A STUDY ON SKEW CODES AND QUANTUM CODES OVER SOME FINITE RINGS

Ph.D. THESIS

by

AMIT SHARMA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE – 247667 (INDIA)
JULY, 2018

A STUDY ON SKEW CODES AND QUANTUM CODES OVER SOME FINITE RINGS

A THESIS

Submitted in partial fulfilment of the requirements for the award of the degree

of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

AMIT SHARMA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE–247667 (INDIA)
JULY, 2018

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in this thesis entitled, **"A STUDY ON SKEW CODES AND QUANTUM CODES OVER SOME FINITE RINGS"** in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy and submitted in the Department of Mathematics of the Indian Institute of Technology Roorkee, Roorkee is an authentic record of my own work carried out during a period from July, 2013 to July, 2018 under the supervision of Dr. Maheshanand, Associate Professor, Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other Institution.

(AMIT SHARMA)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(Maheshanand)
Supervisor

Date**: July , 2018**

Dedicated

to

My Loving Wife and Parents

Abstract

Coding Theory deals with the construction and analysis of error-correcting codes for the reliable and efficient transmission of information through noisy channels. Since its inception, it has grown in to a large area, intersecting several disciplines and using several sophisticated mathematical techniques. The branch of coding theory that mainly uses algebraic tools is known as Algebraic Coding Theory. Initially, algebraic codes were constructed as vector spaces over finite fields. However, later on many rings have also been considered in place of fields, and codes were studied as modules over finite rings. A recent addition to coding theory literature is skew codes, in which algebraic codes are constructed using skew polynomial rings. Several results have been obtained on these codes, and many new good codes have been obtained in this setting.

This thesis deals with some families of codes in the setting of skew polynomial rings over some extensions of $\mathbb{Z}_4$ and $\mathbb{F}_q$, where $\mathbb{Z}_4$ is the ring of integers modulo 4 and $\mathbb{F}_q$ is a finite field. These are skew-cyclic codes, skew-constacyclic codes, 2D skew-cyclic codes etc. In addition, quantum codes over $\mathbb{F}_4 + u\mathbb{F}_4$ have also been studied.

In this context, we have defined a new class of skew-cyclic codes over the mixed alphabet $\mathbb{F}_3(\mathbb{F}_3 + v\mathbb{F}_3), v^2 = v$. We call these codes $\mathbb{F}_3(\mathbb{F}_3 + v\mathbb{F}_3)$-skew cyclic codes, and they can be seen as a generalization of double cyclic codes [25] and $\mathbb{Z}_2(\mathbb{Z}_2+u\mathbb{Z}_2)$-linear cyclic codes [6]. We have obtained a structure of skew-cyclic codes over $\mathbb{F}_3+v\mathbb{F}_3$ by defining a division algorithm on $(\mathbb{F}_3+v\mathbb{F}_3)[x, \theta]$. Using this structure, we have obtained the structures of $\mathbb{F}_3(\mathbb{F}_3 + v\mathbb{F}_3)$-skew cyclic codes and their generating

sets. The duals of these codes have also been studied. Also, we have studied a class of skew-cyclic codes over $\mathbb{F}_p + w\mathbb{F}_p, w^2 = 1$, wherein the generating sets of these codes have been obtained.

The extensions of $\mathbb{Z}_4$ such as $\mathbb{Z}_4 + u\mathbb{Z}_4$ have attracted the attention of a lot of researchers in last few years. Some studies have shown that the codes over these rings are promising and can produce codes with better parameters. However, there has been a relatively little study on skew codes over these types of rings. We study a class of skew-constacyclic codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = 0$. By defining an automorphism θ on $\mathbb{Z}_4 + u\mathbb{Z}_4$, we study these codes as left $(\mathbb{Z}_4 + u\mathbb{Z}_4)[x, \theta]$-submodules of $\frac{(\mathbb{Z}_4+u\mathbb{Z}_4)[x,\theta]}{\langle x^n-\alpha\rangle}$, where $\alpha = 1 + 2u$, a unit in $\mathbb{Z}_4 + u\mathbb{Z}_4$. A necessary and sufficient condition for a skew-constacyclic code over $\mathbb{Z}_4 + u\mathbb{Z}_4$ to be principally generated has been obtained. Duals of these codes have also been studied and these codes have been further generalized to double skew-constacylic codes. By finding the Gray images of these codes some new good $\mathbb{Z}_4$-linear codes having parameters $(6, 4^4 2^2, 2_L), (18, 4^4 2^1, 10_L), (18, 4^4 2^2, 7_L)$ and $(18, 4^4 2^4, 7_L)$ have been obtained. Moreover, we have reported these codes to the database of $\mathbb{Z}_4$-codes [8]. A class of skew-cyclic codes over the ring $GR(4, 2) + vGR(4, 2), v^2 = v$, has also been studied.

We have also studied skew codes in the more general setting of a skew-polynomial ring with automorphism and derivation. In this context, we have studied a class of skew-cyclic codes over $\mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$, with derivation. We denote these codes by δ_θ-cyclic codes. These codes are studied as left $(\mathbb{Z}_4 + w\mathbb{Z}_4)[x, \theta, \delta_\theta]$-submodules of $\frac{(\mathbb{Z}_4+w\mathbb{Z}_4)[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$, where θ is an automorphism of $\mathbb{Z}_4 + w\mathbb{Z}_4$ and δ_θ a derivation on $\mathbb{Z}_4 + w\mathbb{Z}_4$. Using a Gray map, some good linear codes over $\mathbb{Z}_4$, via residue codes of these codes, have been obtained. A generator matrix of the dual code of a free δ_θ-cyclic code of even length over $\mathbb{Z}_4 + w\mathbb{Z}_4$ has been obtained. These codes are further generalized to double skew-cyclic codes with derivation. The classification of these codes also led to some new good $\mathbb{Z}_4$-codes.

There is another generalization of cyclic codes, known as 2D cyclic codes. Recently, Li & Li [65] have studied 2D skew-cyclic codes over a finite field $\mathbb{F}_q$. We generalize the study of 2D skew-cyclic codes over $\mathbb{F}_q$ to 2D skew-cyclic codes over $\mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$. The structure of these codes has been obtained by defining a division algorithm on the bivariate polynomial ring $(\mathbb{F}_q + w\mathbb{F}_q)[x, y, \theta_1, \theta_2]$, where θ_1, θ_2 are two commuting automorphisms of $\mathbb{F}_q + w\mathbb{F}_q$. These codes have been studied as left $(\mathbb{F}_q + w\mathbb{F}_q)[x, y, \theta_1, \theta_2]$-submodules of $\frac{(\mathbb{F}_q+w\mathbb{F}_q)[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$. A brief description of the duals of these codes has also been given. A decomposition of these codes has been presented, via which a generating set of a 2D skew-cyclic code over $\mathbb{F}_q + w\mathbb{F}_q$ is determined using generating sets of its component 2D skew-cyclic codes over $\mathbb{F}_q$.

The relationship between quantum information and classical information has become a subject of much study in recent years. The construction of quantum codes using classical linear codes was given by Calderbank et al. [31]. Motivated by the recent progress in this field, we have studied quantum codes over $\mathbb{F}_4+u\mathbb{F}_4, u^2 = 0$. In our study, we use the structure of cyclic codes of arbitrary length over $\mathbb{F}_4+u\mathbb{F}_4$ to find out the conditions for these codes to contain their duals. By the CSS construction and a Gray map, the parameters of the corresponding quantum codes over $\mathbb{F}_4$ have been obtained. Also, using augmentation, we enlarge a code with dual containing property to a new code having the same property, and we have got some good quantum codes over $\mathbb{F}_4$ using this technique. A table showing some good quantum codes that we have obtained over $\mathbb{F}_4$ is also given.

Publications

The following papers have been produced during this research.

Journal Papers:

1. **Amit Sharma** and Maheshanand Bhaintwal: $\mathbb{F}_3R$-skew cyclic codes, *International Journal of Information and Coding Theory*, Vol. 3, No. 3 (2016), $234-251$, Inderscience.

2. **Amit Sharma** and Maheshanand Bhaintwal: A class of skew-constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, *International Journal of Information and Coding Theory*, Vol. 4, No. 4 (2017), $286-303$, Inderscience.

3. **Amit Sharma**, Ramakrishna Bandi and Maheshanand Bhaintwal: Quantum codes via cyclic codes of arbitrary length over $\mathbb{F}_4+u\mathbb{F}_4$, *Discrete Mathematics, Algorithms, and Applications*, Vol. 10, No. 3 (2018), 1850033, World Scientific.

4. **Amit Sharma** and Maheshanand Bhaintwal: A class of skew-cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$ with derivation, Under revision, *Advances in Mathematics of Communications*, AIMS.

5. **Amit Sharma** and Maheshanand Bhaintwal: A Class of 2D skew-cyclic codes over $\mathbb{F}_q+u\mathbb{F}_q$, Communicated.

Conference Papers:

1. **Amit Sharma** and Maheshanand Bhaintwal: On skew-cyclic codes over $GR(4,2)+uGR(4,2)$, In Proc. *The Seventh International Workshop on Signal Design and its Applications in Communications* (IWSDA'2015), Indian Institute of Science Bangalore, Bengaluru, India, September 13-18 (2015), pp. $52-56$ (Available on IEEE Explore).

2. **Amit Sharma** and Maheshanand Bhaintwal: Additive skew-cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, In Proc. *The* 6^{th} *International Conference on Computer Science and Computational Mathematics* (ICCSCM'2017), Langkawi, Malaysia, May 4-5 (2017), pp. 397-402.

Acknowledgement

I would like to express my sincere gratitude to my supervisor, Dr. Maheshanand Bhaintwal for his dedicated help, inspiration, advice, encouragement and continuous support, throughout my Ph.D. It has been almost five years since I am working with him, and through this time, he has guided me in all aspects of my life. His insightfulness in asking the most fundamental questions is awe-inspiring and has helped me immensely in my research. His passion for research and dedication to teaching have influenced me profoundly. He taught me not only to be a better researcher, but also a better teacher, and a better person. Working with him over the years has made my experience truly wonderful.

I am also thankful to Prof. N. Sukavanam, Head of the Department, and former Heads of the Department, Mathematics for providing the necessary facilities to carry out the research work. My sincere thanks must also go to my student research committee members: Prof. P. Sateesh Kumar, Department of Computer Science and Engineering, Prof. Kusum Deep and Prof. Sanjeev Kumar, Department of Mathematics, for sparing their valuable time in reviewing and critically examining my research progress.

I gratefully acknowledge the funding agency, Council of Scientific & Industrial Research (CSIR), India, for providing financial support for my Ph.D. thesis work.

My heartfelt thanks to my senior Dr. Ramakrishna Bandi for his guidance. My special thanks to fellow lab mates, Srinivasulu B., Soumak Biswas, Raj Kumar, Charul and my Ph.D. batch mates for always standing by my side and sharing a great relationship as friends. I will forever cherish the warmth shown by them.

I owe my most profound gratitude towards my better half, Palika Prabhakar, for her constant support and continuing encouragement. Her unfailing love has always been my strength. Without her help, I would not have been able to complete much of what I have done and become who I am. A special thanks to my brothers Kapil and Nitin, brothers-in-law Rahil and Agam for their love and affection. My sincere regard goes to my parents and parents-in-law for their love and moral support.

Amit Sharma

List of Tables

Table of Contents

Chapter 1

Introduction

1.1 Origins of coding theory

Communication is deeply rooted in the human behavior and is as old as the mankind itself. Error-correcting codes, a part of the theory of communication, is still a young subject that deals with the reliable transmission of data through noisy channels. The secure and reliable transmission of information over noisy channels is a fundamental requirement in digital communication, and coding theory plays a vital role in it. Coding theory is the art of adding redundancy to the message analytically so that if some error occurs during the transmission of the message it can still be recovered due to the redundancy added.

Coding theory originated with the works of Hamming [49] and Shannon [88]. Hamming devised a way of encoding information so that if a single error occurs during the transmission, it could be corrected. Shannon's seminal work "A Mathematical theory of communication" [88] gave birth to coding theory and information theory. Shannon proved that almost error-free communication can be achieved through a channel at any rate below a number, known as the capacity of the channel. The approximation to this ideal has the property that if a digital signal is altered in some reasonable way during the transmission, the original message can still be recovered. However, Shannon's results were probabilistic and existential but not constructive. That is, any information regarding the construction of codes to achieve the channel capacity had not been given by him. Hamming was the first to develop a family of codes, known as Hamming codes, which could correct single errors. Although, these codes were not as good to achieve channel capacity given by Shannon, they were considered important because they have shown the construction of such codes which fit in Shannon's theory. Since then, most work in coding theory is devoted to constructing codes that have efficient encoding and decoding algorithms and which have good error correcting capability.

For the last seventy years, the theory of error-correcting codes has grown into an area intersecting many scientific disciplines including electrical engineering, mathematics and computer science having applications in almost all digital transmission systems and devices such as compact disc recording, cellular telephone transmission, data storage etc. Besides these, coding theory has applications in the field of cryptography and design theory. The constructions of codes require techniques from a surprisingly wide range of mathematics. The area of coding theory which mainly uses algebraic tools for the analysis of codes is known as algebraic coding.

1.2 Development of the subject

Classically error correcting codes have been studied as subspaces of vector spaces over finite fields. In 1957, Prange [80, 81] introduced cyclic codes over a finite field $\mathbb{F}_q$ and characterized these codes with ideals in the ring $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$, where n is the length of code. This relationship between cyclic codes and ideals has facilitated the construction of important families of codes such as BCH codes and Reed-Solomon codes.

Coding theorists have studied various families of linear and cyclic codes in past six decades. Different approaches and tools have been applied and many codes with good parameters and properties have been produced [10, 11, 12, 55]. Recently, a tremendous interest in codes over more general algebraic structure such as rings has been seen, where the codes have been studied as modules over finite rings. The study of codes using finite rings began with the works of Blake [20, 21], which were followed by the works of Spiegel [97, 98] and Shanker [87]. However, this area generated the main interest of researchers after a landmark paper in 1994 by Hammons et al. [50], wherein they have shown that certain good non-linear binary codes such as binary Kerdock codes, Preparata codes, Goethals codes and Delsarte-Goethals codes are the Gray images of some linear codes over $\mathbb{Z}_4$. This was shown by expoiting the isometry between (${\mathbb{Z}_4}^n$, Lee distance) and (${\mathbb{Z}_2}^{2n}$, Hamming distance). Using the Gray map, a new set of linear and non-linear binary codes have been constructed as the Gray images of some codes over $\mathbb{Z}_4$. This approach has thus helped to view some non-linear binary codes as images of linear quaternary codes. A lot of research has been done on codes over $\mathbb{Z}_4$ and other integer rings [23, 32, 100, 34, 61, 47, 18, 78, 19, 44, 46, 92], as well as on codes over some more general finite rings [22, 37, 82, 108, 103, 104, 68, 67, 13, 71, 72, 73]. Many good codes over finite rings have been obtained.

The works described so far are in the commutative setting, i.e., the alphabet and the polynomial algebra used to describe the codes are commutative. Recently, Boucher et al. [26] have added a new direction in coding theory by studying codes in the non-commutative setting of skew polynomial rings. In [26], they introduced a new concept by defining cyclic codes using skew polynomial rings, and studied skew-cyclic codes over a finite field $\mathbb{F}_q$ as ideals of $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1\rangle}$, where $\mathbb{F}_q[x,\theta]$ is the skew polynomial ring by automorphism over $\mathbb{F}_q$, and θ is the corresponding automorphism. This work has been further generalized in many ways [27, 28, 2, 58, 1, 16, 41, 48, 65]. In [27], skew-cyclic codes have been generalized to Galois rings, which is a more general structure. Boucher et al. [28] have then studied skew codes as modules over skew polynomial rings. Abualrub et al. [2] have generalized this class to skew quasi-cyclic codes and Bhaintwal [16] has studied skew quasi-cyclic codes over Galois rings. Jitman et al. [58] further generalized this work by studying a class of skew constacyclic codes over finite chain rings. Aydin et al. [1] have introduced a class of θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. They have defined a division algorithm on the skew polynomial ring $(\mathbb{F}_2 + v\mathbb{F}_2)[x, \theta]$, where θ is an automorphism of $\mathbb{F}_2 + v\mathbb{F}_2$, in a new way such that the generators of these codes and their duals can be obtained. In [41] and [48], the some work on skew codes has been done on $\mathbb{F}_p + v\mathbb{F}_p$ and $\mathbb{F}_q + v\mathbb{F}_q$, respectively. The class of skew-cyclic codes has been further generalized to 2D skew-cyclic codes over $\mathbb{F}_q$ by Li & Li in [65].

1.2.1 Motivation for our investigations

In this section, we present a short survey of the works from the literature that have motivated our research.

A lot of ideas have been applied to construct different types of linear codes with rich algebraic structures and good parameters. Cyclic codes form an important class of linear codes with good algebraic structure and they are being investigated since they were introduced by Prange [80]. Recently, codes using rings have attracted the attention of many researchers and many good codes have been produced in this class. In particular, cyclic codes and their generalizations such as constacyclic codes, quasi-cyclic codes etc. have been studied extensively over rings. But this work was restricted to codes defined over commutative algebraic structures.

Recently, there has been an interest on the study of codes over skew polynomial rings which are, in general, non-commutative rings. Work in this direction was initiated by Boucher et al. [26]. They studied codes of length n over a finite field $\mathbb{F}_q$ as left ideals of the quotient ring $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1\rangle}$ with $|\theta|$ dividing n, where $\mathbb{F}_q[x,\theta]$ is the skew polynomial ring over $\mathbb{F}_q$ and θ is the corresponding automorphism of $\mathbb{F}_q$. Such codes are known as skew-cyclic codes. If the condition that $|\theta|$ divides n is not imposed, the resulting structure $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1\rangle}$ is no more a ring because $\langle x^n - 1\rangle$ need not be a two sided ideal of $\mathbb{F}[x,\theta]$. For arbitrary f, n does not need such a restriction. The case was generalized to the study of codes of length n as ideals of the rings $\frac{\mathbb{F}_q[x,\theta]}{\langle f\rangle}$, where f is a central polynomial in $\mathbb{F}[x,\theta]$ and $\langle f\rangle$ is the two sided ideal generated by f in $\mathbb{F}_q[x,\theta]$ [29]. Some good codes have been obtained in this class. This work has been extended further by many researchers [27, 58, 2, 96]. In [96], Siap et al. removed the restriction of $|\theta|$ dividing n and studied the structure of skew-cyclic codes over finite fields having arbitrary length. In this setting, the skew codes have been defined as left $\mathbb{F}_q[x,\theta]$-submodules of left $\mathbb{F}_q[x,\theta]$-module $\frac{\mathbb{F}_q[x,\theta]}{\langle f\rangle}$, where f is any polynomial in $\mathbb{F}_q[x,\theta]$. If $f = x^n - 1$ and $|\theta| = m$, then the skew-cyclic codes of length n as left $\mathbb{F}_q[x,\theta]$-submodules of $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1\rangle}$ give following relations. Skew-cyclic codes are equivalent to cyclic codes, if $(m,n) = 1$, and they are equivalent to quasi-cyclic codes of length n and index d, if $(m,n) = d$, where d is greater than 1.

The ring $\mathbb{F}_q[x,\theta]$ is left and right Euclidean. Therefore the cyclic codes and skew-cyclic codes over $\mathbb{F}_q$ share most properties. Since the polynomials in skew polynomial rings possess more factors than in the commutative case, there are many ideals in this setting. Therefore there are better possibilities of finding good codes. This gives us a strong motivation for studying codes in this setting.

Most of the works discussed above are on finite fields and finite chain rings such as Galois rings. Recently, skew-cyclic codes over some finite non-chain rings have also been studied [1, 41, 48, 94, 43]. In [1], Abualrub et al. defined a class of skew-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ with $v^2 = v$, and obtained a structure thereof. They also presented some examples of optimal binary self-dual codes through this class. In [41], Gao has studied principally generated skew-cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ with $v^2 = v$. Gursoy et al. [48] presented a different approach to construct skew-cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$. The results of [48] have been generalized to $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q, v^2 = v$, by Shi et al. [94]. Gao et al. [43] has studied a class of skew constacyclic codes over $\mathbb{F}_q + v\mathbb{F}_q, v^2 = v$. Recently, some new types of codes over rings have been proposed [4, 7, 6, 25, 9]. In [25], Borges et al. have studied $\mathbb{Z}_2$-double cyclic code as $\mathbb{Z}_2[x]$-submodule of $\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}$. In [6], Abualrub et. al. have studied linear cyclic codes as submodules of $\mathbb{Z}_2^\alpha \times (\mathbb{Z}_2 + u\mathbb{Z}_2)^\beta$, which in polynomial form are $(\mathbb{Z}_2 + u\mathbb{Z}_2)[x]$-submodules of $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha-1\rangle} \times \frac{(\mathbb{Z}_2+u\mathbb{Z}_2)[x]}{\langle x^\beta-1\rangle}$. However, the works given in [4, 7, 6, 25, 9] have been done over commutative setting. These works, especially [6], have motivated us to generalize such codes to the non-commutative setting of skew-polynomial rings. This resulted into a new class of skew-cyclic codes, which we termed as $\mathbb{F}_3R$-skew cyclic codes, $R = \mathbb{F}_3 + v\mathbb{F}_3, v^2 = v$. We have obtained a division algorithm on $R[x,\theta]$ using which we present the structure of a skew-cyclic code for the different possibilities on the minimum degree polynomial in the code. Thus $\mathbb{F}_3R$-skew cyclic codes have been studied as left $(\mathbb{F}_3+v\mathbb{F}_3)[x,\theta]$-submodules of the left module $\frac{\mathbb{F}_3[x]}{\langle x^\alpha-1\rangle}\times\frac{(\mathbb{F}_3+v\mathbb{F}_3)[x,\theta]}{\langle x^\beta-1\rangle}$ and their generators have been obtained. Further, we have studied a class of skew-cyclic codes and a class of additive skew-cyclic codes over $\mathbb{F}_p+w\mathbb{F}_p$ with $w^2=1$. Chapter 3 covers these results.

The study of codes over $\mathbb{Z}_4$ always generated a special interest and have provided many useful results. There has been a lot of work on codes over $\mathbb{Z}_4$ since the realization in [50] that some binary non-linear codes with good parameters are Gray images of some $\mathbb{Z}_4$- linear codes. Recently, Yildiz and Karadeniz [104] have studied linear and self-dual codes over $\mathbb{Z}_4+u\mathbb{Z}_4, u^2=0$. We have studied a class of skew constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4, u^2=0$. These results are presented in Chapter 4. In the literature, many good codes have been obtained over $\mathbb{Z}_4$ via Gray images of codes over the extensions of $\mathbb{Z}_4$ and these codes have been updated to the database of $\mathbb{Z}_4$-codes [8] (maintained by Aydin and Asamov). Through skew-constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, we have obtained many new good codes over $\mathbb{Z}_4$, and these new codes have been updated to the database of $\mathbb{Z}_4$-codes [8]. Further in Chapter 5, we have generalized this work and studied a class of skew-cyclic codes over $\mathbb{Z}_4+w\mathbb{Z}_4, w^2=1$ with derivation. In this class also, we have obtained some new $\mathbb{Z}_4$-linear codes.

Another family of codes that we have considered in this thesis is 2D-skew cyclic codes. This class was first introduced by Ikai et al. [52] and then further studied by Imai [54]. Recently, Li & Li [65] have introduced a generalization of 2D cyclic codes over finite fields, wherein they have studied 2D skew-cyclic codes of length ml over $\mathbb{F}_q$ as left $\mathbb{F}_q[x,y,\theta_1,\theta_2]$-submodules of $\frac{R[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$, where θ_1,θ_2 are automorphisms of $\mathbb{F}_q$. Inspired by this work, we have generalized 2D skew-cyclic codes over $\mathbb{F}_q$ to the ring $R=\mathbb{F}_q+w\mathbb{F}_q, w^2=1$. We have obtained the generating sets of these codes. The results have been presented in Chapter 6.

Quantum error correcting codes have received much attention of coding theorists in recent years. Like classical information processing, a reliable quantum information processing requires mechanisms to reduce the effects of internal (operational) and external (environmental) noises. Fortunately, it is possible to facilitate the damaging effects of decoherence by applying quantum error-correcting codes, so that one can have more reliable quantum communication schemes and quantum computers. Initially it was assumed that classical error-correction is not possible for quantum information, as classical information can be duplicated but copying quantum information is not possible due to the no-cloning theorem [102]. However, it was shown that it is possible to encode quantum information so that errors can be corrected [95]. The problem of finding good quantum codes has turned out to be the problem of finding classical error-correcting codes that contain their duals [31].

Shor [95] discovered the first quantum error-correcting codes. Afterwards, the construction of quantum codes using classical linear codes was given by Calderbank et al. [31]. Construction of several quantum codes with good parameters have been done using classical codes over finite fields with dual containing property [63, 64, 84, 59, 83]. The study of quantum codes using finite rings was initiated by Qian et al. [84], wherein they have studied quantum codes using cyclic codes of odd length over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. In [59], Kai and Zhu have used cyclic codes of odd length over $\mathbb{F}_4 + u\mathbb{F}_4$, $u^2 = 0$ to construct quantum codes over $\mathbb{F}_4$. Further, Qian [83] has presented a construction of quantum codes via cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, without the restriction on the length of the code. We have explored and generalized this work in Chapter 7, in which we consider the ring $R = \mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$, for the construction of quantum codes through cyclic codes having arbitrary length over R. We have considered cyclic codes of both odd length and even length such that they contain their duals, and corresponding to these codes we have obtained some optimal quantum codes over $\mathbb{F}_4$.

Throughout the thesis, all the computations to find codes have been done with MAGMA Computational Algebra System [101] .

1.3 Contribution and organization of the thesis

Objective: The objective of this thesis is to study and analyse different classes of linear codes such as skew-cyclic codes, skew-constacyclic codes, additive skew cyclic codes, double skew-cyclic codes etc. using univariate and bivariate (non-commutative) skew polynomial rings over some extensions of $\mathbb{Z}_4$ and $\mathbb{F}_q$. Further, we also aim to obtain good codes over $\mathbb{Z}_4$ and $\mathbb{F}_q$ via the Gray images of such codes.

Brief description of our contribution:

- We have introduced a class of skew-cyclic codes over the mixed alphabets $\mathbb{F}_3(\mathbb{F}_3 + v\mathbb{F}_3)$, which is a generalization of double cyclic code and cyclic codes over mixed alphabets in commutative setting.

- Cyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4, u^2 = 0$, are well studied. We have introduced a class of skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = 0$, which is further generalized to double skew-constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$. Through these codes, we have obtained $(\mathbf{6}, \mathbf{4^4 2^2}, \mathbf{2_L})$, $(\mathbf{18}, \mathbf{4^4 2^1}, \mathbf{10_L})$ and $(\mathbf{18}, \mathbf{4^4 2^4}, \mathbf{7_L})$ linear codes over $\mathbb{Z}_4$ via Gray map, that improve the minimum Lee distances of existing codes by $1, 4$ and 1, respectively. These new codes have been reported and added to the database of $\mathbb{Z}_4$-codes [8].

- We have further generalized our work, given in Chapter 4, by introducing a class of skew-cyclic codes over $\mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$ with an automorphism and a derivation. In this class too, we have obtained some good codes over $\mathbb{Z}_4$.

- In the literature there has been a limited study on 2D cyclic codes. In particular, rings have not been considered as alphabet for these codes. We have presented a class of 2D skew-cyclic codes over $R = \mathbb{F}_q+w\mathbb{F}_q, w^2 = 1$. By defining some properties of a skew polynomial ring in two variables $R[x, y, \theta_1, \theta_2]$, where θ_1, θ_2 are commuting automorphisms of R, we have presented a division algorithm on $R[x, y, \theta_1, \theta_2]$. With the help of this, we have obtained the structure of a 2D skew-cyclic code over R. Some examples have been given to illustrate the results.

- We have studied the construction of quantum codes over $\mathbb{F}_4$ through cyclic codes. Cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$ with dual containing property have been studied for odd lengths only. We have studied a class of cyclic codes of arbitrary length over $\mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$ such that these codes contain their duals. Using these codes and a Gray map on $\mathbb{F}_4 + u\mathbb{F}_4$, the parameters of the corresponding quantum codes over $\mathbb{F}_4$ have been obtained.

Organization of the Thesis

The main content of the thesis is contained in five chapters (Chapter 3 to Chapter 7). The thesis is organized as follows.

In **Chapter 2**, some preliminaries and basic concepts are discussed. This forms the required background for later chapters.

In **Chapter 3**, we define a new class of skew-cyclic codes, termed as $\mathbb{F}_3R$-skew cyclic codes, where R denotes the ring $\mathbb{F}_3 + v\mathbb{F}_3, v^2 = v$. Some structural properties of skew-cyclic codes over R and $\mathbb{F}_3R$-skew cyclic codes have been given in Section 3.3 and Section 3.4, respectively. The generator polynomials of these codes are studied. Some examples are given to illustrate the results. An optimal ternary code is obtained as the Gray image of an $\mathbb{F}_3R$-skew cyclic code. We further study a class of skew-cyclic codes over $\mathbb{F}_p + w\mathbb{F}_p, w^2 = 1$ in Section 3.5 .

Chapter 4 focuses on skew codes over $\mathbb{Z}_4+u\mathbb{Z}_4$. In Section 4.3, we characterize the skew polynomial ring $R[x, \theta]$, where $R = \mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = 0$ and θ is an automorphism of R, and study a class of skew-constacyclic codes over R. We determine the structural properties of these codes. They have been further generalized to double skew-constacyclic codes over R in Section 4.5, through which we have been able to obtain some good codes over $\mathbb{Z}_4$. Also, we have studied a class of skew-cyclic codes over $GR(4,2)+vGR(4,2), v^2 = v$ in Section 4.6.

In **Chapter 5**, we study skew-cyclic codes with derivation over $R = \mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$. We present some structural properties of R and the skew polynomial ring $R[x, \theta, \delta_\theta]$, where θ is an automorphism of R and δ_θ a derivation on R. In Section 5.3, δ_θ-cyclic codes are studied. Their torsion codes and residue codes have also been studied in the same section. In Section 5.4, the duals of δ_θ-cyclic codes of even length over R have been obtained. In Section 5.5, we have generalized δ_θ-cyclic codes to double δ_θ-cyclic codes and obtained some good codes over $\mathbb{Z}_4$ from this class also. Table 5.1 and Table 5.2 show some good linear codes over $\mathbb{Z}_4$, which have been obtained as the Gray images of the above mentioned codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$ by using Magma Computational Algebra System.

In **Chapter 6**, we extend skew codes to bivariate skew polynomial rings. Section 6.2 includes some basic definitions and properties of the bivariate skew polynomial ring $R[x, y, \theta_1, \theta_2]$, where $R = \mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$ and θ_1, θ_2 are two commuting automorphisms of R. We introduce a class of 2D skew-cyclic codes over R in Section 6.3, and by defining a division algorithm on $R[x, y, \theta_1, \theta_2]$, generating sets of these codes have been obtained. Their relation with skew-cyclic codes over R has also been given in the same section. Section 6.4 presents the duals of 2D skew-cyclic codes. A decomposition of a 2D skew-cyclic code over R into 2D skew-cyclic codes over $\mathbb{F}_q$ has been given in Section 6.5.

Chapter 7 deals with the study of quantum codes over $\mathbb{F}_4$ obtained via cyclic codes over $\mathbb{F}_4+u\mathbb{F}_4$. Our main aim is to find the conditions under which a cyclic code over $\mathbb{F}_4+u\mathbb{F}_4$ contains its dual. We describe the structures and conditions of cyclic codes of odd length and even length over $R = \mathbb{F}_4 + u\mathbb{F}_4,\ u^2 = 0$, in Subsection 7.2.1 and Subsection 7.2.2, respectively, such that these codes contain their duals. A Gray map is defined on $(\mathbb{F}_4 + u\mathbb{F}_4)^n$ to $\mathbb{F}_4^{2n}$ such that it preserves the dual containing property of a code. Using Gray map and CSS construction, the parameters of corresponding quantum codes over $\mathbb{F}_4$ have been obtained.

Chapter 8 presents conclusion and gives some possible directions for further research based on the work done in this thesis.

Chapter 2

Basic Concepts and Background

In this chapter, we give some preliminaries and basic results on coding theory that are needed for the results in later chapters.

2.0.1 Block codes

We assume that the information from the source is coming in the form of a sequence of symbols from an alphabet Σ with q distinct symbol. In block codes, the information sequence is divided into blocks of length k. These blocks are called messages or message blocks. Thus a message block m is an element of Σ^k. A redundancy is added to each message block so that if some symbols of the message are corrupted due to noise during transmission, we can still recover it from the redundancy added. These new blocks of length $n \geq k$ are called the codewords. The set C of all such codewords is called a block code. Thus $C \subseteq \Sigma^n$.

If a codeword $x \in C$ is transmitted and $y \in \Sigma^n$ is the received word such that $y \neq x$, then we say that an error has occurred and the vector $e = y - x$ is called the error vector. To measure the error-correcting capability of a code C, a distance function, called the Hamming distance, is defined on Σ^n. The Hamming distance between two elements $x, y \in \Sigma^n$ is defined as the number of positions in which x and y differ, i.e.,

$$d_H(x,y) = |\{i \ \mid \ x_i \neq y_i, \ i = 1, 2, \cdots, n\}|.$$

Definition 2.0.1. *The minimum Hamming distance $d(C)$ of a code C is defined as*

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

The Hamming weight $w(x)$ of a word $x \in \Sigma^n$ is defined as the number of non-zero coordinates of x, and the Hamming weight of code C is the minimum weight among all the non-zero codewords in C. It is well known that if a code has the minimum distance d then it has the capability to detect and correct up to $d - 1$ and $\lfloor \frac{d-1}{2} \rfloor$ errors, respectively.

2.0.2 Codes over finite fields

2.0.2.1 Linear codes

Linear codes are the most studied class among all types of block codes since they are easier to analyse, construct, encode, and decode. To introduce linear codes, we let the alphabet Σ to be a finite field $\mathbb{F}_q$ with $q = p^r$ elements, where p is a prime. Then $\Sigma^n = \mathbb{F}_q^n$ is an n-dimensional vector space over $\mathbb{F}_q$. A linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. We denote C an $[n, k]$-code, if it has dimension k. In addition, if C has minimum distance d, we say that C is $[n, k, d]$-code. The rate of code C is k/n.

One immediate advantage of linear codes is that the minimum distance and the minimum weight of the code coincide, and so it is easy to determine the minimum distance of a code. Another advantage of linear codes is that they can simply be represented by matrices. An $[n, k]$ code C can be represented either by a $n \times k$ matrix G whose row space is C or by an $(n - k) \times n$ matrix H whose null space is C. G is called a generator matrix of C and H is called a parity-check matrix of C. Thus the rows of G forms a basis for C and H satisfies the conditions that it has rank $n - k$ and $Hc^{\perp} = 0\ \forall\ c \in C$. Obviously we have $GH^T = 0$. After applying some elementary row and column operations, G can be put in a unique form $[I_k|\ A]$, where A is an $k \times (n-k)$ matrix. Such a generator matrix is known to be in standard form. In this case, the parity check matrix for C is $H = [-A^{\perp}|I_{n-k}]$.

The dual code of an $[n, k]$ code C over $\mathbb{F}_q$ is defined as

$$C^{\perp} = \{v \in \mathbb{F}_q^n \ \mid \ u \cdot v = 0 \text{ for all } u \in C\},$$

where $u \cdot v$ denotes the ordinary inner product of vectors u and v. If H is a parity check matrix of C, then it is a generator matrix of $C^{\perp}$. Similarly, a generator matrix G of C is a parity-check matrix of $C^{\perp}$.

The following result establishes a relation between the minimum distance of a linear code and its parity-check matrix.

Theorem 2.0.2. *([79, Corollary 2.6]) "A linear code C has minimum distance d if and only if its parity check matrix has a set of d linearly dependent columns but no set of $d-1$ linearly dependent columns."*

2.0.2.2 Cyclic codes

Cyclic codes are one of the most commonly used linear codes in practice. We present here some basic definitions and fundamental properties of cyclic codes.

Definition 2.0.3. *(Cyclic codes) A linear code C is said to be a cyclic code if it is invariant under the operation of cyclic shift, i.e., whenever $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, the cyclic shift $(c_{n-1}, c_0, c_1, \cdots, c_{n-2})$ of c is also in C.*

There is a bijection between $\mathbb{F}_q^n$ and the residue class ring $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$ by the correspondence $c = (c_0, c_1, \cdots, c_{n-1}) \leftrightarrow c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. We use the polynomial notation $c(x)$ and c interchangeably. The element $xc(x)$ in $\frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$ then corresponds to the cyclic shift $(c_{n-1}, c_0, \cdots, c_{n-2})$ of $(c_0, c_1, \cdots, c_{n-1})$. Thus $xc(x)$ represents the cyclic shift of $c(x)$. Let C be a cyclic code of length n over $\mathbb{F}_q$. Then C is invariant under cyclic shift operation, so $xc(x)$, and hence $x^tc(x), t \geq 0$ are in C. By linearity, it follows that $a(x)c(x) \in C$ for all $a(x) \in \mathbb{F}_q[x]$. Thus cyclic codes are precisely the ideals of the quotient ring $R_n = \frac{F_q[x]}{\langle x^n-1\rangle}$, and the study of cyclic codes of length n over $\mathbb{F}_q$ reduces to the study of ideals in R_n. Since $\mathbb{F}_q[x]$ is a principal ideal domain, R_n is a principal ideal ring, and hence cyclic codes of length n over $\mathbb{F}_q$ are the principal ideals of R_n. The following facts hold for a cyclic code C of length n over $\mathbb{F}_q$:

- there exists a unique minimal degree polynomial $g(x)$ in C such that $C = \langle g(x) \rangle$,
- $g(x)$ divides $x^n - 1$.

$g(x)$ is called a generator polynomial of C. The cyclic codes of length n over $\mathbb{F}_q$ are thus completely determined by the factors of $x^n - 1$ over $\mathbb{F}_q$. If deg $g(x) = k$, then the set $\{g(x), xg(x), ..., x^{n-k-1}g(x)\}$ forms a basis for C. Let $x^n - 1 = g(x)h(x)$. Then $h(x)$ is known as the check polynomial of C. Moreover, $h^*(x) = x^{n-k}h(x^{-1})$, the reciprocal polynomial of $h(x)$, is a generator polynomial for the dual code $C^\perp$ of C.

Cyclic codes can also be defined in terms of roots of unity. Since $g(x)|x^n - 1$, the roots of $g(x)$ over $\mathbb{F}_q$ are n^{th} roots of unity. Let the roots of $g(x)$ be $\alpha_1, \alpha_2, \cdots, \alpha_k$, C can then be defined as

$$C = \{v(x) \in R_n \mid v(\alpha_i) = 0 \ \forall \ i = 1, 2, \cdots, k\}.$$

The set $T = \{\alpha_i \ \mid \ i = 1, 2, \cdots, k\}$ is called the *defining set* of C.
The following result is well known.

Theorem 2.0.4. *(BCH bound) Let C be a cyclic code of length n over $\mathbb{F}_q$, and let ζ be a primitive n^{th} root of unity in an extension field of $\mathbb{F}_q$. If the zeros of C include consecutive elements $\{\zeta^i \ \mid \ b \leq i \leq b+\delta-2\}$, where $\delta > 1$ and $b \geq 0$, then $d(C) \geq \delta$.*

2.0.2.3 Constacyclic codes

Constacyclic codes are an immediate and remarkable generalization of cyclic codes. They were introduced by Berlekamp [15], and have been studied extensively [11, 51, 56, 57, 89].

Let λ be a unit in $\mathbb{F}_q$, i.e., $\lambda \in \mathbb{F}_q^*$, the set of non-zero elements of $\mathbb{F}_q$. Then we define a map Γ_λ on $\mathbb{F}_q^n$ as

$$\Gamma_\lambda((v_0, v_1, \cdots, v_{n-1})) = (\lambda v_{n-1}, v_0, v_2, \cdots, v_{n-2}),$$

where $(v_0, v_1, \cdots, v_{n-1}) \in \mathbb{F}_q^n$. We call Γ_λ the λ-shift operator. A *λ-constacyclic code* is a linear code C which is invariant under Γ_λ, i.e, $\Gamma_\lambda(C) = C$. In particular, if $\lambda = 1$, then C is simply a cyclic code over $\mathbb{F}_q$.

In polynomial form, a λ-constacyclic code of length n over $\mathbb{F}_q$ corresponds to an ideal of the quotient ring $\frac{\mathbb{F}_q[x]}{\langle x^n - \lambda \rangle}$. The residue class ring $\frac{\mathbb{F}_q[x]}{\langle x^n - \lambda \rangle}$ is a principal ideal ring and so a λ-constacyclic code of length n over $\mathbb{F}_q$ is generated by a single element. Many results of λ-constacyclic codes over $\mathbb{F}_q$ are similar to the case of cyclic codes over $\mathbb{F}_q$.

2.0.3 Local rings

Let R be a finite commutative ring with identity. An ideal M of R is said to be a *maximal* ideal of R if $M \neq R$ and M is not contained in any proper ideal of R.

Definition 2.0.5. *"A ring R is said to be a local ring if R has a unique maximal ideal."*

It is well known that R is a local ring if and only if all the non-units of R form an ideal of R. If R has more than one maximal ideals then it is called a *semi-local* rings.

Examples of commutative local rings are finite fields, $\mathbb{Z}_{p^n}$, Galois rings etc., whereas the ring of matrices $\left\{ \begin{bmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{bmatrix} \middle| \ a, b, c, d \in \mathbb{Z}_p \right\}$ forms a non-commutative local ring over $M_{3\times 3}(\mathbb{Z}_p)$.

Definition 2.0.6. *Let R be a finite commutative ring with identity. Then R is called a finite chain ring if the lattice of all its ideals form a chain under set inclusion,* *i.e, if the ideals of R are of the form*

$$\langle 0\rangle \subset I_1 \subset I_2 \subset \cdots \subset I_n \subseteq R,$$

for some positive integer n.

The chain rings are principal ideal rings having unique maximal ideal, and hence every chain ring is a local ring. For instance, $\mathbb{Z}_{p^m}$, the ring of integers modulo p^m, is a finite chain ring. Let R be a finite chain ring with $M = \langle\lambda\rangle$ as its unique maximal ideal. Let t be the nilpotency of λ. Then the ideals of R form the following chain:

$$\langle 0\rangle = \langle\lambda^t\rangle \subsetneq \langle\lambda^{t-1}\rangle \subsetneq \langle\lambda^{t-2}\rangle \subsetneq \cdots \subsetneq \langle\lambda\rangle \subsetneq \langle\lambda^0\rangle = R.$$

Theorem 2.0.7. *[37, Proposition 2.1]) "For a finite commutative ring R the following conditions are equivalent:*

1. *R is a local ring and the maximal ideal of R is principal,*

2. *R is a local principal ideal ring,*

3. *R is a chain ring."*

Let R be a local ring with the unique maximal ideal M. Then the quotient ring $\frac{R}{M}$ is a finite field, called the residue field of R and is denoted by $\overline{R}$, i.e., $\overline{R} = \frac{R}{M}$. Denote the projection map $R \rightarrow \overline{R}$ by $-$. The image of an element a under this map is denoted by $\overline{a}$. In the usual way, the map $-$ is extended to $R[x] \rightarrow \overline{R}[x]$.

Theorem 2.0.8. *[37, Proposition 2.2] "Let R be a finite commutative chain ring with maximal ideal $M = \langle\lambda\rangle$, and let t be the nilpotency of λ. Then*

1. *For some prime p and positive integers $k, l (k \geq l), |R| = p^k, |\overline{R}| = p^l$, and the characteristic of R and $\overline{R}$ are powers of p.*

2. *For $i = 0, 1, \cdots, t, |\langle\lambda^i\rangle| = |\overline{R}|^{t-i}$. In particular, $|R| = |\overline{R}|^t$, i.e., $k = lt$."*

2.0.3.1 Galois rings

Galois rings are a special case of finite commutative local rings. Let $q = p^r$, p a prime and r a positive integer. Galois rings are extensions of $\mathbb{Z}_q$, which are useful to study codes over $\mathbb{Z}_q$.

Definition 2.0.9. *"A polynomial $f(x)$ over ring $\mathbb{Z}_q[x]$ is said to be a basic irreducible polynomial if $f(x)$ $(mod\, p)$ is an irreducible polynomial in $\mathbb{Z}_p[x]$, and a basic primitive polynomial if $f(x)$ $(mod\, p)$ is a primitive polynomial in $\mathbb{Z}_p[x]$."*

We denote $f(x)(\text{mod } p)$ by $\overline{f}(x)$. Consider the residue class ring $GR(q, m) = \frac{\mathbb{Z}_q[x]}{\langle f(x)\rangle}$, where $f(x) \in \mathbb{Z}_q[x]$ is a monic basic irreducible polynomial of degree m. Then $GR(q, m)$ is called the Galois ring of degree m over $\mathbb{Z}_q$ having characteristic q and cardinality q^m. It is a local ring with maximal ideal $\langle p\rangle = pGR(q, m)$ and residue field $\overline{GR(q, m)} = GR(q, m)/\langle p\rangle = F_{p^m}$.

Let $\xi = x + \langle f(x)\rangle$. Then ξ is a root of $f(x)$ and $GR(q, m) = \mathbb{Z}_q[\xi]$. Moreover $GR(q, m)$ is a free module of rank m over $\mathbb{Z}_q$ with basis $\{1, \xi, \xi^2, \cdots, \xi^{m-1}\}$. So, for all $c \in GR(q, m)$, we have $c = \sum_{i=1}^{m-1} c_i \xi^i$, where $c_i \in \mathbb{Z}_q$. This is known as the additive form of elements of $GR(q, m)$.

Remark 2.0.9.1. *The Galois rings of same order are isomorphic, as in the case of finite fields.*

There is an element η in $GR(q, m)$ such that $o(\eta) = p^m - 1$, so-called a primitive element of $GR(q, m)$. If η is root of a basic primitive polynomial $f(x)$ of degree m over $\mathbb{Z}_q$ which divides $x^{p^m-1} - 1$ in $\mathbb{Z}_q[x]$, then every element $c \in GR(q, m) = \mathbb{Z}_q[x]/\langle f(x)\rangle$ can be expressed as

$$c = a_0 + a_1 p + a_2 p^2 + \cdots + a_{r-1} p^{r-1}$$

where $a_0, a_1, \cdots, a_{r-1} \in \tau = \{0, 1, \eta, \cdots, \eta^{p^m-1}\}$. τ is known as the Teichm$\ddot{u}$ller set of $GR(q, m)$. This representation is called the p-adic representation of elements of $GR(q, m)$ and also known as the multiplicative forms of elements of $GR(q, m)$.

Set of all automorphisms on $GR(q,m)$ form a group, denoted by $Gal(GR(q,m))$ and called Galois group of $GR(q,m)$. This is a cyclic group of order m and generated by the Frobenius automorphism $\phi : GR(q,m) \to GR(q,m)$, defined by $\phi(c) = a_0^p + pa_1^p + p^2a_2^p + \cdots + p^{r-1}a_{r-1}^p$, where $c \in GR(q,m)$ is expressed as $c = a_0 + pa_1 + p^2a_2 + \cdots + p^{r-1}a_{r-1}$. The elements fixed by the automorphism ϕ are precisely the elements of the subring $\mathbb{Z}_q$.

2.0.4 Codes over finite rings

Let R be a finite commutative ring with identity. A subset C of R^n is said to be a linear code of length n over R, if it is an R-submodule of R^n. Unlike in the case of vector spaces, submodules may not be free. So C may not have a basis. However, we can still define a generator matrix for C. A generator matrix of C is a matrix whose rows form a minimal spanning set for C. As noted above, the rows of C may not be linearly independent. The order of minimal spanning set of C is called the *rank* of C. The *free rank* of C is maximum of the ranks of R-free submodules of C.

The Hamming weight and the Hamming distance on R^n can be defined similarly as in the case of vector spaces. Other terminologies like, cyclic codes, constacyclic codes, quasi cyclic codes, that are used over finite fields, can be generalized to R in the usual way. For example, a cyclic code over R can be seen as an ideal of the quotient ring $\frac{R[x]}{\langle x^n-1\rangle}$. Dual of a code, self-dual codes, self orthogonal codes over R are defined similarly as in the case of finite fields.

