On Cyclic Codes and Their Generalizations over Some Finite Non-Chain Rings and Construction of Quantum and LCD Codes

The thesis submitted in partial fulfillment

for the Award of Degree

DOCTOR OF PHILOSOPHY

by

Pradeep Rai

DEPARTMENT OF MATHEMATICAL SCIENCES

INDIAN INSTITUTE OF TECHNOLOGY

(BANARAS HINDU UNIVERSITY)

VARANASI -221005

Roll No: 19121005 **December 2024**

भारतीय प्रौद्योगिकी संस्थान
काशी हिन्दू विश्वविद्यालय

IIT INDIAN INSTITUTE OF TECHNOLOGY
BANARAS HINDU UNIVERSITY

CERTIFICATE

It is certified that the work contained in this thesis titled "**On Cyclic Codes and Their Generalizations over Some Finite Non-chain Rings and Construction of Quantum and LCD Codes**" by **Pradeep Rai** has been carried out under my supervision and this work has not been submitted elsewhere for a degree.
It is further certified that the student has fulfilled all the requirements of the Comprehensive Examination, Candidacy, and SOTA for the award of the Ph.D. degree.

Dr. Ashok Ji Gupta
(Supervisor)
Associate Professor
Department of Mathematical Sciences
Indian Institute of Technology
(Banaras Hindu University)
Varanasi– 221005, Uttar Pradesh
India

पर्यवेक्षक/Supervisor
गणितीय विज्ञान विभाग
Department of Mathematical Sciences
भारतीय प्रौद्योगिकी संस्थान
Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय)
(Banaras Hindu University)
वाराणसी/Varanasi-221005

Dr. Bhupendra Singh
(Co-Supervisor)
Scientist 'F'
Centre for Artificial Intelligence & Robotics (CAIR), Defence Research & Development Organization (DRDO)
Bengaluru-560093, Karnataka
India

DECLARATION BY THE CANDIDATE

I, **Pradeep Rai**, certify that the work embodied in this thesis is my own bonafide work and carried out by me under the supervision of **Dr. Ashok Ji Gupta** from **July 2019** to **June 2024** at the **Department of Mathematical Sciences, Indian Institute of Technology (Banaras Hindu University), Varanasi**. The matter embodied in this thesis has not been submitted for the award of any other degree/diploma. I declare that I have faithfully acknowledged and given credits to the research workers wherever their works have been cited in my work in this thesis. I further declare that I have not willfully copied any other's work, paragraphs, text, data, results, *etc.*, reported in journals, books, magazines, reports dissertations, theses, *etc.*, or available at websites and have not included them in this thesis and have not cited as my own work.

Date: 27/12/2024

Place: Varanasi

PRai

(Pradeep Rai)

CERTIFICATE BY THE SUPERVISOR

It is certified that the above statement made by the student is correct to the best of my/our knowledge.

Dr. Ashok Ji Gupta
Department of Mathematical Sciences
Indian Institute of Technology
(Banaras Hindu University)
Varanasi-221005

पर्यवेक्षक / Supervisor
गणितीय विज्ञान विभाग
Department of Mathematical Sciences
भारतीय प्रौद्योगिकी संस्थान
Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय)
(Banaras Hindu University)
वाराणसी / Varanasi-221005

27.12.2024

Head
Department of Mathematical Sciences
Indian Institute of Technology
(Banaras Hindu University)
Varanasi-221005

विभागाध्यक्ष / HEAD
गणितीय विज्ञान विभाग
Department of Mathematical Sciences
भारतीय प्रौद्योगिकी संस्थान
Indian Institute of Technology
(काशी हिन्दू विश्वविद्यालय)
(Banaras Hindu University)
वाराणसी / Varanasi-221005

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: ***On Cyclic Codes and Their Generalizations over Some Finite Non-chain Rings and Construction of Quantum and LCD Codes***

Name of the Student: ***Pradeep Rai***

Copyright Transfer

The undersigned hereby assigns to the Indian Institute of Technology (Banaras Hindu University), Varanasi all rights under copyright that may exist in and for the above thesis submitted for the award of the Ph.D. degree.

Date: 27/12/2024

Place: Varanasi

PRai

(Pradeep Rai)

Note: However, the author may reproduce or authorize others to reproduce material extracted verbatim from the thesis or derivative of the thesis for the author's personal use provided that the source and the Institute copyright notice are indicated.

