A, T, G, C\}$. Define $\Phi : \mathcal{C} \rightarrow S_{\mathcal{D}_4}^{\alpha+\beta}$ by

$$\Phi(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) = \phi(a_0)\phi(a_1) \cdots \phi(a_{\alpha-1})\phi(b_0)\phi(b_1) \cdots \phi(b_{\beta-1}), \quad (4.1.1)$$

for all $(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathcal{C}$.

Example 4.1.4. From Example 4.1.3, we can obtain a DNA code $\mathcal{D}_1$ from the code $\mathcal{C}$ as follows:

$$\mathcal{D}_1 = \Phi(\mathcal{C}) = \{AAAAAAA, AAATTTT, AAAGCGC, AAACGCG, \\ TTTAAAA, TTTTTTT, TTTGCGC, TTTGCGG\}.$$

From the above example, we can see that for any DNA strand, v , in $\mathcal{D}_1$, its DNA pair, v^{rc} , is not in $\mathcal{D}_1$, except for the DNA strand AAAAAAA and TTTTTTT. For example, the DNA strand $5' - AAATTTT - 3' \in \mathcal{D}_1$, its DNA pair is $5' - AAAATTTT - 3' \notin \mathcal{D}_1$. This means that the code $\mathcal{C}$ can provide only a single DNA strand.

For any double cyclic code $\mathcal{C}$ of length (α, β) over R , we let $\hat{\mathcal{C}}$ be the set

$$\hat{\mathcal{C}} = \{(b; a) \in R^{\beta, \alpha} : (a; b) \in \mathcal{C}\} \subseteq R^{\beta, \alpha}.$$

Example 4.1.5. From Example 4.1.3 we can obtain $\hat{\mathcal{C}}$ as follows:

$$\hat{\mathcal{C}} = \{(0, 0, 0, 0; 0, 0, 0), (u, u, u, u; 0, 0, 0), (1, 1 + u, 1, 1 + u; 0, 0, 0), \\ (1 + u, 1, 1 + u, 1; 0, 0, 0), (0, 0, 0, 0; u, u, u), (u, u, u, u; u, u, u), \\ (1, 1 + u, 1, 1 + u; u, u, u), (1 + u, 1, 1 + u, 1; u, u, u)\}.$$

Moreover, a DNA code $\mathcal{D}_2$ from the code $\hat{\mathcal{C}}$ is

$$\mathcal{D}_2 = \Phi(\hat{\mathcal{C}}) = \{AAAAAAA, TTTTAAA, GCGCAAA, CGCGAAA, \\ AAAATTT, TTTTTTT, GCGCTTT, CGCGTTT\}.$$

The above example shows that all of the DNA pairs of DNA strands in Example 4.1.4 are in $\mathcal{D}_2$. Then, we can generate a DNA code $\mathcal{D}$ from $\mathcal{C} \cup \hat{\mathcal{C}}$. We provide the steps for generating a DNA code from a double cyclic DNA code as follows:

The process of generating a DNA code from a double cyclic DNA code

Step 1: Construct a double cyclic DNA code $\mathcal{C}$ of length (α, β) over R .

Step 2: Construct the code $\hat{\mathcal{C}} = \{(b; a) \in R^{\beta, \alpha} : (a; b) \in \mathcal{C}\}$ from the code $\mathcal{C}$.

Step 3: Generate a DNA code $\mathcal{D}$ from $\mathcal{C} \cup \hat{\mathcal{C}}$, by using the mapping Φ defined as (4.1.1).

Therefore, we can generate a DNA code $\mathcal{D}$ from $\mathcal{C} \cup \hat{\mathcal{C}}$, where $\mathcal{C}$ is a double cyclic DNA code of length (α, β) over R . For any double cyclic code $\mathcal{C}$ of length (α, β) over R and $v \in \mathcal{C}$, we observe that $v \neq v^{rc}$, when α or β is an odd positive integer. Since the length α in this thesis will always be an odd positive integer, by Definition 4.1.2, we obtain that a double cyclic code $\mathcal{C}$ is a double cyclic DNA code if $\mathcal{C}$ is a reversible-complement code. This means that we will focus the study on necessary and sufficient conditions for double cyclic codes to be reversible and reversible-complement codes.

4.1.1 Reversible codes

This section presents important properties for studying the conditions of reversible codes. The purpose of this section is to present the theoretical tools needed for proofs in the next sections.

For any $v = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in R^{\alpha, \beta}$, its polynomial representation is

$$\begin{aligned} v(x) &= (a(x); b(x)) \\ &= (a_0 + a_1x + \dots + a_{\alpha-1}x^{\alpha-1}; b_0 + b_1x + \dots + b_{\beta-1}x^{\beta-1}) \in R_{\alpha, \beta}. \end{aligned}$$

Since $v^r = (a_{\alpha-1}, a_{\alpha-2}, \dots, a_0; b_{\beta-1}, b_{\beta-2}, \dots, b_0)$, we have

$$\begin{aligned} v^r(x) &= (a_{\alpha-1} + a_{\alpha-2}x + \dots + a_0x^{\alpha-1}; b_{\beta-1} + b_{\beta-2}x + \dots + b_0x^{\beta-1}) \\ &= (x^{\alpha-1-\deg(a(x))}a^*(x); x^{\beta-1-\deg(b(x))}b^*(x)). \end{aligned}$$

This means that we can view the reverse of v as a polynomial

$$v^r(x) = (x^{\alpha-1-\deg(a(x))}a^*(x); x^{\beta-1-\deg(b(x))}b^*(x)).$$

Example 4.1.6. Let $v = (0, 1, 1+u, 0; 1, u, 0, 1, 1+u) \in R^{4,5}$. Then, the polynomial representation of v is

$$v(x) = (x + (1+u)x^2; 1 + ux + x^3 + (1+u)x^4) = (a(x); b(x)).$$

The reverse of v is $v^r = (0, 1+u, 1, 0; 1+u, 1, 0, u, 1)$ and the polynomial representation of v^r is

$$\begin{aligned} v^r(x) &= ((1+u)x + x^2; 1 + u + x + ux^3 + x^4) \\ &= (xa^*(x); b^*(x)). \end{aligned}$$

Proposition 4.1.7. Let $v, w \in R^\alpha \times R^\beta$ and $k \in R$. Suppose that $v(x)$ and $w(x)$ are polynomials in $R_{\alpha,\beta}$ that correspond to v and w , respectively. Then,

1. $(v + w)^r = v^r + w^r$,
2. $(k * v)^r = k * v^r$,
3. $(v(x) + w(x))^r = v^r(x) + w^r(x)$.

Proof. Let

$$v = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \text{ and } w = (a'_0, a'_1, \dots, a'_{\alpha-1}; b'_0, b'_1, \dots, b'_{\beta-1})$$

be elements in $R^\alpha \times R^\beta$ and $k \in R$. Suppose that the polynomial representations of v and w are $v(x) = (a(x); b(x))$ and $w(x) = (a'(x); b'(x))$, respectively.

1. Consider,

$$\begin{aligned}
 (v + w)^r &= (a_0 + a'_0, a_1 + a'_1, \dots, a_{\alpha-1} + a'_{\alpha-1}; b_0 + b'_0, b_1 + b'_1, \dots, b_{\beta-1} + b'_{\beta-1})^r \\
 &= (a_{\alpha-1} + a'_{\alpha-1}, a_{\alpha-2} + a'_{\alpha-2}, \dots, a_0 + a'_0; \\
 &\quad b_{\beta-1} + b'_{\beta-1}, b_{\beta-2} + b'_{\beta-2}, \dots, b_0 + b'_0) \\
 &= (a_{\alpha-1}, a_{\alpha-2}, \dots, a_0; b_{\beta-1}, b_{\beta-2}, \dots, b_0) \\
 &\quad + (a'_{\alpha-1}, a'_{\alpha-2}, \dots, a'_0; b'_{\beta-1}, b'_{\beta-2}, \dots, b'_0) \\
 &= v^r + w^r.
 \end{aligned}$$

2. Consider,

$$\begin{aligned}
 (k * v)^r &= (ka_0, ka_1, \dots, ka_{\alpha-1}; kb_0, kb_1, \dots, kb_{\beta-1})^r \\
 &= (ka_{\alpha-1}, ka_{\alpha-2}, \dots, ka_0; kb_{\beta-1}, kb_{\beta-2}, \dots, kb_0) \\
 &= kv^r.
 \end{aligned}$$

3. Without loss of generality, suppose that $\deg(a(x)) \leq \deg(a'(x))$ and $\deg(b(x)) \leq \deg(b'(x))$. Consider,

$$\begin{aligned}
 (v(x) + w(x))^r &= (a(x) + a'(x); b(x) + b'(x))^r \\
 &= (x^{\alpha-1-\deg(a'(x))}(a(x) + a'(x))^*; x^{\beta-1-\deg(b'(x))}(b(x) + b'(x))^*) \\
 &= (x^{\alpha-1-\deg(a'(x))} \left(x^{\deg(a'(x))-\deg(a(x))} a^*(x) + a'^*(x) \right); \\
 &\quad x^{\beta-1-\deg(b'(x))} \left(x^{\deg(b'(x))-\deg(b(x))} b^*(x) + b'^*(x) \right)) \\
 &= (x^{\alpha-1-\deg(a(x))} a^*(x) + x^{\alpha-1-\deg(a'(x))} a'^*(x); \\
 &\quad x^{\beta-1-\deg(b(x))} b^*(x) + x^{\beta-1-\deg(b'(x))} b'^*(x)) \\
 &= (x^{\alpha-1-\deg(a(x))} a^*(x); x^{\beta-1-\deg(b(x))} b^*(x)) \\
 &\quad + (x^{\alpha-1-\deg(a'(x))} a'^*(x); x^{\beta-1-\deg(b'(x))} b'^*(x)) \\
 &= v^r(x) + w^r(x).
 \end{aligned}$$

Therefore, from 1. – 3., we can complete the proof. $\square$

Proposition 4.1.8. *Let $(a(x); b(x))$ be an element in $R_{\alpha, \beta}$ and k be a positive integer. Then,*

$$(x^k a(x); x^k b(x))^r = x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)),$$

where $m = n = 0$ or m, n are the smallest positive integers such that

$$\begin{aligned} m\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^{\alpha-1})}) &\geq 0 \text{ and} \\ n\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^{\beta-1})}) &\geq 0. \end{aligned}$$

Proof. Let $(a(x); b(x)) \in R_{\alpha, \beta}$ and $k \in \mathbb{Z}^+$. We divide the proof into four cases as follows:

Case 1. $\deg(x^k a(x)) \leq \alpha - 1$ and $\deg(x^k b(x)) \leq \beta - 1$:

Then, $(x^k a(x))^* = a^*(x)$ and $(x^k b(x))^* = b^*(x)$. Hence,

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= (x^{\alpha-1-\deg(x^k a(x))} (x^k a(x))^*; \\ &\quad x^{\beta-1-\deg(x^k b(x))} (x^k b(x))^*) \\ &= (x^{\alpha-1-\deg(x^k a(x))} a^*(x); x^{\beta-1-\deg(x^k b(x))} b^*(x)) \\ &= x^{\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{\beta-1-\deg(x^k b(x))} * (0; b^*(x)). \end{aligned}$$

This means that

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)), \end{aligned}$$

where $m = 0 = n$.

Case 2. $\deg(x^k a(x)) \geq \alpha$ and $\deg(x^k b(x)) \geq \beta$:

Then, $x^k a(x) = (x^\alpha - 1)q_1(x) + h_1(x)$ and $x^k b(x) = (x^\beta - 1)q_2(x) + h_2(x)$, where $q_1(x), q_2(x), h_1(x), h_2(x) \in R[x]$ and $\deg(h_1(x)) \leq \alpha - 1$ and $\deg(h_2(x)) \leq \beta - 1$.

Hence,

$$\begin{aligned} a^*(x) &= (x^k a(x))^* = (x^\alpha - 1)q_1^*(x) + x^i h_1^*(x) \text{ and} \\ b^*(x) &= (x^k b(x))^* = (x^\beta - 1)q_2^*(x) + x^j h_2^*(x), \end{aligned}$$

where $i = \deg((x^\alpha - 1)q_1(x)) - \deg(h_1(x))$ and $j = \deg((x^\beta - 1)q_2(x)) - \deg(h_2(x))$.

Thus, there exist the smallest positive integers m, n such that $m\alpha - i \geq 0$ and $n\beta - j \geq 0$. So,

$$h_1^*(x) = [x^{m\alpha-i} a^*(x)]_{(x^{\alpha-1})} \text{ and } h_2^*(x) = [x^{n\beta-j} b^*(x)]_{(x^{\beta-1})}.$$

Consider,

$$\begin{aligned}
 (x^k a(x); x^k b(x))^r &= (h_1(x); h_2(x))^r \\
 &= (x^{\alpha-1-\deg(h_1(x))} h_1^*(x); x^{\beta-1-\deg(h_2(x))} h_2^*(x)) \\
 &= (x^{\alpha-1-\deg(h_1(x))} x^{m\alpha-i} a^*(x); 0) \\
 &\quad + (0; x^{\beta-1-\deg(h_2(x))} x^{n\beta-j} b^*(x)) \\
 &= x^{(m+1)\alpha-1-\deg((x^\alpha-1)q_1(x))} * (a^*(x); 0) \\
 &\quad + x^{(n+1)\beta-1-\deg((x^\beta-1)q_2(x))} * (0; b^*(x)).
 \end{aligned}$$

Since $\deg((x^\alpha-1)q_1(x)) = \deg(x^k a(x))$ and $\deg((x^\beta-1)q_2(x)) = \deg(x^k b(x))$, we have

$$\begin{aligned}
 (x^k a(x); x^k b(x))^r &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\
 &\quad + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)).
 \end{aligned}$$

Case 3. $\deg(x^k a(x)) \leq \alpha-1$ and $\deg(x^k b(x)) \geq \beta$:

Then, $x^k b(x) = (x^\beta-1)q_2(x) + h_2(x)$, where $q_2(x), h_2(x) \in R[x]$ and $\deg(h_2(x)) \leq \beta-1$. Hence,

$$\begin{aligned}
 a^*(x) &= (x^k a(x))^* \text{ and} \\
 b^*(x) &= (x^\beta-1)q_2^*(x) + x^j h_2^*(x),
 \end{aligned}$$

where $j = \deg((x^\beta-1)q_2(x)) - \deg(h_2(x))$. Then, there exists the smallest positive integer n such that $n\beta-j \geq 0$ and so, $h_2^*(x) = [x^{n\beta-j} b^*(x)]_{(x^\beta-1)}$. Hence,

$$\begin{aligned}
 (x^k a(x); x^k b(x))^r &= (x^k a(x); h_2(x))^r \\
 &= (x^{\alpha-1-\deg(x^k a(x))} (x^k a(x))^*; x^{\beta-1-\deg(h_2(x))} h_2^*(x)) \\
 &= (x^{\alpha-1-\deg(x^k a(x))} a^*(x); 0) \\
 &\quad + (0; x^{\beta-1-\deg(h_2(x))} x^{n\beta-j} b^*(x)) \\
 &= x^{\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\
 &\quad + x^{(n+1)\beta-1-\deg((x^\beta-1)q_2(x))} * (0; b^*(x)).
 \end{aligned}$$

Since $\deg((x^\beta-1)q_2(x)) = \deg(x^k b(x))$, we have

$$(x^k a(x); x^k b(x))^r = x^{\alpha-1-\deg(x^k a(x))} * (a^*(x); 0)$$

$$+ x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)).$$

Case 4. $\deg(x^k a(x)) \geq \alpha$ and $\deg(x^k b(x)) \leq \beta - 1$:

Then, $x^k a(x) = (x^\alpha - 1)q_1(x) + h_1(x)$, where $q_1(x), h_1(x) \in R[x]$ and $\deg(h_1(x)) \leq \alpha - 1$. Hence,

$$a^*(x) = (x^\alpha - 1)q_1^*(x) + x^i h_1^*(x) \text{ and}$$

$$b^*(x) = (x^k b(x))^*,$$

where $i = \deg((x^\alpha - 1)q_1(x)) - \deg(h_1(x))$. Then, there exists the smallest positive integer m such that $m\alpha - i \geq 0$ and so, $h_1^*(x) = [x^{m\alpha-i} a^*(x)]_{(x^\alpha-1)}$. Hence,

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= (h_1(x); x^k b(x))^r \\ &= (x^{\alpha-1-\deg(h_1(x))} h_1^*(x); x^{\beta-1-\deg(x^k b(x))} (x^k b(x))^*) \\ &= (x^{\alpha-1-\deg(h_1(x))} x^{m\alpha-i} a^*(x); x^{\beta-1-\deg(x^k b(x))} b^*(x)) \\ &= x^{(m+1)\alpha-1-\deg((x^\alpha-1)q_1(x))} * (a^*(x); 0) \\ &\quad + x^{\beta-1-\deg(x^k b(x))} * (0; b^*(x)). \end{aligned}$$

Since $\deg((x^\alpha - 1)q_1(x)) = \deg(x^k a(x))$, we have

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{\beta-1-\deg(x^k b(x))} * (0; b^*(x)). \end{aligned}$$

In all four cases, we can conclude that

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)), \end{aligned}$$

where m, n are 0 or the smallest positive integers such that $m\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $n\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$. $\square$

Example 4.1.9. Let $(a(x); b(x)) = (x^2 + x; x + 1) \in R_{3,5}$.

We will compute $(x^2 a(x); x^2 b(x))^r$. Since $\deg(x^2 a(x)) = 4$, $\deg([x^2 a(x)]_{(x^3-1)}) = 1$, $\deg(x^2 b(x)) = 3$, we obtain that $m = 1$ such that $1(3) - 4 + 1 \geq 0$ and $n = 0$. By Proposition 4.1.8, we obtain that

$$(x^2(x^2 + x); x^2(x + 1))^r = x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0)$$

$$\begin{aligned}
& + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)) \\
& = x^{6-1-4} * (x+1; 0) + x^{5-1-3} * (0; x+1) \\
& = (x(x+1); 0) + (0; x(x+1)) \\
& = (x^2 + x; x^2 + x).
\end{aligned}$$

If we calculate directly, we have

$$\begin{aligned}
(x^2(x^2 + x); x^2(x+1))^r &= (x^4 + x^3 \pmod{x^3 - 1}; x^3 + x^2 \pmod{x^5 - 1})^r \\
&= (x+1; x^3 + x^2)^r \\
&= (x^{3-1-1}(x+1); x^{5-1-3}(x+1)) \\
&= (x^2 + x; x^2 + x).
\end{aligned}$$

4.1.2 Reversible-complement codes

In this section, we investigate the necessary and sufficient conditions for double cyclic codes to be reversible-complement codes. Recall that, for any $a \in R$, $\bar{a} = u + a$. This means that

$$\bar{0} = u, \bar{1} = 1 + u, \bar{u} = 0, \text{ and } \overline{1+u} = 1.$$

Lemma 4.1.10. *Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . If $\mathcal{C}$ is reversible-complement, then $\mathcal{C}$ contains the codeword*

$$(\underbrace{u, u, \dots, u}_{\alpha}; \underbrace{u, u, \dots, u}_{\beta}) := u\mathbb{I}(x) = (u + ux + \dots + ux^{\alpha-1}; u + ux + \dots + ux^{\beta-1}).$$

Proof. Suppose that $\mathcal{C}$ is a reversible-complement code. Consider,

$$\begin{aligned}
(\underbrace{0, 0, \dots, 0}_{\alpha}; \underbrace{0, 0, \dots, 0}_{\beta})^{rc} &= (\bar{0}, \bar{0}, \dots, \bar{0}; \bar{0}, \bar{0}, \dots, \bar{0}) \\
&= (\underbrace{u + 0, u + 0, \dots, u + 0}_{\alpha}; \underbrace{u + 0, u + 0, \dots, u + 0}_{\beta}) \\
&= (\underbrace{u, u, \dots, u}_{\alpha}; \underbrace{u, u, \dots, u}_{\beta}) + (\underbrace{0, 0, \dots, 0}_{\alpha}; \underbrace{0, 0, \dots, 0}_{\beta}).
\end{aligned}$$

Since $(\underbrace{0, 0, \dots, 0}_\alpha; \underbrace{0, 0, \dots, 0}_\beta)^{rc}$ and $(\underbrace{0, 0, \dots, 0}_\alpha; \underbrace{0, 0, \dots, 0}_\beta)$ are in $\mathcal{C}$, we obtain that $(\underbrace{u, u, \dots, u}_\alpha; \underbrace{u, u, \dots, u}_\beta) \in \mathcal{C}$. This implies that

$$u\mathbb{I}(x) = (u + ux + \dots + ux^{\alpha-1}; u + ux + \dots + ux^{\beta-1}) \in \mathcal{C}.$$

□

The following theorem provides helpful conditions for double cyclic codes to be reversible-complement codes and is used to support the proofs in other sections on reversible-complement codes.

Theorem 4.1.11. *Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . Then, $\mathcal{C}$ is reversible-complement if and only if*

1. $\mathcal{C}$ is a reversible code and
2. $(\underbrace{u, u, \dots, u}_\alpha; \underbrace{u, u, \dots, u}_\beta) \in \mathcal{C}$.

Proof. Suppose that $\mathcal{C}$ is a reversible-complement code. By Lemma 4.1.10, we obtain that $(\underbrace{u, u, \dots, u}_\alpha; \underbrace{u, u, \dots, u}_\beta) \in \mathcal{C}$. Let $\mathbf{v} = (a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathcal{C}$. Then, $\mathbf{v}^{rc} \in \mathcal{C}$. Consider,

$$\begin{aligned} \mathbf{v}^{rc} &= (\overline{a_{\alpha-1}}, \overline{a_{\alpha-2}}, \dots, \overline{a_0}; \overline{b_{\beta-1}}, \overline{b_{\beta-2}}, \dots, \overline{b_0}) \\ &= (u + a_{\alpha-1}, u + a_{\alpha-2}, \dots, u + a_0; u + b_{\beta-1}, u + b_{\beta-2}, \dots, u + b_0) \\ &= (\underbrace{u, u, \dots, u}_\alpha; \underbrace{u, u, \dots, u}_\beta) + \mathbf{v}^r. \end{aligned}$$

This implies that $\mathbf{v}^r \in \mathcal{C}$. Therefore, $\mathcal{C}$ is a reversible code.

On the other hand, let $\mathbf{v} \in \mathcal{C}$. Then, $\mathbf{v}^r \in \mathcal{C}$. By the above part, we have $\mathbf{v}^{rc} = (\underbrace{u, u, \dots, u}_\alpha; \underbrace{u, u, \dots, u}_\beta) + \mathbf{v}^r \in \mathcal{C}$. Thus, $\mathcal{C}$ is a reversible-complement code. □

4.2 The case α and β are both odd positive integers

In this section, we will provide the necessary and sufficient conditions for the double cyclic codes to be reversible and reversible-complement codes where both α and β are odd positive integers. Throughout this section, we let α and β be odd positive integers.

4.2.1 Reversible codes

Next, we will study the conditions for a non-separable double cyclic code $\mathcal{C}$ of length (α, β) over R to be reversible. By Proposition 4.1.8, for any $(a(x); b(x))$ in $R_{\alpha, \beta}$ and a positive integer k ,

$$(x^k a(x); x^k b(x))^r = x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)),$$

where $m = n = 0$ or m, n are the smallest positive integers such that

$$m\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0 \text{ and } n\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0.$$

For any odd positive integer α , we obtain that $\beta = (2\gamma + 1)\alpha$ is also an odd positive integer, where γ is a non-negative integer. By applying Proposition 4.1.8, we will obtain the following result:

Corollary 4.2.1. *Let $(a(x); b(x)) \in R_{\alpha, \beta}$ and k be a positive integer.*

Suppose that $\beta = (2\gamma + 1)\alpha$ and $\deg(b(x)) = 2\gamma\alpha + \deg(a(x))$, where $\gamma \in \mathbb{Z}^+ \cup \{0\}$. Then,

$$(x^k a(x); x^k b(x))^r = x^{(M(2\gamma+1)+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); b^*(x)),$$

where $M = 0$ or M is the smallest positive integer such that $M\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $M\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$.