2.1 Skew polynomial rings

We start with a brief introduction to skew polynomial rings. The investigation of skew polynomial rings is an important and active research area in non-commutative algebra. A systematic study of these rings was done by Ore [76] in 1933, whereas Noether and Schmeidler [75] were the first to consider these kinds of rings. Since then, these rings have been studied extensively. Recently skew polynomial rings have been successfully applied in many areas, for example control theory and coding theory. In this section we give some basic definitions and results on skew polynomial rings and on linear codes over skew polynomial rings.

Definition 2.1.1. *(Skew Polynomial Ring) "Let $\mathbb{F}_q$ be a finite field and θ an automorphism of $\mathbb{F}_q$. The skew polynomial ring $\mathbb{F}_q[x,\theta]$ is the set of polynomials over $\mathbb{F}_q$ in which the addition is defined as the usual addition of polynomials and the multiplication is defined by the rule*

$$(ax^i)(bx^j) = a\theta^i(b)x^{i+j},$$

which is extended to the elements of $\mathbb{F}_q[x,\theta]$ using associativity and distributivity."

The ring $\mathbb{F}_q[x,\theta]$ is a non-commutative ring. An element $g(x) \in \mathbb{F}_q[x,\theta]$ is said to be a right divisor of $f(x) \in \mathbb{F}_q[x,\theta]$ if there exists $q(x) \in \mathbb{F}_q[x,\theta]$ such that $f(x) = q(x)g(x)$. In this case, $f(x)$ is called a left multiple of $g(x)$. A left divisor of $f(x)$ can be defined similarly. We use the symbol $a|b$ to denote that a is a right divisor of b. In the sequel, division always means a right division. The ring $\mathbb{F}_q[x,\theta]$ is a right (left) Euclidean ring. The right (left) division is defined on $\mathbb{F}_q[x,\theta]$ as follows.

Lemma 2.1.2. *[74] "Let $f(x), g(x) \in \mathbb{F}_q[x,\theta]$. Then*

1. *$deg\ (f(x) + g(x)) \leq max\{deg\ f(x), deg\ g(x)\}$*

2. *$deg\ f(x)g(x) = deg\ f(x) + deg\ g(x)$.*

3. *$\mathbb{F}_q[x,\theta]$ has no nonzero zero-divisor.*

4. *The units of $\mathbb{F}_q[x,\theta]$ are the units of $\mathbb{F}_q$."*

Lemma 2.1.3. *[74] "Let $f(x), g(x) \in \mathbb{F}_q[x,\theta]$ be two arbitrary polynomials with $g(x) \neq 0$ and $deg\ \ g(x) < deg\ \ f(x)$. Then there exist $q(x), r(x) \in \mathbb{F}_q[x,\theta]$ such that $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or $deg\ \ r(x) < deg\ \ g(x)$."*

The aforementioned result is the division algorithm with division on the right by $g(x)$. The left division algorithm can be obtained similarly.

2.1.1 Coding with skew polynomial rings

Boucher et al. [26] introduced skew-cyclic codes using skew polynomial rings. Since then a lot of work has been done on codes using skew polynomial rings. We present, in this subsection, some important results about linear, cyclic, constacyclic, quasi-cylic codes in the non-commutative setting of skew polynomial rings.

2.1.1.1 Skew codes over finite fields

Let $\mathbb{F}_q$ denote the finite field and θ an automorphism of $\mathbb{F}_q$.

Definition 2.1.4. *(Skew-cyclic code) "A linear code C of length n over $\mathbb{F}_q$ is said to be a skew-cyclic code if for all $v = (v_0, v_1, \cdots, v_{n-1}) \in C$, the skew-cyclic shift $T_\theta(v) = (\theta(v_{n-1}), \theta(v_0), \theta(v_1), \cdots, \theta(v_{n-2}))$ of c is also in C."*

Definition 2.1.5. *(Central polynomial) "A polynomial $f(x) \in \mathbb{F}_q[x, \theta]$ is said to be a central polynomial if $f(x)r(x) = r(x)f(x)$ for all $r(x) \in \mathbb{F}_q[x, \theta]$."*

The ideal generated by a central polynomial $f(x) \in \mathbb{F}_q[x, \theta]$ is a two sided ideal of $\mathbb{F}_q[x, \theta]$. We use the notation $|\theta|$ for the order of the automorphism θ.

Lemma 2.1.6. *[96] $(x^n - 1) \in \mathbb{F}_q[x, \theta]$ lies in the center $Z(\mathbb{F}_q[x, \theta])$ of $\mathbb{F}_q[x, \theta]$ if and only if $|\theta| \mid n$.*

Lemma 2.1.7. *([26], Lemma 1) "If n is a positive integer such that $|\theta|$ divides n, then the ring $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1 \rangle}$ is a principal left ideal ring in which left ideals are generated by $g(x)$, where $g(x)$ is a right divisor of $x^n - 1$ in $\mathbb{F}_q[x, \theta]$."*

Theorem 2.1.8. *([26], Theorem 1) "Let n be a positive integer such that $|\theta|$ divides n. Then a code C is a θ-cyclic code if and only if C is a left ideal of the ring $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1 \rangle}$."*

In [96], Siap et al. have defined skew-cyclic codes without imposing the restriction that $|\theta| \mid n$. If we remove the restriction that $|\theta| \mid n$, then the ideal $\langle x^n - 1 \rangle$ is only a left ideal of $\mathbb{F}_q[x, \theta]$ and hence $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1 \rangle}$ is not a ring, it is only a left $\mathbb{F}_q[x, \theta]$-module. A skew-cyclic code over $\mathbb{F}_q$ is then only a left submodule of $\frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1 \rangle}$. We have the following result.

Theorem 2.1.9. *([96], Theorem 10) "A code C in $R_n = \frac{\mathbb{F}_q[x,\theta]}{\langle x^n-1\rangle}$ is a skew-cyclic code if and only if C is a left $\mathbb{F}_q[x,\theta]$-submodule of the left $\mathbb{F}_q[x,\theta]$-module R_n."*

Theorem 2.1.10. *([96], Theorem 12) "Let $C = \langle f(x)\rangle$ be a left submodule of R_n. Then $f(x)$ is a right divisor of $x^n - 1$."*

Theorem 2.1.11. *([96], Theorem 13) "Let $C = \langle g(x)\rangle$ be a left submodule of R_n where $g(x)$ is a right divisor of $x^n - 1$ of degree r, and $x^n - 1 = h(x)g(x)$. Then C is a free left $\mathbb{F}_q$-submodule with a basis $B = \{g(x), xg(x), x^2g(x), \cdots, x^{n-r-1}g(x)\}$, and dim $C = n - r$."*

Further, if $|\theta|$ is coprime to n, then skew-cyclic codes over $\mathbb{F}_q$ coincide with cyclic codes.

Theorem 2.1.12. *([96], Theorem 16) "Let C be a skew-cyclic code of length n over $\mathbb{F}_q$ and let θ be an automorphism of $\mathbb{F}_q$ with $|\theta| = m$. If $(m,n) = 1$, then C is a cyclic code of length n."*

Another condition for a skew-cyclic code to coincide with a cyclic code has been given by Boucher et al. [29].

Lemma 2.1.13. *([29], Lemma 4) "Suppose that $f(x) = x^n - 1 \in \mathbb{F}_q[x,\theta]$ generates a two-sided ideal. A θ-cyclic code generated by a right divisor $g(x)$ of $f(x)$ of degree less than n generates a cyclic code if and only if all the coefficients of $g(x)$ are in $\mathbb{F}_q^\theta$, the fixed field of θ in $\mathbb{F}_q$."*

2.1.1.2 Skew codes over finite rings

Skew codes have been studied over finite rings by several researchers. Boucher et al. [27] have studied a class of skew constacyclic codes over Galois rings. This work has been generalized in many ways. Jitman et al. [58] have studied skew constacyclic codes over finite chain rings, and Bhaintwal [16] has studied a class of skew quasi-cyclic codes over Galois rings. Many other rings have been considered to study skew-codes [41, 1, 48].

Let R be a finite commutative ring with identity, and let θ be an automorphism of R. Then, as in the case of fields, the set of polynomials $R[x,\theta]$ forms a skew polynomial ring over R. $R[x,\theta]$ is in general a non-commutative ring and is no more left or right Euclidean ring. Also, $R[x,\theta]$ is not a unique factorization ring. This is shown by the following example.

Example 2.1.14. *Let $R = GR(p^s, m)$ with $p = s = m = 2$, where $GR(p^s, m)$ denotes a Galois ring. Let $\theta : GR(4,2) \to GR(4,2)$ be such that $\theta(a+2b) = a^2 + 2b^2$, where $a, b \in T = \{0, 1, \xi, \xi^2\}$, the Teichmüller set of $GR(4,2)$. Two distinct factorizations of $x^4 - 1$ in $GR(4,2)$ are $(x+1)(x+1)(x+2\xi+1)(x+2\xi+3)$ and $(x^2+2\xi+1)(x^2+2\xi+3)$.*

Jitman et al. [58] have generalized the study of skew-cyclic codes to finite chain rings. In particular, a finite chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}, u^2 = 0$, has been considered and classification of skew constacyclic code over same has been done.

Definition 2.1.15. *(Skew-quasi cyclic code) "Let R be a commutative finite ring with identity. Let θ be an automorphism of R. Let $n = ls$ such that order of θ divides s. A linear code C over R is called a skew quasi-cyclic code of length n and index l if*

$$a = \begin{pmatrix} a_{0,0}, a_{0,1}, \cdots, a_{0,l-1}, a_{1,0}, a_{1,1}, \cdots, a_{1,l-1}, \\ \cdots, a_{s-1,0}, a_{s-1,1}, \cdots, a_{s-1,l-1} \end{pmatrix} \in C$$

implies that

$$T_{\theta,l}(a) = \begin{pmatrix} \theta(a_{s-1,0}), \theta(a_{s-1,1}), \cdots, \theta(a_{s-1,l-1}), \theta(a_{0,0}), \theta(a_{0,1}), \cdots, \theta(a_{0,l-1}), \\ \theta(a_{1,0}), \theta(a_{1,1}), \cdots, \theta(a_{1,l-1}), \cdots, \theta(a_{s-2,0}), \theta(a_{s-2,1}), \cdots, \theta(a_{s-2,l-1}) \end{pmatrix} \in C,$$

and l is the smallest positive integer satisfying this condition."

In particular, if θ is the identity automorphism of R, then C is simply a quasi-cyclic code over R. Further for $l = 1$, C is a skew-cyclic code over R.

In polynomial form, a skew quasi-cyclic code C of length ls and index l over R is a left $\frac{R[x,\theta]}{\langle x^s-1\rangle}$-submodule of $\left[\frac{R[x,\theta]}{\langle x^s-1\rangle}\right]^l$.

In [16], skew quasi-cyclic codes over $GR(q, m)$ have been studied thoroughly. In [1, 41, 48], skew-cyclic codes have been studied over $\mathbb{F}_2+v\mathbb{F}_2$, $\mathbb{F}_p+v\mathbb{F}_p$, and $\mathbb{F}_q+v\mathbb{F}_q$, respectively, in which mainly the results of [26, 27, 58] have been generalized.

Chapter 3

Skew-cyclic Codes over Some Extensions of $\mathbb{F}_p$

3.1 Introduction

A recent development in coding theory is the study on codes over rings and more general structures. The work in this direction attracted more attention especially after a landmark paper of Hammons et al. [50]. Since then, different rings have been considered and their Gray images have been determined to achieve good linear and non-linear codes. In recent years, some new kinds of codes over rings have been proposed [4, 7, 6, 25, 24, 9]. However, most of this work has been done over commutative setting. Recently, there has been an interest on the study of codes over skew polynomial rings, after Boucher et al. [26] introduced skew-cyclic codes. Abualrub et al. [6] have studied $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-linear cyclic codes. These codes can also be seen as a generalization of double cyclic codes [24].

Motivated from the works [6] and [24], we study a new class of skew-cyclic codes over the mixed alphabet $\mathbb{F}_3R$, where $R = \mathbb{F}_3 + v\mathbb{F}_3, v^2 = v$. We call these codes $\mathbb{F}_3R$-skew cyclic codes. We first define a division algorithm on $R[x, \theta]$ to obtain the structure of skew-cyclic codes over R, and then using this we obtain the structure of $\mathbb{F}_3R$-skew cyclic codes. Further, we have also studied a class of skew-cyclic codes over $S = \mathbb{F}_p + v\mathbb{F}_p, v^2 = 1$, where p is a prime.

3.2 Properties of the ring $R = \mathbb{F}_3 + v\mathbb{F}_3$ and $R[x, \theta]$

Throughout the chapter, we denote $R = \mathbb{F}_3 + v\mathbb{F}_3 = \{0, 1, 2, v, 2v, 1+v, 1+2v, 2+v, 2+2v\}, v^2 = v$, where $\mathbb{F}_3 = \{0, 1, 2\}$ is the finite field with 3 elements. R is a semi-local ring with two maximal ideals $\langle v \rangle$ and $\langle v+2 \rangle$. The units of R are $1, 2, 1+v$, and $2+2v$. Moreover $R = \langle v \rangle \oplus \langle v+2 \rangle$.

Define $\theta : R \to R$ by

$$\theta(a + vb) = a + (1 - v)b, \tag{3.1}$$

for all $a + vb \in R$. One can easily check that θ is an automorphism of R. Moreover, the order of θ is 2, since $\theta^2(x) = x$ for all $x \in R$. With this automorphism, the skew polynomial ring $R[x, \theta]$ over R is defined (see Definition 2.1.1).

The center $Z(R[x, \theta])$ of $R[x, \theta])$ is $\mathbb{F}_3[x^2]$. We recall that the ring $R[x, \theta]$ may not be a left or right Euclidean ring, but still the division algorithm can be applied on certain elements of $R[x, \theta]$. There is a version of division on $R[x, \theta]$, given below, that directly follows from Theorem II.11 in [74].

Lemma 3.2.1 (Left division algorithm). *[74] "Let $f(x), g(x) \in R[x, \theta]$ such that the leading coefficient of $g(x)$ is a unit. Then there exist two polynomials $q(x)$ and $r(x)$ in $R[x, \theta]$ such that*

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

where $r(x) = 0$ or $deg\ r(x) < deg\ g(x)$."

The right division algorithm on $R[x, \theta]$ can similarly be defined.

The polynomials in $R[x, \theta]$ do not necessarily factorize uniquely as shown by the following example.

Example 3.2.2. *The factors of degree 2 of $x^4 - 1$ in $R[x, \theta]$ are given by the expression*

$$x^4 - 1 = (ax^2 + bx + c)(dx^2 + ex + f),$$

where the possible values of a, b, c, d, e, f can be any row of the following table:

rows	a	b	c	d	e	f
1	1	0	2	1	0	1
2	1	0	$v+1$	1	0	$2v+2$
3	1	v	$v+1$	1	$2v$	$2v+2$
4	1	$v+2$	$v+1$	1	$2v+1$	$2v+2$
5	1	$2v$	$v+1$	1	v	$2v+2$
6	1	$2v+1$	$v+1$	1	$v+2$	$2v+2$
7	2	0	$v+1$	2	0	$2v+2$
8	2	v	$v+1$	2	$2v$	$2v+2$
9	2	$v+2$	$v+1$	2	$2v+1$	$2v+2$
10	2	$2v$	$v+1$	2	v	$2v+2$
11	2	$2v+1$	$v+1$	2	$v+2$	$2v+2$

The above example shows that there are many right divisors of x^4-1, and hence more skew-cyclic codes of length 4 over R than cyclic codes over R with same length. This indicates that there are more possibilities for getting better codes in the setting of skew polynomial rings.

We define the Gray map on R, $\phi_1 : R \to \mathbb{F}_3^2$, as

$$\phi_1(a+vb) = (b, a+b).$$

Clearly ϕ_1 is a linear map. The Gray weight $wt_G(x)$ of an element $x \in R$ is defined as $wt_G(x) = wt_H(\phi_1(x))$, where wt_H denotes the Hamming weight. Thus the Gray weights of elements of R are as follows:

Element	*Gray weight*
0	0
1	1
2	1
v	2
$2v$	2
$1+v$	2
$1+2v$	1
$2+v$	1
$2+2v$	2

The map ϕ_1 is then extended componentwise to R^n as $\Phi_1 : R^n \to \mathbb{F}_3^{2n}$. The weight of $x = (x_1, x_2, \cdots, x_n) \in R^n$ is $wt_G(x) = \sum_{i=1}^{n} wt_G(x_i)$. Φ_1 is a distance preserving map, since for any $x, y \in R^n$, we have $d_G(x, y) = wt_G(x - y) = wt_H(\Phi_1(x - y)) = wt_H(\Phi_1(x) - \Phi_1(y)) = d_H(\Phi_1(x), \Phi_1(y))$.

3.3 Skew-cyclic codes over R

In this section, some structural properties and generating sets of skew-cyclic codes over R have been discussed.

For arbitrary n, $R_n = \frac{R[x,\theta]}{\langle x^n-1\rangle}$ is a left $R[x, \theta]$-module with multiplication defined as $a(x)(f(x) + \langle x^n - 1\rangle) = a(x)f(x) + \langle x^n - 1\rangle$ for any $a(x) \in R[x, \theta]$. In this case, $\langle x^n - 1\rangle$ denotes the left ideal of $R[x, \theta]$ generated by $x^n - 1$. To associate the vectors of R^n to the polynomials in R_n, we define an R-module isomorphism from R^n to R_n as

$$(c_0, c_1, \cdots, c_{n-1}) \mapsto c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

A skew-cyclic code C over R can similarly be defined as in the case of fields, see Definition 2.1.4. The following result is an immediate generalization of [96, Theorem 10]. The proof is omitted.

Theorem 3.3.1. *[96] "A code C of length n in R_n is a skew-cyclic code if and only if C is a left $R[x,\theta]$-submodule of the left $R[x,\theta]$-module R_n."*

3.3.1 Generator polynomials of skew-cyclic codes over R

Now we discuss the form of generator polynomials of a skew-cyclic code over R which is necessary for constructing the generator polynomials of $\mathbb{F}_3R$-skew cyclic codes. We consider different cases that a skew-cyclic code over R may have, and determine the generator polynomials for all these cases.

Let C be a skew-cyclic code over R. We have the following cases:

1. A code C has a minimal degree polynomial having its leading coefficient a unit.

2. There is no polynomial in C which has its leading coefficient a unit.

3. There is a polynomial in C whose leading coefficient is a unit but it is not a minimal degree polynomial in C.

In the first case, let there is a polynomial $g(x)$ of minimal degree in C having the leading coefficient a unit. Then by Lemma 3.2.1 we have, for any $c(x) \in C$ there exist $q(x), r(x) \in R[x,\theta]$, where deg $r(x) <$ deg $g(x)$ or $r(x) = 0$, such that

$$c(x) = q(x)g(x) + r(x).$$

This gives $r(x) \in C$ and consequently $r(x) = 0$ as $g(x)$ is a minimal degree polynomial in C. Therefore C is generated by $g(x)$.

Example 3.3.2. *Let C be the skew-cyclic code of length 4 over R with generator matrix*

$$\begin{bmatrix} 1+v & 0 & 1 & 0 \\ 0 & 2+2v & 0 & 1 \end{bmatrix}.$$

Then C contains an element $g(x) = x^2+1+v$ of minimal degree whose leading coefficient is a unit, and so $C = \langle g(x) \rangle$. Moreover, we note that there is no polynomial of degree less than 2 in C.

Next we consider the case when there is no polynomial in C having its leading coefficient a unit. We require following lemmas to address this case.

Lemma 3.3.3. *Let $g(x)$ be a minimal degree polynomial in $R[x,\theta]$ having its leading coefficient a non-unit. Then $g(x)$ will be of the type $vg_1(x)$ or $(v+2)g_2(x)$ for some $g_1(x), g_2(x) \in \mathbb{F}_3[x]$.*

Proof: Let $g(x) = g_0 + g_1x + \cdots + g_rx^r$, where g_r is a non-unit. The non-units of R are of the type av or $a(v+2)$, $a = 1, 2$. Suppose $g_r = av$, $a = 1$ or 2. Then $(v+2)g(x)$ is a polynomial of degree less than that of $g(x)$. But as $g(x)$ is a minimal degree polynomial, so $(v+2)g(x) = 0$, i.e., $(v+2)g_i = 0$ for all $i = 0, 1, 2 \cdots, r$. Thus each $g_i = avg_i'$, for $a = 1$ or 2, and so $g(x) = vg_1(x)$, where $g_1(x)$ is a polynomial over $\mathbb{F}_3$. Similarly, when $g(x)$ has the leading coefficient $a(v+2)$ for $a = 1$ or 2, we can prove that $g(x) = (v+2)g_2(x)$ for some $g_2(x) \in \mathbb{F}_3[x]$. ■

Lemma 3.3.4. *Let $f(x), g(x) \in R[x,\theta]$ be two polynomials with their leading coefficients non-units. Then there exist $q(x)$ and $r(x)$ in $R[x,\theta]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$ or $r(x)$ is a polynomial with its leading coefficient a unit and having degree at most deg $f(x)$.

Proof: Let $f(x) = f_0+f_1x+\cdots+f_tx^t$, $f_t \neq 0$ and $g(x) = g_0+g_1x+\cdots+g_sx^s$, $g_s \neq 0$, and $s \leq t$. Since g_s is a non-unit, $g_s = av$ or $a(v+2)$, $a = 1$ or 2.
Suppose $g_s = av$. We have two cases: $t-s$ is odd or even. Suppose $t-s$ is odd. Then $\theta^{t-s}(g_s) = \theta(g_s)$, as the order of θ is 2. Define a polynomial $l_1(x) = f(x) - ax^{t-s}g(x)$. The leading coefficient of $l(x)$ is $f_t - a\theta^{t-s}(g_s)$= $f_t - a(a(1+2v))$=$f_t - a^2(1+2v)$=$f_t-(1+2v)$, as $a^2 = 1$. The possible values of f_t are $v, 2v, v+2, 2v+1$, and $f_t - (1+2v)$ is either a unit or 0 for each value of f_t except for $f_t = v+2$. If $f_t = v+2$, define $l_2(x) = f(x) - (v+2)ax^{t-s}g(x)$. The leading coefficient of $l_2(x)$ is 0. So by combining both the cases, we see that we have a polynomial $l(x) = l_1(x)$ or $l_2(x)$, whose leading

coefficient is either a unit or 0. If the leading coefficient of $l(x)$ is 0, then $l(x)$ has degree less than that of $f(x)$. Therefore in either case, we have

$$f(x) = q(x)g(x) + l(x), \tag{3.2}$$

where

$$q(x) = \begin{cases} ax^{t-s} & \text{for } \ f_t \neq v+2 \\ (v+2)ax^{t-s} & \text{for } \ f_t = v+2. \end{cases}$$

Now if the leading coefficient of $l(x)$ is a unit, we are done. Suppose deg $l(x) <$ deg $f(x)$. To prove the result we apply mathematical induction on the degree of $f(x)$. Consider $t = 0$. Then $f(x) = f_0$ and $g(x) = g_0$, and hence $f(x) = q_1(x)g(x) + r_1(x)$, where $r_1(x)$ is given by the following table, where the elements in the first row denote the possible values of f, the elements in the first column denote the possible values of g and the other elements in the table denote the corresponding value of $r_1(x)$.

$g \setminus f$	v	$2v$	$1+2v$	$v+2$
v	0	0	1	2
$2v$	0	0	1	2
$1+2v$	1	2	0	0
$v+2$	1	2	0	0

It is clear from the table that either $r = 0$ or r is a unit. Therefore the result is true for $t = 0$. We assume that the result is true for every polynomial of degree $k < t =$ deg $f(x)$ in $R[x, \theta]$. Since deg $l(x) < t$, by induction hypothesis, $l(x) = Q(x)g(x) + S(x)$ for some $Q(x), S(x)$ in $R[x, \theta]$ such that $S(x) = 0$ or deg $S(x) <$ deg $g(x)$ or $S(x)$ is polynomial of degree at most deg $l(x)$, having its leading coefficient a unit. By (6.3.12), we have $f(x) = q(x)g(x) + Q(x)g(x) + S(x) = (q(x) + Q(x))g(x) + S(x)$, where $S(x)$ has the same conditions as above. Similarly, we can prove the result if $t - s$ is even. Further, the result can be proved similarly when $g_s = a(v + 2)$. ■

Now we prove the following two theorems using Lemma 3.3.3 and Lemma 3.3.4.

Theorem 3.3.5. *Let C be a skew-cyclic code over R such that there does not exist any polynomial in C whose leading coefficient is a unit. Let $g(x)$ be a minimal degree* *polynomial in C. Then $C = \langle g(x) \rangle$. Moreover $g(x) = vg_1(x)$ or $g(x) = (v+2)g_2(x)$ for some $g_1(x), g_2(x) \in \mathbb{F}_3[x]$.*

Proof: Let $c(x) \in C$ be a codeword. Let $g(x)$ be a non-zero minimal degree polynomial in C. Since $c(x)$ and $g(x)$ are two polynomials with leading coefficients non-units, by Lemma 3.3.4, there exist $q'(x)$ and $r'(x)$ in $R[x, \theta]$ such that $c(x) = q'(x)g(x) + r'(x)$, where $r'(x) = 0$ or deg $r'(x) <$ deg $g(x)$ or $r'(x)$ is a polynomial of degree at most deg $c(x)$, having its leading coefficient a unit. But the last two cases do not arise, as $g(x)$ is a minimal degree polynomial and C has no polynomial with its leading coefficient a unit. Therefore $C = \langle g(x) \rangle$. Rest follows from Lemma 3.3.3. ■

Example 3.3.6. *Let C be the skew-cyclic code generated by the matrix*

$$\begin{bmatrix} 2v & 0 & v & 0 \\ 0 & v+2 & 0 & 1+2v \end{bmatrix}.$$

Then the corresponding code is given by

$$C = \left\{ \begin{array}{ccc} (0,0,0,0), & (v,0,2v,0), & (v,v+2,2v,2v+1) \\ (2v,2v+1,v,v+2), & (2v,v+2,v,2v+1), & (v,2v+1,2v,v+2) \\ (0,2v+1,0,v+2), & (2v,0,v,0), & (0,v+2,0,2v+1) \end{array} \right\}.$$

It can easily be verified that C is a skew-cyclic code which is not free and it does not contain any codeword with corresponding polynomial having leading coefficient a unit. Moreover C is generated by a minimal degree polynomial $g(x) = vx^2 + 2v$.

Corollary 3.3.6.1. *If $g(x) = vg_1(x)$ i.e., $C = \langle vg_1(x) \rangle$, then $g_1(x) | x^n - 1$.*

Proof: Since $g_1(x)$ is a polynomial over $\mathbb{F}_3$, and $\mathbb{F}_3[x, \theta]$ is a left Euclidean ring, we have

$$x^n - 1 = q(x)g_1(x) + r(x)$$

for some $q(x), r(x)$ in $\mathbb{F}_3[x, \theta]$ such that $r(x) = 0$ or deg $r(x) <$ deg $g_1(x)$.

Suppose $r(x) \neq 0$. Let $q_1(x), q_2(x)$ be two polynomials such that $q_1(x)$ contains precisely the even power terms of $q(x)$, and $q_2(x)$ contains the odd power term of

$q(x)$. Then $x^n - 1 = (q_1(x) + q_2(x))g_1(x) + r(x)$, and so

$$\begin{aligned} v(x^n - 1) &= v(q_1(x) + q_2(x))g_1(x) + vr(x) \\ &= vq_1(x)g_1(x) + vq_2(x)g_1(x) + vr(x) \\ &= q_1(x)(1 + 2v)g_1(x) + q_2(x)vg_1(x) + vr(x) \\ &= (q_2(x) + 2q_1(x))vg_1(x) + \underbrace{q_1(x)g_1(x) + vr(x)} \end{aligned}$$

Since deg $r(x) <$ deg $g_1(x)$, and $q_1(x), g_1(x)$ are polynomials over $\mathbb{F}_3$, so $q_1(x)g_1(x) + vr(x)$ is a polynomial with its leading coefficient a unit, which is a contradiction. Therefore $r(x) = 0$ and so $g_1(x)|x^n - 1$. ■

For example, in Example 2, we have $g(x) = ag'(x)$ where $a = v$ and $g'(x) = (x^2 + 2)$, and $(x^2 + 2)|(x^4 - 1)$.

Now we consider the case when there exist a polynomial in C with leading coefficient a unit but is not of minimal degree in C.

Theorem 3.3.7. *Let C be a skew-cyclic code over R having a polynomial with leading coefficient a unit and no minimal degree polynomial in C has its leading coefficient a unit. Let $g(x)$ be a minimal degree polynomial in C and $h(x)$ a minimal degree polynomial in C among the polynomials with their leading coefficient a unit . Then $C = \langle g(x), h(x)\rangle$.*

Proof: Let $c(x) \in C$ be any codeword. Then

$$c(x) = q(x)h(x) + r(x) \tag{3.3}$$

for some $q(x),\ r(x) \in R[x, \theta]$, where $r(x) = 0$ or deg $r(x) <$ deg $h(x)$. If $r(x) = 0$, then $C \subseteq \langle g(x), h(x)\rangle$. Suppose $r(x) \neq 0$. Then $r(x)$ must have its leading coefficient a non-unit, as $h(x)$ is a minimal degree polynomial with its leading coefficient a unit. Therefore by Lemma 3.3.4, we have

$$r(x) = q_1(x)g(x) + r_1(x) \tag{3.4}$$

for some $q_1(x), r_1(x) \in R[x, \theta]$, where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$ or $r_1(x)$ has its leading coefficient a unit and degree at most deg $r(x)$. If $r_1(x) = 0$, then

$C \subseteq \langle g(x), h(x)\rangle$ (by 3.3, 3.4). Other two cases do not arise, because $g(x)$ is a minimal degree polynomial in C, and $r_1(x)$ cannot have its leading coefficient a unit as deg $r_1(x) <$ deg $r(x) <$ deg $h(x)$ and $h(x)$ is a minimal degree polynomial with leading coefficient a unit. It is obvious that $\langle g(x), h(x)\rangle \subseteq C$. Hence $C = \langle g(x), h(x)\rangle$. ■

Example 3.3.8. *Let C be a skew-cyclic code of length 4 over R with a spanning set*

$$S = \left\{ \begin{array}{ccc} (v, v, 0, 0), & (0, 1+2v, 1+2v, 0), & (0, 0, v, v) \\ (1+2v, 0, 0, 1+2v), & (1, 1, 1, 1) & \end{array} \right\}.$$

Then the corresponding code is given by

$$\left\{ \begin{array}{ccc}
(0,0,v,v) & (v+2,v+2,2,2) & (2v,2,v+2,0) \\
(2v+2,1,1,2v+2) & (2,2,2v+2,2v+2) & (1,1,v+1,v+1) \\
(2v+1,0,0,2v+1) & (1,v,0,2v+1) & (0,v+2,v+2,0) \\
(0,0,2v,2v) & (v,1,v+1,2v) & (2v,2,2v+2,v) \\
(v+1,v+1,2v+1,2v+1) & (2v,v+1,2v+1,0) & (v+1,2v,2v,v+1) \\
(v+2,0,0,v+2) & (v+2,2v+1,2v+1,v+2) & (2v+1,0,v,1) \\
(v,2v+2,v+2,0) & (2,v+1,2v+1,v+2) & (1,2v+2,v+2,2v+1) \\
(2,2,v+2,v+2) & (1,2v+2,2,v+1) & (v,2v+2,2,2v) \\
(1,1,2v+1,2v+1) & (v+2,v+2,2v+2,2v+2) & (v+2,0,2v,2) \\
(v+1,2v,v,1) & (2v,2v,v,v) & (2,2v,2v,2) \\
(2v+2,1,v+1,2) & (2v+1,2v+1,1,1) & (12v+2,2v+2,1) \\
(2v,v+1,v+1,2v) & (2,2v,v,2v+2) & (2v,2v,2v,2v) \\
(2v,2v,0,0) & (v+1,2v,0,2v+1) & (v,2v+2,2v+2,v) \\
(0,0,0,0) & (2,v+1,v+1,2) & (2,2v,0,v+2) \\
(2v+1,v+2,v+2,2v+1) & (2,2,2,2) & (2v+2,v,v,2v+2) \\
(v,1,1,v) & (v+2,v+2,v+2,v+2) & (2v+1,v+2,2,v+1) \\
(2v+2,1,2v+1,v+2) & (2v+1,2v+1,v+1,v+1) & (0,v+2,2,2v) \\
(2v+2,2v+2,2,2) & (v+2,0,v,2v+2) & (0,2v+1,v+1,2v) \\
(0,v+2,2v+2,v) & (2v,v+1,1,v) & (2v+2,2v+2,2v+2,2v+2) \\
(2v+1,v+2,2v+2,1) & (2v+1,2v+1,2v+1,2v+1) & (v+2,2v+1,1,2v+2) \\
(2,v+1,1,2v+2) & (v,v,v,v) & (v+1,2,v+2,2v+1) \\
(2v+1,0,2v,v+1) & (v+1,2,2,v+1) & \boldsymbol{(v,\ v,\ 0,\ 0)} \\
(1,v,2v,v+1) & (v,v,2v,2v) & (v+1,v+1,1,1) \\
(2v+2,2v+2,v+2,v+2) & (2v+2,v,2v,2) & \boldsymbol{(1,\ 1,\ 1,\ 1)} \\
(v+1,2,2v+2,1) & (v+1,v+1,v+1,v+1) & (v,1,2v+1,0) \\
(1,v,v,1) & (2v,2,2,2v) & (2v+2,v,0,v+2) \\
(0,2v+1,2v+1,0) & (0,2v+1,1,v) & (v+2,2v+1,v+1,2)
\end{array} \right\}.$$

We can easily check that there is a codeword with associated minimal degree polynomial $g(x) = v+vx$ whose leading coefficient is a non-unit. Also $h(x) = 1+x+x^2+x^3$

is a minimal degree polynomial in C with its leading coefficient a unit. The corresponding codewords are highlighted. Therefore C can be written as $C = \langle g(x), h(x) \rangle$.

3.4 $\mathbb{F}_3R$-Skew cyclic codes

In this section, we determine the structure of $\mathbb{F}_3R$-skew cyclic codes.

A code C of length n is said to be an $\mathbb{F}_3R$*-code* if the coordinates of the codewords are partitioned in two blocks of lengths α and β such that the set of the first blocks are element of $\mathbb{F}_3^\alpha$ and the set of the second blocks are elements of R^β.

For convenience, we denote $\mathbb{F}_3^\alpha \times R^\beta$ by $\mathbb{F}_3^\alpha R^\beta$. Let $\pi : R \rightarrow \mathbb{F}_3$ be the projection map defined by $\pi(r + vq) = r$. It is clear that π is a ring homomorphism. For any $d \in R$ and $v = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) \in \mathbb{F}_3^\alpha R^\beta$, we define

$$dv = (\pi(d)a_0, \pi(d)a_1, \cdots, \pi(d)a_{\alpha-1}, db_0, db_1, \cdots, db_{\beta-1}). \tag{3.5}$$

With this multiplication, $\mathbb{F}_3^\alpha R^\beta$ is an R-module.

Let Θ be an automorphism of R.

Definition 3.4.1. *A subset C of $\mathbb{F}_3^\alpha R^\beta$ is called an* $\mathbb{F}_3R$-skew cyclic code *if*

1. *C is an R-submodule of $\mathbb{F}_3^\alpha R^\beta$ and*

2. *For any $v = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) \in C$, its $\alpha\beta$-skew cyclic shift, which is $(\Theta(a_{\alpha-1}), \Theta(a_0), \Theta(a_1), \Theta(a_{\alpha-2}), \Theta(b_{\beta-1}), \Theta(b_0), \Theta(b_1), \cdots, \Theta(b_{\beta-2}))$, is also in C.*

In particular, if Θ is the identity map, then C is called an $\mathbb{F}_3R$-cyclic code.

For the rest of the chapter, we consider the $\mathbb{F}_3R$-skew cyclic codes with respect to automorphism θ, defined in section 3.2.

Remark 3.4.1.1. *$\theta(a_i) = a_i$ for $0 \leq i \leq \alpha - 1$, as $a_i \in \mathbb{F}_3$ (the fixed field of θ).*

In polynomial representation, an element $c = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1})$ in C can be identified with

$$c(x) = (a(x), b(x)),$$

where $a(x) = a_0+a_1x+\cdots+a_{\alpha-1}x^{\alpha-1} \in \frac{\mathbb{F}_3[x]}{\langle x^\alpha-1\rangle}$ and $b(x) = b_0+b_1x+\cdots+b_{\beta-1}x^{\beta-1} \in \frac{R[x,\theta]}{\langle x^\beta-1\rangle}$. This identification gives a one-to-one correspondence between $\mathbb{F}_3^\alpha R^\beta$ and $R_{\alpha,\beta} = \frac{\mathbb{F}_3[x]}{\langle x^\alpha-1\rangle} \times \frac{R[x,\theta]}{\langle x^\beta-1\rangle}$. For convenience we denote $(a(x), b(x))$ by $(a(x) \mid b(x))$. We define the multiplication of any $r(x) \in R[x,\theta]$ and $(g_1(x) \mid g_2(x)) \in R_{\alpha,\beta}$ as

$$r(x)(g_1(x) \mid g_2(x)) = (\pi(r(x))g_1(x) \mid r(x)g_2(x)),$$

where $\pi(r(x))g_1(x)$ is the ordinary multiplication of polynomials over $\mathbb{F}_3$ and $r(x)g_2(x)$ is the multiplication of polynomials in $R[x,\theta]$. With this multiplication, $R_{\alpha,\beta}$ is a left $R[x,\theta]$-module. It can easily be seen that if $c(x) = (a(x) \mid b(x))$ represents the codeword c, then $xc(x)$ represents the $\alpha\beta$-skew cyclic shift of c.

Theorem 3.4.2. *A code C is an $\mathbb{F}_3R$-skew cyclic code if and only if C is a left $R[x,\theta]$-submodule of the left module $\mathbb{F}_3[x]/\langle x^\alpha - 1\rangle \times R[x,\theta]/\langle x^\beta - 1\rangle$.*

Proof: Let C be an $\mathbb{F}_3R$-skew cyclic code. Let $c \in C$, and let the associated polynomial of c be $c(x) = (a_1(x) \mid a_2(x))$. As $xc(x)$ is an $\alpha\beta$-skew cyclic shift of c, so $xc(x) \in C$. By linearity of C, $r(x)c(x) \in C$ for any $r(x) \in R[x,\theta]$. So C is a left $R[x,\theta]$-submodule of $R_{\alpha,\beta}$. Converse is straightforward. ■

Theorem 3.4.3. *An $\mathbb{F}_3R$-skew cyclic code is equivalent to an $\mathbb{F}_3R$-cyclic code if α, β both are odd integers.*

Proof: Let C be an $\mathbb{F}_3R$-skew cyclic code. Let $\gamma = lcm(\alpha,\beta)$. Then γ is odd, and so $gcd(\gamma,2) = 1$. Therefore there exist two integers a, b such that $\gamma a + 2b = 1$ and so $2b = 1 - \gamma a = 1 + \gamma l$ for some $l > 0$, where $l = -a \pmod{\gamma}$. Let $c(x) = (a(x) \mid b(x)) \in C$, where $a(x) = \sum_{i=0}^{\alpha-1} a_ix^i$ and $b(x) = \sum_{i=0}^{\beta-1} b_ix^i$.

Then

$$\begin{aligned}
x^{2b}c(x) &= x^{2b}\left(\sum_{i=0}^{\alpha-1} a_i x^i \mid \sum_{i=0}^{\beta-1} b_i x^i\right)\\
&= \left(\sum_{i=0}^{\alpha-1} a_i x^{i+2b} \mid \sum_{i=0}^{\beta-1} \theta^{2b}(b_i) x^{i+2b}\right)\\
&= \left(\sum_{i=0}^{\alpha-1} a_i x^{i+1+\gamma l} \mid \sum_{i=0}^{\beta-1} \theta^{2b}(b_i) x^{i+1+\gamma l}\right)\\
&= \left(\sum_{i=0}^{\alpha-2} a_i x^{i+1+\gamma l} + a_{\alpha-1}x^{\alpha+\gamma l} \mid \sum_{i=0}^{\beta-2} a_i x^{i+1+\gamma l} + a_{\beta-1}x^{\beta+\gamma l}\right), \quad (\text{as } \theta^2(x) = x \ \forall \ x \in R)\\
&= \left(\sum_{i=0}^{\alpha-2} a_i x^{i+1} + a_{\alpha-1} \mid \sum_{i=0}^{\beta-2} a_i x^{i+1} + a_{\beta-1}\right), \text{ since } x^\alpha = x^\beta = x^\gamma = 1.
\end{aligned}$$

Thus $x^{2b}c(x)$ is just an $\alpha\beta$-cyclic shift of $c(x)$. So C is an $\mathbb{F}_3R$-cyclic code. Hence the result. ■

Now we discuss the generator polynomials of $\mathbb{F}_3R$-skew cyclic codes. Recall that an $\mathbb{F}_3R$-skew cyclic is a left $R[x,\theta]$-submodule of $R_{\alpha,\beta}$. We define two projection maps π_α and π_β on $R_{\alpha,\beta}$ such that for any $v(x) = (a(x) \mid b(x)) \in R_{\alpha,\beta}$,

$$\pi_\alpha(v(x)) = a(x) \text{ and } \pi_\beta(v(x)) = b(x).$$

Denote the restrictions of π_α, π_β to a code C also by π_α, π_β.

Lemma 3.4.4. *Let C be an $\mathbb{F}_3R$-skew cyclic code of length n. Then $\pi_\alpha(C) = C_\alpha$ is a cyclic code of length α over $\mathbb{F}_3$ and $\pi_\beta(C) = C_\beta$ is a skew-cyclic code of length β over R.*

Proof: Since C is a submodule of $R_{\alpha.\beta}$, it is clear that $\pi_\alpha(C)$ is an ideal of $\mathbb{F}_3[x]/\langle x^\alpha - 1\rangle$ and $\pi_\beta(C)$ is an $R[x,\theta]$-submodule of $R[x,\theta]/\langle x^\beta - 1\rangle$. The result follows. ■

Theorem 3.4.5. *Let C be an $\mathbb{F}_3R$-skew cyclic code of length $n = \alpha + \beta$. Then we have the following cases:*

1. *If C_β contains a minimal degree polynomial whose leading coefficient is a unit, then $C = \langle (g_1(x) \mid 0), (l(x) \mid g_2(x))\rangle$, where $g_1(x)$ is a generator polynomial of C_α and $g_2(x)$ is a generator polynomial of C_β, and $g_1(x)|x^\alpha - 1, g_2(x)|x^\beta - 1$.*

2. *If C_β has no polynomial whose leading coefficient is a unit, then $C = \langle(g_1(x) \mid 0), (l(x) \mid g_2(x))\rangle$, where $g_1(x)$ is a generator polynomial of C_α and $g_2(x)$ is a generator polynomial of C_β, and $g_2(x) = vg_2'(x)$ or $g_2(x) = (v+2)g_2'(x)$ for some $g_2'(x) \in \mathbb{F}_3[x]$.*

3. *If C_β does not contain any minimal degree polynomial whose leading coefficient is a unit, and if $g_2(x)$ is a minimal degree polynomial in C_β, and $h_2(x)$ is a minimal degree polynomial in C_β among the polynomials having leading coefficient a unit, then $C = \langle(g_1(x) \mid 0), (l_1(x) \mid g_2(x)), (l_2(x) \mid h_2(x))\rangle$, where $g_1(x)$ is a generator polynomial of C_α, and $l_1(x), l_2(x)$ are some polynomials in $\frac{\mathbb{F}_3[x]}{\langle x^\alpha - 1\rangle}$.*

Proof:

1. Let C be an $\mathbb{F}_3R$-skew cyclic code of length n. Then $\pi_\alpha(C)$ is a cyclic code over $\mathbb{F}_3$ and so an ideal of $\frac{\mathbb{F}_3[x]}{\langle x^\alpha - 1\rangle}$. Define $C' = \{(a(x) \mid b(x)) \in C \ : \ b(x) = 0\}$. Then $\pi_\alpha(C') \cong C'$. Clearly $\pi_\alpha(C')$ is also an ideal of $\frac{\mathbb{F}_3[x]}{\langle x^\alpha - 1\rangle}$. Let $\pi_\alpha(C')$ be generated by $g_1(x)$. Then C' is generated by $(g_1(x) \mid 0)$. Also C_β is a skew-cyclic code over R and there is a polynomial $g_2(x)$ of minimal degree in C_β with leading coefficient a unit. Therefore $C_\beta = \langle g_2(x)\rangle$. Since $g_2(x) \in C_\beta$, there is an element $(l(x) \mid g_2(x)) \in C$ for some $l(x) \in \frac{\mathbb{F}_3[x]}{\langle x^\alpha - 1\rangle}$. Now for any $(a(x), b(x)) \in C$, we have $b(x) = \pi_\beta((a(x) \mid b(x))) = \lambda(x)g_2(x)$ for some $\lambda(x) \in \frac{R[x,\theta]}{\langle x^\beta - 1\rangle}$.

   Consider

   $$(a(x) \mid b(x)) - \lambda(x)(l(x) \mid g_2(x)) = (a(x) - \lambda(x)l(x) \mid 0) \tag{3.6}$$

   Since $(a(x) - \lambda(x)l(x) \mid 0) \in C'$, we have $(a(x) - \lambda(x)l(x) \mid 0) = t(x)(g_1(x) \mid 0)$ for some $t(x) \in \frac{\mathbb{F}_3[x]}{\langle x^\alpha - 1\rangle}$. Therefore by (3.6) we have

   $$(a(x) \mid b(x)) = \lambda(x)(l(x) \mid g_2(x)) + t(x)(g_1(x) \mid 0)$$

   and so $C \subseteq \langle(g_1(x) \mid 0), (l(x) \mid g_2(x)\rangle$. Also $\langle(g_1(x) \mid 0), (l(x) \mid g_2(x)\rangle \subseteq C$ is obvious. Therefore $C = \langle(g_1(x) \mid 0), (l(x) \mid g_2(x)\rangle$.

2. This part directly follows from Theorem 3.3.5 and Part 1 above.

3. Let C_β satisfy the given conditions. Then $C_\beta = \langle g_2(x), h_2(x)\rangle$. Using the same notation as in part 1, we see that any $b(x) \in C_\beta$ can be written as $b(x) = \lambda(x)g_2(x)+\gamma(x)h_2(x)$ for some $\lambda(x), \gamma(x) \in \frac{R[x,\theta]}{\langle x^\beta-1\rangle}$. Since $g_2(x), h_2(x) \in C_\beta$, there are two codewords $(l_1(x) \mid g_2(x)), (l_2(x) \mid h_2(x)) \in C$ for some $l_1(x), l_2(x) \in \frac{\mathbb{F}_3[x]}{\langle x^\alpha-1\rangle}$, respectively.

   Now for any $(a(x) \mid b(x)) \in C$, we have

$$\begin{aligned} & (a(x) \mid b(x)) - (\lambda(x)(l_1(x) \mid g_2(x)) + \gamma(x)(l_2(x) \mid h_2(x)) \\ = \ & (a(x) \mid b(x)) - (\lambda(x)l_1(x) + \gamma(x)l_2(x)) \mid \lambda(x)g_2(x) + \gamma(x)h_2(x)) \\ = \ & (a(x) - (\lambda(x)l_1(x) + \gamma(x)l_2(x)) \mid 0). \qquad (3.7) \end{aligned}$$

   Also, $(a(x) - (\lambda(x)l_1(x) + \gamma(x)l_2(x)) \mid 0) \in C'$. So $(a(x) - (\lambda(x)l_1(x) + \gamma(x)l_2(x)) \mid 0) = s(x)(g_1(x) \mid 0)$ for some $s(x) \in \frac{\mathbb{F}_3[x,\theta]}{\langle x^\alpha-1\rangle}$. So by (3.7)

$$(a(x) \mid b(x)) = s(x)(g_1(x) \mid 0) + \lambda(x)(l_1(x) \mid g_2(x)) + \gamma(x)(l_2(x) \mid h_2(x)).$$

   Therefore $C \subseteq \langle (g_1(x) \mid 0), (l_1(x) \mid g_2(x)), (l_2(x) \mid h_2(x)\rangle$. Hence the result.