DEDICATED

TO

MY BELOVED FAMILY

ACKNOWLEDGEMENTS

Earning a Ph.D. in Mathematics from such a prestigious institute is a once-in-a-lifetime experience, and I firmly believe that experiences are the true treasures of life. As I complete this doctoral thesis, I wish to extend my heartfelt gratitude to several individuals whose contributions and support have been invaluable in its preparation and completion.

First and foremost, I express my deepest reverence to the Almighty Lord Mahadev and Maa Saraswati for granting me the courage to face life's complexities, blessing me with this opportunity, and endowing me with the strength to accomplish this significant milestone.

I am profoundly grateful to my thesis supervisor, **Dr. Ashok Ji Gupta**, Department of Mathematical Sciences and my co-supervisor, **Dr. Bhupendra Singh**, Sc 'F', CAIR, DRDO for their unwavering guidance and constant support throughout my research journey. Their insightful feedback and encouragement have inspired me to strive for excellence, and I consider myself privileged to have pursued my doctoral degree under their guidance.

I extend my sincere gratitude to several individuals at the Department of Mathematical Sciences, IIT (BHU), Varanasi. I am especially thankful to Prof. (Retd.) B. M. Pandeya for his consistent motivation and encouragement throughout my research. My heartfelt thanks go to Prof. Sanjay Kumar Pandey, Head of the Department, for providing all the necessary facilities. I also appreciate the support and cooperation of the Department of Mathematical Sciences office staff.

I am indebted to my seniors—Dr. Shiv Kumar, Dr. Sonal Gupta, Dr. Satish Kumar, and Dr. Kaushal Gupta—for their insightful discussions, guidance, and unwavering support. I also thank my fellow researcher, Mr. Mukul Kumar Verma, for his valuable assistance. A special mention goes to my dear friends, Mr. Gaurav, Mr. Krishan Kumar, Mr. Pradeep Yadav, and Dr. Sitaram Yadav, for their constant companionship and unwavering support during my wonderful days on campus. I am

also grateful to my batch-mates and all the research scholars of the department for fostering a positive and collaborative work environment. My heartfelt thanks also go to my friends Dr. Pushpendra Sharma, Mr. Raju Kumar Singh, Mr. Nilesh Kumar, and Mr. Anupam Pathak for their unending support, encouragement, and honest opinions, which gave me the strength to achieve my dreams.

I am deeply indebted to the Indian Institute of Technology (BHU), Varanasi, for providing financial support and the essential resources required for my research. My sincere gratitude also extends to the Centre for Artificial Intelligence & Robotics (CAIR), Defence Research & Development Organization (DRDO), Bengaluru, for their resources and support. I am thankful to Mr. Karthik Srivatsan and Md. Kashif Sharif, CAIR, DRDO, Bengaluru, for the fruitful discussions during my visit to CAIR.

This thesis is dedicated to my parents, the Late Mr. Brijendra Rai and Mrs. Shiv Kumari Rai, whose love, patience, and unwavering support have been the foundation of my success. This achievement would not have been possible without their encouragement and sacrifices. I also express my gratitude to my siblings, Mr. Prabhakar Rai and Mrs. Vibha Rai, for their constant love and support. I am thankful to my cousins—Mr. Alok Sharma, Mr. Ritesh Rai, Mrs. Alisha Sharma, and Mr. Ritik Rai—for standing by me throughout my academic journey.

Lastly, this acknowledgment would be incomplete without mentioning the great visionary Bharat Ratna Pt. Madan Mohan Malaviya, whose vision and efforts led to the establishment of this divine center of knowledge. I express my deepest respect and gratitude to him.

