Group ring and its Application in the Construction of Some Extremal Self-dual codes

A Thesis
Submitted for the award of degree of
Doctor of Philosophy
in Mathematics
by

Shefali Gupta
(2K18/PHD/AM/11)

Under the supervision of
Dr. Dinesh Udar

Department of Applied Mathematics
Delhi Technological University
Bawana Road, Delhi 110042 (India)

17 November 2024

To my parents and husband, they were like pillars throughout my entire journey. Thank you for all your support and guidance. Without their help, it wouldn't have been possible.

Certificate

Department of Applied Mathematics
Delhi Technological University, Delhi

This is to certify that the research work embodied in the thesis entitled "Group ring and its Application in the Construction of Some Extremal Self-dual codes" submitted by Shefali Gupta (2K18/PHD/AM/11) is the result of her original research carried out in the Department of Applied Mathematics, Delhi Technological University, Delhi, for the award of **Doctor of Philosophy** under the supervision of **Dr. Dinesh Udar**.

It is further certified that this work is original and has not been submitted in part or fully to any other university or institute for the award of any degree or diploma.

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

Date: 17 November 2024
Place: Delhi , India

Dr. Dinesh Udar
(Supervisor)

Prof. R. Srivastava
(Head of Department)

Declaration

I declare that I worked under the guidance of ***Dr. Dinesh Udar*** at the Department of Applied Mathematics, Delhi Technological University, Delhi, India, to complete the research work described in this thesis entitled, "**Group ring and its Application in the Construction of Some Extremal Self-dual codes**" to be awarded the degree of ***Doctor of Philosophy in Mathematics***. Also, I declare that I have previously submitted none of this thesis work in whole or in part to any other college or institute for the award of any degree or diploma.

I certify that this thesis is an expression of my views in my own words. When I have borrowed another person's thoughts or words, I have properly acknowledged and referenced the sources. In addition, I affirm that I have followed all rules governing academic honesty and integrity and have not created or manipulated any idea, data, or source in my work.

Shefali Gupta

Date: 17 November 2024 (2K18/PHD/AM/11)

Acknowledgements

I had a tonne of support and help throughout my studies from many people. I want to take this chance to thank every one of them.

First, I want to thank my supervisor, Dr. Dinesh Udar, for his patient instruction and steadfast confidence in me. I feel privileged that he has given his time and knowledge to my Ph.D. experience. I am tremendously fortunate to have a supervisor who cares about his students and encourages them to pursue their career and personal ambitions.

I want to express my profound gratitude to Prof. Sangita Kansal, DRC Chairperson, Department of Applied Mathematics, DTU, for her inspiring leadership. I also want to thank the Head of the Department, Prof. R. Srivastava, and other department faculty members for giving me all the resources required for my research work. I also want to thank the Department of Applied Mathematics office staff for all of their help.

Finally, I want to express my gratitude to my parents for their unwavering love and assistance. Their ongoing comfort and inspiration are responsible for my successes and triumphs. My husband deserves heartfelt thanks for his unwavering support and concern for my research. The completion of this long journey wouldn't have been possible without his help. Also, I wish to thank my parents-in-law for supporting me to continue my research work.

At last, I want to express my gratitude to the Almighty God for his unending blessings and for directing me in the proper direction to finish this Ph.D. thesis.

Shefali Gupta

DTU Delhi

Abstract

In this thesis, the new construction of extremal Type I and Type II self-dual codes of various lengths has been done using the group ring. Due to the numerous theoretical and practical applications of group rings and algebraic coding theory in cryptography and error correction, these topics have received much research attention. The thesis is divided into seven chapters. Chapter 1 includes relevant definitions and concepts from the literature that are pertinent to the topics employed in this thesis.

The second chapter focuses on constructing extremal self-dual codes of length 16. For the first time, they are generated using the unitary units in a group ring with the Quaternion group. Various code modification techniques are being applied in the correct order to self-dual codes, which improves the rates (ratio of information symbol to code length) and error-handling capacity of the code.

Chapter three focuses on a new construction for self-dual codes that uses the concept of double-bordered construction, group rings, and reverse circulant matrices. Using groups of orders $2, 3, 4$, and 5, and by applying the construction over the binary field F_2 and the ring $F_2 + uF_2$, an extremal binary self-dual codes of various lengths: $12, 16, 20, 24, 32, 40$, and 48 are obtained. The significance of this new construction is the construction of the unique Extended Binary Golay Code $[24, 12, 8]$, and the unique Extended Quadratic Residue $[48, 24, 12]$ Type II linear block code. Moreover, the existing relationship between units and non-units with the self-dual codes presented in (23) is also strengthened by limiting the conditions given in the corollaries of (23). Additionally, a relationship between idempotent and self-dual codes is also established.

In chapter four the concept of $\frac{n}{r}$-th borders around the matrix is introduced. Here n and r are the natural numbers such that r divides n. We have shown that this construction is efficacious for any groups of order r (where r is a natural number such that r divides n), over the Frobenius ring R_k. We discover extremal binary self-dual codes of lengths 32, 40, the well-known Extended Binary Golay Code, i.e., [24, 12, 8], and Extended Quadratic Residue Code, i.e., $[48, 24, 12]$ by two different ways.

In chapter five, we introduce the double-bordered construction of self-dual codes whose generator matrix is of the form $M = [I_n|A]$ where A is a block matrix consisting of blocks that come from group rings and the elements in the first row cannot completely determine the block matrix A. We demonstrate that this construction is feasible for a group of order $2n$ where n is a natural number, over the Frobenius ring R_k. We show the significance of this new construction by constructing several extremal self-dual codes of lengths 20, 40, 32, and 64 over the field F_2 and the ring $F_2 + uF_2$.

Chapter six focuses on the new technique for the construction of self-dual codes. Double borders are introduced around a new altered form of a four-circulant matrix. Using this new construction over the field F_2 and the ring $F_2 + uF_2$ and groups of orders $2, 3, 4, 5, 7$, and 9, we generate extremal binary self-dual codes of the following lengths: $12, 20, 24, 32, 40, 48, 64$, and 80.

In chapter seven we introduce a new class of ring, which is the $*$-version of the semiclean ring, i.e., the $*$-semiclean ring. A $*$-ring is $*$-semiclean if each element is the sum of a $*$-periodic element and a unit. Many properties of $*$-semiclean rings are discussed. It is proved that if $p \in P(R)$ such that pRp and $(1-p)R(1-p)$ are $*$-semiclean rings, then R is also a $*$-semiclean ring. As a result, the matrix ring $M_n(R)$ over a $*$-semiclean ring is $*$-semiclean. A characterization that when the group rings RC_r and RG are $*$-semiclean is done, where R is a finite commutative local ring, C_r is a cyclic group of order r, and G is a locally finite abelian group. We have also found sufficient conditions when the group rings RC_3, RC_4, RQ_8, and RQ_{2n} are $*$-semiclean, where R is a commutative local ring. We have also demonstrated that the group ring $\mathbb{Z}_2 D_6$ is a $*$-semiclean ring (which is not a $*$-clean ring). We have characterized the $*$-semicleanness of F_qG in terms of LCD and self-orthogonal abelian codes under the classic involution, where F_q is a finite field with q elements and G is a finite abelian group.

Table of Contents

List of Figures

List of Tables

List of Symbols

Set Theory

$\mathbb{N}$	the set of natural numbers

Group and Ring Theory

G	the group
R	the ring
RG	the group ring
v	an element of RG
$\sigma(v)$	the group ring matrix of an element $v \in RG$
F	the field
$\bar{F}$	the algebraic closure of F
F_q	the finite field with q elements
$\mathbb{Z}$	the ring of integers
C_i	the cyclic group of order i
$F_2 + uF_2$	$= \{a + bu \mid a, b \in F_2, u^2 = 0\}$
$M_n(R)$	matrix ring of $n \times n$ matrices over R
S_n	the symmetric group of order $n!$
D_{2n}	the dihedral group of order $2n$
Q_{2n}	the quaternion group of order $2n$
$J(R)$	the jacobson radical of R

$U(R)$	the group of all units of R
$I(R)$	the set of all idempotents of R
$N(R)$	the set of all nilpotents of R
$P(R)$	the set of all projections of R
$Pri^{*}(R)$	the set of all $*$-periodic elements of R
R_k	the commutative Frobenious ring with characteristic 2
$\mathbb{Z}_p$	the ring of integers modulo p
$\mathbb{Z}_{(p)}$	the localization of $\mathbb{Z}$ at the prime ideal generated by p
I	an ideal
R/I	the factor ring
$R[x]$	the polynomial ring
$R[[x]]$	the power series ring
$\hat{G}$	$= \{\phi \mid \phi : G \to \bar{F}$ a homomorphism$\}$
$End(N)$	the endomorphism of the module N
ξ	the augmentation mapping
$V(RG)$	the set of normalized units of RG
$V_{*}(RG)$	the set of unitary units of RG

Coding Theory

$\mathfrak{C}$	the linear code
M_σ	the generator matrix of the code $\mathfrak{C}_\sigma$
QR	the Quadratic Residue Code
$d(a,b)$	$\lvert\{\, i \mid 1 \leq i \leq n,\ a_i \neq b_i \,\}$
d_{min}	$\min\{\, d(a,b) \mid a \neq b\}$
$w(a)$	the weight of a codeword a

d_L	the Lee distance of the code $\mathfrak{C}$
$d_H(\mathfrak{C})$	the hamming distance of the code $\mathfrak{C}$
$\mathfrak{C}^\perp$	$= \{\mathbf{l} \in R^n \mid < \mathbf{l}, \mathbf{m} >_E = 0 \ \forall \mathbf{m} \in \mathfrak{C}\}$
$Aut(\mathfrak{C})$	the order of the automorphism group of $\mathfrak{C}$
UC_i	the unique divisible self-dual codes
UCM_i	the generator matrix of the code UC_i
PC_i	the linear punctured code
mds	the maximum distance separable code
C_{ext}/EX_i	the linear extended code
CJ	the juxtapose code
w	the message
E/E_i	the encoded message
e	the error
r	the received vector
q	the decode message
Q	the parity check matrix
s	the syndrome

Matrices

C	the reverse circulant matrix
$det(A)$	the determinant of the matrix A
I_n	the identity matrix of $n \times n$ order
T	the idempotent matrix
f_A	the first row of the matrix A

Chapter 1

Introduction

"This chapter presents a brief review of the past and present developments in the field of Algebraic Coding Theory. This chapter introduces definitions, ideas, and techniques that we will require in our later chapters."

Coding theory studies code properties and aims to ensure error-less communication through noisy channels. The books "Algebraic Codes for Data Transmission" by Richard (4) and "Fundamentals of Error-Correcting Codes" by Huffman (32) serve as the primary source of information on the coding theory presented here.
In the study and development of error-correcting codes up until now, algebra has been a significant factor. In 2009, Ted and Paul Hurley (34) introduced the concept of codes from zero divisors and units in group rings. The algebraic structures that are pertinent to the research are defined throughout the chapter. The goal is to make the explanation of codes in later chapters easier.

1.1 Preliminaries

In this section, we recall some definitions and theorems related to abstract algebra and coding theory that will interest the whole thesis. Throughout the thesis, in code construction, we will assume all rings are finite, commutative, and Frobenius rings with a multiplicative identity.

1.1.1 Groups, Rings, and Fields

The definitions of the terms ’group’ and ’ring’ from abstract algebra are assumed to be familiar to the reader. Additionally, the reader is assumed to know the common defini-

tions, theorems, and terms connected with groups, rings, and fields. All these definitions and theories can be found in any standard algebra book, such as Contemporary Abstract Algebra, by Joseph A. Gallian, see (20). In this thesis, the term F_2 stands for the smallest finite field with two elements, and the standard notation $G =<$ generators | relation $>$ is used to denote a group G, where the term, "generators" is a list of the group's generators and "relations" is a list of combinations of the generators that equal the group's identity. Throughout the thesis, we will take only finite groups.
Now we will define some of the terms used in the study of linear algebra.

1.1.2 Modules, Submodules, Vector Spaces, and Subspaces

Let $R(+, \times)$ be a ring and $(G, \star)$ be a commutative group. Then under an operation $\circ : R \times G \to G$, the group G is called left module over R if the following axioms are satisfied:

1. $(a + b) \circ g = (a \circ g) + (b \circ g)$.
2. $a \circ (g \star h) = (a \circ g) \star (a \circ h)$.
3. $(a \times b) \circ g = a \circ (b \circ g)$.
4. $1 \circ g = g$.

Here, a, b are arbitrary elements of R, and g, h are arbitrary elements of G.
Similarly, a group G is called the right module over R if it satisfies all the above four axioms under an operation $\circ : G \times R \to G$ with the relevant changes to the order of the group and ring elements in the four axioms.
A non-empty subset $H \subset G$ is called a submodule (or R-submodule) of G if H is a subgroup of the additive group of G that is closed under scalar multiplication.
A vector space is a module over a field (41, p. 193). A subspace of a vector space is a submodule of it (50, p. 78).

1.1.3 Basis and Dimensions

Let V be a vector space. A set of vectors in V, say B is called the basis of V if every element of the vector space V can be written as a unique finite linear combination of elements of the set B.
The number of elements in the basis of the vector space is called the dimension of the vector space.

1.1.4 Group rings and Ring of matrices

Let R be a ring and G be a group of order n. Then the elements of the group ring RG are of the form $\sum_{i=1}^{n} \alpha_i g_i$, $\alpha_i \in R$, $g_i \in G$. In a group ring, the cardinality of the ring and the group can be infinite, but in our construction of codes, we will consider both the ring and the group of finite cardinality.

The addition of the two elements of the group rings is defined coordinate-wise, i.e.,

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i.$$

The product of the two elements of the group rings is defined by

$$(\sum_{i=1}^{n} \alpha_i g_i)(\sum_{j=1}^{n} \beta_i g_i) = \sum_{i,j} \alpha_i \beta_j g_i g_j.$$

The book "An Introduction to Group Rings" by Milies and Sehgal (50) contained detailed information about group rings.

In 2006, T. Hurley was the first to introduce the relationship between group rings and rings of matrices.