Proof. Suppose that $\beta = (2\gamma + 1)\alpha$ and $\deg(b(x)) = 2\gamma\alpha + \deg(a(x))$, where $\gamma \in \mathbb{Z}^+ \cup \{0\}$. By Proposition 4.1.8,

$$(x^k a(x); x^k b(x))^r = x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0)$$

$$+ x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)),$$

where $m = n = 0$ or m, n are the smallest positive integers such that $m\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $n\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$. Let $M = \max\{m, n\}$. Then, $M = 0$ or M is the smallest positive integer such that

$$M\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0 \text{ and}$$

$$M\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0.$$

Without loss of generality, we suppose that $M = m$. Then $M = n + n'$ for some non-negative integer n' . Since $\deg(x^k b(x)) = 2\gamma\alpha + \deg(x^k a(x))$, hence

$$(M(2\gamma+1)+1)\alpha - 1 - \deg(x^k a(x)) = (n+1)\beta - 1 - \deg(x^k b(x)) + n'\beta.$$

Hence,

$$\begin{aligned} & x^{(M(2\gamma+1)+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); b^*(x)) \\ &= x^{(m+1)\alpha-1-\deg(x^k a(x))} x^{2m\gamma\alpha} * (a^*(x); 0) \\ &\quad + x^{(n+1)(2\gamma+1)\alpha-1-\deg(x^k b(x))} x^{n'\beta} * (0; b^*(x)) \\ &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)) \\ &= (x^k a(x); x^k b(x))^r. \end{aligned}$$

Therefore, $(x^k a(x); x^k b(x))^r = x^{(M(2\gamma+1)+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); b^*(x))$, where $M = 0$ or M is the smallest positive integer such that $M\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $M\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$. $\square$

Remark 4.2.2. Let α, β be positive integers and $\mathcal{C}$ be a double cyclic code of length (α, β) over R . Define

$$\varphi_\alpha : \mathcal{C} \longrightarrow R^\alpha \text{ by } \varphi_\alpha(\mathbf{a}; \mathbf{b}) = \mathbf{a} \text{ for all } (\mathbf{a}; \mathbf{b}) \in \mathcal{C} \text{ and}$$

$$\varphi_\beta : \mathcal{C} \longrightarrow R^\beta \text{ by } \varphi_\beta(\mathbf{a}; \mathbf{b}) = \mathbf{b} \text{ for all } (\mathbf{a}; \mathbf{b}) \in \mathcal{C}.$$

We can see that if $\mathcal{C}$ is a reversible code, then $\varphi_\alpha(\mathcal{C})$ and $\varphi_\beta(\mathcal{C})$ are reversible cyclic codes of length α and β over R , respectively. Moreover, $\tau_\beta(\mathcal{C})$ is the set of all polynomial representations of codewords in $\varphi_\beta(\mathcal{C})$.

The following lemmas are tools for proving the main theorem in this section.

Lemma 4.2.3. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ and $l(x)$ satisfy Theorem 3.2.1. If $\mathcal{C}$ is reversible, then $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal.*

Proof. Suppose that $\mathcal{C}$ is reversible. From Remark 4.2.2, we obtain that $\varphi_\beta(\mathcal{C})$ is reversible. Then, $\langle g_0(x) + ug_1(x) \rangle$ is a reversible cyclic code of length β over R . By Theorem 2.4.24, we obtain that $g_0(x)$ and $g_1(x)$ are self-reciprocal. We claim that $\langle (f_0(x) + uf_1(x); 0) \rangle$ is also double reversible cyclic code of length (α, β) over R . Since $\langle (f_0(x) + uf_1(x); 0) \rangle$ is an $R[x]$ -submodule of $R_{\alpha, \beta}$, thus $\langle (f_0(x) + uf_1(x); 0) \rangle$ is a double cyclic code of length (α, β) over R .

Assume that $I = \langle (f_0(x) + uf_1(x); 0) \rangle$ is not reversible. There is $v(x) \in I \subseteq \mathcal{C}$ such that $v^r(x) \in \mathcal{C} \setminus I$. Hence, $v(x) = \lambda(x) * (f_0(x) + uf_1(x); 0)$ and $v^r(x) = (x^{\alpha-1-\deg(h(x))}h^*(x); 0)$, where $[\lambda(x)(f_0(x) + uf_1(x))]_{(x^\alpha-1)} = h(x)$. Thus,

$$\begin{aligned} v^r(x) &= (x^{\alpha-1-\deg(h(x))}h^*(x); 0) \\ &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g_0(x) + ug_1(x)), \end{aligned}$$

where $\lambda_1(x), \lambda_2(x) \in R[x]$ and $\lambda_2(x) \neq 0$. This implies that

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x)]_{(x^\alpha-1)} = x^{\alpha-1-\deg(h(x))}h^*(x) \quad (4.2.1)$$

$$[\lambda_2(x)(g_0(x) + ug_1(x))]_{(x^\beta-1)} = 0. \quad (4.2.2)$$

By (4.2.2), we have that $\lambda_2(x)(g_0(x) + ug_1(x)) \equiv 0 \pmod{x^\beta - 1}$. By Remark 3.2.5, we have $\lambda_2(x) = \frac{x^\beta-1}{g_1(x)}\gamma_0(x) + u\frac{x^\beta-1}{g_0(x)}\gamma_1(x)$, where $\gamma_0(x), \gamma_1(x) \in \mathbb{F}_2[x]$. By Lemma 3.2.3, we obtain that

$$(f_0(x) + uf_1(x)) \mid \left[\frac{x^\beta-1}{g_1(x)}l(x) + u\frac{x^\beta-1}{g_0(x)}l(x) \right] \text{ in } \frac{R[x]}{\langle x^\alpha-1 \rangle}.$$

Then, $\lambda_2(x)l(x) \equiv q(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}$, where $q(x) \in R[x]$. By (4.2.1), we obtain that

$$[(\lambda_1(x) + q(x))(f_0(x) + uf_1(x))]_{(x^\alpha-1)} = x^{\alpha-1-\deg(h(x))}h^*(x).$$

Thus, $v^r(x) = (x^{\alpha-1-\deg(h(x))}h^*(x); 0) = (\lambda_1(x) + q(x)) * (f_0(x) + uf_1(x); 0) \in I$, which is a contradiction. Hence, $I = \langle (f_0(x) + uf_1(x); 0) \rangle$ is a reversible code. Therefore, $\varphi_\alpha(I) = \langle f_0(x) + uf_1(x) \rangle$ is a reversible cyclic code of length α over R . By Theorem 2.4.24, $f_0(x)$ and $f_1(x)$ are self-reciprocal. $\square$

From the above theorem, we studied the necessary condition of $f_0(x), f_1(x), g_0(x), g_1(x)$ for a reversible code $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$, where the lengths α and β are odd positive integers. Next, we will study the necessary condition of $l(x)$ for $\mathcal{C}$, when $\beta = (2\gamma + 1)\alpha$ and γ is a non-negative integer.

Lemma 4.2.4. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length $(\alpha, \beta = (2\gamma + 1)\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ and $l(x)$ satisfy Theorem 3.2.1 and γ is a non-negative integer. Suppose that $\deg(g_0(x) + ug_1(x)) = 2\gamma\alpha + \deg(l(x))$.*

If $\mathcal{C}$ is reversible, then

$$(f_0(x) + uf_1(x)) \mid \left(l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x) \right)$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\eta_1(x), \eta_2(x) \in \mathbb{F}_2[x]$ such that $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta - 1}{g_0(x)} = 1$ and $i = \deg(g_0(x)) - \deg(g_1(x))$.

Proof. Let $\beta = (2\gamma + 1)\alpha$, where γ is a non-negative integer. Suppose that $\mathcal{C}$ is a reversible code. By Lemma 4.2.3, we obtain that $f_0(x), f_1(x), g_0(x)$ and $g_1(x)$ are self-reciprocal. Since $(l(x); g_0(x) + ug_1(x)) \in \mathcal{C}$,

$$\begin{aligned} & (x^{\alpha-1-\deg(l(x))}l^*(x); x^{\beta-1-\deg(g_0(x)+ug_1(x))}(g_0(x) + ug_1(x))^*) \\ &= (l(x); g_0(x) + ug_1(x))^r \in \mathcal{C} \end{aligned}$$

This implies that

$$\begin{aligned} & (l^*(x); (g_0(x) + ug_1(x))^*) \\ &= x^{2\gamma\alpha + \deg(l(x)) + 1} * (x^{\alpha-1-\deg(l(x))}l^*(x); x^{\beta-1-\deg(g_0(x)+ug_1(x))}(g_0(x) + ug_1(x))^*) \in \mathcal{C}. \end{aligned}$$

Hence,

$$\begin{aligned} & (l^*(x); (g_0(x) + ug_1(x))^*) \\ &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g_0(x) + ug_1(x)), \end{aligned}$$

where $\lambda_1(x), \lambda_2(x) \in R[x]$. So,

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x)]_{(x^\alpha-1)} = l^*(x) \text{ and} \quad (4.2.3)$$

$$[\lambda_2(x)(g_0(x) + ug_1(x))]_{(x^\beta-1)} = g_0(x) + ux^i g_1(x), \quad (4.2.4)$$

where $i = \deg(g_0(x)) - \deg(g_1(x))$. Consider,

$$[u(g_0(x) + ug_1(x))]_{(x^\beta-1)} = ug_0(x) \text{ and} \quad (4.2.5)$$

$$\left[\frac{x^\beta - 1}{g_0(x)} (g_0(x) + ug_1(x)) \right]_{(x^\beta-1)} = \frac{x^\beta - 1}{g_0(x)} ug_1(x). \quad (4.2.6)$$

Since $\gcd(g_0(x), \frac{x^\beta-1}{g_0(x)}) = 1$, there exist $\eta_1(x), \eta_2(x) \in \mathbb{F}_2[x]$ such that $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta-1}{g_0(x)} = 1$. Thus,

$$\begin{aligned} ug_1(x) &= ug_1(x) \left(\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta-1}{g_0(x)} \right) \\ &= ug_0(x)g_1(x)\eta_1(x) + ug_1(x)\frac{x^\beta-1}{g_0(x)}\eta_2(x). \end{aligned}$$

By (4.2.5) and (4.2.6), we obtain that

$$ug_1(x) \equiv \left(u\eta_1(x)g_1(x) + \eta_2(x)\frac{x^\beta-1}{g_0(x)} \right) (g_0(x) + ug_1(x)) \pmod{x^\beta-1}.$$

Hence,

$$ux^i g_1(x) \equiv x^i \left(u\eta_1(x)g_1(x) + \eta_2(x)\frac{x^\beta-1}{g_0(x)} \right) (g_0(x) + ug_1(x)) \pmod{x^\beta-1}$$

and

$$\begin{aligned} g_0(x) &= g_0(x) + ug_1(x) + ug_1(x) \\ &\equiv \left(1 + u\eta_1(x)g_1(x) + \eta_2(x)\frac{x^\beta-1}{g_0(x)} \right) (g_0(x) + ug_1(x)) \pmod{x^\beta-1}. \end{aligned}$$

Therefore,

$$\begin{aligned} & g_0(x) + ux^i g_1(x) \\ & \equiv \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right) (g_0(x) + ug_1(x)) \pmod{x^\beta - 1}. \end{aligned}$$

By (4.2.4), we obtain that

$$\begin{aligned} & \lambda_2(x)(g_0(x) + ug_1(x)) \\ & \equiv \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right) (g_0(x) + ug_1(x)) \pmod{x^\beta - 1}. \end{aligned}$$

Then,

$$\begin{aligned} & \left(\lambda_2(x) - \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right) \right) (g_0(x) + ug_1(x)) \\ & \equiv 0 \pmod{x^\beta - 1}. \end{aligned}$$

This implies that

$$\lambda_2(x) - \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right) = \frac{x^\beta - 1}{g_1(x)}h_1(x) + u\frac{x^\beta - 1}{g_0(x)}h_2(x),$$

where $h_1(x), h_2(x) \in \mathbb{F}_2[x]$. Then,

$$\lambda_2(x) = \frac{x^\beta - 1}{g_1(x)}h_1(x) + u\frac{x^\beta - 1}{g_0(x)}h_2(x) + \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right).$$

By Lemma 3.2.3, we have

$$\frac{x^\beta - 1}{g_1(x)}h_1(x)l(x) + u\frac{x^\beta - 1}{g_0(x)}h_2(x)l(x) \equiv q(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

By (4.2.3), we have

$$\begin{aligned} l^*(x) & \equiv \lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x) \pmod{x^\alpha - 1} \\ & \equiv \lambda_1(x)(f_0(x) + uf_1(x)) + \frac{x^\beta - 1}{g_1(x)}h_1(x)l(x) + u\frac{x^\beta - 1}{g_0(x)}h_2(x)l(x) \\ & \quad + \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right)l(x) \pmod{x^\alpha - 1} \\ & \equiv \lambda_1(x)(f_0(x) + uf_1(x)) + q(x)(f_0(x) + uf_1(x)) \\ & \quad + \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right)l(x) \pmod{x^\alpha - 1} \\ & \equiv (\lambda_1(x) + q(x))(f_0(x) + uf_1(x)) \end{aligned}$$

$$+ \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}\right)l(x) \pmod{x^\alpha - 1}.$$

Then,

$$\begin{aligned} l^*(x) + \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}\right)l(x) \\ \equiv (\lambda_1(x) + q(x))(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}. \end{aligned}$$

This implies that

$$(f_0(x) + uf_1(x)) \mid \left(l^*(x) + \left(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}\right)l(x)\right)$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. □

By Lemmas 4.2.3 and 4.2.4, we obtain the next result.

Theorem 4.2.5. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length $(\alpha, \beta = (2\gamma + 1)\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ and $l(x)$ satisfy Theorem 3.2.1 and γ is a non-negative integer. Suppose that $\deg(g_0(x) + ug_1(x)) = 2\gamma\alpha + \deg(l(x))$.*

Then, $\mathcal{C}$ is reversible if and only if

1. $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal and
2. $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x))$
in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\eta_1(x), \eta_2(x) \in \mathbb{F}_2[x]$ such that $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta - 1}{g_0(x)} = 1$
and $i = \deg(g_0(x)) - \deg(g_1(x))$.

Proof. Suppose that $\mathcal{C}$ is reversible. By Lemmas 4.2.3 and 4.2.4, we obtain the results.

On the other hand, we suppose that $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal and

$$(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x))$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\eta_1(x), \eta_2(x) \in \mathbb{F}_2[x]$ such that $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta - 1}{g_0(x)} = 1$ and $i = \deg(g_0(x)) - \deg(g_1(x))$. Since $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta - 1}{g_0(x)} = 1$, we obtain that

$$\begin{aligned} & \left[(1 + (1 + x^i)u\eta_1(x)g_1(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)})(g_0(x) + ug_1(x)) \right]_{(x^\beta - 1)} \\ &= g_0(x) + ux^i g_1(x). \end{aligned}$$

Since $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$,

$$\begin{aligned} & l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x) \\ & \equiv k(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}, \end{aligned}$$

where $k(x) \in R[x]$. So,

$$\begin{aligned} & (l^*(x); (g_0(x) + ug_1(x))^*) \\ &= ((f_0(x) + uf_1(x))k(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) \\ & \quad + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x); \\ & \quad (g_0(x) + ug_1(x)) + (1 + x^i)u\eta_1(x)g_1(x)(g_0(x) + ug_1(x)) \\ & \quad + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}(g_0(x) + ug_1(x))) \\ &= k(x) * (f_0(x) + uf_1(x); 0) + (l(x); g_0(x) + ug_1(x)) \\ & \quad + \left((1 + x^i)u\eta_1(x)g_1(x) \right) * (l(x); g_0(x) + ug_1(x)) \\ & \quad + \left((1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)} \right) * (l(x); g_0(x) + ug_1(x)). \end{aligned}$$

This implies that $(l^*(x); (g_0(x) + ug_1(x))^*) \in \mathcal{C}$. Since $\gcd(f_0(x), \frac{x^\alpha - 1}{f_0(x)}) = 1$, there exist $\eta'_1(x), \eta'_2(x) \in \mathbb{F}_2[x]$ such that $\eta'_1(x)f_0(x) + \eta'_2(x)\frac{x^\alpha - 1}{f_0(x)} = 1$. Then, we obtain that

$$\begin{aligned} & \left[(1 + (1 + x^j)u\eta'_1(x)f_1(x) + (1 + x^j)\eta'_2(x)\frac{x^\alpha - 1}{f_0(x)})(f_0(x) + uf_1(x)) \right]_{(x^\alpha - 1)} \\ &= f_0(x) + ux^j f_1(x), \end{aligned}$$

where $j = \deg(f_0(x)) - \deg(f_1(x))$. Hence,

$$((f_0(x) + uf_1(x))^*; 0)$$

$$\begin{aligned}
&= (f_0(x) + ux^j f_1(x); 0) \\
&= (1 + (1 + x^j)u\eta'_1(x)f_1(x) + (1 + x^j)\eta'_2(x)\frac{x^\alpha - 1}{f_0(x)}) * (f_0(x) + uf_1(x); 0) \in \mathcal{C}.
\end{aligned}$$

This implies that $((f_0(x) + uf_1(x))^*; 0) \in \mathcal{C}$. Next, we will show that $\mathcal{C}$ is reversible. Let $v(x) \in \mathcal{C}$. Then,

$$v(x) = \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g_0(x) + ug_1(x)),$$

where $\lambda_1(x), \lambda_2(x) \in R[x]$. Consider,

$$v^r(x) = (\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r.$$

By Proposition 4.1.7, we have

$$v^r(x) = (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r + (\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r.$$

Suppose that $\lambda_1(x) = a_0 + a_1x + \dots + a_tx^t \in R[x]$ for some non-negative integer t . We consider

$$\begin{aligned}
(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r &= \left(\sum_{i=0}^t a_i x^i (f_0(x) + uf_1(x)); 0 \right)^r \\
&= \sum_{i=0}^t a_i * (x^i (f_0(x) + uf_1(x)); 0)^r.
\end{aligned}$$

By Proposition 4.1.8, there exists $m_i \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^i (f_0(x) + uf_1(x)); 0)^r = x^{(m_i+1)\alpha-1-\kappa} * ((f_0(x) + uf_1(x))^*; 0),$$

where $\kappa = \deg(x^i (f_0(x) + uf_1(x)))$ and $0 \leq i \leq t$. This implies that

$$(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r \in \mathcal{C}.$$

Suppose that $\lambda_2(x) = b_0 + b_1x + \dots + b_sx^s \in R[x]$ for some non-negative integer s . We consider

$$(\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r = \left(\sum_{j=0}^s b_j x^j l(x); \sum_{j=0}^s b_j x^j (g_0(x) + ug_1(x)) \right)^r$$

$$= \sum_{j=0}^s b_j * (x^j l(x); x^j (g_0(x) + u g_1(x)))^r.$$

By Corollary 4.2.1, there exists $n_j \in \mathbb{Z}^+ \cup \{0\}$ such that

$$\begin{aligned} & (x^j l(x); x^j (g_0(x) + u g_1(x)))^r \\ &= x^{(n_j(2\gamma+1)+1)\alpha-1-\deg(x^j l(x))} * (l^*(x); (g_0(x) + u g_1(x))^*), \end{aligned}$$

where $0 \leq j \leq s$. This implies that $(\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + u g_1(x)))^r \in \mathcal{C}$. Hence,

$$v^r(x) = (\lambda_1(x)(f_0(x) + u f_1(x)); 0)^r + (\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + u g_1(x)))^r \in \mathcal{C}.$$

Therefore, $\mathcal{C}$ is a reversible code. $\square$

Corollary 4.2.6. *Let $\mathcal{C} = \langle (f_0(x) + u f_1(x); 0), (l(x); g_0(x) + u g_1(x)) \rangle$ be a double cyclic code of length $(\alpha, \beta = (2\gamma + 1)\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ and $l(x)$ satisfy Theorem 3.2.1 and γ is a non-negative integer. Suppose that $\deg(g_0(x)) = \deg(g_1(x)) = 2\gamma\alpha + \deg(l(x))$.*

Then, $\mathcal{C}$ is reversible if and only if $f_0(x), f_1(x), g_0(x)$ and $g_1(x)$ are self-reciprocal and $(f_0(x) + u f_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. By Theorem 4.2.5, we obtain that $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal and

$$(f_0(x) + u f_1(x)) \mid (l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x))$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\eta_1(x), \eta_2(x) \in \mathbb{F}_2[x]$ such that $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta - 1}{g_0(x)} = 1$ and $i = \deg(g_0(x)) - \deg(g_1(x))$. Since $\deg(g_0(x)) = \deg(g_1(x))$, $i = 0$. Hence, $(f_0(x) + u f_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

On the other hand, suppose that $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal and $(f_0(x) + u f_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Then,

$$\begin{aligned} & \left[(1 + (1 + x^i)u\eta_1(x)f_1(x) + (1 + x^i)\eta_2(x)\frac{x^\alpha - 1}{f_0(x)})(f_0(x) + u f_1(x)) \right]_{(x^\alpha - 1)} \\ &= f_0(x) + u x^i f_1(x), \end{aligned}$$

where $\eta_1(x)f_0(x) + \eta_2(x)\frac{x^\alpha-1}{f_0(x)} = 1$ and $i = \deg(f_0(x)) - \deg(f_1(x))$. Hence,

$$\begin{aligned} & ((f_0(x) + uf_1(x))^*; 0) \\ &= (f_0(x) + ux^j f_1(x); 0) \\ &= (1 + (1 + x^j)u\eta_1(x)f_1(x) + (1 + x^j)\eta_2(x)\frac{x^\alpha-1}{f_0(x)}) * (f_0(x) + uf_1(x); 0) \in \mathcal{C}. \end{aligned}$$

Since $\deg(g_0(x)) = \deg(g_1(x))$, we have $(g_0(x) + ug_1(x))^* = g_0(x) + ug_1(x)$. Since $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha-1 \rangle}$, there is a polynomial $q(x)$ in $R[x]$ such that $l(x) + l^*(x) \equiv q(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha-1}$. Then,

$$(l^*(x); (g_0(x) + ug_1(x))^*) = q(x) * (f_0(x) + uf_1(x); 0) + (l(x); (g_0(x) + ug_1(x))).$$

Hence, $(l^*(x); (g_0(x) + ug_1(x))^*) \in \mathcal{C}$. Similar to the last part of the proof of Theorem 4.2.5, we let $v(x) \in \mathcal{C}$. Then,

$$v(x) = \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g_0(x) + ug_1(x)),$$

where $\lambda_1(x), \lambda_2(x) \in R[x]$. Consider,

$$v^r(x) = (\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r.$$

By Proposition 4.1.7, we have

$$v^r(x) = (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r + (\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r.$$

Suppose that $\lambda_1(x) = a_0 + a_1x + \cdots + a_tx^t \in R[x]$ for some non-negative integer t . We consider

$$\begin{aligned} (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r &= \left(\sum_{i=0}^t a_i x^i (f_0(x) + uf_1(x)); 0 \right)^r \\ &= \sum_{i=0}^t a_i * (x^i (f_0(x) + uf_1(x)); 0)^r. \end{aligned}$$

By Proposition 4.1.8, there exists $m_i \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^i (f_0(x) + uf_1(x)); 0)^r = x^{(m_i+1)\alpha-1-\kappa} * ((f_0(x) + uf_1(x))^*; 0),$$

where $\kappa = \deg(x^i (f_0(x) + uf_1(x)))$ and $0 \leq i \leq t$. This implies that

$$(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r \in \mathcal{C}.$$

Suppose that $\lambda_2(x) = b_0 + b_1x + \cdots + b_sx^s \in R[x]$ for some non-negative integer s . We consider

$$\begin{aligned} (\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r &= \left(\sum_{j=0}^s b_j x^j l(x); \sum_{j=0}^s b_j x^j (g_0(x) + ug_1(x)) \right)^r \\ &= \sum_{j=0}^s b_j * (x^j l(x); x^j (g_0(x) + ug_1(x)))^r. \end{aligned}$$

By Corollary 4.2.1, there exists $n_j \in \mathbb{Z}^+ \cup \{0\}$ such that

$$\begin{aligned} &(x^j l(x); x^j (g_0(x) + ug_1(x)))^r \\ &= x^{(n_j(2\gamma+1)+1)\alpha-1-\deg(x^j l(x))} * (l^*(x); (g_0(x) + ug_1(x))^*), \end{aligned}$$

where $0 \leq j \leq s$. This implies that $(\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r \in \mathcal{C}$. Hence,

$$v^r(x) = (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r + (\lambda_2(x)l(x); \lambda_2(x)(g_0(x) + ug_1(x)))^r \in \mathcal{C}.$$

Therefore, $\mathcal{C}$ is a reversible code. □

The following examples are double cyclic codes of length (α, β) over the ring R , which are reversible codes derived from the theorems presented in this section:

Example 4.2.7. Let $\alpha = 3 = \beta$. Then, $\gamma = 0$. Consider,

$$x^\alpha - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x].$$

Suppose $\mathcal{C} = \langle (m_1(x) + u; 0), (x^2 + (1 + u)x + 1; (1 + u)m_2(x)) \rangle$. Let $l(x) = x^2 + (1 + u)x + 1$. Then, $\deg((1 + u)m_2(x)) = \deg(l(x))$ and $l(x) = l^*(x)$. Hence, $(m_1(x) + u) \mid (l(x) + l^*(x))$. Since $x^2 + (1 + u)x + 1 = x(m_1(x) + u) + 1$, $\mathcal{C}$ can be reduce as

$$\mathcal{C} = \langle (m_1(x) + u; 0), (1; (1 + u)m_2(x)) \rangle.$$

By Corollary 4.2.6, we obtain that the code $\mathcal{C}$ is a reversible code and $|\mathcal{C}| = 128$. In addition, a double cyclic code generated from $\mathcal{C}$ is given in Table 18.

