REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

VECTORIAL CYCLIC CODES AND THEIR ALGEBRAIC STRUCTURES

Sümeyra BEDİR

DOCTOR OF PHILOSOPHY THESIS
Department of Mathematics
Program of Mathematics

Advisor
Prof. Dr. Bayram Ali ERSOY

July, 2019

REPUBLIC OF TURKEY
YILDIZ TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

VECTORIAL CYCLIC CODES AND THEIR ALGEBRAIC STRUCTURES

A thesis submitted by Sümeyra BEDİR in partial fulfillment of the requirements for the degree of **DOCTOR OF PHILOSOPHY** is approved by the committee on 01.07.2019 in Department of Mathematics, Program of Mathematics.

Prof. Dr. Bayram Ali ERSOY
Yildiz Technical University
Advisor

Approved By the Examining Committee

Prof. Dr. Bayram Ali ERSOY, Advisor
Yildiz Technical University _____

Prof. Dr. A. Göksel AGARGUN, Member
Yildiz Technical University _____

Prof. Dr. Ismail KUCUK, Member
Istanbul Sabahattin Zaim University _____

Assoc. Prof Dr. Emre KOLOTOGLU, Member
Yildiz Technical University _____

Assist. Prof. Dr. Fatih TEMIZ, Member
Istanbul Gelisim University _____

I hereby declare that I have obtained the required legal permissions during data collection and exploitation procedures, that I have made the in-text citations and cited the references properly, that I haven't falsified and/or fabricated research data and results of the study and that I have abided by the principles of the scientific research and ethics during my Thesis Study under the title of Vectorial Cyclic Codes and Their Algebraic Structures supervised by my supervisor, Prof. Dr. Bayram Ali ERSOY. In the case of a discovery of false statement, I am to acknowledge any legal consequence.

Sümeyra BEDİR

Signature

Dedicated to my mother-in-law

ACKNOWLEDGEMENTS

My PhD study has been a long and hard journey all for me, for my advisor, for my colleagues, for my family and friends. First, I would like to thank my previous advisor Prof. Dr. Irfan SIAP for his enlightening vision and continuous guidance through selecting and developing a research subject and method. Next and most, for his great patience, compassion and guidance through the finish line, I would like to thank my current advisor Prof. Dr. Bayram Ali ERSOY. I would like to thank all the jury members and thesis periodic evaluation committee members for all their valuable contributions. Special thanks to Prof. Dr. Ihsan KAYA, Prof. Dr. Ismail KUCUK, Prof. Dr. Eyup BAGCI and all the academic and executive staff of Graduate School of Natural and Applied Sciences for their guidance through my academic studies during my research assistant-ship.

From my family, I would like to thank mostly to whom I dedicate this thesis to, my mother-in-law. She has been always behind the scenes; taking care of my twin sons, cooking and keeping the house hold in place of me while I was on research. I would never be able to count her contributions to my life and to my education. Next I would like to thank to my husband, my sons, my mother, father, father-in-law for all their devotion and motivation.

All my friends and colleagues, great thanks to you for being with me in this journey.

Sümeyra BEDİR

TABLE OF CONTENTS

LIST OF SYMBOLS

A^{tr}	Transpose of a Matrix A
A^{-1}	Multiplicative Inverse of a Matrix A
F_q^*	Unit Group of Finite Field F_q

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
GQC	Generalized Quasi-cyclic
QC	Quasi-cyclic

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Vectorial Cyclic Codes and Their Algebraic Structures

Sümeyra BEDİR

Department of Mathematics
Doctor of Philosophy Thesis

Advisor: Prof. Dr. Bayram Ali ERSOY

In Algebraic Coding Theory, constructing codes with optimal parameters, discovering new code families and subfamilies, proposing new algebraic coding methods, generalizing and applying these methods to various algebraic structures or constructing best known codes in different and preferably more efficient ways have all been important research subjects.

In this study, polycyclic codes, which are based on polycyclic shift that creates vector-circulant matrices, are examined over different algebraic structures. The term "multi polycyclic codes" is contributed to the literature, with introducing generator and parity check conditions and duality theorems especially over skew polynomial rings. Moreover, a polycyclic code construction method is proposed over matrix spaces.

Keywords: Linear codes, Polycyclic codes, Vector-circulant matrices, Pseudo-cyclic codes

ÖZET

Vektörel Devirli Kodlar ve Cebirsel Yapıları

Sümeyra BEDİR

Matematik Anabilim Dalı
Doktora Tezi

Danışman: Prof. Dr. Bayram Ali ERSOY

Cebirsel Kodlama Teorisi'nde optimal parametrelere sahip kodlar üretilmesi, yeni kod aileleri ve alt ailelerinin keşfedilmesi, yeni cebirsel kodlama metodlarının önerilmesi, bu metodların ceşitli cebirsel yapılar üzerinde genelleştirilmesi ve uygulanması veya bilinen en iyi kodların farklı ve tercihen daha etkili yollarla oluşturulması önemli araştırma alanları olagelmiştir.

Bu çalışmada, vektör-devirli matrisler oluşturmayı sağlayan çoklu devir lineer dönüşümü temelli çoklu devirli kodlar, değişik cebirsel yapılar üzerinde ele alınmıştır. "Multi polycyclic" kod tanımı literatüre kazandırılmış, bununla birlikte üreteç ve parite-kontrol durumları ve duallik teoremleri özellikle skew polinom halkaları üzerinde sunulmuştur. Ayrıca, matris uzayları üzerinde çoklu devirli kod üretme metodu önerilmiştir.

Anahtar Kelimeler: Lineer kodlar, Çoklu devirli kodlar, Vektör-devirli matrisler, Pseudo-devirli kodlar

YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

1
Introduction

1.1 Literature Review

Algebraic Coding Theory, specifically the "Error Correcting Codes" has been attracting many researchers for years in terms of relating the more practical and industrial research areas of Information Transmission and Information Security to theoretical backgrounds with underlying algebraic structures. There are many books covering Coding Theory and its applications. But the core ones which this thesis will mainly be referring to for the main concepts of Coding Theory are books of Xing and Ling [1], Huffman and Pless [2] and Peterson and Weldon [3].

First studies of error correcting codes started over Finite Fields [4]. There are still remarkable research on codes over finite fields mostly dealing with optimal code search [5]. Studies are extended to codes over finite chain rings in recent years [6–8].

In algebraic coding theory, not only building new construction methods, exploring optimal parameters, finding new codes and new algebraic structures, but building new criss-cross relationships between known construction methods and existing algebraic structures also bring out promising results. One example of this might be construction of codes over matrix spaces. "Gabudilin codes", "array codes", "codes correcting lattice errors" are all of this kind [9–11].

Another algebraic structure that highly attracted the coding theorists has been Skew Polynomial Rings [12]. Thanks to its noncommutative structure, applying the well known code construction methods over skew polynomial rings has resulted in obtaining codes with optimal parameters directly.

Polycyclic codes were first introduced in [3], as "pseudo-cyclic codes" corresponding to shortened codes. After more than thirty years, a direct construction method has been introduced for this family of codes [13]. Similar to cyclic or constacyclic codes, polycyclic codes were examined as an efficient direct construction method for obtaining codes with good parameters [14–16].

1.2 Objective of the Thesis

This thesis concentrates on the construction method of polycyclic codes, which depends actually on a vector-circulant linear transformation. This invertible transformation is represented with companion matrices of polynomials which creates the base quotient ring. The way that this transformation and its inverse affects the codewords, builds an interesting code structure.

The main results of this study involve examining structural properties of polycyclic codes and their duals, generators and dual generators over finite fields, finite chain rings and skew polynomial rings; introducing a vectorial cyclic construction of codes over matrix spaces and introducing multi-polycyclic codes and their algebraic structures over both finite fields and skew polynomial rings.

1.3 Original Contribution

Even though the construction method had been previously defined, this study includes many original applications. One of them is applying the construction method to codes over matrix spaces. Another original part is characterization of dual generator polynomials of polycyclic codes. Finally, multi polycyclic codes over skew polynomial rings with clarifications on generator and parity check conditions are also of original work.

2
Preliminaries

Coding theory can be considered as an inter-disciplinary research field, tying up communications, electronics, computer sciences and mathematics over decades. The practice lies basically over attaining reliable information transmission and storage via noisy communication channels. The simplest diagram for the information transmission is given in Figure 2.1.

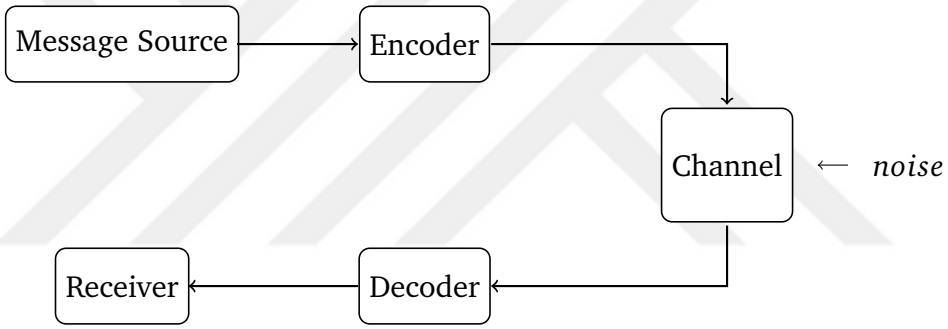

Figure 2.1 Information transmission

Consider ASCII encoding where every single character (letters, numbers, etc.) is represented with an 8-bits $\{0,1\}$-string. It encodes the message words in human language to words that computers can understand.

This way of coding is called "source coding", which may fail to detect errors that happen during transmission, since every single bit change (error) results a reasonably misinterpreted new message. With spending a little cost on speed and storage, adding some more bits, "channel decoding", increases redundancy and enhances error detection.

Involving channel decoding, the above diagram becomes as in Figure 2.2.

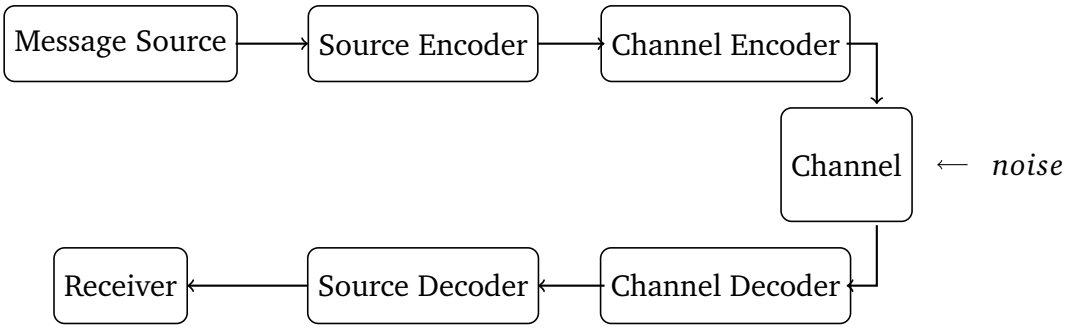

Figure 2.2 Channel encoding

Error correcting is a different story, which sometimes require a retransmission, mostly applicable in two-way channels. However, there are information storage systems, like when the equipment is not rewritable, that employ one-way channels, where asking for retransmission is not possible. In any case, error-correcting capability is affected by the very same algebraic structural dependencies as the code's error-detecting capability.

There are also differences in communication systems in terms of operating the information sequence that is transmitted. One type of coding which is called "block codes" divides the information sequence into equally long sections or blocks before processing them. Whereas another type called "tree codes" operates on the sequence without breaking it.

Consequently, being affected by somewhat conflicting dependencies, coding theory has its basic natural goals and/or problems, which can be summarized as follows

- Find codes with higher error-detection and correction capabilities (requires additional length),
- Obtain fast and effective encoding and decoding methods,
- Enhance easy transmission,
- Transfer maximum amount of information per time.

2.1 Basic Definitions

Definition 2.1. A set $A = \{a_1, a_2, ..., a_q\}$ with cardinality q is referred to as a *code alphabet* whose elements are called *code symbols*. A q-ary word of length n over the alphabet A is a sequence $c = c_1c_2...c_n$ where $c_i \in A$, $\forall i$.

Definition 2.2. A q-ary *block code* C over the alphabet A is a non-empty set of q-ary words having the same length n. Elements of C are called *codewords*.

Definition 2.3. The **Size** of a code C is the number of codewords in C, and denoted by $|C|$.

Definition 2.4. The **Information Rate** of a code C with length n over A is defined to be $\log_q |C|/n$.

Definition 2.5. The **Minimum (Hamming) Distance** of a code C is

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

where $d(x, y)$ stands for the distance with respect to the Hamming metric between codewords x, y; namely, the number of places where x and y differ.

A code in general, with length n, size M and minimum distance d is denoted with its parameters as an (n, M, d)-code.

The decoding procedure, which is actually the rule for finding the most possible codeword to be sent when a message is received with error, is tied with the capabilities of the channel in terms of detecting or correcting errors. This capability is shown to be highly dependent to the minimum distance of the code. A code C with minimum distance d, can detect up to $d-1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors [1].

Upon the fundamental definitions above, there comes the main problem of coding theory; given a q-ary alphabet, a length n and a minimum distance d, find a code with these parameters and the maximal possible number M of codewords. Therefore, "good" codes are those with small n for fast transmission, large M to permit a wide variety of messages and large d for detecting and correcting large number of errors.

For a fixed n and d, an (n, M, d)-code with the largest possible size M is called an *optimal code*. There are upper and lower bounds for these optimal numbers for both linear and nonlinear codes. The reader may refer to [1] for the descriptions of well known bounds. This study will consider the up-to-date conditions of constructions given in [17] for codes with good parameters as well as for optimal codes.

2.2 Linear Codes

Definition 2.6. Let F_q be a finite field with q elements. A linear code C of length n over F_q is a subspace of the vector space ${F_q}^n$.

Due to their algebraic, structural and computational advantages, such as being mathematically descriptive, providing easy encoding and decoding, etc. linear codes have taken more attention among algebraic coding theoretical research.

Linear codes are considered as subspaces of vector spaces. In this point of view, each codeword is regarded as a vector rather than being a sequence of symbols and the algebraic structure over which the code is defined is exactly the alphabet for linear codes[1]. The size of a linear code is identified with its dimension(k) as a subspace, i.e. $M = q^k$. A linear code C over F_q with length n, dimension k and minimum distance d is therefore expressed as an $[n, k, d]_q$-code. The orthogonal complement of a linear code is defined to be the *dual code* of C and denoted by $C^{\perp}$.

One of the most mathematically advantageous aspects of studying linear codes is the ability to use the correspondence between vectors and polynomials. Thereby one can regard a codeword as either a vector or as its corresponding polynomial and all the computational flexibility of polynomial rings helps a lot in the big picture.

Being a subspace also provides linear codes to be expressible with its basis vectors. Having the basis means having the general information about the whole code. The basis vectors form the rows of so-called *generator matrix* G of a linear code C. On the other hand, rows of a *parity-check matrix* H for C is formed by the basis vectors of $C^{\perp}$. Generator and parity check matrices are used in encoding and decoding linear codes respectively and they enhance faster procedures compared to arbitrary nonlinear codes. The subspace definition of linear codes may be given in two ways; giving G as a basis for C, or defining C as the null space of H. Combining both gives us the equation $GH^{tr} = 0$.

Another advantage of a linear code arise while computing its minimum distance. Its linear structure allows the minimum distance to be directly the smallest Hamming weight of its nonzero codewords.

Before giving details about common classes of linear codes, the following image will help us figure out the structural generalizations among them. We will soon have more information about their specifications and relations.

[1] In order to keep the definition simple, the alphabet for linear codes are kept as finite fields. However, linear codes can also be defined over rings.

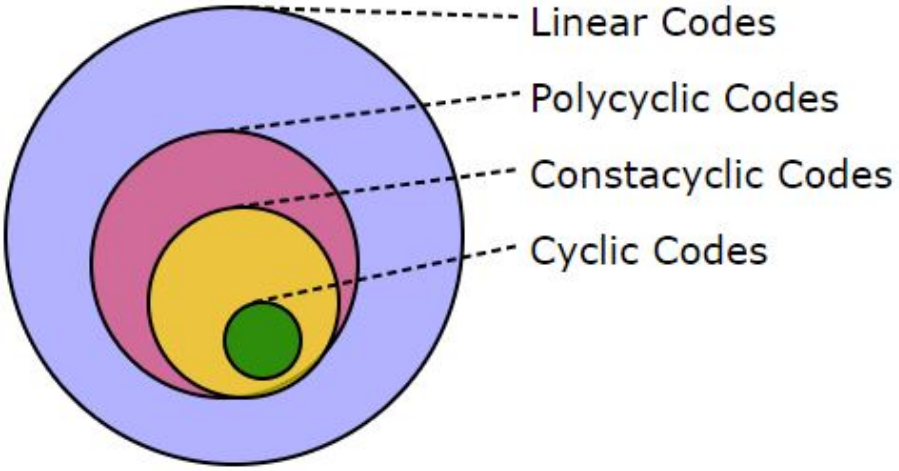

Figure 2.3 Generalization of some classes of linear codes

2.2.1 Cyclic Codes

Algebraically, besides linearity, more structures such as cyclicity has allowed easier implementation of codes. Cyclic codes were first introduced in 1957 [4].