Theorem 1.1.1. *(33) Let R be a ring, $G = \{g_1, g_2, \cdots, g_n\}$ be the finite group of order n, and $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n$ be an element of the group ring RG. Then there exists a bijective ring homomorphism $\sigma : v \to \sigma(v)$ between the group ring RG and the matrix $\sigma(v)$ of $n \times n$ order over R.*

The matrix is

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1} g_1} & \alpha_{g_1^{-1} g_2} & \cdots & \alpha_{g_1^{-1} g_n} \\ \alpha_{g_2^{-1} g_1} & \alpha_{g_2^{-1} g_2} & \cdots & \alpha_{g_2^{-1} g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1} g_1} & \alpha_{g_n^{-1} g_2} & \cdots & \alpha_{g_n^{-1} g_n} \end{pmatrix}.$$

Example 1.1.2. *The Cyclic group is defined as $G = C_n = \{ z \mid z^n = 1 \}$ such that $v = \alpha_0 + \alpha_1 z + \alpha_2 z^2 + \cdots + \alpha_{n-1} z^{n-1} \in RC_n$, here $(\alpha_i,\ i = 1 \text{ to } n-1) \in R$. Then by Theorem 1.1.1, we have $\sigma(v) = circ\begin{bmatrix}\alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1}\end{bmatrix}$.*

Example 1.1.3. *(9) The Quaternion group is defined as $G = Q_8 = \{x, y \mid x^4 = 1, x^2 = y^2, xy = y^{-1}x\}$ such that $v = \sum_{j=0}^{3} x^j(\alpha_j + \alpha_{j+4} y) \in F_{2^k} Q_8$, here $\alpha_j, \alpha_{j+4} \in F_{2^k}$. Then by Theorem 1.1.1, we have, $\sigma(v) = \begin{bmatrix} A & B \\ C & A^T \end{bmatrix}$, where $A = circ\begin{bmatrix}\alpha_0 & \alpha_1 & \alpha_2 & \alpha_3\end{bmatrix}$, $B = circ\begin{bmatrix}\alpha_4 & \alpha_5 & \alpha_6 & \alpha_7\end{bmatrix}$, and $C = circ\begin{bmatrix}\alpha_6 & \alpha_5 & \alpha_4 & \alpha_7\end{bmatrix}$.*

1.1.5 Linear codes

A linear code $\mathfrak{C}[n, k, d]$ is a k-dimensional subspace of the vector space F^n of all n-tuples over a finite field F. The elements of $\mathfrak{C}$ are called codewords. A linear code $\mathfrak{C}[n, k, d]$ is defined by three parameters namely 'n' length, 'k' dimension, and 'd' minimum distance. The two parameters 'k' and 'd' of a code are important as they are directly proportional to the rate and error-correction capability of a code. The linear combination of codewords of the code $\mathfrak{C}$ is also a codeword of code $\mathfrak{C}$ over F. The code over the field F_2 is called binary code.

1.1.6 Minimum distance

The minimum distance of the code $\mathfrak{C}[n, k, d]$ is defined as $d_{min} = \min\{ d(a, b) \mid a \neq b\}$ for $\mathfrak{C}$. Here, $d(a, b) = |\{ i \mid 1 \leq i \leq n, a_i \neq b_i \}|$, where $a = (a_1, a_2, \cdots, a_n), b = (b_1, b_2, \cdots, b_n) \in F_2^n$ are the codewords for the code $\mathfrak{C}$. The elements a_i are called the components of the codeword. The more the minimum distance more will be the error-correction capability of a code.

1.1.7 Generator matrices

Code can be described in terms of a generator matrix. The generator matrix of the linear code $\mathfrak{C}[n, k]$ is a $k \times n$ matrix for which rows form a basis of $\mathfrak{C}$. The standard form of a generator matrix is $M = [I_k|A]$, where I_k is the $k \times k$ identity matrix and A is the matrix of order $k \times n - k$, see (48, Theorem 5.5). The null space of a generator matrix is called the dual code of the code $\mathfrak{C}$.

1.1.8 Self-dual codes

The Euclidean inner product between two elements, says $\mathbf{l} = \{l_1, l_2, \cdots, l_n\}$ and $\mathbf{m} = \{m_1, m_2, \cdots, m_n\}$ of R^n, is given by $< \mathbf{l}, \mathbf{m} >_E = \sum l_i m_i$. The dual $\mathfrak{C}^\perp$ of code $\mathfrak{C}$ is defined as

$$\mathfrak{C}^\perp = \{\mathbf{l} \in R^n | < \mathbf{l}, \mathbf{m} >_E = 0 \ \forall \mathbf{m} \in \mathfrak{C}\}.$$

If $\mathfrak{C} \subseteq \mathfrak{C}^\perp$, then the code $\mathfrak{C}$ is said to be self-orthogonal, and if $\mathfrak{C} = \mathfrak{C}^\perp$, then the code $\mathfrak{C}$ is said to be self-dual. Throughout the chapters, two types of binary self-dual codes are built: Type I and Type II. The binary self-dual code $\mathfrak{C}$ is said to be of Type I if the weight of all its codewords is divisible by two, and of Type II if the weight of all its codewords is divisible by four.

Theorem 1.1.4. *(49) Let $d_I(n)$ and $d_{II}(n)$ represent the minimum distance of Type I and Type II codes of length n, respectively. Then*

$$d_{II} \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$$

and

$$d_I \leq \begin{cases} 4\left\lfloor \frac{n}{24} \right\rfloor + 4 & if n \not\equiv 22 (mod\, 24) \\ 4\left\lfloor \frac{n}{24} \right\rfloor + 6 & if n \equiv 22 (mod\, 24). \end{cases}$$

Self-dual codes that attain these bounds are known as extremal self-dual codes. For more details on self-dual codes over the Frobenius ring, see (13), (16), (51), and (52).

1.1.9 Equivalent codes

Two codes are equivalent if one can be obtained from another by reordering the component of the code. If one matrix is obtained from another matrix by column permutation then the resultant codes from both matrices are equivalent. Codes that are equivalent share the same length, size, and minimum distance.

1.1.10 Ring $F_2 + uF_2$

The commutative Frobenius ring with characteristic 2 is denoted by R_k. For $k \geq 1$, the ring R_k is defined as

$$F_2[u_1, u_2, \cdots, u_k]/\langle u_1^2, u_2^2, \cdots, u_k^2 \rangle,$$

such that $u_i u_j = u_j u_i,\ 1 \leq i \neq j \leq k$. The ring R_k can be recursively expressed as

$$R_k = R_{k-1} + u_k R_{k-1}.$$

In the thesis, we will do all the computational calculations for generating self-dual codes over the ring $F_2 + uF_2$. The ring $F_2 + uF_2$ or R_1 is defined as a commutative Frobenius ring of characteristic 2 with the 4 elements $0, 1, u$, and $1 + u$ and the condition that $u^2 = 0$. The ring $F_2 + uF_2$ is isomorphic to $F_2[X]/\langle X^2 \rangle$ and is represented as

$$F_2 + uF_2 = \{a + bu | a, b \in F_2, u^2 = 0\}.$$

The Lee weights of the elements $0, 1, u$, and $1 + u$ of the ring $F_2 + uF_2$ are $0, 1, 2$, and 1 respectively.

The Gray map ϕ is a map defined from $(F_2 + uF_2)^n$ to F_2^{2n} in such a way that $\phi(a + bu) = (b, a + b)$, where $a, b \in F_2$. This is a distance-preserving mapping, which means that the Lee distance d_L of a code $\mathfrak{C}(n, 2^k, d_L)$ over $(F_2 + uF_2)^n$ equals the Hamming distance d_H of a code $\phi(\mathfrak{C})(2n, k, d_H)$.

Theorem 1.1.5. *The Gray image of a linear self-dual code $\mathfrak{C}$ of length n over $F_2 + uF_2$ is a binary linear self-dual code $\phi(\mathfrak{C})$ of length $2n$.*

The natural projection Ω from $F_2 + uF_2$ to F_2 is defined as follows:

$$\Omega : F_2 + uF_2 \to F_2, \quad \Omega(a + bu) = a.$$

Let $\mathfrak{C}$ be a linear code over $F_2 + uF_2$ and $B = \Omega(\mathfrak{C})$. Then B is a projection of $\mathfrak{C}$ into F_2 and $\mathfrak{C}$ is a lift of B into $F_2 + uF_2$. The projection of a self-orthogonal code is always self-orthogonal, but the projection of a self-dual code need not be self-dual. For more details on R_k, see (12), (14), and (15).

1.2 Literature review and Historical context

As one of the most well-known families of codes, self-dual codes have drawn much attention from the coding theory community. These codes have drawn the attention of numerous academics due to their connections to lattices, cryptography, and combinatorial objects like designs and association schemes. Among the self-dual codes, the classification of extremal binary self-dual codes is a topic of active research, since the extremal binary self-dual codes attain the maximum distance for the code of a particular length.
Since 1960, the construction of self-dual is an area of great interest for researchers. In 1969, both Chen (6) and Karlin (36) introduced the concept of a pure double circulant method for building extremal self-dual codes. The classical technique for the construction of self-dual codes is to consider the generator matrix of the form $M = [I_n|A]$, here I_n is the $n \times n$ identity matrix and A is a $n \times n$ circulant matrix satisfying the condition $AA^T = -I_n$. This technique was modified further by introducing the border around the matrix A, that is, by replacing the matrix A with the matrix of the form

$$\left[\begin{array}{c|ccc} \alpha & \gamma & \cdots & \gamma \\ \hline \gamma & & & \\ \vdots & & B & \\ \gamma & & & \end{array}\right].$$

Here B is a $(n-1) \times (n-1)$ circulant matrix, and α and $\gamma \in R$. Since their introduction, these approaches have been widely utilized to create self-dual codes (25) and (26). This approach was broadened in (22) to consider matrices A that result from group rings, that is considering the generator matrix of the form $M = [I_n|\ \sigma(v)]$, here $\sigma(v)$ is a group ring matrix of $n \times n$ order. In 2019, Steven T. Dougherty further modified this construction by introducing a border to a matrix I_n and the group ring matrix A in the quest for some more new extremal self-dual codes of various lengths. The generator matrix for which is defined as

$$M = \left[\begin{array}{c|ccc|c|ccc} \alpha & \gamma & \cdots & \gamma & \beta & \delta & \cdots & \delta \\ \hline \gamma & & & & \delta & & & \\ \vdots & & I_n & & \delta & & \sigma(v) & \\ \gamma & & & & \delta & & & \end{array}\right].$$

In 2020, Joe Gildea extended this concept by introducing the concept of double-bordered construction. He defined the generator matrix of the form

$$M = \left[\begin{array}{cc|cccccc|cc|cccccc} \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_3 & \beta_4 & \cdots & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \cdots & \beta_7 & \beta_8 & \cdots & \beta_8 \\ \beta_2 & \beta_1 & \beta_4 & \cdots & \beta_4 & \beta_3 & \cdots & \beta_3 & \beta_6 & \beta_5 & \beta_8 & \cdots & \beta_8 & \beta_7 & \cdots & \beta_7 \\ \hline \beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \beta_3 & \beta_4 & & & & I_n & & & \beta_7 & \beta_8 & & & & \sigma(v) & & \\ \beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & & \end{array}\right].$$

In 2003, Betsumiya (3) gave the four-circulant construction method for building extremal binary self-dual codes over rings. The generator matrix M for this is of the form

$$M = \left[\begin{array}{cc|cc} I_n & & A & B \\ & I_n & B^T & A^T \end{array}\right].$$

Here, A and B are the circulant matrices of $n \times n$ order satisfying the condition $AA^T + BB^T = -I_n$ over the ring. If the ring is of characteristic 2, then the condition for the generation of self-dual code is redefined as $AA^T + BB^T = I_n$. Several modifications of this technique are also done in the literature, one of them is replacing both the matrices A and B with the group ring matrices $\sigma(v_1)$ and $\sigma(v_2)$, where v_1 and v_2 are the elements of the group ring.

In the upcoming chapters, we will use the concepts mentioned above and blend them in such a way that the new resultant generator matrix can construct those extremal self-dual codes that cannot be obtained by the generator matrix at the individual level and one of the significant contributions is the construction of the Extended Binary Golay and the Extended Quadratic Residue Code as both these codes have numerous applications. Under this construction, we establish the link between units/non-units and idempotents in the group ring and corresponding self-dual codes. Using this connection for some particular examples of groups over the field F_2 and the ring $F_2 + uF_2$ we can construct many extremal binary self-dual codes of different lengths.

1.3 Chapter-by-chapter summary of the thesis

The thesis is divided into seven chapters, the contents of which are as follows:

Chapter 1 consists of basic definitions, basic concepts of algebra, coding theory, and the preliminaries of the results obtained in the literature. We then provide a brief review of the algebraic coding theory. We will discuss how group rings can generate the extremal self-dual codes.

Chapter 2 focuses on the construction of extremal self-dual codes of length 16. For the first time, they are generated using the unitary units in a group ring with the Quaternion group. Various code modification techniques are being applied in the correct order to self-dual codes, resulting in a significant improvement in the rates (ratio of information symbol to code length) and error-handling capability of the code.

Chapter 3 deals with the building self-dual codes that use the concept of double-bordered construction, group rings, and reverse circulant matrices. Using groups of orders $2, 3, 4,$ and 5, and by applying the construction over the binary field F_2 and the ring $F_2 + uF_2$, we obtain extremal binary self-dual codes of various lengths: $12, 16, 20, 24, 32, 40,$ and 48. In particular, we show its significance by constructing the unique Extended Binary Golay Code $[24, 12, 8]$ and the unique Extended Quadratic Residue $[48, 24, 12]$ Type II linear block code. Moreover, we strengthen the existing relationship between units and non-units with the self-dual codes presented by Gildea, by limiting the conditions in the corollaries of (23). Additionally, we establish a relationship between idempotent and self-dual codes.

Chapter 4 focuses on building Extended Binary Golay Code and Extended Quadratic Residue Code. In 2019, by Doughtery (19) the concept of a single border was introduced. In 2020, by Gildea (24) the concept of double borders was introduced. In the chapter, we have extended the Gildea and Doughtery concept by introducing the $\frac{n}{r}$-th borders around the matrix. Here n and r are the natural numbers such that r divides n. We have shown that this construction is efficacious for any groups of order r over the Frobenius ring R_k. The motivation of this chapter is to construct extremal binary self-dual codes of various lengths that are not obtained in (19) and (24).