Example 4.2.8. Let $\alpha = 3$ and $\gamma = 1$. Then, $\beta = (2\gamma + 1)\alpha = 9$. Consider,

$$x^3 - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and}$$

$$x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1) = m_1(x)m_2(x)m_3(x) \in \mathbb{F}_2[x].$$

Suppose $\mathcal{C} = \langle ((1 + u)m_2(x); 0), (ux + u; m_1(x)m_3(x) + um_3(x)) \rangle$. By Theorem 3.2.1, we obtain that the code $\mathcal{C}$ is a double cyclic code of length $(3, 9)$ over R . Let $l(x) = ux + u$ and $i = \deg(g_0(x)) - \deg(g_1(x)) = 1$. Then, $\deg(m_1(x)m_3(x) + um_3(x)) = 6 + \deg(l(x))$. Since $m_1(x)m_3(x)$ and $\frac{x^\beta - 1}{m_1(x)m_3(x)}$ are coprime, we obtain that

$$\begin{aligned} 1 &= \eta_1(x)m_1(x)m_3(x) + \eta_2(x)\frac{x^\beta - 1}{m_1(x)m_3(x)} \\ &= xm_1(x)m_3(x) + (x^6 + x^4 + 1)\frac{x^\beta - 1}{m_1(x)m_3(x)}. \end{aligned}$$

Consider,

$$\begin{aligned} l^*(x) + l(x) + (1 + x^i)u\eta_1(x)m_3(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{m_1(x)m_3(x)}l(x) \\ &= (1 + x)(x^6 + x^4 + 1)(x^2 + x + 1)(ux + u) \\ &\equiv (ux + u)(x^2 + x + 1) \pmod{x^3 - 1} \\ &\equiv 0 \pmod{x^3 - 1}. \end{aligned}$$

Hence, $((1 + u)m_2(x)) \mid [l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x)]$ in $\frac{R[x]}{\langle x^3 - 1 \rangle}$. By Theorem 4.2.5, we obtain that $\mathcal{C}$ is a reversible code and $|\mathcal{C}| = 128$.

In addition, a double cyclic code generated from $\mathcal{C}$ is given in Table 19.

4.2.2 Reversible-complement codes

By using the results in the Section 4.2.1 and Theorem 4.1.11, we get the results in this section directly.

Proposition 4.2.9. Let $\mathcal{C}$ be a double cyclic code of length (α, β) over R . Suppose that $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (0; g_0(x) + ug_1(x)) \rangle$ is a separable code, where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ satisfy Theorem 3.2.1. Then, $\mathcal{C}$ is reversible-complement if and only if $f_0(x), f_1(x), g_0(x)$ and $g_1(x)$ are self-reciprocal and $u\mathbb{I}(x) \in \mathcal{C}$.

Theorem 4.2.10. Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length $(\alpha, \beta = (2\gamma + 1)\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ and $l(x)$ satisfy Theorem 3.2.1 and γ is non-negative integer. Suppose that $\deg(g_0(x) + ug_1(x)) = 2\gamma\alpha + \deg(l(x))$.

Then, $\mathcal{C}$ is reversible-complement if and only if

1. $u\mathbb{I}(x) = (u + ux + \cdots + ux^{\alpha-1}; u + ux + \cdots + ux^{\beta-1}) \in \mathcal{C}$,
2. $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal and
3. $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x) + (1+x^i)u\eta_1(x)g_1(x)l(x) + (1+x^i)\eta_2(x)\frac{x^\beta-1}{g_0(x)}l(x))$ in $\frac{R[x]}{(x^\alpha-1)}$, where $\eta_1(x), \eta_2(x) \in \mathbb{F}_2[x]$ such that $\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta-1}{g_0(x)} = 1$ and $i = \deg(g_0(x)) - \deg(g_1(x))$.

Corollary 4.2.11. Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$ be a double cyclic code of length $(\alpha, \beta = (2\gamma + 1)\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g_0(x), g_1(x)$ and $l(x)$ satisfy Theorem 3.2.1 and $\gamma \in \mathbb{Z}^+ \cup \{0\}$. Suppose that $\deg(g_0(x)) = \deg(g_1(x)) = 2\gamma\alpha + \deg(l(x))$.

Then, $\mathcal{C}$ is reversible-complement if and only if

1. $u\mathbb{I}(x) = (u + ux + \cdots + ux^{\alpha-1}; u + ux + \cdots + ux^{\beta-1}) \in \mathcal{C}$,
2. $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal and
3. $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{(x^\alpha-1)}$.

The following example is a double cyclic code of length (α, β) over the ring R , which is a reversible-complement code derived from the theorems presented in this section:

Example 4.2.12. Let $\alpha = 3$ and $\beta = 9$. Consider,

$$x^3 - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and}$$

$$x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1) = m_1(x)m_2(x)m_3(x) \in \mathbb{F}_2[x].$$

Suppose $\mathcal{C} = \langle ((1 + u)m_1(x); 0), (x^2; (1 + u)m_2(x)m_3(x)) \rangle$. By Corollary 4.2.6, $\mathcal{C}$ is a reversible code. Moreover, $\mathcal{C}$ can be reduced as

$$\mathcal{C} = \langle ((1 + u)m_1(x); 0), (1; (1 + u)m_2(x)m_3(x)) \rangle.$$

Consider,

$$u\mathbb{I}(x) = u * ((1 + u)m_1(x); 0) + ux^2 * (1; (1 + u)m_2(x)m_3(x)) \in \mathcal{C}.$$

By Corollary 4.2.11, $\mathcal{C}$ is a reversible-complement code and $|\mathcal{C}| = 64$. In addition, a DNA code $\mathcal{D}$ of length 12 with minimum Hamming distance 2 from $\mathcal{C} \cup \hat{\mathcal{C}}$ has 126 codewords, which are given in Table 20.

4.3 The case α is an odd and β is an even positive integer

In this section, we will provide the necessary and sufficient conditions for the double cyclic codes to be reversible and reversible-complement codes where α is an odd positive integer and β is an even positive integer. Throughout this section, we let α be an odd positive integer and β be an even positive integer.

4.3.1 Reversible codes

Next, we will study the conditions for a non-separable double cyclic code $\mathcal{C}$ of length (α, β) over R to be reversible. By Proposition 4.1.8, for any $(a(x); b(x))$ in $R_{\alpha, \beta}$ and a positive integer k ,

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)), \end{aligned}$$

where $m = n = 0$ or m, n are the smallest positive integers such that

$$\begin{aligned} m\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) &\geq 0 \text{ and} \\ n\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) &\geq 0. \end{aligned}$$

For any odd positive integer α , we obtain that $\beta = 2\gamma\alpha$ is an even positive integer, where γ is a non-negative integer. By applying Proposition 4.1.8, we will obtain the following result.

Corollary 4.3.1. *Let $(a(x); b(x)) \in R_{\alpha, \beta}$ and k be a positive integer.*

Suppose that $\beta = 2\gamma\alpha$ and $\deg(b(x)) = (2\gamma - 1)\alpha + \deg(a(x))$, where γ is

a non-negative integer. Then,

$$(x^k a(x); x^k b(x))^r = x^{(2M\gamma+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); b^*(x)),$$

where $M = 0$ or M is the smallest positive integer such that $M\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $M\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$.

Proof. Suppose that $\beta = 2\gamma\alpha$ and $\deg(b(x)) = (2\gamma - 1)\alpha + \deg(a(x))$. By Proposition 4.1.8, we obtain that

$$\begin{aligned} (x^k a(x); x^k b(x))^r &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) \\ &\quad + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)), \end{aligned}$$

where $m = n = 0$ or m, n are the smallest positive integers such that $m\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $n\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$. Let $M = \max\{m, n\}$. Then, $M = 0$ or M is the smallest positive integer such that

$$\begin{aligned} M\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) &\geq 0 \text{ and} \\ M\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) &\geq 0. \end{aligned}$$

Without loss of generality, we suppose that $M = m$. Then, $M = n + n'$ for some non-negative integer n' . Since $\deg(x^k b(x)) = \deg(x^k a(x)) + (2\gamma - 1)\alpha$,

$$\begin{aligned} (2M\gamma + 1)\alpha - 1 - \deg(x^k a(x)) &= 2n\gamma\alpha + 2n'\gamma\alpha + \alpha - 1 - \deg(x^k a(x)) \\ &= n\beta + n'\beta + \alpha - 1 - \deg(x^k a(x)) \\ &= n\beta + n'\beta + \alpha - 1 - \deg(x^k b(x)) + 2\gamma\alpha \\ &= (n + 1)\beta - 1 - \deg(x^k b(x)) + n'\beta. \end{aligned}$$

Hence,

$$\begin{aligned} &x^{(2M\gamma+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); b^*(x)) \\ &= x^{m(2\gamma)\alpha+\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) + x^{(n+1)\beta-1-\deg(x^k a(x))+n'\beta} * (0; b^*(x)) \\ &= x^{(m+1)\alpha-1-\deg(x^k a(x))+m(2\gamma-1)\alpha} * (a^*(x); 0) + x^{(n+1)\beta-1-\deg(x^k a(x))+n'\beta} * (0; b^*(x)) \\ &= x^{(m+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); 0) + x^{(n+1)\beta-1-\deg(x^k b(x))} * (0; b^*(x)) \\ &= (x^k a(x); x^k b(x))^r. \end{aligned}$$

Therefore,

$$(x^k a(x); x^k b(x))^r = x^{(2M\gamma+1)\alpha-1-\deg(x^k a(x))} * (a^*(x); b^*(x)),$$

where $M = 0$ or M is the smallest positive integer such that $M\alpha - \deg(x^k a(x)) + \deg([x^k a(x)]_{(x^\alpha-1)}) \geq 0$ and $M\beta - \deg(x^k b(x)) + \deg([x^k b(x)]_{(x^\beta-1)}) \geq 0$. $\square$

Remark 4.3.2. Let $q_0(x) + uq_1(x)$ and $g_0(x) + ug_1(x)$ be polynomials over R such that $q_0(x), q_1(x), g_0(x), g_1(x) \in \mathbb{F}_2[x]$ and $g_0(x) \neq 0$ and $g_1(x) \neq 0$.

If $(q_0(x) + uq_1(x))(g_0(x) + ug_1(x)) = 0$, then $q_0(x) + uq_1(x) = 0$.

Moreover, if $g_0(x) = 0$ and $g_1(x) \neq 0$, then $q_0(x) = 0$.

Proof. Suppose that $(q_0(x) + uq_1(x))(g_0(x) + ug_1(x)) = 0$. Consider,

$$q_0(x)g_0(x) + u(q_0(x)g_1(x) + q_1(x)g_0(x)) = 0.$$

Hence, we obtain that

$$q_0(x)g_0(x) = 0 \text{ and} \tag{4.3.1}$$

$$q_0(x)g_1(x) + q_1(x)g_0(x) = 0. \tag{4.3.2}$$

By multiplying $g_1(x)$ and $g_0(x)$ in both sides of equations (4.3.1) and (4.3.2), respectively, we obtain that

$$q_0(x)g_0(x)g_1(x) = 0 \text{ and}$$

$$q_0(x)g_1(x)g_0(x) + q_1(x)g_0(x)g_0(x) = 0.$$

Hence, $q_1(x)g_0(x)g_0(x) = 0$. Since $g_0(x)g_0(x) \neq 0$, $q_1(x) = 0$. This implies that $q_0(x) = 0$. Therefore, $q_0(x) + uq_1(x) = 0$. Moreover, if $g_0(x) = 0$, then, $uq_0(x)g_1(x) = 0$. Hence, $q_0(x) = 0$. $\square$

The following lemmas are tools for proving the main theorem for double cyclic codes of length (α, β) over R type 1.

Lemma 4.3.3. Let $\mathcal{C} = \langle (f_0(x), f_1(x); 0), (l(x); g(x) + up(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), l(x)$ satisfy Theorem 3.3.1 (Type 1).

If $\mathcal{C}$ is a reversible code, then

1. $f_0(x), f_1(x)$ and $g(x)$ are self-reciprocal and
2. $x^i p^*(x) = p(x)$ or $g(x) = x^i p^*(x) + p(x)$, where $i = \deg(g(x)) - \deg(p(x))$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. From Remark 4.2.2, we obtain that $\langle g(x) + up(x) \rangle$ is a reversible cyclic code of length β over R . By Theorem 2.4.24, we obtain that

1. $g(x)$ is self-reciprocal,
2. $x^i p^*(x) = p(x)$ or $g(x) = x^i p^*(x) + p(x)$, where $i = \deg(g(x)) - \deg(p(x))$.

Let $I = \langle (f_0(x) + uf_1(x); 0) \rangle \subseteq \mathcal{C}$. We claim that I is a reversible code. Since I is an $R[x]$ -submodule of $R_{\alpha, \beta}$, I is a double cyclic code of length (α, β) over R .

Assume that I is not a reversible code. Then, there exists a polynomial $v(x) \in I$ such that $v^r(x) \in \mathcal{C} - I$. Hence,

$$\begin{aligned} v(x) &= \lambda(x) * (f_0(x) + uf_1(x); 0) \text{ for some } \lambda(x) \in R[x] \text{ and} \\ v^r(x) &= (x^{\alpha-1-\deg(h(x))} h^*(x); 0), \text{ where } h(x) = [\lambda(x)(f_0(x) + uf_1(x))]_{(x^\alpha-1)}. \end{aligned}$$

This implies that

$$\begin{aligned} v^r(x) &= (x^{\alpha-1-\deg(h(x))} h^*(x); 0) \\ &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g(x) + up(x)) \end{aligned}$$

for some $\lambda_1(x), \lambda_2(x) \in R[x]$ such that $\lambda_2(x) \neq 0$. Thus,

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x)]_{(x^\alpha-1)} = x^{\alpha-1-\deg(h(x))} h^*(x) \text{ and} \quad (4.3.3)$$

$$[\lambda_2(x)(g(x) + up(x))]_{(x^\beta-1)} = 0. \quad (4.3.4)$$

By (4.3.4) and Remark 4.3.2, $\lambda_2(x) = \frac{x^\beta-1}{g(x)+up(x)} k(x)$, where $k(x) \in R[x]$. By Lemma 3.3.2, we have

$$(f_0(x) + uf_1(x)) \mid \left(\frac{x^\beta-1}{g(x)+up(x)} k(x) l(x) \right) \text{ in } \frac{R[x]}{\langle x^\alpha-1 \rangle}.$$

Then, $\lambda_2(x)l(x) = \lambda_3(x)(f_0(x) + uf_1(x)) + q_1(x)(x^\alpha-1)$ for some $\lambda_3(x), q_1(x) \in R[x]$. By (4.3.3), there exists $q_2(x) \in R[x]$ such that

$$(\lambda_1(x) + \lambda_3(x))(f_0(x) + uf_1(x)) = q_2(x)(x^\alpha-1) + x^{\alpha-1-\deg(h(x))} h^*(x).$$

This means that $(x^{\alpha-1-\deg(h(x))}h^*(x); 0) \in I$, which is a contradiction. Hence, I is a reversible code. By Theorem 2.4.24, $f_0(x)$ and $f_1(x)$ are self-reciprocal. $\square$

From the above theorem, we studied the necessary condition of $f_0(x)$, $f_1(x)$, $g(x)$ and $p(x)$ for a reversible code $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$. Next, we will study the necessary condition of $l(x)$ for $\mathcal{C}$, when $\beta = 2\gamma\alpha$ and γ is a non-negative integer.

Lemma 4.3.4. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), l(x)$ satisfy Theorem 3.3.1 (Type 1). Suppose that $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l(x))$.

If $\mathcal{C}$ is a reversible code, then

1. $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Or
2. $(f_0(x) + uf_1(x)) \mid (l^*(x) + (1 + u)l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. Since $(l(x); g(x) + up(x)) \in \mathcal{C}$, we obtain that

$$(x^{\alpha-1-\deg(l(x))}l^*(x); x^{\beta-1-\deg(g(x)+up(x))}(g(x) + up(x)))^* = (l(x); g(x) + up(x))^r \in \mathcal{C}.$$

This implies that

$$\begin{aligned} & (l^*(x); (g(x) + up(x))^*) \\ &= x^{(2\gamma-1)\alpha+\deg(l(x))+1} * (x^{\alpha-1-\deg(l(x))}l^*(x); 0) \\ & \quad + x^{(2\gamma-1)\alpha+\deg(l(x))+1} * (0; x^{\beta-1-\deg(g(x)+up(x))}(g(x) + up(x))^*) \\ &= x^{(2\gamma-1)\alpha+\deg(l(x))+1} * (l(x); g(x) + up(x))^r \in \mathcal{C}. \end{aligned}$$

Hence, there exist $\lambda_1(x), \lambda_2(x) \in R[x]$ such that

$$(l^*(x); (g(x) + up(x))^*) = \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g(x) + up(x)).$$

This means that

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l(x)]_{(x^\alpha-1)} = l^*(x) \text{ and} \quad (4.3.5)$$

$$[\lambda_2(x)(g(x) + up(x))]_{(x^\beta-1)} = g(x) + ux^i p^*(x), \quad (4.3.6)$$

where $i = \deg(g(x)) - \deg(p(x))$. By Lemma 4.3.3, we have $x^i p^*(x) = p(x)$ or $g(x) = x^i p^*(x) + p(x)$.

Firstly, assume that $x^i p^*(x) = p(x)$. From (4.3.6), we obtain that

$$\lambda_2(x)(g(x) + up(x)) \equiv g(x) + up(x) \pmod{x^\beta - 1}.$$

Then,

$$(\lambda_2(x) + 1)(g(x) + up(x)) \equiv 0 \pmod{x^\beta - 1}.$$

Hence, by Remark 4.3.2, $\lambda_2(x) = 1 + \frac{x^\beta-1}{g(x)+up(x)}h_1(x)$ for some $h_1(x) \in R[x]$. By (4.3.5), there is $q_1(x) \in R[x]$ such that

$$\lambda_1(x)(f_0(x) + uf_1(x)) + l(x) + \frac{x^\beta - 1}{g(x) + up(x)}h_1(x)l(x) = q_1(x)(x^\alpha - 1) + l^*(x).$$

By Lemma 3.3.2, we have $(f_0(x) + uf_1(x)) \mid \frac{x^\beta-1}{g(x)+up(x)}l(x)$ in $\frac{R[x]}{\langle x^\alpha-1 \rangle}$ and so

$$(f_0(x) + uf_1(x)) \mid \frac{x^\beta - 1}{g(x) + up(x)}h_1(x)l(x) \text{ in } \frac{R[x]}{\langle x^\alpha - 1 \rangle}.$$

Thus, there is $q_2(x) \in R[x]$ such that

$$\frac{x^\beta - 1}{g(x) + up(x)}h_1(x)l(x) \equiv q_2(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

Hence,

$$l(x) + l^*(x) \equiv (\lambda_1(x) + q_2(x))(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

This implies that $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha-1 \rangle}$.

Lastly, we will assume that $g(x) = x^i p^*(x) + p(x)$. From (4.3.6), we obtain that

$$[\lambda_2(x)(g(x) + up(x))]_{(x^\beta-1)} = (1 + u)(g(x) + up(x)).$$

Hence,

$$\lambda_2(x)(g(x) + up(x)) \equiv (1 + u)(g(x) + up(x)) \pmod{x^\beta - 1}.$$

This implies that $(\lambda_2(x) + 1 + u)(g(x) + up(x)) \equiv 0 \pmod{x^\beta - 1}$. Then, by Remark 4.3.2, we obtain that $\lambda_2(x) = (1 + u) + \frac{x^\beta - 1}{g(x) + up(x)} h_2(x)$ for some $h_2(x) \in R[x]$. From (4.3.5), there exists a polynomial $q_3(x) \in R[x]$ such that

$$\begin{aligned} & \lambda_1(x)(f_0(x) + uf_1(x)) + (1 + u)l(x) + \frac{x^\beta - 1}{g(x) + up(x)} h_2(x)l(x) \\ & \equiv l^*(x) \pmod{x^\alpha - 1}. \end{aligned}$$

By Lemma 3.3.2, we have $(f_0(x) + uf_1(x)) \mid l(x) \frac{x^\beta - 1}{g(x) + up(x)}$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$ and so

$$(f_0(x) + uf_1(x)) \mid \frac{x^\beta - 1}{g(x) + up(x)} h_2(x)l(x) \text{ in } \frac{R[x]}{\langle x^\alpha - 1 \rangle}.$$

Thus, there is $q_4(x) \in R[x]$ such that

$$\frac{x^\beta - 1}{g(x) + up(x)} h_2(x)l(x) \equiv q_4(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

Hence,

$$(1 + u)l(x) + l^*(x) \equiv (\lambda_1(x) + q_4(x))(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

Therefore, we obtain that $(f_0(x) + uf_1(x)) \mid (l^*(x) + (1 + u)l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. $\square$

By using Lemma 4.3.3 and Lemma 4.3.4, we can obtain the following Theorem.

Theorem 4.3.5. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), l(x)$ satisfy Theorem 3.3.1 (Type 1). Suppose that $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l(x))$ and $i = \deg(g(x)) - \deg(p(x))$.

Then, $\mathcal{C}$ is a reversible code if and only if

1. $f_0(x), f_1(x)$ and $g(x)$ are self-reciprocal and
2. (a) $x^i p^*(x) = p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Or
 (b) $g(x) = x^i p^*(x) + p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + (1 + u)l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. We obtain conditions 1 and 2 from Lemmas 4.3.3 and 4.3.4.

On the other hand, we suppose that conditions 1 and 2 are true. Consider,

$$(l^*(x); g^*(x) + ux^i p^*(x)) = (l^*(x); g(x) + ux^i p^*(x)), \quad (4.3.7)$$

where $i = \deg(g(x)) - \deg(p(x))$. If $x^i p^*(x) = p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, then there is $q_1(x) \in R[x]$ such that

$$l^*(x) + l(x) \equiv q_1(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

From (4.3.7), we obtain that

$$(l^*(x); g^*(x) + ux^i p^*(x)) = q_1(x) * (f_0(x) + uf_1(x); 0) + (l(x); g(x) + up(x)) \in \mathcal{C}.$$

Next, if $g(x) = x^i p^*(x) + p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + (1+u)l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $i = \deg(g(x)) - \deg(p(x))$, then there is $q_2(x) \in R[x]$ such that

$$l^*(x) + (1+u)l(x) \equiv q_2(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

From (4.3.7), we obtain that

$$\begin{aligned} & (l^*(x); g^*(x) + ux^i p^*(x)) \\ &= q_2(x) * (f_0(x) + uf_1(x); 0) + (1+u) * (l(x); g(x) + up(x)) \in \mathcal{C}. \end{aligned}$$

Therefore, $(l^*(x); g^*(x) + ux^i p^*(x)) \in \mathcal{C}$. Since $\gcd(f_0(x), \frac{x^\alpha - 1}{f_0(x)}) = 1$, there exist $\eta'_1(x), \eta'_2(x) \in \mathbb{F}_2[x]$ such that $\eta'_1(x)f_0(x) + \eta'_2(x)\frac{x^\alpha - 1}{f_0(x)} = 1$. Then, we obtain that

$$\begin{aligned} & \left[\left(1 + (1+x^j)u\eta'_1(x)f_1(x) + (1+x^j)\eta'_2(x)\frac{x^\alpha - 1}{f_0(x)} \right) (f_0(x) + uf_1(x)) \right]_{(x^\alpha - 1)} \\ &= f_0(x) + ux^j f_1(x), \text{ where } j = \deg(f_0(x)) - \deg(f_1(x)). \end{aligned}$$

Hence,

$$\begin{aligned} & ((f_0(x) + uf_1(x))^*; 0) \\ &= (f_0(x) + ux^j f_1(x); 0) \\ &= \left(1 + (1+x^j)u\eta'_1(x)f_1(x) + (1+x^j)\eta'_2(x)\frac{x^\alpha - 1}{f_0(x)} \right) * (f_0(x) + uf_1(x); 0) \in \mathcal{C}. \end{aligned}$$

This implies that $((f_0(x) + uf_1(x))^*; 0) \in \mathcal{C}$. Next, we will prove that $\mathcal{C}$ is a reversible code. Let $v(x) \in \mathcal{C}$. Then, there exist $\lambda_1(x), \lambda_2(x) \in R[x]$ such that

$$v(x) = \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l(x); g(x) + up(x)).$$

By Proposition 4.1.7, we get

$$v^r(x) = (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r + (\lambda_2(x)l(x); \lambda_2(x)(g(x) + up(x)))^r.$$

Suppose that $\lambda_1(x) = b_0 + b_1x + \dots + b_sx^s \in R[x]$ for some non-negative integer s . We consider

$$\begin{aligned} (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r &= \left(\sum_{i=0}^s b_i x^i (f_0(x) + uf_1(x)); 0 \right)^r \\ &= \sum_{i=0}^s b_i * (x^i (f_0(x) + uf_1(x)); 0)^r. \end{aligned}$$

By Proposition 4.1.8, there exists $m_i \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^i (f_0(x) + uf_1(x)); 0)^r = x^{(m_i+1)\alpha-1-\kappa} * ((f_0(x) + uf_1(x))^*; 0),$$

where $\kappa = \deg(x^i (f_0(x) + uf_1(x)))$ and $0 \leq i \leq s$. This implies that

$$(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r \in \mathcal{C}.$$

Suppose that $\lambda_2(x) = c_0 + c_1x + \dots + c_tx^t \in R[x]$ for some non-negative integer t . We consider

$$\begin{aligned} (\lambda_2(x)l(x); \lambda_2(x)(g(x) + up(x)))^r &= \left(\sum_{j=0}^t c_j x^j l(x); \sum_{j=0}^t c_j x^j (g(x) + up(x)) \right)^r \\ &= \sum_{j=0}^t c_j * (x^j l(x); x^j (g(x) + up(x)))^r. \end{aligned}$$

By Corollary 4.3.1, there exists $n_j \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^j l(x); x^j (g(x) + up(x)))^r = x^{((2n_j+1)\alpha-1-\deg(x^j l(x)))} * (l^*(x); (g(x) + up(x))^*),$$

where $0 \leq j \leq t$. Then, $(\lambda_2(x)l(x); \lambda_2(x)(g(x) + up(x)))^r \in \mathcal{C}$. This implies that $v^r(x) \in \mathcal{C}$. Therefore, $\mathcal{C}$ is a reversible code. $\square$

The following lemmas are tools for proving the main theorem for double cyclic code of length (α, β) over R type 2.