Definition 2.7. A linear code C is called *cyclic* if whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C so is its cyclic shift $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$.

Cyclic codes are invariant subspaces of ${F_q}^n$ under the transformation which applies cyclic shift to a vector. Cyclic codes involve the practical use of the following correspondence

$$\begin{aligned} \pi : {F_q}^n &\longrightarrow F_q[x]/(x^n - 1) \\ (c_0, c_1, \ldots, c_{n-1}) &\longmapsto c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}. \end{aligned} \tag{2.1}$$

Each codeword $(c_0, c_1, \ldots, c_{n-1})$ is associated to a polynomial $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ in $F_q[x]$ and every cyclic code corresponds to an ideal of $F[x]/(x^n - 1)$. The representation matrix for the cyclic shift transformation, which we will denote by T (getting the corresponding polynomial as a subscript), is precisely the companion matrix of the polynomial $x^n - 1$ and any monic divisor of this polynomial generates a cyclic code. At the first hand, we have got the advantage of identifying a code with only one polynomial, which is called a generator polynomial for C, rather than a matrix of basis vectors. Moreover, the dimension of C is determined directly to be k if the degree of the generator polynomial is $n - k$.

Let C be a cyclic $[n, k, d]_q$-code over a finite field F_q, generated by $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$, i.e. $C = (g(x)) \leq F[x]/(x^n - 1)$ with $\pi^{-1}(g(x)) = g$. Then the generator matrix G of C can be obtained as follows

$$G = \begin{bmatrix} g \\ gT_{x^n-1} \\ gT_{x^n-1}^2 \\ \vdots \\ gT_{x^n-1}^{n-1} \end{bmatrix}_{nxn} \quad where \;\; T_{x^n-1} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ \vdots & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{nxn} . \tag{2.2}$$

We get

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_{n-1} & g_0 & \cdots & g_{n-2} \\ \ddots & \ddots & \ddots & \ddots \\ g_1 & \cdots & g_{n-1} & g_0 \end{bmatrix}_{nxn} \tag{2.3}$$

and G becomes the following matrix with rank k

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ & \ddots & & \ddots & & \ddots & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}_{kxn} . \tag{2.4}$$

Expression 2.2 points out that the cyclic code C as a subspace, is invariant under the cyclic shift transformation and G can also be obtained by evaluating $g(x)$ with T_{x^n-1}, i.e $G = g(T_{x^n-1})$ [18].

The dual code of a cyclic code C is also cyclic. Reciprocal of the polynomial $h(x) = x^n - 1/g(x)$, denoted with $h^R(x)$, generates the dual code of C. Parity check matrix H for C can be obtained from evaluating $h(T_{x^n-1}^{tr})$ [18–20].

2.2.2 Constacyclic Codes

Constacyclic codes are a one step more generalized type of linear codes. The definition was first introduced by [21] in 1968.

Definition 2.8. Let $\alpha \in F_q^*$. A linear code C is called α—*constacyclic* if whenever $(c_0, c_1, \ldots, c_{n-1})$ is in C so is its α—constacyclic shift $(\alpha c_{n-1}, c_0, c_1, \ldots, c_{n-2})$.

An α—constacyclic code corresponds to an ideal of $F[x]/(x^n - \alpha)$. The representation matrix for α—constacyclic shift, which we will denote by $T_{x^n-\alpha}$ is the companion matrix of the polynomial $x^n - \alpha$ and any monic divisor of this polynomial generates an α—constacyclic code.

Let C be an α—constacyclic $[n,k,d]_q$-code over a finite field F_q, generated by $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$, i.e. $C = (g(x)) \leq F[x]/(x^n - \alpha)$. Then the generator matrix G of C can be obtained as follows

$$G = \begin{bmatrix} g \\ gT_{x^n-\alpha} \\ gT^2_{x^n-\alpha} \\ \vdots \\ gT^{n-1}_{x^n-\alpha} \end{bmatrix}_{nxn} \quad where \;\; T_{x^n-\alpha} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ \vdots & 0 & \cdots & 0 & 1 \\ \alpha & 0 & \cdots & \cdots & 0 \end{bmatrix}_{nxn} . \tag{2.5}$$

We obtain a generator matrix as an α—twistulant matrix

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ \alpha g_{n-1} & g_0 & \cdots & g_{n-2} \\ \ddots & \ddots & \ddots & \ddots \\ \alpha g_1 & \cdots & \alpha g_{n-1} & g_0 \end{bmatrix}_{nxn} . \tag{2.6}$$

Similar to the cyclic case, G can also be obtained by evaluating $g(x)$ with $T_{x^n-\alpha}$, i.e $G = g(T_{x^n-\alpha})$ [18].

The dual code of an α—constacyclic code C is shown to be an α^{-1}—constacyclic code [22]. A parity check matrix for C can be obtained by evaluating $h(T^{tr}_{x^n-\alpha})$. For a concrete generating polynomial of the dual code we will give a general theorem in Chapter 5.

2.2.3 Polycyclic Codes

Polycyclic codes over finite fields were first introduced in [3]. Although every polycyclic code corresponds to a shortened cyclic code over finite fields, polycyclic codes have attracted many researchers with their rich algebraic structure especially in terms of introducing a direct construction [13–16].

Let $c = (c_0, c_1, \ldots, c_{n-1})$ be any vector in F_q^n. We fix a shift vector $v = (v_0, v_1, \ldots, v_{n-1})$ and define the following linear transformation on F_q^n

$$\tau_v : (c_0, c_1, \ldots, c_{n-1}) \mapsto (v_0c_{n-1}, c_0 + v_1c_{n-1}, \ldots, c_{n-2} + v_{n-1}c_{n-1}) \tag{2.7}$$

It has the following representation matrix which is exactly the companion matrix for

$f(x) = x^n - v(x)$ and we have $\tau_v(c) = c.T_{x^n - v(x)}$.

$$T_{x^n - v(x)} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 0 \\ \vdots & 0 & \cdots & 0 & 1 \\ v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \end{bmatrix}_{nxn} \tag{2.8}$$

The following small example illustrates the case.

Example 2.1. *Let $c = (c_0, c_1, c_2)$ be a vector in some vector space F_q^3. Let $v = (v_0, v_1, v_2)$ be the shift vector.*

Thus we have

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ v_0 & v_1 & v_2 \end{bmatrix}$$

And the transformation τ_v maps $c = (c_0, c_1, c_2)$ to the vector $\tau_v(c) = (v_0c_2, c_0 + v_1c_2, c_1 + v_2c_2)$ as follows;

$$\tau_v(c) = c \cdot T = \begin{bmatrix} c_0 & c_1 & c_2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ v_0 & v_1 & v_2 \end{bmatrix} = \begin{bmatrix} v_0c_2 & c_0 + v_1c_2 & c_1 + v_2c_2 \end{bmatrix}$$

Here, T is exactly the companion matrix for $f(x) = x^3 - (v_0 + v_1x + v_2x^2)$.

Definition 2.9 (Polycyclic Code)**.** A linear code C with length n over a finite field F_q is called *polycyclic* with respect to the vector $v = (v_0, v_1, \ldots, v_{n-1}) \in F_q^n$, if whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is its v—polycyclic shift $(v_0c_{n-1}, c_0 + v_1c_{n-1}, \ldots, c_{n-2} + v_{n-1}c_{n-1})$.

A polycyclic code with respect to v is invariant under τ_v and corresponds to an ideal of $F[x]/(x^n - v(x))$. Any monic divisor of the polynomial $x^n - v(x)$ generates a v—polycyclic code.

Let C be a v—polycyclic $[n, k, d]_q$-code over a finite field F_q, generated by $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$, i.e. $C = (g(x)) \leq F[x]/(x^n - v(x))$. Then the generator matrix G of C can be obtained as follows

$$G = \begin{bmatrix} g \\ gT_{x^n-v(x)} \\ gT^2_{x^n-v(x)} \\ \vdots \\ gT^{n-1}_{x^n-v(x)} \end{bmatrix}_{nxn} \tag{2.9}$$

So we get G as a $v-$ vector circulant matrix [23]

$$G = \begin{bmatrix} g \\ \tau_v(g) \\ \tau^2_v(g) \\ \vdots \\ \tau^{n-1}_v(g) \end{bmatrix}_{nxn} \tag{2.10}$$

G can also be obtained by evaluating $g(x)$ with $T_{x^n-v(x)}$, i.e., $G = g(T_{x^n-v(x)})$ [20].

Notice that any cyclic code is polycyclic with respect to $v = (1, 0, \ldots, 0)$ with $v(x) = 1$ and any constacyclic code with respect to α, is polycyclic with respect to $v = (\alpha, 0, \ldots, 0)$ with $v(x) = \alpha$.

3
The Dual Code and Sequential Codes

3.1 Dual Code of a Polycyclic Code

The dual code of a polycyclic code is a type of "sequential code" [14].

Definition 3.1 (Sequential Codes)**.** A linear code C with length n over a finite field F is called *sequential* with respect to the the vector $\omega = (\omega_0, \omega_1, \ldots, \omega_{n-1})$, if there is a function $\varphi_\omega : F^n \longrightarrow F$ such that whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is $(\varphi_\omega(c_0, c_1, \ldots, c_{n-1}), c_0, c_1, \ldots, c_{n-2})$.

Let C be a polycyclic code with respect to $v = (v_0, v_1, \ldots, v_{n-1})$, with generating polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}$, and let $h(x) = (x^n - v(x))/g(x)$. Set $\omega = (v_0^{-1}, -v_{n-1}/v_0, -v_{n-2}/v_0, \ldots, -v_1/v_0)$. And consider the following transformation on F^n

$$\rho_\omega : (c_0, c_1, \ldots, c_{n-1}) \mapsto (\omega_{n-1}c_0 + \omega_{n-2}c_1 + \cdots + \omega_0 c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \tag{3.1}$$

The matrix representation for ρ_ω is exactly $(T^{-1}_{x^n - v(x)})^{tr}$, and note that v_0 should be invertible in any case.

The dual code of a polycyclic code with respect to $v = (v_0, v_1, \ldots, v_{n-1})$ is therefore a sequential code with respect to $\omega = (v_0^{-1}, -v_{n-1}/v_0, \ldots, -v_1/v_0)$, where $\varphi_\omega(c_0, c_1, \ldots, c_{n-1}) = \omega_{n-1}c_0 + \omega_{n-2}c_1 + \cdots + \omega_0 c_{n-1}$. A parity check matrix H can either be obtained by evaluating $h(T^{tr}_{x^n - v(x)})$ or $h^R((T^{-1}_{x^n - v(x)})^{tr})$.

Having sequential codes defined, the generalizations in Figure (2.3) becomes as in the below figure [1].

[1] Actually, the familiy of sequential codes are wide. Here we only refer them as the dual codes of polycyclic codes.

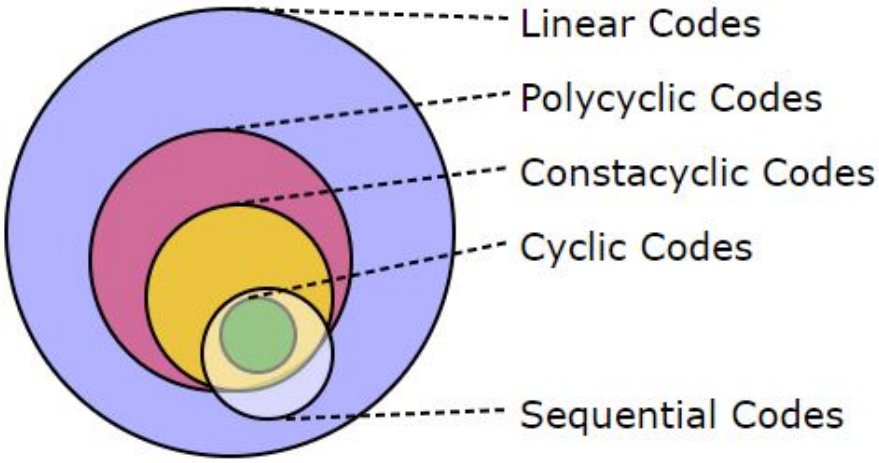

Figure 3.1 Sequential codes in the generalization of linear codes

Polycyclic codes and their duals are fully characterized over finite fields and finite chain rings [13, 16, 20]. They have been constructed as module-θ codes using skew polynomial rings [24].

Polycyclic codes have an ideal structure, and over the corresponding polynomial ring, we are able to find a generating polynomial/ a generating vector and this provides constructing a vector-circulant generating matrix. However, sequential codes do not have an ideal structure. The transformation does not correspond to multiplication by x in the polynomial correspondence. So, the question is: How can we obtain a generating polynomial/ generating vector a for the dual code of a polycyclic code so that we obtain a direct construction as follows

$$H = \begin{bmatrix} \cdots & a & \cdots \\ \cdots & \rho_\omega(a) & \cdots \\ \cdots & \rho_\omega^2(a) & \cdots \\ & \vdots & \\ \cdots & \rho_\omega^{n-1}(a) & \cdots \end{bmatrix}_{nxn} \quad \Longrightarrow a = ???$$

The problem of finding a concrete generator for the dual code of polycyclic codes over rings will be solved in Chapter 4 and a more concrete generalization of the duality theorems for multi-twisted and multi polycyclic codes will be covered in Chapter 5. Here we will give our method for polycyclic codes over finite fields which will provide a slight introduction to those more complex applications.

3.2 Shortening and Puncturing on Linear Codes

Shortening procedure is exactly as follows: Let C' be an $[n, k', d']$-linear code over F_q. For a fixed $1 \leq i \leq n$, form the subset A of C' consisting of the codewords with the i^{th} position equal to 0. Delete the i^{th} position from all the words in A to form a code C. Then C is an $[n-1, k, d]$-linear code over F_q with $k'-1 \leq k \leq k'$, $d \geq d'$ [1].

A polycyclic code with generating polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}$ can be obtained by shortening a cyclic code C' generated by $g(x)$.

On the other hand, puncturing procedure is as follows: Let C' be an $[n+r, k, d+r]$-linear code over F_q. Choose a codeword in C' with weight $d+r$. Choose its r non-zero coordinates, and delete these coordinates from all the codewords of C'. Then the new code C, is an $[n, k, d]$-linear code over F_q [1].

The dual code of a polycyclic code with generating polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}$ can be obtained by puncturing the dual code of a cyclic code C' generated by $g(x)$.

3.3 From Shortening and Puncturing to Polycyclic Codes and Their Duals

Following the intuitions we get from the above correspondences, we derived a formula to obtain a generating vector for the dual codes of polycyclic codes. We used the cyclic code generated by $g(x)$ as a divisor of $x^N - 1$ where N is the smallest length for which $f(x)$ divides $x^N - 1$. The proof will be given in the noncommutative case.

Theorem 3.1. *Let $h(x)g(x) = f(x)$, $\deg(fx) = n$, $\deg(g(x)) = n-k$ and let N be smallest number for which $f(x)$ divides $x^N - 1$. Let $p(x) = \frac{x^N-1}{f(x)} = \sum_{i=0}^{N-n} p_i x^i$ and let C be the polycyclic code generated by $g(x)$ of length n. Then the dual code $C^{\perp}$ is generated by the vector $a = (a_0, a_1, \ldots, a_{n-1})$ and its $n-k-1$ sequential shifts, where*

$$a_0 = p_0 h_0, a_i = \sum_{j=0}^{i-1} p_{N-n-j} h_{n-i+j},\ 1 \leq i \leq n-1.$$

We will give the proof in Chapter 4 for polycyclic codes over skew polynomial rings, which will trivially hold for commutative case. The following small example illustrates the theorem.

Example 3.1. *Let F be the finite field with 4 elements; $F_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$. Let $g(x) = \alpha^2 + \alpha x^2 + x^3, h(x) = 1 + \alpha x + x^2$ and $f(x) = g(x)h(x) = x^5 + \alpha x^3 + x^2 + x + \alpha^2$.*

Let $T_{f(x)}$ be the companion matrix of $f(x)$.

Consider the polycyclic code C generated by $g(x)$ over F_4.

We obtain the generating matrix of C as follows;

$$G = \begin{bmatrix} \cdots & g & \cdots \\ \cdots & g \cdot T_{f(x)} & \cdots \end{bmatrix}_{2x5} = \begin{bmatrix} \alpha^2 & 0 & \alpha & 1 & 0 \\ 0 & \alpha^2 & 0 & \alpha & 1 \end{bmatrix}_{2x5}$$

We have $f(x)|x^{15}-1$ and we set $N = 15$.