In **chapter 5** we introduce the concept of double borders around the generator matrix $M = [I_n|A]$, where A is a block matrix consisting of blocks that come from group rings such that the elements in the first row cannot completely determine the block matrix A. We demonstrate that this construction is feasible for a group of order n, over the Frobenius ring R_k. We show the significance of this new construction by constructing several extremal self-dual codes of lengths 20, 40, 32, and 64 over the field F_2 and the ring $F_2 + uF_2$.

Chapter 6 focuses on the new technique for building self-dual codes. Double borders are introduced around a new altered form of a four-circulant matrix. Using this new construction over the field F_2 and the ring F_2+uF_2 and groups of orders $2, 3, 4, 5, 7$, and 9, we generate extremal binary self-dual codes of the following lengths: $12, 20, 24, 32, 40, 48, 64$, and 80.

In **Chapter 7** we introduce a new class of ring, which is the $*$-version of the semiclean ring, i.e., the $*$-semiclean ring. A ring R is called semiclean if every element of R can be expressed as sum of a periodic element and a unit. A $*$-ring is $*$-semiclean if each element is sum of a $*$-periodic element and a unit. Many properties of $*$-semiclean rings are discussed. It is proved that if $p \in P(R)$ (here, $P(R)$ represents the set of projections of a ring R) such that pRp and $(1-p)R(1-p)$ are $*$-semiclean rings, then R is also a $*$-semiclean ring. As a result, the matrix ring $M_n(R)$ over a $*$-semiclean ring is $*$-semiclean. The characterization of the group rings RC_r and RG in terms of the $*$-semicleanness of the rings are given, where R is a finite commutative local ring, C_i is a cyclic group of order i, and G is a locally finite abelian group. We have also given sufficient conditions when the group rings RC_3, RC_4, RQ_8, and RQ_{2n} are $*$-semiclean, where R is a commutative local ring. We have demonstrated that the group ring $\mathbb{Z}_2D_6$ is a $*$-semiclean ring (which is not a $*$-clean ring). We characterize the $*$-semicleanness of F_qG in terms of LCD and self-orthogonal abelian codes under the classic involution, where F_q is a finite field with q elements and G is a finite abelian group.

We now move on to Chapter 2, which involves the construction of extremal self-dual codes using unitary units in a group ring with the Quaternion group.

Chapter 2

Self-dual and modified codes over Q_8 group ring

This chapter focuses on constructing extremal binary self-dual codes of length 16. *For the first time, they are generated using the unitary units in a group ring with the Quaternion group. Various code modification techniques are being applied in the correct order to self-dual codes, which improves the rates (ratio of information symbol to code length) and error-handling capability of the code.*

2.1 Introduction

The chapter arose from the concept given by Neill in (47) of constructing self-dual codes from the unitary units of group algebra. In 2009, Hurley (34) and (35) introduced the concept of code generation using zero divisors and units. One of the most significant families of the code is the self-dual codes over fields. Because of its significant contribution to lattices, designs, and coding theory, self-dual codes have achieved great importance in literature (42). In Chapters 3 and 10 of (4), Blahut has discussed various linear code modification techniques.

Section 2.2.1 and 2.3.1 explain the construction of Type I and Type II and other unique divisible self-dual codes from the unitary units of group algebra $\mathbb{F}_{2^k}Q_8$, for $k = 1$ and 2 respectively. Moreover, we have shown that up to equivalence, one code of Type I and two codes of Type II of length sixteen exist. In further sections 2.2.2 and 2.3.2 modification techniques are strategically used to enhance unique self-dual codes obtained in sections 2.2.1 and 2.3.1 respectively.

Sections 2.3.2 and 2.3.3 discuss the encoding and decoding methods (Nearest neighbor and Syndrome decoding (32)) of such codes which can correct t-errors (here $t = \lfloor \frac{d-1}{2} \rfloor$). Throughout the chapter, SAGE software (54) is used to carry out all the computer calculations.

2.1.1 Self-dual codes and Unitary units

The following definition describes the formation of self-dual codes in the group ring RG.

Definition 2.1.1. *(34) Let $|G| = n = 2s$ and $a \in RG$. Then a generates the self-dual code, if a satisfies the following conditions $a^2 = 0$, $a = a^T$, $aa^T = 0$, and the matrix $\sigma(a) = A$ has rank s.*

Definition 2.1.2. *(50) The augmentation mapping $\xi : RG \to R$ is a homomorphism, defined as*

$$\xi\left(\sum_{g\in G} \gamma_g g\right) = \sum_{g\in G} \gamma_g,$$

where $\gamma_g \in R$.

Definition 2.1.3. *(50) Let $U(RG)$ denote the set of unit elements of the group ring RG. Then the normalized units of the group ring RG is defined as*

$$V(RG) = \{u \in U(RG) \mid \xi(u) = 1\}.$$

Definition 2.1.4. *(50) An anti-automorphism map $\star : RG \to RG$ of order two is defined as*

$$\left(\sum_{g\in G} \gamma_g g\right)^{\star} = \sum_{g\in G} \gamma_g g^{-1},$$

where $\gamma_g \in R$. Then the unitary units of group ring RG is define as

$$V_\star(RG) = \{v \in V(RG) \mid v^{-1} = v^\star\}.$$

Theorem 2.1.5. *(48, Theorem 5.5) Let M be the generator matrix for the $[n, k]$ code. Then by using the elementary row operations the generator matrix M can be reduced to an equivalent matrix of the standard form $[I_k|B]$ where B is the matrix of $k \times (n-k)$ order and I_k is the identity matrix of $k \times k$ order.*

The relation between self-dual codes and unitary units of a group ring, as in (47), is defined as follows. Suppose M is the generator matrix of the self-dual code i.e. $MM^T = 0$.

Then for M of the form $[I|\ \sigma(v)]$, we have

$$MM^T = \begin{bmatrix} I & \sigma(v) \end{bmatrix} \begin{bmatrix} I \\ \sigma(v)^T \end{bmatrix} = I + \sigma(v)\sigma(v)^T = I + \sigma(v)\sigma(v^\star) = I + \sigma(vv^\star).$$

Thus $MM^T = 0$ gives $I + \sigma(vv^\star) = 0$, i.e. $vv^\star = 1$, which implies $v^\star = v^{-1}$. So from definition 2.1.4 we can say that $v \in RG$ corresponds to a unitary unit of RG. Accordingly, from Example 1.1.3 and Theorem 2.1.5 we conclude that the generator matrix for generation of self-dual codes from unitary units of Quaternion group over the fields $\mathbb{F}_2$ and $\mathbb{F}_4$ is of the form

$$M = \left[\begin{array}{cc|cc} I & 0 & A & B \\ 0 & I & C & A^T \end{array}\right], \tag{2.1}$$

where I is the identity matrix.

2.2 Codes in $\mathbb{F}_2 Q_8$

2.2.1 Self-dual codes from unitary units of $\mathbb{F}_2 Q_8$

Now, we will study the group algebra $\mathbb{F}_2 Q_8$. This structure has 2^8 possible codes. Now consider a set M that contains all possible generator matrices of the form (2.1). There are 256 generator matrices for $\mathbb{F}_2 Q_8$. One of them is mentioned below:

$$M = \left[\begin{array}{cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0
\end{array}\right].$$

Figure 2.1: Generator matrix of $\mathbb{F}_2 Q_8$

Next, we obtain the self-dual code using the $MM^T = 0$ condition. There are 64 self-dual codes. One of the generator matrices of a self-dual code is shown below:

$$M = \left[\begin{array}{cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&1&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&1\\
0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&0\\
0&0&0&0&1&0&0&0&0&1&0&1&1&0&0&0\\
0&0&0&0&0&1&0&0&1&0&1&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&1&0&1&0&0&1&0\\
0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&1
\end{array}\right].$$

Figure 2.2: Self-dual generator matrix of $\mathbb{F}_2 Q_8$

The codes obtained are identical. Using the *is_permutation_equivalent* command in the SAGE software we compare all the self-dual codes for equivalence over $\mathbb{F}_2$ and filter only the unique ones. In this step, four unique matrices are obtained. The unique self-dual generator matrices along with their code representation are shown below:

$$UCM_0 = \left[\begin{array}{cccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0
\end{array}\right].$$

Figure 2.3: Unique self-dual generator matrix of the code $UC_0[16, 8, 2]$

$$UCM_1 = \left[\begin{array}{cccccccc|cccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0\\ 0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\ 0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1\\ 0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&1\\ 0&0&0&0&1&0&0&0&1&1&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&0\\ 0&0&0&0&0&0&1&0&1&0&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&0 \end{array}\right].$$

Figure 2.4: Unique self-dual generator matrix of the code $UC_1[16,8,4]$

$$UCM_2 = \left[\begin{array}{cccccccc|cccccccc} 1&0&0&0&0&0&0&0&1&0&0&0&1&1&1&1\\ 0&1&0&0&0&0&0&0&0&1&0&0&1&1&1&1\\ 0&0&1&0&0&0&0&0&0&0&1&0&1&1&1&1\\ 0&0&0&1&0&0&0&0&0&0&0&1&1&1&1&1\\ 0&0&0&0&1&0&0&0&1&1&1&1&1&0&0&0\\ 0&0&0&0&0&1&0&0&1&1&1&1&0&1&0&0\\ 0&0&0&0&0&0&1&0&1&1&1&1&0&0&1&0\\ 0&0&0&0&0&0&0&1&1&1&1&1&0&0&0&1 \end{array}\right].$$

Figure 2.5: Unique self-dual generator matrix of the code $UC_2[16,8,4]$

$$UCM_3 = \left[\begin{array}{cccccccc|cccccccc} 1&0&0&0&0&0&0&0&1&1&1&0&1&1&1&1\\ 0&1&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\ 0&0&1&0&0&0&0&0&1&0&1&1&1&1&1&1\\ 0&0&0&1&0&0&0&0&1&1&0&1&1&1&1&1\\ 0&0&0&0&1&0&0&0&1&1&1&1&1&0&1&1\\ 0&0&0&0&0&1&0&0&1&1&1&1&1&1&0&1\\ 0&0&0&0&0&0&1&0&1&1&1&1&1&1&1&0\\ 0&0&0&0&0&0&0&1&1&1&1&1&0&1&1&1 \end{array}\right].$$

Figure 2.6: Unique self-dual generator matrix of the code $UC_3[16, 8, 4]$

For each of the four codes listed above. The last 8 elements i.e. $0, 0, 0, 0, 0, 1, 0, 0$ in the first row of UCM_0 act as the coefficient of 1, x, x^2, x^3, y, xy, x^2y, x^3y. The following table is obtained from this.

Table 2.1: Coefficients table for $\mathbb{F}_2Q_8$

v	1	x	x^2	x^3	y	xy	x^2y	x^3y	d
0	0	0	0	0	0	1	0	0	2
1	0	0	0	0	1	1	1	0	4
2	1	0	0	0	1	1	1	1	4
3	1	1	1	0	1	1	1	1	4

Now we will verify that every element is unitary by computing $v_i * v_i^\star$ for $i = 0$ to 3, the outcome should be 1 in each case.
Consider the first element, we have $v_0 = xy$ and $v_0^\star = (xy)^{-1} = x^3y$. Multiplying v_0 and $v_0^\star$ yields $v_0 * v_0^\star = x^4y^2 = 1$.
For the second element, we have $v_1 = y + xy + x^2y$ and $v_1^\star = (y)^{-1} + (yx)^{-1} + (x^2y)^{-1} = x^2y + x^3y + y$. Multiplying v_1 and $v_1^\star$ gives

$$\begin{aligned} v_1 * v_1^\star &= x^5y^2 + 2x^4y^2 + 2x^3y^2 + 2x^2y^2 + xy^2 + y^2 \\ &= y^2 = 1. \end{aligned}$$

For the third element, we have $v_2 = 1 + y + xy + x^2y + x^3y$ and $v_2^\star = 1 + x^2y + x^3y + y + xy$. Multiplying v_2 and $v_2^\star$ yields

$$\begin{aligned} v_2 * v_2^\star &= x^6y^2 + 2x^5y^2 + 3x^4y^2 + 4x^3y^2 + 3x^2y^2 + 2y^2x \\ &\quad + y^2 + yx^3 + yx^2 + yx + y + 1 + y + xy + x^2y + x^3y \\ &= 4x^4y^2 + y^2x^2 + y^2 + 1 = 1. \end{aligned}$$

Similarly, considering the fourth element, we have $v_3 = 1 + x + x^2 + y + xy + x^2y + x^3y$ and $v_3^\star = 1 + x^3 + x^2 + x^2y + x^3y + y + xy$. Multiplying v_3 and $v_3^\star$ gives

$$\begin{aligned} v_3 * v_3^\star &= x^6y^2 + x^6y + 2x^5y^2 + 3x^5y + x^5 + 3x^4y^2 + 4x^4y + 2x^4 + 4y^2x^3 \\ &+ 6yx^3 + 2x^3 + 3x^2y^2 + 5x^2y + 2x^2 + 2xy^2 + 3xy + x + y^2 + 2y + 1 \\ &= 1 + 2x^2y + 2xy + 2x - 1 + 1 = 1. \end{aligned}$$

Remark 2.2.1. *The four unique divisible self-dual codes such as $UC_0[16, 8, 2]$, $UC_1[16, 8, 4]$, $UC_2[16, 8, 4]$, and $UC_3[16, 8, 4]$ are obtained with divisors 2, 4, 2, and 4 respectively. The UC_0 and UC_2 are Type I codes, and the UC_1 and UC_3 are Type II codes. Moreover, the codes UC_1, UC_2, and UC_3 are extremal self-dual codes. The code UC_0 can detect one error, and the codes UC_1, UC_2, and UC_3 can correct one error.*

2.2.2 Modified codes of unique self-dual codes in $\mathbb{F}_2Q_8$

In this section using the modifying techniques on unique self-dual codes, we enhance them by generating new codes having high error-correction capability and good rate.

Product code

Consider linear codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ as $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ respectively, then their product code $\mathfrak{C}_{prod}$ is given by the form $[n_1n_2, k_1k_2, d_1d_2]$.
Applying the product code approach on UC_i for $i = 0$ to 3 generates sixteen product codes categorized by the following forms, one code of the form $[256, 64, 4]$, six codes of the form $[256, 64, 8]$, and nine codes of the form $[256, 64, 16]$.