Lemma 4.3.6. *Let $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$ be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), a(x), l_1(x), l_2(x)$ satisfy Theorem 3.3.1 (Type 2).*

If $\mathcal{C}$ is a reversible code, then

1. $f_0(x), f_1(x), g(x)$ and $a(x)$ are self-reciprocal,
2. $a(x) \mid (x^i p^*(x) + p(x))$, where $i = \deg(g(x)) - \deg(p(x))$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. From Remark 4.2.2, we obtain that $\langle g(x) + up(x), ua(x) \rangle$ is a reversible cyclic code of length β over R . By Theorem 2.4.24, we obtain that

1. $g(x)$ and $a(x)$ are self-reciprocal,
2. $a(x) \mid (x^i p^*(x) + p(x))$.

Let $I = \langle (f_0(x) + uf_1(x); 0) \rangle \subseteq \mathcal{C}$. We claim that I is a reversible code. Since I is an $R[x]$ -submodule of $R_{\alpha, \beta}$, I is a double cyclic code of length (α, β) over R .

Assume that I is not a reversible code. Then, there exists a polynomial $v(x) \in I$ such that $v^r(x) \in \mathcal{C} - I$. Hence,

$$\begin{aligned} v(x) &= \lambda(x) * (f_0(x) + uf_1(x); 0) \text{ for some } \lambda(x) \in R[x] \text{ and} \\ v^r(x) &= (x^{\alpha-1-\deg(h(x))} h^*(x); 0), \text{ where } h(x) = [\lambda(x)(f_0(x) + uf_1(x))]_{(x^{\alpha-1})}. \end{aligned}$$

This implies that

$$\begin{aligned} v^r(x) &= (x^{\alpha-1-\deg(h(x))} h^*(x); 0) \\ &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l_1(x); g(x) + up(x)) \\ &\quad + \lambda_3(x) * (l_2(x); ua(x)) \end{aligned}$$

for some $\lambda_1(x), \lambda_2(x), \lambda_3(x) \in R[x]$ such that $\lambda_2(x) \neq 0$ and $\lambda_3(x) \neq 0$. Thus,

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l_1(x) + \lambda_3(x)l_2(x)]_{(x^{\alpha-1})} = x^{\alpha-1-\deg(h(x))} h^*(x) \quad (4.3.8)$$

$$[\lambda_2(x)(g(x) + up(x)) + \lambda_3(x)ua(x)]_{(x^\beta-1)} = 0. \quad (4.3.9)$$

By (4.3.9), $u\lambda_2(x)g(x) \equiv 0 \pmod{x^\beta - 1}$. Hence, by Remark 4.3.2, $\lambda_2(x) = uh_1(x) + \frac{x^\beta-1}{g(x)}h_2(x)$. By substituting $\lambda_2(x)$ in (4.3.9), we have

$$ug(x)h_1(x) + u\frac{x^\beta-1}{g(x)}p(x)h_2(x) + u\lambda_3(x)a(x) \equiv 0 \pmod{x^\beta - 1}.$$

Since $a(x) \mid g(x)$ and $a(x) \mid \frac{x^\beta-1}{g(x)}p(x)$, we obtain that

$$\left(\frac{g(x)}{a(x)}h_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)h_2(x) + \lambda_3(x)\right)ua(x) \equiv 0 \pmod{x^\beta - 1}.$$

Hence, by Remark 4.3.2, $\lambda_3(x) = \frac{g(x)}{a(x)}h_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)h_2(x) + \frac{x^\beta-1}{a(x)}h_3(x) + uh_4(x)$ for some $h_3(x), h_4(x)$ are in $\mathbb{F}_2[x]$. Consider,

$$\begin{aligned} \lambda_2(x)l_1(x) + \lambda_3(x)l_2(x) &= uh_1(x)l_1(x) + \frac{x^\beta-1}{g(x)}h_2(x)l_1(x) + \frac{g(x)}{a(x)}h_1(x)l_2(x) \\ &\quad + \frac{x^\beta-1}{g(x)a(x)}p(x)h_2(x)l_2(x) + \frac{x^\beta-1}{a(x)}h_3(x)l_2(x) \\ &\quad + uh_4(x)l_2(x) \\ &= \left(uh_1(x)l_1(x) + \frac{g(x)}{a(x)}h_1(x)l_2(x)\right) \\ &\quad + \left(\frac{x^\beta-1}{g(x)}h_2(x)l_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)h_2(x)l_2(x)\right) \\ &\quad + \frac{x^\beta-1}{a(x)}h_3(x)l_2(x) + uh_4(x)l_2(x). \end{aligned}$$

By Lemma 3.3.3, we have $(f_0(x) + uf_1(x)) \mid (\lambda_2(x)l_1(x) + \lambda_3(x)l_2(x))$ in $\frac{R[x]}{(x^\alpha-1)}$. Then, $\lambda_2(x)l_1(x) + \lambda_3(x)l_2(x) \equiv q_2(x)(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}$ for some $q_2(x) \in R[x]$. By (4.3.8), we obtain that

$$(\lambda_1(x) + q_2(x))(f_0(x) + uf_1(x)) \equiv x^{\alpha-1-\deg(h(x))}h^*(x) \pmod{x^\alpha - 1}.$$

This means that $(x^{\alpha-1-\deg(h(x))}h^*(x); 0) \in I$, which is a contradiction. Hence, I is a reversible code. By Theorem 2.4.24, $f_0(x)$ and $f_1(x)$ are self-reciprocal. $\square$

From the above theorem, we studied the necessary condition of $f_0(x), f_1(x), g(x), p(x)$ and $a(x)$ for a reversible code $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$. Next, we will study the necessary condition of $l_1(x)$ and $l_2(x)$ for $\mathcal{C}$, when $\beta = 2\gamma\alpha$ and γ is a non-negative integer.

Lemma 4.3.7. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), a(x), l_1(x), l_2(x)$ satisfy Theorem 3.3.1 (Type 2). Suppose that $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l_1(x))$ and $i = \deg(g(x)) - \deg(p(x))$.

If $\mathcal{C}$ is a reversible code, then $f_0(x) + uf_1(x)$ divides

$$l_1^*(x) + l_1(x) + \kappa(x)l_2(x)$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\kappa(x) \in \mathbb{F}_2[x]$ such that $a(x)\kappa(x) = x^i p^*(x) + p(x)$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. Since $(l_1(x); g(x) + up(x)) \in \mathcal{C}$,

$$(x^{\alpha-1-\deg(l_1(x))} l_1^*(x); x^{\beta-1-\deg(g(x)+up(x))} (g(x) + up(x))^*) = (l_1(x); g(x) + up(x))^r \in \mathcal{C}.$$

Thus,

$$(l_1^*(x); (g(x) + up(x))^*) = x^{(2\gamma-1)\alpha + \deg(l_1(x)) + 1} * (l_1(x); g(x) + up(x))^r \in \mathcal{C}.$$

Then, there exist $\lambda_1(x), \lambda_2(x), \lambda_3(x) \in R[x]$ such that

$$(l_1^*(x); (g(x) + up(x))^*) = \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l_1(x); g(x) + up(x)) + \lambda_3(x) * (l_2(x); ua(x)).$$

By Lemma 4.3.6, we get $g(x)$ is self-reciprocal and there exists $\kappa(x) \in \mathbb{F}_2[x]$ such that $a(x)\kappa(x) = x^i p^*(x) + p(x)$. Then,

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l_1(x) + \lambda_3(x)l_2(x)]_{(x^\alpha-1)} = l_1^*(x) \text{ and} \quad (4.3.10)$$

$$[\lambda_2(x)(g(x) + up(x)) + u\lambda_3(x)a(x)]_{(x^\beta-1)} = g(x) + up(x) + ua(x)\kappa(x). \quad (4.3.11)$$

From (4.3.11), we get $\lambda_2(x)ug(x) \equiv ug(x) \pmod{x^\beta - 1}$ and thus

$$(\lambda_2(x) + 1)ug(x) \equiv 0 \pmod{x^\beta - 1}.$$

Then, there exist polynomials $\omega_1(x), \omega_2(x) \in \mathbb{F}_2[x]$ such that $\lambda_2(x) = 1 + u\omega_1(x) + \frac{x^\beta - 1}{g(x)}\omega_2(x)$. By substituting $\lambda_2(x)$ in (4.3.11), we have

$$ug(x)\omega_1(x) + \frac{x^\beta - 1}{g(x)}p(x)\omega_2(x) + u\lambda_3(x)a(x) + ua(x)\kappa(x) \equiv 0 \pmod{x^\beta - 1}.$$

Since $a(x) \mid g(x)$ and $a(x) \mid \frac{x^\beta - 1}{g(x)}p(x)$, we obtain that

$$\left(\frac{g(x)}{a(x)}\omega_1(x) + \frac{x^\beta - 1}{g(x)a(x)}p(x)\omega_2(x) + \lambda_3(x) + \kappa(x) \right) ua(x) \equiv 0 \pmod{x^\beta - 1}.$$

Hence, $\lambda_3(x) = \frac{g(x)}{a(x)}\omega_1(x) + \frac{x^\beta - 1}{g(x)a(x)}p(x)\omega_2(x) + \kappa(x) + uh_1(x) + \frac{x^\beta - 1}{a(x)}h_2(x)$ for some $h_1(x), h_2(x) \in \mathbb{F}_2[x]$. By substituting $\lambda_2(x)$ and $\lambda_3(x)$ in (4.3.10), we have

$$\begin{aligned} q(x)(x^\alpha - 1) + l_1^*(x) &= \lambda_1(x)(f_0(x) + uf_1(x)) + \left(1 + u\omega_1(x) + \frac{x^\beta - 1}{g(x)}\omega_2(x) \right) l_1(x) \\ &\quad + \left(\frac{g(x)}{a(x)}\omega_1(x) + \frac{x^\beta - 1}{g(x)a(x)}p(x)\omega_2(x) + \kappa(x) \right) l_2(x) \\ &\quad + uh_1(x)l_2(x) + \frac{x^\beta - 1}{a(x)}h_2(x)l_2(x), \end{aligned}$$

where $q(x) \in R[x]$. By Lemma 3.3.3, we obtain that $f_0(x) + uf_1(x)$ divides

$$\begin{aligned} &uh_1(x)l_2(x), \frac{x^\beta - 1}{a(x)}h_2(x)l_2(x), \left(u\omega_1(x)l_1(x) + \frac{g(x)}{a(x)}\omega_1(x)l_2(x) \right) \text{ and} \\ &\left(\frac{x^\beta - 1}{g(x)}\omega_2(x)l_1(x) + \frac{x^\beta - 1}{g(x)a(x)}p(x)\omega_2(x)l_2(x) \right) \end{aligned}$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Hence, there is $h_3(x) \in R[x]$ such that

$$l_1^*(x) + l_1(x) + \kappa(x)l_2(x) \equiv (\lambda_1(x) + h_3(x))(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

This implies that $f_0(x) + uf_1(x)$ divides $l_1^*(x) + l_1(x) + \kappa(x)l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. $\square$

Lemma 4.3.8. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), a(x), l_1(x), l_2(x)$ satisfy Theorem 3.3.1 (Type 2). Suppose that $\deg(ua(x)) = (2\gamma - 1)\alpha + \deg(l_2(x))$.

If $\mathcal{C}$ is a reversible code, then $(f_0(x) + uf_1(x)) \mid (l_1^*(x) + l_2(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. Since $(l_2(x); ua(x)) \in \mathcal{C}$,

$$(x^{\alpha-1-\deg(l_2(x))}l_2^*(x); ux^{\beta-1-\deg(ua(x))}a^*(x)) = (l_2(x); ua(x))^r \in \mathcal{C}.$$

Thus,

$$\begin{aligned} & (l_2^*(x); ua^*(x)) \\ &= x^{(2\gamma-1)\alpha+\deg(l_2(x))+1} * (x^{\alpha-1-\deg(l_2(x))} l_2^*(x); ux^{\beta-1-\deg(ua(x))} a^*(x)) \in \mathcal{C}. \end{aligned}$$

Then, there exist $\lambda_1(x), \lambda_2(x), \lambda_3(x) \in R[x]$ such that

$$\begin{aligned} (l_2^*(x); ua^*(x)) &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l_1(x); g(x) + up(x)) \\ &\quad + \lambda_3(x) * (l_2(x); ua(x)). \end{aligned}$$

By Lemma 4.3.6, we get $a(x)$ is self-reciprocal. Then,

$$[\lambda_1(x)(f_0(x) + uf_1(x)) + \lambda_2(x)l_1(x) + \lambda_3(x)l_2(x)]_{(x^\alpha-1)} = l_2^*(x) \text{ and} \quad (4.3.12)$$

$$[\lambda_2(x)(g(x) + up(x)) + u\lambda_3(x)a(x)]_{(x^\beta-1)} = ua(x). \quad (4.3.13)$$

From (4.3.13), we get $u\lambda_2(x)g(x) \equiv 0 \pmod{x^\beta - 1}$. Hence, there exist $\eta_1(x), \eta_2(x) \in R[x]$ such that $\lambda_2(x) = u\eta_1(x) + \frac{x^\beta-1}{g(x)}\eta_2(x)$. By substituting $\lambda_2(x)$ in (4.3.13), we have

$$ug(x)\eta_1(x) + u\frac{x^\beta-1}{g(x)}p(x)\eta_2(x) + u\lambda_3(x)a(x) + ua(x) \equiv 0 \pmod{x^\beta - 1}.$$

Since $a(x) \mid g(x)$ and $a(x) \mid \frac{x^\beta-1}{g(x)}p(x)$, we obtain that

$$\left(\frac{g(x)}{a(x)}\eta_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)\eta_2(x) + \lambda_3(x) + 1 \right) ua(x) \equiv 0 \pmod{x^\beta - 1}.$$

Hence, $\lambda_3(x) = 1 + \frac{g(x)}{a(x)}\eta_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)\eta_2(x) + uh_1(x) + \frac{x^\beta-1}{a(x)}h_2(x)$ for some $h_1(x), h_2(x) \in \mathbb{F}_2[x]$. By substituting $\lambda_2(x)$ and $\lambda_3(x)$ in (4.3.12), we have

$$\begin{aligned} q(x)(x^\alpha - 1) + l_2^*(x) &= \lambda_1(x)(f_0(x) + uf_1(x)) + \left(u\eta_1(x) + \frac{x^\beta-1}{g(x)}\eta_2(x) \right) l_1(x) \\ &\quad + \left(1 + \frac{g(x)}{a(x)}\eta_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)\eta_2(x) \right) l_2(x) \\ &\quad + uh_1(x)l_2(x) + \frac{x^\beta-1}{a(x)}h_2(x)l_2(x), \text{ where } q(x) \in R[x]. \end{aligned}$$

By Lemma 3.3.3, we obtain that $f_0(x) + uf_1(x)$ divides

$$\begin{aligned} & uh_1(x)l_2(x), \frac{x^\beta-1}{a(x)}h_2(x)l_2(x), \left(u\eta_1(x)l_1(x) + \frac{g(x)}{a(x)}\eta_1(x)l_2(x) \right) \text{ and} \\ & \left(\frac{x^\beta-1}{g(x)}\eta_2(x)l_1(x) + \frac{x^\beta-1}{g(x)a(x)}p(x)\eta_2(x)l_2(x) \right) \end{aligned}$$

in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Hence, there is $h_3(x) \in R[x]$ such that

$$l_2^*(x) + l_2(x) \equiv (\lambda_1(x) + h_3(x))(f_0(x) + uf_1(x)) \pmod{x^\alpha - 1}.$$

This implies that $f_0(x) + uf_1(x)$ divides $l_2^*(x) + l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. $\square$

By Lemmas 4.3.6, 4.3.7 and 4.3.8, we obtain the following Theorem.

Theorem 4.3.9. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), a(x), l_1(x), l_2(x)$ satisfy Theorem 3.3.1 (Type 2). Suppose that $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l_1(x))$, $\deg(ua(x)) = (2\gamma - 1)\alpha + \deg(l_2(x))$ and $i = \deg(g(x)) - \deg(p(x))$.

Then, $\mathcal{C}$ is a reversible code if and only if

1. $f_0(x), f_1(x), g(x)$ and $a(x)$ are self-reciprocal,
2. $a(x) \mid (x^i p^*(x) + p(x))$,
3. $f_0(x) + uf_1(x)$ divides $l_1^*(x) + l_1(x) + \kappa(x)l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\kappa(x) \in \mathbb{F}_2[x]$ such that $a(x)\kappa(x) = x^i p^*(x) + p(x)$ and
4. $f_0(x) + uf_1(x)$ divides $l_2^*(x) + l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Proof. Suppose that $\mathcal{C}$ is a reversible code. By Lemmas 4.3.6, 4.3.7 and 4.3.8, we obtain the conditions 1 – 4.

On the other hand, suppose that conditions 1 – 4 are true. We will show that $((f_0(x) + uf_1(x))^*; 0), (l_1^*(x); (g(x) + up(x))^*)$ and $(l_2^*(x); ua^*(x))$ are in $\mathcal{C}$. Since $\gcd(f_0(x), \frac{x^\alpha - 1}{f_0(x)}) = 1$, there exist $\eta'_1(x), \eta'_2(x) \in \mathbb{F}_2[x]$ such that $\eta'_1(x)f_0(x) + \eta'_2(x)\frac{x^\alpha - 1}{f_0(x)} = 1$. Then, we obtain that

$$\begin{aligned} & \left[\left(1 + (1 + x^j)u\eta'_1(x)f_1(x) + (1 + x^j)\eta'_2(x)\frac{x^\alpha - 1}{f_0(x)} \right) (f_0(x) + uf_1(x)) \right]_{(x^\alpha - 1)} \\ &= f_0(x) + ux^j f_1(x), \text{ where } j = \deg(f_0(x)) - \deg(f_1(x)). \end{aligned}$$

Hence, $((f_0(x) + uf_1(x))^*; 0) \in \mathcal{C}$.

Next, we will show that $(l_1^*(x); (g(x) + up(x))^*) \in \mathcal{C}$. Let $i = \deg(g(x)) - \deg(p(x))$ and $a(x)\kappa(x) = x^i p^*(x) + p(x)$. By condition 3, there exist polynomials $\lambda_1(x)$ in $R[x]$ such that

$$l_1^*(x) \equiv \lambda_1(x)(f_0(x) + uf_1(x)) + l_1(x) + \kappa(x)l_2(x) \pmod{x^\alpha - 1}.$$

Hence,

$$\begin{aligned} & (l_1^*(x); g(x) + ux^i p^*(x)) \\ &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + (l_1(x); g(x) + up(x)) + \kappa(x) * (l_2(x); ua(x)) \in \mathcal{C}. \end{aligned}$$

Finally, we will show that $(l_2^*(x); ua^*(x)) \in \mathcal{C}$. By condition 4, there exists polynomial $\lambda_2(x)$ in $R[x]$ such that

$$l_2^*(x) \equiv \lambda_2(x)(f_0(x) + uf_1(x)) + l_2(x) \pmod{x^\alpha - 1}.$$

Hence,

$$(l_2^*(x); ua^*(x)) = \lambda_2(x) * (f_0(x) + uf_1(x); 0) + (l_2(x); ua(x)) \in \mathcal{C}.$$

Similar to the proof of Theory 4.3.5, we let $v(x) \in \mathcal{C}$. Then, there exist $\lambda_1(x)$, $\lambda_2(x)$, $\lambda_3(x) \in R[x]$ such that

$$\begin{aligned} v(x) &= \lambda_1(x) * (f_0(x) + uf_1(x); 0) + \lambda_2(x) * (l_1(x); g(x) + up(x)) \\ &\quad + \lambda_3(x) * (l_2(x); ua(x)). \end{aligned}$$

By Proposition 4.1.7, we get

$$\begin{aligned} v^r(x) &= (\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r + (\lambda_2(x)l_1(x); \lambda_2(x)(g(x) + up(x)))^r \\ &\quad + (\lambda_3(x)l_2(x); \lambda_3(x)ua(x))^r. \end{aligned}$$

Next, we will show that $(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r$, $(\lambda_2(x)l_1(x); \lambda_2(x)(g(x) + up(x)))^r$ and $(\lambda_3(x)l_2(x); \lambda_3(x)ua(x))^r$ are in $\mathcal{C}$.

First, suppose that $\lambda_1(x) = b_0 + b_1x + \dots + b_sx^s \in R[x]$ for some non-negative integer s . We consider

$$(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r = \left(\sum_{i=0}^s b_i x^i (f_0(x) + uf_1(x)); 0 \right)^r$$

$$= \sum_{i=0}^s b_i * (x^i(f_0(x) + uf_1(x)); 0)^r.$$

By Proposition 4.1.8, there exists $m_i \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^i(f_0(x) + uf_1(x)); 0)^r = x^{(m_i+1)\alpha-1-k} * ((f_0(x) + uf_1(x))^*; 0),$$

where $k = \deg(x^i(f_0(x) + uf_1(x)))$ and $0 \leq i \leq s$. This implies that

$$(\lambda_1(x)(f_0(x) + uf_1(x)); 0)^r \in \mathcal{C}.$$

Second, suppose that $\lambda_2(x) = c_0 + c_1x + \dots + c_tx^t \in R[x]$ for some non-negative integer t . We consider

$$\begin{aligned} (\lambda_2(x)l_1(x); \lambda_2(x)(g(x) + up(x)))^r &= \left(\sum_{i=0}^t c_i x^i l_1(x); \sum_{i=0}^t c_i x^i (g(x) + up(x)) \right)^r \\ &= \sum_{i=0}^t c_i * (x^i l_1(x); x^i (g(x) + up(x)))^r. \end{aligned}$$

By Corollary 4.3.1, there exists $n_i \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^i l_1(x); x^i (g(x) + up(x)))^r = x^{((2n_i\gamma+1)\alpha-1-\deg(x^i l_1(x)))} * (l_1^*(x); (g(x) + up(x))^*),$$

where $0 \leq i \leq t$. Then, $(\lambda_2(x)l_1(x); \lambda_2(x)(g(x) + up(x)))^r \in \mathcal{C}$.

Finally, suppose that $\lambda_3(x) = d_0 + d_1x + \dots + d_zx^z \in R[x]$ for some non-negative integer z . We consider

$$\begin{aligned} (\lambda_3(x)l_2(x); \lambda_3(x)ua(x))^r &= \left(\sum_{i=0}^z d_i x^i l_2(x); \sum_{i=0}^z d_i x^i ua(x) \right)^r \\ &= \sum_{i=0}^z d_i * (x^i l_2(x); x^i ua(x))^r. \end{aligned}$$

By Corollary 4.3.1, there exists $q_i \in \mathbb{Z}^+ \cup \{0\}$ such that

$$(x^i l_2(x); x^i ua(x))^r = x^{(2q_i\gamma+1)\alpha-1-\deg(x^i l_2(x))} * (l_2^*(x); ua^*(x)),$$

where $0 \leq i \leq z$. Then, $(\lambda_3(x)l_2(x); \lambda_3(x)ua(x))^r \in \mathcal{C}$. This implies that $v^r(x) \in \mathcal{C}$. Therefore, $\mathcal{C}$ is a reversible code. $\square$

The following examples are double cyclic codes of length (α, β) over the ring R , which are reversible codes derived from the theorems presented in this section.

Example 4.3.10. Let $\alpha = 3$ and $\beta = 6$. Consider,

$$x^3 - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and}$$

$$x^6 - 1 = (x + 1)^2(x^2 + x + 1)^2 = m_1(x)^2m_2(x)^2 \in \mathbb{F}_2[x].$$

Suppose $\mathcal{C} = \langle ((1 + u)m_1(x)m_2(x); 0), (1; m_1(x)m_2(x)) \rangle$. Let $l(x) = 1$. Then, $\deg(m_1(x)m_2(x)) = 3 + \deg(l(x))$. Since $p(x) = 0$, $x^i p^*(x) = p(x)$ and $l^*(x) + l(x) = 0$. Then, by Theorem 4.3.5, we obtain that $\mathcal{C}$ is a reversible code. In addition, double cyclic code generated from $\mathcal{C}$ is given in Table 21.

Example 4.3.11. Let $\alpha = 3$ and $\beta = 6$. Consider,

$$x^3 - 1 = (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and}$$

$$x^6 - 1 = (x + 1)^2(x^2 + x + 1)^2 = m_1(x)^2m_2(x)^2 \in \mathbb{F}_2[x].$$

Suppose

$$\mathcal{C} = \langle (m_1(x)m_2(x) + um_2(x); 0), (m_2(x); m_1(x)m_2(x)^2 + um_2(x)), (0; um_1(x)m_2(x)) \rangle.$$

Let $l_1(x) = m_2(x)$ and $l_2(x) = 0$. Then, $\deg(m_1(x)m_2(x)^2 + um_2(x)) = 3 + \deg(l_1(x))$ and $\deg(m_1(x)m_2(x)) = 3 + \deg(l_2(x))$. Consider,

$$x^i p^*(x) + p(x) = x^3 m_2(x) + m_2(x) = (x^3 + 1)m_2(x) = m_1(x)m_2(x)^2.$$

Hence, $a(x) \mid (x^i p^*(x) + p(x))$ and $k(x) = m_2(x)$. Since

$$l_1^*(x) + l_1(x) + \kappa(x)l_2(x) = 0 \text{ and } l_2^*(x) + l_2(x) = 0,$$

$f_0(x) + uf_1(x)$ divides $l_1^*(x) + l_1(x) + \kappa(x)l_2(x)$ and $l_2^*(x) + l_2(x)$ in $\frac{R[x]}{\langle x^3 - 1 \rangle}$. Then, by Theorem 4.3.9, we obtain that $\mathcal{C}$ is a reversible code. In addition, double cyclic code generated from $\mathcal{C}$ is given in Table 22.