In this case we have

$$p(x) = \frac{x^N - 1}{f(x)} = \alpha + \alpha^2 x + \alpha x^2 + \alpha^2 x^3 + \alpha^2 x^5 + \alpha x^6 + x^7 + \alpha x^8 + x^{10}.$$

Using the above formula

$$a_0 = p_0 h_0,\ a_i = \sum_{j=0}^{i-1} p_{N-n-j} h_{n-i+j},$$

we get

$$a = (\alpha, 0, 0, 1, \alpha)$$

So the parity check matrix H can be obtained as follows

$$H = \begin{bmatrix} \cdots & a & \cdots \\ \cdots & a \cdot (T_{f(x)}^{-1})^{tr} & \cdots \\ \cdots & a \cdot ((T_{f(x)}^{-1})^{tr})^2 & \cdots \end{bmatrix}_{3x5} = \begin{bmatrix} \alpha & 0 & 0 & 1 & \alpha \\ 0 & \alpha & 0 & 0 & 1 \\ 1 & 0 & \alpha & 0 & 0 \end{bmatrix}_{3x5}.$$

4
Polycyclic Codes over Rings

In this chapter, we will explore polycyclic code constructions over some ring theoretic algebraic structures. We start with quaternary polycyclic codes and then give an example to polycyclic codes over a finite chain ring. We examine polycyclic codes over skew polynomial rings and introduce duality theorems for both constacyclic and polycyclic codes over skew polynomial rings.

4.1 Quaternary Polycyclic Codes

4.1.1 Codes over $\mathbb{Z}_4$

The reader may refer to [25] for the preliminary facts given below and more on quaternary codes.

A linear code C of length n over $\mathbb{Z}_4$ is a submodule of $\mathbb{Z}_4^n$, and its generator matrix in standard form is given as

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{bmatrix} \tag{4.1}$$

where A and D are matrices with entries from $\{0,1\} \subset \mathbb{Z}_4$, B is a matrix with entries from $\mathbb{Z}_4$ and I denotes the identity matrix. In this form, C is called a type $4^{k_1}2^{k_2}$ quaternary code with size $4^{k_1}2^{k_2}$. If $k_2 = 0$, then C is called a *free* $\mathbb{Z}_4$*-code*.

The Lee weights of $0, 1, 2, 3 \in \mathbb{Z}_4$, denoted by $w_L(0), w_L(1), w_L(2), w_L(3)$ respectively, are defined as $w_L(0) = 0, w_L(1) = 1, w_L(2) = 2$ and $w_L(3) = 1$. The Lee weight of a codeword in a $\mathbb{Z}_4$-code is the sum of Lee weights of its coordinates.

The Gray map ϕ, defined below, is used to obtain $\mathbb{Z}_2$-codes from $\mathbb{Z}_4$-codes. Since it is a weight preserving map, the minimum Lee weight of a linear $\mathbb{Z}_4$-code is the minimum Hamming weight of its Gray image, which is a length $2n$, usually nonlinear, $\mathbb{Z}_2$-code.

$$\begin{array}{rccc} \phi: & \mathbb{Z}_4^n & \longrightarrow & \mathbb{Z}_2^{2n} \\ & 0 & \longmapsto & 00 \\ & 1 & \longmapsto & 01 \\ & 2 & \longmapsto & 11 \\ & 3 & \longmapsto & 10 \end{array}$$

Cyclic codes over $\mathbb{Z}_4$ correspond to ideals in $\mathbb{Z}_4[x]/(x^n-1)$. In order to have principal ideals, we should have odd n, so that we can factorize x^n-1 into distinct, pairwise coprime, basic irreducible factors uniquely.

Lemma 4.1. *If $g(x)$ is a basic irreducible factor of x^n-1, the linear code C over $\mathbb{Z}_4$ generated by $g(x)$ is a free $\mathbb{Z}_4$-code of type $4^{n-\deg g(x)}$.*

Theorem 4.2. *Let n be an odd integer and C be a linear cyclic code over $\mathbb{Z}_4$ of length n. Then $C=(g_1(x)g_2(x), 2g_1(x)g_3(x))$, where $g_1(x), g_2(x), g_3(x)$ are unique monic polynomials such that $g_1(x)g_2(x)g_3(x)=x^n-1$. In this case, $|C|=4^{\deg g_3(x)}2^{\deg g_2(x)}$.*

Since we have odd n, $\mathbb{Z}_4[x]/(x^n-1)$ is a principal ideal ring so C can be generated principally. Having $g_2(x)$ and $g_3(x)$ coprime, we can write $C=(g_1(x)g_2(x), 2g_1(x))$ so that C corresponds to the principal ideal generated by $g_1(x)g_2(x)+2g_1(x)$ [25].

Theorem 4.3. *The dual code of C is also a linear cyclic $\mathbb{Z}_4$-code, and $C^\perp = (g_3^R(x)g_2^R(x), 2g_3^R(x)g_1^R(x))$ with $|C^\perp|=4^{\deg g_1(x)}2^{\deg g_3(x)}$, where C is as defined above and $g_i^R(x)$ are reciprocal polynomials of $g_i(x)$, for $i=1,2,3$ respectively.*

Similar to C, $C^\perp$ can also be generated principally by $g_3^R(x)g_2^R(x)+2g_3^R(x)$.

Let $C=(g(x)=g_1(x)g_2(x)+2g_1(x))$ be a cyclic quaternary code. Keeping the generator matrix as in the form of (2.2), we can obtain G by evaluating $g(T_{x^n-1})$ and similarly H can be obtained from evaluating $g_3^R(x)g_2^R(x)+2g_3^R(x)$ with $(T_{x^n-1}^{-1})^{tr}$.

4.1.2 Polycyclic Codes over $\mathbb{Z}_4$

In order to obtain polycyclic codes over $\mathbb{Z}_4$, we assume that the polynomial $f(x)=x^n-v(x)$ is a square free, monic, regular polynomial with $\deg v(x)<n$.

So let $f(x)=x^n-v(x)=f_1.f_2.....f_t$ be the factorization of $f(x)$ over $\mathbb{Z}_4$ into pairwise coprime, monic, basic irreducible factors. The polycyclic code generated by $g(x)=$

$f_{i_1}.f_{i_2}.....f_{i_r} = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}, 1 \leq i_j \leq t$ has a generator matrix

$$G = \begin{bmatrix} g_0 & \cdots & g_{n-1} \\ - & gT_{f(x)} & - \\ - & gT^2_{f(x)} & - \\ & \vdots & \\ - & gT^{n-1}_{f(x)} & - \end{bmatrix}_{nxn}. \tag{4.2}$$

Let $C = (g_1(x)g_2(x), 2g_1(x)g_3(x))$ where $g_1(x), g_2(x), g_3(x)$ are unique monic polynomials such that $g_1(x)g_2(x)g_3(x) = x^n - v(x)$. In this case, since $g_2(x)$ and $g_3(x)$ are coprime, we can write $C = (g_1(x)g_2(x), 2g_1(x))$ so that C corresponds to the principal ideal generated by $g_1(x)g_2(x) + 2g_1(x)$. Therefore we obtain the generator matrix for C by evaluating $(g_1(x)g_2(x) + 2g_1(x))(T_{f(x)})$.

For the dual code on the other hand, a generator matrix can be obtained by substituting $(T^{-1}_{f(x)})^{tr}$ in $g^R_3(x)g^R_2(x) + 2g^R_3(x)$. The following example illustrates the construction of a polycyclic quaternary code.

Example 4.1. *Consider the quotient polynomial ring $\mathbb{Z}_4[x]/(f(x))$, where $f(x) = x^{15} + x^{11} + x^{10} + x^8 + x^5 + x^4 + x^2 + 1$.*

$f(x)$ has a unique factorization over $\mathbb{Z}_4[x]$ into basic irreducible polynomials as follows:

$$\begin{aligned} f(x) &= x^{15} + x^{11} + x^{10} + x^8 + x^5 + x^4 + x^2 + 1 \\ &= g_1(x)g_2(x)g_3(x), \\ g_1(x) &= x^2 + x + 3, \\ g_2(x) &= x^{12} + 2x^{10} + 3x^9 + x^8 + x^7 + 3x^6 + 2x^5 + x^4 + x^3 + x^2 + 2x + 1, \\ g_3(x) &= x + 3. \end{aligned}$$

Consider the linear $\mathbb{Z}_4$-code $C = (g_1(x)g_2(x), 2g_1(x)g_3(x))$. The generator matrix of C when turned into standard form is

$$\begin{aligned} G &= [g_1(x)g_2(x) + 2g_1(x)](T_{f(x)}) \\ &= \begin{bmatrix} 1 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 3 & 3 & 0 & 1 & 3 & 3 & 1 \\ 0 & 2 & 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 2 \end{bmatrix}. \end{aligned}$$

C is a length 15, type $4^1 2^2$ polycyclic linear code over $\mathbb{Z}_4$ which has minimum Lee weight 15, while the largest minimum Lee weight of the existing constructed linear $\mathbb{Z}_4$-codes of length 15 and size ≥ 16 is 14.

This code has a linear Gray image which corresponds to the near-optimal binary code $[30, 4, 15]$.

There are many examples of good linear polycyclic quaternary codes which do not have a construction introduced in the database [26]. Table 4.1 gives a few examples of polycyclic quaternary codes which are constructed using the software Magma [27] and have at least twice the size of the existing linear codes with the same length and same Lee weight in the database. g stands for the generating polynomial of the corresponding v-polycyclic linear quaternary code. A polynomial of the form $1 + x + x^3 + 2x^4$ is represented with 1^2012 for simplicity.

Table 4.1 Some good polycyclic quaternary codes

v	g	Polycyclic Code	Size	Best Around	Size
$3^3 03^3 030^6$	$3^2 210^2 301^2 0^5$	$[15, 4^6 2^1, 8]$	8192	$[15, 4^6 2^0, 8]$	4096
$3030^3 30^2 30^6$	$3131^3 0321^2 01^2 0^2$	$[16, 4^3 2^1, 12]$	128	$[16, 4^3 2^0, 12]$	64
$3^2 03^2 0^2 3^2 0^2 30^5$	$1031010^2 2^2 310^5$	$[17, 4^6 2^1, 10]$	8192	$[17, 4^6 2^0, 10]$	4096
$30^2 3^5 030^2 3^2 0^4$	$12023030^2 123210^4$	$[18, 4^5 2^1, 12]$	2048	$[18, 4^5 2^0, 12]$	1024
$3^2 0^3 30^2 3^2 030^2 30^4$	$303^2 0^4 10101^3 01^2 0$	$[19, 4^2 2^1, 18]$	32	$[19, 4^2 2^0, 18]$	16
$3^2 0^6 30^{11}$	$10^2 23^4 10321^2 2010^3$	$[20, 4^4 2^1, 14]$	512	$[20, 4^4 2^0, 14]$	256
$3^4 0^9 30^2 30^3$	$301^3 03021^2 30^2 3^2 210^2$	$[20, 4^3 2^4, 14]$	1024	$[20, 4^4 2^0, 14]$	256
$303^2 0^3 3^3 0^3 303^2 0^3$	$1^2 0^2 210^3 2^2 3^2 010^5$	$[20, 4^6 2^1, 12]$	8192	$[20, 4^6 2^0, 12]$	4096
$30^2 30^4 3^3 0^{10}$	$31212^3 0232301^2 210^4$	$[21, 4^5 2^1, 14]$	2048	$[21, 4^5 2^0, 14]$	1024
$303030^2 3^2 030^4 30^5$	$1^2 0^2 210^3 2^2 3^2 010^5$	$[21, 4^8 2^1, 12]$	131072	$[21, 4^8 2^0, 12]$	65536
$30^3 3^4 0^2 303^3 0^7$	$30^2 313^2 030^2 2^2 10210^5$	$[22, 4^6 2^1, 14]$	8192	$[22, 4^5 2^0, 14]$	1024
$3^2 0^2 303^3 0^2 30^{12}$	3030132320213213010^6	$[24, 4^7 2^1, 14]$	32768	$[24, 4^5 2^0, 14]$	1024
$3^3 030^3 303^2 0^{13}$	$32120^3 1^4 231230^2 310^5$	$[25, 4^6 2^3, 14]$	32768	$[25, 4^5 2^0, 14]$	1024
$30^5 30^5 30^{12}$	$132020^2 210101^3 0210^7$	$[25, 4^8 2^1, 14]$	131072	$[25, 4^5 2^0, 14]$	1024
$3^4 0^4 3^2 0^{16}$	$10^2 203^2 01^3 0^2 212121^2 010^4$	$[26, 4^5 2^2, 16]$	4096	$[26, 4^5 2^0, 16]$	1024
$3^3 03^2 0^3 3^2 0^{15}$	$3031^3 3^2 2^3 310^2 13121^2 0^5$	$[26, 4^6 2^1, 16]$	8192	$[26, 4^5 2^0, 16]$	1024
$30^4 3^2 0^2 3^2 0^2 303030^8$	$1^2 232^2 012^2 1203231023^2 10^4$	$[26, 4^5 2^4, 16]$	16384	$[26, 4^5 2^0, 16]$	1024
$3^2 03^2 0^3 30^3 303^3 0^9$	$1313230131^3 31^4 0^2 10^6$	$[26, 4^7 2^1, 16]$	32768	$[26, 4^5 2^0, 16]$	1024
$3^3 0^3 30^{20}$	$31^2 2012^2 131213^2 2301010^6$	$[27, 4^7 2^5, 11]$	524288	$[27, 4^8 2^0, 11]$	65536
$30^2 3^5 0^{19}$	$31^2 230^2 120^2 32121^2 21^2 0^7$	$[27, 4^8 2^4, 11]$	1048576	$[27, 4^8 2^0, 11]$	65536
$3^5 03^2 030^{17}$	$323^2 02^2 0303212^2 0^2 10^9$	$[27, 4^{10} 2^2, 11]$	4194304	$[27, 4^8 2^0, 11]$	65536
$3^3 0^{25}$	$1321203^2 10313^2 2^3 3210^8$	$[28, 4^9 2^1, 14]$	524288	$[28, 4^7 2^0, 13]$	16384
$3^3 0^3 30^{21}$	$13023^2 01^2 20212^2 102^2 03^2 10^5$	$[28, 4^6 2^3, 16]$	32768	$[28, 4^6 2^0, 15]$	4096
$3^2 0^2 303^2 0^2 3^3 0^{15}$	$30101310^2 1^3 01^2 01^2 210^8$	$[28, 4^9 2^2, 16]$	1048576	$[28, 4^7 2^0, 13]$	16384
$30^2 30^{25}$	$3121^2 23^2 02130131302^2 10^8$	$[29, 4^9 2^3, 13]$	2097152	$[29, 4^8 2^0, 13]$	65536

4.2 Polycyclic Codes over Finite Chain Rings

While linear codes were initially studied over finite fields, starting with quaternary codes, more general structures have been taken into consideration. For the detailed progress in research we refer the reader to [6].

In order to examine polycyclic codes over finite chain rings, we first give some basic preliminaries about these rings from [28].

An associative finite ring with unity is called a *chain ring* if its ideals are linearly ordered under inclusion. Finite chain rings are principal ideal rings; every ideal of these rings is generated by a single element. They are also *local rings*; they have unique maximal ideals. For a finite chain ring R, let M be the unique maximal ideal with generator γ. Then the ideals of R satisfy a chain of the following form where a is called the *nilpotency index* of γ.

$$R = (\gamma^0) \supsetneq M = (\gamma^1) \supsetneq (\gamma^2) \supsetneq (\gamma^3) \supsetneq \cdots \supsetneq (\gamma^a) = (0)$$

While constructing linear codes over finite chain rings, we are going to be dealing with factorization of polynomials and we also need a Euclidean type algorithm, therefore we make use of the following definitions and theorems.

Definition 4.1. Let $K = R/M$ be the residue field of R. A polynomial f in $R[x]$ is called *basic irreducible* if its image μf under the natural projection $\mu : R[x] \longrightarrow K[x]$, is irreducible over $K[x]$.

Definition 4.2. A *primary* polynomial is a polynomial which generates a primary ideal; an ideal $I \neq R$, for which $xy \in I$ implies $x \in I$ or $y^n \in I$ for some $n \in \mathbb{Z}^+$.

Definition 4.3. A polynomial f in $R[x]$ is called *regular*, if it is not a zero divisor.

We have the following equivalent conditions for regular polynomials.

Theorem 4.4 ([28])**.** *Let $f = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial in $R[x]$. Then the following are equivalent:*

(i) *f is regular,*

(ii) *The ideal $(a_0, a_1, \cdots, a_n) = R$,*

(iii) *a_i is a unit in R for some i, $0 \leq i \leq n$,*

(iv) *$\mu f \neq 0$.*

Theorem 4.5 (Hensel's Lemma, [28]). *Let f be a polynomial in $R[x]$ and $\mu f = \overline{g_1} \cdots \overline{g_n}$ be the factorization of μf over K into pairwise coprime polynomials $\overline{g_1}, \ldots, \overline{g_n}$. Then there exist polynomials $g_1, \ldots, g_n$ in $R[x]$ such that*

(i) $g_1, \ldots, g_n$ *are pairwise coprime,*

(ii) $\mu g_i = \overline{g_i}$, *for all* i, $0 \leq i \leq n$,

(iii) $f = g_1 \cdots g_n$.