Remark 2.2.2. *This approach raises the error-correction capability for given self-dual codes UC_i for $i = 0$ to 3 by almost sevenfold. Newly constructed product codes of form $[256, 64, 8]$ and $[256, 64, 16]$ can correct three and seven errors respectively.*

Subcode

A subcode is a code that is part of or subordinate to another code. Using the expurgating approach i.e. (Fix n; decrease k; increase d) on UC_i for $i = 0$ to 3 we generate the subcode of UC_i for $i = 0$ to 3 having high error-correction capability .
The code UC_0 have eight subcodes of the form $[16, 1, 2]$, twenty-eight subcodes of the form $[16, 2, 2]$, fifty-six subcodes of the form $[16, 3, 2]$, seventy subcodes of the form $[16, 4, 2]$, fifty-six subcodes of the form $[16, 5, 2]$, twenty-eight subcodes of the form

$[16,6,2]$, and eight subcodes of the form $[16,7,2]$.
Similarly, the code UC_1 have eight subcodes of the form $[16,1,4]$, twenty-eight subcodes of the form $[16,2,4]$, fifty-six subcodes of the form $[16,3,4]$, seventy subcodes of the form $[16,4,4]$, fifty-six subcodes of the form $[16,5,4]$, twenty-eight subcodes of the form $[16,6,4]$, and eight subcodes of the form $[16,7,4]$.
The code UC_2 have eight subcodes of the form $[16,1,6]$, sixteen subcodes of the form $[16,2,6]$, twelve subcodes of the form $[16,2,4]$, fifty-six subcodes of the form $[16,3,4]$, seventy subcodes of the form $[16,4,4]$, fifty-six subcodes of the form $[16,5,4]$, twenty-eight subcodes of the form $[16,6,4]$, and eight subcodes of the form $[16,7,4]$.
The code UC_3 have eight subcodes of the form $[16,1,8]$, twenty-eight subcodes of the form $[16,2,4]$, fifty-six subcodes of the form $[16,3,4]$, seventy subcodes of the form $[16,4,4]$, fifty-six subcodes of the form $[16,5,4]$, twenty-eight subcodes of the form $[16,6,4]$, and eight subcodes of the form $[16,7,4]$.

Remark 2.2.3. *Newly constructed subcodes of form* $[16,2,6]$ *and* $[16,1,8]$ *can correct two and three errors respectively.*

Construction_x

Consider linear codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ as $[n,k_1,d_1]$ and $[n,k_2,d_2]$ respectively, such that $\mathfrak{C}_2$ is subcode of $\mathfrak{C}_1$. The parameters of the codes satisfies the conditions $k_1 > k_2$ and $d_1 < d_2$. If a code $\mathfrak{C}_3$ $[n_3,k_3,d_3]$ exist and satisfies the conditions $k_3 + k_1 = k_2$ and $d_3 + d_1 \leq d_2$, then a new code can be constructed, defined as $\mathfrak{C}_{new}[n+n_3,k_1,d_3+d_1]$.
As shown above $[16,1,8]$ and $[16,7,4]$ are subcodes of $UC_3[16,8,4]$. Taking $\mathfrak{C}_1$, $\mathfrak{C}_2$, and $\mathfrak{C}_3$ as $[16,8,4]$, $[16,1,8]$, and $[16,7,4]$ respectively the newly obtained code $\mathfrak{C}_x$ is $[32,8,8]$.

Remark 2.2.4. *This technique generates a highly efficient code* $[32,8,8]$ *having four times more information rate than a* $[16,1,8]$ *subcode of* $UC_3[16,8,4]$ *and has a three error-correction capability i.e three times more efficient in error-correction than* $UC_3[16,8,4]$.

Punctured code

The code $\mathfrak{C}[n,k,d]$ can be punctured at the i-th coordinate by removing the i-th coordinate from each of its code words. Applying the Puncturing approach i.e. (Fix n; decrease k; decrease d) on UC_i for $i = 0$ to 3 generates the linear punctured code of UC_i for $i = 0$ to 3 with high rates.

Puncture $UC_0[16,8,2]$ code at 3rd co-ordinate generates the $[15,8,1]$ linear punctured code. Puncturing the resultant code at the 3rd coordinate for 12 times generates the $[3,3,1]$ linear punctured code. Puncture $[3,3,1]$ code at 2nd co-ordinate generates $[2,2,1]$ linear punctured code. Puncture $[2,2,1]$ at 1st co-ordinate generates $PC_0[1,1,1]$ linear punctured code.
Similarly, puncture the $UC_1[16,8,4]$ and $UC_2[16,8,4]$ codes at 3rd co-ordinate gives $\mathfrak{C}_1[15,8,3]$ and $\mathfrak{C}_2[15,8,3]$ linear punctured codes respectively. Now again puncture the resultant codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ at 3rd co-ordinate gives $PC_1[14,8,3]$ and $PC_2[14,8,3]$ linear punctured codes respectively.
Puncture the $UC_3[16,8,4]$ code at 3rd co-ordinate gives $PC_3[15,8,3]$ linear punctured code.

Remark 2.2.5. *Puncturing unique self-dual codes raises the code quality by increasing the code rate of UC_0, UC_1, UC_2, and UC_3 from $1/2$ to 1, $1/2$ to $8/14$, $1/2$ to $8/14$, and $1/2$ to $8/15$ respectively.*

Extended code

With the addition of a coordinate, longer codes can be constructed. Pick up the extension so that only even vectors are in the new code. The extension of the code $\mathfrak{C}[n,k,d]$ is defined as

$$\mathfrak{C}_{ext} = \{y_1y_2y_3\cdots y_{n+1} \in F_q^{n+1} \mid y_1y_2y_3...y_n \in \mathfrak{C} \textit{ with } y_1+y_2+y_3+...+y_{n+1}=0\}.$$

Applying the extending approach i.e. (Fix k; increase n; increase d) on $PC_0[1,1,1]$, $PC_1[14,8,3]$, $PC_2[14,8,3]$, and $PC_3[15,8,3]$ generates the $EX_0[2,1,2]$, $EX_1[15,8,4]$, $EX_2[15,8,4]$, and $EX_3[16,8,4]$ extended linear codes with rate $1/2$, $8/15$, $8/15$, and $1/2$ respectively.

Remark 2.2.6. *Using this approach we generate a mds code $EX_0[2,1,2]$ from UC_0 and raise the information rate for both the given self-dual codes UC_i for $i=1$ to 2 from $1/2$ to $8/15$ without affecting its error-correction capability.*

Juxtapose code

Let M be the generator matrix of the binary linear code $\mathfrak{C}[n,k,d]$. The new linear binary code $CJ[2n,k,d']$ can be constructed by juxtaposing two or more copies of the generator matrix $[M|M]$. Using the juxtapose code approach on UC_i for $i=0$ to 3 gives the sixteen juxtapose codes categorized by the following forms, one code of the form $[32,8,4]$, six codes of the form $[32,8,6]$, and nine codes of the form $[32,8,8]$.

Remark 2.2.7. *This approach improves the error-correction capability for given self-dual codes UC_i for $i = 0$ to 3. Newly constructed juxtapose codes of form* $[32, 8, 6]$ *and* $[32, 8, 8]$ *can correct two and three errors respectively, whereas the codes UC_i for $i = 0$ to 3 can correct up to one error.*

2.2.3 Encoding and Decoding

Encoding

Encoding is a process of conversion of information from one type to another. The message block w of k bits is encoded into n bits by evaluating $E = w * M$. Here, M is the generator matrix.
Considering the message $w = [0, 1, 1, 0, 1, 1, 0, 1]$ and using UCM_0 as the generator matrix, the message w is encoded as $E_0 = [0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1]$. Similarly using UCM_1, UCM_2, UCM_3 as the generator matrix the word w is encoded as $E_1 = [0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0]$, $E_2 = [0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1]$, and $E_3 = [0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1]$ respectively. Since the generator matrices UCM_i, for $i = 0$ to 3 are in their standard form thus the first eight bits of encoded words are information bits and the rest are check bits.

Decoding

The process of extracting a code word $\mathfrak{C}[n, k, d]$ (a message m) from the received message r is known as decoding. The parameter d of a code $\mathfrak{C}[n, k, d]$ plays a vital role in the error-correcting capability of a code.

Nearest neighbor decoding The process of finding a code word z in $\mathfrak{C}$ ($|\mathfrak{C}| = q^n$) that is nearest to the received vector r is known as nearest neighbor decoding. A sphere $S_t(r)$ of radius ($0 \leq t \leq \lfloor \frac{d-1}{2} \rfloor$) center around the received vector r is drawn and we check all the elements of $S_t(r)$ and choose the code word lets say z, that is present in $\mathfrak{C}$ and is closest to the received vector r. This test fails for $t > \lfloor \frac{d-1}{2} \rfloor$.
The nearest neighbor decoding method always decodes the received vector r correctly whenever there are at most t errors in the received vector. But, if the received vector contains more than t errors, it will not always decode correctly.
Let the message sent to the receiver is $w = [0, 1, 1, 0, 1, 1, 0, 1]$. Using the code $\mathfrak{C}_x$ and the command $\mathfrak{C}_x.encode(w)$ in SAGE software the message w is encoded as $[0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1]$.

Let the error introduced in the message while passing through the channel is $e = [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0]$. Thus the message received by the receiver is $r = [0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1]$. Using SAGE software and Nearest neighbor decoding algorithm the message decoded by the decoder is $q = [0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1]$. The entire process which is explained above is shown below.

```
sage: Cx = C1.construction_x(C3,C2)
sage: print(Cx)
[32, 8] linear code over GF(2)
sage: print(Cx.minimum_distance())
4
sage: D = codes.decoders.LinearCodeNearestNeighborDecoder(Cx)
sage: word = vector(GF(2), (0, 1, 1, 0, 1, 1, 0, 1))
sage: Cx.encode(word)
(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)
sage: S=Cx.encode(word)
sage: w_err = S + vector(GF(2), (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0))
sage: D.decode_to_code(w_err)
(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)
```

Figure 2.7: Encoding and decoding using C_x code

Syndrome decoding algorithm Syndrome decoding is a highly effective process to decode a linear code across a noisy network. In the previous method, we have to construct a table containing the nearest code word for every 2^n vectors of $\mathbb{F}_2^n$. In syndrome decoding, one can find the nearest code word for the received vector by looking up a syndrome-error table which contains only $2^{n-k} - 1$ vectors of $\mathbb{F}_2^n$.

Algorithm

Let $r = x + e$ be the received vector. Here, x is the code word and e is the error introduced while passing through the channel.

- Find syndrome $s = Qr^T$. Here, Q is the parity check matrix.
  - If $s = 0$, the received vector r has no error, i.e. $r = x$ and we are done otherwise we switch to the next step.
- Construct syndrome table of order $2^{n-k} - 1$, consisting of two columns syndrome s and error e respectively.
- If $s \neq 0$ in the first step, then corresponding to s find the error e using the table constructed in the second step and then compute $x = r - e$.

Consider the message $w = [0, 1, 1, 0, 1, 1, 0, 1]$. Using UC_3 the above message is encoded as $x = [0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1]$. Let the error introduced in the message while passing through the channel is $e = [0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$. The message received by the receiver is $r = [0,0,1,0,1,1,0,1,0,0,1,1,0,0,0,1]$. Using SAGE software and the command $UC[3].syndrome(r)$ the syndrome for the receive vector r is

$$s = [0,1,0,0,0,0,0,0]. \tag{2.2}$$

Now using commands $D = codes.decoders.LinearCodeSyndromeDecoder(UC[3])$ and $D.syndrome\_table()$ in SAGE the syndrome table of order $2^8 - 1$ is constructed.

```
(0, 0, 1, 1, 1, 1, 1, 0): (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0),
(0, 0, 1, 1, 1, 1, 1, 1): (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 0, 0, 0): (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 0, 0, 1): (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 0, 1, 0): (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 0, 1, 1): (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 1, 0, 0): (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 1, 0, 1): (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 1, 1, 0): (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 0, 1, 1, 1): (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0),
(0, 1, 0, 0, 1, 0, 0, 0): (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 1, 0, 0, 1): (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 1, 0, 1, 0): (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0),
(0, 1, 0, 0, 1, 0, 1, 1): (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0),
(0, 1, 0, 0, 1, 1, 0, 0): (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),
```

Figure 2.8: Syndrome table

Using the syndrome table we can say that the error in the received vector corresponding to syndrome s (2.2) is $e = [0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$. Thus the code word is $x = r - e = [0,1,1,0,1,1,0,1,0,0,1,1,0,0,0,1]$.

2.3 Codes in $\mathbb{F}_4 Q_8$

2.3.1 Self-dual codes from unitary units of $\mathbb{F}_4 Q_8$

This structure has 4^8 possible codes, each of which is built using code written in SAGE software. There are 65536 generator matrices for $\mathbb{F}_4 Q_8$ and 1024 self-dual codes. Using the permutation_equivalent command, one unique code of distance two, one unique code of distance three, and sixteen unique codes of distance four are obtained. The following table is generated from this.

Table 2.2: Coefficients table for $\mathbb{F}_4Q_8$

v	1	x	x^2	x^3	y	xy	x^2y	x^3y	d
0	0	0	0	0	0	1	0	0	2
1	0	0	0	0	w+1	0	w	0	3
2	0	0	0	0	w	1	w	0	4
3	0	0	0	0	1	1	1	0	4
4	0	0	0	0	w+1	w	w	w	4
5	1	0	0	0	w	w	w	w	4
6	1	0	0	0	w+1	w	w+1	w	4
7	1	0	0	0	1	w	1	w	4
8	1	0	0	0	1	1	1	1	4
9	w	0	w	0	w+1	w	w	w	4
10	w	0	w	0	1	w+1	1	w	4
11	w	1	w	0	w	w	w	w	4
12	w	1	w	0	w+1	w	w+1	w	4
13	w	1	w	0	1	w	1	w	4
14	1	1	1	0	1	1	1	1	4
15	w	w	w	w	w+1	w	w	w	4
16	w	w	w	w	w+1	w+1	w+1	w	4
17	w+1	w	w	w	1	w+1	1	w+1	4

We are going to verify that every element is unitary by computing $v_i * v_i^\star$ for $i =$ 0 to 17, the outcome should be 1 in each case.

Consider the first element, we have $v_0 = xy$ and $v_0^\star = (xy)^{-1} = x^3y$. Multiplying v_0 and $v_0^\star$, we obtain $v_0 * v_0^\star = x^4y^2 = 1$.