■

Theorem 3.4.6. *Let C_1 be the repetition code of length α over $\mathbb{F}_3$ and C_2 be the repetition code of length β over R. Let $g_1(x)$ be a monic generator polynomial of C_1 and $g_2(x)$ be a monic generator polynomial of C_2. Then the code C defined as $C = \langle (g_1(x) \mid (1+v)g_2(x))\rangle$ is an $\mathbb{F}_3R$-skew cyclic code of length $n = \alpha+\beta$. Moreover $C = C_1 \times C_2$, and the minimum distance of C is $min(\alpha, \beta)$.*

Proof: We have $g_1(x) = 1+x+x^2+\cdots+x^{\alpha-1}$ and $g_2(x) = 1+x+x^2+\cdots+x^{\beta-1}$. Then clearly $C = \langle (g_1(x) \mid (1+v)g_2(x))\rangle$ is an $\mathbb{F}_3R$-skew cyclic code with minimal spanning set $\{(g_1(x) \mid (1+v)g_2(x)), x(g_1(x) \mid (1+v)g_2(x))\}$, since $x^ig_j(x) = g_j(x)$, $j = 1, 2$, and $x^{2i}(1+v)g_2(x) = (1+v)g_2(x)$ for all integers i as order of θ is 2.

Now to prove $C = C_1 \times C_2$, it is sufficient to show that $C = \langle (g_1(x) \mid 0), (0 \mid g_2(x))\rangle$. Since $C \subseteq \langle (g_1(x) \mid 0), (0 \mid g_2(x))\rangle$ is obvious, we need only to show $\langle (g_1(x) \mid 0), (0 \mid g_2(x))\rangle \subseteq$

C. Let $a = (g_1 \mid (1+v)g_2(x)) \in C$. Then $xa = x(g_1(x) \mid (1+v)g_2(x)) = (xg_1(x) \mid x(1+v)g_2(x)) = (xg_1(x) \mid (2+2v)xg_2(x)) = (g_1(x) \mid (2+2v)g_2(x))$. Therefore $a + xa = (g_1(x) \mid (1+v)g_2(x)) + (g_1(x) \mid (2+2v)g_2(x)) = (2g_1(x) \mid 0)$, and so $2(2g_1(x) \mid 0) = (g_1(x) \mid 0) \in C$. Also, $2a + xa = (0 \mid (1+v)g_2(x)) \in C$, and so $(1+v)(0 \mid (1+v)g_2(x)) = (0 \mid g_2(x)) \in C$. Hence $C = C_1 \times C_2$. Since minimal distance of C_1 is α and that of C_2 is β, the minimal distance of C is min (α, β). ■

Example 3.4.7. *Let $\alpha = \beta = 2$. Then C is an $\mathbb{F}_3R$-skew cyclic code with a generator matrix*

$$\begin{bmatrix} 1 & 1 & v+1 & v+1 \\ 1 & 1 & 2+2v & 2+2v \end{bmatrix},$$

and the corresponding code is given by

$$\left\{ \begin{array}{cccc} (2,2,1,1), & (0,0,v+2,v+2), & (0,0,v+1,v+1), & (2,2,2v+1,2v+1), \\ (1,1,2,2), & (2,2,0,0), & (1,1,2v,2v), & (0,0,2,2), \\ (2,2,v+1,v+1), & (0,0,2v+1,2v+1), & (0,0,2v+2,2v+2) & (1,1,0,0), \\ (0,0,1,1), & (1,1,v,v), & (0,0,0,0), & (2,2,2,2), \\ (2,2,v+2,v+2), & (0,0,2v,2v), & (2,2,v,v), & (1,1,v+1,v+1), \\ (1,1,v+2,v+2), & (2,2,2v,2v), & (0,0,v,v), & (1,1,1,1), \\ (1,1,2v+2,2v+2), & (1,1,2v+1,2v+1), & (2,2,2v+2,2v+2) & \end{array} \right\}.$$

Also,

$$C = \langle (g_1(x) \mid 0), (l(x) \mid (1+v)g_2(x)) \rangle = \langle (l(x) \mid (1+v)g_2(x)) \rangle = \langle (g_1(x) \mid 0), (0 \mid g_2(x)) \rangle,$$

where $g_1(x) = x+1$, $l(x) = x+1$ and $g_2(x) = x+1$.

3.4.1 Duals of $\mathbb{F}_3R$-skew cyclic codes

We define an inner product on $\mathbb{F}_3^{\alpha}R^{\beta}$ as follows:

Let $x = (x_{1,0}, x_{1,1}, \cdots, x_{1,\alpha-1}, x_{2,0}, x_{2,1}, \cdots, x_{2,\beta-1})$, $y = (y_{1,0}, y_{1,1}, \cdots, y_{1,\alpha-1}, y_{2,0}, y_{2,1}, \cdots, y_{2,\beta-1})$ be two words in $\mathbb{F}_3^{\alpha}R^{\beta}$. Then the inner product of x and y is defined by $x \cdot y = \sum_{i=0}^{\alpha-1} x_{1,i}y_{1,i} + \sum_{j=0}^{\beta-1} x_{2,j}y_{2,j}$, where the first sum is determined over $\mathbb{F}_3$ and the second sum is determined over R.

Definition 3.4.8. *Let C be an $\mathbb{F}_3R$-skew cyclic code of length $\alpha+\beta$. Then its dual is defined as*

$$C^{\perp} = \{x \in \mathbb{F}_3^{\alpha}R^{\beta} \ : \ x \cdot c = 0 \textit{ for all } c \in C\}.$$

Lemma 3.4.9. *Let C be an $\mathbb{F}_3R$-skew cyclic code. Then for any $x \in C^{\perp}$ and $y \in C$, we have $\theta(x \cdot^{\alpha,\beta} T_{\theta}^{j}(y)) = T_{\theta}(x) \cdot^{\alpha,\beta} T_{\theta}^{j+1}(y)$.*

Proof: Let $x = (x_{1,0}, x_{1,1}, \cdots, x_{1,\alpha-1}, x_{2,0}, x_{2,1}, \cdots, x_{2,\beta-1}) \in C^{\perp}$ and $y = (y_{1,0}, y_{1,1}, \cdots, y_{1,\alpha-1}, y_{2,0}, y_{2,1}, \cdots, y_{2,\beta-1}) \in C$. Then by definition ${}^{\alpha,\beta}T_{\theta}(x) = (\theta(x_{1,\alpha-1}), \theta(x_{1,0}), \cdots, \theta(x_{1,\alpha-2}), \theta(x_{2,\beta-1}), \theta(x_{2,0}), \cdots, \theta(x_{2,\beta-2}))$ and ${}^{\alpha,\beta}T_{\theta}^{j+1}(y) = (\theta^{j+1}(y_{1,\alpha-j-1}), \theta^{j+1}(y_{1,\alpha-j}), \theta^{j+1}(y_{1,\alpha-j+1}) \cdots, \theta^{j+1}(y_{1,\alpha-j-2}), \theta^{j+1}(y_{2,\beta-j-1}), \theta^{j+1}(y_{2,\beta-j}), \theta^{j+1}(y_{2,\beta-j+1}) \cdots, \theta^{j+1}(y_{2,\beta-j-2}))$, where j is a fixed index, and indices are computed modulo α and β for the two parts. Now

$$\begin{aligned}
{}^{\alpha,\beta}T_{\theta}(x) \cdot^{\alpha,\beta} T_{\theta}^{j+1}(y) &= \theta(x_{1,\alpha-1}) \cdot \theta^{j+1}(y_{1,\alpha-j-1}) + \theta(x_{1,0}) \cdot \theta^{j+1}(y_{1,\alpha-j}) \\
&\quad + \cdots + \theta(x_{1,\alpha-2}) \cdot \theta^{j+1}(y_{1,\alpha-j-2}) + \theta(x_{2,\beta-1}) \cdot \theta^{j+1}(y_{2,\beta-j-1}) \\
&\quad + \cdots + \theta(x_{2,\beta-2}) \cdot \theta(y_{2,\beta-j-2}) \\
&= \theta[x_{1,\alpha-1} \cdot \theta^{j}(y_{1,\alpha-j-1}) + x_{1,0} \cdot \theta^{j}(y_{1,\alpha-j}) + \cdots + x_{1,\alpha-2} \cdot \theta^{j}(y_{1,\alpha-j-2}) \\
&\quad + x_{2,\beta-1} \cdot \theta^{j}(y_{2,\beta-j-1}) + \cdots + x_{2,\beta-2} \cdot \theta^{j}(y_{2,\beta-j-2})] \\
&= \theta[x \cdot^{\alpha,\beta} T_{\theta}^{j}(y)].
\end{aligned}$$

Hence the result. ■

Theorem 3.4.10. *Let C be an $\mathbb{F}_3R$-skew cyclic code of length $n = \alpha+\beta$ such that β is even. Then $C^{\perp}$ is also an $\mathbb{F}_3R$-skew cyclic code of same length.*

Proof: Let $\gamma = lcm(\alpha, \beta)$. Then γ is even (since β is even). Therefore $T_{\theta}^{\gamma}(v) = v$ for all $v \in C$, and so any element $c \in C$ can be written as $c =^{\alpha,\beta} T_{\theta}^{j}(b)$ for some $b \in C$ *and* $0 \leq j \leq \gamma-1$. Now to prove $C^{\perp}$ is $\mathbb{F}_3R$-skew cyclic, we need to show that for any $x \in C^{\perp}$, ${}^{\alpha,\beta}T(x) \in C^{\perp}$, i.e., ${}^{\alpha,\beta}T_{\theta}(x) \cdot^{\alpha,\beta} T_{\theta}^{j}(b) = 0$ for all $b \in C$, $0 \leq j \leq \gamma-1$. By Lemma 3.4.9, we have $0 = \theta(0) = \theta(x \cdot^{\alpha,\beta} T_{\theta}^{j}(b)) =^{\alpha,\beta} T_{\theta}(x) \cdot^{\alpha,\beta} T_{\theta}^{j}(b)$. Hence the result. ■

3.4.2 Gray images

In this section, we define a Gray map on $\mathbb{F}_3R$, and then extend it to $\mathbb{F}_3^{\alpha}R^{\beta}$. We discuss the Gray images of $\mathbb{F}_3R$-skew cyclic codes.

Define a Gray map $\phi : \mathbb{F}_3 R \to \mathbb{F}_3^3$ by

$$\phi(a, b+vc) = (a, \phi_1(b+vc)) = (a, c, b+c),$$

where $b+vc \in R$. ϕ can then be extended componentwise from $\mathbb{F}_3^\alpha R^\beta$ to $\mathbb{F}_3^n$ as

$$\Phi(a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) = (a_0, a_1, \cdots, a_{\alpha-1}, \phi_1(b_0), \phi_1(b_1), \cdots, \phi_1(b_{\beta-1})),$$

for all $(a_0, a_1, \cdots, a_{\alpha-1}) \in \mathbb{F}_3^\alpha$ and $(b_0, b_1, \cdots, b_{\beta-1}) \in R^\beta$, where $n = \alpha + \beta$.

Lemma 3.4.11. *The Gray map Φ is an $\mathbb{F}_3$-linear map which preserves the distance from $\mathbb{F}_3^\alpha R^\beta$ to $\mathbb{F}_3^{\alpha+2\beta}$, i.e., $d_G(x,y) = d_H(\Phi(x), \Phi(y))$ for $x, y \in \mathbb{F}_3^\alpha R^\beta$.*

Proof: Consider

$$\begin{aligned} d_G(x,y) &= w_G(x-y) \\ &= w_H(\Phi(x-y)) \\ &= w_H(\Phi(x) - \Phi(y)) \\ &= d_H(\Phi(x), \Phi(y)). \end{aligned}$$

Hence the result. ■

Now we consider an example of an $\mathbb{F}_3 R$-skew cyclic code and find out its Gray image. The code so obtained is an optimal code over $\mathbb{F}_3$.

Example 3.4.12. *Let C be an $\mathbb{F}_3 R$-skew cyclic code of length 8 with the generator matrix*

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & v+1 & v+1 & v & v \\ 0 & 1 & 1 & 1 & 1+2v & 2v+2 & 2v+2 & 1+2v \\ 1 & 0 & 1 & 1 & v & v & v+1 & v+1 \\ 1 & 1 & 0 & 1 & 2v+2 & 1+2v & 1+2v & 2v+2 \end{bmatrix}.$$

Then the Gray image $\Phi(C)$ of C is an optimal ternary linear code with parameters $[12, 7, 4]$.

3.5 Skew-cyclic codes over $S = \mathbb{F}_p + w\mathbb{F}_p$

In this subsection, we study and explore a class of skew-cyclic codes over $\mathbb{F}_p + w\mathbb{F}_p, w^2 = 1$. In the rest of the chapter, we denote $S = \mathbb{F}_p + w\mathbb{F}_p$ with $w^2 = 1$. S is a semi-local ring with two maximal ideals namely $\langle 1 + w\rangle$ and $\langle 1 - w\rangle$.

Theorem 3.5.1. *An element $a + wb \in S$ is a non-unit if and only if $a = \pm b$.*

Proof: Suppose $a = \pm b$. Then $a + wb = a(1 \pm w)$. Since $a(1 \pm w)(1 \mp w) = 0$, it follows that $a + wb$ is a non-unit. Conversely, suppose $a + wb$ is a non-unit. Clearly $a \neq 0$ and $b \neq 0$, for otherwise, $a + wb$ will be a unit. Since S is a finite ring, $a + wb$ is a zero divisor. So there exists a non-zero element $c + wd \in S$ such that $(a + wb)(c + wd) = 0$. From this we get $ac + bd = 0$ and $bc + ad = 0$. These relations give us $a^2 = b^2$, noting that $c \neq 0$ and $d \neq 0$. Hence $a = \pm b$. ■

Corollary 3.5.1.1. *An element of S is a non-unit if and only if it is of the form $a(1 \pm w)$ for some $a \in \mathbb{F}_p$.*

We define a Gray map $\phi' : S \to \mathbb{F}_p$ such that

$$\phi'(a + wb) = (b, a + b).$$

ϕ' can be extended componentwise to $\Phi' : S^n \to {\mathbb{F}_p}^{2n}$. Φ' is a weight preserving map, i.e., $w_L(x) = w_H(\Phi'(x))$, where w_L denotes the Lee weight of x. In other words, for any $0 \neq x = (a + wb) \in S$,

$$w_L(x) = \begin{cases} 1, & \text{if } \ b = 0 \text{ or } a + b = 0 \ (\text{mod } p) \\ 2, & \text{otherwise} \end{cases}.$$

Also, $w_L(0) = 0$.

For instance, if $p = 3$, then the Lee weights of elements of $\mathbb{F}_3 + w\mathbb{F}_3$ are as given below:

x	0	1	2	w	$2w$	$1+w$	$1{+}2w$	$2+w$	$2{+}2w$
$w_L(x)$	0	1	1	2	2	2	1	1	2

3.5.1 Properties of $S[x,\sigma]$

We define a map $\sigma : S \to S$ such that

$$\sigma(a+wb) = a - wb,$$

for all $a + wb \in S$. It is easy to check that σ is an automorphism of S. In particular for $p = 2$, σ is the identity automorphism of S.

As discussed in Section 3.2, $S[x,\sigma]$ forms a non-commutative skew polynomial ring. Moreover, the left/right division can be defined on some elements of $S[x,\sigma]$ similarly as for $R[x,\theta]$. This is stated as follows.

Lemma 3.5.2 (Right division algorithm). *Let $f(x), g(x) \in S[x,\sigma]$ such that $g(x)$ has its leading coefficient a unit. Then*

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

for some $q(x), r(x) \in S[x,\sigma]$, where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.

We note that $S[x,\sigma]$ is not a unique factorization ring, which can be seen from the following example.

Example 3.5.3. *Let $p = 5$. Then $x^2 - 1$ can be factorized in $S[x,\sigma]$ in following different ways.*

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

Therefore polynomials in $S[x,\sigma]$ possess more factors than in $S[x]$.

Lemma 3.5.4. *Let S be a left-submodule of left $S[x,\sigma]$-module $\frac{S[x,\sigma]}{\langle x^n - 1\rangle}$. Suppose $f(x)$ is a minimal degree polynomial in S such that its leading coefficient is a non-unit. Then $f(x)$ can always be written in the form $f(x) = (1+w)f'(x)$ or $f(x) = (1-w)f''(x)$, where $f'(x), f''(x)$ are polynomials in $\mathbb{F}_p[x]$.*

Proof: Let $f(x) = f_0 + f_1x + \cdots f_rx^r$ such that f_r is a non-unit. Then $f_r = a(1+w)$ or $f_r = b(1-w)$ for some $a, b \in \mathbb{F}_p^*$. Let $f_r = a(1+w)$. Then $((p-1)w+1)f(x)$ is a polynomial in S of degree less than that of $f(x)$. But $f(x)$ is a minimal degree polynomial in S, so $((p-1)w+1)f(x) = 0$. Therefore $((p-1)w+1)f_i = 0$ for all $i = 0, 1, \cdots, r$. Thus $f_i = b_i(1+w)$ for some $b_i \in \mathbb{F}_p$. Hence $f(x) = (1+w)f'(x)$, where $f'(x) \in \mathbb{F}_p[x]$. Similarly, if $f_r = b(1-w)$, we have $f(x) = (1-w)f''(x)$. ■

Theorem 3.5.5. *Let S be a left-submodule of left $S[x,\sigma]$-module $\frac{S[x,\sigma]}{\langle x^n-1\rangle}$. Suppose $f(x), g(x)$ are polynomials in S such that the leading coefficients of both the polynomials are non-units. Then we have*

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

such that $r(x) = 0$ or deg $r(x) <$ deg $g(x)$ or $r(x)$ is a polynomial with its leading coefficient a unit and deg $r(x) \leq$ deg $f(x)$.

Proof: Let $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_rx^r$ and $g(x) = g_0 + g_1x + g_2x^2 + \cdots g_sx^s$. Without loss of generality, we may assume $s \leq r$. Since g_s is a non-unit, $g_s = a(1+w)$ or $g_s = b(1-w)$ for some $a, b \in \mathbb{F}_p^*$. Let $g_s = a(1+w)$. Also f_r is of the form $f_r = c(1+w)$ or $f_r = d(1-w)$ for some $c, d \in \mathbb{F}_p^*$. If $f_r = c(1+w)$, consider the polynomial

$$l(x) = \begin{cases} f(x) - ab^{-1}x^{r-s}g(x), & \text{if } r-s \text{ is even} \\ f(x) + ab^{-1}x^{r-s}g(x), & \text{if } r-s \text{ is odd.} \end{cases}$$

$$\left(\begin{array}{c}\text{Similarly, if } f_r = d(1-w), \text{ we can choose } l(x) \text{ as follows:} \\ l(x) = \begin{cases} f(x) + ab^{-1}x^{r-s}g(x), & \text{if } r-s \text{ is even} \\ f(x) - ab^{-1}x^{r-s}g(x), & \text{if } r-s \text{ is odd.} \end{cases}\end{array}\right)$$

We discuss only the case when $f_r = c(1+w)$. The other case can similarly be proved.

From above, we can write $f(x)$ as

$$f(x) = q(x)g(x) + l(x) \tag{3.8}$$

for a suitable choice of $q(x)$ according to the values of $r-s$. Then $l(x)$ is either a polynomial with degree less than that of $f(x)$ or the leading coefficient of $l(x)$ is a unit. Now if the leading coefficient of $l(x)$ is a unit, then we have

$$f(x) = \begin{cases} ab^{-1}x^{r-s}g(x) + l(x), & \text{if } r-s \text{ is even} \\ -ab^{-1}x^{r-s}g(x) + l(x) & \text{if } r-s \text{ is odd,} \end{cases}$$

and so we are done. Otherwise we apply induction on the degree of $f(x)$. For $r = 0$, we have $s = 0$, and so

$$f_0 = q_0g_0 + r_0 \ , \text{ where } r_0 = 0 \text{ and } q_0 = ca^{-1}.$$

(If $f_r = d(1-w)$, then $r_0 = 2d$ and $q_0 = -da^{-1}$.)
Therefore the result is true for $r = 0$. We assume that the result is true for all polynomials of degree less than r. Since $l(x)$ has degree less than r, $l(x) = Q(x)g(x)+R(x)$ such that $R(x) = 0$ or deg $R(x)$ <deg $g(x)$ or $R(x)$ has leading coefficient a unit and degree at most deg $l(x)$. Now by (3.8), we have

$$f(x) = (q(x) + Q(x))g(x) + R(x).$$

The result follows from this. Similarly, we can prove the result if $g_s = b(1-w)$ for some $b \in \mathbb{F}_p^*$. ■

Next we determine the structure of a skew-cyclic codes over S.

Lemma 3.5.6. *[96] The set $S_n = \frac{S[x,\sigma]}{\langle x^n-1\rangle}$ forms a left $S[x,\sigma]$-module under the left multiplication defined by*

$$r(x)(f(x) + \langle x^n - 1\rangle) = r(x)f(x) + \langle x^n - 1\rangle$$

for all $r(x) \in S[x,\sigma]$.

A skew-cyclic code C is a left $S[x,\sigma]$-submodule of $\frac{S[x,\sigma]}{\langle x^n-1\rangle}$.

Now we present the structure of skew-cyclic codes over S. Theorem 3.5.7, Theorem 3.5.9 and Theorem 3.5.11 below present this for different possibilities on the minimal degree polynomial in a code.

Theorem 3.5.7. *Let C be a skew-cyclic code over S such that C contains a minimal degree polynomial $g(x)$ with its leading coefficient a unit. Then $C = \langle g(x) \rangle$. Moreover $g(x) \mid x^n - 1$, and so C is a free code.*

Proof: The proof follows from the minimality condition on $g(x)$ and the division algorithm (Lemma 3.5.2). ■

Example 3.5.8. *Let $p = 3$. Let C be a skew-cyclic code of length 4 over S with generator matrix*

$$\begin{bmatrix} 1+w & 0 & 1+w & 0 \\ 0 & 1-w & 0 & 1-w \end{bmatrix}.$$

Then the corresponding code is given by

$$\left\{ \begin{array}{ccc}
(0,0,0,0), & (2w+1,1,2w+1,1), & (w+1,0,w+1,0) \\
(w+2,2w+2,w+2,2w+2), & (2,w+2,2,w+2), & (1,1,1,1) \\
(1,2w,1,2w), & (0,2,0,2), & (w+1,2w+2,w+1,2w+2) \\
(2w+1,0,2w+1,0), & (2w,2w+2,2w,2w+2), & (2w+2,2w+2,2w+2,2w+2) \\
(w+1,w+1,w+1,w+1), & (2w,w+2,2w,w+2), & (2w+1,w+2,2w+1,w+2) \\
(w+2,2w,w+2,2w), & (w+2,0,w+2,0), & (w,w+2,w,w+2) \\
(2w+1,2w,2w+1,2w), & (1,w,1,w), & (w,1,w,1) \\
(w+1,2w+1,w+1,2w+1), & (2w,1,2w,1), & (w,w,w,w) \\
(2w+2,w+1,2w+2,w+1), & (w,2w,w,2w), & (2,0,2,0) \\
(w+2,w+2,w+2,w+2), & (1,w+1,1,w+1), & (1,2,1,2) \\
(2w+1,2,2w+1,2), & (1,2w+2,1,2w+2), & (2w,w+1,2w,w+1) \\
(1,w+2,1,w+2), & (0,w+2,0,w+2), & (0,2w+2,0,2w+2) \\
(w+2,2,w+2,2), & (0,w,0,w), & (2,2,2,2) \\
(w,2w+1,w,2w+1), & (w+1,2,w+1,2), & (2w,0,2w,0) \\
(2,2w+1,2,2w+1), & (w+2,1,w+2,1), & (w+1,w+2,w+1,w+2) \\
(0,2w+1,0,2w+1), & (2w+2,1,2w+2,1), & (2,w+1,2,w+1) \\
(0,2w,0,2w), & (2w+1,2w+1,2w+1,2w+1), & (w+1,w,w+1,w) \\
(2w,2w+1,2w,2w+1), & (0,w+1,0,w+1), & (w,2,w,2) \\
(2w+1,w,2w+1,w), & (2w+1,w+1,2w+1,w+1), & (2w+2,2w,2w+2,2w) \\
(2,2w+2,2,2w+2), & (2w+2,0,2w+2,0), & (2w+2,2w+1,2w+2,2w+1) \\
(w+2,w+1,w+2,w+1), & (2w+1,2w+2,2w+1,2w+2), & (2w,2,2w,2) \\
(2,2w,2,2w), & (2,w,2,w), & (0,1,0,1) \\
(w,2w+2,w,2w+2), & (w+2,2w+1,w+2,2w+1), & (2w+2,2,2w+2,2) \\
(2w,w,2w,w), & (w+2,w,w+2,w), & (w,0,w,0) \\
(1,2w+1,1,2w+1), & (2w+2,w+2,2w+2,w+2), & (1,0,1,0) \\
(w+1,1,w+1,1), & (2,1,2,1), & (w+1,2w,w+1,2w) \\
(2w+2,w,2w+2,w), & (2w,2w,2w,2w), & (w,w+1,w,w+1)
\end{array} \right\}.$$

C has a minimal degree polynomial $g(x) = 1 + x^2$ with its leading coefficient a unit.

Hence C can be written as $C = \langle g(x) \rangle$. Moreover $1 + x^2 \mid x^4 - 1$, and hence C is a free code.

Theorem 3.5.9. *Let C be a skew-cyclic code over S such that it has no polynomial with its leading coefficient a unit. Let $f(x)$ be a minimal degree polynomial in C. Then $C = \langle f(x) \rangle$.*

Proof: The proof follows by the minimality condition on $f(x)$ and the division algorithm discussed in Theorem 3.5.5. ■

Example 3.5.10. *Let $p = 5$. Let C be a skew-cyclic code of length 2 over S generated by the matrix:*

$$\begin{bmatrix} 1+w & 0 \\ 0 & 1+4w \end{bmatrix}.$$

Then C is given as

$$\left\{ \begin{array}{ccccc} (0,0), & (0,4w+1), & (0,w+4), & (2w+2,4w+1), & (4w+4,3w+2) \\ (3w+3,4w+1), & (0,2w+3), & (3w+3,2w+3), & (w+1,w+4), & (3w+3,3w+2) \\ (3w+3,0), & (2w+2,3w+2), & (w+1,4w+1), & (4w+4,4w+1), & (w+1,0) \\ (4w+4,w+4), & (w+1,2w+3), & (2w+2,w+4), & (2w+2,2w+3), & (w+1,3w+2) \\ (0,3w+2), & (2w+2,0), & (3w+3,w+4), & (4w+4,2w+3), & (4w+4,0) \end{array} \right\}.$$

We note that C has no codeword with corresponding polynomial having its leading coefficient a unit, and $f(x) = 1 + w$ is a minimal degree polynomial in C. Hence $C = \langle f(x) \rangle$.

Theorem 3.5.11. *Let C be a skew-cyclic code over S such that it has a polynomial with its leading coefficient a unit, but no minimal degree polynomial has its leading coefficient a unit. Let $f(x)$ be a minimal degree polynomial in C and $g(x)$ be a minimal degree polynomial in C among the polynomials having their leading coefficients a unit. Then $C = \langle f(x), g(x) \rangle$.*

Proof: Let $c(x) \in C$ be any codeword. Then by division algorithm (Lemma 3.5.2) we have

$$c(x) = q_1(x)g(x) + r_1(x),$$

where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$. If $r_1(x) = 0$, then we are done. Let $r_1(x) \neq 0$. Then the leading coefficient of $r_1(x)$ must be non-unit, as deg $r_1(x) <$ deg $g(x)$. Again by division algorithm (Theorem 3.5.5), we have

$$r_1(x) = q_2(x)f(x) + r_2(x),$$

where $r_2(x) = 0$ or deg $r_2(x) <$ deg $f(x)$ or the leading coefficient of $r_2(x)$ is unit. The last two conditions cannot be true, as $f(x)$ is a minimal degree polynomial in C and deg $r_2(x) \leq$ deg $r_1(x) <$ deg $g(x)$. Therefore $r_2(x) = 0$, and hence

$$c(x) = q_1(x)g(x) + q_2(x)f(x).$$

Hence $C = \langle f(x), g(x)\rangle$. ■

Example 3.5.12. *Let $p = 3$. Let C be a skew-cyclic code of length 4 over S spanned by the rows of the following matrix:*

$$\begin{bmatrix} 1+w & 0 & 0 & 0 \\ 0 & 1-w & 0 & 0 \\ 0 & 0 & 1+w & 0 \\ 0 & 0 & 0 & 1-w \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

We note that C has a minimal degree polynomial $f(x) = 1 + w$ and a minimal degree polynomial with its leading coefficient a unit in C is $g(x) = 1 + x^2$. Therefore $C = \langle g(x), f(x)\rangle$.

3.6 Additive skew-cyclic codes over S

In this section we define additive skew-cyclic codes over S. These codes are sub-codes of skew-cyclic codes over S. However, they are still closed under the skew-cyclic shift operation. We have obtained some good codes via this class.

Definition 3.6.1. *A code C is said to be an additive skew-cyclic code of length n over S if*

1. *C is a subgroup of S^n, and*
2. *$T_\sigma(c) = (\sigma(c_{n-1}), \sigma(c_0), \sigma(c_1), \cdots, \sigma(c_{n-2})) \in C$, whenever $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, where $T_\sigma(c)$ denotes the skew-cyclic shift of c.*

Lemma 3.6.2. *A code C is an additive skew-cyclic code of length n over S if and only if it is a left $\mathbb{F}_p[x]$-submodule of left $\mathbb{F}_p[x]$-module $\frac{S[x,\sigma]}{\langle x^n-1\rangle}$.*

Proof: Let C be an additive skew-cyclic code over S. Then for all $c_1(x), c_2(x) \in C$, $c_1(x) + c_2(x) \in C$ and $xc_1(x)$, which is the skew-cyclic shift of $c(x)$, belongs to C. Therefore $r(x)c(x) \in C$ for all $r(x) \in \mathbb{F}_p[x]$ and $c(x) \in C$. Hence C is an $\mathbb{F}_p[x]$-submodule. Converse is straightforward. ■

Now we give some examples of an additive skew-cyclic code and additive cyclic code over S.

Example 3.6.3. *Let $p = 5$. Let $C_1 = \langle 1 + wx\rangle$ be an additive skew-cyclic code of length 2 over S with generator matrix as:*

$$\begin{bmatrix} 1 & w \\ 4w & 1 \end{bmatrix}.$$

Then the corresponding code is given by

$$\left\{ \begin{array}{ccccc} (0,0), & (w+1,w+4), & (4w+3,3w+1), & (4w+4,4w+1), & (2w+1,w+3) \\ (2,2w), & (2w+3,3w+3), & (3w+3,3w+2), & (2w,3), & (4w+2,2w+1) \\ (4w,1), & (w+2,2w+4), & (3w+4,4w+2), & (1,w), & (3,3w) \\ (w,4), & (2w+4,4w+3), & (4w+1,w+1), & (4,4w), & (3w,2) \\ (w+3,3w+4), & (3w+1,w+2), & (3w+2,2w+2), & (w+4,4w+4), & (2w+2,2w+3) \end{array} \right\}.$$

The parameters of $\Phi'(C_1)$ are $[4, 2, 3]$, which is an MDS code over $\mathbb{F}_5$.

Similarly, we consider the additive cyclic code $C_2 = \langle 1 + wx\rangle$ over S generated by the matrix

$$\begin{bmatrix} 1 & w \\ w & 1 \end{bmatrix}.$$

The corresponding code is given by

$$\left\{\begin{array}{ccccc} (0,0), & (3,3w), & (4w+1,w+4), & (w+1,w+1), & (w+3,3w+1) \\ (4w,4), & (4,4w), & (2w+3,3w+2), & (2w,2), & (w+4,4w+1) \\ (3w+3,3w+3), & (2w+1,w+2), & (2,2w), & (w,1), & (w+2,2w+1) \\ (2w+2,2w+2), & (3w+1,w+3), & (4w+2,2w+4), & (3w,3), & (1,w) \\ (3w+2,2w+3), & (4w+4,4w+4), & (2w+4,4w+2), & (3w+4,4w+3), & (4w+3,3w+4) \end{array}\right\}.$$

The parameters of $\Phi'(C_2)$ are $[4,2,2]$. We note that $\Phi'(C_1)$ has improved parameters as compared to $\Phi'(C_2)$ even though the generator polynomials of C_1 and C_2 are same.

In the following example, we present a skew-cyclic code and an additive skew-cyclic code over S having the same generator polynomial.

Example 3.6.4. *Let $p = 5$. Let $C_1 = \langle wx + w\rangle$ be a skew-cyclic code of length 2 over S having the generator matrix:*

$$\begin{bmatrix} w & w \end{bmatrix}.$$

Then the corresponding code is

$$\left\{\begin{array}{ccccc} (0,0), & (2w+4,2w+4), & (w,w), & (w+4,w+4), & (1,1) \\ (4w+1,4w+1), & (3w+2,3w+2), & (3w+4,3w+4), & (2w+2,2w+2), & (w+3,w+3) \\ (3,3), & (4w,4w), & (3w+1,3w+1), & (4w+3,4w+3), & (3w+3,3w+3) \\ (w+2,w+2), & (2w+1,2w+1), & (4w+2,4w+2), & (w+1,w+1), & (4,4) \\ (4w+4,4w+4), & (3w,3w), & (2w+3,2w+3), & (2,2), & (2w,2w) \end{array}\right\}.$$

The parameters of $\Phi'(C_1)$ are $[4,2,2]$.

Similarly, let $C_2 = \langle wx + w\rangle$ be a additive skew-cyclic code of length 2 over S having the generator matrix:

$$\begin{bmatrix} w & w \end{bmatrix}.$$

Then the corresponding code is given by

$$\left\{ (0,0), \quad (3w,3w), \quad (w,w), \quad (4w,4w), \quad (2w,2w) \right\}.$$

Here C_2 is a sub-code of C_1, which still satisfies the skew-cyclic shift property. The parameters for $\Phi'(C_2)$ are $[4,1,4]$.

Similarly, we give some more examples, and some good codes over $\mathbb{F}_p$ via skew-cyclic and additive skew-cyclic codes over S are obtained. Here $*$ denotes optimal code with those parameters.

1. Let $p = 5$. Let $C_1 = \langle 1 + wx \rangle$. Then
   (a) if C_1 is a skew-cyclic code, then $\Phi'(C_1)$ is a $[4, 4, 1]^*$ code over $\mathbb{F}_5$.
   (b) if C_1 is an additive skew-cyclic code, then $\Phi'(C_1)$ is a $[4, 2, 3]^*$ code over $\mathbb{F}_5$.
2. Let $p = 5$. Let $C_2 = \langle (4w + 2)x + w + 3 \rangle$. Then
   (a) if C_2 is a skew-cyclic code, then $\Phi'(C_2)$ is an $[8, 6, 2]^*$ code over $\mathbb{F}_5$.
   (b) if C_2 is an additive skew-cyclic code, then $\Phi'(C_2)$ is an $[8, 3, 4]$ code over $\mathbb{F}_5$.
3. Let $p = 3$. Let $C_3 = \langle (w + 2) + (w + 2)x + (w + 1)x^2 + 2x^3 \rangle$. Then
   (a) if C_3 is a skew-cyclic code, then $\Phi'(C_3)$ is an $[8, 6, 2]^*$ code over $\mathbb{F}_3$.
   (b) if C_3 is an additive skew-cyclic code, then $\Phi'(C_3)$ is an $[8, 4, 4]^*$ code over $\mathbb{F}_3$.
4. Let $p = 3$. Let $C_4 = \langle (w+2) + (w+2)x + (w+2)x^2 + (w+2)x^3 + (2w+2)x^5 \rangle$. Then
   (a) if C_4 is a skew-cyclic code, then $\Phi'(C_4)$ is a $[12, 12, 1]^*$ code over $\mathbb{F}_3$.
   (b) if C_4 is an additive skew-cyclic code, then $\Phi'(C_4)$ is a $[12, 6, 5]$ code over $\mathbb{F}_3$.

3.7 Double skew-cyclic and double additive skew-cyclic codes over S

Double skew-cyclic codes and additive double skew-cyclic codes over S are defined as follows.

Let C be a submodule of $S^{\alpha+\beta}$. Then C is said to be double skew-cyclic code if for any $c = (a_0, a_1, \cdots, a_{\alpha-1} \mid b_0, b_1, \cdots, b_{\beta-1})$ in C, we have $(\sigma(a_{\alpha-1}), \sigma(a_0), \cdots, \sigma(a_{\alpha-2}) \mid \sigma(b_{\beta-1}), \sigma(b_0), \cdots, \sigma(b_{\beta-2}))$ in C.

We define a double additive skew-cyclic code C_a if it is a subgroup of $S^{\alpha+\beta}$, and is invariant under the shift operator defined above.

In polynomial form, a double additive skew-cyclic code C_a over S is a left $\mathbb{F}_p[x]$-submodule of $\mathbb{F}_p[x]$-module $\frac{S[x,\sigma]}{\langle x^\alpha - 1\rangle} \times \frac{S[x,\sigma]}{\langle x^\beta - 1\rangle}$ with respect to the multiplication

$$r(x)c(x) = r(x)(a(x) \mid b(x)) = (r(x)a(x) \mid r(x)b(x)),$$

for all $r(x) \in \mathbb{F}_p[x]$ and $c(x) = (a(x) \mid b(x)) \in \frac{S[x,\sigma]}{\langle x^\alpha - 1\rangle} \times \frac{S[x,\sigma]}{\langle x^\beta - 1\rangle}$.

Example 3.7.1. *Let $p = 5$. Let C be a double additive skew-cyclic code of length $4(= 2 + 2)$ over S generated by the matrix:*

$$\begin{bmatrix} 1 & w & 1 & w \\ 4w & 1 & 4w & 1 \end{bmatrix}.$$

Then the parameters of $\Phi'(C)$ are $[8, 2, 6]^*$, which is an optimal code over $\mathbb{F}_5$. The parameters can be verified from the full code given below.

$$\left\{\begin{array}{ccc} (0,0,0,0), & (4w,1,4w,1), & (w+2,2w+4,w+2,2w+4) \\ (3w+2,2w+2,3w+2,2w+2), & (3,3w,3,3w), & (2w+3,3w+3,2w+3,3w+3) \\ (4,4w,4,4w), & (3w+1,w+2,3w+1,w+2), & (2,2w,2,2w) \\ (4w+2,2w+1,4w+2,2w+1), & (4w+4,4w+1,4w+4,4w+1), & (3w+4,4w+2,3w+4,4w+2) \\ (2w,3,2w,3), & (3w,2,3w,2), & (w+3,3w+4,w+3,3w+4) \\ (2w+4,4w+3,2w+4,4w+3), & (4w+1,w+1,4w+1,w+1), & (2w+2,2w+3,2w+2,2w+3) \\ (1,w,1,w), & (w+1,w+4,w+1,w+4), & (2w+1,w+3,2w+1,w+3) \\ (3w+3,3w+2,3w+3,3w+2), & (w+4,4w+4,w+4,4w+4), & (4w+3,3w+1,4w+3,3w+1) \\ (w,4,w,4) & & \end{array}\right\}.$$

Example 3.7.2. *Let $p = 5$. Let C be a double additive skew-cyclic code of length $6(= 2 + 4)$ over S having generator matrix:*

$$\begin{bmatrix} 1 & w & w+3 & -w+2 & 0 & 0 \\ -w & 1 & 0 & -w+3 & w+2 & 0 \\ 1 & w & 0 & 0 & w+3 & -w+2 \\ -w & 1 & w+2 & 0 & 0 & -w+3 \end{bmatrix}.$$

Then $\Phi'(C)$ has the parameters $[12, 4, 6]$.

In a similar way, we have obtained some more codes over $\mathbb{F}_p$ through double skew-cyclic and double additive skew-cyclic codes over S. These are given below.

1. Let $p = 3$. For $\alpha = 2$ and $\beta = 4$, let $C_1 = \langle(w+wx \mid 2+(w+1)x+2x^2+(w+1)x^3)\rangle$. Then

(i) if C_1 is a double skew-cyclic code over S, then $\Phi'(C_1)$ is a $[12, 4, 4]$ code over $\mathbb{F}_3$.

(ii) if C_1 is a double additive skew-cyclic code over S, then $\Phi'(C_1)$ is a $[12, 2, 8]$ code over $\mathbb{F}_3$.

2. Let $p = 5$. For $\alpha = 2$ and $\beta = 4$, let $C_2 = \langle(1 + wx \mid 1 - wx + (1 + w)x^2 + wx^3)\rangle$. Then

(i) if C_2 is a double skew-cyclic code over S, then $\Phi'(C_2)$ is a $[12, 6, 3]$ code over $\mathbb{F}_5$.

(ii) if C_2 is a double additive skew-cyclic code over S, then $\Phi'(C_2)$ is a $[12, 3, 7]$ code over $\mathbb{F}_5$.

3. Let $p = 3$. For $\alpha = 4$ and $\beta = 4$, let $C_3 = \langle(w + x + x^2| (w + 2) + (w + 2)x + 2x^2 + (w + 1)x^3)\rangle$. Then

(i) if C_3 is a double skew-cyclic code over S, then $\Phi'(C_3)$ is a $[16, 8, 4]$ code over $\mathbb{F}_3$.

(ii) if C_3 is a double additive skew-cyclic code over S, then $\Phi'(C_3)$ is a $[16, 4, 9]^*$ code over $\mathbb{F}_3$.

4. Let $p = 5$. For $\alpha = 4$ and $\beta = 4$, let $C_4 = \langle(1 - x + (1 + w)x^2 + 2x^3 \mid 2 + 2x + (w + 2)x^2 + wx^3)\rangle$. Then

(i) if C_4 is a double skew-cyclic code over S, then $\Phi'(C_4)$ is a $[16, 8, 4]$ code over $\mathbb{F}_5$.

(ii) if C_4 is a double additive skew-cyclic code over S, then $\Phi'(C_4)$ is a $[16, 4, 10]$ code over $\mathbb{F}_5$.

3.8 Conclusion

In this chapter, we have studied $\mathbb{F}_3R$-skew cyclic codes, where $R = \mathbb{F}_3 + v\mathbb{F}_3, v^2 = v$. By obtaining the structure of skew-cyclic codes over R using a new division algorithm defined on $R[x, \theta]$, the structure for $\mathbb{F}_3R$-skew cyclic codes has been obtained. We have also defined a class of skew-cyclic codes over $S = \mathbb{F}_p + w\mathbb{F}_p$, and their generating sets are obtained. Additive skew-cyclic codes over S have been studied as sub-codes of skew-cyclic codes over S.

Chapter 4

Skew-constacyclic and Skew-cyclic Codes over Extensions of $\mathbb{Z}_4$

4.1 Introduction

Cyclic codes are one of the most studied linear codes. Constacyclic codes are an immediate generalization of cyclic codes. They have been studied extensively over finite fields as well as over some finite rings [11, 91, 90, 33, 85, 62, 107, 60, 36, 106, 82, 5], and many good codes have been obtained in this class. Recently this class has been generalized to skew constacyclic codes [27, 58, 40, 38]. In this chapter we study skew-constacyclic codes and skew-cyclic codes over some extension rings of $\mathbb{Z}_4$.

It may be noted that two popular rings $\mathbb{Z}_4$ and $\mathbb{F}_2+u\mathbb{F}_2$, $u^2=0$, are not suitable for defining skew codes as they do not have any non-trivial automorphism, and the resulting skew codes coincide with simple linear codes. So different classes of skew codes have been defined on some other structures such as $\mathbb{F}_2+v\mathbb{F}_2$ [1], $\mathbb{F}_p+v\mathbb{F}_p$ [41] and $\mathbb{F}_q+v\mathbb{F}_q$ [48] with $v^2=v$, where non-trivial automorphisms exist. Motivated by the these works, we define a class of skew-constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4, u^2=0$. We characterize the skew polynomial ring $R[x,\theta]$, where $R=\mathbb{Z}_4+u\mathbb{Z}_4,\ u^2=0$, and θ is an automorphism of R, and introduce a class of skew-constacyclic codes over R. Some structural properties of these codes are determined. These codes are further generalized to double skew-constacyclic codes, through which we have been able to obtain some good codes over $\mathbb{Z}_4$. Also, a class of skew-cyclic codes over $GR(4,2) + vGR(4,2), v^2 = v$ has also been studied in this chapter.

4.2 The ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$

We denote $R = \mathbb{Z}_4 + u\mathbb{Z}_4,\ u^2 = 0$. The ring R has the characteristic 4 and the cardinality 16. Moreover R is isomorphic to the ring $\mathbb{Z}_4[u]/\langle u^2\rangle$. It can easily be seen that the ideal $\langle 2, u\rangle$ is the unique maximal ideal of R, and hence it is a local ring. Its residue field is $\mathbb{F}_2$. An element $a + ub$ of R is a unit if and only if a is unit. Thus the units of R are $1, 3, 1+u, 1+2u, 1+3u, 3+u, 3+2u, 3+3u$. To know more about the ring R, we refer to [104, 14].

4.2.1 Skew polynomial ring $R[x, \theta]$

Define a map θ on R such that

$$\theta(a + ub) = a + (u + 2)b$$

for all $a + ub \in R$. Then θ is an automorphism of R of order 2. By Definition 3.2, $R[x, \theta]$ forms a skew-polynomial ring.

Although, $R[x, \theta]$ is a non-commutative ring and not a left or right Euclidean ring, the following result is true for $R[x, \theta]$.

Lemma 4.2.1. *[74] Let $f(x), g(x) \in R[x, \theta]$ be such that the leading coefficient of $g(x)$ is a unit. Then there exist $q(x), r(x) \in R[x, \theta]$ such that $f(x) = q(x)g(x) + r(x)$, where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.*

Lemma 4.2.2. *The set $Z_f = \{0, 1, 2, 3, 2u, 1+2u, 2+2u, 3+2u\}$ is the fixed sub-ring of R under θ.*

The following result directly follows from the discussion on Page 25 of [74].

Theorem 4.2.3. *The center $Z(R[x, \theta])$ of $R[x, \theta]$ is $Z_f[x^2]$.*

Corollary 4.2.3.1. *Let $f = x^n - 1$. Then $f \in Z(R[x, \theta])$ if and only if n is even. Further $x^n - \alpha \in Z(R[x, \theta])$ if and only if n is even and α is fixed by θ.*

If we do not assume that α is fixed by θ, then the result does not hold. For instance, let n be even and $\alpha = 1 + u$ a unit in R, which is not fixed by θ. Then $(x^n - (1 + u))ux = ux(x^n - (u + 2)) \neq ux(x^n - (1 + u))$, and hence $(x^n - (1 + u))$ is not a central element.

The following result is straightforward.

Theorem 4.2.4. *Let n be a positive integer and α a unit in R. Then the following statements are equivalent:*

(i) $x^n - \alpha$ is central in $R[x, \theta]$.

(ii) $\langle x^n - \alpha \rangle$ is a two sided ideal.

(iii) n is even and α is fixed by θ.

Since $R[x, \theta]$ does not have the unique factorization property, polynomials in $R[x, \theta]$ may have many factors as compared to the commutative case. In particular, $x^n - \alpha$, where $\alpha \in R$ is a unit, has in general more than one factorization. The following example illustrates this.

Example 4.2.5. *Let $\alpha = 1 + 2u$. The factorization, up to non-associates, of $x^3 - (1 + 2u)$ in $R[x, \theta]$ is given by*

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

Remark 4.2.5.1. *For odd n, factorization in $R[x]$ is unique [14], but as the above example shows, the same is not true for $R[x, \theta]$.*

The above example shows that there may be more (θ, α)-constacyclic codes over R than α-constacyclic codes over R.

4.2.2 Gray map

On $\mathbb{Z}_4$, the Lee weight (w_L) is defined as $w_L(0) = 0,\ w_L(1) = 1,\ w_L(2) = 2,\ w_L(3) = 1$, and the Lee weight (w_L) of a vector $v \in {\mathbb{Z}_4}^2$ is then defined as the rational sum of the Lee weights of its coordinates. Define a Gray map $\phi : R \to {\mathbb{Z}_4}^2$ such that

$$\phi(a + vb) = (b, a + b),$$

and for any $x \in R$, we define $w_G(x) = w_L(\phi(x))$, where $w_G(x)$ denotes the Gray weight of x. Thus, the Gray weights of the elements of R are defined as:

x	0	1	2	3	v	$2v$	$3v$	$1+v$
$w_G(x)$	0	1	2	1	2	4	2	3
x	$1+2v$	$1+3v$	$2+v$	$2+2v$	$2+3v$	$3+v$	$3+2v$	$3+3v$
$w_G(x)$	3	1	2	2	2	1	3	3

Remark 4.2.5.2. *ϕ can be extended componentwise to $\Phi : R^n \to {\mathbb{Z}_4}^{2n}$. Also the Gray weight of $x \in R^n$ is then defined as the rational sum of Gray weights of its coordinates.*

Now onward, we write the parameters of a linear code over $\mathbb{Z}_4$ as $(n, 4^{k_1}2^{k_2}, d_L)$, which is the standard form for parameters of codes over $\mathbb{Z}_4$.