It is also shown in terms of irreducibilty that for a regular polynomial f, if μf is irreducible in $K[x]$ then f is irreducible in $R[x]$. Moreover, if μf has distinct zeros in the algebraic closure of K, then f is irreducible if and only if μf is irreducible. So, we have the following factorization theorem for regular polynomials over R.

Theorem 4.6 ([28]). *Let f be a regular polynomial in $R[x]$. Then, $f = \delta g_1 \cdots g_n$ where δ is a unit and $g_1, \ldots, g_n$ are pairwise coprime regular primary polynomials. If $f = \beta h_1 \cdots h_m$ is another factorization of f where β is a unit and $h_1, \ldots, h_m$ are pairwise coprime regular primary polynomials, then $m = n$ and $g_i = h_i$ up to reordering.*

It is also a consequence of the given facts for a square-free monic regular polynomial f that, this factorization into pairwise coprime monic basic irreducible factors is unique up to associates and reordering.

A Euclidean type algorithm also holds as follows:

Theorem 4.7. *Let f and g be polynomials in $R[x]$ such that g is regular. Then, there exist polynomials $q, r \in R[x]$ with $f = qg + r$ and* $\deg(r) < \deg(g)$.

4.2.1 Polycyclic Codes as Invariant Submodules over Finite Chain Rings

In this part, we are going to examine polycyclic codes as invariant submodules of a finite chain ring R. The idea was sparkled by the work [23], where new codes were found by constructing arbitrary vector circulant matrices. This kind of matrices generate some invariant submodules which we classify below. The notion of invariant subspaces were introduced in [18] for cyclic and constacyclic cases, and generalized for the cyclic codes over finite chain rings in [19].

Let f be a square-free, monic regular polynomial in $R[x]$, where R is a finite chain ring. As a consequence of the above facts, we have a unique factorization of f into pairwise coprime, monic, basic irreducible polynomial factors over R. Let $f(x) = x^n - v(x) =$

$f_1.f_2.....f_t$ be the factorization. Each factor creates an invariant submodule over R. We may apply the same method as in [18, 19] in order to construct polycyclic codes over finite chain rings.

The following example illustrates the construction of a polycyclic code over a finite chain ring. We note that, a generator matrix for a linear code over Galois rings of type $GR(p^l, m)$ can be written in the following standard form where the blocks $A_i, B_j, ..., D$ have entries from $GR(p^l, m)$, and $I'_{k_i}s$ are identity matrices of size k_i.

$$G = \begin{bmatrix} I_{k_1} & A_1 & \cdots & \cdots & \cdots & A_l \\ 0 & pI_{k_2} & pB_1 & \cdots & \cdots & pB_{l-1} \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & p^{l-1}I_{k_l} & p^{l-1}D \end{bmatrix} \tag{4.3}$$

Example 4.2. *Let $R = GR(2^2, 3)$ be the Galois ring obtained from the quotient ring $\mathbb{Z}_4[x]/(p(x))$ where $p(x)$ is a basic irreducible polynomial of degree 3 with ξ as a primitive root. And let $f(x) = x^7 + 3x^6 + x^4 + 3x^3 + x + 3$. So we have $v(x) = x^6 + 3x^4 + x^3 + 3x + 1$ and hence $v = (1, 3, 0, 1, 3, 0, 1)$ and further $f(x)$ has a unique factorization into basic irreducible polynomials g_1, g_2, g_3, g_4 over R as*

$$\begin{aligned} f(x) &= g_1(x)g_2(x)g_3(x)g_4(x) \\ g_1(x) &= (x+3), \\ g_2(x) &= (x^2 + 3\xi x + 1), \\ g_3(x) &= (x^2 + (3\xi^2 + 2)x + 1), \\ g_4(x) &= (x^2 + (\xi^2 + \xi + 1)x + 1) \end{aligned}$$

and we have

$$T_{f(x)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 3 & 0 & 1 & 3 & 0 & 1 \end{bmatrix}.$$

Let C be the polycyclic code generated by $g_3(x)g_4(x), 2g_3(x)$. We obtain a generator matrix by evaluating $[g_3g_4 + 2g_3](T_{f(x)})$. In standard form we get

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & \xi+1 & \xi^2+1 & 2\xi^2+\xi \\ 0 & 0 & 1 & \xi & \xi^2+1 & 2\xi^2+\xi & 3 \\ 0 & 0 & 0 & 2 & 0 & 2\xi^2+2\xi+2 & 2\xi^2 \\ 0 & 0 & 0 & 0 & 2 & 2\xi^2 & 2 \end{bmatrix}$$

and C is a $(7, 4^9 2^6)$ linear code over R.

4.3 Polycyclic Codes over Skew Polynomial Rings

Skew polynomial rings were introduced by Ore in [29] and studied further by Jacobson [30] and McDonald [28]. For the last two decades, research on linear codes has been shifted to cyclic codes over noncommutative rings, known as skew cyclic codes intensively [12]. These are larger than the commutative ones and surely contain them as subfamilies. The pace for exploring these families has not been as in the commutative case. The problems due to the skewness property are more challenging.

Definition 4.4. Let F_q be a finite field of order q and θ be an automorphism of F_q. The set of polynomials

$$F_q[x;\theta] = \{a_0 + a_1 x + \cdots + a_n x^n | a_i \in F_q,\, n \in \mathbb{N}\}$$

is called skew polynomial ring over F_q, where addition is ordinary but multiplication is defined for all $a, b \in F_q$ as

$$\left(ax^i\right) * \left(bx^j\right) = a\theta^i(b)x^{i+j}.$$

Skew polynomial rings are noncommutative unless θ is the identity automorphism. $F_q[x;\theta]$ is left and right Euclidean, i.e. both right and left division algorithms hold and any left or right ideal is principal. Factorization is not unique in $F_q[x;\theta]$. Let $f(x)$ be a polynomial in $F_q[x;\theta]$. If $f(x)p(x) = p(x)f(x)$ for all $p(x) \in F_q[x;\theta]$, then $f(x)$ is called a central polynomial. The set of central polynomials of $F_q[x;\theta]$ is called the center of $F_q[x;\theta]$ and denoted by $\mathscr{Z}(F_q[x;\theta])$. Further, $f(x)$ is a central polynomial if and only if it is of the form

$$f(x) = a_0 + a_1 x^m + a_2 x^{2m} + \cdots + a_n x^{nm} \tag{4.4}$$

where $a_i \in F_q^\theta$ (the fixed field of θ in F_q) and $m = |\langle\theta\rangle|$ is the order of θ [28].

We write $g(x)|_r f(x)$, if $g(x)$ is a right divisor of $f(x)$. The following lemma shows that two factors of a central polynomial commute [31].

Lemma 4.8. *Let $f(x) = h(x)g(x)$ in $F_q[x;\theta]$. If $f(x) \in \mathscr{Z}(F_q[x;\theta])$, then $h(x)g(x) = g(x)h(x)$.*

4.3.1 Skew Cyclic and Skew Constacyclic Codes

In [12], Boucher et al. generalized cyclic codes by using skew polynomial rings.

Definition 4.5. A linear code C of length n over F_q is called *skew cyclic*, if it is invariant

under the skew cyclic shift, i.e.

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

Boucher et al. show that skew cyclic codes are ideals of the ring $F_q[x;\theta]/(x^n-1)$, whenever $x^n-1 \in \mathscr{Z}(F_q[x;\theta])$ [12]. Later, the restriction on x^n-1 to be a central polynomial is removed by considering skew cyclic codes as left $F_q[x;\theta]$-submodules of $F_q[x;\theta]/(x^n-1)$ in [32]. Skew cyclic codes, being a generalization of cyclic codes and covering a large and rich subclass of linear codes, present many advantages while searching for linear codes with structures and in some cases good parameters. In many recent studies such as [12, 33], new record breaking codes were obtained via using skew polynomials.

The following preliminary result can be derived directly from Theorem 6, 7 and Lemma 2 of [32] by using similar methods, hence the proof is omitted.

Lemma 4.9. *Let C be a left $F_q[x;\theta]$-submodule of $F_q[x;\theta]/(f(x))$ where $f(x) \neq 0$ and $deg(f(x)) > 0$. Let $g(x)$ be a monic polynomial of minimum degree in C. Then $g(x)$ is unique and C is principally generated by $g(x)$, i.e, $C = (g(x))$. Moreover, $g(x)$ is a right divisor of $f(x)$ in $F_q[x;\theta]$ and $|C| = q^{deg(f(x))-deg(g(x))}$.*

Now we give the definition for a skew α-constacyclic code.

Definition 4.6. Let $\alpha \in F_q^*$. A linear code C is called *skew α—constacyclic* if it is invariant under skew α-constacyclic shift, i.e,

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (\alpha\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

Skew constacyclic codes were introduced in [7] and some properties of this family are given in [34] and [8]. In polynomial representation, skew α-constacyclic codes correspond to left $F_q[x;\theta]$-submodules of $F_q[x;\theta]/(x^n-\alpha)$. ioIn fact, a skew α-constacyclic code C of length n is principally generated by a right divisor $g(x)$ of $x^n-\alpha$ in $F_q[x;\theta]$, i.e. $C = (g(x))$.

4.3.2 Duality Theorem for Skew Constacyclic Codes

In this section, given the generator of a skew constacyclic code, we introduce a direct method of finding the generator of the dual code explicitly. Throughout this section we set $m|n$, where $m = |\langle\theta\rangle|$.

Lemma 4.10. *Let $x^n - \alpha \in F_q[x;\theta]$, $o(\alpha)$ be the multiplicative order of α in F_q^* and $N = o(\alpha)n$. Then, $x^n - \alpha$ is a right divisor of the central polynomial $x^N - 1$ in $F_q[x;\theta]$.*

Proof. Let $N = o(\alpha)n$. Then,

$$x^N - 1 = (\alpha^{-1} + \alpha^{-2}x^n + \alpha^{-3}x^{2n} + \cdots + \alpha^{-o(\alpha)}x^{(o(\alpha)-1)n})(x^n - \alpha).$$

■

Since $m|n$, we have $x^N - 1 \in \mathscr{Z}(F_q[x;\theta])$ and from Lemma 4.8, $x^N - 1 = (x^n - \alpha)(\alpha^{-1} + \alpha^{-2}x^n + \alpha^{-3}x^{2n} + \cdots + \alpha^{-o(\alpha)}x^{(o(\alpha)-1)n})$. We simply use the expression $\frac{x^N-1}{x^n-\alpha}$ for the right division of $x^N - 1$ by $x^n - \alpha$.

Lemma 4.11. *Let $\alpha_i \in F_q^*$ and n_i be a positive integer such that $m|n_i$, for $1 \leq i \leq l$. Then,*

$$x^{n_i} - \alpha_i |_r x^N - 1$$

where $N = lcm(n_1, n_2, \ldots, n_l)lcm(o(\alpha_1), \ldots, o(\alpha_l))$.

Proof. By Lemma 4.10, we have

$$(\alpha_i^{-1} + \alpha_i^{-2}x^{n_i} + \alpha_i^{-3}x^{2n_i} + \cdots + \alpha_i^{-o(\alpha_i)}x^{(o(\alpha_i)-1)n_i})(x^{n_i} - \alpha_i) = x^{n_i o(\alpha_i)} - 1$$

and we also have

$$o(\alpha_i)n_i | lcm(n_1, n_2, \ldots, n_l)lcm(o(\alpha_1), \ldots, o(\alpha_l)).$$

Hence,

$$x^{n_i o(\alpha_i)} - 1 |_r x^N - 1.$$

Therefore $x^{n_i} - \alpha_i |_r x^N - 1$. ■

In [8], Lemma 3.1 shows that the dual of a skew α-constacyclic code is a skew α^{-1}-constacyclic code, with a restriction on α being fixed by θ. This lemma holds for any $\alpha \in F_q^*$, and can be proved by using the same method.

Lemma 4.12 ([8], Lemma 3.1)**.** *Let C be a skew α-constacyclic code of length n over F_q, where $\alpha \in F_q^*$. Then the dual code $C^\perp$ is a skew α^{-1}-constacyclic code of length n over F_q.*

In order to determine the generator polynomials of dual codes, the following definition will be crucial.

Definition 4.7. Let n be a positive integer and $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in F_q[x;\theta]$ with $\deg(a(x)) \leq n-1$. We define

$$a^{\langle n,\alpha\rangle}(x) = \alpha^{-1}a_0 + \theta(a_{n-1})x + \theta^2(a_{n-2})x^2 + \cdots + \theta^{n-1}(a_1)x^{n-1}.$$

Let $x^n - \alpha = a(x)g(x)$ with $deg(a(x)) = k$ and $C = (g(x))$. If we were dealing with the case $\alpha = 1$, i.e, skew cyclic case, skew reciprocal polynomial of $a(x)$, which is defined as $a^R(x) = a_k + \theta(a_{k-1})x + \cdots + \theta^k(a_0)x^k$, would be a right divisor of $x^n - 1$ and thus a generator polynomial for $C^\perp$ [31]. However, for the skew constacyclic case, $x^n - \alpha = a(x)g(x)$ does not imply $a^R(x)|_r x^n - \alpha^{-1}$ nor does it imply $C^\perp = (a^R(x))$. In [24] the authors determined that $C^\perp = (h^R(x))$ where $h(x)$ is a polynomial satisfying $x^n - \theta^{-k}(\alpha) = g(x)h(x)$, this guarantees the existence but is implicit and the process involves a query to find such a polynomial $h(x)$. Later in [34] in Theorem 6.1, authors obtained the generator of the dual code in terms of $h(x)$, while $x^n - \alpha = h(x)g(x)$, by using the properties of skew generalized circulant matrices.

In the following theorem, we give an alternative algorithm to find the generator polynomial of $C^\perp$ directly by using $a^{\langle n,\alpha\rangle}(x)$.

Theorem 4.13. *Let $x^n - \alpha = a(x)g(x)$ in $F_q[x;\theta]$ and C be a skew α-constacyclic code generated by $g(x)$. Then, $a^{\langle n,\alpha\rangle} \in C^\perp$. Moreover, $C^\perp = (x^k a^{\langle n,\alpha\rangle}(x))$, where $k = deg(a(x))$.*

Proof. Let $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$ and $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. Let us multiply both sides of $x^n - \alpha = a(x)g(x)$ from left by $\frac{x^N-1}{x^n-\alpha}$, where $N = o(\alpha)n$. We obtain

$$x^N - 1 = \frac{x^N - 1}{x^n - \alpha}a(x)g(x).$$

Since $x^N - 1 \in \mathscr{Z}(F_q[x;\theta])$, from Lemma 4.8 we can write $x^N - 1 = g(x)\frac{x^N-1}{x^n-\alpha}a(x)$, which means

$$g(x)(\alpha^{-1} + \alpha^{-2}x^n + \alpha^{-3}x^{2n} + \cdots + \alpha^{-o(\alpha)}x^{(o(\alpha)-1)n})a(x) = 0 \pmod{x^N - 1}.$$

This is equivalent to

$$g(x)\alpha^{-1}a(x) + g(x)\alpha^{-2}a(x)x^n + \cdots + g(x)a(x)x^{(o(\alpha)-1)n} = 0 \pmod{x^N - 1} \quad (4.5)$$

since $\alpha^{-o(\alpha)} = 1$ and $x^n \in \mathscr{Z}(F_q[x;\theta])$.

The coefficient of x^0 in Equation (4.5) is $g_0\alpha^{-1}a_0 + g_1\theta(a_{n-1}) + g_2\theta^2(a_{n-2}) + \cdots + g_{n-1}\theta^{n-1}(a_1) = 0$ which implies $g \cdot a^{\langle n,\alpha\rangle} = 0$. To prove $a^{\langle n,\alpha\rangle} \in C^\perp$, we need to show

that $a^{\langle n,\alpha\rangle}$ is orthogonal to all skew α-constacyclic shifts of g. Let us denote the skew α-constacyclic shift by T_α. If we multiply Equation (4.5) with x from left, then the coefficient of x^0 becomes

$$\theta(g_{n-1})a_0 + \theta(g_0)\theta(a_{n-1}) + \theta(g_1)\theta^2(a_{n-2}) + \cdots + \theta(g_{n-2})\theta^{n-1}(a_1) = 0.$$

This implies that $T_\alpha(g) \cdot a^{\langle n,\alpha\rangle} = 0$. Similarly, if we multiply Equation (4.5) with x^i from left, we obtain $T^i_\alpha(g) \cdot a^{\langle n,\alpha\rangle} = 0$. Thus, we have $a^{\langle n,\alpha\rangle} \in C^\perp$.