For the second element, we have $v_1 = (w+1)y + wx^2y$ and $v_1^\star = (w+1)(y)^{-1} + w(x^2y)^{-1} = (w+1)x^2y + wy$. Multiplying v_1 and $v_1^\star$, we obtain

$$\begin{aligned} v_1 * v_1^\star &= w^2y^2 + wy^2 + w^2x^4y^2 + 2w^2x^2y^2 + wx^4y^2 + 2wx^2y^2 + x^2y^2 \\ &= 2w^2y^2 + 2wy^2 + 1 = 1. \end{aligned}$$

For the third element, we have $v_2 = wy + xy + wx^2y$ and $v_2^\star = w(y)^{-1} + (xy)^{-1} + w(x^2y)^{-1} = wx^2y + x^3y + wy$ which yields

$$\begin{aligned} v_2 * v_2^\star &= w^2y^2 + wx^5y^2 + w^2x^4y^2 + x^4y^2 + 2wx^3y^2 + 2w^2y^2x^2 + wxy^2 \\ &= 2w^2y^2 + 2wxy^2 + y^2 = 1. \end{aligned}$$

For the fourth element, we have $v_3 = y + xy + x^2y$ and $v_3^\star = (y)^{-1} + (xy)^{-1} + (x^2y)^{-1} = x^2y + x^3y + y$ which yields

$$\begin{aligned} v_3 * v_3^\star &= y^2x^5 + 2y^2x^4 + 2y^2x^3 + 2y^2x^2 + y^2x + y^2 \\ &= 2y^2x + y^2 = 1. \end{aligned}$$

For the fifth element, we have $v_4 = (w+1)y + wxy + wx^2y + wx^3y$ and $v_4^\star = (w+1)x^2y + wx^3y + wy + wxy$. Multiplying v_4 and $v_4^\star$, we obtain

$$\begin{aligned} v_4 * v_4^\star &= y^2w^2 + y^2w + y^2w^2x^2 + y^2wx + y^2w^2 \\ &\quad + y^2w + y^2x^2 + y^2w^2x^2 + y^2wx \\ &= y^2x^2 = 1. \end{aligned}$$

Considering the sixth element, we have $v_5 = 1 + wy + wxy + wx^2y + wx^3y$ and $v_5^\star = 1 + wx^2y + wx^3y + wy + wxy$. Multiplying v_5 and $v_5^\star$, we obtain

$$\begin{aligned} v_5 * v_5^\star &= w^2y^2 + w^2y^2x^6 + 2w^2y^2x^5 + 3w^2y^2x^4 + 4w^2y^2x^3 \\ &\quad + 3w^2y^2x^2 + x^2 + 2wyx + 1 \\ &= 2w^2y^2 + 2w^2y^2x^2 + 1 \\ &= 1. \end{aligned}$$

Similarly for $n = 6$ to 17, we obtain $v_n * v_n^\star = 1$ for the following pair of elements:

$$\begin{aligned} v_6 &= 1 + (w+1)y + wxy + (w+1)x^2y + wx^3y. \\ v_6^\star &= 1 + (w+1)x^2y + wx^3y + (w+1)y + wxy. \\ v_7 &= 1 + y + wxy + x^2y + wx^3y. \\ v_7^\star &= 1 + x^2y + wx^3y + y + wxy. \\ v_8 &= 1 + y + xy + x^2y + x^3y. \\ v_8^\star &= 1 + x^2y + x^3y + y + xy. \\ v_9 &= w + wx^2 + (w+1)y + wxy + wx^2y + wx^3y \\ v_9^\star &= w + wx^2 + (w+1)x^2y + wx^3y + wy + wxy. \\ v_{10} &= w + wx^2 + y + (w+1)xy + x^2y + wx^3y. \\ v_{10}^\star &= w + wx^2 + x^2y + (w+1)x^3y + y + wxy. \\ v_{11} &= w + x + wx^2 + wy + wxy + wx^2y + wx^3y. \\ v_{11}^\star &= w + x^3 + wx^2 + wx^2y + wx^3y + wy + wxy. \end{aligned}$$

$$v_{12} = w + x + wx^2 + (w+1)y + wxy + (w+1)x^2y + wx^3y.$$
$$v_{12}^{\star} = w + x^3 + wx^2 + (w+1)x^2y + wx^3y + (w+1)y + wxy.$$
$$v_{13} = w + x + wx^2 + y + wxy + x^2y + wx^3y.$$
$$v_{13}^{\star} = w + x^3 + wx^2 + x^2y + wx^3y + y + wxy.$$
$$v_{14} = 1 + x + x^2 + y + xy + x^2y + x^3y.$$
$$v_{14}^{\star} = 1 + x^3 + x^2 + x^2y + x^3y + y + xy.$$
$$v_{15} = w + wx + wx^2 + wx^3 + (w+1)y + wxy + wx^2y + wx^3y.$$
$$v_{15}^{\star} = w + wx^3 + wx^2 + wx + (w+1)x^2y + wx^3y + wy + wxy.$$
$$v_{16} = w + wx + wx^2 + wx^3 + (w+1)y + (w+1)xy + (w+1)x^2y + wx^3y.$$
$$v_{16}^{\star} = w + wx^3 + wx^2 + wx + (w+1)x^2y + (w+1)x^3y + (w+1)y + wxy.$$

and

$$v_{17} = w + 1 + wx + wx^2 + wx^3 + y + (w+1)xy + x^2y + (w+1)x^3y.$$
$$v_{17}^{\star} = w + 1 + wx^3 + wx^2 + wx + x^2y + (w+1)x^3y + y + (w+1)xy.$$

Remark 2.3.1. *The eighteen unique divisible self-dual codes, such as one code of the form $UC_0[16,8,2]$, one code of the form $UC_1[16,8,3]$, and the rest of codes UC_i for $i = 2$ to 17 of the form $[16,8,4]$ are obtained. The codes UC_0 and UC_1 can detect one error, and the codes UC_i for $i = 2$ to 17 can correct one error.*

2.3.2 Modified codes of unique self-dual codes in $\mathbb{F}_4Q_8$

Product code

Apply the product code approach on UC_i for $i = 0$ to 17 generates three hundred and twenty-four product codes categorized by the following forms, one code of the form $[256,64,4]$, two codes of the form $[256,64,6]$, thirty-two codes of the form $[256,64,8]$, one code of the form $[256,64,9]$, thirty-two codes of the form $[256,64,12]$, and two hundred and fifty-six codes of the form $[256,64,16]$.

Remark 2.3.2. *This approach raises the error-correction capability for given self-dual codes UC_i for $i = 0$ to 17 by almost sevenfold. Newly constructed product codes of form $[256,64,6]$, $[256,64,8]$, $[256,64,9]$, $[256,64,12]$, and $[256,64,16]$ can correct two, three, four, five, and seven errors respectively.*

Subcode

A code part of or subordinate to another code. There are 8, 28, 56, 70, 56, 28, 8 subcodes of dimension 1, 2, 3, 4, 5, 6, 7 respectively for all the uniquely generated self-dual codes of $\mathbb{F}_4Q_8$.

Using Expurgating approach we generate eight subcodes of the form $[16,1,2]$, twenty-eight subcodes of the form $[16,2,2]$, fifty-six subcodes of the form $[16,3,2]$, seventy subcodes of the form $[16,4,2]$, fifty-six subcodes of the form $[16,5,2]$, twenty-eight subcodes of the form $[16,6,2]$, and eight subcodes of the form $[16,7,2]$ of UC_0.

There are two hundred and fifty-six subcodes of UC_1 which are as follows, eight of the form $[16,1,4]$, twenty-eight of the form $[16,2,3]$, fifty-six of the form $[16,3,3]$, seventy of the form $[16,4,3]$, fifty-six of the form $[16,5,3]$, twenty-eight of the form $[16,6,3]$, and eight of the form $[16,7,3]$.

The subcodes of UC_2 and UC_3 are as follows, eight of the form $[16,1,4]$, twenty-eight of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_4 are as follows, eight of the form $[16,1,5]$, sixteen of the form $[16,2,5]$, twelve of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_5 and UC_8 are as follows, eight of the form $[16,1,6]$, sixteen of the form $[16,2,6]$, twelve of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_6 and UC_7 are as follows, eight of the form $[16,1,6]$, twenty-four of the form $[16,2,6]$, four of the form $[16,2,4]$, thirty-two of the form $[16,3,6]$, twenty-four of the form $[16,3,4]$, sixteen of the form $[16,4,6]$, fifty-four of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_9 are as follows, eight of the form $[16,1,7]$, sixteen of the form $[16,2,7]$, eight of the form $[16,2,6]$, four of the form $[16,2,4]$, thirty-two of the form $[16,3,6]$, twenty-four of the form $[16,3,4]$, sixteen of the form $[16,4,6]$, fifty-four of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{10} are as follows, eight of the form $[16,1,7]$, twenty-four of the form $[16,2,7]$, four of the form $[16,2,4]$, thirty-two of the form $[16,3,6]$, twenty-four of the form $[16,3,4]$, sixteen of the form $[16,4,6]$, fifty-four of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{11} are as follows, eight of the form $[16,1,8]$, twenty-four of the form $[16,2,6]$, four of the form $[16,2,4]$, thirty-two of the form $[16,3,6]$, twenty-four of the form $[16,3,4]$, sixteen of the form $[16,4,6]$, fifty-four of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{12} are as follows, eight of the form $[16,1,8]$, sixteen of the form $[16,2,7]$, eight of the form $[16,2,6]$, four of the form $[16,2,4]$, thirty-two of the form $[16,3,6]$, twenty-four of the form $[16,3,4]$, sixteen of the form $[16,4,6]$, fifty-four of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{13} are as follows, eight of the form $[16,1,8]$, sixteen of the form $[16,2,7]$, twelve of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{14} are as follows, eight of the form $[16,1,8]$, twenty-eight of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{15} are as follows, eight of the form $[16,1,9]$, twenty-eight of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{16} are as follows, eight of the form $[16,1,9]$, sixteen of the form $[16,2,7]$, twelve of the form $[16,2,4]$, fifty-six of the form $[16,3,4]$, seventy of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

The subcodes of UC_{17} are as follows, eight of the form $[16,1,9]$, sixteen of the form $[16,2,7]$, eight of the form $[16,2,6]$, four of the form $[16,2,4]$, thirty-two of the form $[16,3,6]$, twenty-four of the form $[16,3,4]$, sixteen of the form $[16,4,6]$, fifty-four of the form $[16,4,4]$, fifty-six of the form $[16,5,4]$, twenty-eight of the form $[16,6,4]$, and eight of the form $[16,7,4]$.

Remark 2.3.3. *The newly constructed subcodes of the form* $[16,1,5]$, $[16,2,6]$, $[16,4,6]$, $[16,2,7]$, $[16,1,8]$, *and* $[16,1,9]$ *can correct two, two, two, three, three, and four errors respectively.*

Construction_x

Use the approach as discussed in sec 2.2.2. Consider the subcodes $[16,1,9]$ and $[16,7,4]$ of $UC_{17}[16,8,4]$. Take $\mathfrak{C}_1$, $\mathfrak{C}_2$, and $\mathfrak{C}_3$ as $[16,8,4]$, $[16,1,9]$, and $[16,7,4]$ linear codes respectively, we obtain new linear code $\mathfrak{C}_x$ of form $[32,8,8]$.

Remark 2.3.4. *The obtain code* $[32,8,8]$ *is more efficient as it is a three error-correcting code with a rate of* $1/4$.

Punctured code

Using SAGE software, puncture $UC_0[16,8,2]$ code at 3rd co-ordinate yields the $[15,8,1]$ linear punctured code. Repeating this process twelve times with the resultant codes yields $[3,3,1]$ linear punctured code. Puncturing $[3,3,1]$ code at 2nd co-ordinate generates $[2,2,1]$ linear punctured code. Now puncture $[2,2,1]$ code at 1st co-ordinate generates $PC_0[1,1,1]$ linear punctured code.
Puncture $UC_1[16,8,3]$ code at 3rd co-ordinate generates $[15,8,2]$ linear punctured code. Now repeat this process two times with the resultant codes, we obtain $[13,8,2]$ linear punctured code. Puncture $[13,8,2]$ code at 0 co-ordinate generates $PC_1[12,8,2]$ linear punctured code.
Puncture UC_i for $i = 2$ to 5, and UC_8 codes at 3rd co-ordinate yields the $\mathfrak{C}_2[15,8,3]$, $\mathfrak{C}_3[15,8,3]$, $\mathfrak{C}_4[15,8,3]$, $\mathfrak{C}_5[15,8,3]$, and $\mathfrak{C}_8[15,8,3]$ linear punctured codes respectively. Puncture $\mathfrak{C}_2$, $\mathfrak{C}_3$, $\mathfrak{C}_4$, $\mathfrak{C}_5$, and $\mathfrak{C}_8$ at 3rd co-ordinate generates the $PC_2[14,8,3]$, $PC_3[14,8,3]$, $PC_4[14,8,3]$, $PC_5[14,8,3]$, and $PC_8[14,8,3]$ linear punctured codes respectively .
Puncture $UC_6[16,8,4]$ code at 3rd co-ordinate generates $[15,8,3]$ linear punctured code, repeat this process two times with resultant code yield $\mathfrak{C}_6[14,8,3]$ linear punctured code. Puncture $\mathfrak{C}_6$ code at 3rd co-ordinate yields $[13,8,3]$ linear punctured code. Puncture $[13,8,3]$ code at 2nd co-ordinate generates $PC_6[12,8,3]$ linear punctured code.
Puncture $UC_7[16,8,4]$ and $UC_{11}[16,8,4]$ codes at 3rd co-ordinate generates $[15,8,3]$ and $[15,8,3]$ linear punctured codes respectively. Now repeat this process two times with the resultant codes yields $\mathfrak{C}_7[13,8,3]$ and $\mathfrak{C}_{11}[13,8,3]$ linear punctured codes. Puncture $\mathfrak{C}_7$ and $\mathfrak{C}_{11}$ codes at 2nd co-ordinate yields $PC_7[12,8,3]$ and $PC_{11}[12,8,3]$ linear punctured codes.
Puncture $UC_9[16,8,4]$ and $UC_{12}[16,8,4]$ codes at 3rd co-ordinate yields $[15,8,3]$ and $[15,8,3]$ linear punctured codes respectively. Now repeat this process two times with resultant codes yields $\mathfrak{C}_9[13,8,3]$ and $\mathfrak{C}_{12}[13,8,3]$ linear codes. Puncture $\mathfrak{C}_9$ and $\mathfrak{C}_{12}$ code at 0-co-ordinate generates $PC_9[12,8,3]$ and $PC_{12}[12,8,3]$ linear punctured codes.
Puncture $UC_{10}[16,8,4]$ and $UC_{17}[16,8,4]$ codes two times at 3rd co-ordinate yields $\mathfrak{C}_{10}[14,8,3]$ and $\mathfrak{C}_{17}[14,8,3]$ linear codes respectively. Now puncture $\mathfrak{C}_{10}$ and $\mathfrak{C}_{17}$ codes at 3-rd co-ordinate generates $[13,8,3]$ and $[13,8,3]$ linear codes. Puncture $[13,8,3]$ and $[13,8,3]$ codes at 0-co-ordinate yields $PC_{10}[12,8,3]$ and $PC_{17}[12,8,3]$ linear punctured codes.