Date: 27/12/2024
Place: Varanasi

PRai

(Pradeep Rai)

Contents

List of Tables

List of Symbols

Symbol	Description
p	Prime number
q	Prime power
$\mathbb{F}_q$	Finite field of order q
$\mathbb{F}_q^*$	Set of nonzero elements of $\mathbb{F}_q$
J	$\{1, 2, 3, 4, 5, 6\}$ (used in Chapter 2)
$\mathcal{S}$	$\mathbb{F}_q[\mathsf{u}, \mathsf{v}, \mathsf{w}]/\langle \mathsf{u}^3 - \mathsf{u}, \mathsf{v}^2 - \mathsf{v}, \mathsf{w}^2 - \mathsf{w}, \mathsf{uv}, \mathsf{vu}, \mathsf{uw}, \mathsf{wu}, \mathsf{vw} - \mathsf{wv}\rangle$
$\mathcal{R}$	$\mathbb{F}_q[u_1, u_2, \ldots, u_r]/\langle u_i^3 - u_i, u_i u_j - u_j u_i\rangle$
$\mathcal{T}$	$\mathbb{F}_q[u_1, u_2, \ldots, u_r]/\langle f_j(u_j), u_i u_j - u_j u_i\rangle$
$\mathcal{U}(R)$	Set of units (whose multiplicative inverse exist) in the ring R
C	Codes over $\mathbb{F}_q$ (except for the codes obtained by decomposition of codes over rings)
$\mathcal{C}$	Codes over rings
$\langle f(y)\rangle$	Ideal generated by $f(y)$
$f^*(y)$	Reciprocal polynomial of $f(y)$
$f^\dagger(y)$	Left monic skew reciprocal polynomial of $f(y)$
$\bar{f}^\dagger(y)$	Hermitian left monic skew reciprocal polynomial of $f(y)$
C	Code over $\mathbb{F}_q$
$\mathcal{C}$	Code over a ring
$a \mid b$	a divides b
$\equiv$	Congruent to
θ	An automorphism of $\mathbb{F}_q$
Θ	An automorphism of ring R, where $R = \mathcal{S}, \mathcal{R}, \mathcal{T}$
$[n, k, d]$	A classical linear code with length n, dimension k, and minimum distance d

Symbol	**Description**
$[[n, k, d]]$	A quantum code with length n, dimension k, and minimum distance d
$[[n, k, d; c]]$	An EAQECCs with length n, dimension k, and minimum distance d using c ebits

Abbreviations

Abbreviation	**Description**
AMDS	Almost Maximum Distance Separable
BKLC	Best Known Linear Code
CSS	Calderbank-Shor-Steane
EAQECC	Entanglement-Assisted Quantum Error-Correcting Code
GCRD	Greatest Common Right Divisor
LCD	Linear Complementary Dual
MDS	Maximum Distance Separable
QECC	Quantum Error-Correcting Code

PREFACE

The theory of error-correcting codes plays a vital role in modern communication systems, ensuring the reliability and efficiency of data transmission across noisy channels. Cyclic codes have emerged as one of the most important classes of error-correcting codes due to their ease of implementation, wide range of applications, and their connection to elegant algebraic structures. In the past few decades, the study of codes over rings has gained significant popularity due to their applications in several modern technologies, such as 5G networks and flash memory systems. This thesis is devoted to the study of certain algebraic codes like cyclic, constacyclic, skew cyclic, and skew constacyclic codes over specific finite non-chain rings. Additionally, it explores their applications in constructing quantum error-correcting codes, which have become increasingly important in the emerging fields of quantum information and computation. Moreover, it examines another significant class of error-correcting codes called linear complementary dual (LCD) codes over these rings.

Throughout this research journey, I have been deeply fascinated by the interplay between algebra, coding theory, and quantum computing. The development of quantum error-correcting codes is critical for realizing practical quantum computers, and this work aims to contribute to this exciting and rapidly evolving field.

This thesis consists of an **Introduction** and **seven chapters**, including **Preliminaries** as the first chapter and **Conclusion and Future Scope** as the last chapter. Chapter 1 provides a comprehensive overview of preliminary concepts, definitions, and results that will be useful for the subsequent chapters.

Introduction gives a general introduction. It also includes an extensive literature review on cyclic codes, their generalizations, and their applications in constructing quantum and LCD codes.

Chapter 1 serves as the foundation of the thesis, introducing essential concepts and definitions from ring theory, classical coding theory, and the theory of quantum error correction.