Now let us show that $C^\perp = (x^k a^{\langle n,\alpha\rangle}(x))$. Since $C^\perp$ is a skew α^{-1}-constacyclic code, it is a left $F_q[x;\theta]$-submodule of $F_q[x;\theta]/(x^n - \alpha^{-1})$. Thus $x^i a^{\langle n,\alpha\rangle}(x) \in F_q[x;\theta]/(x^n - \alpha^{-1})$ also belongs to $C^\perp$. We have

$$deg(a(x)) = k \implies deg(x^k a^{\langle n,\alpha\rangle}(x)) = k \text{ in } F_q[x;\theta]/(x^n - \alpha^{-1}).$$

Since the quotient ring is principal and the dimension of $C^\perp$ is $n-k$, there is no polynomial in $C^\perp$ with degree less than k. Therefore $C^\perp$ is indeed generated by $x^k a^{\langle n,\alpha\rangle}(x)$. ■

4.3.3 Skew Polycyclic Codes and Their Duals

Polycyclic codes have been extended to noncommutative case in [15]. It is shown that a skew polycyclic code generated by a right divisor $g(x)$ of $f(x) = x^n - v(x)$ is invariant under $T_{f(x)} \circ \Theta$, where $\Theta(c) := (\theta(c_0), \theta(c_1), \ldots, \theta(c_{n-1}))$. For this case, a v-skew polycyclic shift of a codeword c is obtained by

$$(T_{f(x)} \circ \Theta)(c) = (\theta(c_0), \theta(c_1), \ldots, \theta(c_{n-1})) \cdot T_{f(x)}$$

The following lemma can be directly proved by applying the results in [14, 24] and [15].

Lemma 4.14. *Let C be a skew polycyclic code generated by a right divisor $g(x)$ of $f(x) = x^n - v(x) \in F_q[x,\theta]$. Then, $C^\perp$ is a sequential code and invariant under $(T^{-1}_{f(x)})^{tr} \circ \Theta$.*

In order to obtain the generating vector for the dual code of a skew polycyclic code, we need to start with the following lemma.

Lemma 4.15. *Let $f(x) \in F_q[x;\theta]$ be a polynomial with a nonzero constant term. Then, there exist a central polynomial $x^N - 1$ such that $f(x)|_r x^N - 1$ in $F_q[x;\theta]$.*

Proof. By Lemma 10 in [31], there exists a polynomial $b(x) = (b_0 + b_1 x^m + \cdots +$

$b_s x^{sm})x^t$ where $m = |\langle\theta\rangle|$, $b_i \in F_q^\theta$ and $s, t \in \mathbb{N}$ such that $f(x)|_r b(x)$. Since $f(x)$ has a nonzero constant term, we get $x^t = 1$ and $b(x) \in \mathscr{Z}(F_q[x;\theta])$.

We know that $\mathscr{Z}(F_q[x;\theta]) = F_q^\theta[x^m]$. Also, there exists a finite field extension of F_q^θ where $b(x)$ splits. These imply that there exists a central polynomial $x^N - 1$ such that $b(x)|x^N - 1$ which completes the proof.

■

Let C be a skew polycyclic code generated by $g(x)|_r f(x)$ where $deg(g(x)) = n-k$. Let x^N-1 be a central polynomial such that $f(x)|_r x^N-1$. In this case, C corresponds to the shortened code applied to the last $N-n$ coordinates of the skew cyclic code $C' = (g(x))$ of length N. Further, the dual code of C corresponds to the punctured code applied to the last $N-(n-k)$ coordinates of the dual code $C'^{\perp}$, which is generated by $a'^{\langle N,1\rangle}(x)$ where $a'(x)g(x) = x^N - 1$. The punctured code, being in the form of a sequential code, does not have an ideal or module structure and multiplication by x does not correspond to the sequential shift under which the code is invariant. However, in the sequel, we find a representative generating vector from which a generator matrix for the dual code can be obtained directly.

Theorem 4.16. *Let $a(x)g(x) = f(x) = x^n - v(x)$ with a nonzero constant term and $deg(g(x)) = n-k$. Let N be smallest number for which $f(x)$ divides $x^N - 1$ and $p(x) = \frac{x^N-1}{f(x)} = \sum_{i=0}^{N-n} p_i x^i$. Suppose C is a skew polycyclic code of length n generated by $g(x)$. Then, the dual code $C^\perp$ is generated by the vector $h = (h_0, h_1, \ldots, h_{n-1})$ and its $n-k-1$ sequential shifts i.e., $\{h, ((T_{f(x)}^{-1})^{tr} \circ \Theta)(h), \cdots, ((T_{f(x)}^{-1})^{tr} \circ \Theta)^{n-k-1}(h)\}$, where*

$$h_0 = p_0 a_0, \text{ and } h_i = \sum_{j=0}^{i-1} \theta^i(p_{N-n-j})\theta^{N-n+i-j}(a_{n-i+j}),\ 1 \le i \le n-1.$$

Proof. Since $x^N - 1$ is a central polynomial such that $f(x)|_r x^N - 1$, we have

$$x^N - 1 = g(x)\frac{x^N - 1}{f(x)}a(x).$$

This implies that

$$g(x)(p_0 + p_1 x + \cdots + p_{N-n}x^{N-n})a(x) = 0 \pmod{x^N - 1}. \tag{4.6}$$

Thus, the coefficient of x^0 in Equation (4.6) is

$$\begin{aligned}
&g_0p_0a_0 + g_1\theta(p_{N-n})\theta^{N-n+1}(a_{n-1}) + \\
&g_2(\theta^2(p_{N-n})\theta^{N-n+2}(a_{n-2}) + \theta^2(p_{N-n-1})\theta^{N-n+1}(a_{n-1})) + \cdots + \\
&g_{n-1}(\theta^{n-1}(p_{N-n})\theta^{N-1}(a_1) + \cdots + \theta^{n-1}(p_{N-2n+2})\theta^{N-n+1}(a_{n-1})) = 0
\end{aligned}$$

which implies $g \cdot h = 0$. Multiplying Equation (4.6) by x^i from the left, we obtain $T^i_{f(x)}(g) \cdot h = 0$.

Now, we consider a skew cyclic code C' of length N generated by $g(x)$. From Theorem 4.13, the dual code of C' of dimension $n-k$ is also generated by $a'^{\langle N,1\rangle}(x)$, where $a'(x) = \frac{x^N-1}{g(x)} = p(x)a(x)$. Let H' be the generator matrix for $C'^{\perp}$ obtained from $a'^{\langle N,1\rangle}$. Now, we show that the first n coordinates of $a'^{\langle N,1\rangle}$ form exactly the coordinates of h in the same order. We have

$$\begin{aligned}
a'(x) =& (p_0 + p_1x + \cdots + p_{N-n}x^{N-n})(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \\
=& p_0a_0 + (p_0a_1 + p_1\theta(a_0))x + \cdots + \\
& (p_{N-n}\theta^{N-n}(a_{n-2}) + p_{N-n-1}\theta^{N-n-1}(a_{n-1}))x^{N-2} + (p_{N-n}\theta^{N-n}(a_{n-1}))x^{N-1}.
\end{aligned}$$

This implies that

$$\begin{aligned}
a'^{\langle N,1\rangle}(x) =& p_0a_0 + \theta(p_{N-n}\theta^{N-n}(a_{n-1}))x + \theta^2(p_{N-n}\theta^{N-n}(a_{n-2}) + p_{N-n-1}\theta^{N-n-1}(a_{n-1}))x^2 \\
& + \cdots + \theta^{n-1}(p_0a_1 + p_1\theta(a_0))x^{N-1}.
\end{aligned}$$

Similarly one can show that the first n coordinates of $x^i a'^{\langle N,1\rangle}(x) \pmod{x^N-1}$ i.e. the first n coordinates of the ith row of H', give the coordinates of $((T^{-1}_{f(x)})^{tr} \circ \theta)^i(h)$ in the same order. This completes the proof since puncturing $C'^{\perp}$ at the last $N-n$ coordinates results in exactly $n-k$ linearly independent rows. ■

Example 4.3. *Let $g(x) = x^3 + \alpha x^2 + \alpha^2|_r f(x) = x^5 + x^2 + \alpha^2 x + \alpha^2$ in $F_4[x;\theta]$ with $|\langle\theta\rangle| = 2$. In this case, $a(x) = x^2 + \alpha x + 1$ and $f(x) = a(x)g(x)$. $C = (g(x))$ becomes a skew v-polycyclic code of length 5, where $v = (\alpha^2, \alpha^2, 1, 0, 0)$. We have $N = 24$, i.e. $f(x)|_r x^{24} - 1$ and $p(x) = \frac{x^{24}-1}{f(x)}$. By Theorem 4.16, we get $h = (\alpha, 0, 0, 1, \alpha^2)$ which is exactly the first 5 coordinates of $a'^{\langle 24,1\rangle}$. The parity check matrix for C can be obtained from $\{h, ((T^{-1}_{f(x)})^{tr} \circ \theta)(h), ((T^{-1}_{f(x)})^{tr} \circ \theta)^2(h)\}$ as*

$$H = \begin{bmatrix} \alpha & 0 & 0 & 1 & \alpha^2 \\ 0 & \alpha^2 & 0 & 0 & 1 \\ 1 & 0 & \alpha & 0 & 0 \end{bmatrix}.$$

5
Polycyclicity of Codes over Matrix Spaces

Codes over matrix spaces have been studied in terms of array codes or Gabudilin codes first in [9] with respect to rank metric and term rank metric instead of the usual Hamming metric defined on usual vector spaces. In matrix spaces, matrices correspond to vectors in usual vector spaces. Note that, matrices over the base field F_q are isomorphic to the vector space over the extension field F_{q^n};

$$F_q^{m\times n} \cong F_{q^n}^m \tag{5.1}$$

5.1 Rank Metric and Term Rank Metric Spaces

The vector space of $m \times n$ matrices over a fixed finite field F_q of q elements become a rank metric and term rank metric space under the rank norm and term rank norm respectively, denoted by M_R, M_{TR}. Given A as an $m \times n$ matrix with $\mathscr{I}(A)$ being the set of rows/columns of A which contains all the nonzero entries of A, the term rank norm is defined as

$$\|A\|_{TR} = \min|\mathscr{I}(A)|\,. \tag{5.2}$$

If A and B are two $m \times n$ matrices, the term rank distance is defined as

$$d_{TR} = \|A-B\|_{TR}\,. \tag{5.3}$$

Codes over matrix spaces are considered as k-dimensional subspaces of $F_q^{m\times n}$. The minimum distance of a code over a term rank metric space, denoted by D_{TR}, should clearly be less than or equal to the minimum of $\{m,n\}$ and assuming without the loss of generality that $m \leq n$, we have

$$D_{TR} = \min_{A\in C-\{0\}} \|A\|_{TR} \leq m. \tag{5.4}$$

The only known bound for optimality of codes over M_{TR} is the Singleton bound, which is expressed in the following version.

$$k \leq n(m - D_{TR} + 1). \tag{5.5}$$

If we have the equality, the code is considered to be optimal.

Gritsenko and Maevskiy [10] have introduced a construction method for optimal codes over M_{TR}, using the correspondence between polynomials and $p(x)$-circulants. With this method, they construct $[n \times n, n]-$ codes, and for construction of $[m \times n, n]-$codes, they address the shortening method. In this study, we introduce a direct polycyclic construction, which will guide as an analogue to the usual construction of codes over ordinary vector spaces in general, and with this method, the cyclic and constacyclic cases for codes over matrix spaces will be classified. We also propose a method for finding the minimum term rank distance of a given code using Pyhton software.

5.1.1 Code Construction and Examples

Let $p(x) = a_0 + a_1 x + \cdots + x^m$ be a monic divisor of degree m of a polynomial $f(x) = x^n - 1$ of degree n and consider the following matrix P_p obtained from the companion matrix of $p(x)$ horizontally joined with an $m \times (n-m)$ block zero-matrix

$$P_p = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ -a_0 & -a_1 & \cdots & -a_{m-1} & 0 & \cdots & 0 \end{bmatrix}_{m \times n}. \tag{5.6}$$

We define a *cyclic shift* by vertically shifting the columns of P_p to the right hand side. We can obtain this shift by multiplying P_p with T_f which is the companion matrix of $f(x) = x^n - 1$;

$$T_f = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n \times n}. \tag{5.7}$$

The F_q sub matrix space spanned by n matrices of cyclic shifts of P_p, constructs a form of a cyclic code over M_{TR}, which we call *a cyclic code associated with* $p(x)$.

For the case where $f = x^n - \alpha, (\alpha \in F_q^*)$, T_f constructs an α-constacyclic shift, therefore we obtain an α-constacyclic code. Finally, for the most general case where f is an arbitrary monic polynomial of degree n, we obtain polycyclic shift and polycyclic codes.

We generalize the structure to the polycyclic case as follows

Definition 5.1. Let F_q be a finite field with q elements and let $f(x)$ be a monic polynomial with $p(x)$ a monic divisor of $f(x)$ over $F_q[x]$, with $\deg f(x) = n$ and $\deg p(x) = m$. Let P_p be the matrix obtained from the companion matrix of $p(x)$ horizontally joined with an $m \times (n-m)$ zero-matrix, and T_f be the companion matrix of f. The F_q- sub matrix space spanned by the following set of $m \times n$ matrices

$$\{P_p T_f^i : i \in [0, n-1]\} \tag{5.8}$$

is a polycyclic code in the rank/term rank metric space over $F_q^{m \times n}$.

Considering the correspondence $\overline{\varphi} : F_q[x] \longrightarrow F_q^{mxn}$ which maps x^i to $P_p(T_f)^i$, multiplying a polynomial by x over the polynomial ring $F_q[x]$, corresponds to the polycyclic shift in $F_q^{m \times n}$, as defined above.

Example 5.1. *Let F_q be the finite field with 4 elements; $F_4 = \{0, 1, \alpha, \alpha^2\}$. Consider $f(x) = x^9 - 1$ and take $p(x) = x^3 + \alpha^2$ as a divisor of f. Therefore we have $m = 3$, $n = 9$, and*

$$P_p = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, T_f = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{9 \times 9}.$$

Applying T_f to P_p, constructs the desired cyclic shift;

$$P_pT_f = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$P_pT_f^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\vdots$$

$$P_pT_f^8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 \end{bmatrix}.$$

And the subspace generated by the spanning set $\{P_pT_f^i : i \in [0,8]\}$ becomes a cyclic $[3\times 9, 9]$—code over the F_4—matrix space of 3×9 matrices.

Example 5.2. *Let F_q be the finite field with 4 elements; $F_4 = \{0,1,\alpha,\alpha^2\}$. Consider $f(x) = x^6 + \alpha^2x^2 + \alpha$ and take $p(x) = x^4 + x^2 + \alpha$ as a divisor of f. We have $m = 4$, $n = 6$, and*

$$P_p = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ a & 0 & 1 & 0 & 0 & 0 \end{bmatrix},\ T_f = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ a & 0 & a^2 & 0 & 0 & 0 \end{bmatrix}.$$

Applying T_f to P_p, constructs a polycyclic shift as follows;

$$P_pT_f = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & \alpha & 0 & 1 & 0 & 0 \end{bmatrix}, P_pT_f^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 & 1 & 0 \end{bmatrix},$$

$$P_pT_f^3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \alpha & 0 & \alpha^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 & 1 \end{bmatrix}, P_pT_f^4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ \alpha & 0 & \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \alpha^2 & 0 & 0 \\ \alpha & 0 & \alpha^2 & 0 & \alpha & 0 \end{bmatrix},$$

$$P_pT_f^5 = \begin{bmatrix} \alpha & 0 & \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \alpha^2 & 0 & 0 \\ 0 & 0 & \alpha & 0 & \alpha^2 & 0 \\ 0 & \alpha & 0 & \alpha^2 & 0 & \alpha \end{bmatrix}.$$

And the subspace generated by the spanning set $\{P_pT_f^i : i \in [0,5]\}$ becomes a polycyclic $[4\times 6, 6]$—code over the F_4—matrix space of 4×6 matrices.

5.1.2 Computing Minimum Term Rank Distance

As in the case in general coding theory, computing minimum distance and obtaining optimal codes is an important issue also for codes over term rank metric spaces. In order to compute minimum term rank distance of a code over a matrix space, graph theoretical methods are addressed [10]. It is shown that, the term rank weight of a matrix A is equal to the maximum size of a matching of the bipartite graph for which A is the bi-adjacency matrix [11]. Currently, there was not any in-built function for computing the term rank of a matrix in commonly used computer algebra systems. As an example for codes over F_4—matrix spaces, we used Magma for obtaing a code over a matrix space and created some Python implementations for computing the minimum term rank distance of this code. In this method, we initially retrieve the list L of all entries (we shall denote any non-integer field-specific element by an integer here) of matrices in the code to a text file and call this file from Python to compute the minimum term rank distance.

We create a code over a matrix space with the Magma code given in Appendix A.1.

Having the code constructed, we compute its minimum term rank distance with applying the Python script given in Appendix A.2.

5.1.3 Constructing Optimal Codes

The following theorem is pointing out the conditions for $p(x)$ and $f(x)$ at which the code becomes optimal. For cyclic $[m \times n, n]$ codes the following result is obtained. For the most general cases the optimality question remains open.