4.3 Skew $(1 + 2u)$-constacyclic codes over R

To study constacyclic codes over R, we first consider some structural properties of $R[x, \theta]/\langle x^n - \alpha\rangle$. Since the ring $R[x, \theta]$ is non-commutative, the ideals of $R[x, \theta]$ may not be two sided ideals. In particular, the ideal $\langle x^n - \alpha\rangle$ of $R[x, \theta]$ is a two sided ideal if and only if n is even and α is fixed by θ. In this case $R_n = \frac{R[x,\theta]}{\langle x^n-\alpha\rangle}$ is therefore a residue class ring. If either n is odd or α is not fixed by θ, the set R_n is only a left $R[x, \theta]$-module with multiplication defined as $r(x)(f(x) + \langle x^n - \alpha\rangle) = r(x)f(x) + \langle x^n - \alpha\rangle$ for any $r(x), f(x) \in R[x, \theta]$. To associate the vectors of R^n with the polynomials in R_n, we define an R-module isomorphism from R^n to R_n as

$$(c_0, c_1, \cdots , c_{n-1}) \mapsto c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$

We recall that, a subset C of R^n is called a (θ,α)-constacyclic code of length n over R if C is an R-submodule of R^n and for any $(c_0, c_1, \cdots, c_{n-1}) \in C$, we have $(\alpha\theta(c_{n-1}), \theta(c_0), \cdots, \theta(c_{n-2})) \in C$. If we denote (θ,α)-constacyclic shift by $T_{\theta,\alpha}$, then an R-submodule of R^n is a (θ,α)-constacyclic code if $T_{\theta,\alpha}(C) = C$. In particular, if $\alpha = 1$, then C is a skew-cyclic code over R.

Throughout the chapter, the notation (θ,α)-constacyclic codes can be read as skew α-constacyclic codes. The following result can be proved easily.

Theorem 4.3.1. *A code C of length n in $R_n = R[x,\theta]/\langle x^n - \alpha\rangle$ is a (θ,α)-constacyclic code if and only if C is a left $R[x,\theta]$-submodule of the left $R[x,\theta]$-module R_n.*

Proof: Straightforward. ■

Corollary 4.3.1.1. *For even n and a unit α fixed by θ, a code C of length n over R is a (θ,α)-constacyclic code if and only if C is a left ideal in R_n.*

Proof: For given conditions, $x^n - \alpha \in Z(R[x,\theta])$, and so R_n is a ring. The result follows. ■

Theorem 4.3.2. *If C is a (θ,α)-constacyclic code of length n over R containing a minimal degree polynomial $g(x)$ whose leading coefficient is a unit, then C is a free code such that $C = \langle g(x)\rangle$ and $g(x)|x^n - \alpha$. Moreover C has a basis $\{g(x), xg(x), \ldots, x^{n-deg\ (g(x))-1}\}$ and $|C| = |R|^{n-deg\ g(x)}$.*

Proof: Let $g(x)$ be a minimal degree polynomial in C with its leading coefficient a unit. Then the result that $C = \langle g(x)\rangle$ follows from the division algorithm (Lemma 4.2.1). Now again by the division algorithm, we get $x^n - \alpha = q(x)g(x) + r(x)$, where $r(x) = 0$ or deg $r(x) <$ deg $g(x)$. Since $x^n - \alpha$ corresponds to the codeword 0 in C, we have $r(x) = -q(x)g(x) \in C$ and so $r(x) = 0$, as $g(x)$ is a minimal degree polynomial in C. Therefore $g(x)|x^n - \alpha$. Now let $x^n - \alpha = h(x)g(x)$ for some $h(x) \in R[x,\theta]$. Since the leading coefficient of $g(x)$ is a unit, the leading coefficient of $h(x)$ must also be a unit. Moreover if deg $g(x)$ is $n-k$, the degree of $h(x)$ must be k. Let

$h(x) = h_0 + h_1 x + \cdots + h_k x^k$, where h_k is a unit. Then $h(x)g(x) = 0(\text{mod } x^n - \alpha)$ implies that $h_0 g(x) + h_1 x g(x) + \cdots h^k x^k g(x) = 0$ in R_n. Therefore $x^k g(x)$, and hence $x^i g(x)$ for $i \geq k$, is a linear combination of $g(x), xg(x), \cdots, x^{k-1}g(x)$, and so $A = \{g(x), xg(x), \cdots, x^{k-1}g(x)\}$ spans C. For independence of A, suppose $a_0 g(x) + a_1 x g(x) + \cdots + a_{k-1} x^{k-1} g(x) = 0$ in R_n for some $a_i \in R,\ 0 \leq i \leq k-1$, i.e., $a(x)g(x) = 0$, where $a(x) = a_0 + a_1 x + \cdots a_{k-1} x^{k-1}$. Then in $R[x, \theta]$, we have $a(x)g(x) = e(x)(x^n - \alpha)$ for some $e(x) \in R[x, \theta]$. The degree of the expression on left hand side is $n-1$, which is possible only if $e(x)$ is zero. Hence $a(x)$ must also be the zero polynomial, and so $a_i = 0$ for all i. Therefore A is R-linearly independent, and hence C is a free code. It immediately follows that $|C| = |R|^{n - \deg\, g(x)}$. ■

The converse of the above theorem is also true, and is given below.

Theorem 4.3.3. *Let C be a principally generated free (θ, α)-constacyclic code of length n over R. Then there exists a minimal degree polynomial $g(x) \in C$ having its leading coefficient a unit such that $C = \langle g(x) \rangle$ and $g(x) \mid x^n - \alpha$.*

Proof: Since C is a principally generated free (θ, α)-constacyclic code of length n over R, using similar arguments as in [17, Proposition 1], it follows that there exists a monic polynomial $g(x)$ in C such that $C = \langle g(x) \rangle$ and $g(x) \mid x^n - \alpha$. Further as in the case of finite fields [69, pp. 191], it can easily be shown that for any $c(x) \in C,\ c(x) = a(x)g(x)$ in $R[x, \theta]$ for some $a(x) \in R[x, \theta]$. Since $g(x)$ is a monic polynomial, deg $c(x) \geq$ deg $g(x)$. Hence the result. ■

Now onward, for this chapter only, we assume that $\alpha = 1 + 2u$.

Example 4.3.4. *Let C be a (θ, α)-constacyclic code generated by the following matrix:*

$$\begin{bmatrix} 1+3u & 1+u & 1+3u \end{bmatrix}.$$

The corresponding code is given by

$$\left\{\begin{array}{ccc} (0,0,0), & (2u+3,3,2u+3), & (3u+3,u+3,3u+3) \\ (2u+1,1,2u+1), & (3u,3u,3u), & (u+3,3u+3,u+3) \\ (u+2,u+2,u+2), & (u,u,u), & (3u+1,u+1,3u+1) \\ (2,2,2), & (1,2u+1,1), & (2u,2u,2u) \\ (3,2u+3,3), & (3u+2,3u+2,3u+2), & (u+1,3u+1,u+1) \\ (2u+2,2u+2,2u+2) & & \end{array}\right\}.$$

The polynomial $g(x) = (1+3u)x^2 + (1+u)x + 1 + 3u$ is a minimal degree polynomial in C with its leading coefficient a unit. Hence $C = \langle g(x) \rangle$. Also $g(x) | x^3 - (1+2u)$, and so the set $\{g(x)\}$ forms a basis of C. Moreover $\Phi(C)$ is a $\mathbb{Z}_4$-linear code with the parameters $(6, 4^2 2^0, 5_L)$, which is a best known $\mathbb{Z}_4$-linear code [8].

Now we give an example of a code which has no minimal degree polynomial with its leading coefficient a unit.

Example 4.3.5. *Let C be a (θ, α)-constacyclic code with generator matrix*

$$G = \begin{bmatrix} u & u & u \\ u+2 & u+2 & u+2 \end{bmatrix}.$$

Then the corresponding code is given by

$$\left\{\begin{array}{ccc} (0,0,0), & (3u+2,3u+2,3u+2), & (2,2,2) \\ (2u,2u,2u), & (u+2,u+2,u+2) & (u,u,u) \\ (2u+2,2u+2,2u+2), & (3u,3u,3u) & \end{array}\right\}.$$

In this example, $C = \langle g(x) \rangle$, where $g(x) = u + ux + ux^2$. A minimal spanning set for this code is $\{g(x), xg(x)\}$, however the set is not $\mathbb{Z}_4$-linearly independent. Hence C is not a free code. $\Phi(C)$ is a $\mathbb{Z}_4$-linear code with the parameters $(6, 4^1 2^1, 6_L)$, which is a best known code with these parameters [8].

In the following example, we choose two non-associate factors $f_1(x) = x + 2u + 3$ and $f_2(x) = ((u+3)x + u + 3)$ of degree 1 of $x^3 - (1+2u)$ in $R[x, \theta]$. Then we calculate the parameters for two (α, θ)-constacyclic codes C_1 and C_2 generated by $f_1(x)$ and $f_2(x)$, respectively. It turns out that C_2 is a new good $\mathbb{Z}_4$-linear code.

Example 4.3.6. *$C_1 = \langle x + (2u+3)\rangle$. Then C_1 is an (α, θ)-constacyclic code of length 3 over R with the parameters $(3, 16^2, 2_L)$ and so $\Phi(C)$ is a $(6, 4^4 2^0, 2_L)$ $\mathbb{Z}_4$-linear code.*

Next $C_2 = \langle (u+3)x + (u+3)\rangle$. Then C_2 is an (α, θ)-constacyclic code of length 3 over R with parameters $(3, 16^2 4^1, 2_L)$ and so $\Phi(C)$ is a $(\mathbf{6}, \mathbf{4^4 2^2}, \mathbf{2_L})$ $\mathbb{Z}_4$-linear code, which is a new good linear code over $\mathbb{Z}_4$ with improved minimum distance by 1, when compared to a code over $\mathbb{Z}_4$ with same length and cardinality [8].

This indicates that new codes can be obtained over $\mathbb{Z}_4$ through skew codes.

Theorem 4.3.7. *Let C be a (θ, α)-constacyclic code of odd length n over R. Then C is an α-constacyclic code over R.*

Proof: Since n is odd, we have $(n, 2) = 1$. Therefore there exist two integers a, b such that $na + 2b = 1$ and so $2b = 1 - na = 1 + nl$, where $l \equiv -a \ (mod\ n)$. Now

$$\begin{aligned} x^{2b}c(x) &= x^{2b}(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) \\ &= \theta^{2b}(c_0)x^{2b} + \theta^{2b}(c_1)x^{2b+1} + \cdots + \theta^{2b}(c_{n-1})x^{2b+n-1} \\ &= \theta^{2b}(c_0)x^{1+nl} + \theta^{2b}(c_1)x^{1+nl+1} + \cdots + \theta^{2b}(c_{n-1})x^{(1+nl)+(n-1)}. \end{aligned}$$

Since order of θ is 2 and $x^n = \alpha$ in R_n, we have

$$\begin{aligned} x^{2b}c(x) &= c_0\alpha^l x + c_1\alpha^l x^2 + \cdots + c_{n-2}\alpha^l x^{n-1} + c_{n-1}\alpha^{l+1} \\ &= \alpha^l(c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}\alpha). \end{aligned}$$

Since $\alpha^{2l} = 1$, so $\alpha^l x^{2b}c(x)$ is an α-constacyclic shift of $c(x)$. Hence the result. ■

Theorem 4.3.8. *Let C be a (θ, α)-constacyclic code of even length n generated by a monic right divisor $g(x)$ of $x^n - \alpha$. Then C is an α-constacyclic code over R if and only if all the coefficients of $g(x)$ are fixed by θ.*

Proof: Let $g(x) = g_0 + g_1x + \cdots + g_{r-1}x^{r-1} + x^r$ be the generator polynomial of a (θ, α)-constacyclic code C. Suppose all the coefficients of $g(x)$ are fixed by θ. Then clearly the corresponding generator matrix G of C will be the generator matrix of an α-constacyclic code over R.

Conversely, suppose C is also an α-constacyclic code. Then C, a left ideal of $R[x,\theta]/\langle x^n - \alpha\rangle$, is an ideal of $R[x]/\langle x^n - \alpha\rangle$ as well. Therefore, $g(x)x \in C$. Moreover $g(x)x - xg(x) \in C$, as C is linear. This implies that $gx - xg = (\theta(g_0) - g_0)x + (\theta(g_1) - g_1)x^2 + \cdots + (\theta(g_{r-1}) - g_{r-1})x^r$ is a multiple of $g(x)$. Since the degrees of $g(x)$ and $g(x)x - xg(x)$ are same, the latter must be a constant multiple of $g(x)$. But the constant term in $g(x)x - xg(x)$ is zero, so we must have $g(x)x - xg(x) = 0$. This implies that $\theta(g_i) = g_i$ for all $i = 0, 1, 2, ..., r$. Hence the result. ■

Theorem 4.3.9. *Let n be odd. Let Λ be a map from $\frac{R[x,\theta]}{\langle x^n-1\rangle}$ to $\frac{R[x,\theta]}{\langle x^n-\alpha\rangle}$ such that*

$$\Lambda(a(x)) = a(\alpha x).$$

Then Λ is an ring isomorphism.

Proof: Since n is odd, we observe that $\alpha^n = \alpha$. Now for any $a(x), b(x) \in R[x,\theta]$, suppose $a(x) = b(x)(\text{mod } x^n - 1)$, i. e., $a(x) - b(x) = q(x)(x^n - 1)$ for some $q(x) \in R[x,\theta]$. Replacing x by αx, we get

$$\begin{aligned} a(\alpha x) - b(\alpha x) &= q(\alpha x)((\alpha x)^n - 1) \\ &= q(\alpha x)((\alpha x)^n - (\alpha^2)), \text{ as } \alpha^2 = 1. \\ &= q(\alpha x)((\alpha x^n - (\alpha^2)), (\alpha^n = \alpha \text{ and } (\alpha x)^n = \alpha^n x^n \text{ as } \theta(\alpha) = \alpha). \\ &= q(\alpha x)\alpha(x^n - \alpha). \end{aligned}$$

Therefore $a(\alpha x) = b(\alpha x)(\text{mod } x^n - \alpha)$.

Thus $a(x) = b(x)(\text{mod } x^n - 1)$ is equivalent to $a(\alpha x) = b(\alpha x)(\text{mod } x^n - \alpha)$. Therefore Λ is one-one. Moreover since the map is between finite sets of same cardinality, it is onto also. It is easy to verify that Λ is a homomorphism. Hence the result. ■

Thus it follows that, for odd n, both the rings $\frac{R[x,\theta]}{\langle x^n-1\rangle}$ and $\frac{R[x,\theta]}{\langle x^n-\alpha\rangle}$ have same ideal structure. Therefore the study of skew-constacyclic codes of odd lengths over R coincides with the study of skew-cyclic codes of odd lengths over R.

4.4 Duals of (θ, α)-constacyclic codes

In this section we study duals of (θ, α)-constacyclic codes over R.

Lemma 4.4.1. *Let C be a code of length n over R, where n is even. Then C is a (θ, α)-constacyclic code iff $C^{\perp}$ is a (θ, α)-constacyclic code.*

Proof: Let $u = (u_0, u_1, \cdots, u_{n-1}) \in C$ and $v = (v_0, v_1, \cdots, v_{n-1}) \in C^{\perp}$ be two arbitrary elements. Since C is (θ, α)-constacyclic code, $T_{\theta,\alpha}^{n-1}(u) = (\theta^{n-1}(\alpha u_1), \theta^{n-1}(\alpha u_2), \cdots, \theta^{n-1}(\alpha u_{n-1}), \theta^{n-1}(u_0)) \in C$. Then

$$\begin{aligned}
0 &= T_{\theta,\alpha}^{n-1}(u) \cdot v \\
&= (\theta^{n-1}(\alpha u_1), \theta^{n-1}(\alpha u_2), \cdots, \theta^{n-1}(\alpha u_{n-1}), \theta^{n-1}(u_0)) \cdot (v_0, v_1, \cdots, v_{n-1}) \\
&= \alpha[(\theta^{n-1}(u_1), \theta^{n-1}(u_2), \cdots, \theta^{n-1}(u_{n-1}), \theta^{n-1}(\alpha^{-1}u_0))] \cdot (v_0, v_1, \cdots, v_{n-1}) \\
&= \alpha[\theta^{n-1}(\alpha^{-1}u_0)v_{n-1} + \sum_{i=1}^{n-1} \theta^{n-1}(u_i)v_{i-1}] \\
&= \alpha(u_0\theta(\alpha^{-1}v_{n-1})) + \sum_{i=1}^{n-1} u_i\theta(v_{i-1}) \text{ (as } \theta^n = I, \text{the identity map)} \\
&= \alpha[T_{\theta,\alpha^{-1}}(v) \cdot u].
\end{aligned}$$

This implies that $T_{\theta,\alpha}(v) \in C^{\perp}$, as $\alpha^{-1} = \alpha$. Therefore C is a (θ, α)-constacyclic code. Conversely, if $C^{\perp}$ is (θ, α)-constacyclic code, then $C = (C^{\perp})^{\perp}$ is also a (θ, α)-constacyclic code. Hence the result. ■

Lemma 4.4.2. *Let $g(x), h(x) \in R[x, \theta]$. If $g(x)h(x)$ is a monic central element of $R[x, \theta]$, then $g(x)h(x) = h(x)g(x)$.*

Proof: Since $g(x)h(x)$ is a central element, we have $h(x)(g(x)h(x)) = (g(x)h(x))h(x)$ for $h(x) \in R[x, \theta]$. Therefore $(h(x)g(x) - g(x)h(x))h(x) = 0$, and so $h(x)g(x) = g(x)h(x)$, as $h(x)$ is a regular polynomial. ■

Lemma 4.4.3. *Let C be a (θ, α)-constacyclic code of even length n over R generated by a monic right divisor $g(x)$ of $x^n - \alpha$. Then $v(x) \in R_n = \frac{R[x,\theta]}{\langle x^n - \alpha \rangle}$ is in C if and only if $v(x)h(x) = 0$ in R_n, where $x^n - \alpha = h(x)g(x)$.*

Proof: Suppose $v(x) \in C$. Then $v(x) = a(x)g(x)$ for some $a(x) \in R_n$. So $v(x)h(x) = a(x)g(x)h(x) = a(x)h(x)g(x) = 0$ in R_n, as $g(x)h(x) = h(x)g(x) = x^n - \alpha$. Conversely, suppose $v(x)h(x) = 0$ in R_n for some $v(x) \in R_n$. Then there exists $r(x) \in R[x,\theta]$ such that $v(x)h(x) = r(x)(x^n - \alpha) = r(x)h(x)g(x) = r(x)g(x)h(x)$. Since $h(x)$ is regular, $v(x) = r(x)g(x)$. Hence the result. ■

Remark 4.4.3.1. *If a code C is generated by a minimal degree polynomial $g(x)$ with its leading coefficient a unit, then there exists a minimal degree monic polynomial $g_1(x)$ such that $C = \langle g_1(x)\rangle$.*

Theorem 4.4.4. *Let C be a (θ,α)-constacyclic code of even length n generated by the minimal degree monic polynomial $g(x) = g_0 + g_1x + \cdots + x^{n-k}$ such that $x^n - \alpha = h(x)g(x)$ for some $h(x) \in R_n$. Let $h(x) = h_0 + h_1x + h_2x^2 + \cdots + x^k$. Then the polynomial $h^*(x) = 1 + \theta(h_{k-1})x + \theta^2(h_{k-2})x^2 + \cdots + \theta^k(h_0)x^k$ generates $C^\perp$.*

Proof: Let $c(x) \in C$. Then $c(x)h(x) = 0$ in R_n. Therefore the coefficients of $x^k, x^{k+1}, \cdots, x^{n-1}$ in $[c_0 + c_1x + c_2x^2 + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}][h_0 + h_1x + h_2x^2 + \cdots + h_{k-1}x^{k-1} + x^k]$ are all zero's. Hence we have

$$\begin{array}{rcl}
c_0 + c_1\theta(h_{k-1}) + c_2\theta^2(h_{k-2}) + \cdots + c_k\theta^k(h_0) & = & 0\\
c_1 + c_2\theta^2(h_{k-1}) + c_3\theta^3(h_{k-2}) + \cdots + c_{k+1}\theta^{k+1}(h_0) & = & 0\\
c_2 + c_3\theta^3(h_{k-1}) + c_4\theta^4(h_{k-2}) + \cdots + c_{k+2}\theta^{k+2}(h_0) & = & 0\\
\vdots \qquad\qquad \vdots & \vdots & \vdots\\
c_{n-k-1}\theta^{n-k-1}(h_{k-1}) + c_{n-k}\theta^{n-k}(h_{k-2}) + \cdots + c_{n-1}\theta^{n-1}(h_0) & = & 0.
\end{array}$$

Let $H^* =$

$$\begin{bmatrix}
1 & \theta(h_{k-1}) & \theta^2(h_{k-2}) & \cdots & \theta^k(h_0) & \cdots & \cdots & 0\\
0 & 1 & \theta^2(h_{k-1}) & \cdots & \cdots & \theta^{k+1}(h_0) & \cdots & 0\\
0 & 0 & 1 & \cdots & \cdots & \theta^{k+1}(h_1) & \cdots & 0\\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots & & \\
0 & 0 & \cdots & \theta^{n-k}(h_{k-2}) & \cdots & \cdots & \cdots & \theta^{n-1}(h_0)
\end{bmatrix}.$$

Then each row of H^* is orthogonal to every element of C. Therefore each row vector of H^* is in $C^\perp$. Since C is a Frobenius ring, $|C||C^\perp| = |R|^n$. Also $|C| = |R|^k$, as deg $g(x) = n - k$. Therefore $|C^\perp| = |R|^{n-k}$. The rows of H^* are linearly independent. So the cardinality of the row span of H^* is $|R|^{n-k}$. Therefore H^* is a generator matrix of $C^\perp$. Since H^* is a circular matrix, the corresponding polynomial $h^*(x) = 1 + \theta(h_{k-1})x + \theta^2(h_{k-2})x^2 + \cdots + \theta^k(h_0)x^k$ is a generator polynomial of $C^\perp$.

■

Example 4.4.5. *Let C be a (θ, α)-constacyclic code of length 4 generated by the monic polynomial $g(x) = x^2+(2u+2)x+3u+3$ such that $x^4-\alpha = (x^2+(2u+2)x+u+1)(x^2+(2u+2)x+3u+3)$, where $\alpha = 1+2u$. If we take $h(x) = (x^2+(2u+2)x+u+1)$, then $h^*(x) = 1+\theta(2u+2)x+\theta^2(u+1)x^2 = (u+1)x^2+(2u+2)x+1$. $h^*(x)$ is also a right divisor of $x^4 - \alpha$, as by Lemma 4.4.2, we have*

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

Also as C is generated by a monic right divisor $g(x)$ of $x^4 - \alpha$, C is a free code with basis $\{g(x), xg(x)\}$. Hence a generator matrix for C is

$$G = \begin{bmatrix} 3u+3 & 2u+2 & 1 & 0 \\ 0 & 3u+1 & 2u+2 & 1 \end{bmatrix}.$$

Since $h^*(x) = (u+1)x^2 + (2u+2)x + 1$, the corresponding circular matrix is given by

$$H = \begin{bmatrix} 1 & 2u+2 & u+1 & 0 \\ 0 & 1 & 2u+2 & u+3 \end{bmatrix}.$$

It can easily be verified that the rows of H are R-linearly independent and $GH^T = 0$. Therefore H is a parity check matrix of C and hence a generator matrix of $C^\perp$. This shows that $h^*(x)$ is a generator polynomial of $C^\perp$ and $C^\perp = \langle h^*(x) \rangle$ is a (θ, α)-constacyclic code over R.

4.5 Double (θ, α)-constacyclic codes

In this section we study double (θ, α)-constacyclic codes over R.

For any $d \in R$ and $v = (a_0, a_1, \cdots, a_{n_1-1}, b_0, b_1, \cdots, b_{n_2-1}) \in R^{n_1+n_2}$, we define

$$dv = (da_0, da_1, \cdots, da_{n_1-1}, db_0, db_1, \cdots, db_{n_2-1}).$$

With this multiplication, $R^{n_1+n_2}$ is an R-module.

A double skew-linear code is an R-submodule of $R^{n_1+n_2}$.

Definition 4.5.1. *A double skew-linear code C is called double (θ, α)-constacyclic code if for a vector $v = (a_0, a_1, \cdots, a_{n_1-1}, b_0, b_1, \cdots, b_{n_2-1}) \in C$, its double (θ, α)-shift, i.e., the vector $(\alpha\theta(a_{n_1-1}), \theta(a_0), \theta(a_1), \theta(a_{n_1-2}), \alpha\theta(b_{n_2-1}), \theta(b_0), \theta(b_1), \cdots, \theta(b_{n_2-2}))$ is also in C.*

We define the multiplication of any $r(x) \in R[x, \theta]$ and $(g_1(x) \mid g_2(x)) \in R_{n_1,n_2} = \frac{R[x,\theta]}{\langle x^{n_1}-\alpha \rangle} \times \frac{R[x,\theta]}{\langle x^{n_2}-\alpha \rangle}$ as

$$r(x)(g_1(x) \mid g_2(x)) = (r(x)g_1(x) \mid r(x)g_2(x)),$$

where $r(x)g_1(x)$ and $r(x)g_2(x)$ are the multiplication of polynomials in $R[x, \theta]$. With this multiplication, R_{n_1,n_2} is a left $R[x, \theta]$-module.

Theorem 4.5.2. *A code C is a double (θ, α)-constacyclic code if and only if it is a left $R[x, \theta]$-submodule of the left module $R[x, \theta]/\langle x^{n_1} - \alpha \rangle \times R[x, \theta]/\langle x^{n_2} - \alpha \rangle$.*

Proof: Let C be a double (θ, α)-constacyclic code. Let $c \in C$, and let the associated polynomial of c be $c(x) = (a_1(x) \mid a_2(x))$. As $xc(x)$ is a double (θ, α)-shift of c, so $xc(x) \in C$. By linearity of C, $r(x)c(x) \in C$ for any $r(x) \in R[x, \theta]$. So C is a left $R[x, \theta]$-submodule of R_{n_1,n_2}. Converse is straightforward. ■

Theorem 4.5.3. *A double (θ, α)-constacyclic code is equivalent to a double α-constacyclic code or double cyclic code if n_1 and n_2 both are odd integers.*

Proof: Let C be a double (θ, α)-constacyclic code. Let $\gamma = lcm(n_1, n_2)$. Then γ is odd, and so $gcd(\gamma, 2) = 1$. Therefore there exist two integers a, b such that

$\gamma a + 2b = 1$ and so $2b = 1 - \gamma a = 1 + \gamma l$ for some $l > 0$, where $l = -a \pmod{\gamma}$. Let $c(x) = (a(x) \mid b(x)) \in C$, where $a(x) = \sum_{i=0}^{n_1-1} a_i x^i$ and $b(x) = \sum_{i=0}^{n_2-1} b_i x^i$.
Then

$$\begin{aligned}
x^{2b}c(x) &= x^{2b}\left(\sum_{i=0}^{n_1-1} a_i x^i \mid \sum_{i=0}^{n_2-1} b_i x^i\right) = \left(\sum_{i=0}^{n_1-1} \theta^{2b}(a_i)x^{i+2b} \mid \sum_{i=0}^{n_2-1} \theta^{2b}(b_i)x^{i+2b}\right)\\
&= \left(\sum_{i=0}^{n_1-1} \theta^{2b}(a_i)x^{i+1+\gamma l} \mid \sum_{i=0}^{n_2-1} \theta^{2b}(b_i)x^{i+1+\gamma l}\right)\\
&= \left(\sum_{i=0}^{n_1-2} a_i x^{i+1+\gamma l} + a_{n_1-1}x^{n_1+\gamma l} \mid \sum_{i=0}^{n_1-2} a_i x^{i+1+\gamma l} + a_{n_2-1}x^{n_2+\gamma l}\right)\\
&= \left(\sum_{i=0}^{n_1-2} a_i x^{i+1} + \alpha a_{n_1-1} \mid \sum_{i=0}^{n_2-2} a_i x^{i+1} + \alpha a_{n_2-1}\right),\\
&\quad (\text{as } x^{n_1} = x^{n_2} = x^{\gamma} = \alpha \text{ and } x^{\gamma l} = 1 \text{ or } \alpha).
\end{aligned}$$

Thus $x^{2b}c(x)$ is a double α-constacyclic shift of $c(x)$ if $x^{\gamma l} = 1$ or a double cyclic shift if $x^{\gamma l} = \alpha$. Hence the result. ■

Theorem 4.5.4. *Let C_1 and C_2 be two principally generated free (θ, α)-constacyclic codes of lengths n_1 and n_2 over R having monic generator polynomials $g_1(x)$ and $g_2(x)$, respectively, such that $g_1(x)|x^{n_1} - \alpha$ and $g_2(x)|x^{n_2} - \alpha$. Then a code C generated by $g(x) = (g_1(x) \mid g_2(x))$ is a double (θ, α)-constacyclic code and $A = \{g(x), xg(x), \cdots, x^{l-1}g(x)\}$ is a spanning set of C, where $l = deg\, h(x)$ and $h(x) = lcm\{h_1(x), h_2(x)\}$.*

Proof: Let $x^{n_1} - \alpha = h_1(x)g_1(x)$ and $x^{n_2} - \alpha = h_2(x)g_2(x)$ for some monic polynomial $h_1(x), h_2(x) \in R[x, \theta]$. Also let $h(x) = lcm\{h_1(x), h_2(x)\}$. Then $h(x)g(x) = h(x)(g_1(x)|g_2(x)) = 0$, as $h(x)g_i(x) = h'(x)h_i(x)g_i(x) = 0$ for $i = 1, 2$. Now let $v(x) \in C$ be any non-zero codeword in C. Then $v(x) = a(x)g(x)$ for some $a(x) \in R[x, \theta]$. By the division algorithm, we have $a(x) = q(x)h(x) + r(x)$, where $r(x) = 0$ or deg $r(x) <$ deg $h(x)$. Then $v(x) = a(x)g(x) = r(x)g(x) = 0$. Since $r(x) = 0$ or deg $r(x) <$ deg $h(x)$, the result follows. ■

In the following example, we use the Theorem 5.5.5 to combine two (θ, α)-constacyclic codes of different lengths and obtain a double (θ, α)-constacyclic code whose Gray image gives a new good $\mathbb{Z}_4$-linear code, and it improves the Lee distance of the existing best code with comparable parameters.

Example 4.5.5. *Let C be a double (θ, α)-constacyclic code of length 9 over R with $n_1 = 3$ and $n_2 = 6$ and with a generator matrix as follow:*

$$\begin{bmatrix} 1 & 1+2u & 1 & 1 & 0 & 1+2u & 0 & 1 & 0 \\ 1+2u & 1 & 1+2u & 0 & 1 & 0 & 1+2u & 0 & 1 \\ 1 & 2u+1 & 1 & 2u+1 & 0 & 1 & 0 & 2u+1 & 0 \end{bmatrix}.$$

The spanning set of C is $\{(g_1(x) \mid g_2(x)), x(g_1(x) \mid g_2(x)), x^2(g_1(x) \mid g_2(x))\}$ which is an R-linearly dependent set as $2(g_1(x) \mid g_2(x)) = 2x^2(g_1(x) \mid g_2(x))$, where $g_1(x) = x^2 + (1 + 2u)x + 1$, $g_2(x) = x^4 + (1 + 2u)x^2 + 1$ and $g_1(x)|x^3 - \alpha$, $g_2(x)|x^6 - \alpha$, where $\alpha = 1 + 2u$. The Gray image $\Phi(C)$ of C is a new good $\mathbb{Z}_4$- linear code with parameters $(\mathbf{18}, \mathbf{4^4 2^1}, \mathbf{10_L})$, and generator matrix

$$\begin{bmatrix} 1 & 0 & 3 & 2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 3 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 3 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 3 & 2 & 3 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 & 2 & 3 & 2 & 1 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \end{bmatrix},$$

which improves the minimum Lee distance by 4 when compared to the existing best known code $(18, 4^4 2^1, 6_L)$ [8].

4.5.1 Some more good codes

The following table shows the generator matrices and parameters of two more codes over $\mathbb{Z}_4$.

Code	Generator matrix	Parameters $(n, 4^{k_1} 2^{k_2}, d_L)$
C_1	G_1	$(18, 4^4 2^2, 7)$
C_2	G_2	$(18, 4^4 2^4, 7)$

where

$$G_1 = \begin{bmatrix} 1&0&0&0&1&0&2&3&0&1&0&1&2&3&2&3&0&3 \\ 0&1&0&0&0&1&1&0&3&2&3&2&1&0&1&0&1&2 \\ 0&0&1&0&1&0&0&0&2&1&0&0&0&3&0&0&2&1 \\ 0&0&0&1&0&1&0&0&3&0&0&0&1&2&0&0&3&0 \\ 0&0&0&0&2&0&2&2&2&2&2&2&2&2&2&2&2&0 \\ 0&0&0&0&0&2&2&2&2&2&2&2&2&2&2&2&0&2 \end{bmatrix}$$

and

$$G_2 = \begin{bmatrix} 1&0&0&0&1&0&0&1&0&1&0&3&2&3&0&1&2&1 \\ 0&1&0&0&0&1&1&0&3&2&1&0&3&0&3&0&3&0 \\ 0&0&1&0&1&0&0&0&2&1&0&0&0&3&0&0&2&1 \\ 0&0&0&1&0&1&0&0&3&0&0&0&1&2&0&0&3&0 \\ 0&0&0&0&2&0&0&0&2&2&0&2&0&0&2&2&0&2 \\ 0&0&0&0&0&2&0&0&2&2&0&2&2&2&0&0&2&0 \\ 0&0&0&0&0&0&2&2&0&0&0&2&2&0&0&2&0&0 \\ 0&0&0&0&0&0&0&0&0&0&2&2&2&2&2&2&0&0 \end{bmatrix}.$$

The code C_1 improves the Lee weight by 1 when compared to existing best code with comparable parameters. Also C_2 is a new code as there is no code with comparable parameters in the database of $\mathbb{Z}_4$-codes, and it further improves C_1 in cardinality.

4.6 Skew-cyclic codes over $\mathcal{R} = GR(4,2) + vGR(4,2)$

In this section, we study skew cyclic codes over the ring $GR(4,2)+vGR(4,2), v^2 = v$, where $GR(4,2)$ is the Galois ring extension of $\mathbb{Z}_4$ of degree 2.

4.6.1 About $\mathcal{R}[x, \Theta]$

We use the notation $\mathcal{R} = GR(4,2) + vGR(4,2)$, $v^2 = v$. $\mathcal{R}$ is a commutative semi-local ring with characteristic 4 and cardinality 16^2. It is isomorphic to the ring $GR(4,2)[v]/\langle v^2 - v\rangle$. The Galois ring $GR(4,2)$ is defined as $GR(4,2) \cong \frac{\mathbb{Z}_4[x]}{\langle f(x)\rangle} \cong \mathbb{Z}_4[\xi]$, where $f(x) = 1 + x + x^2$ is a basic primitive polynomial of degree 2 over $\mathbb{Z}_4$

and ξ is a root of $f(x)$. Thus ξ is a primitive element of $GR(4,2)$. Every element a of $GR(4,2)$ can uniquely be expressed as $a = a_1 + \xi a_2$, where $a_1, a_2 \in \mathbb{Z}_4$. Therefore an element $a + vb$ of $\mathcal{R}$ can be expressed as $a + vb = (a_1 + vb_1) + \xi(a_2 + vb_2)$, where $a_1, a_2, b_1, b_2 \in \mathbb{Z}_4$.

Define a map $\Theta : \mathcal{R} \to \mathcal{R}$ such that

$$\Theta(a + vb) = \Theta((a_1 + vb_1) + \xi(a_2 + vb_2)) = (a_1 + vb_1) + \xi^2(a_2 + vb_2)$$

for all $a + vb \in \mathcal{R}$. One can easily verify that Θ is an automorphism of $\mathcal{R}$ which fixes the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$. Moreover, when restricted to $GR(4,2)$, Θ is the Frobenius automorphism of $GR(4,2)$. The set $\mathcal{R}[x, \Theta]$ forms a skew polynomial ring in which the addition and multiplications are defined similarly as in the case of skew polynomial rings over fields.

The following version of right division algorithm holds for $\mathcal{R}[x, \Theta]$.

Lemma 4.6.1. *[74] Let $f, g \in \mathcal{R}[x, \Theta]$ be such that the leading coefficient of g is a unit. Then there exist $q, r \in \mathcal{R}[x, \Theta]$ such that $f = qg + r,\ r = 0$ or $deg(r) < deg(g)$.*

Theorem 4.6.2. *The center $Z(\mathcal{R}[x, \Theta])$ of $\mathcal{R}[x, \Theta]$ is $(\mathbb{Z}_4 + v\mathbb{Z}_4)[x^2]$.*

Proof: We know $\mathbb{Z}_4 + v\mathbb{Z}_4$ is the fixed ring of Θ. Since the order of Θ is 2, for any non-negative integer i, we have $x^{2i}a = \Theta^{2i}(a)x^{2i} = ax^{2i}$ for all $a \in \mathcal{R}$. It gives $x^{2i} \in Z(\mathcal{R}[x, \Theta])$, and hence all polynomials of the form $f = a_0 + a_1x^2 + a_2x^4 + \cdots + a_tx^{2t}$ with $a_i \in \mathbb{Z}_4 + v\mathbb{Z}_4$ are in the center. Conversely, for any $f = f_0 + f_1x + f_2x^2 + \cdots + f_kx^k \in Z(\mathcal{R}[x, \Theta])$ we have $fx = xf$ which gives that all f_i are fixed by Θ, so that $f_i \in \mathbb{Z}_4 + v\mathbb{Z}_4$. Further, choose $a \in \mathcal{R}$ such that $\Theta(a) \neq a$. Then it follows from the relation $af = fa$ that $f_i = 0$ for all odd indices i. Thus $f = a_0 + a_1x^2 + a_2x^4 + \cdots + a_tx^{2t} \in (\mathbb{Z}_4 + v\mathbb{Z}_4)[x^2]$.

Corollary 4.6.2.1. *Let $f = x^n - 1$. Then $f \in Z(\mathcal{R}[x, \Theta])$ if and only if n is even.*

We denote the skew-cyclic shift of a word $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{R}^n$ by $T_\Theta(c)$ and it is defined similarly as in the Definition 2.1.4. Thus a submodule C of $\mathcal{R}^n$ is a skew-cyclic code if $T_\Theta(C) = C$.

Definition 4.6.3. *A skew-linear code C of length n over the ring $\mathcal{R}$ is a left $\mathcal{R}[x,\Theta]$-submodule of left module $\frac{\mathcal{R}[x,\Theta]}{\langle f(x)\rangle}$, where $f(x)$ is a polynomial of degree n over $\mathcal{R}[x,\Theta]$.*

Theorem 4.6.4. *A code C of length n in $\mathcal{R}_n = \mathcal{R}[x,\Theta]/\langle x^n-1\rangle$ is a skew-cyclic code if and only if C is a left $\mathcal{R}[x,\Theta]$-submodule of the left $\mathcal{R}[x,\Theta]$-module $\mathcal{R}_n$.*

Proof: Straightforward. ■

Corollary 4.6.4.1. *For even n, a skew-linear code of length n over $\mathcal{R}$ is a skew-cyclic code if and only if C is a left ideal in $\mathcal{R}_n$.*

Proof: For even n, $x^n-1 \in Z(\mathcal{R}[x,\Theta])$, and so, $\mathcal{R}_n$ is a ring. The result follows.

Definition 4.6.5. *A skew-cyclic code of length n is said to be principally generated if it is a left cyclic submodule of $\mathcal{R}_n$, i.e., there exists $g(x) \in \mathcal{R}[x,\Theta]$ such that $C = \mathcal{R}g = \langle g(x)\rangle$.*

Next result shows a sufficient condition for a principally generated skew-cyclic code over $\mathcal{R}$ to be free, and is a generalization of [16, Theorem 2].

Theorem 4.6.6. *Let C be a skew-cyclic code of length n over $\mathcal{R}$. If there exists a monic polynomial $g(x)$ of minimal degree in $\mathcal{R}$. Then $C = \langle g(x)\rangle$ such that $g(x)$ is a right divisor of x^n-1 and C is a principally generated free skew-cyclic code of length n over $\mathcal{R}$.*

Proof: The proof is similar to the proof of Theorem 4.3.2 in Section 4.3. ■

Theorem 4.6.7. *Let C be a skew-cyclic code of length n over $\mathcal{R}$ generated by a monic polynomial $g(x)$ which is a right divisor of x^n-1, i.e $x^n-1 = h(x)g(x)$ for some $h(x) \in \mathcal{R}[x,\Theta]$. Then a polynomial $f(x) = p(x)g(x)$ will generate the same code C if and only if $p(x)$ and $h(x)$ are right co-prime.*

Proof: The proof is similar to the proof of [16, Theorem 3]. ■

Theorem 4.6.8. *Let C be a skew-cyclic code of odd length n over $\mathcal{R}$. Then C is a cyclic code over $\mathcal{R}$.*

Proof: The proof is similar to that of Theorem 4.3.7 in this chapter. ■

Theorem 4.6.9. *Let C be a free skew-cyclic code of even length n generated by a monic right divisor $g(x)$ of $x^n - 1$. Then C is a cyclic code over $\mathcal{R}$ if and only if all the coefficient of $g(x)$ are fixed under the automorphism Θ of $\mathcal{R}$.*

Proof: The proof is similar to that of Theorem 4.3.8. ■

Theorem 4.6.10. *Let C be a skew-cyclic code of even length n over $\mathcal{R}$. Then C is equivalent to a quasi-cyclic code of index 2 over $\mathcal{R}$.*

Proof: By letting $n = 2N$, we can write $c \in \mathcal{R}$ as $c = (c_{0,0}, c_{0,1}, c_{1,0}, c_{1,1}, \cdots, c_{N-1,0}, c_{N-1,1})$. Since Θ^2 is the identity map, and $T_\Theta^i(c) \in C$ for all i, so we have $T_\Theta^2(c) = (c_{N-1,0}, c_{N-1,1}, c_{0,0}, c_{0,1}, \cdots, c_{N-2,0}, c_{N-2,1}) \in C$. Therefore C is equivalent to a quasi-cyclic code of index 2.

4.6.2 Duals of skew-cyclic codes over $\mathcal{R}$

Lemma 4.6.11. *Let C be a skew-cyclic code of even length n over $\mathcal{R}$. Then $\Theta(a \cdot T_\Theta^j(b)) = T_\Theta(a) \cdot T_\Theta^{j+1}(b)$ for all $a \in C^\perp$ and $b \in C$, for any $j \geq 0$.*

Proof: Let $a = (a_0, a_1, \cdots, a_{n-1}) \in C^\perp$ and $b = (b_0, b_1, \cdots, b_{n-1}) \in C$. By definition $T_\Theta(a) = (\Theta(a_{n-1}), \Theta(a_0), \cdots, \Theta(a_{n-2}))$ and $T_\Theta^{j+1}(b) = (\Theta^{j+1}(b_{n-j-1}), \Theta^{j+1}(b_{n-j}), \cdots,$ $\Theta^{j+1}(b_{n-j-2}))$, where i, j are fixed indices. Therefore $T_\Theta(a) \cdot T_\Theta^{j+1}(b) = \Theta(a_{n-1})\Theta^{j+1}(b_{n-j-1}) + \Theta(a_0)\Theta^{j+1}(b_{n-j}) + \cdots + \Theta(a_{n-2})\Theta^{j+1}(v_{i,n-j-2}) = \Theta[a_{n-1}\Theta^j(b_{n-j-1}) + a_0\Theta^j(b_{n-j}) + \cdots + a_{n-2}\Theta^j(b_{n-j-2})] = \Theta(a \cdot T_\Theta^j(b))$. Therefore $\Theta(a \cdot T_\Theta^j(b)) = T_\Theta(a) \cdot T_\Theta^{j+1}(b)$.

Theorem 4.6.12. *If C is skew-cyclic code of even length n over $\mathcal{R}$, then $C^\perp$ is also skew-cyclic of length n over $\mathcal{R}$.*

Proof: Any element c of C can be expressed as $T_\Theta^j(b)$ for some integer $0 \leq j \leq n-1$ and $b \in C$, as n is even, and so $T_\Theta^n(c) = c$ for all c in $\mathcal{R}^n$. To show that $C^\perp$ is also a skew-cyclic code, it is sufficient to show that for any $a \in C^\perp$, we have $T_\Theta(a) \cdot T_\Theta(c) = 0$ for all $c \in C$. However this follows from Lemma 4.6.11, and the fact that if $a \cdot c = 0$, then $\Theta(a \cdot c) = \Theta(0) = 0$. Hence the result.

4.7 A decomposition of skew-cyclic codes over $\mathcal{R}$

The ring $\mathcal{R} = \frac{\mathcal{R}_1[v]}{\langle v^2-v\rangle}$, where $\mathcal{R}_1 = GR(4,2)$ can be written as

$$\mathcal{R} = vGR(4,2) + (1-v)GR(4,2)$$

by the Chinese Remainder Theorem.

Let C be a skew-linear code of length n over $\mathcal{R}$. Define

$$C_1 = \{x \in \mathcal{R}_1^n \mid \exists\ y \in \mathcal{R}_1^n, vx + (1-v)y \in C\}$$

$$C_2 = \{y \in \mathcal{R}_1^n \mid \exists\ x \in \mathcal{R}_1^n, vx + (1-v)y \in C\}.$$

Clearly, C_1 and C_2 are skew-linear codes of length n over $\mathcal{R}_1$, and C can be expressed as

$$C = vC_1 \oplus (1-v)C_2.$$

Theorem 4.7.1. *Let $C = vC_1 \oplus (1-v)C_2$ be a skew-linear code over $\mathcal{R}$. Then C is a skew-cyclic code over $\mathcal{R}$ if and only if C_1, C_2 are skew-cyclic codes over $\mathcal{R}_1$.*

Proof: Let T_Θ denote the skew-cyclic shift operator on C as well as on C_i for $i = 1, 2$. For any $c \in C$, we have $T_\Theta(c) = vT_\Theta(c_1) + (1-v)T_\Theta(c_2)$, where $c = vc_1 + (1-v)c_2$. Suppose C_1, C_2 are skew- cyclic codes over $\mathcal{R}_1$. Then $T_\Theta(c_i) \in C_i$ for $i = 1, 2$ and so $T_\Theta(c) \in C$.

Conversely, suppose C is a skew-cyclic code over $\mathcal{R}$. Then $T_\Theta(c) \in C$ for all $c \in C$. This implies that $vT_\Theta(c_1) + (1-v)T_\Theta(c_2) \in C$, and so by the definitions of C_1 and C_2, $T_\Theta(c_1) \in C_1$ and $T_\Theta(c_2) \in C_2$. Hence the result. ■

The following Theorem is generalization of [42, Proposition 3].

Theorem 4.7.2. *Let C be a skew-linear code of length n over $\mathcal{R}$. Then $C^\perp = vC_1^\perp \oplus (v-1)C_2^\perp$. Moreover,*

(i) if C is a skew-cyclic code of length n over $\mathcal{R}$, then $C^\perp$ is also a skew-cyclic code of length n over $\mathcal{R}$.

(ii) *C is self-dual skew-cyclic code of length n over $\mathcal{R}$ if and only if C_1 and C_2 both are self-dual skew-cyclic codes of length n over $\mathcal{R}_1$.*

Proof: Define

$$A = \{x \in {\mathcal{R}_1}^n \mid \exists\; y \in {\mathcal{R}_1}^n,\; vx + (1-v)y \in C^{\perp}\}$$

$$B = \{y \in {\mathcal{R}_1}^n \mid \exists\; x \in {\mathcal{R}_1}^n,\; vx + (1-v)y \in C^{\perp}\}.$$

Clearly $C^{\perp} = vA \oplus (1-v)B$. If $x = va + (1-v)b \in C$ and $y = vc + (1-v)d \in C^{\perp}$, then $x \cdot y = 0$ gives $a \cdot c = 0$ and $b \cdot d = 0$, as $v^2 = v$. Therefore $A \subseteq {C_1}^{\perp}$, since for any $c \in A$, $a \cdot c = 0$ for all $a \in C_1$. In the reverse direction, let $e \in {C_1}^{\perp}$ and $x = va + (1-v)b \in C$. Then $ve \cdot x = 0$, and so, $ve \in C^{\perp}$. Due to the unique expression of elements of $C^{\perp}$, we have $e \in A$. So $A = C_1^{\perp}$. Similarly $B = {C_2}^{\perp}$.