4.3.2 Reversible-complement codes

By using the results in the section 4.3.1 and Theorems 4.1.11, we get the results in this section directly.

Theorem 4.3.12. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x) + uf_1(x), g(x), p(x), l(x)$ satisfy Theorem 3.3.1 (Type 1). Suppose that $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l(x))$ and $i = \deg(g(x)) - \deg(p(x))$.

Then, $\mathcal{C}$ is a reversible-complement code if and only if

1. $u\mathbb{I}(x) = (u + ux + \cdots + ux^{\alpha-1}; u + ux + \cdots + ux^{\beta-1}) \in \mathcal{C}$,
2. $f_0(x), f_1(x)$ and $g(x)$ are self-reciprocal and
3. (a) $x^i p^*(x) = p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$. Or
(b) $g(x) = x^i p^*(x) + p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + (1 + u)l(x))$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

Theorem 4.3.13. *Let γ be a non-negative integer and*

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$$

be a double cyclic code of length $(\alpha, \beta = 2\gamma\alpha)$ over R , where the polynomials $f_0(x), f_1(x), g(x), p(x), a(x), l_1(x), l_2(x)$ satisfy Theorem 3.3.1 (Type 2). Suppose that $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l_1(x))$, $\deg(ua(x)) = (2\gamma - 1)\alpha + \deg(l_2(x))$ and $i = \deg(g(x)) - \deg(p(x))$.

Then, $\mathcal{C}$ is a reversible-complement code if and only if

1. $u\mathbb{I}(x) = (u + ux + \cdots + ux^{\alpha-1}; u + ux + \cdots + ux^{\beta-1}) \in \mathcal{C}$,
2. $f_0(x), f_1(x), g(x)$ and $a(x)$ are self-reciprocal,
3. $a(x) \mid (x^i p^*(x) + p(x))$,

4. $f_0(x) + uf_1(x)$ divides $l_1^*(x) + l_1(x) + \kappa(x)l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$, where $\kappa(x) \in \mathbb{F}_2[x]$ such that $a(x)\kappa(x) = x^i p^*(x) + p(x)$ and
5. $f_0(x) + uf_1(x)$ divides $l_2^*(x) + l_2(x)$ in $\frac{R[x]}{\langle x^\alpha - 1 \rangle}$.

The following examples are double cyclic codes of length (α, β) over the ring R , which are reversible-complement codes derived from the theorems presented in this section.

Example 4.3.14. Let $\alpha = 3$ and $\beta = 6$. Consider,

$$\begin{aligned} x^3 - 1 &= (x + 1)(x^2 + x + 1) = m_1(x)m_2(x) \in \mathbb{F}_2[x] \text{ and} \\ x^6 - 1 &= (x + 1)^2(x^2 + x + 1)^2 = m_1^2(x)m_2^2(x) \in \mathbb{F}_2[x]. \end{aligned}$$

Suppose $\mathcal{C} = \langle ((1 + u)m_1(x); 0), (m_2(x) + u; m_1(x)m_2(x)^2) \rangle$. By Theorem, 4.3.5, we obtain that $\mathcal{C}$ is a reversible code. Consider,

$$u\mathbb{I}(x) = u * (m_2(x) + u; m_1(x)m_2(x)^2) \in \mathcal{C}.$$

By Theorem 4.3.12, we have $\mathcal{C}$ is a reversible-complement code. Moreover, $\mathcal{C}$ can be written as $\mathcal{C} = \langle ((1 + u)m_1(x); 0), (1 + u; m_1(x)m_2(x)^2) \rangle$. In addition, a DNA code $\mathcal{D}$ of length 9 with minimum Hamming distance 2 from $\mathcal{C} \cup \hat{\mathcal{C}}$ has 126 codewords, which are given in Table 23.

Example 4.3.15. From example 4.3.11, we obtain that

$$\mathcal{C} = \langle (m_1(x)m_2(x) + um_2(x); 0), (m_2(x); m_1(x)m_2(x)^2 + um_2(x)), (0; m_1(x)m_2(x)) \rangle$$

is a reversible code. Consider,

$$u\mathbb{I}(x) = x * (m_2(x); m_1(x)m_2(x)^2 + um_2(x)) \in \mathcal{C}.$$

By Theorem 4.3.13, we have $\mathcal{C}$ is a reversible-complement code. In addition, a DNA code $\mathcal{D}$ of length 9 with minimum Hamming distance 2 from $\mathcal{C} \cup \hat{\mathcal{C}}$ has 60 codewords, which are given in Table 24.

CHAPTER V

CONCLUSION

Throughout this chapter, we let α, β be positive integers, $R = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$ and $R_\alpha = \frac{R[x]}{\langle x^\alpha - 1 \rangle}$. In this thesis, we have studied the algebraic structure of double cyclic codes of length (α, β) over R . We have classified the study of the algebraic structure of double cyclic codes into 2 sections, depending on the types of lengths α and β as follows:

1. The case α and β are both odd integers.
2. The case α is an odd and β is an even integer.

The algebraic structure of double cyclic codes of length (α, β) over R are given in Table 7.

Table 7 The structure of double cyclic codes of length (α, β) over R

Both α and β are odd	$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$, where $f_0(x), f_1(x), g_0(x), g_1(x) \in \mathbb{F}_2[x]$ and $l(x) \in R[x]$ with $f_1(x) \mid f_0(x) \mid (x^\alpha - 1)$ and $g_1(x) \mid g_0(x) \mid (x^\beta - 1)$
α is an odd	Type 1
β is an even	$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle$, where $f_0(x), f_1(x), g(x), p(x) \in \mathbb{F}_2[x]$ and $l(x) \in R[x]$ with $f_1(x) \mid f_0(x) \mid (x^\alpha - 1), g(x) \mid (x^\beta - 1),$ $(g(x) + up(x)) \mid (x^\beta - 1), g(x) \mid p(x)(\frac{x^\beta - 1}{g(x)})$
	Type 2
	$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$, where $f_0(x), f_1(x), g(x), p(x), a(x) \in \mathbb{F}_2[x]$ and $l_1(x), l_2(x) \in R[x]$ with $f_1(x) \mid f_0(x) \mid (x^\alpha - 1),$ $a(x) \mid g(x) \mid (x^\beta - 1), a(x) \mid p(x)(\frac{x^\beta - 1}{g(x)})$

Furthermore, in Lemmas 3.2.2 - 3.2.3 and Lemmas 3.3.2 - 3.3.3, the prop-

erties of the polynomials $l(x)$, $l_1(x)$, and $l_2(x)$, derived from the structure of the double cyclic code $\mathcal{C}$ in Table 7, are examined and summarized in Table 8.

Table 8 The properties of polynomials $l(x)$, $l_1(x)$ and $l_2(x)$ derived from the structures of double cyclic code $\mathcal{C}$ in Table 7

Both α and β are odd	1. We can assume that $\deg(l(x)) < \deg(f_0(x) + uf_1(x))$ 2. $\frac{x^\beta-1}{g_1(x)}l(x)$ and $u\frac{x^\beta-1}{g_0(x)}l(x)$ are divisible by $f_0(x) + uf_1(x)$ in R_α
α is an odd β is an even	Type 1: 1. We can assume that $\deg(l(x)) < \deg(f_0(x) + uf_1(x))$ 2. $\frac{x^\beta-1}{g(x)+up(x)}l(x)$ and $u\frac{x^\beta-1}{g(x)}l(x)$ are divisible by $f_0(x) + uf_1(x)$ in R_α Type 2: 1. We can assume that $\deg(l_1(x)) < \deg(f_0(x) + uf_1(x))$ and $\deg(l_2(x)) < \deg(f_0(x) + uf_1(x))$ 2. $ul_2(x)$, $u\frac{x^\beta-1}{g(x)}l_1(x)$, $\frac{x^\beta-1}{a(x)}l_2(x)$, $ul_1(x) + \frac{g(x)}{a(x)}l_2(x)$ and $\frac{x^\beta-1}{g(x)}l_1(x) + p(x)\frac{x^\beta-1}{g(x)a(x)}l_2(x)$ are divisible by $f_0(x) + uf_1(x)$ in R_α

These above structures have been used to investigate conditions for double cyclic codes suitable for DNA codes. We have provided the notations for double cyclic codes, including reversible, complement, and reversible-complement, to study the conditions of the codes suitable for DNA codes. A double cyclic code $\mathcal{C}$ of length (α, β) over R which is suitable for DNA codes is called a double cyclic DNA code, that is, the code $\mathcal{C}$ is a double cyclic code and a reversible-complement code, such that $v^{rc} \neq v$ for all $v \in \mathcal{C}$. Since the length α of a double cyclic code $\mathcal{C}$ in this thesis always be odd, we obtain that $v \neq v^{rc}$ for all $v \in \mathcal{C}$. We have classified the study of the conditions for double cyclic codes suitable for DNA codes into 2 sections, depending on the types of lengths α and β as follows:

5.1 The case α and β are both odd positive integers

Let γ be a non-negative integer. In this case, we let

$$\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g_0(x) + ug_1(x)) \rangle$$

be a double cyclic code of length (α, β) over R , where the polynomials $f_0(x), f_1(x), l(x), g_0(x), g_1(x)$ satisfy Tables 7 and 8.

Suppose that $u\mathbb{I}(x) = (u + ux + \dots + ux^{\alpha-1}, u + ux + \dots + ux^{\beta-1})$, $i = \deg(g_0(x)) - \deg(g_1(x))$ and $\eta_1(x), \eta_2(x)$ are polynomials in $\mathbb{F}_2[x]$ such that

$$\eta_1(x)g_0(x) + \eta_2(x)\frac{x^\beta - 1}{g_0(x)} = 1.$$

The conditions for the code $\mathcal{C}$ to be a reversible-complement code are given in Table 9.

Table 9 The conditions for a double cyclic code $\mathcal{C}$ suit for DNA codes

Type of codes	Conditions
Non-separable code	1. $\beta = (2\gamma + 1)\alpha$ 2. $\deg(g_0(x) + ug_1(x)) = 2\gamma\alpha + \deg(l(x))$ 3. $f_0(x), f_1(x), g_0(x), g_1(x)$ are self-reciprocal 4. $l^*(x) + l(x) + (1 + x^i)u\eta_1(x)g_1(x)l(x) + (1 + x^i)\eta_2(x)\frac{x^\beta - 1}{g_0(x)}l(x)$ is divisible by $f_0(x) + uf_1(x)$ in R_α 5. $u\mathbb{I}(x) \in \mathcal{C}$

For a separable code $\mathcal{C}$, the conditions only apply to items 3 and 5.

5.2 The case α is an odd and β is an even positive integer

Let γ be a non-negative integer. In this case, we will classify double cyclic codes of length (α, β) over R into 2 types as follows:

$$\text{Type 1: } \mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l(x); g(x) + up(x)) \rangle,$$

Type 2: $\mathcal{C} = \langle (f_0(x) + uf_1(x); 0), (l_1(x); g(x) + up(x)), (l_2(x); ua(x)) \rangle$,

where polynomials $f_0(x), f_1(x), g(x), p(x), a(x), l(x), l_1(x), l_2(x)$ in Types 1 and 2 satisfy Table 7 and 8.

Suppose that $u\mathbb{L}(x) = (u + ux + \dots + ux^{\alpha-1}; u + ux + \dots + ux^{\beta-1})$ and $i = \deg(g(x)) - \deg(p(x))$. The conditions for a double cyclic code $\mathcal{C}$ types 1 and 2 to be a reversible-complement code are given in Tables 10 and 11, respectively.

Table 10 The conditions for a double cyclic code $\mathcal{C}$ type 1 suit for DNA codes

Type of codes	Conditions
Separable	1. $f_0(x), f_1(x)$ and $g(x)$ are self-reciprocal 2. $x^i p^*(x) = p(x)$ or $g(x) = x^i p^*(x) + p(x)$ 3. $u\mathbb{L}(x) \in \mathcal{C}$
Non-separable	1. $\beta = 2\gamma\alpha$ 2. $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l(x))$ 3. $f_0(x), f_1(x)$ and $g(x)$ are self-reciprocal 4. $x^i p^*(x) = p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + l(x))$ in R_α. Or $g(x) = x^i p^*(x) + p(x)$ and $(f_0(x) + uf_1(x)) \mid (l^*(x) + (1 + u)l(x))$ in R_α 5. $u\mathbb{L}(x) \in \mathcal{C}$

To generate DNA codes from our results, we let $\mathcal{C}$ be a code of length $n = \alpha + \beta$ over R and $S_{\mathcal{D}_4} = \{A, T, G, C\}$. We have defined a mapping Φ from $\mathcal{C}$ into $S_{\mathcal{D}_4}^{\alpha+\beta}$ as

$$\Phi(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) = \phi(a_0)\phi(a_1) \cdots \phi(a_{\alpha-1})\phi(b_0)\phi(b_1) \cdots \phi(b_{\beta-1}),$$

for all $(a_0, a_1, \dots, a_{\alpha-1}; b_0, b_1, \dots, b_{\beta-1}) \in \mathcal{C}$, where

$$\phi(0) = A, \phi(1) = G, \phi(u) = T \text{ and } \phi(1 + u) = C.$$

We have provided the process for generated a DNA codes as follows:

Table 11 The conditions for a double cyclic code $\mathcal{C}$ type 2 suit for DNA codes

Type of codes	Conditions
Separable	1. $f_0(x), f_1(x), g(x)$ and $a(x)$ are self-reciprocal 2. $a(x) \mid (x^i p^*(x) + p(x))$ 3. $u\mathbb{I}(x) \in \mathcal{C}$
Non-separable	1. $\beta = 2\gamma\alpha$ 2. $\deg(g(x) + up(x)) = (2\gamma - 1)\alpha + \deg(l_1(x))$ and $\deg(ua(x)) = (2\gamma - 1)\alpha + \deg(l_2(x))$ 3. $f_0(x), f_1(x), g(x)$ and $a(x)$ are self-reciprocal 4. $a(x) \mid (x^i p^*(x) + p(x))$ 5. $l_1^*(x) + l_1(x) + \kappa(x)l_2(x)$ is divisible by $f_0(x) + uf_1(x)$ in R_α, where $\kappa(x) \in \mathbb{F}_2[x]$ such that $a(x)\kappa(x) = x^i p^*(x) + p(x)$ 6. $l_2^*(x) + l_2(x)$ is divisible by $f_0(x) + uf_1(x)$ in R_α 7. $u\mathbb{I}(x) \in \mathcal{C}$

The process of generating a DNA code from a double cyclic DNA code

Step 1: Construct a double cyclic DNA code $\mathcal{C}$ of length (α, β) over R .

Step 2: Construct the code $\hat{\mathcal{C}} = \{(b; a) \in R^{\beta, \alpha} : (a; b) \in \mathcal{C}\}$ from the code $\mathcal{C}$.

Step 3: Generate a DNA code $\mathcal{D}$ from $\mathcal{C} \cup \hat{\mathcal{C}}$.

In future studies, it is interesting to investigate the algebraic structure and properties of double cyclic codes over different finite rings, similar to the previous study of cyclic codes. Additionally, constructing DNA codes from more complex structures, such as double cyclic codes over finite rings and non-separable cyclic codes over mixed alphabets, is appealing. Finally, in practical terms, it is interesting to produce DNA codes for use in DNA data storage or the real world.



APPENDIX

APPENDIX

Table 12 Codewords from double cyclic code $\mathcal{C}_1$ of length $(3, 5)$ in Example 3.2.8

$(0, u, u; 1, 1 + u, 1, 1 + u, 1 + u)$	$(0, u, u; 1, 1, 1, 1, 1)$	$(u, 0, u; 1, 1 + u, 1, 1 + u, 1)$
$(0, u, u; 1 + u, 1 + u, 1, 1 + u, 1 + u)$	$(0, u, u; 1 + u, 1, 1, 1, 1)$	$(u, 0, u; 1 + u, 1 + u, 1, 1 + u, 1)$
$(0, 0, 0; 1, 1 + u, 1 + u, 1 + u, 1)$	$(u, 0, u; 0, u, u, u, 0)$	$(0, 0, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u, 1)$
$(u, 0, u; u, u, u, u, 0)$	$(u, 0, u; 0, 0, 0, 0, u)$	$(u, u, 0; 1, 1 + u, 1, 1 + u, 1 + u)$
$(u, 0, u; u, 0, 0, 0, u)$	$(u, u, 0; 1 + u, 1 + u, 1, 1 + u, 1 + u)$	$(0, u, u; 0, u, 0, 0, 0)$
$(0, u, u; u, 0, 0, 0, u)$	$(0, u, u; u, u, 0, 0, 0)$	$(0, u, u; u, u, 0, 0, u)$
$(0, u, u; 1, 1, 1 + u, 1 + u, 1 + u)$	$(u, 0, u; 0, 0, 0, u, 0)$	$(u, 0, u; 0, 0, 0, 0, u)$
$(u, 0, u; u, 0, 0, 0, u)$	$(u, 0, u; u, 0, 0, u, u)$	$(u, u, 0; 1, 1, 1 + u, 1 + u, 1 + u)$
$(u, u, 0; 1 + u, 1, 1 + u, 1 + u, 1 + u)$	$(0, u, u; 0, u, 0, u, 0)$	$(0, u, u; 0, u, 0, u, u)$
$(0, u, u; u, u, 0, u, 0)$	$(0, u, u; 1, 1, 1, 1, 1 + u)$	$(u, 0, u; 1, 1, 1, 1, 1)$
$(0, u, u; 1 + u, 1, 1, 1, 1 + u)$	$(u, u, 0; 0, 0, u, 0, 0)$	$(u, 0, u; 1 + u, 1, 1, 1, 1)$
$(0, 0, 0; 1, 1 + u, 1 + u, 1 + u, 1 + u)$	$(u, u, 0; u, 0, u, 0, 0)$	$(0, 0, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(0, u, u; u, u, u, u, u)$	$(0, 0, 0; 1 + u, 1, 1 + u, 1, 1)$	$(u, u, 0; 0, u, 0, u, u)$
$(u, u, 0; u, u, 0, u, u)$	$(u, 0, u; 0, u, 0, 0, 0)$	$(0, 0, 0; u, u, u, u, 0)$
$(u, 0, u; 0, u, 0, 0, u)$	$(u, 0, u; u, u, 0, 0, 0)$	$(0, 0, 0; 1, 1 + u, 1, 1, 1 + u)$
$(u, u, 0; 1, 1 + u, 1 + u, 1 + u, 1)$	$(0, 0, 0; 1 + u, 1 + u, 1, 1, 1 + u)$	$(0, 0, 0; 0, 0, 0, 0, 0)$
$(u, u, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1)$	$(0, 0, 0; u, 0, 0, 0, 0)$	$(u, 0, u; u, u, u, 0, u)$
$(0, u, u; 1, 1 + u, 1, 1, 1)$	$(0, 0, 0; 0, 0, u, 0, u)$	$(0, u, u; 1 + u, 1 + u, 1, 1, 1)$
$(0, 0, 0; u, 0, u, 0, u)$	$(0, 0, 0; 1, 1, 1, 1 + u, 1)$	$(0, 0, 0; 1 + u, 1, 1, 1 + u, 1)$
$(u, u, 0; 1 + u, 1 + u, 1 + u, 1, 1)$	$(u, 0, u; 0, u, 0, u, 0)$	$(u, 0, u; u, u, 0, u, 0)$
$(u, 0, u; 1, 1, 1, 1, 1 + u)$	$(u, 0, u; 1 + u, 1, 1, 1, 1 + u)$	$(0, 0, 0; 1, 1, 1 + u, 1, 1 + u)$
$(u, 0, u; 0, u, u, u, u)$	$(0, 0, 0; 1 + u, 1, 1 + u, 1, 1 + u)$	$(u, 0, u; u, u, u, u, u)$
$(0, 0, 0; 0, 0, u, u, 0)$	$(0, 0, 0; 0, 0, u, u, u)$	$(0, 0, 0; 0, u, 0, u, 0)$
$(0, u, u; 1, 1, 1 + u, 1, 1)$	$(0, 0, 0; u, 0, u, u, u)$	$(0, u, u; 1 + u, 1, 1 + u, 1, 1)$
$(u, u, 0; 1, 1 + u, 1 + u, 1, 1 + u)$	$(u, 0, u; 1 + u, 1 + u, 1 + u, 1, 1 + u)$	$(u, u, 0; 1, 1 + u, 1 + u, 1 + u, 1 + u)$
$(u, u, 0; 1, 1, 1 + u, 1, 1)$	$(u, u, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(u, u, 0; 1 + u, 1, 1 + u, 1, 1)$
$(0, u, u; 1, 1 + u, 1, 1, 1 + u)$	$(0, u, u; 1 + u, 1, 1 + u, 1 + u, 1 + u)$	$(u, 0, u; 1, 1, 1 + u, 1 + u, 1)$
$(u, 0, u; 1 + u, 1, 1 + u, 1 + u, 1)$	$(0, 0, 0; 1, 1, 1, 1 + u, 1 + u)$	$(0, 0, 0; 1, 1 + u, 1 + u, 1, 1)$
$(0, 0, 0; 1 + u, 1 + u, 1 + u, 1, 1)$	$(0, 0, 0; 1 + u, 1, 1, 1 + u, 1 + u)$	$(0, u, u; 0, 0, u, 0, 0)$
$(0, u, u; 0, 0, u, 0, u)$	$(0, u, u; u, u, 0, 0, 0)$	$(u, u, u; 1 + u, 1 + u, 1, 1, 1 + u)$
$(0, 0, 0; 0, u, u, 0, 0)$	$(0, u, u; 1, 1, 1, 1 + u, 1)$	$(u, u, 0; 1 + u, 1 + u, 1, 1 + u, 1)$
$(u, u, 0; 0, 0, 0, 0, 0)$	$(0, u, u; 1 + u, 1, 1, 1 + u, 1)$	$(0, 0, 0; 0, u, u, 0, u)$
$(u, u, 0; u, 0, 0, 0, 0)$	$(0, 0, 0; u, u, u, 0, u)$	$(0, u, u; u, u, 0, u, u)$
$(u, 0, u; 1, 1 + u, 1, 1 + u, 1 + u)$	$(u, 0, u; 1 + u, 1 + u, 1, 1 + u, 1 + u)$	$(u, u, 0; 0, 0, u, 0, u)$
$(u, u, 0; u, 0, u, 0, u)$	$(u, u, 0; 1, 1, 1, 1 + u, 1)$	$(u, u, 0; 1 + u, 1, 1, 1 + u, 1)$
$(0, u, u; 1, 1 + u, 1 + u, 1 + u, 1)$	$(0, u, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(0, 0, 0; 1, 1 + u, 1, 1 + u, 1)$
$(0, 0, 0; 1 + u, 1 + u, 1, 1 + u, 1)$	$(0, u, u; 0, 0, u, u, 0)$	$(0, 0, 0; 0, u, u, u, 0)$
$(0, u, u; u, 0, u, u, 0)$	$(u, 0, u; u, u, 0, 0, u)$	$(0, 0, 0; u, u, u, u, 0)$
$(u, u, 0; 1, 1, 1 + u, 1, 1 + u)$	$(0, 0, 0; 0, 0, 0, 0, u)$	$(u, u, 0; 1 + u, 1, 1 + u, 1, 1 + u)$