Puncture $UC_{13}[16,8,4]$ code at 3rd co-ordinate generates $[15,8,3]$ linear punctured code. Now puncture $[15,8,3]$ linear code at 0-co-ordinate yields $PC_{13}[14,8,3]$ linear punctured code.
Puncture $UC_{14}[16,8,4]$ and $UC_{15}[16,8,4]$ linear codes at 3rd co-ordinate yields $PC_{14}[15,8,3]$ and $PC_{15}[15,8,3]$ linear punctured codes.
Puncture $UC_{16}[16,8,4]$ code twice at 3rd co-ordinate generates $PC_{16}[14,8,3]$ linear punctured code.

Remark 2.3.5. *Puncturing a unique self-dual codes raises code quality by increasing a code rate of UC_i for $i = 0$ to 17 from $\frac{1}{2}$ to 1, $\frac{2}{3}$, $\frac{4}{7}$, $\frac{4}{7}$, $\frac{4}{7}$, $\frac{4}{7}$, $\frac{2}{3}$, $\frac{2}{3}$, $\frac{4}{7}$, $\frac{2}{3}$, $\frac{2}{3}$, $\frac{2}{3}$, $\frac{2}{3}$, $\frac{4}{7}$, $\frac{8}{15}$, $\frac{8}{15}$, $\frac{4}{7}$, $\frac{2}{3}$ respectively.*

Extended code

Applying the Extending approach on the punctured codes $PC_0[1,1,1]$, $PC_1[12,8,2]$, $PC_2[14,8,3]$, $PC_3[14,8,3]$, $PC_4[14,8,3]$, $PC_5[14,8,3]$, $\mathfrak{C}_6[14,8,3]$, $PC_7[12,8,3]$, $PC_8[15,8,3]$, $PC_9[12,8,3]$, $\mathfrak{C}_{10}[14,8,3]$, $PC_{11}[12,8,3]$, $PC_{12}[12,8,3]$, $PC_{13}[14,8,3]$, $PC_{14}[15,8,3]$, $PC_{15}[15,8,3]$, $PC_{16}[14,8,3]$, and $PC_{17}[14,8,3]$ which are obtain in section 2.3.2 generates its extended codes $EX_0[2,1,2]$, $EX_1[13,8,3]$, $EX_2[15,8,4]$, $EX_3[15,8,4]$, $EX_4[15,8,4]$, $EX_5[15,8,4]$, $EX_6[15,8,4]$, $EX_7[13,8,4]$, $EX_8[15,8,4]$, $EX_9[13,8,4]$, $EX_{10}[15,8,4]$, $EX_{11}[13,8,4]$, $EX_{12}[13,8,4]$, $EX_{13}[15,8,4]$, $EX_{14}[16,8,4]$, $EX_{15}[16,8,4]$, $EX_{16}[15,8,4]$, and $EX_{17}[15,8,4]$ respectively.

Remark 2.3.6. *After applying the operations of Puncturing and Extending on the UC_i for $i = 0$ to 17 codes the new improve codes we obtain are $EX_0[2,1,2]$ this is mds code as it is of form $[n,k,n-k+1]$, $EX_1[13,8,3]$ it can correct one error with rate $8/13$, $EX_2[15,8,4]$, $EX_3[15,8,4]$, $EX_4[15,8,4]$, $EX_5[15,8,4]$, $EX_6[15,8,4]$, $EX_8[15,8,4]$, $EX_{10}[15,8,4]$, $EX_{13}[15,8,4]$, $EX_{16}[15,8,4]$, and $EX_{17}[15,8,4]$ they can correct one error with rate $8/15$, $EX_7[13,8,4]$ and $EX_9[13,8,4]$ can correct one error with rate $8/13$, $EX_{11}[13,8,4]$ and $EX_{12}[13,8,4]$ can correct one error with rate $8/13$, $EX_{14}[16,8,4]$ and $EX_{15}[16,8,4]$ they can correct one error with rate $1/2$.*

Juxtapose code

Applying the juxtapose code approach on UC_i for $i = 0$ to 17 generates three hundred and twenty-four juxtapose codes categorized by the following forms, one code of the form $[32,8,4]$, two codes of the form $[32,8,5]$, five codes of the form $[32,8,6]$, six codes of the form $[32,8,7]$, three hundred and ten codes of the form $[32,8,8]$.

Remark 2.3.7. *This approach gives an improvement for given UC_i for $i = 0$ to 17 unique self-dual linear codes by getting a lot more realistic and relevant codes as the newly constructed juxtapose codes of form $[32, 8, 5]$, $[32, 8, 6]$, $[32, 8, 7]$, and $[32, 8, 8]$ can correct two, two, three, and three errors respectively, whereas the error-correction capability of UC_i for $i = 2$ to 17 is one.*

2.3.3 Encoding and Decoding

The process of encoding and decoding for the case of $\mathbb{F}_4 Q_8$ is similar to the approach followed in $\mathbb{F}_2 Q_8$.

Chapter 3

Group ring construction of the $[24, 12, 8]$ and $[48, 24, 12]$ Type II linear block code

This chapter focuses on a new construction for self-dual codes that uses the concept of double-bordered construction, group rings, and reverse circulant matrices. Using groups of orders $2, 3, 4,$ and 5, and by applying the construction over the binary field F_2 and the ring F_2+uF_2, an extremal binary self-dual codes of various lengths: $12, 16, 20, 24, 32, 40,$ and 48 are obtained. The significance of this new construction is the construction of the unique Extended Binary Golay Code $[24, 12, 8]$ and the unique Extended Quadratic Residue $[48, 24, 12]$ Type II linear block code. Moreover, the existing relationship between units and non-units with the self-dual codes presented in (23) is also strengthened by limiting the conditions given in the corollaries of (23). Additionally, a relationship between idempotent and self-dual codes is also established.

3.1 Introduction

Many researchers are interested in constructing extremal binary self-dual codes over Frobenius rings since these codes are linked to other mathematical structures and have numerous applications.

Extremal Type II codes have gotten the most attention in the literature because of their strong relation to sphere packings. These codes fulfill the formula $[n, \frac{n}{2}, 4\lfloor \frac{n}{24} \rfloor + 4]$, $n = 8m$ (where m is a natural number) for [length, dimension, and distance] (32, p. 346). The Extended Binary Golay Code i.e. [24, 12, 8] is the first putative code in the Type II series of codes when n equals twenty-four. The second putative code in this series is the Extended Quadratic Residue Code i.e. [48, 24, 12]. In this chapter, we have constructed both codes using a new construction.

In 1990, the code [24, 12, 8] was constructed using ideals in the group algebra F_2S_4; see (2) for details. In 2008, the [24, 12, 8] code was constructed from F_2D_{24}; see (43) for details. The most common approach to constructing an Extended Binary Golay Code and Extended Quadratic Residue Code is to extend the Binary Golay Code of length 23 by an even parity bit and the Quadratic Residue Code of length 47 by an even parity bit. A new way of constructing the Extended Binary Golay Code and the Extended Quadratic Residue Code is defined in this chapter. We construct the code here by blending the concept of double-bordered constructions of self-dual codes from group rings over Frobenius rings (24) with constructing self-dual codes from group rings and reverse circulant matrices (23).

The following is an outline of the work in this chapter: Section 3.2 presents the new constructions and the theoretical results. Section 3.3 presents numerical results for the Extended Binary Golay Code, Extended Quadratic Residue Code, and extremal binary self-dual codes of various lengths obtained by directly applying our construction over a field F_2 and ring $F_2 + uF_2$ with SAGE (54). The chapter wraps up with the conclusion of our work.

3.2 Main matrix construction

Here we present our main construction. As mentioned above, we define a double border around the matrix given in (23). The motivation is to produce extremal binary self-dual codes of various lengths. The most important codes are the Extended Binary Golay Code, i.e., [24, 12, 8] and the Extended Quadratic Residue Code, which we shall call Extended QR, the only known [48, 24, 12] code, via our construction, that could not be obtained in (23) and (24). Let $v_1, v_2 \in RG$, where R is a finite commutative Frobenius ring of characteristic 2 and G is a group of order n. The matrix is defined as follows:

$$M_\sigma = \left[\begin{array}{cc|c|c|cc|c|c}
\beta_1 & \beta_2 & \beta_3 \cdots \beta_3 & \beta_4 \cdots \beta_4 & \beta_5 & \beta_6 & \beta_7 \quad \cdots \quad \beta_7 & \beta_8 \quad \cdots \quad \beta_8 \\
\beta_2 & \beta_1 & \beta_4 \cdots \beta_4 & \beta_3 \cdots \beta_3 & \beta_6 & \beta_5 & \beta_8 \quad \cdots \quad \beta_8 & \beta_7 \quad \cdots \quad \beta_7 \\
\hline
\beta_3 & \beta_4 & & & \beta_7 & \beta_8 & & \\
\vdots & \vdots & I_n & 0 & \vdots & \vdots & \sigma(v_1) & \sigma(v_2)+C \\
\beta_3 & \beta_4 & & & \beta_7 & \beta_8 & & \\
\hline
\beta_4 & \beta_3 & & & \beta_8 & \beta_7 & & \\
\vdots & \vdots & 0 & I_n & \vdots & \vdots & \sigma(v_2)^T+C & \sigma(v_1)^T \\
\beta_4 & \beta_3 & & & \beta_8 & \beta_7 & &
\end{array}\right]. \tag{3.1}$$

Let $\mathfrak{C}_\sigma$ be a code generated through the matrix M_σ. Then code $\mathfrak{C}_\sigma$ has length $4n+4$.

Lemma 3.2.1. *Let R be a finite commutative Frobenius ring with characteristic 2, and $G = \{g_1, g_2, \cdots, g_n\}$ be a finite group of order n, so that*

$$N_\sigma = \begin{pmatrix} \sigma(v_1) & \sigma(v_2)+C \\ \sigma(v_2)^T + C & \sigma(v_1)^T \end{pmatrix},$$

where v_1 and v_2 are the elements of RG, $\sigma(v_1)$ and $\sigma(v_2)$ are group-ring matrices of $n \times n$ order, and C is a reverse circulant matrix of $n \times n$ order over R. Then

$$\sigma(v_k)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \sigma(v_k)^T\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\mu_k\\ \vdots \\ \mu_k\end{pmatrix} \ (k=1,2),$$

where $\mu_1 = \sum_{g\in G} \alpha_g$, $\mu_2 = \sum_{g\in G} \beta_g$.

Let η denote the sum of all elements of the first row of matrix C. Then

$$(\sigma(v_2)+C)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = (\sigma(v_2)^T + C)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\mu_2+\eta\\ \vdots \\ \mu_2+\eta\end{pmatrix}.$$

Proof. *Clearly, $\sigma(v_1) = (\alpha_{g_i^{-1}g_j})_{i,j=1,\cdots,n}$, $\sigma(v_2) = (\beta_{g_i^{-1}g_j})_{i,j=1,\cdots,n}$, and $C = (\gamma_{ij})_{i,j=1,\cdots,n}$.*

Now, the $i-th$ element of column $\sigma(v_1)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n} \alpha_{g_i^{-1}g_j} = \sum_{g\in G} \alpha_{g_i^{-1}g} = \sum_{g\in G} \alpha_g = \mu_1, g_i \in G, g_i^{-1} \in G,$$

and the $i-th$ *element of column* $\sigma(v_1)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{n}\alpha_{g_j^{-1}g_i}=\sum_{g\in G}\alpha_{g^{-1}g_i}=\sum_{g\in G}\alpha_{gg_i}=\sum_{g\in G}\alpha_g=\mu_1, g_i\in G.$$

Thus,

$$\sigma(v_1)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\sigma(v_1)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\begin{pmatrix}\mu_1\\ \vdots\\ \mu_1\end{pmatrix}.$$

Similarly, the $i-th$ *element of column* $\sigma(v_2)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{n}\beta_{g_i^{-1}g_j}=\sum_{g\in G}\beta_{g_i^{-1}g}=\sum_{g\in G}\beta_g=\mu_2, g_i\in G, g_i^{-1}\in G,$$

and the $i-th$ *element of column* $\sigma(v_2)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{n}\beta_{g_j^{-1}g_i}=\sum_{g\in G}\beta_{g^{-1}g_i}=\sum_{g\in G}\beta_{gg_i}=\sum_{g\in G}\beta_g=\mu_2, g_i\in G.$$

Thus,

$$\sigma(v_2)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\sigma(v_2)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\begin{pmatrix}\mu_2\\ \vdots\\ \mu_2\end{pmatrix}.$$

Furthermore, the $i-th$ *element of column* $C\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{n}\gamma_{ij}=\gamma_{i1}+\gamma_{i2}+\cdots+\gamma_{in}=\eta.$$

Thus,

$$C\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\begin{pmatrix}\eta\\ \vdots\\ \eta\end{pmatrix}.$$

Hence,

$$(\sigma(v_2)+C)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=(\sigma(v_2)^T+C)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\begin{pmatrix}\mu_2+\eta\\ \vdots\\ \mu_2+\eta\end{pmatrix}.$$

□

In 2020, (23, Theorem 2.5), Gildea, Kaya, and Yildiz introduced a matrix and showed that, under certain conditions, we can generate self-dual codes of order $4n$ by a group of order n. In Theorem 3.2.2, we extend this result by introducing a double border around their matrix and demonstrating that, under certain conditions, we can generate self-dual codes of order $4n+4$ by a group of order n. In (24), Gildea introduced the concept of the double-bordered construction. Their main matrix construction does not involve a reverse circulant matrix. In our main matrix construction, we have used a reverse circulant matrix. Moreover, their main theorem, i.e, (24, Theorem 3.2), was restricted for the group of order $2p$ (p is odd prime) only but, by Theorem 3.2.2, we have extended it to any group of order n ($n \in \mathbb{N}$). As a result, we can construct those extremal self-dual codes that can not be attained by the technique used in (24), i.e., extremal self-dual codes of length 12, 20, 40 are constructed as shown in Table 3.1, Table 3.5, and Table 3.6 respectively. By blending both the concepts of (23) and (24) in Theorem 3.2.2, we can construct those extremal self-dual codes that have not been obtained in (23) and (24). In particular, we can build the well-known Extended Binary Golay Code, as shown in (Table 3.7, Code G_2), the Extended QR code, as shown in (Table 3.8, Code L_2), and various other extremal self-dual codes which are listed in Section 3.3.