(i) Let C be a skew-cyclic code over $\mathcal{R}$. Then C_1 and C_2 are skew-cyclic codes over $\mathcal{R}_1$ by Theorem 7.1. Therefore ${C_1}^{\perp}$ and ${C_2}^{\perp}$ are skew-cyclic codes over $\mathcal{R}_1$, since the dual of a skew-cyclic code over $\mathcal{R}_1$ is a skew-cyclic code. Again by Theorem 7.1 and the above discussion, $C^{\perp}$ is a skew-cyclic code over $\mathcal{R}$.

(ii) Suppose C_1 and C_2 are self-dual skew-cyclic codes over $\mathcal{R}_1$. Then C is a self-dual skew-cyclic code over $\mathcal{R}$, as $C^{\perp} = vC_1^{\perp} \oplus (1-v)C_2^{\perp}$. Conversely, if C is a self-dual skew-cyclic code over $\mathcal{R}$, then C_1 and C_2 are self orthogonal codes over $\mathcal{R}_1$, i.e $C_1 \subseteq {C_1}^{\perp}$ and $C_2 \subseteq {C_2}^{\perp}$. Let $e \in {C_1}^{\perp}$. Then there exists $l \in \mathcal{R}_1$ such that $ve + (1-v)l \in C^{\perp} = C$. By the uniqueness of the expressions of elements of C, $e \in C_1$, and so $C_1^{\perp} = C_1$. Similarly ${C_2}^{\perp} = C_2$. Hence the result.

For any element $a + vb \in \mathcal{R}$, where $a, b \in GR(4,2)$, define a Gray map $\varphi : \mathcal{R} \to GR(4,2)^2$ by $\varphi(a + vb) = (a + b, a)$. It can easily be proved that φ is a ring isomorphism and can be extended (denoted by the same symbol φ) componentwise to $\varphi : \mathcal{R}^n \to GR(4,2)^{2n}$. The Gray weight ($w_G$) of any $x = a + vb \in \mathcal{R}^n$ is defined as the Hamming weight of its Gray image, i.e., $w_G(x) = w_H(\varphi(x)) = w_H(a + b, a)$.

Lemma 4.7.3. *The Gray map $\varphi : \mathcal{R}^n \to {GR(4,2)}^{2n}$ is a $GR(4,2)$-linear and distance preserving map.*

Proof: Let $x = a+vb \in \mathcal{R}^n$ and $\varphi(x) = (a+b, a)$. Then clearly $\varphi(x+y) = \varphi(x)+\varphi(y)$ and $\varphi(ex) = e\varphi(x)$ for any $e \in GR(4, 2)$. Therefore φ is $GR(4, 2)$-linear. Now $d_G(x, y) = w_G(x - y) = w_H(\varphi(x - y)) = w_H(\varphi(x) - \varphi(y)) = d_H(\varphi(x), \varphi(y))$. Hence the result.

Theorem 4.7.4. *Let C be a skew-linear code of length n over $\mathcal{R}$. Then $\varphi(C) = C_1 \otimes C_2$ and $|C| = |C_1||C_2|$. Moreover $\varphi(C)$ is also a skew-linear code of length $2n$ over $GR(4, 2)$.*

Proof: Since $C = vC_1+(1-v)C_2$, where C_1, C_2 are as defined above. Let $x \in \varphi(C)$. Then there exists $va + (1 - v)b \in C$ such that $x = \varphi(va + (1 - v)b) = (a, b)$. It gives $x \in C_1 \otimes C_2$, and so $\varphi(C) \subseteq C_1 \otimes C_2$.

Conversely, let $(a, b) \in C_1 \otimes C_2$. Since $a \in C_1$ and $b \in C_2$, we have $x = av + (1 - v)b \in C$. Also $\varphi(x) = (a, b)$, gives $(a, b) = \varphi(x) \in \varphi(C)$. Hence $\varphi(C) = C_1 \otimes C_2$. Also $|C| = |\varphi(C)|$, so $|C| = |C_1||C_2|$.

For the second part, since φ is a linear map, so $\varphi(C)$ is also a linear code. Also, $\varphi(C)$ is obviously a code of length $2n$. ■

Theorem 4.7.5. *Let C be a skew-linear code of length n over $\mathcal{R}$. If C is self-dual, then $\varphi(C)$ is a skew-linear self-dual code of length $2n$ over $GR(4, 2)$.*

Proof: Let $x = va + (1 - v)b \in C$ and $y = vc + (1 - v)d \in C^\perp$. Then $x \cdot y = 0$, and so $a \cdot c = 0$ and $b \cdot d = 0$. Also $\varphi(x) \cdot \varphi(y) = (a, b) \cdot (c, d) = (a \cdot c, b \cdot d) = (0, 0)$. It shows that $\varphi(C^\perp) \subseteq \varphi(C)^\perp$. Further, we have $|C| = 16^n$, as C is self-dual and $|C||C^\perp| = |\mathcal{R}|^n$. Since $|C| = |\varphi(C)|$, we have $|\varphi(C)| = |\varphi(C)^\perp)| = 16^n$. Hence $\varphi(C) = \varphi(C)^\perp$. $\varphi(C)$ is thus a self-dual code of length $2n$ over $GR(4, 2)$.

Theorem 4.7.6. *Let C be a skew-cyclic code of length n over $\mathcal{R}$. Then $\varphi(C)$ is a skew-2-quasi cyclic code of length $2n$ over $GR(4, 2)$.*

Proof: Since $\varphi(C) = C_1 \otimes C_2$, where both C_1 and C_2 are skew-cyclic codes over $GR(4, 2)$, therefore C_1, C_2 are left $GR(4, 2)[x, \Theta]$-submodules of the left module $\frac{GR(4,2)[x,\Theta]}{\langle x^n-1\rangle}$. Now by the definition of a 2-quasi cyclic code, and the fact that $\varphi(C)$ is a $GR(4,2)[x,\Theta]$-submodule of the left module $[\frac{GR(4,2)[x,\Theta]}{\langle x^n-1\rangle}]^2$, it follows that $\varphi(C)$ is a skew 2-quasi cyclic code of length $2n$ over $GR(4,2)$.

4.8 Conclusion

We have studied a class of skew-constacyclic code over a ring $\mathbb{Z}_4+u\mathbb{Z}_4, u^2=0$. A new good $\mathbb{Z}_4$-linear code $(\mathbf{6}, \mathbf{4^4 2^2}, \mathbf{2_L})$ is obtained through this class. For even length, dual of these codes are discussed and a relation between the generator polynomial of a code and that of its dual is shown. These codes have been then generalized to double skew-constacyclic codes, and we have obtained new good $\mathbb{Z}_4$-linear codes with parameters $(\mathbf{18}, \mathbf{4^4 2^1}, \mathbf{10_L})$, $(\mathbf{18}, \mathbf{4^4 2^2}, \mathbf{7_L})$ and $(\mathbf{18}, \mathbf{4^4 2^4}, \mathbf{7_L})$ via the Gray map. Further, we have extended this study by defining a class of skew-cyclic codes over $GR(4,2)+vGR(4,2), v^2=v$.

Chapter 5

Skew-cyclic Codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$ with Derivation

5.1 Introduction

After their introduction by Boucher et al. [26], skew-cyclic codes have been generalized in many ways [27, 28, 29, 58, 96, 16, 48]. However, almost all this work has been done in the setting of skew-polynomial rings with automorphism only. In [30], Boucher et al. studied linear codes using skew-polynomial rings with automorphism and derivation. In this chapter, we have considered a class of skew-cyclic codes in the setting of the skew polynomial ring $R[x, \theta, \delta_\theta]$, where $R = \mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$; θ is an automorphism of R, and δ_θ is a derivation on R.

5.2 Properties of $R = \mathbb{Z}_4 + w\mathbb{Z}_4$

In this section, we present some basic definitions and results that are necessary to understand the further results.

We fix the notation $R = \mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$ for this chapter. Note that $R \cong \frac{Z_4[w]}{\langle w^2-1\rangle}$. An element $a + wb \in R$ is a unit if and only if exactly one of a and b is a unit. Therefore the units of R are

$$1, 3, w, 3w, w+2, 2w+3, 2w+1, 3w+2.$$

In a finite ring, an element is either a unit or a zero divisor. Hence the non-units of R are

$$0, 3w+3, 2w+2, w+1, 2, 3w+1, 2w, w+3.$$

There are total 7 ideals of R (including the zero ideal), and they form a lattice with inclusion operation whose (lattice) diagram is shown in Figure 5.2.

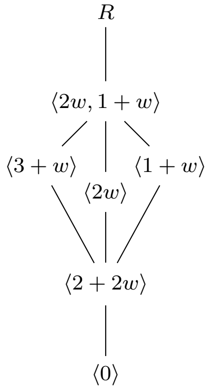

Figure: 5.2

In Figure 5.2, we have

$\langle 0\rangle = \{0\}$,

$\langle 2w\rangle = \{0, 2w, 2, 2+2w\}$,

$\langle 1+w\rangle = \{0, 1+w, 2+2w, 3+3w\}$,

$\langle 3+w\rangle = \{0, w+3, 2w+2, 3w+2\}$,

$\langle 2+2w\rangle = \{0, 2w+2\}$,

$\langle 2w, 1+w\rangle = \{3w+3, 0, 2w+2, w+1, 2, 3w+1, 2w, w+3\}$,

$\langle 1\rangle = R$.

Thus R is a local-ring having $\langle 2w, 1+w\rangle$ its unique maximal ideal. To know more about the ring R, we refer to [77, 93].

Define a map $\theta : R \to R$ such that

$$\theta(a+wb) = a + (w+2)b.$$

One can easily verify that θ is an automorphism of R. Moreover, since $\theta^2(x) = x$ for all $x \in R$, and θ is not the identity map, the order of θ is 2.

Definition 5.2.1. *Let* $\mathbf{R}$ *be a finite ring and* Θ *be an automorphism of* $\mathbf{R}$. *Then a map* $\Delta_\Theta : \mathbf{R} \to \mathbf{R}$ *is said to be a derivation on* $\mathbf{R}$ *if*

$$\Delta_\Theta(x+y) = \Delta_\Theta(x) + \Delta_\Theta(y) \text{ and } \Delta_\Theta(xy) = \Delta_\Theta(x)y + \Theta(x)\Delta_\Theta(y).$$

We define a map $\delta_\theta : R \to R$ such that

$$\delta_\theta(a+wb) = (1+w)(\theta(a+wb) - (a+wb)).$$

That is, $\delta_\theta(a+wb) = (1+w)(a+wb+2b-a-wb) = 2b+2wb.$

Theorem 5.2.2. *The map* δ_θ *is a derivation on* R.

Proof: Let $x, y \in R$. Then by definition,

$$\begin{aligned}
\delta_\theta(x+y) &= (1+w)(\theta(x+y) - (x+y)) \\
&= (1+w)(\theta(x) - x) + (1+w)(\theta(y) - y) \\
&= \delta_\theta(x) + \delta_\theta(y).
\end{aligned}$$

Also,

$$\begin{aligned}
\delta_\theta(xy) &= (1+w)(\theta(xy) - xy) \\
&= (1+w)\theta(x)\theta(y) - (1+w)xy \\
&= (1+w)\theta(x)\theta(y) - (1+w)xy + (1+w)\theta(x)y - (1+w)\theta(x)y \\
&= (1+w)\theta(x)(\theta(y) - y) - (1+w)(x - \theta(x))y \\
&= \theta(x)(1+w)(\theta(y) - y) + (1+w)(\theta(x) - x)y \\
&= \delta_\theta(x)y + \theta(x)\delta_\theta(y).
\end{aligned}$$

Thus δ_θ is a derivation on R. ■

The following table gives images of elements of R under δ_θ.

x	0	1	2	3	w	$2w$	$3w$	$1+w$
$\delta_\theta(x)$	0	0	0	0	$2+2w$	0	$2+2w$	$2+2w$
x	$1+2w$	$1+3w$	$2+w$	$2+2w$	$2+3w$	$3+w$	$3+2w$	$3+3w$
$\delta_\theta(x)$	0	$2+2w$	$2+2w$	0	$2+2w$	$2+2w$	0	$2+2w$

Remark 5.2.2.1. *We note that for* $n \geq 2$, *we have* ${\delta_\theta}^n(x) = 0$ *for all* $x \in R$.

5.2.1 Skew polynomial ring $\mathbf{R}[x, \Theta, \Delta_\Theta]$

Let $\mathbf{R}$ be a ring with automorphism Θ and derivation Δ_Θ. Then the skew polynomial ring $\mathbf{R}[x, \Theta, \Delta_\Theta]$ is the set of all polynomials over $\mathbf{R}$ with addition as the ordinary addition of polynomials and multiplication defined by

$$xa = \Theta(a)x + \Delta_\Theta(a) \tag{5.1}$$

for any $a \in \mathbf{R}$, which is then extended to all elements of $\mathbf{R}[x, \Theta, \Delta_\Theta]$ in the usual manner. The following example illustrates it.

Example 5.2.3. *Let $f = x^2 + a_0x + a_1$ and $g = x + b_0$ are in $R[x, \theta, \delta_\theta]$. Then*

$$f + g = x^2 + (a_0 + 1)x + a_1 + b_0 = g + f.$$

Also,

$$\begin{aligned} fg &= (x^2 + a_0x + a_1)(x + b_0) \\ &= x^2(x + b_0) + a_0x(x + b_0) + a_1(x + b_0) \\ &= x^3 + b_0x^2 + a_0x^2 + a_0(\theta(b_0)x + \delta_\theta(b_0)) + a_1x + a_1b_0 \quad \textit{(By Corollary 5.2.6.1)} \\ &= x^3 + (b_0 + a_0)x^2 + (a_0\theta(b_0) + a_1)x + a_0\delta_\theta(b_0) + a_1b_0 \end{aligned}$$

and

$$\begin{aligned} gf &= (x + b_0)(x^2 + a_0x + a_1) \\ &= x(x^2 + a_0x + a_1) + b_0(x^2 + a_0x + a_1) \\ &= x^3 + (\theta(a_0)x + \delta_\theta(a_0))x + (\theta(a_1)x + \delta_\theta(a_1)) + b_0x^2 + b_0a_0x + b_0a_1 \\ &= x^3 + (\theta(a_0) + b_0)x^2 + (\delta_\theta(a_0) + \theta(a_1) + b_0a_0)x + \delta_\theta(a_1) + b_0a_1. \end{aligned}$$

Therefore $fg \neq gf$. Thus $R[x, \theta, \delta_\theta]$ is a non-commutative ring.

Let $R^\theta = \{0, 1, 2, 3, 2w, 1 + 2w, 3 + 2w, 2 + 2w\}$. Then R^θ is a subring of R, fixed elementwise by θ, i.e., $\theta(a) = a$ for all $a \in R^\theta$. Also $\delta_\theta(a) = 0$ for all $a \in R^\theta$. Therefore we have $xa = ax$ for all $a \in R^\theta$.

As usual $R[x, \theta, \delta_\theta]$ is not a unique factorization ring, we often have more factors of a polynomial in $R[x, \theta, \delta_\theta]$ than in $R[x]$ (shown in Example 5.3.12 below).

Lemma 5.2.4. *Let $a \in R$. Then $\theta(a) - a \neq \delta_\theta(b)$ for any $b \in R$ unless a, b both are fixed by θ.*

Proof: Let $\theta(a) - a = \delta_\theta(b)$ for some arbitrary fixed values of a and b. The only possible values of $\delta_\theta(b)$ are 0 and $2w + 2$. If $\delta_\theta(b) = 0$, then a and b both are fixed by θ and we are done. Suppose $\delta_\theta(b) = 2w + 2$. But $\theta(a) - a$ does not contain w, we get a contradiction. Hence the result. ■

If we consider the skew polynomial ring over R with automorphism only, i.e., $R[x, \theta]$, then the center of $R[x, \theta]$ is $R^\theta[x^2]$ [74]. However, in the present case, i.e., in $R[x, \theta, \delta_\theta]$, we have the following result.

Theorem 5.2.5. *A polynomial $f(x) \in R[x, \theta, \delta_\theta]$ is a central element if and only if $f(x) \in R^\theta[x]$ such that the coefficients of all odd powers of x belong to the set $S = \{0, 2, 2w, 2 + 2w\}$.*

Proof: We prove the result for a polynomial of odd degree. It can be proved similarly for polynomials of even degree. Let $f(x) = f_0 + f_1 x + \cdots + f_k x^k \in R[x, \theta, \delta_\theta]$ be a polynomial of odd degree. Suppose $f(x)$ is a central element. Then

$$\begin{aligned} 0 &= xf(x) - f(x)x \\ &= \delta_\theta(f_0) + \sum_{i=0}^{k-1} (\theta(f_i) + \delta_\theta(f_{i+1}))x^{i+1} + \theta(f_k)x^{k+1} - \sum_{i=0}^{k} f_i x^{i+1}. \end{aligned}$$

Equating coefficients of all terms to zero we get

$$\delta_\theta(f_0) = 0, \tag{5.2}$$

$$(\theta(f_i) - f_i + \delta_\theta(f_{i+1})) = 0 \text{ for } i = 0, 1, 2, \cdots, k-1 \tag{5.3}$$

$$\theta(f_k) - f_k = 0. \tag{5.4}$$

From Equations (3), (4), (5) and Lemma 5.2.4, we have all f_i's fixed by θ, $i = 0, 1, \cdots, k$.

Again since $f(x)$ is a central element, we have $f(x)a = af(x)$ for all $a \in R$.

Choose $a \in R$, which is not fixed by θ, i.e., $\theta(a) \neq a$. Then

$$\begin{aligned} 0 &= af(x) - f(x)a \\ &= \sum_{i=0}^{k} af_i x^i - \sum_{j=0}^{\frac{k-1}{2}} (f_{2j}a + f_{2j+1}\delta_\theta(a))x^{2j} - \sum_{l=0}^{\frac{k-1}{2}} f_{2l+1}\theta(a)x^{2l+1} \\ &= \sum_{j=0}^{\frac{k-1}{2}} (af_{2j} - f_{2j}a - f_{2j+1}\delta_\theta(a))x^{2j} + \sum_{j=0}^{\frac{k-1}{2}} (af_{2l+1} - f_{2l+1}\theta(a))x^{2l+1} \\ &= \sum_{j=0}^{\frac{k-1}{2}} (f_{2j+1}\delta_\theta(a))x^{2j} - \sum_{j=0}^{\frac{k-1}{2}} f_{2l+1}(a - \theta(a))x^{2l+1}. \end{aligned}$$

This implies that $f_{2l+1}(a-\theta(a)) = 0$ and $f_{2j+1}(\delta_\theta(a)) = 0$ for all $j, l = 0, 1, 2, \cdots \frac{k-1}{2}$. Since all f_i are fixed, the coefficients f_{2l+1} which satisfy the above conditions are precisely the elements of S. Combining both the cases we get the required result.

Conversely, suppose $f(x)$ satisfies the given conditions. Then to show that $f(x)a(x) = a(x)f(x)$ for all $a(x) \in R[x, \theta, \delta_\theta]$, it is sufficient to show that $(a_ix^i)(f_jx^j) = (f_jx^j)(a_ix^i)$ for $0 \leq i \leq$ deg $a(x)$ and $0 \leq j \leq$ deg $f(x)$. We have

$$(a_ix^i)(f_jx^j) = a_if_jx^{i+j}, \text{as all } f_i \text{ are fixed by } \theta. \tag{5.5}$$

Also,

$$(f_jx^j)(a_ix^i) = \begin{cases} f_ja_ix^{i+j}, & \text{if } j \text{ is even} \\ f_j(\theta(a_i)x + \delta_\theta(a_i))x^{i+j-1}, & \text{if } j \text{ is odd.} \end{cases} \tag{5.6}$$

If j is odd and $f_j \in S$, then $f_j\delta_\theta(a) = 0$ and $f_j\theta(a) = f_ja$ for all $a \in R$, and so (6) gives

$$(f_jx^j)(a_ix^i) = f_j(\theta(a_i)x + \delta_\theta(a_i))x^{i+j-1} = f_ja_ix^{i+j}. \tag{5.7}$$

Therefore by (5), (6), (7), we have the required result. ■

Lemma 5.2.6. *For any element $a \in R$, $\delta_\theta(\theta(a)) + \theta(\delta_\theta(a)) = 0$. Also, $x^2a = ax^2 \ \forall \ a \in R$.*

Proof: Let $a = a' + wb' \in R$. Then $\delta_\theta(\theta(a)) = \delta_\theta(a' + (w+2)b') = 2b' + 2wb'$, and $\theta(\delta_\theta(a)) = \theta(2b' + 2wb') = 2b' + 2wb' = -(2b' + 2wb') = -\delta_\theta(\theta(a))$, which proves the first part. Further, $xa = \theta(a)x + \delta_\theta(a)$. Multiplying both sides by

x, we get $x^2a = x\theta(a)x + x\delta_\theta(a) = [\theta^2(a)x + \delta_\theta(\theta(a)]x + \theta(\delta_\theta(a))x + {\delta_\theta}^2(a) = ax^2 + [\delta_\theta(\theta(a)) + \theta(\delta_\theta(a))]x + {\delta_\theta}^2(a) = ax^2$, using the first part of this lemma and noting that ${\delta_\theta}^2(a) = 0$ for all $a \in R$. ■

Corollary 5.2.6.1. *For any element $a \in R$,*

$$x^n a = \begin{cases} (\theta(a)x + \delta_\theta(a))x^{n-1}, & \text{if } n \text{ is odd} \\ ax^n, & \text{if } n \text{ is even.} \end{cases}$$

The ring $R[x, \theta, \delta_\theta]$ is not a left/right Euclidean ring, so division algorithm does not hold in it. But we can still apply division algorithm on some particular elements of $R[x, \theta, \delta_\theta]$. This is given by the next result.

Theorem 5.2.7 (Right division algorithm)**.** *Let $f(x), g(x) \in R[x, \theta, \delta_\theta]$ be such that $g(x)$ has leading coefficient a unit. Then*

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

for some $q(x), r(x) \in R[x, \theta, \delta_\theta]$, where $r(x) = 0$ or deg $r(x)$ <deg $g(x)$.

Proof: Let $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_rx^r$ and $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_sx^s$, where g_s is a unit. If $r < s$, then $f(x) = 0 \cdot g(x) + f(x)$ gives the required result. Suppose $r \geq s$. We define a polynomial $h(x) = f(x) - A(x)g(x)$, where

$$A(x) = \begin{cases} f_r\theta(g_s^{-1})x^{r-s}, & \text{if } r - s \text{ is odd} \\ f_rg_s^{-1}x^{r-s}, & \text{if } r - s \text{ is even} \end{cases}.$$

Clearly, $h(x)$ is a polynomial of degree one less than the degree of $f(x)$. We prove the result by implementing induction on deg $f(x)$. Assume that the result is true for every polynomial having degree less than deg $f(x)$. Obviously result is true for deg $f(x) = 0$. So let deg $f(x) > 0$. Since deg $h(x) <$ deg $f(x)$, there exist $q_1(x)$, $r_1(x)$ such that $h(x) = q_1(x)g(x) + r_1(x)$, where $r_1(x) = 0$ or deg $r_1(x) <$ deg $g(x)$ and so $f(x) = q_1(x)g(x) + r_1(x) + A(x)g(x) = (q_1(x) + A(x))g(x) + r_1(x)$. Thus we obtain $f(x) = q(x)g(x) + r(x)$, where $q(x) = q_1(x) + A(x)$ and $r(x) = r_1(x)$. Hence the result. ■

A left division algorithm can similarly be proved. In this chapter, division always means a right division.

Example 5.2.8. *Consider the polynomials $f(x), g(x) \in R[x, \theta, \delta_\theta]$ such that $f(x) = (1 + w)x^2 + (2 + 2w)x + w$ and $g(x) = wx + (1 + w)$. Here $r = 2, s = 1, f_2 = 1 + w, g_1 = w$. Let $A(x) = f_2\theta(g_1^{-1})x^{2-1} = (1 + w)(w + 2)x = (3w + 3)x$. Then*

$$\begin{aligned} A(x)g(x) &= (3w+3)x(wx+(1+w)) \\ &= (3w+3)(\theta(w)x+\delta_\theta(w))x+(3w+3)(\theta(1+w)x+\delta_\theta(1+w)) \\ &= (3w+3)((w+2)x+2+2w)x+(3w+3)((w+3)x+2+2w) \\ &= (w+1)x^2+0.x+0.x+0 \\ &= (w+1)x^2 \end{aligned}$$

We define $h(x) = f(x) - A(x)g(x) = (2 + 2w)x + w$. Now repeating the above argument on $h(x)$, we get $h(x) = (2+2w)g(x)+w$, and so $f(x) = h(x)+A(x)g(x) = (2 + 2w)g(x) + w + (3w + 3)xg(x) = ((2 + 2w) + (3w + 3)x)g(x) + w$. Therefore we have $f(x) = q(x)g(x) + r(x)$, where $q(x) = (2 + 2w) + (3w + 3)x$ and $r(x) = w$.

5.2.2 Gray map

On $\mathbb{Z}_4$, the Lee weight (w_L) is defined as $w_L(0) = 0,\ w_L(1) = 1,\ w_L(2) = 2,\ w_L(3) = 1$. The Lee weight $w_L(w)$ of a vector $w \in {\mathbb{Z}_4}^2$ is then defined as the rational sum of the Lee weights of its coordinates. Define a Gray map $\phi : R \to {\mathbb{Z}_4}^2$ such that

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

For any $x \in R$, we define the Gray weight $w_G(x)$ of x as $w_G(x) = w_L(\phi(x))$. The Gray weights of the elements of R are as follows:

x	0	1	2	3	w	$2w$	$3w$	$1+w$
$w_G(x)$	0	1	2	1	2	4	2	3
x	$1+2w$	$1+3w$	$2+w$	$2+2w$	$2+3w$	$3+w$	$3+2w$	$3+3w$
$w_G(x)$	3	1	2	2	2	1	3	3

The map ϕ is extended componentwise to $\Phi : R^n \to {\mathbb{Z}_4}^{2n}$, and we define the Gray weight of $x \in R^n$ as the rational sum of Gray weights of its coordinates.

Now onward, we write the parameters of a linear code C over $\mathbb{Z}_4$ as $(n, 4^{k_1}2^{k_2}, d_L)$, and say that the type of the code is $4^{k_1}2^{k_2}$, where d_L denotes the minimum Lee distance of C.

Theorem 5.2.9. *(Lee Distance Bound [39]) "If C is a linear code of length n over $\mathbb{Z}_4$ with parameters $(n, 4^{k_1}2^{k_2}, d_L)$, then $d_L \leq 2n - 2k_1 - k_2 + 1$."*

A linear code over $\mathbb{Z}_4$ which satisfies the above bound with equality is called a *Maximum Lee Distance Separable (MLDS)* code.

5.3 δ_θ-cyclic codes over R

In this section, we define a class of skew-cyclic codes over R and call them δ_θ-cyclic codes over R.

A linear code of length n over R is a submodule of R^n. By identifying R^n with $\frac{R[x,\theta,\delta_\theta]}{\langle f(x)\rangle}$, where $f(x)$ is an arbitrary polynomial of degree n over R, we can associate a word $a = (a_0, a_1, \ldots, a_{n-1})$ to the corresponding polynomial $a(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$. Moreover $\frac{R[x,\theta,\delta_\theta]}{\langle f(x)\rangle}$ is a left $R[x, \theta, \delta_\theta]$-module with respect to the multiplication $r(x)(a(x) + \langle f(x)\rangle) = r(x)a(x) + \langle f(x)\rangle$.

Definition 5.3.1. *A code C of length n over R is said to be a δ_θ-linear code if it is a left $R[x, \theta, \delta_\theta]$-submodule of $\frac{R[x,\theta,\delta_\theta]}{\langle f(x)\rangle}$, where $f(x)$ is an arbitrary polynomial of degree n over R. In addition, if $f(x)$ is a central polynomial in $R[x, \theta, \delta_\theta]$, we call C a central δ_θ-linear code.*

Definition 5.3.2 (δ_θ-cyclic code)**.** *A code C of length n over R is said to be δ_θ-cyclic code over R if C is a δ_θ-linear code and whenever $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, we have $T_{\delta_\theta}(c) = (\theta(c_{n-1}) + \delta_\theta(c_0), \theta(c_0) + \delta_\theta(c_1), \theta(c_1) + \delta_\theta(c_2), \ldots, \theta(c_{n-2}) + \delta_\theta(c_{n-1})) \in C$, where T_{δ_θ} is the δ_θ-cyclic shift operator.*

Lemma 5.3.3. *If $v(x) = v_0 + v_1x + v_2x^2 + \ldots + v_{n-1}x^{n-1} \in \frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$ represents the word $v = (v_0, v_1, \ldots, v_{n-1})$ in R^n, then $xv(x)$ represents the word $(\theta(v_{n-1}) + \delta_\theta(v_0), \theta(v_0) + \delta_\theta(v_1), \theta(v_1) + \delta_\theta(v_2), \ldots, \theta(v_{n-2}) + \delta_\theta(v_{n-1}))$ in R^n.*

Proof: We have

$$\begin{aligned}
xv(x) &= x\left(\sum_{i=0}^{n-1} v_ix^i\right) = \sum_{i=0}^{n-1} x(v_ix^i) = \sum_{i=0}^{n-1}(\theta(v_i)x + \delta_\theta(v_i))x^i \\
&= \sum_{i=0}^{n-1} \theta(v_i)x^{i+1} + \sum_{i=0}^{n-1} \delta_\theta(v_i)x^i = \sum_{i=1}^{n} \theta(v_{i-1})x^i + \sum_{i=0}^{n-1} \delta_\theta(v_i)x^i \\
&= \sum_{i=1}^{n-1} \theta(v_{i-1})x^i + \sum_{i=1}^{n-1} \delta_\theta(v_i)x^i + \theta(v_{n-1})x^n + \delta_\theta(v_0)x^0 \\
&= \sum_{i=1}^{n-1}(\theta(v_{i-1}) + \delta_\theta(v_i))x^i + (\theta(v_{n-1}) + \delta_\theta(v_0)) \qquad \text{(since } x^n = 1) \\
&= \sum_{i=0}^{n-1}(\theta(v_{i-1}) + \delta_\theta(v_i))x^i,
\end{aligned}$$

where the indices are computed modulo n. Hence the result. ■

Theorem 5.3.4. *A code C of length n over R is a δ_θ-cyclic code if and only if C is an $R[x, \theta, \delta_\theta]$-submodule of $R_{n,\delta_\theta} = \frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$.*

Proof: Suppose C is a δ_θ-cyclic code of length n over R. Then for any $c(x) \in C$, the δ_θ-cyclic shift, $xc(x)$ also belongs to C (by Lemma 5.3.3), and hence $x^ic(x) \in C$ for all $i \in \mathbb{N}$. It follows that $a(x)c(x) \in C$ for all $a(x) \in R[x, \theta, \delta_\theta]$. Hence the result. Converse is straightforward. ■

Corollary 5.3.4.1. *If C is a δ_θ-cyclic code of even length n, then C is an ideal of $R_{n,\delta_\theta} = \frac{R[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$.*

Proof: For even n, the ideal $\langle x^n - 1\rangle$ is a two sided ideal and so R_{n,δ_θ} is a ring. Hence the result. ■

Remark 5.3.4.1. *A δ_θ-cyclic code of an even length n over R is a central δ_θ-linear code. However, the converse is not true. This is shown by the following example.*

Example 5.3.5. *Let C be a code of length 4 over R generated by the right divisor $g(x) = (1+2w)x^2-1$ of $f(x) = (2w+1)x^4+(2w+2)x^2+1 = (x^2-1)((1+2w)x^2-1)$. Since $f(x)$ is a central polynomial in $R[x, \theta, \delta_\theta]$, C is a central δ_θ-linear code. We obtained, using MAGMA, that $(3w + 1, 3w + 2, 3w + 1, w) \in C$, but its δ_θ-cyclic shift, i.e., $(3w, w+1, w+2, w+1)$ is not in C. Hence C is not a δ_θ-cyclic code over R.*

Theorem 5.3.6. *Let C be a δ_θ-cyclic code of length n over R. Then we have the following results:*

1. *C is simply a cyclic code of length n over R, if n is odd.*
2. *C is a quasi-cyclic code of length n and index 2 over R, if n is even.*

Proof:

1. Since n is odd, we have $(n, 2) = 1$. Therefore there exist two integers a, b such that $na + 2b = 1$ and so $2b = 1 - na = 1 + nl$, where $l \equiv -a \ (mod\ n)$. Let $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ be a codeword. Now by Lemma 5.2.6, $x^{2b}c(x) = x^{2b}(c_0 + c_1x + \cdots + c_{n-1}x^{n-1}) = c_0x^{2b} + c_1x^{2b+1} + \cdots + c_{n-1}x^{2b+n-1}$. Therefore $x^{2b}c(x) = c_0x^{1+nl} + c_1x^{1+nl+1} + \cdots + c_{n-1}x^{(1+nl)+(n-1)} = c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}$, which is the cyclic shift of $c(x)$. Hence the result.
2. For any codeword $c(x)$ in C, $x^2c(x) \in C$ and it represents the cyclic shift of c by two positions (by Lemma 5.2.6). Also, in general, C is not cyclic. So 2 is the smallest integer t such that $x^tc(x) \in C$ for any $c(x) \in C$. Therefore C is quasi-cyclic code of index 2.

■

Theorem 5.3.7. *Let C be a δ_θ-cyclic code of length n over R such that C contains a minimum degree polynomial $g(x)$ with its leading coefficient a unit. Then $C = \langle g(x)\rangle$. Moreover $g(x) \mid (x^n - 1)$ and the set $\{g(x), xg(x), \ldots, x^{n-deg\ g(x)-1}g(x)\}$ forms a basis for C.*

Proof: Since C contains a minimum degree polynomial having its leading coefficient a unit, the proof follows from similar arguments as in the case of finite fields [96].

■

The converse of Theorem 5.3.7 is also true.

Theorem 5.3.8. *Let C be a free δ_θ-cyclic code of length n over R. Then there exists a minimum degree polynomial $g(x)$ such that $C = \langle g(x) \rangle$ and $g(x) \mid x^n - 1$.*

Proof: Straightforward. ■

Example 5.3.9. *Let C be a δ_θ-cyclic code of length 6 over R generated by the right divisor $g(x) = (w+2)x^3 + 2x^2 + 3w$ of $x^6 - 1$. Then the set $\{g(x), xg(x), x^2g(x)\} = \{(w+2)x^3 + 2x^2 + 3w, wx^4 + 2wx^3 + (3w+2)x + 2w + 2, (w+2)x^5 + 2x^4 + 3wx^2\}$ forms a basis for C. Therefore C has cardinality 16^3.*

Now we present a form of the generator matrix of a free δ_θ-cyclic code of length n over R.

Let $C = \langle g(x) \rangle$ be a δ_θ-cyclic code of length n over R generated by a right divisor $g(x)$ of $x^n - 1$. Then the generator matrix of C is an $(n-k) \times n$ matrix

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{n-k-1}g(x) \end{bmatrix}_{(n-k)\times n},$$

where $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$. More precisely, if $n-k$ is even, then $G =$

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) \end{bmatrix}$$

and if $n-k$ is odd, then

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & 0 & g_0\cdots & g_{k-2} & g_{k-1} & g_k \end{bmatrix}.$$

For example, for the δ_θ-cyclic code C given in Example 5.3.9, the generator matrix of C can be given as

$$\begin{bmatrix} 3w & 0 & 2 & w+2 & 0 & 0 \\ 2w+2 & 3w+2 & 0 & 2w & w & 0 \\ 0 & 0 & 3w & 0 & 2 & w+2 \end{bmatrix}.$$

5.3.1 Residue and torsion codes

In this sub-section, we study the residue codes and torsion codes associated with linear codes over R.

Definition 5.3.10. *Let C be a linear code of length n over R. Then*

$$Res(C)=\{x:\ x+wy\in C \textit{ for some } y\in {\mathbb{Z}_4}^n\}$$

and

$$Tor(C)=\{x:\ wx\in C\}$$

are called the residue code and the torsion code, respectively, of C.

$Res(C)$ and $Tor(C)$ are linear codes of length n over $\mathbb{Z}_4$.

Theorem 5.3.11. *Let C be a linear code of length n over R.*

1. *If $x+wy\in C$, then $x,y\in Res(C)$, and hence $Res(C)=\{y\mid x+wy\in C \text{ for some } x\in {\mathbb{Z}_4}^n\}$.*

2. *$Tor(C)\subseteq C$, hence $min\{d_L(Tor(C))\}\geq min\{d_G(C)\}$.*

Proof: For first part, since $x + wy \in C$, we have $wx + y \in C$ as $w^2 = 1$. This gives $y \in Res(C)$. Also $x + wy \in C$ implies $x \in Res(C)$. The proof of the second part is straightforward. ■

Example 5.3.12. *Let $f(x) = x^8 - 1$. Then two different factorizations of $f(x)$ are as follows:*

$$\begin{aligned} x^8 - 1 &= (x^2 - 1)(x^6 + x^4 + x^2 + 1) \\ &= ((3w + 2)x^2 + 2wx + w + 2)((3w + 2)x^6 + 2wx^5 + (3w + 2)x^4 + (3w + 2)x^2 + 2wx + 3w + 2). \end{aligned}$$

Consider two distinct factors of degree 6 of $x^8 - 1$ as $f_1 = x^6 + x^4 + x^2 + 1, f_2 = (3w + 2)x^6 + 2wx^5 + (3w + 2)x^4 + (3w + 2)x^2 + 2wx + 3w + 2$. Then we have δ_θ-cyclic codes $C_1 = \langle f_1 \rangle$ and $C_2 = \langle f_2 \rangle$ of length 8 over R. A spanning set for C_i is $\{f_i, xf_i\}$ for $i = 1, 2$. Moreover, C_2 exists due to the factor f_2, which exists only in $R[x, \theta, \delta_\theta]$, not in $R[x]$ or $R[x, \theta]$. Now $\Phi(C_1)$ and $\Phi(C_2)$ are linear codes of length 16 over $\mathbb{Z}_4$ having parameters $(16, 4^4, 4)$, $(16, 4^4, 8)$, respectively. Also $Res(C_1)$ has the parameters $(8, 4^2, 4)$ and $Res(C_2)$ has the parameters $(8, 4^2, 8)^*$, which is a good linear code over $\mathbb{Z}_4$ [8].

Example 5.3.13. *Let C be a δ_θ-cyclic code of length 9 over R generated by $g(x) = 3x^8+2wx^7+(w+1)x^6+(2w+2)x^5+2wx^4+(w+2)x^3+2x^2+(w+2)x+w+2$. Consider a subcode C_1 of C having spanning set $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)\}$. Now the parameters of $\Phi(C_1)$ are $(18, 4^{10}, 4)$ and the parameters of $Res(C_1)$ are $(\mathbf{9}, \mathbf{4^8 2^1}, \mathbf{2})$. $Res(C_1)$ is a new good linear code over $\mathbb{Z}_4$ and has twice as many codewords as in the existing best known code with comparable parameters [8]. A generator matrix of $Res(C_1)$ over $\mathbb{Z}_4$ is given by*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

Further, let $C_2 = \{(u \mid u+v) \mid u, v \in Res(C_1)\}$*. Then the parameters* C_2 *are* $(\mathbf{18}, \mathbf{4^{16}2^2}, \mathbf{2})$*, which is a new good linear code over* $\mathbb{Z}_4$ *and improves the minimum Lee distance of code by* 1 *when compared to existing best code with comparable parameters [8].*

Example 5.3.14. *Let* C *be a* δ_θ*-cyclic code of length* 4 *over* R *with generator matrix*

$$\begin{bmatrix} 1+w & w & 1 & 0 \\ 2+2w & 1+3w & 2+w & 1 \\ 1 & 0 & 1+w & w \end{bmatrix}.$$

Then $\Phi(C)$ *has parameters* $(8, 4^6, 2)$*, which is a best known linear code over* $\mathbb{Z}_4$*. Also* $Res(C)$ *has a generator matrix*

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

The parameters for $Res(C)$ *are* $(4, 4^3 2^1, 2)$*, which is a best known good code over* $\mathbb{Z}_4$*. Moreover* $Res(C)$ *is an* $MLDS$ *code. Now let* $C_1 = \{(u \mid u+v) \mid u, v \in Res(C)\}$*. Then* C_1 *is an* $(\mathbf{8}, \mathbf{4^6 2^2}, \mathbf{2})$ *code over* $\mathbb{Z}_4$*, which is a new good linear code over* $\mathbb{Z}_4$ *and improves the minimum Lee distance by* 1 *when compared to existing best known code with comparable parameters [8].*

Table 5.1: Some good linear codes over $\mathbb{Z}_4$

	$\Phi(C)$	$Res(C)$	C^*
Set of generators	$(n, 4^{k_1}2^{k_2}, d_L)$	$(n, 4^{k_1}2^{k_2}, d_L)$	$(n, 4^{k_1}2^{k_2}, d_L)$
$\{g_1(x), xg_1(x), x^2g_1(x)\}$	$(10, 4^6, 2)$	$(5, 4^4 2^1, 2)^*$	$(\mathbf{10}, \mathbf{4^8 2^2}, \mathbf{2})^{**}$
$\{g_2(x), xg_2(x), x^2g_2(x)\}$	$(20, 4^6, 8)$	$(10, 4^6, 4)^*$	$(20, 4^{12}, 4)^*$
$\{g_3(x), xg_3(x), x^2g_3(x)\}$	$(20, 4^6, 6)$	$(10, 4^5, 6)^*$	$(20, 4^{10}, 6)$
$\{g_4(x), xg_4(x), x^2g_4(x), x^3g_4(x)\}$	$(24, 4^8, 6)$	$(12, 4^8, 4)^*$	$(24, 4^{16}, 4)^*$
$\{g_5(x), xg_5(x), x^2g_5(x), x^3g_5(x)\}$	$(28, 4^8, 6)$	$(14, 4^8, 5)^*$	$(28, 4^{16}, 5)^*$
$\{g_6(x), xg_6(x), x^2g_6(x), x^3g_6(x)\}$	$(30, 4^8, 6)$	$(15, 4^8, 6)^*$	$(30, 4^{16}, 6)$
$\{g_7(x), xg_7(x), x^2g_7(x), x^3g_7(x)\}$	$(36, 4^8, 8)$	$(18, 4^8, 8)^*$	$(36, 4^{16}, 8)^*$

Table 5.1 shows some good linear codes that we have obtained over $\mathbb{Z}_4$ via the Gray images and residue codes of skew-linear codes with derivation (not necessarily δ_θ-cyclic codes) over R. In table 5.1, we have

$C^* = \{(u \mid u+v) : u, v \in Res(C)\}$, * := Existing good code, ** := New good code,

and

$$g_1(x) = 2wx^4 + x^3 + (w+2)x^2 + 2wx + (w+1)$$

$$g_2(x) = wx^9 + (w+1)x^8 + 2wx^7 + (w+2)x^6 + 2x^5 + (w+1)x^4 + x^2 + wx + (w+1)$$

$$g_3(x) = wx^9 + (w+1)x^8 + (3w+3)x^7 + (2w+2)x^6 + (3w+2)x^5 + 2x^4 + x^2 + wx + w + 1$$

$$g_4(x) = 2x^{11} + wx^{10} + 2x^9 + (w+1)x^8 + 2wx^7 + (w+1)x^6 + 2x^5 + 2wx^4 + (3w+3)x^3 + (2w+3)x^2 + (w+2)x + 2$$

$$g_5(x) = 2wx^{13} + (w+1)x^{12} + wx^{11} + (w+2)x^{10} + 2x^9 + (w+1)x^8 + 2wx^7 + (w+1)x^6 + 2x^5 + wx^4 + (w+3)x^3 + 2x^2 + 2x + 2$$

$$g_6(x) = (w+1)x^{14} + 2x^{13} + (w+1)x^{12} + 2x^{11} + wx^{10} + 2x^9 + (w+1)x^8 + 2wx^7 + (w+1)x^6 + 2x^5 + (2w+3)x^4 + 3x^3 + (w+2)x^2 + 2x + 2$$

$$g_7(x) = 2x^{17} + 2x^{16} + 2x^{15} + (3w+3)x^{14} + (2w+2)x^{13} + (w+1)x^{12} + 2x^{11} + wx^{10} +$$

$2x^9+(w+1)x^8+2x^7+(w+1)x^6+2x^5+2wx^4+(w+2)x^3+wx^2+(w+2)x+2$

5.4 Duals of δ_θ-cyclic codes over R

In this section, we find the structure of the dual of a free δ_θ-cyclic code of even length n over R.

To determine a generator matrix of the dual of a free δ_θ-cyclic code C, we need to find the parity-check matrix of C. For this, we first require some lemmas.

Lemma 5.4.1. *For even n, x^n-1 is a central element of $R[x,\theta,\delta_\theta]$, and hence $x^n-1=h(x)g(x)=g(x)h(x)$ for some $g(x),h(x)\in R[x,\theta,\delta_\theta]$.*

Proof: The proof is similar to the proof of Lemma 4.4.2 in Chapter 4. ■

Remark 5.4.1.1. *If C is a δ_θ-cyclic code generated by a minimum degree polynomial $g(x)$ with its leading coefficient a unit, then there exists a minimum degree monic polynomial $g'(x)$ in C such that $C=\langle g'(x)\rangle$.*

Lemma 5.4.2. *Let C be a δ_θ-cyclic code of even length n over R generated by a monic right divisor $g(x)$ of x^n-1. Then $v(x)\in R_{n,\delta_\theta}$ is in C if and only if $v(x)h(x)=0$ in R_{n,δ_θ}, where $x^n-1=h(x)g(x)$.*

Proof: Suppose $v(x)\in C$. Then $v(x)=a(x)g(x)$ for some $a(x)\in R_{n,\delta_\theta}$. So $v(x)h(x)=a(x)g(x)h(x)=a(x)h(x)g(x)=0$ in R_{n,δ_θ} (by Lemma 5.4.1). Conversely, suppose $v(x)h(x)=0$ in R_{n,δ_θ} for some $v(x)\in R_{n,\delta_\theta}$. Then there exists $q(x)\in R[x,\theta,\delta_\theta]$ such that $v(x)h(x)=q(x)(x^n-1)=q(x)h(x)g(x)=q(x)g(x)h(x)$. Since $h(x)$ is regular, $v(x)=q(x)g(x)$. Hence the result. ■

Lemma 5.4.3. *Let $a\in R$ be a unit in R. Then $\theta(a)+\delta_\theta(b)$ is a unit for all $b\in R$.*

Proof: Let $d=\theta(a)+\delta_\theta(b)$, where $a,b\in R$ such that a is a unit. Let $\theta(a)=\alpha+w\beta$. Then $\alpha+w\beta$ is a unit, and hence either α or β is a unit but not both. We know $\delta_\theta(b)$ is either 0 or $2w+2$ for all $b\in R$. If $\delta_\theta(b)=0$, then we are done. Otherwise $d=(\alpha+2)+w(\beta+2)$. Also, any $c\in\mathbb{Z}_4$ is a unit if and only if $c+2$ is a unit. Hence d is a unit. ■

Theorem 5.4.4. *Let $C = \langle g(x) \rangle$ be a principally generated δ_θ-cyclic code of even length n over R such that $x^n - 1 = h(x)g(x)$ for some $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k \in R[x, \theta, \delta_\theta]$, where k is odd. Then the matrix $H =$*

$$\begin{bmatrix} h_k & \theta(h_{k-1}) + \delta_\theta(h_k) & h_{k-2} & \cdots & \theta(h_0) + \delta_\theta(h_1) & \cdots & 0 & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_0 & \delta_\theta(h_0) & \cdots & 0 \\ 0 & 0 & h_k & h_{k-2} & \theta(h_{k-3}) + \delta_\theta(h_{k-2}) & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & h_k & \theta(h_{k-1}) + \delta_\theta(h_k) & \cdots & h_1 & \theta(h_0) + \delta_\theta(h_1) \end{bmatrix}$$

is a parity-check matrix for C.