Theorem 5.1. *Let F_q be a finite field with q elements and $p(x)$ a divisor polynomial of $f(x) = x^n - 1$ over $F_q[x]$, with $\deg p(x) = m$. Let P_p and T_f be as defined above. The cyclic $[m \times n, n]$ code C associated with $p(x)$ is optimal when $p(x) = x^m - a_0$, where $a_0 \in F_q^*$.*

Proof. For any polynomial $p(x) = \sum_{i=0}^{m} a_i x^i$, a matrix $A \in C$, namely a $c_i \in F_q (i \in [0, n-1])$-linear combination of basis matrices $P_p T_f^i : i \in [0, n-1]$, will look like

$$A = \begin{bmatrix} c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & c_{n-3} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ c_{n-m+1} & \cdots & c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} \\ -\gamma_0 & -\gamma_1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \gamma_{n-1} \end{bmatrix}_{m \times n}$$

where for $i \in [0, n-1]$ we have

$$\gamma_i = c_0 a_i + c_1 a_{i-1} + \cdots + c_i a_0 + \underbrace{0 + \cdots + 0}_{(n-m)} + c_{n-m+1+i} a_{m-1} + \cdots + c_{n-2} a_{i+2} + c_{n-1} a_{i+1}. \quad (5.9)$$

It is shown in [11] that

$$\|A\|_{TR} = \max_{\tau} |\Delta_\tau(A)| \quad (5.10)$$

where the diagonal

$$\Delta_\tau = \{(0, \tau(0)), (1, \tau(1)), \cdots, (m-1, \tau(m-1))\} \quad (5.11)$$

is a set of positions in a matrix $A \in F_q^{m \times n}$, and τ is an injection from $[0, m-1]$ to $[0, n-1]$. $|\Delta_\tau(A)|$ denotes the number of nonzero entries in Δ_τ.

For the case where $p(x)$ is of the form $x^m - a_0, (a_0 \in F_q^*)$, we have

$$A=\begin{bmatrix} c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & c_{n-3} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ c_{n-m+1} & \cdots & c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} \\ -c_0a_0 & -c_1a_0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -c_{n-1}a_0 \end{bmatrix}_{m\times n}$$

We know that there exists at least one nonzero coefficient in the linear combination for all $A \in C$, say $c_t \in F_q (t \in [0, n-1])$. The diagonal

$$\Delta_\tau = \{c_t = (0,1), c_t = (1,2), \cdots, c_t = (m-1, n-1), -c_t a_0 = (m, 0)\}$$

corresponding to the nonzero coefficient c_t, gives the desired $\max_\tau |\Delta_\tau(A)| = m$. Therefore, we have $\|A\|_{TR} = m, \forall A \in C$, which makes C optimal. ■

6
Multi Polycyclic Codes

6.1 Generalized Quasi-cyclic Codes

Definition 6.1. An (n, k) linear block code of dimensions $n = ln_o$ and $k = lk_o$, is called *quasi-cyclic* if every cyclic shift of a codeword by n_o symbols is also a codeword.

Quasi-cyclic (QC) codes are another view of a generalization of cyclic codes. In the above definition, a quasi-cyclic code actually has l cyclic components of the same length. Quasi-cyclic codes are shown to be asymptotically good [35]. Many studies have been conducted in terms of either exploring their algebraic structures [36–38] or obtaining codes with good parameters [5, 39–41]. Recently, skew quasi-cyclic codes are introduced and some skew QC codes having minimum Hamming distances larger than previously best known linear codes of the same length and dimension are obtained [33].

Definition 6.2. Let C be a linear code over F_q and

$$c = (c_{1,1}, \ldots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \ldots, c_{2,n_2-1}, c_{2,n_2}, \ldots, c_{l,1}, \ldots, c_{l,n_l-1}, c_{l,n_l})$$

be a codeword of C. If a generalized quasi-cyclic shift of c;

$$(c_{1,n_1}, c_{1,1}, \ldots, c_{1,n_1-1}, c_{2,n_2}, c_{2,1}, \ldots, c_{2,n_2-1}, \ldots, c_{l,n_l}, c_{l,1}, \ldots, c_{l,n_l-1})$$

is also a codeword in C, then C is a *generalized quasi-cyclic code* of length $(n_1, n_2, \ldots, n_l)$.

Generalized quasi-cyclic (GQC) codes are QC codes with cyclic components of different lengths [42]. In [43], structures of the dual codes of GQC codes were studied by giving a complete theory of generator polynomial matrices of GQC codes, including a relation formula between generator polynomial matrices and parity-check polynomial matrices through their equations. We give a brief summary of this theory here in order to clarify the steps in applications to constacyclic and polycyclic cases.

Definition 6.3. Let C be a GQC code, and let $G = (g_{i,j})$ be an lxl matrix whose entries are in $F_q[x]$ and whose rows are codewords of C. If $g_{i,j} = 0$ for all $1 \leq i, j \leq l$ with $i > j$, namely, G is of the form

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{bmatrix}_{lxl}$$

and moreover, for all $1 \leq i \leq l$, $g_{i,i}$ has the minimum degree among all codewords of the form $(0, \ldots, 0, c_i, \ldots, c_l) \in C$ with $c_i \neq 0$, then G is called a **generator polynomial matrix** of C. If $g_{i,i}$ is monic for all $1 \leq i \leq l$ and G satisfies $\deg g_{i,j} < \deg g_{j,j}$ for all $1 \leq i \neq j \leq l$, then G is called **reduced.**

Definition 6.4. Let C be a GQC code, and let $H = (h_{i,j})$ be an lxl matrix whose entries are in $F_q[x]$ and whose rows are codewords of $C^{\perp}$. If $h_{i,j} = 0$ for all $1 \leq i, j \leq l$ with $i < j$, namely, H is of the form

$$H = \begin{bmatrix} h_{1,1} & 0 & \cdots & 0 \\ h_{2,1} & h_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ h_{l,1} & h_{l,2} & \cdots & h_{l,l} \end{bmatrix}_{lxl}$$

and moreover, for all $1 \leq i \leq l$, $h_{i,i}$ has the minimum degree among all codewords of the form $(c_1, \ldots, c_i, 0, \ldots, 0) \in C^{\perp}$ with $c_i \neq 0$, then H is called a **parity-check polynomial matrix** of C. If $h_{i,i}$ is monic for all $1 \leq i \leq l$ and H satisfies $\deg h_{i,j} < \deg h_{j,j}$ for all $1 \leq i \neq j \leq l$, then H is called **reduced.**

For each GQC code, the reduced generator polynomial matrix and the reduced parity-check polynomial matrix are uniquely determined. From any generator polynomial matrix and parity-check polynomial matrix, we can obtain the reduced ones by elementary row operations of polynomial matrices. The exact algorithm for obtaining the reduced generator polynomial matrix from a generator matrix G of a GQC code, which is called Buchberger's Algorithm, is described briefly as follows [43].

We start with the polynomial representation

$$G' = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,l} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ c_{k,1} & \cdots & c_{k,l-1} & c_{k,l} \end{bmatrix}_{kxl}$$

where $c_{i,j} \in F_q[x]$ for $1 \leq i \leq k$ and $1 \leq j \leq l$. Let c_i denote the i^{th} row of G' for $1 \leq i \leq k$. In this algorithm, the following manipulations of the polynomial matrix are carried out inductively.

1. If $c_{1,1} = \cdots = c_{k,1} = 0$, then set $c_1 = (x^{n_1} - 1, 0, \ldots, 0)$ and stop. If $c_{1,1} \neq 0$ and $c_{2,1} = \cdots = c_{k,1} = 0$, then stop.
2. By exchanging c_1 for another row of $c_2, \ldots, c_k$ if it is required, we can assume that $c_{1,1}$ has the minimum degree among nonzero $c_{1,1}, \ldots, c_{k,1}$.
3. Compute $p_i, r_i \in F_q[x]$ such that $c_{i,1} = p_i c_{1,1} + r_i$ with $\deg r_i < \deg c_{1,1}$ for all $2 \leq i \leq k$ and replace c_i with $c_i - p_i c_1$ for all $2 \leq i \leq k$, and go to step 1.

After the above manipulations, $c_1 = (c_{1,1}, \ldots, c_{1,l})$ is denoted by $g_1 = (g_{1,1}, \ldots, g_{1,l})$ and then we have $g_{1,1} = \gcd(c_{1,1}, \ldots, c_{k,1})$ from the initial matrix G'.

Now, G' is converted to;

$$G'' = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & c_{2,2} & \cdots & c_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & c_{k,2} & \cdots & c_{k,l} \end{bmatrix}_{kxl}$$

where $c_{i,j}$ in G'' is generally unequal to $c_{i,j}$ in G'.

Next, we apply the above manipulation to the submatrix;

$$\begin{bmatrix} c_{2,2} & \cdots & c_{2,l} \\ \ddots & \ddots & \vdots \\ c_{k,2} & \cdots & c_{k,l} \end{bmatrix}$$

and continuing recursively we obtain the reduced form G.

6.2 Multi-twisted and Skew Multi-twisted Codes

Multi-twisted codes have been proposed by Aydin and Halilović [44] and their duals have been explored recently by Sharma et al. [45].

Definition 6.5. Let C be a linear code over F_q and

$$c = (c_{1,1}, \ldots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \ldots, c_{2,n_2-1}, c_{2,n_2}, \ldots, c_{l,1}, \ldots, c_{l,n_l-1}, c_{l,n_l})$$

be a codeword of C. Let $\alpha_1, \alpha_2, \ldots, \alpha_l \in F_q^*$ and $\overline{\alpha} = (\alpha_1, \ldots, \alpha_l)$.

If $\overline{\alpha}$-multi-twisted shift of c;

$$(\alpha_1 c_{1,n_1}, c_{1,1}, \ldots, c_{1,n_1-1}, \alpha_2 c_{2,n_2}, c_{2,1}, \ldots, c_{2,n_2-1}, \ldots, \alpha_l c_{l,n_l}, c_{l,1}, \ldots, c_{l,n_l-1})$$

is also a codeword in C for all $c \in C$, then C is an $\overline{\alpha}$-multi-twisted code of length $(n_1, n_2, \ldots, n_l)$.

Definition 6.6. Let C be a linear code over F_q and

$$c = (c_{1,1}, \ldots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \ldots, c_{2,n_2-1}, c_{2,n_2}, \ldots, c_{l,1}, \ldots, c_{l,n_l-1}, c_{l,n_l})$$

be a codeword of C. Let θ be an automorphism of F_q, $\alpha_1, \alpha_2, \ldots, \alpha_l \in F_q^*$ and $\overline{\alpha} = (\alpha_1, \ldots, \alpha_l)$. If skew $\overline{\alpha}$-multi-twisted shift of c;

$$M_{\overline{\alpha}}(c) = (\alpha_1\theta(c_{1,n_1}), \theta(c_{1,1}), \ldots, \theta(c_{1,n_1-1}), \alpha_2\theta(c_{2,n_2}), \theta(c_{2,1}), \ldots, \theta(c_{2,n_2-1}), \ldots, \alpha_l\theta(c_{l,n_l}), \theta(c_{l,1}), \ldots, \theta(c_{l,n_l-1}))$$

is also a codeword in C, then C is a skew $\overline{\alpha}$-multi-twisted code of length $(n_1, n_2, \ldots, n_l)$.

Briefly, a multi-twisted code is a GQC code with different constacyclic components. The case where $\alpha_i = 1$ for all $1 \leq i \leq l$ corresponds to a skew GQC code [46], and the case where $l = 1$ corresponds to a skew constacyclic code which is invariant under skew α-constacyclic shift [7].

Let $R = F_q[x;\theta]$ and $R_i = F_q[x;\theta]/(x^{n_i} - \alpha_i)$. In polynomial representation form, a skew $\overline{\alpha}$-multi-twisted code C is a left R-submodule of $M = R_1 \times R_2 \times \ldots \times R_l$. Here, we adopt and extend the method introduced in [43] to a family of skew $\overline{\alpha}$-multi-twisted codes. Let

$$\begin{aligned} &\phi : F_q[x;\theta]^l \to M \\ &(f_1, f_2, \ldots, f_l) \to (f_1 \mod (x^{n_1} - \alpha_1), f_2 \mod (x^{n_2} - \alpha_2), \ldots, f_l \mod (x^{n_l} - \alpha_l)) \end{aligned}$$

For a skew $\overline{\alpha}$-multi-twisted code C, define $D = \phi^{-1}(C)$. For the zero codeword $(0, 0, \ldots, 0) \in C$, its preimage $\phi^{-1}((0, 0, \ldots, 0))$ consists of the vectors of the following form:

$$(\underbrace{0, \ldots, 0}_{i-1}, x^{n_i} - \alpha_i, \underbrace{0, \ldots, 0}_{l-i}) \tag{6.1}$$

for all $1 \leq i \leq l$. Conversely, if a left R-submodule $D \subset F_q[x;\theta]^l$ includes l polynomial

vectors of the form (6.1), then $\phi(D)$ determines a skew $\overline{\alpha}$-multi-twisted code.

We view a skew $\overline{\alpha}$-multi-twisted code C in $F_q[x;\theta]^l$ as a submodule and identify each skew $\overline{\alpha}$-multi-twisted code with an $l \times l$ polynomial generator matrix.

The below results are immediate consequences of the corresponding ones in the commutative case [43].

Lemma 6.1. *Let G be an $l \times l$ reduced polynomial matrix. Then G is the reduced generator polynomial matrix of a skew $\overline{\alpha}$-multi-twisted code C if and only if there exists an $l \times l$ matrix A with entries in $F_q[x;\theta]$ such that*

$$AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]. \tag{6.2}$$

Lemma 6.2. *Let G be an $l \times l$ reduced polynomial matrix and $A = [a_{i,j}]$ be a matrix satisfying (6.2). Then A is an upper triangular matrix, satisfying* $\deg(a_{i,i}) > \deg(a_{i,j})$ *for all $1 \leq i, j \leq l$.*

6.2.1 Duality Theorem for Skew Multi-twisted codes

In this part, we state and prove a theorem that reveals the structure of dual codes of skew $(\alpha_1, \ldots, \alpha_l)$-multi-twisted codes. This goal is achieved by generalizing Theorem 4.13 for $l > 1$ and obtaining the reduced parity-check polynomial matrices of skew $(\alpha_1, \ldots, \alpha_l)$-multi-twisted codes from their reduced generator polynomial matrices. Throughout this section we set $m|n_i$, where $m = |\langle\theta\rangle|$.

Theorem 6.3. *Let C be a skew $(\alpha_1, \ldots, \alpha_l)$-multi-twisted code of length $(n_1, \ldots, n_l)$ over F_q. Then, the dual code $C^\perp$ is a skew $(\alpha_1^{-1}, \ldots, \alpha_l^{-1})$-multi-twisted code.*

Proof. Let $M_{\overline{\alpha}^{-1}}(c)$ be the skew $(\alpha_1^{-1}, \ldots, \alpha_l^{-1})$-multi-twisted shift of c. Let

$$c = (c_{1,1}, \ldots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \ldots, c_{2,n_2-1}, c_{2,n_2}, \ldots, c_{l,1}, \ldots, c_{l,n_l-1}, c_{l,n_l}) \in C$$

and

$$d = (d_{1,1}, \ldots, d_{1,n_1-1}, d_{1,n_1}, d_{2,1}, \ldots, d_{2,n_2-1}, d_{2,n_2}, \ldots, d_{l,1}, \ldots, d_{l,n_l-1}, d_{l,n_l}) \in C^\perp,$$

then $c \cdot d = \sum_{j=1}^{l} \sum_{i=1}^{n_j} c_{j,i} d_{j,i} = 0$. We want to show that $c \cdot M_{\overline{\alpha}^{-1}}(d) = 0$, i.e. $M_{\overline{\alpha}^{-1}}(d) \in C^\perp$.

Since C has a finite number of codewords, there exist a number s such that $M_{\overline{\alpha}}^s(c) = c$.