Chapter 2 studies cyclic codes over a non-chain ring $\mathbb{F}_q[\mathsf{u},\mathsf{v},\mathsf{w}]/\langle \mathsf{u}^3-\mathsf{u}, \mathsf{v}^2-\mathsf{v}, \mathsf{w}^2-\mathsf{w}, \mathsf{uv}, \mathsf{vu}, \mathsf{uw}, \mathsf{wu}, \mathsf{vw}-\mathsf{wv}\rangle$ denoted as $\mathcal{S}$. This chapter discusses the structural properties of cyclic codes over $\mathcal{S}$ and their duals. It establishes some important results on the generator matrix of the Gray image of linear codes over $\mathcal{S}$ and the Gray image of cyclic codes over $\mathcal{S}$. Additionally, it presents the construction of quantum and LCD codes from cyclic codes over $\mathcal{S}$.

Chapter 3 investigates skew cyclic codes over a non-chain ring $\mathbb{F}_q[u_1,u_2,\ldots,u_r]/\langle u_i^3-u_i, u_iu_j-u_ju_i\rangle_{i,j=1}^r$ denoted as $\mathcal{R}$. This chapter examines the structural properties of skew cyclic codes over $\mathcal{R}$ and their duals. Furthermore, it provides methods for constructing quantum and LCD codes from skew cyclic codes over $\mathcal{R}$, leading to the construction of many new codes with improved parameters.

Chapter 4 delves into skew constacyclic codes over a general non-chain ring $\mathbb{F}_q[u_1,u_2,\ldots,u_r]/\langle f_i(u_i), u_iu_j-u_ju_i\rangle_{i,j=1}^r$ denoted as $\mathcal{T}$. It presents several key results on the structural properties of skew constacyclic codes over $\mathcal{T}$. It is proved that the Gray image of a skew constacyclic codes over $\mathcal{T}$ is a skew quasi-$(\alpha_{11\ldots1},\alpha_{11\ldots2},\ldots,\alpha_{l_1l_2\ldots l_r})$-twisted code.

The findings of Chapter 4 are utilized in Chapter 5 to construct quantum and LCD codes. This chapter investigates the Euclidean and Hermitian duals of skew constacyclic codes over $\mathcal{T}$ develop methods for constructing quantum codes from Euclidean and Hermitian dual-containing skew constacyclic codes over $\mathcal{T}$. Moreover, quantum codes over nine different rings (belonging to the class of non-chain rings) are also constructed. Consequently, many new and improved quantum codes are obtained. Moreover, this chapter studies Euclidean and Hermitian skew constacyclic LCD codes over $\mathcal{T}$, leading to the construction of several MDS, AMDS, and BKLCs as Gray images of these codes.

The construction of quantum codes which are discussed in Chapters 2, 3, and 5 requires dual-containing codes. In 2006, Brun [21] proposed the construction of quantum codes using shared entanglement which does not require dual-containing codes. Chapter 6 focuses on the construction of entanglement-assisted quantum error-correcting codes (EAQECCs) from constacyclic codes over $\mathcal{T}$. It is proven that under a polynomial Gray map, the image of constacyclic codes over $\mathcal{T}$ is a

cyclic code. Furthermore, a method to construct EAQECCs from these codes is established, resulting in many new EAQECCs.

Chapter 7 provides a chapter-wise summary of this thesis. It also outlines the future scope of the research in this direction and proposes several open problems for further investigation.

I hope that the results presented in this thesis will not only enhance the understanding of coding theory over finite non-chain rings but also inspire further research into the direction of generalizations of cyclic codes, their study over finite rings and construction of quantum codes from them.

Introduction

Error-correcting codes are fundamental to modern communication systems, ensuring the reliable transmission of information across noisy channels. With the rapid growth of digital communication, including emerging technologies like 5G networks and quantum computing, the study of error-correcting codes has become increasingly important. Among various types of error-correcting codes, cyclic codes have gained significant attention due to their structural simplicity, ease of implementation, and broad range of applications in both classical and quantum contexts.

Over the past few decades, the study of codes over rings has gained substantial traction, particularly in the context of non-chain rings. These algebraic structures provide a rich framework for developing codes with improved properties and enhanced performance. In particular, codes like cyclic, constacyclic, skew cyclic, and skew constacyclic codes over finite rings have been widely studied over the past 15 years. Furthermore, the development of quantum error-correcting codes (QECCs) has become critical for the realization of fault-tolerant quantum computing, making the study of these codes over specialized rings especially relevant.