$(u, 0, u; 0, u, 0, u, u)$	$(0, 0, 0; 1 + u, 1, 1 + u, 1 + u, 1)$	$(u, 0, u; u, u, 0, u, u)$
$(0, 0, 0; 0, 0, 0, u, 0)$	$(0, 0, 0; 0, 0, 0, u, u)$	$(0, 0, 0; u, 0, 0, u, 0)$
$(u, u, 0; 1, 1, 1, 1 + u, 1 + u)$	$(u, u, 0; 1, 1 + u, 1 + u, 1, 1)$	$(0, 0, 0; u, 0, 0, u, u)$
$(u, u, 0; 1 + u, 1 + u, 1 + u, 1, 1)$	$(u, u, 0; 1 + u, 1, 1, 1 + u, 1 + u)$	$(0, u, u; 1, 1 + u, 1 + u, 1 + u, 1 + u)$
$(u, u, 0; 0, u, u, 0, 0)$	$(0, u, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(u, u, 0; 0, u, u, 0, u)$
$(u, u, 0; u, u, u, 0, 0)$	$(u, 0, u; 1, 1 + u, 1 + u, 1 + u, 1)$	$(u, u, 0; u, u, u, 0, u)$
$(u, 0, u; 1 + u, 1 + u, 1 + u, 1 + u, 1)$	$(0, 0, 0; 1, 1, 1, 1, 1)$	$(0, 0, 0; 1 + u, 1, 1, 1, 1)$
$(u, 0, u; 1, 1 + u, 1, 1, 1)$	$(0, u, u; 1 + u, 1 + u, 1, 1 + u)$	$(0, u, u; 0, 0, 0, 0, 0)$
$(u, 0, u; 1 + u, 1 + u, 1, 1, 1)$	$(0, u, u; 0, 0, 0, 0, u)$	$(0, u, u; u, 0, 0, 0, 0)$
$(0, 0, 0; 0, u, 0, 0, 0)$	$(0, 0, 0; u, u, 0, 0, 0)$	$(u, u, 0; 1, 1 + u, 1, 1 + u, 1)$
$(0, 0, 0; u, u, 0, 0, u)$	$(0, 0, 0; 0, u, 0, 0, u)$	$(u, u, 0; 1 + u, 1 + u, 1, 1 + u, 1)$
$(u, u, 0; 0, u, u, 0, 0)$	$(0, u, u; u, 0, 0, 0, u)$	$(u, u, 0; u, u, u, u, 0)$
$(u, u, 0; 0, 0, 0, 0, u)$	$(u, u, 0; u, 0, 0, 0, u)$	$(0, u, u; 1, 1, 1 + u, 1, 1 + u)$
$(0, u, u; 0, 0, 0, 0, 0)$	$(u, 0, u; 1, 1, 1 + u, 1, 1)$	$(0, u, u; 1 + u, 1, 1 + u, 1, 1 + u)$
$(0, u, u; u, 0, 0, 0, 0)$	$(u, 0, u; 1, 1 + u, 1 + u, 1 + u, 1 + u)$	$(u, 0, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(u, 0, u; 1 + u, 1, 1 + u, 1, 1)$	$(0, 0, 0; 0, u, 0, u, 0)$	$(0, 0, 0; u, u, 0, u, 0)$
$(u, u, 0; 1, 1, 1 + u, 1 + u, 1)$	$(0, u, u; 0, 0, u, u, u)$	$(0, 0, 0; 1, 1, 1, 1, 1 + u)$
$(0, 0, 0; 1 + u, 1, 1, 1, 1 + u)$	$(0, u, u; u, 0, u, u, u)$	$(0, 0, 0; 0, u, u, u, u)$
$(0, 0, 0; u, u, u, u, u)$	$(u, u, 0; 0, 0, 0, u, 0)$	$(u, u, 0; 0, 0, 0, u, u)$
$(u, u, 0; u, 0, 0, u, 0)$	$(u, u, 0; u, 0, 0, u, u)$	$(u, 0, u; 1, 1 + u, 1, 1, 1 + u)$
$(u, 0, u; 1 + u, 1 + u, 1, 1, 1 + u)$	$(u, 0, u; 0, 0, 0, 0, 0)$	$(u, 0, u; u, 0, 0, 0, 0)$
$(u, u, 0; 1, 1, 1, 1, 1)$	$(u, u, 0; 1 + u, 1, 1, 1, 1)$	$(u, 0, u; 0, 0, u, 0, u)$
$(0, u, u; 1, 1, 1, 1 + u, 1 + u)$	$(0, u, u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$	$(u, 0, u; u, 0, u, 0, u)$
$(0, u, u; 1 + u, 1 + u, 1 + u, 1, 1)$	$(0, u, u; 1 + u, 1, 1, 1 + u, 1 + u)$	$(u, 0, u; 1, 1, 1, 1 + u, 1)$
$(0, 0, 0; 1 + u, 1 + u, 1, 1, 1)$	$(0, 0, 0; 1, 1 + u, 1, 1, 1)$	$(0, u, u; 0, u, u, 0, 0)$
$(0, u, u; u, u, u, 0, u)$	$(0, u, u; 0, u, u, 0, u)$	$(0, u, u; u, u, u, 0, 0)$
$(u, u, 0; u, u, u, 0, 0)$	$(u, u, 0; 0, u, 0, 0, u)$	$(u, u, 0; 0, u, 0, 0, u)$
$(u, 0, u; 1 + u, 1, 1 + u, 1, 1 + u)$	$(u, u, 0; u, u, 0, 0, u)$	$(u, 0, u; 1, 1, 1 + u, 1, 1 + u)$
$(u, 0, u; 0, 0, u, u, 0)$	$(0, 0, 0; 1, 1 + u, 1, 1 + u, 1 + u)$	$(0, 0, 0; 1 + u, 1 + u, 1, 1 + u, 1 + u)$
$(u, 0, u; u, 0, u, u, u)$	$(u, 0, u; 0, 0, u, u, u)$	$(u, 0, u; u, 0, u, u, 0)$
$(0, u, u; 0, u, u, u, 0)$	$(0, u, u; 1, 1 + u, 1, 1 + u, 1)$	$(0, u, u; 1 + u, 1 + u, 1, 1 + u, 1)$
$(0, u, u; u, u, u, u, 0)$	$(0, 0, 0; 1, 1, 1 + u, 1, 1)$	$(0, u, u; 0, u, u, u, u)$
$(u, u, 0; u, u, u, 0, 0)$	$(u, u, 0; 0, u, 0, u, 0)$	$(0, u, u; u, 0, 0, 0, u)$
$(u, u, 0; u, u, u, u, u)$	$(u, u, 0; 1, 1, 1, 1, 1 + u)$	$(u, u, 0; 0, u, 0, 0, u)$
$(0, u, u; 1 + u, 1 + u, 1 + u, 1, 1 + u)$	$(0, u, u; 1, 1 + u, 1 + u, 1, 1 + u)$	$(u, u, 0; 1, 1 + u, 1 + u, 1, 1)$
$(u, 0, u; 1 + u, 1 + u, 1 + u, 1, 1)$	$(u, 0, u; 1, 1, 1, 1 + u, 1 + u)$	$(0, 0, 0; 1, 1 + u, 1 + u, 1 + u)$
$(0, 0, 0; 1 + u, 1, 1 + u, 1 + u, 1 + u)$	$(u, 0, u; 0, u, u, 0, 0)$	$(u, 0, u; 0, u, u, 0, u)$
$(u, 0, u; u, u, u, 0, 0)$	$(u, u, 0; 1, 1 + u, 1 + u, 1, 1 + u)$	$(0, u, u; 1, 1, 1 + u, 1 + u, 1)$
$(u, u, 0; 1 + u, 1 + u, 1 + u, 1, 1 + u)$	$(0, 0, 0; 0, 0, u, 0, 0)$	$(0, u, u; 1 + u, 1, 1 + u, 1 + u, 1)$
$(0, 0, 0; u, 0, u, 0, 0)$	$(0, u, u; 0, 0, 0, u, u)$	$(0, 0, 0; 0, u, 0, u, u)$
$(0, u, u; u, 0, 0, u, u)$	$(0, 0, 0; u, u, 0, u, u)$	$(u, u, 0; 1, 1 + u, 1, 1)$
$(u, u, 0; 1 + u, 1, 1 + u, 1 + u, 1)$		

Table 13 Codewords from double cyclic code C_2 of length $(3, 5)$ in
Example 3.2.8

$(1, 1, 0; 0, 0, 0, 0, 0)$	$(1, u, 1 + u; u, u, u, u, u)$
$(0, u, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(1 + u, 1 + u, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(1 + u, 1, u; u, u, u, u, u)$	$(1, 1 + u, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(1, 1, 0; u, u, u, u, u)$	$(1 + u, u, 1; u, u, u, u, u)$
$(u, u, 0; 0, 0, 0, 0, 0)$	$(0, 1 + u, 1 + u; u, u, u, u, u)$
$(0, u, u; 0, 0, 0, 0, 0)$	$(u, u, 0; u, u, u, u, u)$
$(1 + u, 0, 1; 1, 1, 1, 1, 1)$	$(0, 0, u; 1, 1, 1, 1, 1)$
$(1, 1 + u, u; 0, 0, 0, 0, 0)$	$(0, 1 + u, 1 + u; 0, 0, 0, 0, 0)$
$(u, 1, 1; 1, 1, 1, 1, 1)$	$(1 + u, u, 1; 0, 0, 0, 0, 0)$
$(u, 0, 0; 1, 1, 1, 1, 1)$	$(1 + u, 1 + u, 0; 0, 0, 0, 0, 0)$
$(u, u, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(0, u, u; u, u, u, u, u)$
$(0, 1, 1 + u; 1, 1, 1, 1, 1)$	$(1, 1 + u, u; u, u, u, u, u)$
$(1 + u, 1 + u, 0; u, u, u, u, u)$	$(1, 0, 1 + u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(0, 1 + u, 1; 1, 1, 1, 1, 1)$	$(u, 1 + u, 1 + u; 1, 1, 1, 1, 1)$
$(1 + u, 0, 1 + u; 0, 0, 0, 0, 0)$	$(1 + u, 1, 0; 1, 1, 1, 1, 1)$
$(1, 1, u; 1, 1, 1, 1, 1)$	$(1, u, 1; 1, 1, 1, 1, 1)$
$(1 + u, 0, 1 + u; u, u, u, u, u)$	$(1 + u, u, 1 + u; 1, 1, 1, 1, 1)$
$(u, 1, 1; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(1 + u, 0, 1; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(0, 0, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(u, u, u; 1, 1, 1, 1, 1)$
$(0, u, 0; 1, 1, 1, 1, 1)$	$(1 + u, 1 + u, u; 1, 1, 1, 1, 1)$
$(u, 0, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(0, 1, 1 + u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(1, 1 + u, 0; 1, 1, 1, 1, 1)$	$(0, 1, 1; 0, 0, 0, 0, 0)$
$(1, 0, 1; 0, 0, 0, 0, 0)$	$(u, 1, 1 + u; 0, 0, 0, 0, 0)$
$(0, 1 + u, 1; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(0, 1, 1; u, u, u, u, u)$
$(1, 0, 1; u, u, u, u, u)$	$(u, 0, u; 0, 0, 0, 0, 0)$
$(0, 0, 0; 0, 0, 0, 0, 0)$	$(u, 1, 1 + u; u, u, u, u, u)$
$(u, 1 + u, 1; 0, 0, 0, 0, 0)$	$(u, 1 + u, 1 + u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(u, 1 + u, 1; u, u, u, u, u)$	$(1 + u, 1, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(u, 0, u; u, u, u, u, u)$	$(1, 1, u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(1, u, 1 + u; 0, 0, 0, 0, 0)$	$(1, u, 1; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(1 + u, u, 1 + u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$	$(0, 0, 0; u, u, u, u, u)$
$(1 + u, 1, u; 0, 0, 0, 0, 0)$	$(1, 0, 1 + u; 1, 1, 1, 1, 1)$

Table 14 Codewords from double cyclic code C_1 of length $(3, 3)$ in Example 3.2.9

$(0, 1 + u, 0; 1 + u, u, 1)$	$(u, u, 1; 1, 1 + u, u)$	$(1 + u, u, 1; 1 + u, 0, 1 + u)$
$(0, u, 0; u, 0, u)$	$(0, u, u; 0, u, u)$	$(u, 0, u; u, 0, u)$
$(1 + u, 1 + u, u; 1 + u, 1, u)$	$(1 + u, 1 + u, 1 + u; 0, 0, 0)$	$(0, u, 1; 1, 1, 0)$
$(1 + u, u, 0; 0, 1, 1)$	$(1, 0, 1; 1, u, 1 + u)$	$(0, 1, 0; 1, u, 1 + u)$
$(u, 1 + u, 1 + u; u, 1 + u, 1)$	$(u, 0, 1; 1 + u, 1 + u, 0)$	$(1 + u, 1, 1 + u; u, 0, u)$
$(u, 1, 1; u, 1, 1 + u)$	$(0, 0, u; u, u, 0)$	$(1 + u, 1, 0; 1 + u, 1 + u, 0)$
$(1 + u, 1 + u, 1; u, u, 0)$	$(1, 1 + u, 1; u, 0, u)$	$(1, 1 + u, u; 1 + u, 1 + u, 0)$
$(1 + u, u, 1 + u; 1, u, 1 + u)$	$(0, 1 + u, 1 + u; u, 1, 1 + u)$	$(1, u, 1 + u; 1, 0, 1)$
$(1, 1, 1 + u; u, u, 0)$	$(1, u, 0; 0, 1 + u, 1 + u)$	$(u, 0, 1 + u; 1, 1, 0)$
$(1 + u, 1, u; 1, 1, 0)$	$(1, u, 1; 1 + u, u, 1)$	$(1, 1, 1; 0, 0, 0)$
$(u, 1, 1 + u; 0, 1 + u, 1 + u)$	$(0, 1, u; 1 + u, 0, 1 + u)$	$(u, 1 + u, 1; 0, 1, 1)$
$(1 + u, 0, 0; u, 1, 1 + u)$	$(u, 1 + u, 0; 1 + u, 0, 1 + u)$	$(u, 1, u; 1 + u, u, 1)$
$(u, u, 0; u, u, 0)$	$(1 + u, u, u; u, 1 + u, 1)$	$(1, 1, 0; 1 + u, 1, u)$
$(1 + u, 1 + u, 0; 1, 1 + u, u)$	$(0, 0, 1; 1 + u, 1, u)$	$(0, 1, 1; u, 1 + u, 1)$
$(1 + u, 1, 1; 0, u, u)$	$(u, 1 + u, u; 1, u, 1 + u)$	$(1, 0, 0; u, 1 + u, 1)$
$(1 + u, 0, u; 0, 1 + u, 1 + u)$	$(1, 1, u; 1, 1 + u, u)$	$(0, 0, 1 + u; 1, 1 + u, u)$
$(0, 1 + u, 1; 0, 1 + u, 1 + u)$	$(1 + u, 0, 1 + u; 1 + u, u, 1)$	$(1, 1 + u, 1 + u; 0, u, u)$
$(u, u, u; 0, 0, 0)$	$(u, 0, 0; 0, u, u)$	$(0, 0, 0; 0, 0, 0)$
$(0, 1, 1 + u; 0, 1, 1)$	$(u, u, 1 + u; 1 + u, 1, u)$	$(1, 1 + u, 0; 1, 1, 0)$
$(0, 1 + u, u; 1, 0, 1)$	$(1, 0, 1 + u; 1 + u, 0, 1 + u)$	$(1, u, u; u, 1, 1 + u)$
$(0, u, 1 + u; 1 + u, 1 + u, 0)$	$(1 + u, 0, 1; 1, 0, 1)$	$(u, 1, 0; 1, 0, 1)$
$(1, 0, u; 0, 1, 1)$		

Table 15 Codewords from double cyclic code C_2 of length $(3, 3)$ in
Example 3.2.9

$(1 + u, 1 + u, 0; u, 1 + u, 1)$	$(1, 1, u; u, 1 + u, 1)$	$(0, 1, u; 1, 1, 0)$
$(0, u, 0; u, u, 0)$	$(0, 0, 1 + u; u, 1 + u, 1)$	$(0, 1, 1; 1 + u, u, 1)$
$(0, 1 + u, 1; 1, 0, 1)$	$(1 + u, u, 1 + u; 1, 1 + u, u)$	$(u, 1 + u, 0; 1, 1, 0)$
$(u, 0, u; u, u, 0)$	$(1, 0, 0; 1 + u, u, 1)$	$(1 + u, 1 + u, 1 + u; 0, 0, 0)$
$(1 + u, 1 + u, 1; 0, u, u)$	$(1 + u, 1 + u, u; u, 1, 1 + u)$	$(1, u, 1; 1 + u, 1, u)$
$(0, u, u; u, 0, u)$	$(0, 0, u; 0, u, u)$	$(0, 1, 1 + u; 1 + u, 0, 1 + u)$
$(u, 1, u; 1 + u, 1, u)$	$(0, u, 1; 0, 1 + u, 1 + u)$	$(1, 1, 1 + u; 0, u, u)$
$(u, 0, 1; 0, 1, 1)$	$(1, u, 1 + u; 1 + u, 1 + u, 0)$	$(1 + u, 1, 0; 0, 1, 1)$
$(1, 0, 1 + u; 1, 1, 0)$	$(1, 1 + u, u; 0, 1, 1)$	$(u, u, 1; u, 1 + u, 1)$
$(u, 1 + u, u; 1, 1 + u, u)$	$(1 + u, 1, 1 + u; u, u, 0)$	$(0, 1, 0; 1, 1 + u, u)$
$(1, 0, u; 1 + u, 0, 1 + u)$	$(u, 1, 1; 1, u, 1 + u)$	$(1, 1 + u, 1; u, u, 0)$
$(0, 1 + u, 1 + u; 1, u, 1 + u)$	$(1 + u, 0, 1 + u; 1 + u, 1, u)$	$(1 + u, u, 1; 1, 1, 0)$
$(u, 0, 1 + u; 0, 1 + u, 1 + u)$	$(u, u, 0; 0, u, u)$	$(1 + u, 1, u; 0, 1 + u, 1 + u)$
$(1, 1, 1; 0, 0, 0)$	$(u, 1 + u, 1 + u; 1 + u, u, 1)$	$(0, 1 + u, 0; 1 + u, 1, u)$
$(1 + u, u, 0; 1 + u, 0, 1 + u)$	$(0, 0, 1; u, 1, 1 + u)$	$(1 + u, 0, 0; 1, u, 1 + u)$
$(1 + u, u, u; 1 + u, u, 1)$	$(0, 1 + u, u; 1 + u, 1 + u, 0)$	$(1, 1, 0; u, 1, 1 + u)$
$(1, u, 0; 1, 0, 1)$	$(u, 1, 1 + u; 1, 0, 1)$	$(u, u, 1 + u; u, 1, 1 + u)$
$(1 + u, 0, 1; 1 + u, 1 + u, 0)$	$(u, 1, 0; 1 + u, 1 + u, 0)$	$(u, u, u; 0, 0, 0)$
$(0, 0, 0; 0, 0, 0)$	$(1 + u, 1, 1; u, 0, u)$	$(0, u, 1 + u; 0, 1, 1)$
$(1, 1 + u, 1 + u; u, 0, u)$	$(u, 0, 0; u, 0, u)$	$(1, 1 + u, 0; 0, 1 + u, 1 + u)$
$(1 + u, 0, u; 1, 0, 1)$	$(1, 0, 1; 1, 1 + u, u)$	$(1, u, u; 1, u, 1 + u)$
$(u, 1 + u, 1; 1 + u, 0, 1 + u)$		

Table 16 Codewords from double cyclic code $\mathcal{C}_1$ of length $(3, 6)$ in Example 3.3.4

$(0, 0, u; 1, 1 + u, u, 1 + u, 1 + u, 0)$	$(1 + u, 1 + u, 1; 1, 1 + u, u, 1 + u, 1 + u, 0)$
$(0, u, 0; 1 + u, u, 1 + u, 1 + u, 0, 1)$	$(1, 1, 1 + u; 1, 1 + u, u, 1 + u, 1 + u, 0)$
$(1 + u, 1 + u, 1 + u; 0, 0, 0, 0, 0, 0)$	$(u, 0, u; 1, u, 1, 1, 0, 1 + u)$
$(0, 0, u; 1 + u, 1, u, 1, 1, 0)$	$(0, u, 0; 1, 0, 1 + u, 1, u, 1)$
$(u, 0, 0; 0, 1 + u, 1, u, 1, 1)$	$(1 + u, 1 + u, 1; 1 + u, 1, u, 1, 1, 0)$
$(1, 1 + u, 1 + u; 0, 1, 1 + u, u, 1 + u, 1 + u)$	$(1 + u, 1, 1; 0, 1, 1 + u, u, 1 + u, 1 + u)$
$(1, 1, 1; u, 0, u, u, 0, u)$	$(1 + u, 1, 1 + u; 1, u, 1, 1, 0, 1 + u)$
$(1, 1, 1 + u; 1 + u, 1, u, 1, 1, 0)$	$(u, 0, u; 1 + u, u, 1 + u, 1 + u, 0, 1)$
$(0, u, u; 0, 1 + u, 1, u, 1, 1)$	$(1 + u, 1, 1 + u; 1 + u, u, 1 + u, 1 + u, 0, 1)$
$(u, u, 0; 1, 1, 0, 1 + u, 1, u)$	$(1, 1, 1; u, u, 0, u, u, 0)$
$(0, 0, 0; 0, 0, 0, 0, 0, 0)$	$(u, 0, u; 1 + u, 0, 1, 1 + u, u, 1 + u)$
$(u, 0, 0; u, 1, 1, 0, 1 + u, 1)$	$(1, 1 + u, 1; 1, u, 1, 1, 0, 1 + u)$
$(0, u, u; u, 1 + u, 1 + u, 0, 1, 1 + u)$	$(u, u, u; 0, 0, 0, 0, 0, 0)$
$(u, u, u; u, 0, u, u, 0, u)$	$(1 + u, 1 + u, 1 + u; 0, u, u, 0, u, u)$
$(1 + u, 1, 1 + u; 1 + u, 0, 1, 1 + u, u, 1 + u)$	$(1, 1 + u, 1 + u; 0, 1 + u, 1, u, 1, 1)$
$(1 + u, 1, 1; 0, 1 + u, 1, u, 1, 1)$	$(1, 1 + u, 1; 1 + u, u, 1 + u, 1 + u, 0, 1)$
$(u, u, 0; 1 + u, 1 + u, 0, 1, 1 + u, u)$	$(0, 0, 0; u, u, 0, u, u, 0)$
$(0, u, u; u, 1, 1, 0, 1 + u, 1)$	$(1 + u, 1 + u, 1 + u; u, 0, u, u, 0, u)$
$(1, 1, 1; 0, u, u, 0, u, u)$	$(u, u, u; u, u, 0, u, u, 0)$
$(1, 1 + u, 1; 1, 0, 1 + u, 1, u, 1)$	$(0, 0, u; 1, 1, 0, 1 + u, 1, u)$
$(1, 1 + u, 1 + u; u, 1 + u, 1 + u, 0, 1, 1 + u)$	$(1 + u, 1, 1; u, 1 + u, 1 + u, 0, 1, 1 + u)$
$(1 + u, 1 + u, 1; 1, 1, 0, 1 + u, 1, u)$	$(u, u, 0; 1, 1 + u, u, 1 + u, 1 + u, 0)$
$(0, u, 0; 1 + u, 0, 1, 1 + u, u, 1 + u)$	$(1, 1, 1; 0, 0, 0, 0, 0, 0)$
$(1, 1 + u, 1; 1 + u, 0, 1, 1 + u, u, 1 + u)$	$(1, 1, 1 + u; 1, 1, 0, 1 + u, 1, u)$
$(1 + u, 1 + u, 1 + u; u, u, 0, u, u, 0)$	$(1, 1 + u, 1 + u; u, 1, 1, 0, 1 + u, 1)$
$(1 + u, 1, 1; u, 1, 1, 0, 1 + u, 1)$	$(0, 0, 0; 0, u, u, 0, u, u)$
$(u, u, 0; 1 + u, 1, u, 1, 1, 0)$	$(u, 0, 0; 0, 1, 1 + u, u, 1 + u, 1 + u)$
$(u, u, u; 0, u, u, 0, u, u)$	$(u, 0, 0; u, 1 + u, 1 + u, 0, 1, 1 + u)$
$(u, 0, u; 1, 0, 1 + u, 1, u, 1)$	$(0, 0, u; 1 + u, 1 + u, 0, 1, 1 + u, u)$
$(0, 0, 0; u, 0, u, u, 0, u)$	$(1 + u, 1 + u, 1; 1 + u, 1 + u, 0, 1, 1 + u, u)$
$(1 + u, 1, 1 + u; 1, 0, 1 + u, 1, u, 1)$	$(1, 1, 1 + u; 1 + u, 1 + u, 0, 1, 1 + u, u)$
$(0, u, 0; 1, u, 1, 1, 0, 1 + u)$	$(0, u, u; 0, 1, 1 + u, u, 1 + u, 1 + u)$

Table 17 Codewords from double cyclic code $\mathcal{C}_2$ of length $(3,6)$ in
Example 3.3.4