Let

$$\begin{aligned} w = M_{\overline{\alpha}}^{s-1}(c) = (&\theta^{-1}(c_{1,2}), \ldots, \theta^{-1}(c_{1,n_1}), \theta^{-1}(\alpha_1^{-1}c_{1,1}), \\ &\theta^{-1}(c_{2,2}), \ldots, \theta^{-1}(c_{2,n_2}), \theta^{-1}(\alpha_2^{-1}c_{2,1}), \\ &\ldots, \theta^{-1}(c_{l,2}), \ldots, \theta^{-1}(c_{l,n_l}), \theta^{-1}(\alpha_l^{-1}c_{l,1})). \end{aligned}$$

Then,

$$\begin{aligned} 0 = w \cdot d = &(\theta^{-1}(c_{1,2})d_{1,1} + \cdots + \theta^{-1}(c_{1,n_1})d_{1,n_1-1} + \theta^{-1}(\alpha_1^{-1}c_{1,1})d_{1,n_1}) + \\ &(\theta^{-1}(c_{2,2})d_{2,1} + \cdots + \theta^{-1}(c_{2,n_2})d_{2,n_2-1} + \theta^{-1}(\alpha_2^{-1}c_{2,1})d_{2,n_2}) + \cdots + \\ &(\theta^{-1}(c_{l,2})d_{l,1} + \cdots + \theta^{-1}(c_{l,n_l})d_{l,n_l-1} + \theta^{-1}(\alpha_l^{-1}c_{l,1})d_{l,n_l}). \end{aligned}$$

Since $\theta(0) = 0$, we have,

$$\begin{aligned} 0 = &[(c_{1,1}, c_{1,2}, \ldots, c_{1,n_1}) \cdot (\alpha_1^{-1}\theta(d_{1,n_1}), \theta(d_{1,1}), \ldots, \theta(d_{1,n_1-1}))] + \\ &[(c_{2,1}, c_{2,2}, \ldots, c_{2,n_1}) \cdot (\alpha_2^{-1}\theta(d_{2,n_2}), \theta(d_{2,1}), \ldots, \theta(d_{2,n_2-1}))] + \cdots + \\ &[(c_{l,1}, c_{l,2}, \ldots, c_{l,n_l}) \cdot (\alpha_l^{-1}\theta(d_{l,n_l}), \theta(d_{l,1}), \ldots, \theta(d_{l,n_l-1}))] \\ = &c \cdot M_{\overline{\alpha}^{-1}}(d). \end{aligned}$$

Therefore $C^{\perp}$ is a skew $(\alpha_1^{-1}, \ldots, \alpha_l^{-1})$-multi-twisted code. ■

Lemma 6.4. *Let G be the reduced generator polynomial matrix of a skew $\overline{\alpha}$-multi-twisted code C, A be the $l \times l$ upper triangular polynomial matrix satisfying $AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]$, and $N = lcm(n_1, \ldots, n_l)lcm(o(\alpha_1), \ldots, o(\alpha_l))$. Then $G'A = diag\,[x^N - 1, \ldots, x^N - 1]$, where*

$$G' = G\,diag\,[\frac{x^N - 1}{x^{n_1} - \alpha_1}, \ldots, \frac{x^N - 1}{x^{n_l} - \alpha_l}].$$

Proof. Let I be the $l \times l$ identity matrix.

$$\begin{aligned} AG = diag\,[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l] &\Rightarrow diag[\frac{x^N - 1}{x^{n_1} - \alpha_1}, \ldots, \frac{x^N - 1}{x^{n_l} - \alpha_l}]AG = (x^N - 1)I \\ &\Rightarrow Gdiag[\frac{x^N - 1}{x^{n_1} - \alpha_1}, \ldots, \frac{x^N - 1}{x^{n_l} - \alpha_l}]AG = G(x^N - 1)I \\ &\Rightarrow G'AG = (x^N - 1)G, \ \text{ since } x^N - 1 \in \mathscr{Z}(F_q[x;\theta]) \\ &\Rightarrow G'AG - (x^N - 1)G = 0 \\ &\Rightarrow (G'A - (x^N - 1)I)G = 0. \end{aligned}$$

Since G is an upper triangular polynomial matrix with nonzero diagonal entries and $F_q[x;\theta]$ has no zero divisors, $G'A - (x^N - 1)I = 0$ which implies $G'A = (x^N - 1)I = diag\,[x^N - 1, \ldots, x^N - 1]$. ■

Theorem 6.5. *Let $G = [g_{i,j}(x)]$ be the reduced generator polynomial matrix of a skew $\overline{\alpha}$-multi-twisted code C of length $(n_1, \ldots, n_l)$ over F_q where $\overline{\alpha} = (\alpha_1, \ldots, \alpha_l) \in (F_q^*)^l$, and let $A = [a_{i,j}(x)]$ be the polynomial matrix which satisfies $AG = diag[x^{n_1} - \alpha_1, \ldots, x^{n_l} - \alpha_l]$. Then,*

$$H = \begin{bmatrix} x^{\deg a_{1,1}} a_{1,1}^{\langle n_1, \alpha_1 \rangle}(x) & 0 & \cdots & 0 \\ x^{\deg a_{2,2}} a_{1,2}^{\langle n_1, \alpha_1 \rangle}(x) & x^{\deg a_{2,2}} a_{2,2}^{\langle n_2, \alpha_2 \rangle}(x) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ x^{\deg a_{l,l}} a_{1,l}^{\langle n_1, \alpha_1 \rangle}(x) & x^{\deg a_{l,l}} a_{2,l}^{\langle n_2, \alpha_2 \rangle}(x) & \cdots & x^{\deg a_{l,l}} a_{l,l}^{\langle n_l, \alpha_l \rangle}(x) \end{bmatrix}_{l \times l}$$

where each i^{th} column of H is considered modulo $x^{n_i} - \alpha_i^{-1}$. If $a_{i,i}(x) = x^{n_i} - \alpha_i$, then we set $x^{\deg a_{i,i}} a_{i,i}^{\langle n_i, \alpha_i \rangle}(x) = x^{n_i} - \alpha_i^{-1}$. Then, H is a parity-check polynomial matrix of C.

Proof. Let $N = lcm(n_1, \ldots, n_k) lcm(o(\alpha_1), \ldots, o(\alpha_l))$ and G' be defined as in Lemma 6.4. From Lemma 6.4 we have $G'A = diag[x^N - 1, \ldots, x^N - 1]$ where

$$\sum_{k=1}^{l} g_{i,k}(x) \frac{x^N - 1}{x^{n_k} - \alpha_k} a_{k,j}(x) = \begin{cases} 0, & i \neq j \\ x^N - 1, & i = j \end{cases}$$

for $1 \leq i, j \leq l$. Thus, for a fixed i and j we have

$$\begin{aligned} g_{i,1}(x) \frac{x^N - 1}{x^{n_1} - \alpha_1} a_{1,j}(x) + g_{i,2}(x) \frac{x^N - 1}{x^{n_2} - \alpha_2} a_{2,j}(x) + \\ \cdots + g_{i,l}(x) \frac{x^N - 1}{x^{n_l} - \alpha_l} a_{l,j}(x) = 0 \pmod{x^N - 1}. \end{aligned} \tag{6.3}$$

From Theorem 4.13, the coefficient of x^0 in Equation 6.3 is

$$g_{i,1} \cdot a_{1,j}^{\langle n_1, \alpha_1 \rangle} + g_{i,2} \cdot a_{2,j}^{\langle n_2, \alpha_2 \rangle} + \cdots + g_{i,l} \cdot a_{l,j}^{\langle n_l, \alpha_l \rangle} = 0,$$

which implies $(g_{i,1}, g_{i,2}, \ldots, g_{i,l}) \cdot (a_{1,j}^{\langle n_1, \alpha_1 \rangle}, a_{2,j}^{\langle n_2, \alpha_2 \rangle}, \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle}) = 0$.

Using the same approach as in the proof of Theorem 4.13, if we multiply Equation (6.3) with x^b from left, then the coefficient of x^0 gives $M_{\overline{\alpha}}^b((g_{i,1}, g_{i,2}, \ldots, g_{i,l})) \cdot (a_{1,j}^{\langle n_1, \alpha_1 \rangle}, a_{2,j}^{\langle n_2, \alpha_2 \rangle}, \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle}) = 0$. Hence, $(a_{1,j}^{\langle n_1, \alpha_1 \rangle}, a_{2,j}^{\langle n_2, \alpha_2 \rangle}, \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle})$ is in $C^\perp$ for all $i, j \in \{1, \ldots, l\}$.

Thus $x^{\deg a_{j,j}}(a_{1,j}^{\langle n_1, \alpha_1 \rangle}(x), a_{2,j}^{\langle n_2, \alpha_2 \rangle}(x), \ldots, a_{l,j}^{\langle n_l, \alpha_l \rangle}(x))$, which is exactly the jth row of H, also belongs to $C^\perp$. Lastly, we need to show that the diagonal entries of H satisfy the minimum degree condition. This can be shown by using similar tools as in Theorem 1 of [43]. The same arguments hold for the skew polynomial case since we are working on left modules. ∎

Here, we give some concrete examples to illustrate our theoretical results.

Example 6.1. *Let θ be an automorphism of F_4 defined by $\theta(\beta) = \beta^2$ for any $\beta \in F_4$, in this case $|\langle\theta\rangle| = 2$. We consider the skew polynomial ring $F_4[x;\theta]$ where $F_4 = \{0, 1, \alpha, \alpha^2\}$. Let*

$$A = \begin{bmatrix} x^4+\alpha^2x^3+\alpha^2x+1 & x^3+x^2+\alpha^2x+\alpha & x^3+\alpha^2x^2+x \\ 0 & x+1 & \alpha^2 \\ 0 & 0 & 1 \end{bmatrix}_{3\times 3}$$

and

$$G = \begin{bmatrix} x^2+\alpha^2x+1 & x^2+\alpha^2x+\alpha & x^3+\alpha^2x^2+1 \\ 0 & x^3+x^2+x+1 & \alpha x^3+\alpha^2x^2+\alpha x+\alpha^2 \\ 0 & 0 & x^4+1 \end{bmatrix}_{3\times 3}.$$

The above matrices satisfy $AG = diag[x^6-1, x^4-1, x^4-1]$. Therefore G is a generator matrix for a skew GQC code C of length $(6,4,4)$ and C is a $[14,5,4]$ code. By Theorem 6.5, the parity-check polynomial matrix for C is

$$H = \begin{bmatrix} x^4+\alpha x^3+\alpha x+1 & 0 & 0 \\ x^5+x^4+\alpha^2x+\alpha^2 & x+1 & 0 \\ x^5+\alpha^2x^4+x^3 & \alpha^2 & 1 \end{bmatrix}_{3\times 3}.$$

Further, we present their corresponding generator matrices of the code and its dual

$$G = \left[\begin{array}{cccccc|cccc|cccc} 1 & \alpha^2 & 1 & 0 & 0 & 0 & \alpha & \alpha^2 & 1 & 0 & 1 & 0 & \alpha^2 & 1 \\ 0 & 1 & \alpha & 1 & 0 & 0 & 0 & \alpha^2 & \alpha & 1 & 1 & 1 & 0 & \alpha \\ 0 & 0 & 1 & \alpha^2 & 1 & 0 & 1 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & \alpha & 1 & \alpha & 1 & 0 & \alpha^2 & 0 & \alpha & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha \end{array}\right]_{5\times 14}$$

and

$$H = \left[\begin{array}{cccccc|cccc|cccc} 1 & \alpha & 0 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 0 & \alpha^2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^2 & \alpha^2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \alpha & \alpha & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & \alpha^2 & \alpha^2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & \alpha & 0 & \alpha & 0 & 0 & 0 & 1 & 0 & 0 \\ \alpha^2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & 1 & 0 \\ 1 & \alpha & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 1 \end{array}\right]_{9\times 14}.$$

Now, one can easily check that $G \cdot H^{tr} = 0$ and the dual code $C^{\perp}$ is a $[14,9,3]$ code.

Example 6.2. *Next we consider again the skew polynomial ring $F_4[x;\theta]$ given in Example 6.1, with the following moderate size matrices:*

$$A = \begin{bmatrix} x^2+\alpha & 1 & 0 \\ 0 & x^4+\alpha^2 & x^2+\alpha \\ 0 & 0 & 1 \end{bmatrix}_{3\times 3},$$

and

$$G = \begin{bmatrix} x^2+\alpha & x^2+\alpha & x^4+\alpha^2 \\ 0 & x^4+\alpha^2 & x^6+\alpha x^4+\alpha^2 x^2+1 \\ 0 & 0 & x^8+\alpha \end{bmatrix}_{3\times 3}.$$

It can be easily shown that $AG = diag[x^4-\alpha^2, x^8-\alpha, x^8-\alpha]$. Therefore G is a generator matrix for a skew $\overline{\alpha}$-multi-twisted code C of length $(4,8,8)$, where $\overline{\alpha} = (\alpha^2, \alpha, \alpha)$,

We have $dim(C) = \sum n_i - deg(g_{i,i}) = 2+4+0 = 6$. C is a $[20,6,4]$ code.

By Theorem 6.5, the parity-check polynomial matrix for C is

$$H = \begin{bmatrix} x^2+\alpha^2 & 0 & 0 \\ \alpha & x^4+\alpha & 0 \\ 0 & x^6+1 & \alpha^2 \end{bmatrix}_{3\times 3}.$$

6.3 Multi Polycyclic Codes

We will call GQC codes with l polycyclic components of different lengths as multi polycyclic codes.

6.3.1 Multi Polycyclic Codes over Skew Polynomial Rings

Definition 6.7. Let C be a linear code over F_q and

$$c = (c_{1,1}, \ldots, c_{1,n_1-1}, c_{1,n_1}, c_{2,1}, \ldots, c_{2,n_2-1}, c_{2,n_2}, \ldots, c_{l,1}, \ldots, c_{l,n_l-1}, c_{l,n_l})$$

be a codeword of C. Let θ be an automorphism of F_q, $f_1 = x^{n_1} - v_1(x), \ldots, f_l = x^{n_l} - v_l(x) \in F_q[x;\theta]$ polynomials with nonzero constant terms and $\overline{v} = (v_1, \ldots, v_l)$. If a skew $\overline{v}$-multi polycyclic shift of c,

$$M_{\overline{v}}(c) = (T_{f_1}(\theta(c_{1,1}), \ldots, \theta(c_{1,n_1-1})), T_{f_2}(\theta(c_{2,1}), \ldots, \theta(c_{2,n_2-1})), \ldots, T_{f_l}(\theta(c_{l,1}), \ldots, \theta(c_{l,n_l-1})))$$

is also a codeword in C, then C is called a skew $\overline{v}$-multi polycyclic code of length $(n_1, n_2, \ldots, n_l)$.

Reduced generator polynomial matrices of skew $\overline{v}$-multi polycyclic codes can be defined in a similar way as in the case of skew $\overline{\alpha}$-multi-twisted codes.

6.3.2 Duality Theorem for Skew Multi Polycyclic Codes

We have seen, for the case $l = 1$, that h is obtained from the first n coordinates of $a'^{\langle N,1\rangle}$, where $a'(x) = \frac{x^N-1}{f(x)}a(x)$. In order to easily interpret this situation in the sequel, let us denote the first n coordinates of $a'^{\langle N,1\rangle}$ by $(a'^{\langle N,1\rangle})_n$.

Theorem 6.6. *Let $f_i(x) = x^{n_i} - v_i(x) \in F_q[x;\theta]$ be polynomials with nonzero constant terms, $\overline{v} = (v_1, \ldots, v_l)$, and $x^N - 1$ be a central polynomial such that $f_i(x)|_r x^N - 1$ for all $1 \leq i \leq l$. Let $G = [g_{i,j}(x)]$ be the reduced generator polynomial matrix of a skew $\overline{v}$-multi polycyclic code C of length $(n_1, \ldots, n_l)$ over F_q. Let $A = [a_{i,j}(x)]$ be the polynomial matrix which satisfies $AG = diag[f_1(x), \ldots, f_l(x)]$.*

Then,

$$\sum_{k=1}^{l} g_{i,k}(x)\frac{x^N-1}{f_k(x)}a_{k,j}(x) = \begin{cases} 0, & i \neq j \\ x^N - 1, & i = j \end{cases}.$$

Moreover, if $h_{i,j} = (a'^{\langle N,1\rangle}_{j,i})_{n_j}$ *where* $a'_{j,i}(x) = \frac{x^N-1}{f_j(x)} a_{j,i}(x)$*, then the block matrix*

$$H = \begin{bmatrix} [h_{1,1}]_{deg(g_{1,1})} & 0 & \cdots & 0 \\ [h_{2,1}]_{deg(g_{2,2})} & [h_{2,2}]_{deg(g_{2,2})} & 0 & \vdots \\ \vdots & \vdots & \ddots & 0 \\ [h_{l,1}]_{deg(g_{l,l})} & [h_{l,2}]_{deg(g_{l,l})} & \cdots & [h_{l,l}]_{deg(g_{l,l})} \end{bmatrix}_{l \times l}$$

is a parity-check matrix of C*, where*

$$[h_{i,j}]_{deg(g_{i,i})} := \begin{bmatrix} h_{i,j} \\ ((T_{f_j}^{-1})^{tr} \circ \Theta)(h_{i,j}) \\ \vdots \\ ((T_{f_j}^{-1})^{tr} \circ \Theta)^{deg(g_{i,i})-1}(h_{i,j}) \end{bmatrix}.$$

Proof. Applying Lemma 6.4, $G'A = diag[x^N - 1, \ldots, x^N - 1]$ implies

$$\sum_{k=1}^{l} g_{i,k}(x) \frac{x^N-1}{f_k(x)} a_{k,j}(x) = \begin{cases} 0, & i \neq j \\ x^N - 1, & i = j, \end{cases}$$

for $1 \leq i, j \leq l$, where $G' = Gdiag[\frac{x^N-1}{f_1}, \ldots, \frac{x^N-1}{f_l}]$. For a fixed i and j we have

$$\begin{aligned} &g_{i,1}(x)\frac{x^N-1}{f_1(x)}a_{1,j}(x) + g_{i,2}(x)\frac{x^N-1}{f_2(x)}a_{2,j}(x) + \\ &\cdots + g_{i,l}(x)\frac{x^N-1}{f_l(x)}a_{l,j}(x) = 0 \pmod{x^N-1}. \end{aligned} \tag{6.4}$$