Proof: Let $c(x) \in C$. Then by Lemma 5.4.2, we have $c(x)h(x) = 0$ in R_{n,δ_θ}. Therefore the coefficients of $x^k, x^{k+1}, \cdots, x^{n-1}$ in $[c_0 + c_1x + c_2x^2 + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}][h_0 + h_1x + h_2x^2 + \cdots + h_{k-1}x^{k-1} + h_kx^k]$ are all zero. So we have

$$\begin{aligned} c_0h_k + c_1(\theta(h_{k-1}) + \delta_\theta(h_k)) + c_2h_{k-2} + \cdots + c_k(\theta(h_0) + \delta_\theta(h_1)) &= 0 \\ c_1(\theta(h_k)) + c_2h_{k-1} + c_3(\theta(h_{k-2}) + \delta_\theta(h_{k-1})) + \cdots + c_{k+1}h_0 + c_{k+2}\delta_\theta(h_0) &= 0 \\ c_2h_k + c_3(\theta(h_{k-1}) + \delta_\theta(h_k)) + c_4h_{k-2} + \cdots + c_{k+1}h_1 + c_{k+2}(\theta(h_0) + \delta_\theta(h_1)) &= 0 \\ &\vdots \\ c_{n-k-1}h_k + c_{n-k}(\theta(h_{k-1}) + \delta_\theta(h_k)) + \cdots + c_{n-2}h_1 + c_{n-1}(\theta(h_0) + \delta_\theta(h_1)) &= 0. \end{aligned}$$

From these equations, it is clear that for any $c \in C$, $cH^T = 0$, and hence $GH^T = 0$. Now each row of H is orthogonal to each $c \in C$, so $span(H) \subseteq C^\perp$. Moreover, H contains a square sub-matrix of order $n - k$ (by taking first $n - k$ coordinates of each row) with non-zero determinant, as it is a lower triangular matrix with all diagonal entries units (by Lemma 5.4.3). This implies that all rows of H are linearly independent. Therefore $|Span(H)| = |R|^{n-k}$. Also $|C||C^\perp| = |R|^n$ and $|C| = |R|^k$ give $|C^\perp| = |R|^{n-k}$. Hence $Span(H) = C^\perp$, and so H is a parity check matrix of C. ■

The above result can similarly be proved for the case when k is even. In this case, matrix H is given as:

$$\begin{bmatrix} h_k & \theta(h_{k-1})+\delta_\theta(h_k) & h_{k-2} & \cdots & h_0 & \delta_\theta(h_0) & \cdots & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_1 & \theta(h_0)+\delta_\theta(h_1) & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & \theta(h_1)+\delta_\theta(h_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & \cdots & \theta(h_k) & h_{k-1} & \cdots & h_1 & \theta(h_0)+\delta_\theta(h_1) \end{bmatrix}.$$

Example 5.4.5. *Let C be a δ_θ-cyclic code of length 6 generated by the polynomial $g(x) = (w+2)x^3+2x^2+3w$ such that $x^6-1 = (wx^3+2wx^2+w)((w+2)x^3+2x^2+3w)$. Let $h(x) = wx^3 + 2wx^2 + w$. Then a parity check matrix of C (by Theorem 5.4.4) is given by*

$$H = \begin{bmatrix} w & 2 & 0 & w+2 & 0 & 0 \\ 0 & w+2 & 2w & 0 & w & 2+2w \\ 0 & 0 & w & 2 & 0 & w+2 \end{bmatrix}.$$

One may verify that $GH^T = 0$ and the rows of H are linearly independent. Therefore H forms a parity check matrix for C.

5.5 Double δ_θ-cyclic codes over R

In this section, we study double δ_θ-cyclic codes over R.

For any $d \in R$ and $v = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) \in R^{\alpha+\beta}$, we define

$$dv = (da_0, da_1, \cdots, da_{\alpha-1}, db_0, db_1, \cdots, db_{\beta-1}).$$

With this multiplication, $R^{\alpha+\beta}$ is an R-module.

Definition 5.5.1. *For an element $v = (a_0, a_1, \cdots, a_{\alpha-1}, b_0, b_1, \cdots, b_{\beta-1}) \in R^{\alpha+\beta}$, the $\delta_\theta(\alpha, \beta)$-cyclic shift of v, denoted by ${}^{\alpha\beta}T_{\delta_\theta}(v)$, is defined as*
${}^{\alpha\beta}T_{\delta_\theta}(v) = (\theta(a_{\alpha-1}) + \delta_\theta(a_0), \theta(a_0) + \delta_\theta(a_1), \theta(a_1) + \delta_\theta(a_2), \cdots, \theta(a_{\alpha-2}) + \delta_\theta(a_{\alpha-1}),$
$\theta(b_{\beta-1}) + \delta_\theta(b_0), \theta(b_0) + \delta_\theta(b_1), \theta(b_1) + \delta_\theta(b_2), \cdots, \theta(b_{\beta-2}) + \delta_\theta(b_{\beta-1}))$.

A double δ_θ-linear code is an R-submodule of $R^{\alpha+\beta}$.

Definition 5.5.2. *A double δ_θ-linear code C is called double δ_θ-cyclic code if C is invariant under the $\delta_\theta(\alpha, \beta)$-cyclic shift ${}^{\alpha\beta}T_{\delta_\theta}$.*

In polynomial representation, $R_{\alpha,\beta} = \frac{R[x,\theta,\delta_\theta]}{\langle x^\alpha - 1\rangle} \times \frac{R[x,\theta,\delta_\theta]}{\langle x^\beta - 1\rangle}$ is a left $R[x, \theta, \delta_\theta]$-module.

It can easily be seen that if $c(x) = (c_1(x) \mid c_2(x)) \in R_{\alpha,\beta}$ represents the word $c \in R^{\alpha+\beta}$, then $xc(x)$ represents the $\delta_\theta(\alpha, \beta)$-cyclic shift of c.

Theorem 5.5.3. *Let C be a δ_θ-linear code of length $n = \alpha + \beta$ over R. Then C is a double δ_θ-cyclic code if and only if it is a left $R[x, \theta, \delta_\theta]$-submodule of the left-module $R[x, \theta, \delta_\theta]/\langle x^\alpha - 1\rangle \times R[x, \theta, \delta_\theta]/\langle x^\beta - 1\rangle$.*

Proof: Suppose C is a double δ_θ-cyclic code. Let $c \in C$, and let the associated polynomial of c be $c(x)$. As $xc(x)$ is a $\delta_\theta(\alpha, \beta)$-cyclic shift of c, so $xc(x) \in C$. By linearity of C, $r(x)c(x) \in C$ for any $r(x) \in R[x, \theta, \delta_\theta]$. So C is left $R[x, \theta, \delta_\theta]$-submodule of $R_{\alpha,\beta}$. Converse is straightforward. ■

Theorem 5.5.4. *A double δ_θ-cyclic code of length $n = \alpha + \beta$ is a double cyclic code if α and β both are odd integers.*

Proof: Let C be a double δ_θ-cyclic code. Let $\gamma = lcm(\alpha, \beta)$. Then γ is odd, and so $gcd(\gamma, 2) = 1$. Therefore there exist two integers a, b such that $\gamma a + 2b = 1$ and so $2b = 1 - \gamma a = 1 + \gamma l$ for some $l > 0$, where $l = -a \pmod{\gamma}$. Let $c(x) = (a(x) \mid b(x)) \in C$, where $a(x) = \sum_{i=0}^{\alpha-1} a_i x^i$ and $b(x) = \sum_{i=0}^{\beta-1} b_i x^i$. Then

$$\begin{aligned}
x^{2b}c(x) &= x^{2b}\left(\sum_{i=0}^{\alpha-1} a_i x^i \mid \sum_{i=0}^{\beta-1} b_i x^i\right) = \left(\sum_{i=0}^{\alpha-1} a_i x^{i+2b} \mid \sum_{i=0}^{\beta-1} b_i x^{i+2b}\right) \\
&= \left(\sum_{i=0}^{\alpha-1} a_i x^{i+1+\gamma l} \mid \sum_{i=0}^{\beta-1} b_i x^{i+1+\gamma l}\right) \\
&= \left(\sum_{i=0}^{\alpha-2} a_i x^{i+1+\gamma l} + a_{\alpha-1}x^{\alpha+\gamma l} \mid \sum_{i=0}^{\alpha-2} a_i x^{i+1+\gamma l} + a_{\beta-1}x^{\beta+\gamma l}\right) \\
&= \left(\sum_{i=0}^{\alpha-2} a_i x^{i+1} + a_{\alpha-1} \mid \sum_{i=0}^{\beta-2} a_i x^{i+1} + a_{\beta-1}\right), \text{(since } x^\alpha = x^\beta = x^\gamma = 1).
\end{aligned}$$

Thus $x^{2b}c(x) = (a'(x) \mid b'(x))$, where $a'(x), b'(x)$ are cyclic shifts of $a(x)$ and $b(x)$, respectively. Hence C is a double cyclic code. ■

Theorem 5.5.5. *Let C_1 and C_2 be two free δ_θ-cyclic codes of lengths n_1 and n_2 over R having monic generator polynomials $g_1(x)$ and $g_2(x)$, respectively, such that $g_1(x)|x^{n_1}-1$ and $g_2(x)|x^{n_2}-1$. Then a code C generated by $g(x) = (g_1(x) \mid g_2(x))$ is a double δ_θ-cyclic code and $A = \{g(x), xg(x), \cdots, x^{l-1}g(x)\}$ is a spanning set of C, where $l = deg\ h(x)$ and $h(x)$ is the least left common multiple of $h_1(x)$ and $h_2(x)$.*

Proof: Let $x^{n_1} - 1 = h_1(x)g_1(x)$ and $x^{n_2} - 1 = h_2(x)g_2(x)$ for some monic polynomials $h_1(x), h_2(x) \in R[x, \theta, \delta_\theta]$. Then $h(x)g(x) = h(x)(g_1(x)|g_2(x)) = 0$, as $h(x)g_i(x) = h'(x)h_i(x)g_i(x) = 0$ for $i = 1, 2$. Now let $v(x) \in C$ be any non-zero codeword in C. Then $v(x) = a(x)g(x)$ for some $a(x) \in R[x, \theta, \delta_\theta]$. By the division algorithm, we have $a(x) = q(x)h(x) + r(x)$, where $r(x) = 0$ or deg $r(x) <$ deg $h(x)$. Then $v(x) = a(x)g(x) = r(x)g(x) = 0$. Since $r(x) = 0$ or deg $r(x) <$ deg $h(x)$, the result follows. ■

Example 5.5.6. *Let C be a double δ_θ-cyclic code of length $n = 10(= 6 + 4)$ over R, which is principally generated by $g(x) = (g_1(x)|g_2(x))$, where $g_1(x) = wx^3+2wx^2+w$ and $g_2(x) = x^2 + 2wx + 1$ such that $g_1(x)|x^6 - 1$ and $g_2(x)|x^4 - 1$. Now let $h(x)$ be the least left common multiple of $h_1(x)$ and $h_2(x)$. Then deg $h(x) = 5$. Therefore the set $\{g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)\}$ forms a spanning set for C. Hence a generator matrix of C is*

$$\left[\begin{array}{cccccc|cccc}
w & 0 & 2w & w & 0 & 0 & 1 & 2w & 1 & 0 \\
2w+2 & w+2 & 0 & 2 & w+2 & 0 & 0 & 1 & 2w & 1 \\
0 & 0 & w & 0 & 2w & w & 1 & 0 & 1 & 2w \\
w+2 & 0 & 2w+2 & w+2 & 0 & 2 & 2w & 1 & 0 & 1 \\
2w & w & 0 & 0 & w & 0 & 1 & 2w & 1 & 0
\end{array}\right].$$

The parameters for $\Phi(C)$ are $[20, 4^9, 4]$. Moreover, $Res(C)$ and $Tor(C)$ have the parameters $[10, 4^5 2^1, 2]$ and $[10, 4^3 2^1, 4]$, respectively.

In Table 2, we present some good linear codes over $\mathbb{Z}_4$ as Gray images and residue codes of double skew-linear codes with derivation (not necessarily δ_θ-cyclic codes) over R.

Table 5.2: Some good linear codes over $\mathbb{Z}_4$

Set of generators	(n, M, d_L)	$(n, 4^{k_1}2^{k_2}, d_L)$	$(n, 4^{k_1}2^{k_2}, d_L)$
$\{h_0(x), xh_1(x)\}$	$(10, 128, 2)$	$(5, 4^3 2^1, 2)^*$	$(10, 4^6 2^2, 2)$
$\{h_1(x), xh_1(x), x^2h_1(x)\}$	$(12, 4096, 2)$	$(6, 4^5 2^1, 2)^*$	$(\mathbf{12}, \mathbf{4^{10}2^2}, \mathbf{2})^{**}$
$\{h_2(x), xh_2(x), x^2h_2(x), x^3h_2(x)\}$	$(14, 65536, 2)$	$(7, 4^6 2^1, 2)^*$	$(14, 4^{12}2^2, 2)$
$\{h_3(x), xh_3(x), x^3h_2(x), x^3h_3(x)\}$	$(16, 65536, 4)$	$(\mathbf{8}, \mathbf{4^7}, \mathbf{2})^{**}$	$(\mathbf{16}, \mathbf{4^{14}}, \mathbf{2})^{**}$

In Table 5.2, we have $C^* = \{(u \mid u+v) : u, v \in Res(C)\}$, * := Existing good code, ** :=New good code, and

$$h_0(x) = ((2+3w) + (1+2w)x + wx^2 \mid 2w + (2+2w)x),$$

$$h_1(x) = ((3w+2) + (1+2w)x + wx^2 \mid 2 + (1+2w)x + 2wx^2),$$

$$h_2(x) = ((1+w) + (1+2w)x + (2+w)x^2 + wx^3 \mid 1 + 2wx + (w+1)x^2),$$

$$h_3(x) = ((1+w) + (1+2w)x + (2+w)x^2 + wx^3 \mid 1 + 2wx + (w+1)x^2 + 2wx^3).$$

Remark 5.5.6.1. *The codes whose parameters are written in bold letters in Table* 1 *and Table* 2 *have improved the parameters of the existing codes having comparable parameters.*

5.6 Conclusion

We have studied a class of skew-cyclic codes over $R = \mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$ with derivation. We have studied these codes as left $R[x, \theta, \delta_\theta]$-submodules. A Gray map is defined on R, and some good linear codes over $\mathbb{Z}_4$ via Gray images, residue codes of these codes have been obtained. The generator matrix of the dual code of a free δ_θ-cyclic code of even length over R is obtained. These codes are generalized to double skew-cyclic codes with derivation. All new linear codes over $\mathbb{Z}_4$, obtained in this paper, have been reported and added to the database of $\mathbb{Z}_4$-codes. It will be interesting to obtain criteria under which the dual of a free δ_θ-cyclic code of even length over R is a δ_θ-cyclic code of same length.

Chapter 6

2D-Skew Cyclic Codes over $\mathbb{F}_q + w\mathbb{F}_q$

6.1 Introduction

Cyclic codes have been generalized in many ways [7, 6, 9, 104, 27, 29, 28, 58]. One of the generalizations of cyclic codes is 2D cyclic codes, which were first introduced by Ikai et al. [52] and then further studied by Imai [54]. Some other authors have also studied this class [53, 70, 105]. Recently, Li & Li [65] have introduced a generalization of 2D cyclic codes over finite fields, wherein they have studied 2D skew-cyclic codes of length ml over $\mathbb{F}_q$ as left $\mathbb{F}_q[x, y, \theta_1, \theta_2]$-submodules of $\frac{\mathbb{F}_q[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$, where θ_1, θ_2 are two commuting automorphisms of $\mathbb{F}_q$. In this chapter, we generalize this work and study 2D skew-cyclic codes over the ring $R = \mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$. We have obtained the generating sets of all possible forms of these codes.

6.2 Properties of the skew polynomial ring $(\mathbb{F}_q + w\mathbb{F}_q)[x, y, \theta_1, \theta_2]$

Let $R = \mathbb{F}_q + w\mathbb{F}_q$, $w^2 = 1$, where $q = p^r$, p a prime. R can be viewed as the quotient ring $\frac{\mathbb{F}_q[w]}{\langle w^2-1\rangle}$ and is a semi-local ring with two maximal ideals namely $\langle 1 + w\rangle$ and $\langle 1 - w\rangle$.

Theorem 6.2.1. *An element $a + wb \in R$ is a non-unit iff $a = \pm b$.*

Proof: The proof is similar to that of Theorem 3.5.1 in Chapter 3. ■

Corollary 6.2.1.1. *An element of R is a non-unit iff it is of the form $a(1 \pm w)$ for some $a \in \mathbb{F}_q$.*

We define a Gray map $\phi : R \to \mathbb{F}_q^2$ such that

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

ϕ can be extended componentwise to $\Phi : R^n \to {\mathbb{F}_q}^{2n}$. Φ is a linear map. Further, we define the Gray weight $w_G(x)$ of any $x \in R^n$ as $w_G(x) = w_H(\Phi(x))$, where w_H denotes the Hamming weight.

We define a bivariate skew polynomial ring over $R = \mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$, and study some properties of the same structure. For this, we first consider two types of automorphisms θ and σ_i on R, defined as

$$\theta(a + wb) = a - wb,$$

and

$$\sigma_i(a + wb) = a^{p^i} + wb^{p^i}, \quad i \le r,\ i \mid r\ .$$

One can easily verify that θ and σ_i are automorphisms of R and $\theta\sigma_i = \sigma_i\theta$ for all i. We use the notation

$$E = \{\sigma_i :\ i \le r,\ i \mid r\}\ .$$

Further we have $|\sigma_i| = r/i$.

Let $\mathcal{R}$ be a finite commutative ring with identity and let θ_1, θ_2 be two automorphisms of $\mathcal{R}$ such that $\theta_1\theta_2 = \theta_2\theta_1$. Then the bivariate skew polynomial ring $\mathcal{R}[x, y, \theta_1, \theta_2]$ is the set of bivariate polynomials over $\mathcal{R}$, i.e.,

$$\mathcal{R}[x, y, \theta_1, \theta_2] = \left\{ \sum_{i=0}^{l-1} \sum_{j=0}^{m-1} a_{i.j} x^i y^j :\quad a_{i,j} \in \mathcal{R};\ m, l \in \mathbb{N} \right\},$$

in which the addition is defined as the ordinary addition of polynomials but the multiplication is defined by the rule

$$x^i y^j a = {\theta_1}^i {\theta_2}^j (a) x^i y^j,$$

which is then extended to all elements of $\mathcal{R}[x, y, \theta_1, \theta_2]$ in the usual way. Let $f(x, y), g(x, y) \in \mathcal{R}[x, y, \theta_1, \theta_2]$. Then $g(x, y) \in \mathcal{R}[x, y, \theta_1, \theta_2]$ is said to be a right divisor of $f(x, y)$ if there exists a $q(x, y) \in \mathcal{R}[x, y, \theta_1, \theta_2]$ such that $f(x, y) = q(x, y)g(x, y)$. In this case, $f(x, y)$ is called a left multiple of $g(x, y)$, and $g(x, y)$ is called a right divisor of $f(x, y)$. In the sequel, division always means right division.

Let $\preceq$ be the usual lexicographical order on $\mathbb{Z} \times \mathbb{Z}$. Then for any $(\alpha, \beta), (\alpha', \beta') \in \mathbb{Z} \times \mathbb{Z}$, we have $(\alpha, \beta) \preceq (\alpha', \beta')$ iff $\alpha < \alpha'$ OR $\alpha = \alpha', \beta \leq \beta'$. If $(\alpha, \beta) \preceq (\alpha', \beta')$ and $(\alpha, \beta) \neq (\alpha', \beta')$, we write $(\alpha, \beta) \prec (\alpha', \beta')$. $\preceq$ is a total order on $\mathbb{Z} \times \mathbb{Z}$.

For any polynomial $f(x, y) \in \mathcal{R}[x, y, \theta_1, \theta_2]$, define

$$V_f = \{(z_1, z_2) \mid f(x, y) \text{ contains a term } ax^{z_1}y^{z_2},\ a \in \mathcal{R}, a \neq 0\}.$$

We define the lex-degree of $f(x, y)$ as the greatest element of V_f w.r.t the total order $\preceq$ on V_f, and denote it by lexdeg $f(x, y)$.

We extend the lexicographical order $\preceq$ to $\mathcal{R}[x, y, \theta_1, \theta_2]$ as follows. For any $f(x, y), g(x, y) \in \mathcal{R}[x, y, \theta_1, \theta_2]$, we define $f(x, y) \preceq g(x, y)$ iff lexdeg $f(x, y) \preceq$ lexdeg $g(x, y)$. Further we consider the zero polynomial to be the smallest element in this ordering.

The lex-leading term of a non-zero polynomial $f(x, y)$ is the term of $f(x, y)$ corresponding to its lex-degree. The lex-leading coefficient of $f(x, y)$ is the coefficient of its lex-degree term.

We define another partial order $\leq$ on $\mathcal{R}[x, y, \theta_1, \theta_2]$ as follows. If lexdeg $f(x, y) = (\alpha, \beta)$ and lexdeg $g(x, y) = (\alpha', \beta')$, then $f(x, y) \leq g(x, y)$ iff $\alpha \leq \alpha'$ and $\beta \leq \beta'$, with the usual less than or equal to relation. The dual of the partial order $\leq$ on $\mathcal{R}[x, y, \theta_1, \theta_2]$ is denoted by the usual notation $\geq$.

6.3 2D skew-cyclic codes over $R = \mathbb{F}_q + w\mathbb{F}_q$

Definition 6.3.1. *Let $\mathcal{R}$ be a finite commutative ring with identity, and let Θ be an automorphism of $\mathcal{R}$. Then a code C is said to be a skew quasi-cyclic code of length ml and index m over $\mathcal{R}$ if*

1. *C is an $\mathcal{R}$-submodule of $\mathcal{R}^n$, and*

2. *for any $c = (c_{0,0}, c_{0,1}, \cdots, c_{0,m-1}, c_{1,0}, c_{1,1}, \cdots, c_{1,m-1}, \cdots, c_{l-1,0}, \cdots, c_{l-1,m-1})$ in C, we have $(\Theta(c_{l-1,0}), \cdots, \Theta(c_{l-1,m-1})), \Theta(c_{0,0})$, $\Theta(c_{0,1}), \cdots, \Theta(c_{0,m-1}), \Theta(c_{1,0}), \Theta(c_{1,1}), \cdots, \Theta(c_{1,m-1}), \cdots, \Theta(c_{l-2,0}), \cdots, \Theta(c_{l-2,m-1}))$ is also in C.*

Let C be a linear code of length n over $\mathcal{R}$, where $n = ml$. Let $c = (a_0, a_1, \cdots, a_{n-1}) \in C$. Then c can be represented as an $l \times m$ matrix as follows.

$$c = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{l-1,0} & a_{l-1,1} & \cdots & \cdots & a_{l-1,m-1} \end{pmatrix}_{(l\times m)}.$$

Define two codes C_1 and C_2 associated with C as follows:

$$C_1 = \left\{ (a_{0,0}, \cdots, a_{0,m-1}, \cdots, a_{l-1,0}, \cdots, a_{l-1,m-1}) \ : \ c = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{l-1,0} & a_{l-1,1} & \cdots & \cdots & a_{l-1,m-1} \end{pmatrix} \in C \right\}$$

$$C_2 = \left\{ (a_{0,0}, \cdots, a_{l-1,0}, \cdots, a_{0,m-1}, \cdots, a_{l-1,m-1}) \ : \ c = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{l-1,0} & a_{l-1,1} & \cdots & \cdots & a_{l-1,m-1} \end{pmatrix} \in C \right\}.$$

Definition 6.3.2. *Let θ_1 and θ_2 be two commuting automorphisms of $\mathcal{R}$. Then a set C is said to be a 2D skew-cyclic code of length n $(= ml)$ over $\mathcal{R}$ if*

1. *C is an $\mathcal{R}$-submodule of $\mathcal{R}^n$,*

2. *the associated codes C_1 and C_2 of C are skew quasi-cyclic codes of indices m and l with automorphisms θ_1 and θ_2, respectively, over $\mathcal{R}$.*

Remark 6.3.2.1. *We denote a 2D skew-cyclic code over $\mathcal{R}$, with automorphisms θ_1 and θ_2 by C_{θ_1,θ_2}. In particular, if θ_2 is the identity map, we simply write $C_{\theta_1,1} = C_{\theta_1}$.*

In polynomial notation, to each word $a \in \mathcal{R}^n$, where $n = ml$ and

$$a = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{l-1,0} & a_{l-1,1} & \cdots & \cdots & a_{l-1,m-1} \end{pmatrix},$$

in matrix form, we associate the polynomial $a(x,y) = \sum_{i=0}^{l-1}\sum_{j=0}^{m-1} a_{i,j}x^iy^j \in \mathcal{R}_{m,l} = \frac{R[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$. This gives a one-to-one correspondence between $\mathcal{R}^n$ and $\mathcal{R}_{m,l}$. The multiplication of two elements $a(x,y)$ and $b(x,y)$ in $\mathcal{R}_{m,l}$ is defined as $a(x,y)b(x,y)$ mod (x^l-1, y^m-1), where $a(x,y)b(x,y)$ is the multiplication of $a(x,y)$ and $b(x,y)$ in the bivariate skew polynomial ring $\mathcal{R}[x,y,\theta_1,\theta_2]$. With this multiplication, the set $\mathcal{R}_{m,l}$ forms a left $\mathcal{R}[x,y,\theta_1,\theta_2]$-module.

Theorem 6.3.3. *A linear code of length ml over $\mathcal{R}$ is a 2D skew-cyclic code over $\mathcal{R}$ iff it is a left $\mathcal{R}[x,y,\theta_1,\theta_2]$-submodule of $\frac{\mathcal{R}[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$.*

Proof: Let C be a 2D skew-cyclic code over $\mathcal{R}$. Then for any $c(x,y) \in C$, $xc(x,y)$ and $yc(x,y)$ are also in C. This implies that $r(x,y)c(x,y) \in C$ for all $r(x,y) \in \mathcal{R}[x,y,\theta_1,\theta_2]$. So C is a left $\mathcal{R}[x,y,\theta_1,\theta_2]$-submodule of $\frac{\mathcal{R}[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$. Converse is straightforward. ■

Theorem 6.3.4. *Let C be a 2D skew-cyclic code of length ml over $\mathcal{R}$. If the order of θ_1 divides l and the order of θ_2 divides m, then the following hold.*

1. *The polynomials $x^l-1, y^m-1 \in \mathcal{R}[x,y,\theta_1,\theta_2]$ are in $Z(\mathcal{R}[x,y,\theta_1,\theta_2])$, where $Z(\mathcal{R}[x,y,\theta_1,\theta_2])$ is the center of $\mathcal{R}[x,y,\theta_1,\theta_2]$.*

2. *C is an ideal of $\frac{\mathcal{R}[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$.*

3. A right divisor of $(x^l - 1)(y^m - 1)$ is also a left divisor of $(x^l - 1)(y^m - 1)$.

Proof:

1. Straightforward.

2. By part 1, $\langle x^l-1, y^m-1\rangle$ is a two sided ideal, and so the quotient set $\frac{\mathcal{R}[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$ is a ring. Hence the result.

3. Let $g(x,y)$ be a right divisor of $(x^l-1)(y^m-1)$, so that $(x^l-1)(y^m-1) = h(x,y)g(x,y)$ for some $h(x,y) \in \mathcal{R}[x,y,\theta_1,\theta_2]$. Since the lex-leading coefficient of $(x^l-1)(y^m-1)$ is a unit, $g(x,y)$ and $h(x,y)$ can be taken such that their lex-leading coefficients are units. Now since $(x^l-1)(y^m-1)$ is a central polynomial, $(x^l-1)(y^m-1)h(x,y) = h(x,y)(x^l-1)(y^m-1)$, and so $h(x,y)g(x,y)h(x,y) = h(x,y)h(x,y)g(x,y)$, which gives $g(x,y)h(x,y) = h(x,y)g(x,y)$, as $h(x,y)$ has its lex-leading coefficient a unit and hence not a zero-divisor.

■

Now we consider 2D skew-cyclic codes over $R = \mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$. Further we take $\theta_1 = \theta$ and $\theta_2 = \sigma$, where $\sigma \in E = \{\sigma_i : i \leq r, i \mid r\}$, σ_i as defined in Section 6.2.

We extend the definition of the consistent set, given in [65] for the case of finite fields, to the present case as follows.

Definition 6.3.5. *Let M be a left submodule of $\frac{R[x,y,\theta,\sigma]}{\langle x^l-1,\ y^m-1\rangle}$. Then a minimal set $B = \{f_1, f_2, \cdots, f_s\} \subseteq M$ is called a consistent set of M if it satisfies the following conditions:*

1. $f_i \ngeq f_j,\ \ 1 \leq i,j \leq s,\ \ i \neq j$, if the lex-leading coefficients of f_i, f_j are either both unit or both non-units.

2. for any $f \in M$ such that the lex-leading coefficient of f is a unit, there exists some $f_i, 1 \leq i \leq s$, with its leading coefficient a unit such that $f \geq f_i$.

3. *for any $f \in M$ such that the lex-leading coefficient a non-unit, there exists some $f_j \in S, 1 \leq j \leq s$, such that $f \geq f_j$.*

Theorem 6.3.6. *Let $f(x,y), g(x,y)$ be two polynomials in $R[x,y,\theta,\sigma]$ such that $f(x,y) \geq g(x,y)$ and the lex-leading coefficient of $g(x,y)$ is a unit. Then there exist two polynomials $q(x,y)$ and $r(x,y)$ in $R[x,y,\theta,\sigma]$ such that*

$$f(x,y) = q(x,y)g(x,y) + r(x,y),$$

where $r(x,y) = 0$ or $r(x,y) \ngeq g(x,y)$.

Proof: The proof is similar to that of Theorem 2.7 in [65]. ■

Theorem 6.3.7. *Let C be a 2D skew-cyclic code of length ml over R. If C has a consistent set $B = \{f_1, f_2, \cdots, f_s\}$ such that the lex-leading coefficient of each f_i is a unit, then $C = \langle f_1, f_2, \cdots, f_s \rangle$.*

Proof: After reordering the polynomials in B, if necessary, we may assume that $f_1 \succ f_2 \succ \cdots \succ f_s$. This strict ordering is possible because $f_i \ngeq f_j$ for $i \neq j$. Let $f(x,y) \in C$. Then by the definition of the consistent set, there exists a polynomial $f_{i_1} \in B$ such that $f(x,y) \geq f_{i_1}$. Since the lex-leading coefficient of f_{i_1} is a unit, by Theorem 6.3.6, there exist polynomials $q_1(x,y), r_1(x,y) \in R[x,y,\theta,\sigma]$ such that

$$f(x,y) = q_1(x,y)f_{i_1} + r_1(x,y),$$

where $r_1(x,y) = 0$ or $r_1(x,y) \ngeq f_{i_1}$. Now $r_1(x,y) \in C$ as C is a linear code. Therefore there exists a polynomial $f_{i_2} \in B$ such that $r_1(x,y) \geq f_{i_2}$. Again from Theorem 6.3.6, there exist $q_2(x,y), r_2(x,y) \in R[x,y,\theta,\sigma]$ such that $r_1(x,y) = q_2(x,y)f_{i_2} + r_2(x,y)$ with $r_2(x,y) = 0$ or $r_2(x,y) \ngeq f_{i_2}$. Repeat the above process until we get $r_k(x,y) = 0$ for some k. Then we have

$$f(x,y) = q_1(x,y)f_{i_1} + q_2(x,y)f_{i_2} + \cdots + q_k(x,y)f_{i_k}.$$

Hence the result. ■

Example 6.3.8. *Let $R = \mathbb{F}_3 + w\mathbb{F}_3$. Let $\theta_1 = \theta$ and θ_2 be the identity map. Let C_θ be a 2D skew-cyclic code of length 3×2 generated by $f(x, y) = x^2y + x + 1, i.e., C = \langle x^2y + x + 1\rangle$. Then a spanning set for C is*

$$S = \{f(x, y), xf(x, y), x^2f(x, y), yf(x, y), xyf(x, y), x^2yf(x, y)\},$$

which is equivalent, in matrix form, to the set

$$\left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

C has a subset $B = \{x + 2, 1 + y\}$ which satisfies the properties of a consistent set of C. Therefore B is a generating set for C, i.e., $C = \langle x + 2, 1 + y\rangle$.

Example 6.3.9. *Let $R = \mathbb{F}_3 + w\mathbb{F}_3$. Let C_θ be a 2D skew-cyclic code of length 2×2 generated by $f(x, y) = (w + 1) + (w + 1)y + (w + 2)x + wxy$, i.e.,*

$$C = \langle (w + 1) + (w + 1)y + (w + 2)x + wxy\rangle.$$

Then a spanning set for C is

$$S = \{f(x, y), yf(x, y), xf(x, y), xyf(x, y)\} \ .$$

Now $B = \{x + 1, 1 - y\}$ forms a consistent set of C, therefore B is a generating set for C, i.e., $C = \langle x + 1, 1 - y\rangle$. Moreover $\Phi(C)$ has parameters $[\mathbf{8}, \mathbf{6}, \mathbf{2}]$, which is an optimal code over $\mathbb{F}_3$.

In the next theorem we consider a special case of Theorem 6.3.7.

Theorem 6.3.10. *Let C be a 2D skew-cyclic code of length ml over R. If C contains a polynomial $g(x, y)$ with its lex-leading coefficient a unit such that $g(x, y) \leq c(x, y)$ for all $c(x, y) \in C$, then $C = \langle g(x, y)\rangle$ and $g(x, y) \mid (x^l - 1)(y^m - 1)$. Moreover, the set*

$$S = \left\{ \begin{array}{cccc} g(x,y), & xg(x,y), & \cdots, & x^{l-a-1}g(x,y) \\ yg(x,y), & yxg(x,y), & \cdots, & yx^{l-a-1}g(x,y) \\ \vdots & \vdots & \ddots & \vdots \\ y^{m-b-1}g(x,y), & y^{m-b-1}xg(x,y), & \cdots, & y^{m-b-1}x^{l-a-1}g(x,y) \end{array} \right\}$$

forms a basis for C, and hence $|C| = |R|^{(l-a)(m-b)}$, where $(a, b) =$ lexdeg $g(x, y)$.

Proof: Let $c(x, y) \in C$ be an arbitrary element. Let lexdeg $g(x, y) = (a, b)$. Since $g(x, y) \in C$ such that $g(x, y) \leq c(x, y)$, by Theorem 6.3.6, there exist polynomials $q(x, y), r(x, y) \in R[x, y, \theta, \sigma]$ such that

$$c(x, y) = q(x, y)g(x, y) + r(x, y) \ ,$$

where $r(x, y) = 0$ or $r(x, y) \ngeq g(x, y)$. Suppose $r(x, y) \neq 0$. Since C is a linear code, $r(x, y) \in C$. But then $g(x, y) \nleq r(x, y)$ gives a contradiction. Therefore $r(x, y) = 0$. Hence $C \subseteq \langle g(x, y)\rangle$. Also, $\langle g(x, y)\rangle \subseteq C$ is obvious. So $C = \langle g(x, y)\rangle$.

Again by applying Theorem 6.3.6 on $(x^l - 1)(y^m - 1)$ and $g(x, y)$, we have $(x^l - 1)(y^m - 1) = Q(x, y)g(x, y) + L(x, y)$ for some $Q(x, y), L(x, y) \in R[x, y, \theta, \sigma]$, with $L(x, y) = 0$ or $L(x, y) \ngeq g(x, y)$. In $R_{m,l}$, the above relation reduces to $L(x, y) = -Q(x, y)g(x, y) \in C$. Since $g(x, y)$ has its lex-leading coefficient a unit, it follows from $L(x, y) \ngeq g(x, y)$ that $L(x, y) = 0$. Hence $g(x, y) \mid (x^l - 1)(y^m - 1)$.

Now for any $c(x, y) \in C$, we have $c(x, y) = q(x, y)g(x, y)$ for some $q(x, y) \in R[x, y, \theta, \sigma]$. Since lexdeg $c(x, y) \leq (l - 1, m - 1)$ and lexdeg $c(x, y) \leq$ lexdeg $q(x, y)$ + lexdeg $g(x, y)$, it follows that lexdeg $q(x, y) \leq (l - a - 1, m - b - 1)$. This proves that S spans C.

For R-linear independence of S, let $a(x, y)g(x, y) = 0$ (in $R_{m,l}$) for some $a(x, y) = \sum\limits_{i=0}^{l-a-1} \sum\limits_{j=0}^{m-a-1} a_{i,j}x^i y^j \ , \ a_{i,j} \in R$. Then, in $R[x, y, \theta, \sigma]$,

$$a(x, y)g(x, y) = a_1(x, y)(x^l - 1) + a_2(x, y)(y^m - 1) \tag{6.1}$$

for some $a_1(x, y), a_2(x, y) \in R[x, y, \theta, \sigma]$ with lexdeg $a_1(x, y)$, lexdeg $a_2(x, y) \leq (l - a - 1, m - b - 1)$. Since the lex-degree of L.H.S of (6.1) is at most $(l - 1, m - 1)$, it follows that $a(x, y)$ must be zero. Hence all $a_{i,j} = 0$, and so S is R-linearly independent. ■

Example 6.3.11. *Let $R = \mathbb{F}_3 + w\mathbb{F}_3$. Let C_θ be a 2D skew-cyclic code of length $6 = 3 \times 2$ over R, defined by $C_\theta = \langle 2 + 2y + (w + 1)x + (w + 1)xy + 2wx^2y + 2wx^2y^2\rangle$. Then the vector form of code C_θ is given by the following set.*

$$\left\{\begin{array}{cc}
(0,0,0,0,0,0), & (w+1,w+1,2w+2,2w+2,0,0) \\
(2,2w+1,w+1,2w,2w), & (w+2,w+2,w+1,w+1,w,w) \\
(w,w,w,w,w,w), & (w,w,w+2,w+2,w+1,w+1) \\
(w+1,w+1,w,w,w+2,w+2), & (w,w,2,2,2w+1,2w+1) \\
(2w+2,2w+2,2,2,w+2,w+2), & (2w,2w,2,2,w+1,w+1) \\
(0,0,1,1,2,2), & (2w,2w,2w+1,2w+1,2w+2,2w+2) \\
(1,1,0,0,2,2), & (w+1,w+1,0,0,2w+2,2w+2) \\
(w+2,w+2,2w+2,2w+2,2,2), & (1,1,w+2,w+2,2w,2w) \\
(2w,2w,w+2,w+2,1,1), & (0,0,2w+1,2w+1,w+2,w+2) \\
(1,1,2w,2w,w+2,w+2), & (2,2,2w,2w,w+1,w+1) \\
(2w+1,2w+1,2w,2w,2w+2,2w+2), & (2,2,2,2,2,2) \\
(w+2,w+2,0,0,2w+1,2w+1), & (2w+2,2w+2,0,0,w+1,w+1) \\
(w+2,w+2,1,1,2w,2w), & (w+2,w+2,w,w,w+1,w+1) \\
(0,0,w,w,2w,2w), & (2,2,2w+2,2w+2,w+2,w+2) \\
(2w,2w,1,1,w+2,w+2), & (2w+1,2w+1,w+2,w+2,0,0) \\
(0,0,w+1,w+1,2w+2,2w+2), & (1,1,w+1,w+1,2w+1,2w+1) \\
(2w+2,2w+2,w+1,w+1,0,0), & (w,w,0,0,2w,2w) \\
(w,w,w+1,w+1,w+2,w+2), & (0,0,w+2,w+2,2w+1,2w+1) \\
(w,w,2w+2,2w+2,1,1), & (2w+2,2w+2,w,w,1,1) \\
(1,1,w,w,2w+2,2w+2), & (2w,2w,2w+2,2w+2,2w+1,2w+1) \\
(2w,2w,2w,2w,2w,2w), & (1,1,2w+2,2w+2,w,w) \\
(2w+2,2w+2,2w+2,2w+2,2w+2,2w+2), & (2w+2,2w+2,1,1,w,w) \\
(w+1,w+1,2w+1,2w+1,1,1), & (w+1,w+1,w+2,w+2,w,w) \\
(w+2,w+2,w+2,w+2,w+2,w+2), & (2,2,2w+1,2w+1,w,w) \\
\underline{\boldsymbol{(2,\ 2,\ 1,\ 1,\ 0,\ 0)}}, & (2w+1,2w+1,w,w,2,2) \\
(2w,2w,0,0,w,w), & (w,w,2w+1,2w+1,2,2) \\
(w+1,w+1,w+1,w+1,w+1,w+1), & (0,0,2w+2,2w+2,w+1,w+1) \\
(2w+1,2w+1,0,0,w+2,w+2), & (w+2,w+2,2,2,2w+2,2w+2) \\
(w+2,w+2,2w,2w,1,1), & (1,1,2,2,0,0) \\
(2w+1,2w+1,2w+1,2w+1,2w+1,2w+1), & (w+1,w+1,2,2,2w,2w) \\
(w+1,w+1,2w,2w,2,2), & (2,2,w+2,w+2,2w+2,2w+2) \\
(w+2,w+2,2w+1,2w+1,0,0), & (w,w,2w,2w,0,0) \\
(2w+2,2w+2,2w,2w,2w+1,2w+1), & (0,0,2w,2w,w,w) \\
(2w+1,2w+1,2w+2,2w+2,2w,2w), & (2w+1,2w+1,1,1,w+1,w+1) \\
(0,0,2,2,1,1), & (1,1,2w+1,2w+1,w+1,w+1) \\
(w+1,w+1,1,1,2w+1,2w+1), & (2w+1,2w+1,2,2,w,w) \\
(2w+2,2w+2,w+2,w+2,2,2), & (2w+1,2w+1,w+1,w+1,1,1) \\
(2,2,w,w,2w+1,2w+1), & (2w,2w,w+1,w+1,2,2) \\
(1,1,1,1,1,1), & (2,2,0,0,1,1) \\
(2w,2w,w,w,0,0), & (w,w,1,1,2w+2,2w+2) \\
(2w+2,2w+2,2w+1,2w+1,2w,2w) &
\end{array}\right\}$$

C_θ contains a monic polynomial $g(x, y) = x - y - 1 + xy$ (underlined in the table) such that $g(x, y) \leq c(x, y)$ for all $c(x, y) \in C_\theta$. Therefore $C_\theta = \langle g(x, y)\rangle$. Also $g(x, y) = x - y - 1 + xy = (x - 1)(y + 1)$, which divides $(x^3 - 1)(y^2 - 1)$. By Theorem 6.3.10, a spanning set for C_θ is

$$S = \{g(x, y), xg(x, y)\} \ ,$$

which is equivalent, in matrix form, to the set

$$S = \left\{ \begin{bmatrix} -1 & -1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ -1 & -1 \\ 1 & 1 \end{bmatrix} \right\}.$$

$|C_\theta| = |R|^{(3-1)(2-1)} = 9^2 = 81$. *The parameters of C_θ and $\Phi(C_\theta)$ are $(6, 9^2, 2_G)$ and $[12, 4, 2]$, respectively.*

The next result presents a division algorithm when the lex-leading coefficient of the divisor is not a unit.

Lemma 6.3.12. *Let $f(x, y), g(x, y) \in R[x, y, \theta, \sigma]$ be two polynomials such that both have their lex-leading coefficients non-units and $g(x, y) \leq f(x, y)$. Then there exist two polynomials $q(x, y), r(x, y) \in R[x, y, \theta, \sigma]$ such that*

$$f(x, y) = q(x, y)g(x, y) + r(x, y),$$

where $r(x, y) = 0$ or $r(x, y) \prec g(x, y)$ or $r(x, y)$ has the lex-leading coefficient a unit with lex-degree at most lexdeg $f(x, y)$.

Proof: Let $f(x, y)$ and $g(x, y)$ have lex-degrees (k_1, s_1) and (k_2, s_2), respectively. Since $g(x, y) \leq f(x, y)$, we have $k_2 \leq k_1, s_2 \leq s_1$. Now since the lex-leading coefficient of $f(x, y)$ is a non-unit, it is either $a(1 + w)$ or $b(1 - w)$ for some $a, b \in \mathbb{F}_q$. Similarly, the lex-leading coefficient of $g(x, y)$ is either $c(1 + w)$ or $d(1 - w)$ for some $c, d \in \mathbb{F}_q$. Suppose the lex-leading coefficient of $f(x, y)$ is $a(1 + w)$ (the result can similarly be proved when the lex-leading coefficient of $f(x, y)$ is $b(1 - w)$). Also suppose that the lex-leading coefficient of $g(x, y)$ is $c(1 + w)$. Define a polynomial

$$H(x, y) = f(x, y) - l(x, y)g(x, y) \ , \tag{6.2}$$

where

$$l(x, y) = \begin{cases} a\sigma^{s_1 - s_2}(c^{-1})x^{k_1 - k_2}y^{s_1 - s_2}, & \text{if } k_1 - k_2 \text{ is odd} \\ -a\sigma^{s_1 - s_2}(c^{-1})x^{k_1 - k_2}y^{s_1 - s_2}, & \text{otherwise.} \end{cases}$$

(We can similarly choose $l(x, y)$ for the case when the lex-leading coefficient of $g(x, y)$ is $d(1 - w)$). Note that we have $\theta(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_q$, $\sigma(w) = w$, and if $k_1 - k_2$ is odd, $\theta^{k_1 - k_2}(c(1 + w)) = c(1 - w)$.

In (6.2), $H(x, y) = 0$ or $H(x, y)$ has the lex-leading coefficient a unit or the lex-leading coefficient of $H(x, y)$ is a non-unit and $H(x, y) \prec f(x, y)$. Now (6.2) can be written as

$$f(x, y) = l(x, y)g(x, y) + H(x, y). \tag{6.3}$$

If $H(x, y) = 0$ or the lex-leading coefficient of $H(x, y)$ is a unit, then we are done. Now suppose $H(x, y) \prec f(x, y)$. If $H(x, y) \prec g(x, y)$, then we are done. Suppose $H(x, y) \succeq g(x, y)$. Then replace $f(x, y)$ by $H(x, y)$ in (6.2), and repeat the process to get a polynomial $H_1(x, y)$ such that

$$H(x, y) = q_1(x, y)g(x, y) + H_1(x, y),$$

where $H_1(x, y) = 0$ or the lex-leading coefficient of $H_1(x, y)$ is a unit or the lex-leading coefficient of $H(x, y)$ is a non-unit and $H_1(x, y) \prec H(x, y)$. Now if $H_1(x, y) = 0$ or the lex-leading coefficient of $H_1(x, y)$ is a unit, then substitute the corresponding value of $H(x, y)$ in (6.3), and we are done. Otherwise keep on repeating the process until we get $H_k(x, y)$ such that $f(x, y) = (q(x, y) + q_1(x, y) + q_2(x, y) + \cdots + q_k(x, y))g(x, y) + H_k(x, y)$ with $H_k(x, y) = 0$ or $H_k(x, y)$ has the lex-leading coefficient a unit or $H_k(x, y) \prec g(x, y)$. Hence the result. ■

Lemma 6.3.13. *Let C be a 2D skew-cyclic code over R such that it does not contain any polynomial with its lex-leading coefficient a unit. Let $f(x, y), g(x, y)$ be any two* *polynomials in C such that $g(x,y) \leq f(x,y)$. Then there exist two polynomials $q(x,y)$ and $r(x,y)$ such that*

$$f(x,y) = q(x,y)g(x,y) + r(x,y),$$

where $r(x,y) = 0$ or $r(x,y) \prec g(x,y)$.