$(u, 0, u; 0, u, 0, 0, u, 0)$	$(1, u, 1 + u; 0, 0, 0, 0, 0, 0)$
$(1, u, 1 + u; u, u, 0, u, u, 0)$	$(0, 0, u; 1 + u, 1, 1, 1 + u, 1 + u)$
$(1 + u, 0, 1; 1 + u, 1 + u, 1 + u, 1, 1)$	$(0, 1, 1; 0, 0, 0, 0, 0, 0)$
$(0, 1, 1; u, u, 0, u, u, 0)$	$(0, 0, 0; u, 0, u, u, 0, u)$
$(u, 1 + u, 1; u, 0, u, u, 0, u)$	$(1 + u, 0, 1; 1 + u, 1 + u, 1, 1, 1 + u)$
$(0, u, 0; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(1 + u, u, 1 + u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$
$(1, 1 + u, 0; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(0, 1 + u, 1; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(0, 0, 0; 0, 0, 0, 0, 0, 0)$	$(u, 0, 0; 1, 1 + u, 1 + u, 1 + u, 1 + u, 1, 1)$
$(u, 1 + u, 1; 0, 0, 0, 0, 0, 0)$	$(0, 0, 0; u, u, 0, u, u, 0)$
$(u, 1 + u, 1; u, u, 0, u, u, 0)$	$(1 + u, 1 + u, u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(0, u, 0; 1 + u, 1, 1, 1 + u, 1 + u)$	$(1, 0, 1; 0, 0, u, 0, 0, u)$
$(1, 1 + u, 0; 1 + u, 1 + u, 1, 1, 1 + u)$	$(u, 1, 1 + u; 0, u, u, 0, u, u)$
$(1 + u, 0, 1 + u; u, 0, u, 0, u, 0)$	$(u, 1, 1; 1, 1 + u, 1 + u, 1 + u, 1 + u, 1)$
$(u, u, 0; 0, u, u, 0, u, u)$	$(1, 1, 0; 0, u, u, 0, u, u)$
$(0, 1 + u, 1; 1, 1, 1 + u, 1 + u, 1 + u)$	$(u, 0, 0; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(0, 0, u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(1, 1, u; 1 + u, 1 + u, 1, 1, 1 + u)$
$(1, u, 1; 1 + u, 1 + u, 1, 1, 1 + u)$	$(u, 0, u; u, 0, u, 0, u, u)$
$(u, 1, 1; 1, 1, 1 + u, 1 + u, 1 + u)$	$(1 + u, 0, 1; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(0, 0, u; 1 + u, 1 + u, 1, 1, 1 + u)$	$(1, 1 + u, u; 0, u, u, 0, u, u)$
$(u, 0, u; 0, 0, 0, 0, 0, 0)$	$(u, 0, u; u, u, 0, u, u, 0)$
$(1, u, 1 + u; u, 0, 0, u, 0, 0)$	$(1 + u, 1 + u, 0; 0, u, u, 0, u, u)$
$(1 + u, 1, 0; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(0, 1, 1; u, 0, 0, u, 0, 0)$
$(0, 1, 1 + u; 1 + u, 1, 1, 1 + u, 1 + u)$	$(1 + u, 0, 1; 1, 1, 1 + u, 1 + u, 1 + u)$
$(0, u, 0; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(1 + u, u, 1 + u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(1 + u, 1, 0; 1 + u, 1, 1, 1 + u, 1 + u)$	$(0, 0, 0; u, 0, 0, u, 0, 0)$
$(0, u, 0; 1 + u, 1 + u, 1, 1, 1 + u)$	$(u, 1 + u, 1 + u; 1 + u, 1, 1, 1 + u, 1 + u)$
$(1, 1 + u, 0; 1, 1, 1 + u, 1 + u, 1 + u)$	$(u, 1, 1; 1 + u, 1 + u, 1 + u, 1, 1)$
$(u, 1 + u, 1; u, 0, 0, u, 0, 0)$	$(0, 0, u; 1, 1 + u, 1 + u, 1 + u, 1)$
$(1, 1 + u, 0; 1 + u, 1 + u, 1 + u, 1 + u, 1)$	$(u, 1, 1 + u; 0, 0, u, 0, 0, u)$
$(0, 1 + u, 1; 1, 1 + u, 1, 1 + u, 1 + u)$	$(u, 0, 0; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(1, 0, 1; u, 0, u, u, 0, u)$	$(0, 1 + u, 1 + u; 0, u, u, 0, u, u)$
$(u, 1, 1 + u; u, u, u, u, u, u)$	$(1, 1, 0; 0, 0, u, 0, 0, u)$
$(u, u, 0; 0, 0, u, 0, 0, u)$	$(1, 1, 0; u, u, u, u, u, u)$
$(u, u, 0; u, u, u, u, u, u)$	$(1, u, 1; 1 + u, 1, 1 + u, 1, 1 + u, 1)$
$(1, 1, u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(0, 0, u; 1, 1, 1 + u, 1 + u, 1 + u)$
$(1, 0, 1 + u; 1 + u, 1 + u, 1, 1, 1 + u)$	$(1, 0, 1; 0, 0, 0, 0, 0, 0)$
$(0, 1, 1 + u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(u, 1, 1 + u; 0, u, 0, 0, u, 0)$
$(1 + u, 0, 1; 1 + u, 1 + u, 1 + u, 1, 1)$	$(1, 1, 0; 0, 0, u, 0, 0, 0)$
$(0, u, u; 0, u, u, 0, u, u)$	$(1, u, 1; 1 + u, 1, 1 + u, 1, 1 + u)$
$(u, u, 0; 0, u, 0, u, 0, u)$	$(0, 1, 1 + u; 1 + u, 1 + u, 1, 1, 1 + u)$
$(1, 1, u; 1 + u, 1, 1, 1 + u, 1 + u)$	$(1 + u, 1, u; 0, u, 0, 0, u, u)$
$(1 + u, 1, 0; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(u, 0, u; u, 0, u, 0, u, u)$
$(1, 1 + u, u; 0, 0, u, 0, 0, u)$	$(1 + u, 0, 1; 1 + u, 1, 1 + u, 1, 1 + u)$
$(1, 1 + u, u; u, u, u, u, u, u)$	$(1 + u, 1 + u, 0; 0, 0, u, 0, 0, u)$
$(1 + u, u, 1; 0, u, u, 0, u, u)$	$(1 + u, u, 1 + u; 1 + u, 1 + u, 1 + u, 1, 1)$
$(0, u, 0; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1 + u, 0, 1 + u; 0, u, 0, 0, u, 0)$
$(1, 1 + u, 0; 1, 1 + u, 1 + u, 1 + u, 1, 1)$	$(1 + u, 1, 0; 1 + u, 1, 1, 1 + u, 1 + u)$
$(u, 1 + u, 1 + u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(u, u, u; 1 + u, 1 + u, 1 + u, 1, 1 + u, 1)$
$(1, 1 + u, u; 0, u, 0, u, 0, u)$	$(1 + u, 1 + u, 0; 0, u, 0, 0, u, 0)$
$(0, u, 0; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1, 1 + u, 0; 1, 1 + u, 1, 1 + u, 1 + u)$
$(1 + u, u, 1 + u; 1, 1 + u, 1, 1 + u, 1 + u)$	$(0, 0, u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(u, 1 + u, 1 + u; 1 + u, 1 + u, 1, 1, 1 + u)$	$(1, u, 1; 1 + u, 1, 1 + u, 1, 1 + u)$
$(1, 1, u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$	$(1 + u, 1 + u, u; 1 + u, 1 + u, 1, 1, 1 + u)$
$(u, u, u; 1 + u, 1, 1, 1 + u, 1 + u)$	$(1, u, 1; 1 + u, 1 + u, 1 + u, 1, 1, 1)$
$(1, 1, u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(u, 1, 1 + u; u, 0, u, u, 0, u)$
$(1, 0, 1 + u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(u, u, 0; u, 0, u, u, 0, u)$
$(0, 1 + u, 1 + u; 0, 0, u, 0, 0, u)$	$(1, 1, 0; u, 0, u, u, 0, u)$
$(0, 1 + u, 1 + u; u, u, u, u, u, u)$	$(1 + u, 1, 0; 1, 1 + u, 1 + u, 1 + u, 1)$
$(0, 0, u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$	$(0, u, u; 0, 0, u, 0, 0, u)$
$(1, 0, 1; u, 0, 0, 0, 0, 0)$	$(u, 1, 1 + u; u, u, 0, u, u, 0)$
$(u, 1, 1 + u; 0, 0, 0, 0, 0, 0)$	$(u, u, 0; u, 0, u, u, 0, u)$
$(0, u, u; u, u, u, u, u, u)$	$(1, 1, 0; u, 0, u, u, 0, u)$
$(1, 0, 1 + u; 1 + u, 1, 1, 1 + u, 1 + u)$	$(u, u, 0; 0, 0, 0, 0, 0, 0)$
$(0, 0, 1; u, 0, 0, 0, 0, 0)$	

$(0, 1 + u, 1 + u; 0, u, 0, 0, u, 0)$	$(u, u, 0; u, u, 0, u, u, 0)$
$(1, 1, 0; 0, 0, 0, 0, 0, 0)$	$(1, 1, 0; u, u, 0, u, u, 0)$
$(0, 1, 1 + u; 1 + u, 1, 1 + u, 1 + u, 1)$	$(0, u, 0; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(1 + u, 0, 1 + u; 0, u, u, 0, u, u)$	$(1 + u, 1, u; 0, 0, u, 0, 0, u)$
$(1 + u, u, 1; 0, 0, u, 0, 0, u)$	$(1 + u, 1, u; u, u, u, u, u, u)$
$(1 + u, u, 1; u, u, u, u, u, u)$	$(1 + u, 1, 0; 1, 1, 1, 1 + u, 1 + u, 1 + u)$
$(0, u, u; 0, u, 0, 0, u, 0)$	$(1 + u, 1 + u, 0; u, 0, u, u, 0, u)$
$(1, 0, 1; 0, u, u, 0, u, u)$	$(u, u, u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$
$(0, u, 0; 1, 1 + u, 1, 1 + u, 1, 1 + u)$	$(1, 1 + u, u; 0, 0, 0, 0, 0, 0)$
$(1 + u, 1, u; 0, u, 0, 0, u, 0)$	$(1 + u, u, 1; 0, u, 0, 0, u, 0)$
$(u, 1 + u, 1 + u; 1, 1, 1, 1 + u, 1 + u, 1 + u)$	$(1, 1 + u, u; u, u, 0, u, u, 0)$
$(1, 1 + u, 0; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1 + u, 1 + u, 0; 0, 0, 0, 0, 0, 0)$
$(1 + u, 1 + u, 0; u, u, 0, u, u, 0)$	$(u, 1 + u, 1 + u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$
$(1, u, 1 + u; 0, u, u, 0, u, u)$	$(u, u, u; 1 + u, 1 + u, 1, 1, 1, 1 + u)$
$(1, 1, u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1, u, 1; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(1, 0, 1 + u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$	$(0, 1, 1; 0, u, u, 0, u, u)$
$(u, 0, 0; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(1 + u, 1 + u, u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$
$(u, 1, 1; 1 + u, 1 + u, 1, 1, 1, 1 + u)$	$(0, 1, 1 + u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(1, u, 1; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1, 1, u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(0, 1 + u, 1 + u; u, 0, u, u, 0, u)$	$(u, 0, 0; 1 + u, 1, 1, 1 + u, 1 + u, 1)$
$(1 + u, 1, 0; 1, 1 + u, 1 + u, 1 + u, 1, 1)$	$(1 + u, 1 + u, u; 1 + u, 1, 1, 1 + u, 1 + u)$
$(0, 0, 0; 0, u, u, 0, u, u)$	$(0, 1, 1 + u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(0, u, u; u, 0, u, u, 0, u)$	$(u, 1 + u, 1; 0, u, u, 0, u, u)$
$(0, 1 + u, 1 + u; 0, 0, 0, 0, 0, 0)$	$(u, 1, 1 + u; u, 0, 0, u, 0, 0)$
$(u, u, 0; u, 0, 0, u, 0, 0)$	$(u, 1 + u, 1 + u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(1, 1, 0; u, 0, 0, u, 0, 0)$	$(0, 1 + u, 1 + u; u, u, 0, u, u, 0)$
$(1 + u, 0, 1 + u; 0, 0, u, 0, 0, u)$	$(1 + u, 1, 0; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(u, u, u; 1, 1 + u, 1 + u, 1 + u, 1 + u, 1)$	$(1 + u, 0, 1 + u; u, u, u, u, u, u)$
$(1 + u, u, 1; u, 0, u, u, 0, u)$	$(1 + u, 1, u; u, 0, u, u, 0, u)$
$(0, u, u; u, 0, u, u, 0, u)$	$(0, u, u; 0, 0, 0, 0, 0, 0)$
$(1, 0, 1; u, u, u, u, u, u)$	$(1 + u, u, 1 + u; 1 + u, 1 + u, 1, 1, 1 + u)$
$(u, u, u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(u, 1 + u, 1 + u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(1 + u, u, 1; 0, 0, 0, 0, 0, 0)$	$(1 + u, 1, u; 0, 0, 0, 0, 0, 0)$
$(1 + u, 1, u; u, u, 0, u, u, 0)$	$(1 + u, 1 + u, u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(1 + u, u, 1; u, u, 0, u, u, 0)$	$(0, 1 + u, 1; 1 + u, 1, 1 + u, 1, 1 + u, 1)$
$(1, 1, u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$	$(1, u, 1; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(u, 0, 0; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(1 + u, 1 + u, 0; u, 0, 0, u, 0, 0)$
$(1, 0, 1; 0, u, 0, 0, u, 0)$	$(u, 0, u; 0, u, u, 0, u, u)$
$(1 + u, 1 + u, u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(1, 0, 1 + u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(1, u, 1 + u; 0, 0, u, 0, 0, u)$	$(1, u, 1 + u; u, u, u, u, u, u)$
$(0, 1, 1; 0, 0, u, 0, 0, u)$	$(0, 1, 1; u, u, u, u, u, u)$
$(u, 1, 1; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(0, 1 + u, 1; 1 + u, 1, 1, 1, 1 + u, 1 + u)$
$(u, 0, 0; 1 + u, 1 + u, 1, 1, 1, 1 + u)$	$(1, 0, 1 + u; 1, 1, 1, 1 + u, 1 + u, 1 + u)$
$(1, u, 1 + u; 0, u, 0, 0, u, 0)$	$(0, 1, 1; 0, u, 0, 0, u, 0)$
$(0, 1, 1 + u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(u, 1, 1; 1 + u, 1, 1, 1 + u, 1 + u)$
$(1 + u, 0, 1; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(0, 0, 0; 0, 0, u, 0, 0, u)$
$(u, 1 + u, 1; 0, 0, u, 0, 0, u)$	$(0, 0, 0; u, u, u, u, u, u)$
$(u, 1 + u, 1; u, u, u, u, u, u)$	$(u, u, u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(0, 1 + u, 1 + u; u, 0, 0, u, 0, 0)$	$(1 + u, 0, 1 + u; u, 0, u, u, 0, u)$
$(1 + u, 0, 1; 1 + u, 1, 1, 1 + u, 1 + u)$	$(0, 0, 0; 0, u, 0, 0, u, 0)$
$(1 + u, u, 1 + u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(u, 1 + u, 1; 0, u, 0, 0, u, 0)$
$(u, 1 + u, 1 + u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1, 1 + u, u; u, 0, u, u, 0, u)$
$(0, u, u; u, 0, 0, u, 0, 0)$	$(u, u, u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(0, 1 + u, 1; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(1 + u, 0, 1 + u; 0, 0, 0, 0, 0, 0)$
$(1 + u, 1 + u, u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(1 + u, 0, 1 + u; u, u, 0, u, u, 0)$
$(1, 0, 1 + u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$	$(1 + u, 1, u; u, 0, 0, u, 0, 0)$
$(1 + u, u, 1; u, 0, 0, u, 0, 0)$	$(1 + u, u, 1 + u; 1 + u, 1, 1, 1 + u, 1 + u)$
$(1, 1 + u, 0; 1 + u, 1, 1, 1 + u, 1 + u)$	$(u, 1, 1; 1, 1 + u, 1, 1 + u, 1, 1)$
$(u, 0, u; 0, 0, u, 0, 0, u)$	$(1, 0, 1; u, u, 0, u, u, 0)$
$(u, 0, u; u, u, u, u, u, u)$	$(u, 1, 1; 1 + u, 1 + u, 1 + u, 1, 1, 1)$
$(1, u, 1 + u; u, 0, u, u, 0, u)$	$(u, 0, 0; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(0, 1 + u, 1; 1 + u, 1 + u, 1, 1, 1 + u)$	$(0, 0, u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$
$(1 + u, 1 + u, u; 1, 1, 1 + u, 1 + u, 1 + u)$	$(0, 1, 1; u, 0, u, 0, u, 0)$

Table 18 Codewords from double cyclic code $\mathcal{C}$ of length $(3, 3)$ in
Example 4.2.7

$(1 + u, 0, 1; 0, 0, 0)$	$(1 + u, 0, 1; u, u, u)$	$(u, 1, 0; 1, 1, 1)$
$(1, 0, 1; 0, 0, 0)$	$(1 + u, 1, 1 + u; 1, 1, 1)$	$(1 + u, u, 1; u, u, u)$
$(1, 1 + u, u; u, u, u)$	$(1, 0, u; 1, 1, 1)$	$(0, 1, 0; 1, 1, 1)$
$(1, u, 1; 0, 0, 0)$	$(1, 1 + u, 1; 1, 1, 1)$	$(1 + u, 1, 0; u, u, u)$
$(1 + u, 1, u; 0, 0, 0)$	$(0, u, 1; 1 + u, 1 + u, 1 + u)$	$(u, u, 1 + u; 1, 1, 1)$
$(0, 1, u; 1 + u, 1 + u, 1 + u)$	$(u, 1, u; 1 + u, 1 + u, 1 + u)$	$(u, 0, 1 + u; 1 + u, 1 + u, 1 + u)$
$(0, u, 1 + u; 1, 1, 1)$	$(1 + u, 0, 0; 1 + u, 1 + u, 1 + u)$	$(0, 1 + u, 1; u, u, u)$
$(1, 1, 1 + u; 1 + u, 1 + u, 1 + u)$	$(0, 0, u; 0, 0, 0)$	$(u, 0, 0; u, u, u)$
$(1 + u, 0, 1 + u; 0, 0, 0)$	$(0, 0, 0; 0, 0, 0)$	$(u, u, 0; u, u, u)$
$(u, 1, 1; 0, 0, 0)$	$(u, u, u; 0, 0, 0)$	$(1, 0, 1 + u; 0, 0, 0)$
$(1 + u, 1 + u, 1 + u; 1, 1, 1)$	$(u, 1 + u, u; 1, 1, 1)$	$(1 + u, u, u; 1 + u, 1 + u, 1 + u)$
$(1 + u, 1, 1; 1 + u, 1 + u, 1 + u)$	$(0, u, 0; 0, 0, 0)$	$(0, 1 + u, 0; 1, 1, 1)$
$(0, u, 0; u, u, u)$	$(1 + u, u, 0; 1 + u, 1 + u, 1 + u)$	$(1, 1 + u, 1 + u; 1, 1, 1)$
$(1 + u, 1 + u, u; 0, 0, 0)$	$(1, u, 1 + u; u, u, u)$	$(1 + u, 1 + u, u; u, u, u)$
$(1, u, 0; 1 + u, 1 + u, 1 + u)$	$(1 + u, 0, u; 1, 1, 1)$	$(1 + u, u, 1; 0, 0, 0)$
$(1 + u, 1 + u, 1; 1, 1, 1)$	$(1, 1 + u, u; 0, 0, 0)$	$(1 + u, 1 + u, 0; u, u, u)$
$(u, u, 1; 1 + u, 1 + u, 1 + u)$	$(u, 1, 1 + u; 0, 0, 0)$	$(1, 1 + u, 0; 0, 0, 0)$
$(0, 1 + u, 1 + u; u, u, u)$	$(0, 1 + u, u; 1 + u, 1 + u, 1 + u)$	$(1 + u, 1, 0; 0, 0, 0)$
$(u, 1, 1 + u; u, u, u)$	$(1, 1 + u, 0; u, u, u)$	$(u, 1, 0; 1 + u, 1 + u, 1 + u)$
$(u, 1 + u, 1; u, u, u)$	$(1 + u, 1, 1 + u; 1 + u, 1 + u, 1 + u)$	$(u, 0, 1; 1, 1, 1)$
$(0, 1, 1 + u; u, u, u)$	$(1, 0, u; 1 + u, 1 + u, 1 + u)$	$(0, 1, 0; 1 + u, 1 + u, 1 + u)$
$(1, 1, 0; u, u, u)$	$(0, 1 + u, 1; 0, 0, 0)$	$(u, 0, 0; 0, 0, 0)$
$(1, 1 + u, 1; 1 + u, 1 + u, 1 + u)$	$(0, 0, 1; 1, 1, 1)$	$(u, u, 1 + u; 1 + u, 1 + u, 1 + u)$
$(u, u, 0; 0, 0, 0)$	$(u, 1 + u, 0; 1, 1, 1)$	$(0, u, 1 + u; 1 + u, 1 + u, 1 + u)$
$(1 + u, u, 1 + u; u, u, u)$	$(1, u, 1 + u; 0, 0, 0)$	$(0, 0, 1 + u; 1, 1, 1)$
$(1 + u, 1 + u, 0; 0, 0, 0)$	$(u, 1 + u, 1 + u; u, u, u)$	$(u, 1 + u, u; 1 + u, 1 + u, 1 + u)$
$(1 + u, 1 + u, 1 + u; 1 + u, 1 + u, 1 + u)$	$(1, 0, 0; 1, 1, 1)$	$(0, 1 + u, 0; 1 + u, 1 + u, 1 + u)$
$(0, 1 + u, 1 + u; 0, 0, 0)$	$(1, 1 + u, 1 + u; 1 + u, 1 + u, 1 + u)$	$(1, 1, u; u, u, u)$
$(1 + u, 0, u; 1 + u, 1 + u, 1 + u)$	$(1, 1, 1; 1, 1, 1)$	$(u, 1 + u, 1; 0, 0, 0)$
$(1, u, u; 1, 1, 1)$	$(1 + u, 1 + u, 1; 1 + u, 1 + u, 1 + u)$	$(0, 1, 1 + u; 0, 0, 0)$
$(1, 1, 0; 0, 0, 0)$	$(0, 1, 1; u, u, u)$	$(0, u, u; u, u, u)$
$(u, 0, 1; 1 + u, 1 + u, 1 + u)$	$(0, u, 1; 1, 1, 1)$	$(1 + u, u, 1 + u; 0, 0, 0)$
$(0, 1, u; 1, 1, 1)$	$(u, 1, u; 1, 1, 1)$	$(1, 0, 1; u, u, u)$
$(0, 0, 1; 1 + u, 1 + u, 1 + u)$	$(u, 0, 1 + u; 1, 1, 1)$	$(1 + u, 0, 0; 1, 1, 1)$
$(u, 1 + u, 0; 1 + u, 1 + u, 1 + u)$	$(1, u, 1; u, u, u)$	$(u, 1 + u, 1 + u; 0, 0, 0)$
$(1, 1, 1 + u; 1, 1, 1)$	$(1 + u, 1, u; u, u, u)$	$(1 + u, 1, 1; 1, 1, 1)$
$(1 + u, u, u; 1, 1, 1)$	$(1, 1, u; 0, 0, 0)$	$(1 + u, u, 0; 1, 1, 1)$
$(0, 0, 1 + u; 1 + u, 1 + u, 1 + u)$	$(u, 0, u; 0, 0, 0)$	$(0, 0, u; u, u, u)$
$(1 + u, 0, 1 + u; u, u, u)$	$(1, 0, 0; 1 + u, 1 + u, 1 + u)$	$(u, 0, u; u, u, u)$
$(1, u, 0; 1, 1, 1)$	$(0, 0, 0; u, u, u)$	$(u, 1, 1; u, u, u)$
$(u, u, u; u, u, u)$	$(1, 0, 1 + u; u, u, u)$	$(u, u, 1; 1, 1, 1)$
$(0, 1, 1; 0, 0, 0)$	$(0, u, u; 0, 0, 0)$	$(1, 1, 1; 1 + u, 1 + u, 1 + u)$
$(0, 1 + u, u; 1, 1, 1)$	$(1, u, u; 1 + u, 1 + u, 1 + u)$	

Table 20 DNA code $\mathcal{D}$ of length 12 obtained from $\mathcal{C} \cup \hat{\mathcal{C}}$ in Example 4.2.12

AAAAAAAAAGGA	AAAAAAAAACCA	TTTTTTTTTATA	GGGGGGGGGGGG	CTCTTTTTTTTT
TTTTTTTTTGCA	AAAAAAAAAACTG	CCCCCCCCCGAT	GGGGGGGGGACT	TCAGGGGGGGGG
TTTTTTTTTGTG	TTTTTTTTTCCT	TGCAAAAAAAAAAA	AAAAAAAAAATAT	TTTTTTTTTTGG
CCCCCCCCCGCG	TTTTTTTTTGAC	GCGCCCCCCCCC	CCCCCCCCCGGG	CCCCCCCCCAGT
GATCCCCCCCCC	AACCCCCCCCCC	AAAAAAAAAATCG	GGGGGGGGGCGAT	CCCCCCCCCCCC
GGGGGGGGGCGC	AAAAAAAAAATTA	GGGGGGGGGGAA	CATGGGGGGGGG	TGTGGGGGGGGG
GGGGGGGGGTCA	GAAGGGGGGGGG	CAACCCCCCCCC	GTGTTTTTTTTT	TTTTTTTTTTCC
TAATTTTTTTTT	GGGGGGGGGATC	GGGGGGGGGCGG	CTCCCCCCCCCC	CTAGGGGGGGGG
GCCGGGGGGGGG	CCCCCCCCCCAA	TTTTTTTTTTCTC	TTTTTTTTTTGGT	AAAAAAAAAAACC
ATCGGGGGGGGG	TTAAAAAAAAAA	AAAAAAAAAAGCT	CCCCCCCCCTTC	TTGGGGGGGGGG
TCCTTTTTTTTT	AAAAAAAAAAACGT	GGCCCCCCCCCC	TTTTTTTTTTTCAG	ACGTTTTTTTTT
CCCCCCCCCACA	GGGGGGGGGTAC	AAAAAAAAAAAAA	CCGGGGGGGGGG	CCAAAAAAAAAAAA
TGAAAAAAAAAA	TTTTTTTTTTAAT	TTTTTTTTTTAGC	CGTAAAAAAAAAA	AAAAAAAAAAATT
CCCCCCCCCCTT	GGGGGGGGGGCC	AAAAAAAAAAGTC	ATGCCCCCCCCC	AGCTTTTTTTTT
CCCCCCCCCAAC	GCATTTTTTTTT	CCCCCCCCCGGC	AAAAAAAAAAGAG	ATATTTTTTTTT
CCCCCCCCCCTCT	TACGGGGGGGGG	AGGAAAAAAAAAA	GGTTTTTTTTTT	AAAAAAAAAATGC
GAGAAAAAAAAAA	ATTAAAAAAAAAA	AAAAAAAAAACAC	CACAAAAAAAAAA	GGGGGGGGGTTG
CGGCCCCCCCCC	TCTCCCCCCCCC	TGGTTTTTTTTT	AAAAAAAAAAGG	CCCCCCCCCGTA
GCTAAAAAAAAAA	GGGGGGGGGGCTA	GTCAAAAAAAAAA	GGGGGGGGGAGA	ACACCCCCCCCC
GACTTTTTTTTT	CCTTTTTTTTTT	GGAAAAAAAAAAAA	TATAAAAAAAAAA	CAGTTTTTTTTT
CGATTTTTTTTT	TTTTTTTTTTGGA	TTCCCCCCCCCC	GTACCCCCCCCC	AATTTTTTTTTT
CCCCCCCCCCTGA	TTTTTTTTTTTAA	AAGGGGGGGGGG	CTGAAAAAAAAAA	TGACCCCCCCCC
CCCCCCCCCATG	GGGGGGGGGGT	CCCCCCCCCTAG	AGTCCCCCCCCC	GGGGGGGGGAAG
TAGCCCCCCCCC	TTTTTTTTTTTTT	CGCGGGGGGGGG	ACCAAAAAAAAAA	GTTGGGGGGGGG
GGGGGGGGGTGT	AGAGGGGGGGGG	TTTTTTTTTTACG	ACTGGGGGGGGG	