Theorem 3.2.2. *Let R be a finite commutative Frobenius ring with characteristic 2, G be a finite group of order n, and $\mathfrak{C}_\sigma$ be a code generated by the matrix M_σ such that rank of a matrix M_σ is $2n+2$. Then $\mathfrak{C}_\sigma$ is a self-dual code of length $4n+4$ if the following conditions are satisfied :*

***Case I:** n is odd*

1. $\sum_{i=0}^{8}\beta_i = 0.$
2. $\sigma(v_1v_2+v_2v_1)+\sigma(v_1)C+C\sigma(v_1)=0.$
3. $\sigma(v_1v_1^*+v_2v_2^*)+\sigma(v_2)C+C\sigma(v_2)^T+C^2=I_n+(\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix}1&\cdots&1\\ \vdots&\ddots&\vdots\\ 1&\cdots&1\end{bmatrix}_{n\times n}.$
4. $\sigma(v_1^*v_2^*+v_2^*v_1^*)+C\sigma(v_1)^T+\sigma(v_1)^TC=0.$

5. $\sigma(v_1^* v_1 + v_2^* v_2) + \sigma(v_2)^T C + C\sigma(v_2) + C^2 = I_n + (\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$.

6. $\beta_3(\beta_1 + 1) + \beta_4\beta_2 + \beta_7(\beta_5 + \mu_1) + \beta_6\beta_8 + (\mu_2 + \eta)\beta_8 = 0$.

7. $\beta_4(\beta_1 + 1) + \beta_3\beta_2 + \beta_8(\beta_5 + \mu_1) + \beta_6\beta_7 + (\mu_2 + \eta)\beta_7 = 0$.

Case II: *n is even*

1. $\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2 = 0$.

2. *Conditions 2 to 7 for this case are the same as for the case 'n is odd'.*

Proof. *Let* $M_\sigma = \begin{bmatrix} M_1 & M_2 & M_3 & M_4 \\ M_2^T & I_{2n} & M_4^T & N_\sigma \end{bmatrix}$, *where* $M_1 = circ(\beta_1,\beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5,\beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, ..., \beta_3) \in R^n$, $A_2 = (\beta_4, ..., \beta_4) \in R^n$, $A_3 = (\beta_7, ..., \beta_7) \in R^n$, $A_4 = (\beta_8, ..., \beta_8) \in R^n$, *and* $N_\sigma = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) + C \\ \sigma(v_2)^T + C & \sigma(v_1)^T \end{bmatrix}$.

Then,

$$M_\sigma M_\sigma^T = \begin{bmatrix} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T & M_1M_2 + M_2 + M_3M_4 + M_4N_\sigma^T \\ M_2^TM_1^T + M_2^T + M_4^TM_3^T + N_\sigma M_4^T & M_2^TM_2 + I_{2n} + M_4^TM_4 + N_\sigma N_\sigma^T \end{bmatrix}.$$

Now,

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + n\beta_{i+2}^2 + \beta_{i+4}^2 + n\beta_{i+6}^2), 0).$$

Case I: *n is odd*

$$\begin{aligned} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T &= circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+2}^2 + \beta_{i+4}^2 + \beta_{i+6}^2), 0) \\ &= circ(\sum_{i=1}^{8}\beta_i^2, 0). \end{aligned}$$

Case II: *n is even*

$$\begin{aligned} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T &= circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+4}^2), 0) \\ &= circ(\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2, 0). \end{aligned}$$

and

$$M_2^TM_2 + I_{2n} + M_4^TM_4 + N_\sigma N_\sigma^T = \sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2 CIRC(\boldsymbol{A}, \boldsymbol{0}) + I_{2n} + N_\sigma N_\sigma^T$$

where $\boldsymbol{A} = circ(\underbrace{1, \cdots, 1}_{n-times})$, $\boldsymbol{0} = circ(\underbrace{0, \cdots, 0}_{n-times})$, *and*

$$N_\sigma N_\sigma^T = \begin{bmatrix} \sigma(v_1v_1^* + v_2v_2^*) + \sigma(v_2)C + C\sigma(v_2)^T + C^2 & \sigma(v_1v_2) + \sigma(v_1)C + \sigma(v_2v_1) + C\sigma(v_1) \\ \sigma(v_1^*v_2^*) + C\sigma(v_1)^T + \sigma(v_2^*v_1^*) + \sigma(v_1)^TC & \sigma(v_2^*v_2) + \sigma(v_2)^TC + C\sigma(v_2) + C^2 + \sigma(v_1^*v_1) \end{bmatrix}.$$

It follows from Lemma 3.2.1 that

$$N_\sigma M_4^T = \begin{bmatrix} \mu_1\beta_7 + \mu_2\beta_8 + \eta\beta_8 & \mu_1\beta_8 + \mu_2\beta_7 + \eta\beta_7 \\ \vdots & \vdots \\ \mu_1\beta_7 + \mu_2\beta_8 + \eta\beta_8 & \mu_1\beta_8 + \mu_2\beta_7 + \eta\beta_7 \\ \mu_2\beta_7 + \eta\beta_7 + \mu_1\beta_8 & \mu_2\beta_8 + \eta\beta_8 + \mu_1\beta_7 \\ \vdots & \vdots \\ \mu_2\beta_7 + \eta\beta_7 + \mu_1\beta_8 & \mu_2\beta_8 + \eta\beta_8 + \mu_1\beta_7 \end{bmatrix}.$$

Additionally, $M_2^T M_1^T + M_2^T + M_4^T M_3^T + N_\sigma M_4^T =$

$$\begin{bmatrix} \beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_6\beta_8 + \mu_1\beta_7 + \mu_2\beta_8 + \eta\beta_8 & \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_1\beta_8 + \mu_2\beta_7 + \eta\beta_7 \\ \vdots & \vdots \\ \beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_6\beta_8 + \mu_1\beta_7 + \mu_2\beta_8 + \eta\beta_8 & \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_1\beta_8 + \mu_2\beta_7 + \eta\beta_7 \\ \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_2\beta_7 + \eta\beta_7 + \mu_1\beta_8 & \beta_4\beta_2 + \beta_3\beta_1 + \beta_3 + \beta_5\beta_7 + \beta_6\beta_8 + \mu_2\beta_8 + \eta\beta_8 + \mu_1\beta_7 \\ \vdots & \vdots \\ \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_2\beta_7 + \eta\beta_7 + \mu_1\beta_8 & \beta_4\beta_2 + \beta_3\beta_1 + \beta_3 + \beta_5\beta_7 + \beta_6\beta_8 + \mu_2\beta_8 + \eta\beta_8 + \mu_1\beta_7 \end{bmatrix}.$$

Clearly, $M_\sigma M_\sigma^T$ *is a symmetric matrix and* $\mathfrak{C}_\sigma$ *is self orthogonal if for* $\sum_{i=0}^{8} \beta_i = 0$, $\sigma(v_1v_2 + v_2v_1) + \sigma(v_1)C + C\sigma(v_1) = 0$, $\sigma(v_1v_1^* + v_2v_2^*) + \sigma(v_2)C + C\sigma(v_2)^T + C^2 = I_n + (\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$, $\sigma(v_1^*v_2^* + v_2^*v_1^*) + C\sigma(v_1)^T + \sigma(v_1)^TC = 0$, $\sigma(v_1^*v_1 + v_2^*v_2) + \sigma(v_2)^TC + C\sigma(v_2) + C^2 = I_n + (\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$, $\beta_3(\beta_1+1)+\beta_4\beta_2+\beta_7(\beta_5+\mu_1)+\beta_6\beta_8+(\mu_2+\eta)\beta_8 = 0$, $\beta_4(\beta_1+1)+\beta_3\beta_2+\beta_8(\beta_5+\mu_1)+\beta_6\beta_7+(\mu_2+\eta)\beta_7 = 0$. *Because the rank of the matrix* M_σ *is* $2n + 2$ *and* $\mathfrak{C}_\sigma$ *is self-orthogonal under the conditions established above, we can conclude that the code* $\mathfrak{C}_\sigma$ *is a self-dual code if all of the preceding conditions are met.* □

In 2020, (23, Corollary 3.2, Corollary 3.3, and Corollary 3.4), Gildea, Kaya, and Korban under certain conditions defined a relationship of units, non-units, and unitary units with self-dual codes, respectively. In Corollary 3.2.3, 3.2.4, 3.2.5, and 3.2.6 we have relaxed both the restrictions, i.e., C commutes with $\sigma(v_1)$ and v_1 commutes with v_2. In addition, we have replaced the condition that both $C\sigma(v_2)^T$ and $C\sigma(v_2)$ must be symmetric with the simple condition that $\sigma(v_2)$ is symmetric, which strengthens the relationship between units, non-units, and unitary units with the self-dual codes.

Corollary 3.2.3. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n, and $\mathfrak{C}_\sigma$ be a self-dual code. Then the elements $v_1v_1^* + v_2v_2^*$, $v_1^*v_1 + v_2^*v_2 \in RG$ are units if the following conditions are satisfied:*

1. $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$.
2. $\sigma(v_2)$ *is symmetric.*
3. $C^2 = 0$.

Proof. *If $\sigma(v_2)$ is symmetric, then $\sigma(v_2)C + C\sigma(v_2)^T = 0$. If $C^2 = 0$ and $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 0$, then $\sigma(v_1v_1^*+v_2v_2^*) = \sigma(v_1^*v_1+v_2^*v_2) = I_n$. Then, $det(\sigma(v_1v_1^*+v_2v_2^*)) = det(\sigma(v_1^*v_1+v_2^*v_2)) = 1$. Hence, $v_1v_1^* + v_2v_2^*$ and $v_1^*v_1 + v_2^*v_2$ are unitary units.* □

Corollary 3.2.4. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and $\mathfrak{C}_\sigma$ be a self-dual code. Then the elements $v_1v_1^* + v_2v_2^*$, $v_1^*v_1 + v_2^*v_2 \in RG$ are non units if the following conditions are satisfied:*

1. $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$.
2. $\sigma(v_2)$ *is symmetric.*
3. $C^2 = 0$.

Proof. *If $\sigma(v_2)$ is symmetric, then $\sigma(v_2)C + C\sigma(v_2)^T = 0$. If $C^2 = 0$ and $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 1$, then*

$$\sigma(v_1v_1^* + v_2v_2^*) = I_n + \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{n\times n} = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}_{n\times n}.$$

Then,

$$
\begin{aligned}
det(\sigma(v_1v_1^* + v_2v_2^*)) &= det\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}_{n\times n} \\
&= (n-1)det\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n} \\
&= 0 \ (if\ n\ is\ odd).
\end{aligned}
$$

Hence, $det(\sigma(v_1v_1^* + v_2v_2^*)) = 0$ and $v_1v_1^* + v_2v_2^*$ is a non-unit by corollary 3 of (33). Similarly, $det(\sigma(v_1^*v_1 + v_2^*v_2)) = 0$ and $v_1^*v_1 + v_2^*v_2$ is a non-unit. □

Corollary 3.2.5. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and $\mathfrak{C}_\sigma$ be a self-dual code. Then the elements $v_1v_1^* + v_2v_2^*$, $v_1^*v_1 + v_2^*v_2 \in RG$ are non units if the following conditions are satisfied:*

1. $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0.$
2. *$\sigma(v_2)$ is symmetric.*
3. $C^2 = I.$

Proof. *If $\sigma(v_2)$ is symmetric, then $\sigma(v_2)C + C\sigma(v_2)^T = 0$. If $C^2 = I$ and $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 0$, then $\sigma(v_1v_1^*+v_2v_2^*) = \sigma(v_1v_1^*+v_2v_2^*) = 0$. Hence, $v_1v_1^*+v_2v_2^*$ and $v_1^*v_1+v_2^*v_2$ are non-units.* □

Corollary 3.2.6. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and $\mathfrak{C}_\sigma$ be a self-dual code. Then the element $v_2 \in RG$ is unitary unit if following conditions are satisfied:*

1. *$\sigma(v_2)$ is symmetric.*
2. $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0.$
3. $C^2 = I.$
4. *v_1 is unitary in RG.*

Proof. *If $\sigma(v_2)$ is symmetric, then $\sigma(v_2)C + C\sigma(v_2)^T = 0$. If $C^2 = I$, $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 0$ and v_1 is unitary in RG, then $\sigma(1 + v_2v_2^*) = \sigma(1 + v_2^*v_2) = 0$. Thus, $v_2v_2^* = v_2^*v_2 = 1$ and v_2 is unitary unit.* □

By Corollary 3.2.7, we have established a relationship between idempotents and self-dual codes, which have been established for the first time in the literature.

Corollary 3.2.7. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and $\mathfrak{C}_\sigma$ be a self-dual code. Then the elements $v_1v_1^* + v_2v_2^*$, $v_1^*v_1 + v_2^*v_2 \in RG$ are idempotents if following conditions are satisfied:*

1. $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1.$
2. $\sigma(v_2)$ *is symmetric.*
3. $C^2 = 0.$

Proof. *If $\sigma(v_2)$ is symmetric, then $\sigma(v_2)C + C\sigma(v_2)^T = 0$.*

If n is odd, then $\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}^2 = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$. *That is*

$\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$ *is an idempotent matrix.*

If $C^2 = 0$ and $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$, then

$$\sigma(v_1v_1^* + v_2v_2^*) = I_n + \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n} = I_n - \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}.$$

If T is an idempotent matrix, then $I - T$ is also an idempotent matrix. Thus, $\sigma(v_1v_1^* + v_2v_2^*)$ is an idempotent matrix and $v_1v_1^* + v_2v_2^*$ is an idempotent element of RG. Similarly, we can say that $v_1^*v_1 + v_2^*v_2$ is an idempotent element of RG. □

3.3 Computational results

In this section, we apply our main construction over the field F_2 and the ring $F_2 + uF_2$ to search for extremal binary self-dual codes of lengths of $12, 16, 20, 24, 32, 40, 48$. We consider groups of orders $2, 3, 4$, and 5, in particular C_2, C_3, C_4, and C_5. We also employ the Gray map to construct the famous Extended QR code. For all our computational calculations, we have used the SAGE software (54).