As in Theorem 4.16, the coefficient of x^0 is;

$$g_{i,1} \cdot (a_{1,j}^{\langle N,1\rangle})_{n_1} + g_{i,2} \cdot (a_{2,j}^{\langle N,1\rangle})_{n_2} + \cdots + g_{i,l} \cdot (a_{l,j}^{\langle N,1\rangle})_{n_l} = 0,$$

which implies $(g_{i,1}, g_{i,2}, \ldots, g_{i,l}) \cdot ((a_{1,j}^{\langle N,1\rangle})_{n_1}, (a_{2,j}^{\langle N,1\rangle})_{n_2}, \ldots, (a_{l,j}^{\langle N,1\rangle})_{n_l}) = 0$. Multiplying Equation (6.4) with x^b from the left, we obtain

$$M_{\overline{v}}^{b}((g_{i,1}, g_{i,2}, \ldots, g_{i,l})) \cdot ((a_{1,j}^{\langle N,1\rangle})_{n_1}, (a_{2,j}^{\langle N,1\rangle})_{n_2}, \ldots, (a_{l,j}^{\langle N,1\rangle})_{n_l}) = 0$$

from the coefficient of x^0. Hence $(h_{j,1}, h_{j,2}, \ldots, h_{j,l}) \in C^{\perp}$ for all $j \in \{1, \ldots, l\}$. For each diagonal block of H we have $a_{i,i}(x)g_{i,i}(x) = f_i(x)$. From Theorem 4.16, the set $\{h_{i,i}, ((T_{f_i}^{-1})^{tr} \circ \Theta)(h_{i,i}), \ldots, ((T_{f_i}^{-1})^{tr} \circ \Theta)^{deg(g_{i,i})-1}(h_{i,i})\}$ is linearly independent for all $1 \leq i \leq l$. Therefore the rows of H are also linearly independent. Since the dimension of $C^{\perp}$ is exactly $\sum_{i=0}^{l} deg(g_{i,i}(x))$, H is a parity-check polynomial matrix of C. ∎

Example 6.3. *Let us take the skew polynomial ring $F_4[x;\theta]$ given in Example 6.1. Let $f_1(x) = x^6+\alpha^2x^2+\alpha^2, f_2(x) = x^8+\alpha^2x^6+x^4+\alpha x^2+a$ and $f_3(x) = x^{10}+\alpha x^6+x^4+\alpha$. In this case, we have $N = 120$, and $f_1(x), f_2(x), f_3(x)|_r x^{120}-1$. Now let us form the following matrices*

$$A = \begin{bmatrix} x^2+\alpha^2 & 0 & 1 \\ 0 & x^4+\alpha x^2+1 & 0 \\ 0 & 0 & x^2+\alpha \end{bmatrix}_{3x3},$$

$$G = \begin{bmatrix} x^4+\alpha^2x^2+1 & 0 & x^6+x^4+\alpha x^2+\alpha \\ 0 & x^4+x^2+\alpha & 0 \\ 0 & 0 & x^8+\alpha x^6+x^4+\alpha^2x^2+1 \end{bmatrix}_{3x3}.$$

We have $AG = diag[f_1(x), f_2(x), f_3(x)]$. Then $G = [g_{i,j}(x)]$ is the reduced generator polynomial matrix of a skew $\overline{v} = (v_1, v_2, v_3)$-multi polycyclic code C of length $(6, 8, 10)$, where $v_1 = (\alpha^2, 0, \alpha^2, 0, 0, 0), v_2 = (\alpha, 0, \alpha, 0, 1, 0, \alpha^2, 0)$ and $v_3 = (\alpha, 0, 0, 0, 1, 0, a, 0, 0, 0)$.

Now, by applying the algorithm presented in Theorem 6.6, we obtain a parity-check matrix for C as

$$H = \begin{bmatrix} [h_{1,1}]_{deg(g_{1,1})} & 0 & 0 \\ [h_{2,1}]_{deg(g_{2,2})} & [h_{2,2}]_{deg(g_{2,2})} & 0 \\ [h_{3,1}]_{deg(g_{3,3})} & [h_{3,2}]_{deg(g_{3,3})} & [h_{3,3}]_{deg(g_{3,3})} \end{bmatrix}_{3x3}$$

where $h_{1,1} = (1, 0, 0, 0, 1, 0), h_{2,1} = \overline{0}, h_{2,2} = (\alpha^2, 0, 0, 0, 1, 0, 1, 0), h_{3,1} = (\alpha, 0, 0, 0, 0, 0), h_{3,2} = \overline{0}$ and $h_{3,3} = (1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$.

7
Results And Discussion

This thesis contributes to studies on error correcting codes in terms of clarifiying structural properties of polycyclic codes which appears to be the most general family of linear codes in terms of cyclicity. We have given generator and parity check conditions for these codes over different algebraic structures. The most important contributions involve introducing multi polycyclic codes which are GQC codes with different polycylic components, giving duality theorems and promoting a new polycyclic construction for codes over matrix spaces. An extensive approach was provided on polycyclic codes over skew polynomial rings.

Even though being constructable with shortening method may seem as a weakness for polycyclic codes, avoiding to start with a huge length cyclic code while using polycyclic codes directly makes it an advantage in terms of storage and time in practice.

Future studies may be on examining decoding procedures for polycyclic codes. One of them may involve neural network decoding. Artificial intelligence techniques have found applications nearly in every technological area with the near-human capabilities of artificial neural networks. There are remarkable number of studies recently in applications of neural networks on decoding of linear codes. Recent studies in neural network decoding for linear block codes show that codes with more structure seem to provide better results in decoding with neural networks. Therefore polycyclic codes are promising for analyzing their neural network decoding performance.

A
Scripts for Computing Minimum Term Rank Distance

A.1 Construction of the Code - Magma Script

```
//Set associated polynomial p, base polynomial f and output file name
//Copy m, n and the output filepath for later use in python function

K<a>:=GF(2^2);
F<x>:= PolynomialRing(K);
p:= x^5 + a^2*x^4 + x^3 + x^2 + a*x + 1;
f:= x^11-1;
m:=Degree(p);
n:=Degree(f);
T:= CompanionMatrix(f);
V:= KMatrixSpace(K,m,n);
M:=MatrixRing(K,n);

Z1 := [0: x in [1..m*(n-m)]];
P := HorizontalJoin(CompanionMatrix(p),Matrix(K, m, n-m, Z1));
B := { V!P*T^i : i in [0..n-1]};
S:= sub< V | B >;

SetOutputFile("5x11.txt");
for s in S do
for i in [1..m] do
for j in [1..n] do
print s[i,j];
end for;
print "$";
end for;
print "@";
end for;
UnsetOutputFile();
```

A.2 Computing Minimum Term Rank Distance - Python Script

```
import numpy as np
import networkx as nx
from networkx.algorithms import bipartite
import itertools
from networkx.convert import _prep_create_using
from networkx.convert_matrix import _generate_weighted_edges
import scipy
from scipy import linalg

# Given a file path of Magma file of the constructed code, computes
    the minimum term rank distance of an m x n code over GF(4)^mn.

def Minimum_Term_Rank_Distance(m,n, filepath):
    fname = filepath
    fhand = open(fname)
    L = list()
    S = str()
    # Denote field-specific elements by 1
    for line in fhand:
        line = line.strip()
        if "a^2" in line:
            line = line.replace("a^2","1")
        elif "a" in line:
            line = line.replace("a","1")
        S = S + line
    M = S.strip().split("@")

    # Remove irrelevant characters inserted for environmental
       implementations
    for s in M:
        s = s.split("$")
        L.append(s)
    for l in L:
        if len(l) < m+1 :
            L.remove(l)
        else:
            l.remove("")

    K = list()
    for item in L:
```

```
        M = list()
        for i in range(m):
            M.append([int(r) for r in item[i]])
        A = scipy.sparse.csr_matrix(M)
        G = nx.bipartite.from_biadjacency_matrix(A)
        D = nx.bipartite.maximum_matching(G)
        termrank = int(len(D.items())/2)
        if termrank != 0:
            K.append(termrank)
    print("D_tr = ", min(K))
```

For the cyclic code in the first example, we call the function with parameters (5,11, "5x11.txt") and we get that it has a minimum term rank distance of 3, and therefore it is optimal.

This example is taken over the field F_4. One may change the field and then slight modifications should be applied to the scripts if there exist more field-specific non-zero and non-integer elements.

References

[1] C. Xing and S. Ling, *Coding Theory: A First Course*. New York, NY, USA: Cambridge University Press, 2003.

[2] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge: Cambridge Univ. Press, 2003.

[3] W. Peterson and E. Weldon, *Error-correcting Codes*. MIT Press, 1972.

[4] E. Prange, *Cyclic Error-correcting Codes in Two Symbols*, ser. AFCRC-TN. Air Force Cambridge Research Center, 1957.

[5] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, "New ternary quasi-cyclic codes with better minimum distances," *IEEE Trans. Information Theory*, vol. 46, no. 4, pp. 1554–1558, 2000.

[6] H. Q. Dinh and S. R. López-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Trans. Information Theory*, vol. 50, no. 8, pp. 1728–1744, 2004.

[7] D. Boucher, P. Solé, and F. Ulmer, "Skew constacyclic codes over galois rings," *Adv. in Math. of Comm.*, vol. 2, no. 3, pp. 273–292, 2008.

[8] S. Jitman, S. Ling, and P. Udomkavanich, "Skew constacyclic codes over finite chain rings," *Adv. in Math. of Comm.*, vol. 6, no. 1, pp. 39–63, 2012.

[9] E. M. Gabidulin, "Optimum codes correcting lattice errors," *Probl Inf Transm.*, vol. 21, no. 2, pp. 103–108, 1997.

[10] V. V. Gritsenko and A. É. Maevskiy, "$p(x)$-circulants over finite fields and probability methods of their construction," *Mathematical Notes*, vol. 96, no. 5, pp. 928–942, 2014.

[11] R. A. Brualdi, K. P. Kiernan, S. A. Meyer, and M. W. Schroeder, "On the t-term rank of a matrix," *Linear Algebra and its Applications*, vol. 436, no. 6, pp. 1632–1643, 2012.

[12] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-cyclic codes," *Appl. Algebra Eng. Commun. Comput.*, vol. 18, no. 4, pp. 379–389, 2007.

[13] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, "Polycyclic codes over galois rings with applications to repeated-root constacyclic codes," *Finite Fields and Their Applications*, vol. 19, no. 1, pp. 16–38, 2013.

[14] S. R. López-Permouth, B. R. Parra-Avila, and S. Szabo, "Dual generalizations of the concept of cyclicity of codes," *Adv. in Math. of Comm.*, vol. 3, no. 3, pp. 227–234, 2009.

[15] M. Matsuoka, "θ-polycyclic codes and θ-sequential codes over finite fields," *International Journal of Algebra*, vol. 5, pp. 65–70, Jan. 2011.

[16] A. Alahmadi, S. Dougherty, A. Leroy, and P. Sole, "On the duality and the direction of polycyclic codes," *Advances in Mathematics of Communications*, vol. 10, no. 4, pp. 921–929, 2016.

[17] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at `http://www.codetables.de`, Accessed on 2019-05-16, 2007.

[18] D. Radkova and A. V. Zanten, "Constacyclic codes as invariant subspaces," *Linear Algebra and its Applications*, vol. 430, no. 2, pp. 855–864, 2009.

[19] M. Wu, "Free cyclic codes as invariant submodules over finite chain rings," *International Mathematical Forum*, vol. 8, no. 37, pp. 1835–1838, 2013.

[20] S. Bedir and I. Siap, "Polycylic quaternary codes," in *International Conference on Coding and Cryptography (ICCC)*, Nov. 2015, pp. 163–170.

[21] E. R. Berlekamp, *Algebraic Coding Theory*, Revised. World Scientific Publishing Co, 2015.

[22] H. Q. Dinh, "Repeated-root constacyclic codes of length 2ps," *Finite Fields and Their Applications*, vol. 18, no. 1, pp. 133–143, 2012.

[23] S. Jitman, "Vector-circulant matrices and vector-circulant based additive codes over finite fields," *Information*, vol. 8, p. 82, Jul. 2017.

[24] D. Boucher and F. Ulmer, "A note on the dual codes of module skew codes," in *Lecture Notes in Computer Science*, vol. 7089, Springer, 2011, pp. 230–243.

[25] Z.-X. X. Wan and C.-H. Wan, *Quaternary Codes*. River Edge, NJ, USA: World Scientific Publishing Co., Inc., 1998.

[26] N. Aydin and T. Asamov, *A Database of Z_4 Codes*, Online available at `http://www.asamov.com/Z4Codes/CODES/ShowCODESTablePage.aspx`, Accessed on 2019-05-16, 2007.

[27] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997, Computational algebra and number theory (London, 1993).

[28] B. R. McDonald, *Finite Rings With Identity*. Marcel Dekker Inc, 1974.

[29] O. Ore, "Theory of non-commutative polynomials," *Ann. of Math.*, vol. 34, pp. 480–508, 1933.

[30] N. Jacobson, *Finite-dimensional division algebras over fields*, 1st ed. 1996. Corr. 2nd printing, ser. Grundlehren Der Mathematischen Wissenschaften. Springer, 1996.

[31] D. Boucher and F. Ulmer, "Coding with skew polynomial rings," *J. Symb. Comput.*, vol. 44, no. 12, pp. 1644–1656, 2009.

[32] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, "Skew cyclic codes of arbitrary length," *IJICoT*, vol. 2, no. 1, pp. 10–20, 2011.

[33] T. Abualrub, A. Ghrayeb, N. Aydin, and I. Siap, "On the construction of skew quasi-cyclic codes," *IEEE Trans. Information Theory*, vol. 56, no. 5, pp. 2081–2090, 2010.

[34] N. Fogarty and H. Gluesing-Luerssen, "A circulant approach to skew-constacyclic codes," *Finite Fields and Their Applications*, vol. 35, pp. 92–114, 2015.

[35] C. L. Chen, W. W. Peterson, and E. J. W. Jr., "Some results on quasi-cyclic codes," *Information and Control*, vol. 15, no. 5, pp. 407–423, 1969.

[36] K. Thomas, "Polynomial approach to quasi-cyclic codes," *Bul. Cal. Math. Soc.*, vol. 69, pp. 51–59, 1977.

[37] J. Conan and G. E. Séguin, "Structural properties and enumeration of quasi cyclic codes," *Appl. Algebra Eng. Commun. Comput.*, vol. 4, pp. 25–39, 1993.

[38] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields," *IEEE Trans. Information Theory*, vol. 47, no. 7, pp. 2751–2760, 2001.

[39] P. P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Des. Codes Cryptography*, vol. 2, no. 1, pp. 81–91, 1992.

[40] T. A. Gulliver and V. K. Bhargava, "Nine good rate (m-1)/pm quasi-cyclic codes," *IEEE Trans. Information Theory*, vol. 38, no. 4, pp. 1366–1369, 1992.

[41] T. A. Gulliver and V. K. Bhargava, "Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4)," *IEEE Trans. Information Theory*, vol. 38, no. 4, pp. 1369–1374, 1992.

[42] I. Siap and N. Kulhan, "The structure of generalized quasi cyclic codes," *Applied Mathematics E-Notes [electronic only]*, vol. 5, Jan. 2005.

[43] H. Matsui, "On generator and parity-check polynomial matrices of generalized quasi-cyclic codes," *Finite Fields and Their Applications*, vol. 34, pp. 280–304, 2015.

[44] N. Aydin and A. Halilovic, "A generalization of quasi-twisted codes: Multi-twisted codes," *Finite Fields and Their Applications*, vol. 45, pp. 96–106, 2017.

[45] A. Sharma, V. Chauhan, and H. Singh, "Multi-twisted codes over finite fields and their dual codes," *Finite Fields and Their Applications*, vol. 51, pp. 270–297, 2018.

[46] J. Gao, L. Shen, and F. Fu, "A chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields," *Cryptography and Communications*, vol. 8, no. 1, pp. 51–66, 2016.

Publications From the Thesis

Contact Information: sbedir@yildiz.edu.tr

Papers

1. S. Bedir, F. Gursoy and I. Siap, "On generalizations of skew quasi-cyclic codes", *Bull. of Korean Math. Society*, under review.

2. S. Bedir, B. A. Ersoy, "On a pseudo-cyclic construction of codes over term rank metric spaces", *Trans. of NAS of Azerbaijan, Issue Mathematics*, accepted: May, 2019.

Conference Papers

1. S. Bedir and I. Siap, "Polycyclic quaternary codes", *International Conference on Coding and Cryptography*, Nov, 2015, Algeria.

2. S. Bedir, E. S. Oztas and I. Siap, "Pseudo-cyclic codes with applications to DNA", *International Congress on Fundamental and Applied Sciences*, Aug, 2016, Istanbul.

3. S. Bedir and B. A. Ersoy, "On a construction of codes over term rank metric spaces", *International Conference on Mathematics and Engineering*, May, 2017, Istanbul.

4. S. Bedir and F. Gursoy, "A note on dual codes of pseudo-cyclic codes", *International Conference on Mathematical Advances and Applications*, May, 2018, Istanbul.