Proof: The proof is straightforward by Lemma 6.3.12 and the fact that there is no polynomial in C with its lex-leading coefficient a unit. ■

Theorem 6.3.14. *Let C be a 2D skew-cyclic code of length ml in $R[x,y,\theta,\sigma]$ such that it does not contain any polynomial with its lex-leading coefficient a unit. Let $B = \{f_1, f_2, \cdots, f_m\}$ be a consistent set of C. Then $C = \langle f_1, f_2, \cdots, f_m \rangle$.*

Proof: We start as in the proof of Theorem 6.3.7. Let $f(x,y) \in C$. Then by the definition of the consistent set, there exists a polynomial $f_{i_1} \in B$ such that $f \geq f_{i_1}$. By Lemma 6.3.13, there exist $q(x,y), r_1(x,y) \in R[x,y,\theta,\sigma]$ such that

$$f(x,y) = q(x,y)f_{i_1} + r(x,y),$$

where $r(x,y) = 0$ or $r(x,y) \prec f_{i_1}$. Now $r(x,y) \in C$, as C is a linear code. Therefore there exists a polynomial $f_{i_2} \in B$ such that $r(x,y) \geq f_{i_2}$. Again by Lemma 6.3.13, there exist $q_1(x,y), r_1(x,y) \in R[x,y,\theta,\sigma]$ such that $r(x,y) = q_1(x,y)f_{i_2} + r_1(x,y)$, with $r_1(x,y) = 0$ or $r_1(x,y) \prec f_{i_2}$. Repeat the above process until we get $r_{s-1}(x,y) = 0$ for some s. Then we have

$$f(x,y) = q(x,y)f_{i_1} + q_1(x,y)f_{i_2} + \cdots + q_{s-1}(x,y)f_{i_s}.$$

Hence the result. ■

Example 6.3.15. *Let $R = \mathbb{F}_3 + w\mathbb{F}_3$. Let C_θ be the 2D skew-cyclic code of length 2×2 over R generated by $f(x,y) = (w+2) + (1+2w)y + (w+1)x$, i.e., $C_\theta = \langle (w+2) + (1+2w)y + (w+1)x \rangle$. Therefore a spanning set for C_θ is*

$$S = \{f(x,y), yf(x,y), xf(x,y), xyf(x,y)\} ,$$

which is equivalent (in matrix form) to the set

$$\left\{ \begin{bmatrix} w+2 & 2w+1 \\ w+1 & 0 \end{bmatrix}, \begin{bmatrix} 2w+1 & w+2 \\ 0 & w+1 \end{bmatrix}, \begin{bmatrix} 2w+1 & 0 \\ 2w+2 & w+1 \end{bmatrix}, \begin{bmatrix} 0 & 2w+1 \\ w+1 & 2w+2 \end{bmatrix} \right\}.$$

The corresponding code (in vector form) is given as

$$\left\{ \begin{array}{ccc}
(2w+1,0,0,2w+2), & (w+2,w+2,0,2w+2), & (0,w+2,2w+2,0) \\
(2w+1,2w+1,2w+2,2w+2), & (0,w+2,w+1,w+1), & (0,2w+1,w+1,0), \\
(2w+1,0,0,w+1), & (w+2,w+2,0,w+1), & (w+2,0,w+1,2w+2), \\
(0,2w+1,2w+2,2w+2), & (2w+1,0,w+1,w+1), & (2w+1,2w+1,0,0), \\
(w+2,0,w+1,0), & (2w+1,w+2,w+1,2w+2), & (w+2,w+2,2w+2,0), \\
(0,0,2w+2,w+1), & (w+2,0,0,2w+2), & (w+2,2w+1,w+1,w+1), \\
(2w+1,2w+1,2w+2,w+1), & (w+2,0,0,w+1), & (0,w+2,w+1,2w+2), \\
(0,2w+1,0,0), & (0,2w+1,2w+2,w+1), & (w+2,w+2,2w+2,2w+2), \\
(2w+1,2w+1,0,2w+2), & (2w+1,0,w+1,2w+2), & (w+2,2w+1,w+1,0), \\
(2w+1,2w+1,0,w+1), & (0,0,w+1,0), & (2w+1,0,2w+2,0), \\
(0,2w+1,0,2w+2), & (w+2,2w+1,w+1,2w+2), & (w+2,w+2,0,0), \\
(0,0,0,2w+2), & (2w+1,2w+1,2w+2,0), & (0,2w+1,0,w+1), \\
(w+2,0,2w+2,2w+2), & (0,0,0,0), & (2w+1,w+2,2w+2,2w+2), \\
(0,0,0,w+1), & (w+2,w+2,2w+2,w+1), & (0,0,w+1,w+1), \\
(0,2w+1,2w+2,0), & (2w+1,2w+1,w+1,w+1), & (0,w+2,2w+2,2w+2), \\
(2w+1,w+2,w+1,0), & (w+2,0,2w+2,0), & (w+2,2w+1,0,2w+2), \\
(0,2w+1,w+1,w+1), & (w+2,0,2w+2,w+1), & (0,w+2,w+1,0), \\
(2w+1,w+2,0,0), & (2w+1,0,2w+2,2w+2), & (2w+1,w+2,2w+2,w+1), \\
(w+2,2w+1,0,w+1), & (0,0,w+1,2w+2), & (0,w+2,0,0), \\
(w+2,w+2,w+1,0), & (w+2,2w+1,2w+2,2w+2), & (2w+1,2w+1,w+1,2w+2), \\
(0,w+2,2w+2,w+1), & (w+2,2w+1,2w+2,0), & (0,2w+1,w+1,2w+2), \\
(0,0,2w+2,0), & (w+2,w+2,w+1,w+1), & (2w+1,0,2w+2,w+1), \\
(2w+1,w+2,0,2w+2), & \underline{(w + 2,\ 0,\ 0,\ 0)}, & (w+2,2w+1,0,0), \\
(2w+1,w+2,0,w+1), & (w+2,2w+1,2w+2,w+1), & (w+2,0,w+1,w+1), \\
(2w+1,0,w+1,0), & (0,w+2,0,2w+2), & (2w+1,w+2,w+1,w+1), \\
(2w+1,2w+1,w+1,0), & (0,0,2w+2,2w+2), & (w+2,w+2,w+1,2w+2), \\
(2w+1,0,0,0), & (0,w+2,0,w+1), & (2w+1,w+2,2w+2,0)
\end{array} \right\}$$

The set $B = \{w+2\}$ is a consistent set of C_θ. So $C_\theta = \langle w+2 \rangle$, where $w+2$ is being considered as a constant bivariate polynomial over R.

The following theorem deals with the case when in a 2D skew-cyclic code C there is a polynomial with its lex-leading coefficient a unit but the polynomial is not of minimal lex-degree.

Theorem 6.3.16. *Let C be a 2D skew-cyclic code over R containing a minimum lex-degree polynomial f_k having its lex-leading coefficient a unit. Let $S = \{f_1, f_2, \cdots, f_k, f_{k+1}, f_{k+2}, \cdots, f_{k+s}\} \subseteq C$ such that $f_j \prec f_i$ for $j > i$ and f_i have their lex-leading coefficients units for $i = 1, 2, \cdots, k$ and non-units otherwise. Also S satisfies the following conditions:*

1. *for $f_i, f_j, f_{i'}, f_{j'} \in S$, $f_i \not\geq f_j$ for $i \neq j, 1 \leq i, j \leq k$ and $f_{i'} \not\geq f_{j'}$ for $i' \neq j', k+1 \leq i', j' \leq k+s$.*
2. *for all $f(x,y) \in C$ such that $f(x,y) \succeq f_k$, there exists $f_i \in S$ such that $f(x,y) \geq f_i$ for some $i \leq k$.*
3. *for any $f(x,y) \in C$ having its lex-leading coefficient a non-unit, there exists $f_j \in S$ such that $f(x,y) \geq f_j$ for some $j > k$.*

Then S forms a generating set for C, i.e., $C = \langle f_1, f_2, \cdots, f_k, f_{k+1}, f_{k+2}, \cdots, f_{k+s}\rangle$.

Proof: Let $c(x,y) \in C$ be any codeword.

Case 1: Suppose $c(x,y) \prec f_k$. Then the lex-leading coefficient of $c(x,y)$ must be a non-unit, as f_k is a minimum lex-degree polynomial in C having its lex-leading coefficient a unit. Therefore there exists $f_{j_1}, k+1 \leq j_1 \leq k+s$, such that $c(x,y) \geq f_{j_1}$. By Theorem 6.3.12,

$$c(x,y) = Q_1(x,y)f_{j_1} + H_1(x,y)$$

for some $Q_1(x,y), H_1(x,y) \in R[x,y,\theta,\sigma]$, where $H_1(x,y) = 0$ or $H_1(x,y) \prec f_{j_1}$ or $H_1(x,y)$ has the lex-leading coefficient a unit with lex-degree at most lexdeg $c(x,y)$. Now proceeding as in Theorem 6.3.14, we get $f_{j_1}, \cdots, f_{j_{k'}}$ such that $c(x,y) = Q_1(x,y)f_{j_1} + Q_2(x,y)f_{j_2} + \cdots + Q_k(x,y)f_{j_{k'}}$.

Case 2: Suppose $c(x,y) \succeq f_k$.

Subcase 1: Suppose $c(x,y)$ has its lex-leading coefficient a unit. Then $c(x,y) \succeq f_k$, and so there exist $f_{i_1} \in S, 1 \leq i_1 \leq k$ such that $c(x,y) \geq f_{i_1}$. So by Theorem 6.3.6, we have

$$c(x,y) = q_1(x,y)f_{i_1} + r_1(x,y), \tag{6.4}$$

for some $q_1(x,y), r_1(x,y) \in R[x,y,\theta,\sigma]$ such that $r_1(x,y) = 0$ or $r_1(x,y) \ngeq f_{i_1}$. Subcase 2: Suppose $c(x,y)$ has its lex-leading coefficient a non-unit. Then there exists $f_{i_2} \in S, k+1 \leq i_2 \leq k+s$ such that $c(x,y) \geq f_{i_2}$, and so by Theorem 6.3.12, we have

$$c(x,y) = q_1'(x,y)f_{i_2} + r_1'(x,y), \tag{6.5}$$

for some $q_1'(x,y), r_1'(x,y) \in R[x,y,\theta,\sigma]$ such that $r_1'(x,y) = 0$ or $r_1'(x,y) \prec f_{i_2}$ or $r_1'(x,y)$ has its lex-leading coefficient a unit. If $r_1'(x,y) = 0$, then we are done. If $r_1'(x,y) \prec f_{i_2}$, then obviously $r_1'(x,y) \prec f_k$, so go to Case 1. Suppose $r_1'(x,y)$ has its lex-leading coefficient a unit. Then go back to Subcase 1 and repeat the steps by replacing $c(x,y)$ by $r_1'(x,y)$. After this, suppose we are left with a remainder $r_2(x,y)$. Check whether $r_2(x,y) \prec f_k$. If so, go to Case 1. Otherwise, repeat all the steps from initial stage by replacing $c(x,y)$ by $r_2(x,y)$ until we get a remainder $r_s(x,y) \prec f_k$ such that

$$c(x,y) = q_1(x,y)f_{i_1} + q_2(x,y)f_{i_2} + \cdots + q_s(x,y)f_{i_s} + H(x,y), \tag{6.6}$$

where $H(x,y) = r_s(x,y)$. Now $H(x,y) \prec f_k$, and so by replacing $c(x,y)$ by $H(x,y)$ in Case 1, we get $H(x,y) = Q_1(x,y)f_{j_1} + Q_2(x,y)f_{j_2} + \cdots + Q_k(x,y)f_{j_{k'}}$. The result follows by substituting $H(x,y)$ in (6.6).

■

Example 6.3.17. *Let C be a 2D skew-cyclic code defined as $C = \langle f(x,y), g(x,y)\rangle$, where $g(x,y) = (w+2)+(2w+1)y+(w+1)x$ and $f(x,y) = 1+y+x+xy$. Therefore the set*

$$S = \{f(x,y), g(x,y), yg(x,y), xg(x,y), yxg(x,y)\}$$

forms a spanning set of C, which is equivalent (in matrix form) to the set

$$\left\{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} w+2 & 2w+1 \\ w+1 & 0 \end{bmatrix}, \begin{bmatrix} 2w+1 & w+2 \\ 0 & w+1 \end{bmatrix}, \begin{bmatrix} 1+2w & 0 \\ 2+2w & w+1 \end{bmatrix}, \begin{bmatrix} 0 & 1+2w \\ w+1 & 1+2w \end{bmatrix}\right\}.$$

Now C has a set $S = \{f_1, f_2\}$, where $f_1 = 1+y$, which is a minimal lex-degree polynomial in C having its lex-leading coefficient a unit, and $f_2 = w+2$, the minimum *lex-degree polynomial in C, having its lex-leading coefficient a non-unit. The set S satisfies the properties of a consistent set of C. Therefore S is a generating set for $C, i.e, C = \langle 1 + y, w + 2\rangle$.*

Theorem 6.3.18. *Let C be a 2D skew-cyclic code of length ml over R such that $gcd(l, |\theta|) = 1$ and $gcd(m, |\sigma|) = 1$. Then C is a 2D-cyclic code of same length over R.*

Proof: Let C_1 and C_2 be the associated codes of C, as defined in the beginning of this section. Then C_1, C_2 are skew quasi-cyclic codes over R of indices m and l, respectively. To show C is a 2D-cyclic code over R, it suffices to show that C_1 and C_2 are quasi-cyclic codes over R. We prove the result for C_1, the same can similarly be proved for C_2. Let $c(x, y) = \sum_{i=0}^{l-1} \sum_{j=0}^{m-1} c_{i,j}x^iy^j \in C$ and $|\theta| = k$. Since $gcd(k, l) = 1$, there exist two integers a and b such that $al + bk = 1$. Therefore $bk = 1 - al$. Now consider

$$\begin{aligned} x^{bk}c(x, y) &= x^{bk}\sum_{i=0}^{l-1}\sum_{j=0}^{m-1} c_{i,j}x^iy^j \\ &= \sum_{i=0}^{l-1}\sum_{j=0}^{m-1} \theta^{bk}(c_{i,j})x^{i+1-al}y^j. \end{aligned}$$

Therefore $x^{bk}c(x, y) = \sum_{i=0}^{l-1} \sum_{j=0}^{m-1} c_{i,j}x^{i+1}y^j$, since $x^l = 1$ and $\theta^k(r) = r$ for all $r \in R$ (as the order of θ is k). Now $x^{bk}c(x, y) \in C$ shows that $\sum_{i=0}^{l-1} \sum_{j=0}^{m-1} c_{i,j}x^{i+1}y^j \in C$ whenever $\sum_{i=0}^{l-1} \sum_{j=0}^{m-1} c_{i,j}x^iy^j \in C$. So C_1 is a quasi-cyclic code (of index m) over R . Similarly we can prove that C_2 is also a quasi-cyclic code (of index l) over R. Hence C is a 2D-cyclic code over R. ■

Lemma 6.3.19. *Let C' be a left submodule of $\frac{R[y,\theta\sigma]}{\langle y^n-1\rangle}$, where $n = ml$ and let C be a left submodule of $\frac{R[x,y,\theta,\sigma]}{\langle x^l-1,\ y^m-1\rangle}$. Let a map $\pi : C' \to C$ be defined as*

$$\pi\left(\sum_{i=0}^{ml-1} a_iy^i\right) = \sum_{j=0}^{l-1}\sum_{k=0}^{m-1} a_{j,k}x^jy^k,$$

where $y^m = x$ and $j = i\ (mod\, l)$, $k = i\ (mod\, m)$. Then π is a bijection iff $gcd(m, l) = 1$.

Proof: The proof follows from the fact that if $a = b \pmod{n_1}$ and $a = b \pmod{n_2}$, then $a = b$ (mod n_1n_2) iff $gcd(n_1, n_2) = 1$. ■

Theorem 6.3.20. *A 2D skew-cyclic code of length n $(= ml)$ over R is equivalent to a skew-cyclic code of length n if $gcd(m, l) = 1$.*

Proof: Let $gcd(m, l) = 1$. Since C is a 2D skew-cyclic code of length ml over R, it is a left submodule of $\frac{R[x,y,\theta,\sigma]}{\langle x^l-1,\ y^m-1\rangle}$. Define a submodule C' of $\frac{R[y,\theta\sigma]}{\langle y^n-1\rangle}$ such that C' is equivalent to C by Lemma 6.3.19. Let $a(y) \in C'$ be an arbitrary polynomial, where $a(y) = \sum_{i=0}^{ml-1} a_i y^i$. To show C is equivalent to a skew-cyclic code, it suffices to show that C' is a skew-cyclic code over R. Consider

$$\begin{aligned} ya(y) &= y\sum_{i=0}^{ml-1} a_i y^i \\ &= \sum_{i=0}^{ml-1} y a_i y^i \\ &= \sum_{i=0}^{ml-1} \theta\sigma(a_i) y^{i+1}. \end{aligned} \tag{6.7}$$

Let π be the corresponding bijection between C and C'. Then

$$\begin{aligned} \pi(ya(y)) &= \pi(\sum_{i=0}^{ml-1} \theta\sigma(a_i)y^{i+1}) \\ &= \sum_{j=0}^{l-1}\sum_{k=0}^{m-1} \theta\sigma(a_{j,k})x^{(i+1) \text{ mod } l}y^{(i+1) \text{ mod } m} \\ &= \sum_{j=0}^{l-1}\sum_{k=0}^{m-1} xya_{j,k}x^{i \text{ mod } l}y^{i \text{ mod } m} \qquad (\text{as } xya = \theta\sigma(a)xy) \\ &= xy\sum_{j=0}^{l-1}\sum_{k=0}^{m-1} a_{j,k}x^{i \text{ mod } l}y^{i \text{ mod } m} \\ &= xy\pi(a(y)). \end{aligned}$$

Since $\pi(a(y)) \in C$, and C is a 2D skew-cyclic codes over R, $xy\pi(a(y)) \in C$. Therefore the pre-image of $xy\pi(a(y))$, i.e., $ya(y)$, which is a skew-cyclic shift of $a(y)$ (by (6.7)), will also belong to C'. Hence C' is a skew-cyclic code of length n over R with automorphism $\theta\sigma$. The result follows. ■

Corollary 6.3.20.1. *Let C be a 2D skew-cyclic code of length ml over R. If $gcd(m, l) = 1$ and $\theta\sigma$ is the identity map on R, then C is equivalent to a cyclic code of length ml over R.*

6.4 Duals of 2D skew-cyclic codes over R

In this section, the duals of 2D skew-cyclic codes of length n $(= ml)$ over R, when $|\theta|$ divides l and $|\sigma|$ divides m, have been studied. The subcodes of such codes, which are themselves 2D skew-cyclic codes over R, are also studied.

Definition 6.4.1. *Let C be a 2D skew-cyclic code of length n over R. Then its dual $C^{\perp}$ is defined as*

$$C^{\perp} = \{a \in R^n \ : \ a \cdot c = 0 \textit{ for all } c \in C\},$$

where $a \cdot c$ is the usual Euclidean inner product of a and c in R^n.

An element $a \in R^{ml}$ can be viewed as $a = (a_0, a_1, \cdots, a_{l-1})$, where $a_i = (a_{i,0}, a_{i,1}, \cdots, a_{i,m-1}) \in R^m$. Let $T_\theta(a) = (\theta(a_{l-1}), \theta(a_0), \cdots, \theta(a_{l-2}))$, where $\theta(a_i) = (\theta(a_{i,0}), \theta(a_{i,1}), \cdots, \theta(a_{i,m-1}))$. Then C is a θ-skew quasi-cyclic code of length ml and index m over R if $T_\theta(a) \in C$ for all $a \in C$.

Lemma 6.4.2. *Let C be a θ-skew quasi-cyclic code of length ml and index m over R. If $a \in C$ and $b \in C^{\perp}$, then $\theta(b \cdot T_\theta^j(a)) = T_\theta(b) \cdot T_\theta^{j+1}(a)$.*

Proof: The proof is similar to the proof of Lemma 3.4.9 in Chapter 3. ■

Lemma 6.4.3. *Let $|\theta| \mid l$. Let C be a θ-skew quasi-cyclic code of length ml and index m over R. Then $C^{\perp}$ is also a θ-skew quasi-cyclic code of length ml and index m over R.*

Proof: Let $a \in C$ and $b \in C^{\perp}$. Then $T_\theta^{l-1}(a) \cdot b = 0$, as $T_\theta^{l-1}(a) \in C$. On applying θ both sides and by Lemma 6.4.2, we get $a \cdot T_\theta(b) = 0$, as $|\theta| \mid l$. So $T_\theta^l(a) = a$. This gives $T_\theta(b) \in C^{\perp}$. Hence $C^{\perp}$ is a θ-skew quasi-cyclic code of index m. ■

Theorem 6.4.4. *Let C be a 2D skew-cyclic code of length ml over R with the associated automorphisms θ and σ such that $|\theta| \mid l$ and $|\sigma| \mid m$. Then $C^{\perp}$ is also a 2D skew-cyclic code of same length over R.*

Proof: Since C is equivalent to a θ-skew quasi cyclic code of index m and a σ-skew quasi cyclic code of index l, the result directly follows from Lemma 6.4.3. ■

The following discussion is similar to the one given in [27, Page 9].

The ring $R[x, y, \theta, \sigma]$ can be localized to the right at the multiplicative set $S = \{x^i y^j \mid i, j \in \mathbb{N}\}$. The existence of the localization of $R[x, y, \theta, \sigma]$ follows from [86, Theorem 2], since S satisfies the following two necessary and sufficient conditions:

- (Right Ore condition:) For all $x^{i_1}y^{j_1} \in S$ and $f(x, y) \in R[x, y, \theta, \sigma]$, there exists $x^{i_2}y^{j_2} \in S$ and $g(x, y) \in R[x, y, \theta, \sigma]$ such that $f(x, y)x^{i_1}y^{j_1} = x^{i_2}y^{j_2}g(x, y)$. To prove this we note that the multiplication rule $x^i y^j a = \theta^i\sigma^j(a)x^i y^j$ allows to shift the powers of x and y from left to right by changing the coefficients.

- If for $x^{i_1}y^{j_1} \in S$ and $f(x, y) \in R[x, y, \theta, \sigma]$, we have $x^{i_1}y^{j_1}f(x, y) = 0$, then there exists $x^{i_2}y^{j_2} \in S$ such that $f(x, y)x^{i_2}y^{j_2} = 0$. Since $x^{i_2}y^{j_2}$ is not a zero-divisor, $f(x, y)$ must be zero.

This shows that the right localization $R[x, y, \theta, \sigma]S^{-1}$ exists. We have $ax^{-1}y^{-1} = x^{-1}y^{-1}\theta\sigma(a)$, where x^{-1} and y^{-1} are inverses of x and y, respectively, in this ring. Now we consider the ring $T \subset R[x, y, \theta, \sigma]S^{-1}$ consisting of the elements $\sum\limits_{i=0}^{l}\sum\limits_{j=0}^{m} x^{-i}y^{-j}a_{i,j}$, where the coefficients are on the right and where the multiplication rule is given as $ax^{-1}y^{-1} = x^{-1}y^{-1}\theta\sigma(a)$. The ring T is isomorphic to the skew polynomial ring $R[x^{-1}, y^{-1}, \theta^{-1}, \sigma^{-1}]$.

Define $\tau : R[x, y, \theta, \sigma] \to T \subset R[x, y, \theta, \sigma]S^{-1}$ as

$$\tau\left(\sum_{i=0}^{l-1}\sum_{i=0}^{m-1} a_{i,j}x^i y^j\right) = \sum_{i=0}^{l-1}\sum_{i=0}^{m-1} x^{-i}y^{-j}a_{i,j}$$

for all $a(x, y) = \sum\limits_{i=0}^{l-1}\sum\limits_{i=0}^{m-1} a_{i,j}x^i y^j$. The map τ is a ring anti-isomorphism. For instance, let $P_1 = \sum\limits_{i=0}^{r}\sum\limits_{j=0}^{t} a_{i,j}x^i y^j$ and $P_2 = \sum\limits_{i'=0}^{r'}\sum\limits_{j'=0}^{t'} b_{i,j}x^{i'}y^{j'}$ be two polynomials in $R[x, y, \theta, \sigma]$.

Then we have $\tau(P_1+P_2)=\tau(P_1)+\tau(P_2)$ and

$$\tau(P_1P_2)=\tau\left(\sum_{i=0}^{r}\sum_{j=0}^{t}a_{i,j}x^iy^j\sum_{i'=0}^{r'}\sum_{j'=0}^{t'}b_{i',j'}x^{i'}y^{j'}\right)=\tau\left(\sum_{k_1=0}^{r+r'}\sum_{k_2=0}^{t+t'}\left(\sum_{\substack{i+i'=k_1\\ j+j'=k_2}}\left(a_{i,j}\theta^i\sigma^j(b_{i',j'})\right)x^{k_1}y^{k_2}\right)\right)$$

$$=\sum_{k_1=0}^{r+r'}\sum_{k_2=0}^{t+t'}\left(\sum_{\substack{i+i'=k_1\\ j+j'=k_2}}(x^{-k_1}y^{-k_2}a_{i,j}\theta^i\sigma^j(b_{i',j'}))\right)=\sum_{k_1=0}^{r+r'}\sum_{k_2=0}^{t+t'}\left(\sum_{\substack{i+i'=k_1\\ j+j'=k_2}}\left(x^{-i'}y^{-j'}x^{-i}y^{-j}\theta^i\sigma^j(b_{i',j'})a_{i,j}\right)\right)$$

$$=\sum_{k_1=0}^{r+r'}\sum_{k_2=0}^{t+t'}\left(\sum_{\substack{i+i'=k_1\\ j+j'=k_2}}\left(x^{-i'}y^{-j'}b_{i',j'}x^{-i}y^{-j}a_{i,j}\right)\right)=\tau(P_2)\tau(P_1).$$

Definition 6.4.5. *Let* $f(x,y)=\sum\limits_{i=0}^{r}\sum\limits_{i=0}^{s}f_{i,j}x^iy^j$ *be of lex-degree* (r,s) *in* $R[x,y,\theta,\sigma]$. *Then the skew-reciprocal polynomial* $f^*(x,y)$ *of* $f(x,y)$ *is defined as* $f^*(x,y)=x^ry^s\tau(f(x,y))=\sum\limits_{i=0}^{r}\sum\limits_{i=0}^{s}x^{r-i}y^{s-j}f_{i,j}=\sum\limits_{i=0}^{r}\sum\limits_{i=0}^{s}\theta^{r-i}\sigma^{s-j}(f_{i,j})x^{r-i}y^{s-j}$.

Lemma 6.4.6. *Let* $|\theta|\mid l$ *and* $|\sigma|\mid m$. *Let* $g(x,y)$ *be a right divisor of* $(x^l-1)(y^m-1)$ *such that* $(x^l-1)(y^m-1)=h(x,y)g(x,y)$. *Then* $h^*(x,y)$ *is also a right divisor of* $(x^l-1)(y^m-1)$.

Proof: Let lexdeg $h(x,y)=(l-r,m-s)$. Applying τ on both sides of the equation $(x^l-1)(y^m-1)=h(x,y)g(x,y)$, we get

$$\tau((x^l-1)(y^m-1))=\tau(h(x,y)g(x,y)).$$

So $(x^{-l}-1)(y^{-m}-1)=\tau(g(x,y))\tau(h(x,y))$. Multiplying both sides by x^ly^m, we get

$$\begin{aligned}(x^l-1)(y^m-1)=x^ly^m(x^{-l}-1)(y^{-m}-1) &= x^ly^m\tau(g(x,y))\tau(h(x,y))\\ &= \tau(g(x,y))x^ly^m\tau(h(x,y)) \qquad (\text{as } |\theta|\mid l,\ |\sigma|\mid m)\\ &= \tau(g(x,y))x^ry^sx^{l-r}y^{m-s}\tau(h(x,y))\\ &= \tau(g(x,y))x^ry^sh^*(x,y).\end{aligned}$$

Hence the result. ■

Corollary 6.4.6.1. *In the above lemma,* $h^*(x,y)$ *is also a left divisor of* $(x^l-1)(y^m-1)$.

Proof: The proof follows from Part 3 of Theorem 6.3.4. ■

Theorem 6.4.7. *Let C be a 2D skew-cyclic code of length $n = lm$ over R with $|\theta| \mid l$ and $|\sigma| \mid m$. Let $C = \langle g(x,y)\rangle$ with $(x^l - 1)(y^m - 1) = h(x,y)g(x,y)$. Then $C' = \langle h^*(x,y)\rangle$ is also a 2D skew-cyclic code of same length over R. Moreover C' is a sub-code of $C^\perp$.*

Proof: By Lemma 6.4.6, $h^*(x,y)$ is also a right divisor of $(x^l-1)(y^m-1)$, and hence by Theorem 6.3.10, C' is a 2D skew-cyclic code over R. Also $(h^*)^*(x,y) = h(x,y)$ annihilates C, which implies that $h^*(x,y) \in C^\perp$, and so $C' \subseteq C^\perp$. ■

Example 6.4.8. *In Example 6.3.11, $C = \langle (x-1)(y+1)\rangle$. Define $C' = \langle (x^2+x+1)(y-1)\rangle$. A spanning set for C' is $\{(x^2+x+1)(y-1)\} = \{-1+y-x+xy-x^2+x^2y\}$. The codewords of C' are:*

$$\left\{\begin{array}{cc} (0,0,0,0,0,0), & (w+2,2w+1,w+2,2w+1,w+2,2w+1) \\ (2w+1,w+2,2w+1,w+2,2w+1,w+2), & (2,1,2,1,2,1) \\ (2w+2,w+1,2w+2,w+1,2w+2,w+1), & (w,2w,w,2w,w,2w) \\ (2w,w,2w,w,2w,w), & (1,2,1,2,1,2) \\ (w+1,2w+2,w+1,2w+2,w+1,2w+2) & \end{array}\right\}.$$

Therefore the parameters for C' are $(6, 9^1, 4_G)$, where 4_G is the minimum Gray weight of C'. It can easily be verified that $C' \subseteq C^\perp$. Moreover C' is properly contained in $C^\perp$, as $|C'| = 9$ and $|C^\perp| = 9^6/9^2 = 9^4$.

6.5 A decomposition of 2D skew-cyclic codes over R

Now onward, we consider $p > 2$. In this section, we decompose a 2D skew-cyclic code over R into 2D skew-cyclic codes over $\mathbb{F}_q$.

We define a map $\xi' : R \to R$ as follows:

$$\xi'(a + wb) = (a+b, a-b).$$

ξ' can be extended componentwise to $\xi : R^n \rightarrow {\mathbb{F}_q}^{2n}$. ξ is a linear map. Further, we define the Lee weight of $x \in R^n$ as $w_L(x) = w_H(\xi(x))$, where $w_H(x)$ denotes the Hamming weight of x.

Let C be a linear code of length n over R. Define two sets as follows:

$$C' = \{(a+b) : a + wb \in C\}$$

and

$$C'' = \{(a-b) : a + wb \in C\}.$$

Then clearly C', C'' are linear codes of length n over R.

Theorem 6.5.1. *Let C be a linear code of length n over R. Then $\xi(C) = C' \times C''$.*

Proof: Let $(a_0, a_1, \cdots, a_{n-1}, b_0, b_1, \cdots, b_{n-1}) \in C' \times C''$, where $a = (a_1, a_2, \cdots, a_{n-1}) \in C'$ and $b = (b_1, b_2, \cdots, b_{n-1}) \in C''$. Since $2a \in C'$ and $2b \in C''$, by definitions of C', C'', there exist a codeword $c = (c_1, c_2, \cdots, c_{n-1}) \in C$ such that $c_i = (a_i + b_i) + w(a_i - b_i)$. Now $2^{-1}\xi(c) = (a_1, a_2, \cdots, a_{n-1}, b_1, b_2, \cdots, b_{n-1}) \in \xi(C)$. Hence $C' \times C'' \subseteq \xi(C)$. Conversely, suppose $x = (a_0, a_1, \cdots, a_{n-1}, b_0, b_1, \cdots, b_{n-1}) = (a, b) \in \xi(C)$, so $2x \in \xi(C)$. Then by the definition of $\xi(C)$, there exists $c = (c_1, c_2, \cdots, c_{n-1}) \in C$ such that $c_i = (a_i + b_i) + w(a_i - b_i)$, and consequently by the definitions of C' and C'', we have $2a \in C'$ and $2b \in C''$. Hence $a \in C'$ and $b \in C''$. This implies that $\xi(C) \subseteq C' \times C''$, and so $\xi(C) = C' \times C''$. ■

Theorem 6.5.2. *Let C be a linear code over R. Then $C = (1+w)C' \oplus (1-w)C''$, where C' and C'' are two linear codes over $\mathbb{F}_q$.*

Proof: Let $a \in C'$ and $b \in C''$. Then $(a+b) + w(a-b) = (1+w)a + (1-w)b \in C$. Therefore $(1+w)C' \oplus (1-w)C'' \subseteq C$. Moreover by Theorem 6.5.1, $|C| = |\xi(C)| = |C' \times C''| = |(1+w)C' \oplus (1-w)C''|$. Hence the result. ■

Corollary 6.5.2.1. *If $C' = C''$ in Theorem 6.5.2, then $C' = C$.*

Proof: We have $C = (1+w)C' \oplus (1-w)C'' = 2C' = C'$, as 2 is an invertible element of R. ■

Theorem 6.5.3. *Let $\sigma', \sigma'' \in E$ be two automorphisms of R. Let $C_{\sigma',\sigma''} = (1+w)C' \oplus (1-w)C''$ be a linear code over R. Then C is a 2D skew-cyclic code of length n over R iff C' and C'' are 2D skew-cyclic codes over $\mathbb{F}_q$ in which the corresponding automorphisms are σ', σ'', restricted to $\mathbb{F}_q$.*

Proof: For convenience, we prove the result in polynomial form. Let $c(x, y) \in C$ be a codeword. Then $c(x, y)$ can be written as $c(x, y) = (1+w)c_1(x, y)+(1-w)c_2(x, y)$, where $c_1(x, y) \in C'$ and $c_2(x, y) \in C''$. Also we have $xc(x, y) = x((1 + w)c_1(x, y) + (1 - w)c_2(x, y)) = (1 + w)xc_1(x, y) + (1 - w)xc_2(x, y)$, as w is fixed by σ', σ''. Then $xc(x, y) \in C$ iff $xc_1(x, y) \in C'$ and $xc_2(x, y) \in C''$. Similarly $yc(x, y) \in C$ iff $yc_1(x, y) \in C'$ and $yc_2(x, y) \in C''$. The result follows. ■

Theorem 6.5.4. *Let $C = (1 + w)C' \oplus (1 - w)C''$ be a 2D skew-cyclic code over R, where C' and C'' are 2D skew-cyclic codes over $\mathbb{F}_q$. Let $A = \{f_1, f_2, \cdots, f_k\}$ be a generating set of C' and $B = \{h_1, h_2, \cdots, h_l\}$ be a generating set of C''. Then C is generated by $\{(1+w)f_1, (1+w)f_2, \cdots, (1+w)f_k, (1-w)h_1, (1-w)h_2, \cdots, (1-w)h_l\}$.*

Proof: Let $c(x, y) = (1 + w)c_1(x, y) + (1 - w)c_2(x, y) \in C$, where $c_1(x, y) = a_1f_1 + a_2f_2 + \cdots + a_kf_k \in C_1$ for some $a_i \in \mathbb{F}_q[x, y, \sigma', \sigma'']$ and $c_2(x, y) = b_1h_1 + b_2h_2 + \cdots + b_lh_l \in C_2$ for some $b_i \in \mathbb{F}_q[x, y, \sigma', \sigma'']$. Then obviously $c(x, y)$ is a linear combination of elements of the sets $(1 + w)A$ and $(1 - w)B$. On the other hand, let $v(x, y) = v_1(1+w)f_1 + v_2(1+w)f_2 + \cdots + v_k(1+w)f_k + w_1(1-w)h_1 + w_2(1-w)h_2 + \cdots + w_l(1 - w)h_l$, where $v_i, w_i \in R[x, y, \sigma', \sigma'']$, be an arbitrary linear combination of the elements of the sets A and B. Also v_i, w_i can be written as $v_i = v'_i + wv''_i$ and $w_i = w'_i + ww''_i$ for some $v'_i, v''_i, w'_i, w''_i \in \mathbb{F}_q[x, y, \sigma', \sigma'']$. Then $(1 + w)v_i = (1+w)(v'_i+wv''_i) = (1+w)(v'_i+v''_i) = (1+w)v'''_i$ and $(1-w)w_i = (1-w)(w'_1+ww''_i) = (1 - w)(w'_1 - w''_i) = (1 - w)w'''_i$, where $v'''_i = v'_i + v''_i, w'''_i = w'_1 - w''_i \in \mathbb{F}_q[x, y, \sigma', \sigma'']$. Therefore $v(x, y) = (1 + w)v'''_1 f_1 + (1 + w)v'''_2 f_2 + \cdots + (1 + w)v'''_k f_k + (1 - w)w'''_1 h_1 + (1-w)w'''_2 h_2 + \cdots + (1-w)w'''_l h_l = (1+w)(v'''_1 f_1 + v'''_2 f_2 + \cdots + v'''_k f_k) + (1-w)(w'''_1 h_1 + w'''_2 h_2 + \cdots + w'''_l h_l) = (1 + w)v'''(x, y) + (1 - w)w'''(x, y)$, where $v'''(x, y) \in C_1$ and $w'''(x, y) \in C_2$. Thus $v(x, y) \in C$. Hence the result. ■

Example 6.5.5. *Let $R = \mathbb{F}_9 + w\mathbb{F}_9$ and $\sigma' = \sigma'' = \sigma$, where σ is defined as $\sigma(a + wb) = a^3 + wb^3$ for all $a + wb \in R$. Let C', C'' be the 2D skew-cyclic codes of length 2×2 over $\mathbb{F}_9$ given by $C' = \langle x + y\rangle$ and $C'' = \langle 1 + x\rangle$ with the restricted automorphism σ on $\mathbb{F}_9$. Then the code $C = (1 + w)C' \oplus (1 - w)C''$ is a 2D skew-cyclic code of length 2×2 over R generated by $\langle(1 + w)(x + y), (1 - w)(1 + x)\rangle$. Moreover $|C'| = |C''| = 9^4$, and so $|C| = 9^8$. The parameters of C', C'' and $\xi(C)$ are $[4, 2, 2], [4, 2, 2]$ and $[8, 4, 2]$, respectively.*

6.6 Conclusion

A class of 2D skew-cyclic codes has been studied over $\mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$. We define a division algorithm on bivariate polynomial ring $R[x, y, \theta, \sigma]$, using which the structure of a 2D skew-cyclic code has been obtained. The relation of a 2D skew-cyclic code and a skew cyclic code is found under certain conditions. Duals of 2D skew-cyclic codes over R have been studied. A decomposition of these codes has been presented, and a generating set of a 2D skew-cyclic code over R is determined using generating sets of its components.

Chapter 7

Quantum Codes from Cyclic Codes over $\mathbb{F}_4 + u\mathbb{F}_4$

7.1 Introduction

The existence of quantum codes was shown by Shor [95]. However, the construction of quantum codes via classical linear codes was due to Calderbank et al. [31]. Since then many coding theorists have considered studying quantum codes over finite fields. Recently finite rings have also been used as alphabets to construct good quantum codes over them. Through the Gray map, good quantum codes have been obtained. In [84], Qian et al. have studied quantum codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$. In [59], Kai and Zhu have constructed quantum codes via cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$, $u^2 = 0$. In [59] and [84], cyclic codes of odd length n have been used to construct quantum codes through the factorization of $x^n - 1$. Some other finite rings have also been considered to obtain good quantum codes [35, 66].

In this chapter, we consider the ring $R = \mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$, for the construction of quantum codes through cyclic codes. We have considered cyclic codes of both odd length and even length over R, and through them we have obtained some optimal quantum codes over $\mathbb{F}_4$. To discuss more about the cyclic codes over R, we have used the structure given by Abualrub and Siap [3].

7.2 Quantum codes via cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$

Let $R = \mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$, and $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}, \omega^3 = 1, \omega^2 = 1+\omega$. Then R is a local ring with characteristic 2 and cardinality 16 having the unique maximal ideal $\langle u \rangle$.

Let C be an R-linear code and $C^\perp$ be the dual of C with respect to the usual inner product. Then C is called self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

We define a Gray map on R^n as $\Phi : R^n \to \mathbb{F}_4^{2n}$ such that

$$\Phi(x + uy) = (y,\ x + y),$$

where $x, y \in R^n$. Φ is an $\mathbb{F}_4$-module isomorphism. We define the Lee weight $w_L(a)$ of $a = x + uy \in R^n$ as $w_L(a) = w_H(\Phi(a)) = w_H(y,\ x + y)$, i.e., the Hamming weight of its Gray image. The Lee distance d_L of two vectors $x,\ y \in R^n$ is defined as the corresponding weight of $x - y$, i.e., $d_L(x, y) = w_L(x - y)$. It is easy to show that Φ is a linear isometry.

A quantum code over $\mathbb{F}_q$ whose length is n, dimension is k, and the minimum distance is d, is denoted by $[[n, k, d]]_q$.

The following result, known as the CSS construction, gives a crucial construction of quantum-error correcting codes over finite fields:

Theorem 7.2.1. *[31, 99] "Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be linear codes over $\mathbb{F}_q$ with $C_2^\perp \subseteq C_1$. Furthermore, let $d = min\{d_1, d_2\}$. Then there exists a quantum error-correcting code $C_Q = [[n, k_1 + k_2 - n, d]]_q$. In particular, if C is an $[n, k, d]_q$-linear code containing its dual, then there exists a quantum error-correcting code $C_Q = [[n, 2k - n, d]]_q$."*

We first prove the following result, which is important for further discussion in this section.

Theorem 7.2.2. *Let C be a linear code of length n over R.*

1. *If C is self-orthogonal, then so is $\Phi(C)$.*

2. *$\Phi(C^{\perp}) = \Phi(C)^{\perp}$, and hence if C is self-dual, then so is $\Phi(C)$.*

3. *If $C^{\perp} \subseteq C$, then $\Phi(C)^{\perp} \subseteq \Phi(C)$.*

Proof:

1. Let C be self-orthogonal. Let $c_1 = a_1 + ub_1$ and $c_2 = a_2 + ub_2$ be two codewords in C, where $a_1, b_1, a_2, b_2 \in \mathbb{F}_4^n$. Then

$$\begin{aligned} c_1 \cdot c_2 &= (a_1 + ub_1) \cdot (a_2 + ub_2) \\ &= a_1 \cdot a_2 + u(a_1 \cdot b_2 + a_2 \cdot b_1). \end{aligned}$$

   Since C is self-orthogonal, $c_1 \cdot c_2 = 0$. So we have $a_1 \cdot a_2 = a_1 \cdot b_2 + a_2 \cdot b_1 = 0$. Then $\Phi(c_1) \cdot \Phi(c_2) = (b_1, a_1 + b_1) \cdot (b_2, a_2 + b_2) = b_1 \cdot b_2 + a_1 \cdot a_2 + a_1 \cdot b_2 + a_2 \cdot b_1 + b_1 \cdot b_2 = 0$. Hence $\Phi(C) \subseteq \Phi(C)^{\perp}$, and thus $\Phi(C)$ is self-orthogonal.

2. Let $\Phi(y) \in \Phi(C^{\perp})$, $y = c + ud \in C^{\perp}$. Then $x \cdot y = 0$ for all $x = a + ub \in C$. This implies that $a \cdot c = 0$ and $b \cdot c + a \cdot d = 0$. This further implies that $\Phi(y) \cdot \Phi(x) = 0$ for all $\Phi(x) \in \Phi(C)$. Therefore $\Phi(C^{\perp}) \subseteq \Phi(C)^{\perp}$.

   Since R is a Frobenius ring, $|C||C^{\perp}| = |R|^n = 16^n$. Then $|\Phi(C^{\perp})| = |C^{\perp}| = \frac{16^n}{|C|} = \frac{4^{2n}}{|\Phi(C)|} = |\Phi(C)^{\perp}|$. Hence $\Phi(C^{\perp}) = \Phi(C)^{\perp}$.

3. Follows from (1) and (2).

■

7.2.1 When n is odd

Now we present some existing results on cyclic codes over R [3]. By using the same, we determine some more results on cyclic codes over R and then obtain the parameters of the corresponding quantum codes.

Theorem 7.2.3. *[3, Theorem 1] "Let C be a cyclic code of length n over R, where n is odd. Then $C = \langle f(x),\ ua(x) \rangle = \langle f(x) + ua(x) \rangle$ for some $f(x), a(x) \in \mathbb{F}_4[x]$, such that $a(x) \mid f(x) \mid x^n - 1$. Moreover $|C| = 16^{n-deg\ f(x)} 4^{deg\ f(x)\text{-}deg\ a(x)}$."*

Lemma 7.2.4. *Let $a(x) \mid f(x) \mid x^n - 1$. Then $\widehat{f}(x) \mid \widehat{a}(x)$.*

Proof: Since $a(x) \mid f(x)$, $f(x) = a(x)b(x)$. We have $x^n - 1 = f(x)\widehat{f}(x) = a(x)b(x)\widehat{f}(x)$. This implies that $\widehat{a}(x) = b(x)\widehat{f}(x)$. Therefore $\widehat{f}(x) \mid \widehat{a}(x)$. ■

Theorem 7.2.5. *Let $C = \langle f(x),\ ua(x)\rangle : a(x) \mid f(x) \mid (x^n - 1)$ be a non-zero cyclic code of odd length n over R. Then the annihilator of C is $A(C) = \langle \widehat{a}(x), u\widehat{f}(x)\rangle$.*

Proof: Since $A(C)$ itself is a cyclic code of length n over R, it can be expressed as $A(C) = \langle f_1(x), ua_1(x)\rangle$, where $a_1(x) \mid f_1(x) \mid (x^n - 1)$. We have $ua_1(x)f(x) = 0 \pmod{x^n - 1}$, as $ua_1(x) \in A(C)$ and $f(x) \in C$. This implies that $ua_1(x)f(x) = (x^n - 1)j(x)$ for some $j(x) \in R[x]$. This gives $\widehat{f}(x) \mid a_1(x)$. Also, $(u\widehat{f}(x))f(x) = 0$ and $(u\widehat{f}(x))(ua(x)) = 0$, which implies that $u\widehat{f}(x) \in A(C)$, this further implies that $a_1(x) \mid \widehat{f}(x)$. Therefore $a_1(x) = \widehat{f}(x)$.

Now $ua(x)f_1(x) = 0$ implies that $\widehat{a}(x) \mid f_1(x)$. Since $a(x) \mid f(x)$, so $\widehat{a}(x)f(x) = 0$. This implies that $\widehat{a}(x) \in A(C)$. Thus $f_1(x) \mid \widehat{a}(x)$. Therefore $f_1(x) = \widehat{a}(x)$. Hence $A(C) = \langle \widehat{a}(x), u\widehat{f}(x)\rangle$. ■

Corollary 7.2.5.1. *Let $C = \langle f(x),\ ua(x)\rangle : a(x) \mid f(x) \mid (x^n - 1)$ be a cyclic code of odd length n over R. Then the dual of C is $C^\perp = \langle \widehat{a}(x)^*, u\widehat{f}(x)^*\rangle$.*

Corollary 7.2.5.2. *Let $C = \langle f(x)\rangle$, i.e., $a(x) = 0$ with $f(x) \mid (x^n - 1)$ be a cyclic code of odd length n over R. Then the dual of C is $C^\perp = \langle \widehat{f}(x)^*\rangle$.*

Lemma 7.2.6. *Let $a(x), b(x) \in R[x]$ be such that $x^n - 1 = a(x)b(x)$ for $b(x) \in R[x]$. Then we have*

1. $(a(x)b(x))^* = a^*(x)b^*(x)$
2. $\widehat{a}^*(x) = \widehat{a^*}(x)$

Proof:

1. $(a(x)b(x))^* = x^n a(\frac{1}{x})b(\frac{1}{x}) = x^{\deg(a(x))}a(\frac{1}{x})x^{\deg(b(x))}b(\frac{1}{x}) = a^*(x)b^*(x)$.
2. Since $x^n - 1 = \widehat{a}(x)a(x)$, $(x^n - 1)^* = \widehat{a}^*(x)a^*(x)$. This implies that $\widehat{a}^*(x) = \frac{x^n - 1}{a^*(x)} = \widehat{a^*}(x)$.

■

Now we give a necessary and sufficient condition for a cyclic code of odd length over R to contain its dual and vice versa.

Theorem 7.2.7. *Let $C = \langle f(x),\ ua(x)\rangle$: $a(x) \mid f(x) \mid (x^n - 1)$ be a cyclic code of odd length n over R. Then*

1. *$C^\perp \subseteq C$ if and only if $f(x) \mid \widehat{a}^*(x)$.*
2. *$C \subseteq C^\perp$ if and only if $\widehat{a}^*(x) \mid f(x)$.*

Proof:

1. Suppose that $C^\perp \subseteq C$. Then $\widehat{a}^*(x) \in C$. Therefore $\widehat{a}^*(x)$ is a linear combination of $f(x)$ and $ua(x)$. Since $\widehat{a}^*(x) \in \mathbb{F}_4[x]$, we get $f(x) \mid \widehat{a}^*(x)$. Conversely, assume that $f(x) \mid \widehat{a}^*(x)$. Then $\widehat{a}^*(x) \in C$. Also we have $a(x) \mid \widehat{f}^*(x)$ (by Lemma 7.2.4). Therefore $C^\perp = \langle \widehat{a}^*(x),\ u\widehat{f}^*(x)\rangle \subseteq \langle f(x),\ ua(x)\rangle = C$.
2. This can be obtained by applying (1) on $C^\perp$ and noting that $(C^\perp)^\perp = C$.