This thesis investigates various classes of algebraic codes, focusing on their structural properties and their applications in constructing quantum error-correcting codes and linear complementary dual (LCD) codes. The work emphasizes the construction of these codes over finite non-chain rings, presenting novel examples with improved parameters that contribute to existing code databases. By examining these codes in the context of a general non-chain ring structure, this study offers insights that enrich the understanding of algebraic coding theory and its applications to quantum codes.

Literature Survey

Error-correcting codes originated with Claude Shannon's [85] groundbreaking paper "A Mathematical Theory of Communication" in 1948. Shannon introduced the concept of channel capacity and proved that reliable communication is possible over a noisy channel using suitable coding schemes, provided that the transmission rate is below the channel capacity. Although Shannon's work was theoretical and did not provide explicit constructions of error-correcting codes, it laid the foundation for coding theory, which later led to the development of practical coding techniques.

The study of cyclic codes began with a series of technical notes by E. Prange from the Air Force Cambridge Research Laboratory, published between 1957 and 1959 [76, 77, 78, 79]. These foundational works laid the groundwork for understanding cyclic codes' algebraic properties, particularly their ability to be implemented efficiently due to their structure. Building on this early work, in 1961, W. W. Peterson published a comprehensive book [72] that compiled various results on cyclic codes. Peterson's treatise significantly advanced the theory of error correction, establishing cyclic codes as a critical area of research in coding theory. This foundation was further solidified by Peterson and E. J. Weldon in their 1972 book [73], which expanded on cyclic codes and their applications in error correction. Cyclic codes have been further generalized as constacyclic codes by Berlekamp [13].

In the early 1990s, the focus on research in coding theory saw a significant shift with the introduction of Linear Complementary Dual (LCD) codes. LCD codes, first introduced by J. L. Massey in 1992 [69], are linear codes with the property that they intersect trivially with their duals. Massey demonstrated the advantages of LCD codes in terms of error correction and cryptographic security, particularly highlighting their resilience to side-channel attacks and fault injection attacks in cryptosystems [24]. By 1994, Yang and Massey had provided a criterion for a cyclic code over a finite field to be LCD [97]. This characterization became the basis for further studies, where researchers explored LCD codes over various finite rings. Sendrier later demonstrated in 2004 that LCD codes satisfy the Gilbert-Varshamov bound [84], which underscores their efficiency in coding theory.

Parallel to the advancements in classical coding theory, the mid-1990s witnessed the birth of quantum error-correction. In 1995, Peter Shor proposed the first quantum error-correcting code in his landmark paper titled "Scheme for reducing decoherence in quantum memory" [87]. This work laid the foundation for protecting quantum information from decoherence, a significant barrier in developing reliable quantum computers. Building upon Shor's ideas, Steane [89] in 1996 introduced further methods for constructing quantum error-correcting codes (QECCs). The development of QECCs saw a breakthrough in 1998 when Calderbank et al. [22] described a systematic method for creating quantum codes using self-orthogonal classical linear codes over finite fields. This method, later known as the CSS (Calderbank-Shor-Steane) construction, allowed for the efficient design of quantum codes that could correct quantum errors induced by various types of noise.

The late 1990s and the early 2000s were marked by significant contributions to the theory of quantum error-correction. In 1999, Rains [83]extended the study of quantum codes by generating numerous non-binary quantum maximum distance separable (MDS) codes, which are optimal in terms of error correction capabilities. This work was pivotal in establishing the framework for quantum codes that meet the quantum Singleton bound, a quantum analogue of the classical Singleton bound. Grassl et al. [40] further advanced the field in 2004 by constructing various categories of quantum MDS codes over finite fields. These developments inspired a series of works by researchers like Ashikhmin [5], Ketkar [54] and Aly [4] who explored the use of classical linear codes over finite fields to design robust quantum codes.

During the same period, research on classical codes extended beyond finite fields to include rings. In 1994, Hammons et al. [43] showed the existence of many good non-linear binary codes using the Gray map. Qian et al. [81] introduced the initial method for constructing quantum codes from cyclic codes of odd length over the finite chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$. Motivated by these studies many researchers obtained quantum codes using cyclic and constacyclic codes which either contain their dual (dual-containing) or contained in their dual (self-orthogonal) over various chain and non-chain rings [3, 6, 7, 8, 10, 12, 27, 29, 30, 36, 37, 39, 49, 50, 52, 55, 58, 66, 67, 80, 91, 95].