Table 21 Codewords from double cyclic code $\mathcal{C}$ of length $(3, 6)$ in
Example 4.3.10

$(0, 1 + u, 1 + u; 0, 1 + u, 1 + u, 0, 1 + u, 1 + u)$	$(1, 0, 0; 1, 0, 0, 1, 0, 0)$
$(1 + u, u, 1; 1 + u, u, 1, 1 + u, u, 1)$	$(u, u, 1; u, u, 1, u, u, 1)$
$(0, 0, 1; 0, 0, 1, 0, 0, 1)$	$(1 + u, 1 + u, 0; 1 + u, 1 + u, 0, 1 + u, 1 + u, 0)$
$(1, 1, u; 1, 1, u, 1, 1, u)$	$(u, 0, 0; u, 0, 0, u, 0, 0)$
$(1, u, 1; 1, u, 1, 1, u, 1)$	$(1 + u, 0, 1 + u; 1 + u, 0, 1 + u, 1 + u, 0, 1 + u)$
$(1 + u, 0, 0; 1 + u, 0, 0, 1 + u, 0, 0)$	$(1 + u, 1 + u, 1 + u; 1 + u, 1 + u, 1 + u, 1 + u, 1 + u, 1 + u)$
$(0, u, u; 0, u, u, 0, u, u)$	$(0, 1 + u, 1; 0, 1 + u, 1, 0, 1 + u, 1)$
$(u, 0, 1 + u; u, 0, 1 + u, u, 0, 1 + u)$	$(0, 1, 1 + u; 0, 1, 1 + u, 0, 1, 1 + u)$
$(1 + u, 1, 0; 1 + u, 1, 0, 1 + u, 1, 0)$	$(1, 0, 1 + u; 1, 0, 1 + u, 1, 0, 1 + u)$
$(0, 0, u; 0, 0, u, 0, 0, u)$	$(1 + u, 0, 1; 1 + u, 0, 1, 1 + u, 0, 1)$
$(u, 1 + u, 0; u, 1 + u, 0, u, 1 + u, 0)$	$(1 + u, 1 + u, 1; 1 + u, 1 + u, 1, 1 + u, 1 + u, 1)$
$(1 + u, 1, 1 + u; 1 + u, 1, 1 + u, 1 + u, 1, 1 + u)$	$(u, 1 + u, 1 + u; u, 1 + u, 1 + u, u, 1 + u, 1 + u)$
$(1, 1 + u, 0; 1, 1 + u, 0, 1, 1 + u, 0)$	$(u, 0, 1; u, 0, 1, u, 0, 1)$
$(0, 1, 1; 0, 1, 1, 0, 1, 1)$	$(1, 1 + u, 1 + u; 1, 1 + u, 1 + u, 1, 1 + u, 1 + u)$
$(1, 0, 1; 1, 0, 1, 1, 0, 1)$	$(1 + u, 1, 1; 1 + u, 1, 1, 1 + u, 1, 1)$
$(1 + u, u, u; 1 + u, u, u, 1 + u, u, u)$	$(u, u, u; u, u, u, u, u, u)$
$(u, 1, 0; u, 1, 0, u, 1, 0)$	$(1, u, u; 1, u, u, 1, u, u)$
$(1, 1, 0; 1, 1, 0, 1, 1, 0)$	$(1, 1 + u, 1; 1, 1 + u, 1, 1, 1 + u, 1)$
$(1, 1, 1 + u; 1, 1, 1 + u, 1, 1, 1 + u)$	$(0, 1 + u, u; 0, 1 + u, u, 0, 1 + u, u)$
$(0, u, 0; 0, u, 0, 0, u, 0)$	$(u, 1 + u, 1; u, 1 + u, 1, u, 1 + u, 1)$
$(u, 1, 1 + u; u, 1, 1 + u, u, 1, 1 + u)$	$(0, u, 1 + u; 0, u, 1 + u, 0, u, 1 + u)$
$(u, 1, 1; u, 1, 1, u, 1, 1)$	$(1 + u, 0, u; 1 + u, 0, u, 1 + u, 0, u)$
$(1 + u, u, 0; 1 + u, u, 0, 1 + u, u, 0)$	$(1 + u, 1 + u, u; 1 + u, 1 + u, u, 1 + u, 1 + u, u)$
$(u, 1 + u, u; u, 1 + u, u, u, 1 + u, u)$	$(u, 0, u; u, 0, u, u, 0, u)$
$(0, 1, u; 0, 1, u, 0, 1, u)$	$(0, u, 1; 0, u, 1, 0, u, 1)$
$(1, 0, u; 1, 0, u, 1, 0, u)$	$(1, u, 0; 1, u, 0, 1, u, 0)$
$(0, 1 + u, 0; 0, 1 + u, 0, 0, 1 + u, 0)$	$(0, 0, 0; 0, 0, 0, 0, 0, 0)$
$(1, 1, 1; 1, 1, 1, 1, 1, 1)$	$(1 + u, 1, u; 1 + u, 1, u, 1 + u, 1, u)$
$(u, u, 0; u, u, 0, u, u, 0)$	$(1 + u, u, 1 + u; 1 + u, u, 1 + u, 1 + u, u, 1 + u)$
$(u, u, 1 + u; u, u, 1 + u, u, u, 1 + u)$	$(0, 0, 1 + u; 0, 0, 1 + u, 0, 0, 1 + u)$
$(1, 1 + u, u; 1, 1 + u, u, 1, 1 + u, u)$	$(1, u, 1 + u; 1, u, 1 + u, 1, u, 1 + u)$
$(0, 1, 0; 0, 1, 0, 0, 1, 0)$	$(u, 1, u; u, 1, u, u, 1, u)$

Table 22 Codewords from double cyclic code $\mathcal{C}$ of length $(3, 6)$ in Example 4.3.11

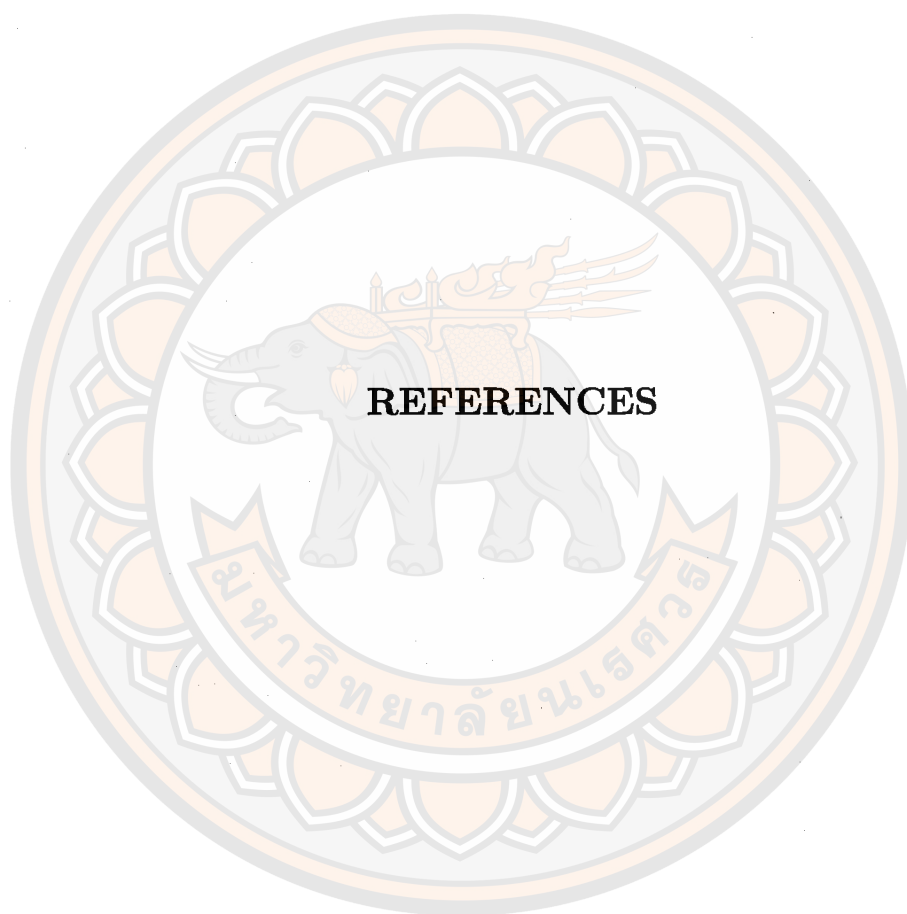
$(1 + u, 1 + u, 1 + u; 1, 1, 1, 1 + u, 1 + u, 1 + u)$	$(1 + u, 1 + u, 1 + u; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(u, u, u; 0, 0, u, 0, 0, u)$	$(0, 0, 0; u, u, 0, u, u, 0)$
$(1 + u, 1 + u, 1 + u; 1 + u, 1 + u, 1, 1, 1, 1 + u)$	$(u, u, u; u, 0, u, u, 0, u)$
$(u, u, u; 0, u, u, 0, u, u)$	$(1, 1, 1; 1, 1 + u, 1 + u, 1 + u, 1, 1)$
$(1, 1, 1; 1 + u, 1 + u, 1, 1, 1, 1 + u)$	$(1, 1, 1; 1, 1, 1, 1 + u, 1 + u, 1 + u)$
$(0, 0, 0; 0, 0, u, 0, 0, u)$	$(1, 1, 1; 1 + u, 1, 1, 1, 1 + u, 1 + u)$
$(1, 1, 1; 1 + u, 1 + u, 1 + u, 1, 1, 1)$	$(0, 0, 0; u, 0, 0, u, 0, 0)$
$(u, u, u; u, u, u, u, u, u)$	$(1 + u, 1 + u, 1 + u; 1, 1 + u, 1, 1 + u, 1, 1 + u)$
$(1 + u, 1 + u, 1 + u; 1 + u, 1, 1 + u, 1, 1 + u, 1)$	$(0, 0, 0; 0, u, u, 0, u, u)$
$(0, 0, 0; u, 0, u, u, 0, u)$	$(1, 1, 1; 1 + u, 1, 1 + u, 1, 1 + u, 1)$
$(0, 0, 0; u, u, u, u, u, u)$	$(u, u, u; 0, 0, 0, 0, 0, 0)$
$(1, 1, 1; 1, 1 + u, 1, 1 + u, 1, 1 + u)$	$(1 + u, 1 + u, 1 + u; 1, 1, 1 + u, 1 + u, 1 + u, 1)$
$(1 + u, 1 + u, 1 + u; 1 + u, 1, 1, 1, 1 + u, 1 + u)$	$(u, u, u; 0, u, 0, 0, u, 0)$
$(u, u, u; u, 0, 0, u, 0, 0)$	$(1 + u, 1 + u, 1 + u; 1 + u, 1 + u, 1 + u, 1, 1, 1)$
$(0, 0, 0; 0, 0, 0, 0, 0, 0)$	$(u, u, u; u, u, 0, u, u, 0)$
$(1, 1, 1; 1, 1, 1 + u, 1 + u, 1 + u, 1)$	$(0, 0, 0; 0, u, 0, 0, u, 0)$

Table 23 DNA code $\mathcal{D}$ of length 9 obtained from $\mathcal{CUC}$ in Example 4.3.14

GGGGGGCTT	CGCCCCCCC	GGGGGGGGC	CCCCCCTGT	CCCCCGGG
AAAAAACCA	GGGGGGCGG	GGGGGGTCT	TTTTTTCAG	GCATTTTTT
TTTTTTGTG	TTTTTTTTT	TTTTTTGCA	AAAAAACTG	TTTTTTAGC
AGACCCCCC	AAAAAAAGG	ATGGGGGGG	GTGTTTTTT	ACAGGGGGG
TTTTTTCTC	GCTAAAAAA	TTTTTTTGG	CGTAAAAAA	CCCCCCTCA
AAAAAATGC	CCTTTTTTT	CCCCCCTACT	TTTTTTTAA	CCCCCCTAC
AATTTTTTT	CATCCCCC	TCCTTTTTT	AAAAAAACC	GGGGGGTGA
AAAAAATAA	GGGGGGGAT	CAAGGGGGG	TAGGGGGGG	TTTTTTTCC
GTAGGGGGG	TTGGGGGGG	CCCCCCCAT	ATATTTTTT	GTCAAAAAA
ACCAAAAAA	TGTCCCCC	CTGAAAAAA	TGAGGGGGG	GGGGGGTTC
GGTTTTTTT	TTTTTTAAT	TCGAAAAAA	TTTTTTCCT	AGTGGGGGG
GGGGGGGCG	GGGGGGGTA	CCCCCAGAA	CGATTTTTT	GAACCCCCC
TTGCCCCC	AGGAAAAAA	CAGTTTTTT	TTTTTTCGA	CCCCCCCCG
AAAAAAGTC	GCGGGGGGG	CGGGGGGGG	GATGGGGGG	TTTTTTACG
TTTTTTATA	GGGGGGAGT	CCCCCGGCC	CCCCCATC	CCCCCGGAA
GACTTTTTT	TATAAAAAA	CTACCCCCC	TTAAAAAAA	CTTGGGGGG
TCTGGGGGG	CCCCCCTTA	AAAAAATAT	TACCCCCC	AAAAAAATT
CACAAAAAA	ACGTTTTTT	AAGCCCCC	GTTCCCCC	CCCCCCTTG
TCACCCCCC	CCGCCCCC	GGGGGGCAA	AAAAAATCG	ATCCCCCCC
TGGTTTTTT	TGCAAAAAA	TAATTTTTT	GGGCCCCC	CCAAAAAAA
TTTTTTGAC	GGAAAAAAA	AAAAAACAC	AGCTTTTTT	ATTAAAAAA
GGGGGGTAG	GGGGGGCCC	AAAAAAGCT	AACGGGGGG	GGGGGGATG
GGGGGGACA	AAAAAATTA	GGGGGGAAC	CTCTTTTTT	AAAAAAGGA
CCCGGGGGG	GCCCCCCCC	ACTCCCCC	GAGAAAAAA	AAAAAAGAG
TTTTTTGGT	CCCCCCAAG	AAAAAACGT	CCCCCGTT	CCCCCCCCG
GGCGGGGGG				

Table 24 DNA code $\mathcal{D}$ of length 9 obtained from $\mathcal{CUC}$ in Example 4.3.15

AAAAATAAT	AATAATTTT	GGGGCGCGC	TTTTTATTA	AAAATAATA
CCGGGGCCCC	GCGCGCCCC	GGGCGGGCC	TTTTTTTTT	GGGCCCGGG
CCCCCGGGC	GCGCGCGGG	TATTATTTT	TTTAAAAAA	CGCGCGGGG
TTATTATTT	CCCCGCGCG	TTTATTATT	CCCCGGGCC	CCCCCGGGG
ATAATATTT	CCGGGCGGG	GGGCGGGC	GGGCCCCC	CCCGGGGGG
CCCGCCCGG	GGGCGCGCG	ATTATTTTT	GCCCGGCC	TTTTATTAT
TTTTTTAAA	AAATTATTA	ATTATTAAA	CCCGGGCCC	CCCGCGCGC
AATAATAAA	AAAAAATAA	CGGGCCGGG	AAAATTATT	TAATAAAAA
TTATTAAAA	TTTATAATA	GGGGGCCCG	CGCGCGCCC	AAATAATAA
TATTATAAA	AAATATTAT	AAAAAATTT	GGCCCGCCC	TTTAATAAT
TTTTAATAA	GGCCCGGGG	AAATTTTTT	GGGGCCCGG	TAATAATTT
GGGGGGCCC	CGGGCCCCC	CCCGGCCCG	GCCCGGGGG	ATAATAAAA



REFERENCES

REFERENCES

1. Shannon CE. A mathematical theory of communication. The Bell system technical journal. 1948 Jul;27(3):379–423.
2. Prange E. Cyclic Error-Correcting Codes in Two Symbols. Mass: Air Force Cambridge Research Center TN-57-103;1957.
3. Hocquenghem A. Codes correcteurs d'erreurs. Chiffers. 1959;2:147–56.
4. Bose RC, Ray-Chaudhuri DK. On a class of error correcting binary group codes. Information and control. 1960 Mar 1;3(1):68–79.
5. Reed IS, Solomon G. Polynomial codes over certain finite fields. Journal of the society for industrial and applied mathematics. 1960 Jun;8(2):300–4.
6. Kanwar P, Lopez-Permouth SR. Cyclic codes over the integers modulo p^m . Finite fields and their applications. 1997 Oct 1;3(4):334–52.
7. Abualrub T, Oehmke R. Cyclic codes of length $2e$ over $\mathbb{Z}_4$. Discrete Applied Mathematics. 2003 May 15;128(1):3–9.
8. Dinh HQ, López-Permouth SR. Cyclic and negacyclic codes over finite chain rings. IEEE Transactions on Information Theory. 2004 Jul 26;50(8):1728–44.
9. Bonnetcaze A, Udaya P. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Transactions on Information Theory. 1999 May;45(4):1250–5.
10. Abualrub T, Siap I. Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$. Designs, Codes and Cryptography. 2007 Mar;42:273–87.
11. Borges J, Fernández-Córdoba C, Pujol J, Rifà J, Villanueva M. $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: Generator matrices and duality. Designs, Codes and Cryptography. 2010 Feb;54(2):167–79.
12. Fernández-Córdoba C, Pujol J, Villanueva M. $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: rank and kernel. Designs, Codes and Cryptography. 2010 Jul;56(1):43–59.
13. Abualrub T, Siap I, Aydin N. $\mathbb{Z}_2\mathbb{Z}_4$ -Additive Cyclic Codes. IEEE Transactions on Information Theory. 2014 Jan 13;60(3):1508–14.
14. Aydogdu I, Siap I, Ten-Valls R. On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$ -linear and cyclic codes. Finite Fields and Their Applications. 2017 Nov 1;48:241–60.

15. Aydogdu I, Abualrub T. The structure of $\mathbb{Z}_2\mathbb{Z}_2$ -additive cyclic codes. *Discrete Mathematics, Algorithms and Applications*. 2018 Aug 16;10(04):1850048.
16. Shi M, Wu R, Krotov DS. On $\mathbb{Z}_p\mathbb{Z}_{p^k}$ -Additive codes and their duality. *IEEE Transactions on Information theory*. 2018 Nov 30;65(6):3841–7.
17. Dinh HQ, Bag T, Upadhyay AK, Bandi R, Chinnakum W. On the Structure of Cyclic Codes Over $\mathbb{F}_qRS$ and Applications in Quantum and LCD Codes Constructions. *IEEE Access*. 2020 Jan 14;8:18902–14.
18. Dinh HQ, Pathak S, Bag T, Upadhyay AK, Bandi R, Yamaka W. On $\mathbb{F}_2RS$ -cyclic codes and their applications in constructing optimal codes. *Discrete Mathematics*. 2021 May 1;344(5):112310.
19. Biswas S, Bhaintwal M. Quantum codes from $\mathbb{Z}_2\mathbb{Z}_2[u]/\langle u^4 \rangle$ -cyclic codes. *Designs, Codes and Cryptography*. 2022 Feb;90(2):343–66.
20. Bhunia DK, Fernández-Córdoba C, Villanueva M. On the Classification of $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$ -Linear Hadamard Codes. 2024 IEEE International Symposium on Information Theory (ISIT); 2024 July 7–12; Athens, Greece: IEEE; 2024. pp. 693–8.
21. Borges J, Fernández-Córdoba C, Ten-Valls R. $\mathbb{Z}_2$ -double cyclic codes. *Designs, Codes and Cryptography*. 2018 Mar;86:463–79.
22. Aydogdu I, Abualrub T, Samei K. $\mathbb{F}_{q^2}$ -double cyclic codes with respect to the Hermitian inner product. *Applicable Algebra in Engineering, Communication and Computing*. 2024 Mar;35(2):151–66.
23. Yao T, Shi M, Solé P. Double cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. *International Journal of Information and Coding Theory*. 2015;3(2):145–57.
24. Gao J, Shi M, Wu T, Fu FW. On double cyclic codes over $\mathbb{Z}_4$. *Finite Fields and Their Applications*. 2016 May 1;39:233–50.
25. Gao J, Hou X. $\mathbb{Z}_4$ -Double Cyclic Codes Are Asymptotically Good. *IEEE Communications Letters*. 2020 May 5;24(8):1593–7.
26. Deng T, Yang J. Double Cyclic Codes over $\mathbb{F}_q + v\mathbb{F}_q$. *Mathematics*. 2020;8(10):1–22.
27. Gao J, Wu T, Fu FW. Hulls of double cyclic codes. *Finite Fields and Their Applications*. 2023 Jun 1;88:102189.
28. Meng X, Gao J, Fu FW. Weight distribution of double cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$. *Finite Fields and Their Applications*. 2024 Mar 1;95:102389.

29. Adleman LM. Molecular computation of solutions to combinatorial problems. *Science*. 1994 Nov 11;266(5187):1021–4.
30. Church GM, Gao Y, Kosuri S. Next-generation digital information storage in DNA. *Science*. 2012 Sep 28;337(6102):1628.
31. Erlich Y, Zielinski D. DNA Fountain enables a robust and efficient storage architecture. *science*. 2017 Mar 3;355(6328):950–4.
32. Organick L, Ang SD, Chen YJ, Lopez R, Yekhanin S, Makarychev K, Racz MZ, Kamath G, Gopalan P, Nguyen B, Takahashi CN. Random access in large-scale DNA data storage. *Nature biotechnology*. 2018 Mar;36(3):242–8.
33. Marathe A, Condon AE, Corn RM. On combinatorial DNA word design. *Journal of Computational Biology*. 2001 Jun 1;8(3):201–19.
34. Nelson DL, Lehninger AL, Cox MM. *Lehninger principles of biochemistry*. 4th ed. US: W. H. Freeman; 2004.
35. Gaborit P, King OD. Linear constructions for DNA codes. *Theoretical Computer Science*. 2005 Apr 15;334(1–3):99–113.
36. Abualrub T, Ghrayeb A, Zeng XN. Construction of cyclic codes over $GF(4)$ for DNA computing. *Journal of the Franklin Institute*. 2006 Jul 1;343(4–5):448–57.
37. Siap I, Abualrub T, Ghrayeb A. Cyclic DNA codes over the ring $\mathbb{F}_2[u]/\langle u^2 - 1 \rangle$ based on the deletion distance. *Journal of the Franklin Institute*. 2009 Oct 1;346(8):731–40.
38. Guenda K, Gulliver TA. Construction of cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$ for DNA computing. *Applicable Algebra in Engineering, Communication and Computing*. 2013 Dec;24:445–59.
39. Liang J, Wang L. On cyclic DNA codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *Journal of Applied Mathematics and Computing*. 2016 Jun;51:81–91.
40. Dinh HQ, Pathak S, Upadhyay AK, Yamaka W. New DNA codes from cyclic codes over mixed alphabets. *Mathematics*. 2020 Nov 6;8(11):1977.
41. Malik DS, Mordeson JN, Sen MK. *Fundamentals of abstract algebra*. New York: McGraw-Hill; 1997.
42. Wan ZX. *Lectures on finite fields and Galois rings*. Singapore: World Scientific Publishing Company; 2003.

- 43. Beachy JA. Introductory lectures on rings and modules. UK: Cambridge University Press; 1999.
- 44. McDonald BR. Finite Rings with Identity. New York: M. Dekker; 1974.
- 45. Lee GT. Abstract algebra: An introductory course. German: Springer; 2018.
- 46. Ling S, Xing C. Coding theory: a first course. UK: Cambridge university press; 2004 Feb 12.
- 47. D'yachkov AG, Erdős PL, Macula AJ, Rykov VV, Torney DC, Tung CS, Vilenkin PA, White PS. Exordium for DNA codes. Journal of Combinatorial Optimization. 2003 Dec;7:369–79.