■

Theorem 7.2.8. *A cyclic code C of odd length n over R of the form $C = \langle f(x), ua(x)\rangle = \langle f(x) + ua(x)\rangle$ with $a(x) \mid f(x) \mid x^n - 1$ is a free code if and only if $C = \langle f(x)\rangle$.*

Proof: Since $a(x) \mid f(x)$, deg $a(x) \leq$ deg $f(x)$. If deg $a(x) =$ deg $f(x)$, then $a(x) = \alpha f(x)$ for some non-zero element $\alpha \in \mathbb{F}_4$, and hence $C = \langle f(x)\rangle$. Now let deg $a(x) <$ deg $f(x)$. Suppose C is a free cyclic code over R. Then there exists a minimal degree polynomial $g(x) \in C$ such that $C = \langle g(x)\rangle$ and $g(x)|x^n - 1$. Since $x^n - 1 \in \mathbb{F}_4[x]$, $g(x)$ can be chosen in such a way that it is a polynomial over $\mathbb{F}_4[x]$. Therefore $g(x)$ must be an associate of $f(x) + ua(x)$. Let $g(x) = (c + ud)(f(x) + ua(x))$ for some unit $c + ud \in R$. If $d = 0$, then clearly $a(x) = 0$. If $d \neq 0$, then $df(x) + ca(x) = 0$, and so $f(x) = cd^{-1}a(x)$, which is a contradiction as deg $a(x) <$ deg $f(x)$. Hence $C = \langle f(x)\rangle$. Conversely, since $f(x) \mid x^n - 1$, so $C = \langle f(x)\rangle$ is a free code. ■

Corollary 7.2.8.1. *A free code $C = \langle f(x) \rangle$ such that $f(x)g(x) = x^n - 1$ satisfies $C^\perp \subseteq C$ if and only if $g(x)g(x)^* = 0$ (mod $x^n - 1$).*

Proof: Suppose $C^\perp \subseteq C$. Then $f(x) \mid g(x)^*$, i.e., $g(x)^* = f(x)p(x)$ for some $p(x) \in R[x]$. Therefore $g(x)g(x)^* = (x^n - 1)p(x)$ and hence $g(x)g(x)^* = 0 \pmod{x^n - 1}$. The converse can be proved similarly. ■

The following theorem presents the construction of quantum codes via cyclic codes of odd lengths over R, using the CSS construction.

Theorem 7.2.9. *Let $C = \langle f(x),\ ua(x) \rangle$ be cyclic code of odd length n over R such that $f(x) \mid \widehat{a}^*(x)$.Then $C^\perp \subseteq C$, and there exists a quantum code C_Q with the parameters $[[2n, 2(n - k_1 - k_2), d_L]]_4$, where $k_1 = deg\ f(x)$, and $k_2 = deg\ a(x)$, and d_L is the minimum Lee distance of C.*

Proof: We have $C = \langle f(x),\ ua(x) \rangle = \langle f(x) + ua(x) \rangle$ and $f(x) \mid \widehat{a}^*(x)$. This implies from Theorem 7.2.7 that $C^\perp \subseteq C$. This further implies from Theorem 7.2.2 that $\Phi(C)^\perp \subseteq \Phi(C)$. Now from Theorem 7.2.3, $|C| = 16^{n-k_1}4^{k_1-k_2}$. Therefore $|\Phi(C)| = 4^{2n-k_1-k_2}$, and so the parameters of $\Phi(C)$ are $[2n, 2n - k_1 - k_2, d_L]_4$. By CSS construction, the quantum code corresponding to $\Phi(C)$ has the parameters $[[2n, 2(2n - k_1 - k_2) - 2n, d_L]]_4$, i.e., $[[2n, 2(n - k_1 - k_2), d_L]]_4$. ■

Corollary 7.2.9.1. *Let C be a free cyclic code of odd length n over R generated by $f(x)$. Then there exists a quantum code C_Q with the parameters $[[2n, 2n - 4k, d_L]]_4$, where $k = deg\ f(x)$ and d_L is the minimum Lee distance of C.*

The following construction helps us to find some optimal quantum codes over $\mathbb{F}_4$. In this construction, we find a new code which contains it dual by augmentation of a code of smaller size and same length that contains its dual. This goes as follows.

Let C_1 be an R-linear code such that C_1 contains its dual, i.e., ${C_1}^\perp \subseteq C_1$. Construct a new code C_2 such that $C_1 \subset C_2$ by adding some rows to the generator matrix of C_1. Since $C_1 \subseteq C_2$, we have ${C_2}^\perp \subseteq {C_1}^\perp$. Then clearly

$${C_2}^\perp \subseteq {C_1}^\perp \subseteq C_1 \subseteq C_2.$$

Thus C_2 is a dual containing code. We can then use the CSS construction to get the quantum code over $\mathbb{F}_4$ corresponding to C_2. Also the quantum code obtained from C_2 has larger size than the quantum code obtained from C_1. This is illustrated by the following example.

Example 7.2.10. *Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Let C_1 be a cyclic code of length 3 over R such that $C_1 = \langle (x+1)(x+\omega), u(x+\omega)\rangle$. Let $f(x) = (x+1)(x+\omega)$ and $a(x) = (x+\omega)$. Then $\widehat{a}^*(x) = (x+1)\omega^2(x+\omega)$ and the dual of C_1 is $C_1^\perp = \langle (x+1)(\omega^2 x+1), u(\omega^2 x+1)\rangle$. C_1 is a self-dual cyclic code over R with the parameters $(3, 16^1 4^1, 3)$. Therefore the parameters of $\Phi(C_1)$ are $[6, 3, 3]$, and the corresponding quantum code has parameters $[[6, 0, 3]]_4$.*

Now we implement the above construction to find new quantum code from C_1. The generator matrix for C_1 is:

$$\begin{bmatrix} \omega + u\omega & 1+\omega+u & 1 \\ 1 & \omega+u\omega & 1+\omega+u \\ 1+\omega+u & 1 & \omega+u\omega \end{bmatrix}.$$

We construct a new code C_2 with generator matrix:

$$\begin{bmatrix} \omega + u\omega & 1+\omega+u & 1 \\ 1 & \omega+u\omega & 1+\omega+u \\ 1+\omega+u & 1 & \omega+u\omega \\ 1+u & 1+u & u \end{bmatrix}.$$

Now as explained above, ${C_2}^\perp \subseteq C_2$, and so $\Phi(C_2)^\perp \subseteq \Phi(C_2)$. The parameters of $\Phi(C_2)$ are $[6, 5, 2]$. Therefore by CSS construction, we get a quantum code with parameters $[[6, 4, 2]]_4$, which is an optimal quantum code [45].

Example 7.2.11. *Let C be a cyclic code of length 3 over R having its generator matrix as*

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

Then C can be written as $C = \langle f(x)\rangle$ where $f(x) = x + \omega$. Since $x^3 + 1 = (x + \omega)(x+1)(x+\omega^2)$, $C^\perp = \langle (x+1)(\omega^2 x + 1)\rangle$. Let $g(x) = (x+1)(x+\omega^2)$. Then

$g^*(x) = (x+1)(x\omega^2+1)$. *Now* $gg^* = (x+1)^2(x+\omega^2)(x\omega^2+1) = (x+1)(x+1)(x+\omega^2)\omega(x+\omega) = (x^3+1)(\omega x+\omega) = 0 \ (mod\, x^3+1)$. *From Corollary 7.2.8.1,* $C^\perp \subseteq C$. *The parameters for* $\Phi(C)$ *are* $[6,4,2]$. *Therefore there exists a CSS-quantum code with parameters* $[[6,2,2]]_4$.

Again let C_2 *be a linear code of length* 3 *over* R *having generator matrix:*

$$\begin{bmatrix} \omega & 1 & 0 \\ 0 & \omega & 1 \\ 0 & u & 0 \end{bmatrix}.$$

Then ${C_2}^\perp \subseteq C_2$ *and from the parameters of* $\Phi(C_2)$, *i.e.,* $[6,5,2]_4$, *the parameters of corresponding* CSS*-quantum codes are* $[[6,4,2]]_4$, *which is an optimal quantum code [45].*

Remark 7.2.11.1. *The weight enumerator of* C_1 *(in Example 7.2.11) is given by*

$$w_C(x,y) = x^6 + 18x^4y^2 + 12x^3y^3 + 81x^2y^4 + 108xy^5 + 36y^6.$$

By MacWilliams identity, i.e.,

$$w_{C^\perp}(x,y) = \frac{1}{|C|}w_C(x+3y, x-y),$$

we have $w_{C_1}(x,y) = x^6 + 6x^3y^3 + 9y^6$. *Therefore the parameters of* $C_1^\perp$ *over* F_4 *are* $[3,1,3]$. *Similarly the weight enumerator for* C_2 *is* $w_{C_2}(x,y) = x^6 + 45x^4y^2 + 120x^3y^3 + 315x^2y^4 + 360xy^5 + 183y^6$, *and so* $w_{C_2^\perp}(x,y) = x^6 + 3y^6$. *Therefore the parameters of* $C_2^\perp$ *are* $[6,1,6]$ *over* $\mathbb{F}_4$.

7.2.2 When n is even

In this part of the section, we present a necessary and sufficient condition for a cyclic code C of even length n over R to contain its dual. This helps us to find quantum codes via these codes, and makes searching of quantum codes over F_4 easy.

Theorem 7.2.12. *[3, Theorem 1,3,4] "Let* C *be a cyclic code of even length* n *over* R.

1. *$C = \langle f(x) + up(x)\rangle$ and $f(x) + up(x) \mid x^n - 1$. Moreover $|C| = 16^{n-r}$ and $C^\perp = \langle (g(x) + uq(x))^*\rangle$, where $x^n - 1 = (f(x) + up(x))(g(x) + uq(x))$. In this case, C is a free cyclic code.*

2. *$C = \langle f(x) + up(x),\ ua(x)\rangle$ and $a(x) \mid f(x) \mid x^n - 1$, $a(x) \mid \widehat{f}(x)p(x)$. Moreover $|C| = 4^{2n-r-t}$, where deg $f(x) = r$, deg $a(x) = t$ and $C^\perp = \langle \widehat{a}^*(x) + ux^l m^*(x), u\widehat{f}^*(x)\rangle$, where $\widehat{f}(x)p(x) = a(x)m(x)$ and $l =$ deg $\widehat{a}(x)-$ deg $m(x)$."*

Theorem 7.2.13 and Theorem 7.2.14 below respectively present a necessary and sufficient condition for a principally generated cyclic code of even length and a non-principally generated cyclic code of even length over R to contain its dual.

Theorem 7.2.13. *Let $C = \langle f(x) + up(x)\rangle$ be a free cyclic code of even length n over R such that $x^n - 1 = (f(x) + up(x))(g(x) + uq(x))$. Then $C^\perp \subseteq C$ if and only if $(g(x) + q(x))(g(x) + q(x))^* = 0$ (mod $x^n - 1$).*

Proof: The proof is straightforward and similar to the odd length case. ■

Theorem 7.2.14. *Let $C = \langle f(x) + up(x), ua(x)\rangle$, where $a(x) \mid f(x) \mid x^n - 1$, $a(x) \mid \widehat{f}(x)p(x)$ be a cyclic code of even length n over R. Then $C^\perp \subseteq C$ if and only if $f(x) \mid \widehat{a}^*(x)$ and $a(x) \mid (x^l m^*(x) - p(x)\frac{\widehat{a}^*(x)}{f(x)})$, where $C^\perp = \langle \widehat{a}^*(x) + ux^l m^*(x), u\widehat{f}^*(x)\rangle$, with $\widehat{f}(x)p(x) = a(x)m(x)$ and $l =$ deg $\widehat{a}(x)-$ deg $m(x)$.*

Proof: First suppose that $C^\perp \subseteq C$. Then $\widehat{a}^*(x) + ux^l m^*(x) = (f(x) + up(x))(\lambda_1(x) + u\lambda_2(x)) + ua(x)\lambda_3(x)$, where $\lambda_i(x) \in \mathbb{F}_4[x]$. By comparing terms on either side, we get

$$\widehat{a}^*(x) = f(x)\lambda_1(x) \tag{7.1}$$

and

$$x^l m^*(x) = p(x)\lambda_1(x) + f(x)\lambda_2(x) + a(x)\lambda_3(x). \tag{7.2}$$

From (7.1), we get $f(x) \mid \widehat{a}^*(x)$, and from (7.2) we get

$$\begin{aligned} \widehat{a}(x)x^l m^*(x) &= \widehat{a}(x)p(x)\lambda_1(x) \text{ mod } (x^n - 1) \\ &= \widehat{a}(x)p(x)\frac{\widehat{a}^*(x)}{f(x)} \text{ mod } (x^n - 1). \end{aligned}$$

This implies that $x^n - 1 \mid \widehat{a}(x)(x^l m^*(x) - p(x)\frac{\widehat{a^*(x)}}{f(x)})$. This in turn implies that $a(x) \mid (x^l m^*(x) - p(x)\frac{\widehat{a^*(x)}}{f(x)})$, as $a(x) \mid x^n - 1$.

Conversely, assume that $f(x) \mid \widehat{a}^*(x)$ and $a(x) \mid (x^l m^*(x) - p(x)\frac{\widehat{a^*(x)}}{f(x)})$. This implies that $\widehat{a}^*(x) = f(x)f'(x)$, and $a(x) \mid (x^l m^*(x) - p(x)\frac{\widehat{a^*(x)}}{f(x)} + f(x)f''(x))$ for some $f'(x), f''(x) \in \mathbb{F}_4[x]$ as $a(x) \mid f(x)$. This further implies that $x^l m^*(x) - p(x)f'(x) + f(x)f''(x) = a(x)a'(x)$ for some $a'(x) \in \mathbb{F}_4[x]$. Thus

$$x^l m^*(x) = p(x)f'(x) + f(x)f''(x) + a(x)a'(x) \tag{7.3}$$

Now,

$$\begin{aligned}
\widehat{a}^*(x) + ux^l m^*(x) &= f(x)f'(x) + u(p(x)f'(x) + f(x)f''(x) + a(x)a'(x)) \\
&= f'(x)(f(x) + up(x)) + uf(x)f''(x) + ua(x)a'(x) \\
&= f'(x)(f(x) + up(x)) + u(f(x) + up(x))f''(x) + ua(x)a'(x) \\
&= (f(x) + up(x))(f'(x) + uf''(x)) + ua(x)a'(x).
\end{aligned}$$

This implies that $\widehat{a}^*(x) + ux^l m^*(x) \in \langle f(x) + up(x),\ ua(x)\rangle = C$. Since $f(x) \mid \widehat{a}^*(x)$, $a(x) \mid \widehat{f}^*(x)$ (from Lemma 7.2.4), and so $u\widehat{f}^*(x) \in C$. Hence $C^\perp = \langle \widehat{a}^*(x) + ux^l m^*(x),\ u\widehat{f}^*(x)\rangle \subseteq C$. ■

Theorem 7.2.15. *1. Let $C = \langle f(x) + up(x)\rangle$, with deg $(f(x) + up(x)) = r$ and $f(x) + up(x) \mid x^n - 1$, be a cyclic code of length n over R such that $C^\perp \subseteq C$. Then there exists a quantum code with the parameters $[[2n, 2n-4r, d_L]]_4$, where d_L is the minimum Lee distance of C.*

2. Let $C = \langle f(x) + up(x),\ ua(x)\rangle$ with deg $(f(x)) = r$, deg $(a(x)) = t$ and $a(x) \mid f(x) \mid x^n - 1$, be a cyclic code of length n over R such that $C^\perp \subseteq C$. Then there exists a quantum code with the parameters $[[2n, 2n - 2r - 2t, d_L]]_4$, where d_L is the minimum Lee distance of C.

Proof: The proofs of both the statements directly follow from the Gray image of C and Theorem 7.2.1. ■

Example 7.2.16. *Let C be a cyclic code of even length 6 over R such that $C = \langle (x+1)^2(x+\omega)(x+\omega^2)+u, u(x+\omega)\rangle$. Then $f(x) = (x+1)^2(x+\omega)(x+\omega^2), p(x) = 1$ and $a(x) = x+\omega$. Since $x^6+1 = (x^3+1)^2 = (x+1)^2(x+\omega)^2(x+\omega^2)^2$ over $\mathbb{F}_4+u\mathbb{F}_4$. This implies that $\widehat{a}(x) = (x+1)^2(x+\omega)(x+\omega^2)^2$, $m(x) = p(x)\frac{\widehat{f(x)}}{a(x)} = (x+\omega^2)$, $l =$ deg $(\widehat{a}(x))-$deg $(m(x)) = 4$ and $\widehat{f}(x) = (x+\omega)(x+\omega^2)$. So*

$$\begin{aligned}
\widehat{a}^*(x) &= (x+1)^2(1+\omega x)(1+\omega^2 x)^2 \\
&= \omega^2(x+1)^2(x+\omega^2)(x+\omega)^2 \\
&= (\omega^2(x+\omega))(x+1)^2(x+\omega^2)(x+\omega) \\
&= (\omega^2(x+\omega))f(x),
\end{aligned}$$

which implies that $f(x) \mid \widehat{a}^*(x)$. Also,

$$\begin{aligned}
x^l m^*(x) - p(x)\frac{\widehat{a}^*(x)}{f(x)} &= x^4(1+x\omega^2) - (x+\omega)\omega^2 \\
&= x^4\omega^2(x+\omega) - \omega^2(x+\omega) \\
&= (x+\omega)\omega^2(x^4-1) \\
&= a(x)\omega^2(x^4-1).
\end{aligned}$$

It follows that $a(x) \mid x^l m^*(x) - p(x)\frac{\widehat{a}^*(x)}{f(x)}$. Therefore from Theorem 7.2.14, $C^\perp \subseteq C$, where $C^\perp = \langle ((x+1)^2(x+\omega^2)(x+\omega)^2 + ux^3(x+\omega), u(x+\omega)(x+\omega^2)\rangle$. Now C has the parameters $(6, 16^2 4^3, 4)$. Therefore the corresponding quantum code has the parameters $[[12, 2, 4]]_4$. Add the vector $(1,\ 1,\ 1,\ 1,\ 1,\ 1)$ to the rows of the generator matrix of C. The parameters of the new code, over R, are $(6, 4^8, 3)$, and so there is a CSS-quantum code C_Q with parameters $[[12, 4, 3]]_4$.

Example 7.2.17. *Let C_1 be a cyclic code of length 4 generated by the matrix:*

$$\begin{bmatrix} 1 & u+1 & 0 & 0 \\ 0 & 1 & u+1 & 0 \\ 0 & 0 & 1 & u+1 \end{bmatrix}.$$

Then, in polynomial form, C_1 can be written as $C = \langle (u+1)x+1\rangle$. Since $x^4-1 = ((u+1)x^3 + x^2 + (u+1)x + 1)((u+1)x+1)$, C_1 is a free cyclic code over R of *free rank* 3 *and parameters* $(4, 4^6, 2)$. $C^\perp = \langle ((u+1)x^3 + x^2 + (u+1)x + 1)^* \rangle = \langle x^3 + (u+1)x^2 + x + u + 1 \rangle$. *Also,* ${C_1}^\perp \subseteq C_1$, *as* $(u+1)x+1 \mid x^3+(u+1)x^2+x+u+1$. *From Theorem 7.2.14, there exists a* $[[8, 4, 2]]_4$ *CSS-quantum code. Now construct a new code* C_2 *by augmentation of* C_1 *such that the generator matrix of* C_2 *is*

$$\begin{bmatrix} 1 & u+1 & 0 & 0 \\ 0 & 1 & u+1 & 0 \\ 0 & 0 & 1 & u+1 \\ \omega^2 & \omega^2 & \omega^2 & u+\omega^2 \end{bmatrix}.$$

Then, as explained in Section 3, $C_2^\perp \subseteq C_2$. *The parameters of* $\Phi(C_2)$ *are* $[8, 7, 2]$. *Therefore there is a CSS-quantum code with parameters* $[[8, 6, 2]]_4$, *which is an optimal quantum code over* $\mathbb{F}_4$ *[45].*

Example 7.2.18. *Let* $C = \langle 1 + x, u \rangle$ *be a cyclic code of length* 4 *over* R. *Then clearly* $C^\perp = \langle u(1+x)^3 \rangle$. *In this case,* $f(x) = 1 + x$ *and* $a(x) = 1$. *Moreover* $f(x) | \widehat{a}(x)^*$, *therefore* $C^\perp \subseteq C$. C *is a* $(4, 4^7, 2)$ *code over* R. *Therefore* C *is an* $[[8, 6, 2]]_4$ *CSS-quantum code, which is an optimal quantum code [45].*

We present another necessary and sufficient condition for a cyclic code of even length n over R to contain its dual.

Theorem 7.2.19. *Let* $C = \langle f(x) + up(x), ua(x) \rangle$ *be a cyclic code of even length* n *over* R. *Then* $C^\perp \subseteq C$ *if and only if* $f(x) \mid a^*(x)$ *and* $\widehat{a}(x)x^l m^*(x) + m(x)\widehat{a}^*(x) = 0$, *where* $C^\perp = \langle \widehat{a}^*(x) + ux^l m^*(x), u\widehat{f}^*(x) \rangle$, *with* $\widehat{f}(x)p(x) = a(x)m(x)$ *and* $l =$ *deg* $\widehat{a}(x) -$ *deg* $m(x)$.

Proof: First suppose that $C^\perp \subseteq C$. Then $\widehat{a}^*(x) + ux^l m^*(x) = (f(x) + up(x))(\lambda_1(x) + u\lambda_2(x)) + ua(x)\lambda_3(x)$, where $\lambda_i(x) \in \mathbb{F}_4[x]$. By comparing the terms on either side, we get

$$\widehat{a}^*(x) = f(x)\lambda_1(x) \tag{7.4}$$

and

$$x^l m^*(x) = p(x)\lambda_1(x) + f(x)\lambda_2(x) + a(x)\lambda_3(x). \tag{7.5}$$

Now we have $(f(x)+up(x))(\widehat{a}(x)+um(x)) = 0$, as $\widehat{a}(x)+um(x)) = 0 \in C^{\perp}$. This implies that

$$\widehat{a}(x)p(x) + m(x)f(x) = 0. \tag{7.6}$$

Then we get

$$\begin{aligned} \widehat{a}(x)x^l m^*(x) &= \widehat{a}(x)p(x)\lambda_1(x) \text{ (from (7.5))} \\ &= -m(x)f(x)\lambda_1(x) \text{ (from (7.6))} \\ &= -m(x)\widehat{a}^*(x) \text{ (from (7.4))}. \end{aligned}$$

Conversely, assume that $f(x) \mid \widehat{a}^*(x)$ and $\widehat{a}x^l m^*(x) + m(x)\widehat{a}^*(x) = 0$. This implies that $\widehat{a}^*(x) = f(x)\beta_1(x)$ for some $\beta_1(x) \in \mathbb{F}_4[x]$, and $\widehat{a}x^l m^*(x) = m(x)\widehat{a}^*(x)$. This in turn implies that

$$\begin{aligned} \widehat{a}(x)x^l m^*(x) &= m(x)f(x)\beta_1(x) \\ &= \widehat{a}(x)p(x)\beta_1(x) \text{ (from (7.6))} \\ &= \widehat{a}(x)(p(x)\beta_1(x) + f(x)\beta_2(x)) \text{ for some } \ \beta_2(x) \in \mathbb{F}_4[x]. \end{aligned}$$

Thus $\widehat{a}(x)(x^l m^*(x) - p(x)\beta_1(x) - f(x)\beta_2(x)) = 0$. It follows that $a(x) \mid (x^l m^*(x) - p(x)\beta_1(x) - f(x)\beta_2(x))$, which implies that $x^l m^*(x) - p(x)\beta_1(x) - f(x)\beta_2(x) = a(x)\beta_3(x)$ for some $\beta_3(x) \in \mathbb{F}_4[x]$. Therefore $x^l m^*(x) = p(x)\beta_1(x) + f(x)\beta_2(x) + a(x)\beta_3(x)$.

Now,

$$\begin{aligned} \widehat{a}^*(x) + ux^l m^*(x) &= f(x)\beta_1(x) + up(x)\beta_1(x) + uf(x)\beta_2(x) + ua(x)\beta_3(x) \\ &= \beta_1(x)(f(x)+up(x)) + uf(x)\beta_2(x) + ua(x)\beta_3(x)(x) \\ &= \beta_1(x)(f(x)+up(x)) + u(f(x)+up(x))\beta_2(x) + ua(x)\beta_3(x)(x) \\ &= (f(x)+up(x))(\beta_1(x)+u\beta_2(x)) + ua(x)\beta_3(x). \end{aligned}$$

This implies that $\widehat{a}^*(x) + ux^l m^*(x) \in \langle f(x)+up(x),\ ua(x)\rangle = C$. Since $f(x) \mid \widehat{a}^*(x)$, $a(x) \mid \widehat{f}^*(x)$ (from Lemma 7.2.4). So $u\widehat{f}^*(x) \in C$. Hence $C^{\perp} = \langle \widehat{a}^*(x) + ux^l m^*(x),\ u\widehat{f}^*(x)\rangle \subseteq C$. ■

The following table shows the codes we obtained in examples of this chapter.

Table 7.1: Quantum codes over $\mathbb{F}_4$

Generators	CSS-Quantum code $[[n, k, d_L]]_4$
$\{f_1(x), xf_1(x), x^2f_1(x)\}$	$[[6, 0, 3]]_4$
$\{f_1(x), xf_1(x), x^2f_1(x)\} \cup \{ux^2 + (1 + u)x + 1 + u\}$	$[[6, 4, 2]]_4^*$
$\{f_2(x), xf_2(x)\}$	$[[6, 2, 2]]_4$
$\{f_2(x), xf_2(x)\} \cup \{ux\}$	$[[6, 4, 2]]_4^*$
$\langle x^2 + wx + 1, u\rangle$	$[[10, 6, 2]]_4$
$\{f_3(x), xf_3(x), x^2f_3(x)\}$	$[[8, 4, 2]]_4$
$\{f_3(x), xf_3(x), x^2f_3(x)\} \cup \{1 + (1 + u)x + ux^2 + x^3\}$	$[[8, 6, 2]]_4^*$
$\{f_4(x), xf_4(x), f_5(x), xf_5(x), x^2f_5(x)\}$	$[[12, 2, 4]]_4$
$\{f_4(x), xf_4(x), f_5(x), xf_5(x), x^2f_5(x)\} \cup \{1+x+x^2+x^3+x^4+x^5\}$	$[[12, 4, 3]]_4$

In the table 7.1, we have

$$f_1(x) = (w + uw) + (1 + w + u)x + x^2,$$

$$f_2(x) = x + w,$$

$$f_3(x) = (u + 1)x + 1,$$

$$f_4(x) = (x + 1)^2(x + w)(x + w^2) + u,$$

$$f_5(x) = u(x + w).$$

7.3 Conclusion

We have studied cyclic codes of both even length and odd length over $\mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$. In each case, a necessary and sufficient condition for a cyclic code to contain its dual has been obtained. Using this, we have calculated the parameters of corresponding quantum codes. Some optimal quantum codes have been obtained by augmentation. We have given some examples for illustration.

Chapter 8

Conclusions and Future Scope

The main purpose of this thesis is a systematic study of classes of linear codes (cyclic, constacyclic, 2D-cyclic codes etc.) using non-commutative skew polynomial rings and for searching of good codes over them. We conclude our thesis with the following points:

- We have defined a new class of skew-cyclic codes over mixed alphabet $\mathbb{F}_3 R$, which we termed as F_3R-skew cyclic codes, where $R = \mathbb{F}_3 + v\mathbb{F}_3, v^2 = v$. We start by obtaining the generating sets of skew-cyclic codes over R using division algorithm on $R[x, \theta]$, where θ is an automorphism of R, and then obtained the structure of $\mathbb{F}_3 R$-skew cyclic codes and their generating sets. Further, we have studied skew-cyclic codes and additive skew-cyclic codes over $\mathbb{F}_p + w\mathbb{F}_p, w^2 = 1$.

- We have extended the study of codes over $\mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = 0$ to skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. Further, these codes are generalized to double skew-constacyclic codes. Using a Gray map, some new good linear codes over $\mathbb{Z}_4$ have been obtained. The parameters of these codes are $(6, 4^4 2^2, 2_L)$, $(18, 4^4 2^1, 10_L), (18, 4^4 2^2, 7_L)$ and $(18, 4^4 2^4, 7_L)$. These new codes have been updated to the database of $\mathbb{Z}_4$-codes.

- We have generalized the study of skew codes over rings to codes over more general skew polynomial rings and studied a class of skew-cyclic codes over

$\mathbb{Z}_4 + w\mathbb{Z}_4, w^2 = 1$, with derivation. The Gray images of the residue codes of these codes have given us some good linear codes which are given in Table 5.1.

- We have studied a generalization of skew-cyclic codes over $R = \mathbb{F}_q + w\mathbb{F}_q, w^2 = 1$ using skew polynomial rings with two variables. These codes are known 2D skew-cyclic codes. These codes have been studied as left $R[x, y, \theta_1, \theta_2]$-submodules of $\frac{R[x,y,\theta_1,\theta_2]}{\langle x^l-1,\ y^m-1\rangle}$, where θ_1, θ_2 are two commuting automorphisms of R. A decomposition of these codes has been presented, and a generating set of a 2D-skew cyclic code over R is obtained using generating sets of its components.

- We have studied quantum codes over $\mathbb{F}_4 + u\mathbb{F}_4, u^2 = 0$. For this, we have used the structure of cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$ having arbitrary length, to find out the conditions for these codes to contain their duals. Then the parameters of corresponding quantum codes over $\mathbb{F}_4$ via CSS construction have been obtained. Further, by augmentation, a code with larger size with dual containing property is obtained from the original code which itself has the dual containing property. We have given a table having some good quantum codes over $\mathbb{F}_4$.

8.1 Directions for future work

We give some possible research directions for the future work that are on the basis of the results obtained in this thesis.

1. The study of skew-codes over non-chain extensions of $\mathbb{Z}_4$, given in Chapter 4 and Chapter 5, can be generalized to non-chain extensions of $\mathbb{Z}_q$, q a prime power. The study over general ring $\mathbb{Z}_q + u\mathbb{Z}_q$ will be an interesting problem in this direction and the resulting structure may lead one to get some new codes with better parameters.

2. The study of quantum error-correction has attracted a lot of attention of researchers in recent years. To study quantum codes using non-commutative

setting of skew polynomial rings will be an interesting and challenging area of research. One may choose the ring $\mathbb{Z}_4 + u\mathbb{Z}_4$ with non-commutative setting for studying these codes.

3. One can also consider the rings of the form $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ with some conditions on u and v, for studying skew-cyclic codes, or other classes like skew constacyclic, skew quasi cyclic etc., over them. Further, the same work can be generalized to $\mathbb{Z}_q + u\mathbb{Z}_q + v\mathbb{Z}_q + uv\mathbb{Z}_q$.

4. To devise algorithms for finding all skew-cyclic codes of particular length and dimension, over the structures discussed in this thesis, will be a rigorous but an exciting and remarkable work.

Bibliography

[1] Abualrub, T., Aydin, N., and Seneviratne, P. On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *Australasian Journal of Combinatorics 54* (2012), 115–126.

[2] Abualrub, T., Ghrayeb, A., Aydin, N., and Siap, I. On the construction of skew quasi-cyclic codes. *IEEE Transactions on Information Theory 56*, 5 (2010), 2081–2090.

[3] Abualrub, T., and 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 42*, 3 (2007), 273–287.

[4] Abualrub, T., and Siap, I. Reversible cyclic codes over $\mathbb{Z}_4$. *Australasian Journal of Combinatorics 38* (2007), 195–205.

[5] Abualrub, T., and Siap, I. Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *Journal of the Franklin Institute 346*, 5 (2009), 520–529.

[6] Abualrub, T., Siap, I., and Aydogdu, I. $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-linear cyclic codes. In *Proceedings of the International MultiConference of Engineers and Computer Scientists, II* (2014).

[7] Aydin, N., Abualrub, T., and Siap, I. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. *IEEE Transactions on Information Theory 60*, 3 (2013), 1508–1514.

[8] Aydin, N., and Asamov, T. A database of $\mathbb{Z}_4$-codes. *Journal of Combinatorics, Information and System Sciences 34*, 1-4 (2009), 1–12.

[9] Aydogdu, I., and Siap, I. On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes. *Linear and Multilinear Algebra 63*, 10 (2015), 2089–2102.

[10] Bakshi, G. K., and Raka, M. Minimal cyclic codes of length p^nq. *Finite Fields and Their Applications 9*, 4 (2003), 432 – 448.

[11] Bakshi, G. K., and Raka, M. A class of constacyclic codes over a finite field. *Finite Fields and Their Applications 18*, 2 (2012), 362–377.

[12] Bakshi, G. K., and Raka, M. Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field. *Finite Fields and Their Applications 19*, 1 (2013), 39–54.

[13] Bandi, R., Tabue, A. F., and Martínez-Moro, E. On counting subring-submodules of free modules over finite commutative frobenius rings. *Designs, Codes and Cryptography* (2017), 1–8.

[14] Bandi, R. K., and Bhaintwal, M. Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. In *Signal Design and its Applications in Communications (IWSDA)* (2015), IEEE, pp. 47–51.

[15] Berlekamp, E. R. *Algebraic Coding Theory.* McGraw-Hill, 1968.

[16] Bhaintwal, M. Skew quasi-cyclic codes over Galois rings. *Designs, Codes and Cryptography 62*, 1 (2012), 85–101.

[17] Bhaintwal, M., and Wasan, S. K. On quasi-cyclic codes over $\mathbb{Z}_q$. *Applicable Algebra in Engineering, Communication and Computing 20*, 5-6 (2009), 459–480.

[18] Bhaintwal, M., and Wasan, S. K. Generalized Reed–Muller codes over $\mathbb{Z}_q$. *Designs, Codes and Cryptography 54*, 2 (2010), 149–166.

[19] Bhandari, M., Gupta, M. K., and Lal, A. K. On $\mathbb{Z}_4$-simplex codes and their gray images. In *Fossorier M., Imai H., Lin S., Poli A. (Eds.)*

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1999. Lecture Notes in Computer Science, vol. 1719, Springer, Berlin, Heidelberg.

[20] Blake, I. F. Codes over certain rings. *Information and Control 20*, 4 (1972), 396–404.

[21] Blake, I. F. Codes over integer residue rings. *Information and Control 29*, 4 (1975), 295–300.

[22] Bonnecaze, A., and Parampalli, U. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Transactions on Information Theory 45*, 4 (1999), 1250–1255.

[23] Bonnecaze, A., Solé, P., and Calderbank, A. R. Quaternary quadratic residue codes and unimodular lattices. *IEEE Transactions on Information Theory 41*, 2 (1995), 366–377.

[24] Borges, J., Fernández-Córdoba, C., and Ten-Valls, R. $\mathbb{Z}_2$-double cyclic codes. *arXiv preprint arXiv:1410.5604* (2014).

[25] Borges, J., Fernández-Córdoba, C., and Ten-Valls, R. $\mathbb{Z}_2$-double cyclic codes. *Designs, Codes and Cryptography 86*, 3 (2018), 463–479.

[26] Boucher, D., Geiselmann, W., and Ulmer, F. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing 18*, 4 (2007), 379–389.

[27] Boucher, D., Solé, P., and Ulmer, F. Skew constacyclic codes over Galois rings. *Advances in Mathematics of Communications 2*, 3 (2008), 273–292.

[28] Boucher, D., and Ulmer, F. Codes as modules over skew polynomial rings. In *IMA International Conference on Cryptography and Coding* (2009), Springer, pp. 38–55.

[29] Boucher, D., and Ulmer, F. Coding with skew polynomial rings. *Journal of Symbolic Computation 44*, 12 (2009), 1644–1656.

[30] Boucher, D., and Ulmer, F. Linear codes using skew polynomials with automorphisms and derivations. *Designs, Codes and Cryptography 70*, 3 (2014), 405–431.

[31] Calderbank, A. R., Rains, E. M., Shor, P., and Sloane, N. J. Quantum error correction via codes over $GF(4)$. *IEEE Transactions on Information Theory 44*, 4 (1998), 1369–1387.

[32] Calderbank, A. R., and Sloane, N. J. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography 6*, 1 (1995), 21–35.

[33] Chen, B., Fan, Y., Lin, L., and Liu, H. Constacyclic codes over finite fields. *Finite Fields and Their Applications 18*, 6 (2012), 1217 – 1231.

[34] Conway, J. H., and Sloane, N. J. Self-dual codes over the integers modulo 4. *Journal of Combinatorial Theory, Series A 62*, 1 (1993), 30–45.

[35] Dertli, A., Cengellenmis, Y., and Eren, S. On quantum codes obtained from cyclic codes over A_2. *International journal of quantum information 13*, 03 (2015), 1550031.

[36] Dinh, H. Q. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *Journal of Algebra 324*, 5 (2010), 940–950.

[37] Dinh, H. Q., and López-Permouth, S. R. Cyclic and negacyclic codes over finite chain rings. *IEEE Transactions on Information Theory 50*, 8 (2004), 1728–1744.

[38] Dinh, H. Q., Nguyen, B. T., and Sriboonchitta, S. Skew constacyclic codes over finite fields and finite chain rings. *Mathematical Problems in Engineering, Article ID: 3965789* (2016).

[39] Dougherty, S. T., and Shiromoto, K. Maximum distance codes over rings of order 4. *IEEE Transanctions on Information Theory 47*, 1 (2001), 400–404.

[40] Fogarty, N., and Gluesing-Luerssen, H. A circulant approach to skew-constacyclic codes. *Finite Fields and Their Applications 35* (2015), 92–114.

[41] Gao, J. Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. *Journal of Applied Mathematics & Informatics 31*, 3-4 (2013), 337–342.

[42] Gao, J. Linear codes over $\mathbb{Z}_9 + u\mathbb{Z}_9$: MacWilliams identity, self-dual codes, quadratic residue codes, and constacyclic codes. *arXiv preprint arXiv:1405.3347* (2014).

[43] Gao, J., Ma, F., and Fu, F. Skew constacyclic codes over the ring $\mathbb{F}_q + v\mathbb{F}_q$. *Applied and Computational Mathematics 6*, 3 (2017), 286–295.

[44] Glynn, D. G., Gulliver, T. A., and Gupta, M. K. On some quaternary self-orthogonal codes. *Ars Combinatoria 85* (2007), 129–154.

[45] Grassl, M. Bounds on the minimum distance of linear codes. *http://www. codetables. de* (2008).

[46] Gupta, M. K. On $\mathbb{Z}_4$ codes satisfying the chain condition. *Australasian Journal of Combinatorics 31* (2005), 263–272.

[47] Gupta, M. K., Bhandari, M. C., and Lal, A. K. On linear codes over $\mathbb{Z}_{2^s}$. *Designs, Codes and Cryptography 36*, 3 (2005), 227–244.

[48] Gursoy, F., Siap, I., and Yildiz, B. Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$. *Advances in Mathematics of Communications 8*, 3 (2014), 313–322.

[49] Hamming, R. W. Error detecting and error correcting codes. *Bell Labs Technical Journal 29*, 2 (1950), 147–160.

[50] Hammons, A. R., Kumar, P. V., Calderbank, R. A., Sloane, N. J. A., and Solé, P. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory 40*, 2 (1994), 301–319.

[51] Hughes, G. Constacyclic codes, cocycles and a $(u + v|u - v)$ construction. *IEEE Transactions on Information Theory 46*, 2 (2000), 674–680.

[52] Ikai, T., Kosako, H., and Kojima, Y. Two-dimensional cyclic codes. *Electronics and Communications in Japan 57A* (1975), 27–35.

[53] Imai, H. Two-dimensional fire codes. *IEEE Transactions on Information Theory 19*, 6 (1973), 796–806.

[54] Imai, H. A theory of two-dimensional cyclic codes. *Information and Control 34*, 1 (1977), 1–21.

[55] Janwa, H., and Lal, A. K. On the generalized hamming weights of cyclic codes. *IEEE Transactions on Information Theory 43*, 1 (1997), 299–308.

[56] Jensen, J. M. Cyclic concatenated codes with constacyclic outer codes. *IEEE transactions on information theory 38*, 3 (1992), 950–959.

[57] Jensen, J. M. A class of constacyclic codes. *IEEE Transactions on Information Theory 40*, 3 (1994), 951–954.

[58] Jitman, S., Ling, S., and Udomkavanich, P. Skew constacyclic codes over finite chain rings. *Advances in Mathematics of Communications 6*, 1 (2012), 39–63.

[59] Kai, X., and Zhu, S. Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. *International Journal of Quantum Information 9*, 02 (2011), 689–700.

[60] Kai, X., Zhu, S., and Wang, L. A family of constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Journal of Systems Science and Complexity 25*, 5 (2012), 1032–1040.

[61] Kanwar, P., and López-Permouth, S. R. Cyclic codes over the integers modulo p^m. *Finite Fields and Their Applications 3*, 4 (1997), 334–352.

[62] Karadeniz, S., and Yildiz, B. $(1 + v)$-constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Journal of the Franklin Institute 348*, 9 (2011), 2625–2632.

[63] La, G., Giuliano, G., and Palazzo Jr, R. Constructions of new families of nonbinary *CSS* codes. *Discrete Mathematics 310*, 21 (2010), 2935–2945.

[64] Li, R., and Li, X. Binary construction of quantum codes of minimum distance three and four. *IEEE Transactions on Information Theory 50*, 6 (2004), 1331–1335.

[65] Li, X., and Li, H. 2-D skew-cyclic codes over $\mathbb{F}_q[x, y; \rho, \theta]$. *Finite Fields and Their Applications 25* (2014), 49–63.

[66] Ling, S., and Solé, P. Nonadditive quantum codes from $\mathbb{Z}_4$-codes. *arXiv print:0704.2122* (2008).

[67] Luo, R., and Parampalli, U. Self-dual cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. In *Signal Design and its Applications in Communications (IWSDA), 2015 Seventh International Workshop on* (2015), IEEE, pp. 57–61.

[68] Luo, R., and Parampalli, U. Self-Dual cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 100*, 4 (2017), 969–974.

[69] MacWilliams, F. J., and Sloane, N. J. A. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[70] Marrow, M. *Detection and Modeling of Two-Dimensional Signals.* University of California, San Diego, 2004.

[71] Martínez-Moro, E., and Rúa, I. F. Multivariable codes over finite chain rings: serial codes. *SIAM Journal on Discrete Mathematics 20*, 4 (2006), 947–959.

[72] Martínez-Moro, E., and Rúa, I. F. On repeated-root multivariable codes over a finite chain ring. *Designs, Codes and Cryptography 45*, 2 (2007), 219–227.

[73] Martínez-Moro, E., Szabo, S., and Yildiz, B. Linear codes over $\frac{\mathbb{Z}_4[x]}{\langle x^2+2x\rangle}$. *International Journal of Information and Coding Theory 3*, 1 (2015), 78–96.

[74] McDonald, B. R. *Finite Rings with Identity.* Marcel Dekker Incorporated, 1974.

[75] Noether, E., and Schmeidler, W. Moduln in nichtkommutativen bereichen, insbesondere aus differential-und differenzenausdrucken. *Mathematische Zeitschrift 8*, 1-2 (1920), 1–35.

[76] Ore, O. Theory of non-commutative polynomials. *Annals of Mathematics* (1933), 480–508.

[77] Ozen, M., Uzekmek, F. Z., Aydin, N., and Ozzaim, N. T. Cyclic and some constacyclic codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}$. *Finite Fields and Their Appications 38* (2016), 27–39.

[78] Parampalli, U., and Bonnecaze, A. Cyclic codes over a linear companion of $\mathbb{Z}_4$. In *Proceedings: IEEE International Symposium on Information Theory* (1998), pp. 398–398.

[79] Pless, V., Brualdi, R. A., and Huffman, W. C. E. *Handbook of Coding Theory.* Elsevier Science Inc., 1998.

[80] Prange, E. Cyclic error-correcting codes in two symbols. *Air Force Cambridge Research Center-AFCRC-TN;57-103* (1957).

[81] Prange, E. Some cyclic error-correcting codes with simple decoding algorithms. *Air Force Cambridge Research Center-TN-58-156* (1958).

[82] Qian, J. Constacyclic and cyclic codes over finite chain rings. *The Journal of China Universities of Posts and Telecommunications 16*, 3 (2009), 122–125.

[83] Qian, J. Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *Journal of Information & Computational Science 10*, 6 (2013), 1715–1722.

[84] Qian, J., Ma, W., and Guo, W. Quantum codes from cyclic codes over finite ring. *International Journal of Quantum Information 7*, 06 (2009), 1277–1283.

[85] Qian, J., Zhang, L., and Zhu, S. $(1 + u)$-constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *Applied Mathematics Letters 19*, 8 (2006), 820–823.

[86] Ribenboim, P. Sur la localisation des anneaux non commutatifs. *Seminaire Dubreil. Algebre et Theorie des Nombres 24* (1972), 1970–1971.

[87] Shankar, P. On BCH codes over arbitrary integer rings. *IEEE Transactions on Information Theory 25*, 4 (1979), 480–483.

[88] Shannon, C. A mathematical theory of communication. *Bell System Technical Journal* (1948), 379–423 & 623–656.

[89] Sharma, A. Repeated-root constacyclic codes of length $l^t p^s$ and their dual codes. *Cryptography and Communications 7*, 2 (2015), 229–255.

[90] Sharma, A., and Rani, S. On constacyclic codes over finite fields. *Cryptography and Communications 8*, 4 (2016), 617–636.

[91] Sharma, A., and Rani, S. Repeated-root constacyclic codes of length $4l^m p^n$. *Finite Fields and Their Applications 40* (2016), 163–200.

[92] Sharma, A., and Sharma, A. K. Construction of self-dual codes over $\mathbb{Z}_{2^m}$. *Cryptography and Communications 8*, 1 (2016), 83–101.

[93] Shi, M., Qian, L., Sok, L., Aydin, N., and Solé, P. On constacyclic codes over $\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}$ and their Gray images. *Finite Fields and Their Applications 45* (2017), 86–95.

[94] Shi, M., Yao, T., Alahmadi, A., and Solé, P. Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E98-A*, 8 (2015), 1845–1848.

[95] Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Physical Review A 52*, 4 (1995), R2493.

[96] Siap, I., Abualrub, T., Aydin, N., and Seneviratne, P. Skew cyclic codes of arbitrary length. *International Journal of Information and Coding Theory 2*, 1 (2011), 10–20.

[97] Spiegel, E. Codes over $\mathbb{Z}_m$. *Information and Control 35*, 1 (1977), 48–51.

[98] Spiegel, E. Codes over $\mathbb{Z}_m$ (revisited). *Information and Control 37* (1978), 100–104.

[99] Steane, A. M. Enlargement of calderbank-shor-steane quantum codes. *IEEE Transactions on Information Theory 45*, 7 (1999), 2492–2495.

[100] Tapia-Recillas, H., and Vega, G. On $\mathbb{Z}_{2^k}$-linear and quaternary codes. *SIAM Journal on Discrete Mathematics 17*, 1 (2003), 103–113.

[101] Wieb Bosma, J. C., and Playoust, C. The Magma algebra system. *I*. The user language. *Journal of Symbolic Computation 24* (1997), 235–265.

[102] Wootters, W. K., and Zurek, W. H. A single quantum cannot be cloned. *Nature 299*, 5886 (1982), 802–803.

[103] Yildiz, B., and Karadeniz, S. Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Designs, Codes and Cryptography 58*, 3 (2011), 221–234.

[104] Yildiz, B., and Karadeniz, S. Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self-dual codes. *Finite Fields and Their Applications 27* (2014), 24–40.

[105] Yoon, S. W., and Moon, J. Two-dimensional cyclic codes correcting known error patterns. In *Global Communications Conference (GLOBECOM), IEEE* (2012), pp. 3231–3236.

[106] Zhu, S., and Kai, X. A class of constacyclic codes over $\mathbb{Z}_{p^m}$. *Finite Fields and Their Applications 16*, 4 (2010), 243–254.

[107] Zhu, S., and Wang, L. A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image. *Discrete Mathematics 311*, 23-24 (2011), 2677–2682.

[108] Zhu, S., Wang, Y., and Shi, M. Some results on cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$. *IEEE Transactions on Information Theory 56*, 4 (2010), 1680–1684.