The study of LCD codes also expanded to finite rings in the mid-2010s. Researchers began exploring the structure of LCD codes over chain rings, as seen in the works of

Durgun [33] and Liu [63]. In 2021, Islam and Prakash [51] constructed new LCD and quantum codes by imposing conditions on cyclic codes over the ring $\mathbb{F}_q[u,v]/\langle u^2-\alpha u, v^2-1, uv-vu\rangle$. Ali et al. [3] extended this line of research by studying cyclic codes over rings such as $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, which led to the construction of new quantum and LCD codes.

Skew polynomial rings as a generalization of polynomial rings were introduced by Ore in [70]. As a generalization of cyclic codes, Boucher et al. [18] developed the idea of skew-cyclic codes or θ-cyclic codes in 2007, where θ is an automorphism of the finite field being used as code alphabet. It is interesting to observe that for an automorphism θ, skew θ-cyclic codes of length n over $\mathbb{F}_q$ can be identified as left submodules in $\mathbb{F}_q[y;\theta]/\langle y^n-1\rangle$. Here $\mathbb{F}_q[y;\theta]$ is a non-commutative in general and called a skew polynomial ring. In $\mathbb{F}_q[y;\theta]$ addition operation is the usual addition of polynomials and multiplication is defined using the rule $y * ay = \theta(a)y^2$. Skew constacyclic codes over finite chain rings have been investigated by Jitman et al. [53]. Motivated by the study of skew cyclic codes over a finite field, Abularab et al. [1] provided a study of skew cyclic codes over the ring $\mathbf{F}_2 + v\mathbf{F}_2$, where $v^2 = v$. In 2014, Li [56] studied skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ with $v^2 = 1$. Further, skew cyclic codes over $\mathbf{F}_q + v\mathbf{F}_q$ were investigated by Gao and Gursoy [42] using two different automorphisms. Yao et al.[98] described the structural properties of skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. Moreover, they provided a formula for the number of skew cyclic codes under certain conditions. Irwansyah et al. [48] studied Θ_S-cyclic codes over a class of non-chain rings A_k. Later, a more general class of non-chain rings B_k was taken into consideration to study skew cyclic codes by Irwansyah et al. [47]. In 2019, Özen et al. [71] derived the conditions for a skew cyclic code over $\mathbb{F}_q$ to be self-orthogonal and dual-containing. Further a rectified version of this criterion was introduced by Bag et al. [11]. Quantum codes have been constructed from skew constacyclic codes over various finite rings and mixed alphabets in [10, 11, 28, 31, 57, 74, 92, 93, 94].

In 2020, Bharadwaj et al. [15], studied skew constacyclic codes over the ring $\mathbb{F}_q[u,v]/\langle f(u), g(v), uv-vu\rangle$ and provided some important results concerning these codes. Being inspired by this study, Prakash et al. [75] provided methods to construct quantum codes from Euclidean and Hermitian dual-containing skew constacyclic codes over the same ring [15]. They also obtained Euclidean and Hermitian

LCD codes and provided many good examples. Recently in 2024, Bharadwaj et al. [14] explored constacyclic codes over a general class of non-chain rings, constructing quantum codes from dual-containing constacyclic codes. This work inspired us to extend these concepts to skew constacyclic codes, presenting methods for constructing quantum codes from both Euclidean and Hermitian dual-containing skew constacyclic codes over this general class of non-chain rings. The focus on non-chain rings has opened new avenues for the development of quantum and LCD codes, leveraging the rich algebraic structures of more generalizations of cyclic codes to achieve codes with better parameters.

In 2006, Brun et al. [21] introduced the concept of entanglement-assisted quantum error-correcting codes (EAQECCs), demonstrating that EAQECCs can be built using any classical linear codes, provided the sender and receiver share pre-established entangled ebits. This construction does not require the dual-containing condition. Following this breakthrough, numerous researchers have developed EAQECCs with favorable parameters [34, 61]. An $[[n, k, d; c]]$ EAQECC can encode k information qubits into n channel qubits with the help of c pairs of maximally entangled states and correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors, where d is the minimum distance of this code. By entanglement-assisted (EA) quantum singleton bound [21], for any EAQECC with , its parameters $[[n, k, d; c]]$, $d \leq \frac{n+2}{2}$ satisfy $2(d-1) \leq n-k+c$, where $0 \leq c \leq n-1$. If an EAQECC attains EA quantum Singleton bound, it is called a *maximum distance separable* EAQECC (MDS EAQECC). The construction of MDS EAQECCs has attracted the attention of many researchers. Recently, Guenda et al. [41] proved that the parameter c of an $[[n, 2n-k+c, d; c]]_q$ EAQECC can be determined by the dimension of the Euclidean hull (or Hermitian hull) of an $[n, k, d]_q$ linear code. Different from Guenda's method, Lu et al. [64] proposed a decomposition of the defining set of constacyclic codes and constructed four classes of MDS EAQECCs with less pre-shared maximally entangled states. Afterward, many researchers have constructed some classes of MDS EAQECCs [38, 44, 59, 65, 82]. Hence, it is interesting to construct EAQECCs from constacyclic codes over a general non-chain ring.

Motivation

The theory of error-correcting codes has long been a cornerstone in the fields of digital communication and information theory, with cyclic codes standing out due to their elegant algebraic structure and practical implementation. Since their introduction by Prange in the late 1950s [76], cyclic codes have been extensively studied and have found applications in various domains, including data transmission, storage systems, and cryptographic protocols. These codes, traditionally studied over finite fields, are well-known for their ability to detect and correct errors efficiently.

However, as the demands for reliable communication have grown, so has the need for more robust and versatile coding schemes. This has led researchers to explore the potential of codes over more general algebraic structures, such as finite rings. The motivation to study codes over rings arises from their rich algebraic properties, which provide new avenues for constructing codes with improved error-correcting capabilities. For instance, the work of Hammons et al. [43] demonstrated that some powerful non-linear codes, which are equivalent to linear codes over certain rings, could outperform classical codes over fields when mapped via the Gray map.

Moreover, the extension of classical coding theory to ring structures has opened up new possibilities for constructing quantum error-correcting codes (QECCs). Quantum computation and communication are inherently prone to errors due to the fragile nature of quantum states, necessitating efficient QECCs to protect information against decoherence and quantum noise. Researchers like Qian [81] have shown that codes over finite rings can serve as a rich source of quantum codes, leading to advancements in quantum information theory.

In addition to their applications in quantum coding theory, codes over rings, particularly Linear Complementary Dual (LCD) codes, have gained attention due to their utility in cryptography. LCD codes, first introduced by Massey [69], provide effective countermeasures against side-channel attacks and fault injection attacks, which are critical for the security of cryptographic systems. The study of LCD codes over rings has further revealed that such codes can meet or exceed the bounds achieved by their counterparts over fields, making them attractive for secure communications [24].

Despite these promising developments, the theory of codes over rings is still not as much developed as its counterpart over finite fields. Many open questions remain regarding the classification, construction, and optimization of these codes. Furthermore, recent works have highlighted the potential of using skew-cyclic and skew-constacyclic codes over rings, which used the concept of automorphisms to introduce new algebraic structures and have shown promise in both classical and quantum coding contexts [18, 88].

Given the increasing complexity of modern communication systems and the rising need for robust error correction, there is a compelling need to further investigate the algebraic properties of codes over rings. This research aims to contribute to this growing field by exploring the constructions of cyclic, skew-cyclic, and LCD codes over various classes of finite rings, with the goal of finding new and better quantum codes.

Therefore, the motivation for this thesis is driven by the dual goals of advancing theoretical knowledge in the area of coding theory over rings and their application in the construction of quantum and LCD codes.

Thesis Objectives

The objective of this thesis is to explore the theory and applications of algebraic codes, specifically cyclic, constacyclic, skew cyclic, and skew constacyclic codes, over finite non-chain rings. The research aims to investigate the structural properties of these codes and their duals, focusing on their role in the construction of quantum error-correcting codes and LCD codes. This work aims to develop new methods for constructing quantum and LCD codes from these algebraic structures, contributing to the advancement of quantum computing and communication systems. Additionally, we aim to extend the study of entanglement-assisted quantum error-correcting codes (EAQECCs) derived from constacyclic codes. Through these efforts, the research aspires to enhance the understanding of coding theory over finite rings and provide novel contributions to the development of fault-tolerant quantum computing systems.