Algorithm:

INPUT: Field F_2.

OUTPUT: Extremal self-dual codes.

1. Generate matrices $\sigma(v)$ of order $n \times n$ by a group of order n, over the field F_2. The structure of the matrix $\sigma(v)$ is described in Theorem 1.1.1.

2. Generate reverse circulant matrices C of order $n \times n$ over the field F_2.

3. Generate boundary matrices M_1, M_2, M_3, and M_4 over the Field F_2, where $M_1 = circ(\beta_1, \beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5, \beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, ..., \beta_3) \in R^n$, $A_2 = (\beta_4, ..., \beta_4) \in R^n$, $A_3 = (\beta_7, ..., \beta_7) \in R^n$, $A_4 = (\beta_8, ..., \beta_8) \in R^n$.

4. Construct the set of generator matrices M_σ of $(2n + 2) \times (4n + 4)$ order having the structure mentioned in Equation (3.1) using all the possible combinations of matrices obtained in Step 1, Step 2, and Step 3.

5. From the given set of generator matrices, collect matrices that satisfy the condition $M_\sigma M_\sigma^T = 0$ and have rank $2n + 2$. These matrices generate self-dual codes $\mathfrak{C}_\sigma$ with parameters $[4n+4, 2n+2, d_{min}]$, where d_{min} is the minimum distance of the code.

6. Evaluate $d_{min} = min\{d(a, b)|a \neq b\}$ for the self-dual codes that are generated from matrices collected in Step 5. Here, $d(a, b) = |\{i|1 \leq i \leq 4n + 4, a_i \neq b_i\}|$, where $a, b \in F_2^{4n+4}$ are the codewords of length $4n + 4$ for the code $\mathfrak{C}_\sigma$.

7. Shortlist matrices from Step 5, whose d_{min} of its corresponding self-dual code matches the minimum distance of extremal self-dual codes of length $4n + 4$. Refer to Theorem 1.1.4 for the minimum distance of extremal self-dual codes. In this step, we obtain matrices that generate the extremal self-dual codes $\mathfrak{C}_\sigma$ of length $4n + 4$.

8. Classify self-dual codes constructed from the matrices obtained in Step 7 are of Type I or Type II. The binary self-dual code $\mathfrak{C}_\sigma$ is said to be of Type I and Type II if the weight of all of its codewords is divisible by two and four respectively. The weight of a codeword a is defined as $w(a) = d(a, 0)$, where $0 = (0, 0, \cdots, 0)$ is the

zero vector.

9. Lift the obtained self-dual codes in Step 8, to the ring $F_2 + uF_2$, as discussed in Section 1.1.10. Generate a set of all possible lifted matrices by mapping an element 0 of F_2 to two elements 0 and u of the ring $F_2 + uF_2$ and element 1 of F_2 is mapped to elements 1 and $1 + u$ of the ring $F_2 + uF_2$.

10. From the given set of uplifted matrices, collect matrices that can generate self-dual codes of length 4n+4, as done in Step 5.

11. Evaluate d_L for the self-dual codes generated from matrices collected in Step 10. Here d_L denotes a code's smallest positive Lee distance. The Lee weight of the ring $F_2 + uF_2$ elements $0, 1, u$, and $1 + u$ are $0, 1, 2$, and 1 respectively. The Lee distance between $4n + 4$ tuple is defined as the sum of Lee weights of the difference between the components of these tuples.

12. Shortlist matrices whose d_L of its corresponding self-dual code matches the minimum distance of extremal self-dual codes of length $2(4n + 4)$. In this step, we obtain matrices that can generate the self-dual codes over the ring $F_2 + uF_2$ of length $4n + 4$, whose binary images are extremal self-dual codes of length $2(4n + 4)$.

13. Classify self-dual codes constructed from the matrices obtained in Step 12 are of Type I or Type II.

3.3.1 Construction from cyclic group of order 2

Here we execute the above construction for $G = C_2$ over the field F_2 and obtain an extremal self-dual code of length 12.

Now, we lift the code A_1 over the Frobenious ring $F_2 + uF_2$ to obtain an extremal self-dual code of length 12, whose binary image is the Type II extremal self-dual code of length 24.

Table 3.1: Self-dual codes of length 12 from C_2 over F_2

$Code(A_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$\lvert Aut(A_i)\rvert$	$Type$
1	$(1,0,1,1,1,0,0,0)$	$(0,0)$	$(0,0)$	$(1,0)$	23040	$[12,6,4]_I$

Table 3.2: The extremal binary self-dual codes of length 24 obtained from $F_2 + uF_2$ lift of A_1.

$Code(I_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$Type$
1	A_1	$(1,u,1,1,1,0,0,u)$	$(0,u)$	$(0,0)$	$(1,0)$	$TypeII$

3.3.2 Construction from cyclic group of order 3

Here we execute the above construction for $G = C_3$ over the field F_2 and obtain an extremal self-dual code of length 16.

Table 3.3: Self-dual codes of length 16 from C_3 over F_2

$Code(B_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$\lvert Aut(B_i)\rvert$	$Type$
1	$(1,0,1,1,1,0,0,0)$	$(0,0,0)$	$(0,0,0)$	$(1,0,0)$	5160960	$[16,8,4]_{II}$
2	$(1,0,0,0,0,0,0,1)$	$(0,0,0)$	$(0,0,0)$	$(1,1,0)$	3612672	$[16,8,4]_{II}$
3	$(1,0,1,1,0,0,0,1)$	$(0,0,0)$	$(0,0,0)$	$(1,1,0)$	73728	$[16,8,4]_I$

Now, we lift the codes B_1, B_2, and B_3 over the Frobenious ring $F_2 + uF_2$ to obtain an extremal self-dual code of length 16, whose binary image is the Type II extremal self-dual code of length 32.

Table 3.4: The extremal binary self-dual codes of length 32 obtained from $F_2 + uF_2$ lift of B_1, B_2, and B_3.

$Code(J_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$Type$
1	B_1	$(1, u, 1, 1, 1, 0, 0, u)$	$(u, 0, 0)$	$(0, 0, 0)$	$(1, 0, 0)$	$TypeII$
2	B_1	$(u+1, 0, 1, u+1, u+1, u, 0, u)$	$(u, 0, 0)$	(u, u, u)	$(u+1, u, u)$	$TypeII$
3	B_2	$(1, 0, 0, 0, 0, 0, 0, 1)$	$(0, u, u)$	$(0, 0, 0)$	$(1, 1, 0)$	$TypeII$
4	B_2	$(u+1, 0, 0, u, u, 0, 0, 1)$	$(u, 0, 0)$	(u, u, u)	$(u+1, u+1, u)$	$TypeII$
5	B_3	$(1, 0, 1, 1, 0, 0, u, 1)$	$(0, u, u)$	$(0, 0, 0)$	$(1, 1, 0)$	$TypeII$
6	B_3	$(u+1, 0, 1, u+1, 0, u, 0, 1)$	$(u, 0, 0)$	(u, u, u)	$(u+1, u+1, u)$	$TypeII$

3.3.3 Construction from cyclic group of order 4

Here we execute the above construction for $G = C_4$ over the field F_2 and obtain an extremal self-dual code of length 20.

Table 3.5: Self-dual codes of length 20 from C_4 over F_2

$Code(D_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$\|Aut(D_i)\|$	$Type$
1	$(1, 0, 1, 1, 1, 0, 0, 0)$	$(0, 0, 0, 0)$	$(0, 0, 0, 0)$	$(1, 0, 0, 0)$	1857945600	$[20, 10, 4]_I$
2	$(1, 0, 1, 1, 1, 0, 0, 0)$	$(0, 0, 0, 0)$	$(0, 0, 0, 0)$	$(1, 1, 1, 0)$	294912	$[20, 10, 4]_I$
3	$(1, 0, 1, 1, 1, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	4423680	$[20, 10, 4]_I$
4	$(1, 0, 1, 1, 1, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 1, 0, 1)$	122880	$[20, 10, 4]_I$

Now, we lift the codes D_1, D_2, D_3, and D_4 over the Frobenious ring $F_2 + uF_2$ to obtain extremal self-dual code of length 20, whose binary image is the Type II extremal self-dual code of length 40.

Table 3.6: The extremal binary self-dual codes of length 40 obtained from $F_2 + uF_2$ lift of D_1 and D_2

$Code(K_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$Type$
1	D_1	$(1, u, 1, 1, 1, 0, 0, u)$	$(0, 0, u, 0)$	$(0, 0, 0, 0)$	$(1, 0, 0, 0)$	$TypeII$
2	D_1	$(1, u, 1, 1, u+1, 0, 0, u)$	$(u, u, 0, u)$	(u, u, u, u)	$(1, 0, u, 0)$	$TypeII$
3	D_2	$(1, u, 1, 1, 1, 0, 0, u)$	$(0, 0, u, 0)$	$(0, 0, 0, 0)$	$(1, 1, 1, u)$	$TypeII$
4	D_2	$(u+1, 0, u+1, u+1, u+1, u, u, 0)$	$(u, u, 0, u)$	(u, u, u, u)	$(u+1, u+1, u+1, 0)$	$TypeII$

3.3.4 Construction from cyclic group of order 5

Here we execute the above construction for $G = C_5$ over the field F_2 and obtain an extremal self-dual code of length 24 of Type I and well-known Extended Binary Golay

Code.

Table 3.7: Self-dual codes of length 24 from C_5 over F_2

$Code(G_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$\lvert Aut(G_i)\rvert$	$Type$
1	$(1,0,0,0,0,0,0,1)$	$(0,0,1,1,0)$	$(0,0,0,0,0)$	$(1,0,1,0,0)$	138240	$[24,12,6]_I$
2	$(1,0,1,1,0,0,0,1)$	$(0,0,1,1,0)$	$(0,0,0,0,0)$	$(1,0,1,0,0)$	244823040	$[24,12,8]_{II}$

Now, we lift the codes G_2 over the Frobenious ring F_2+uF_2 to obtain an extremal self-dual code of length 24, whose binary image is the well-known Extended QR code.

Table 3.8: The extremal binary self-dual codes of length 48 obtained from $F_2 + uF_2$ lift of E_2.

$Code(L_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	f_C	$Type$
1	G_2	$(1,0,1,1,0,0,0,1)$	$(0,u,1,1,u)$	$(0,0,0,u,u)$	$(1,0,1,0,0)$	$[48,24,10]_I$
2	G_2	$(u+1,0,u+1,u+1,0,u,u,u+1)$	$(u,0,u+1,u+1,0)$	(u,u,u,u,u)	$(u+1,u,u+1,0,0)$	$[48,24,12]_{II}$

3.4 Conclusion

We presented a new method for creating self-dual codes using group rings. By doing so, we were able to show the relevance of this new construction by constructing extremal binary self-double codes of various lengths: $12, 16, 20, 24$ (Extended Binary Golay Code), $32, 40$, and most importantly, we have completed the exhaustive search for $[48, 24, 12]$ self-dual doubly-even codes begun in (28), (29), and (44). We established a link between unitary units/units/non-units and idempotents with self-dual codes. Due to the computing limits imposed by the construction approach, we consider the groups of orders $2, 3, 4$, and 5. These computational techniques can be applied to several families of rings and several groups within this framework.

Chapter 4

$\frac{n}{r}$-th bordered constructions of self-dual codes from Group rings over Frobenius rings

---

In this chapter, we introduce the concept of $\frac{n}{r}$-th borders around the matrix. Here n and r are the natural numbers such that r divides n. We have shown that this construction is efficacious for any group of order r (where r is a natural number such that r divides n), over the Frobenius ring R_k. We discover extremal binary self-dual codes of lengths 32*,* 40*, the well-known Extended Binary Golay Code, i.e.,* $[24, 12, 8]$*, and Extended Quadratic Residue Code, i.e.,* $[48, 24, 12]$ *by two different ways.*

4.1 Introduction

A conventional technique for constructing self-dual code over rings and finite fields is to consider a generator matrix of the form $[I_n \mid A]$ where A satisfies the condition $AA^T = -I$. The numerous modifications of the work mentioned above have been done in the hope of extremal self-dual codes of various lengths, see (19) and (24). In (19), the concept of single border is introduced, and in (24), the concept of double border is there. In this chapter, we extend the above work by constructing a $\frac{n}{r}$-th bordered construction to I_n and $\sigma(v)$, where $\sigma(v)$ is the group ring matrix. We emphasize the importance of this new construction by constructing both the significant codes, Extended Binary Golay Code and Extended Quadratic Residue Code in two different ways, that is, by using triple-bordered and fourth-bordered constructions, as listed in Tables 4.1, 4.2, 4.3, and 4.4.

The rest of the work in the chapter is organized as follows: In Section 4.2, we describe the new $\frac{n}{r}$ -th bordered matrix construction from group ring and prove our main results. In section 4.3, we find the extremal binary self-dual codes of different lengths by applying the construction on a different order of groups and list the obtained binary self-dual codes in tables. In section 4.4, we end up with the conclusion and the direction for potential future scope.

4.2 The $\frac{n}{r}$-th bordered construction from group ring

In this section, we have described our main matrix construction. The motivation of this chapter is to construct extremal self-dual codes of various lengths that are not obtained in (19) and (24). Let $v_1, v_2, \cdots, v_{\frac{n}{r}} \in RG$ where R is a finite commutative Frobenius ring with characteristic 2 and G is a finite group of order r where (r is natural number). Define the matrix as below: M_σ =

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c|c}
\alpha_1\ \alpha_2\ \cdots\ \alpha_{\frac{n}{r}} & \gamma_1\ \cdots\ \gamma_1 & \gamma_2\ \cdots\ \gamma_2 & \cdots & \gamma_{\frac{n}{r}}\ \cdots\ \gamma_{\frac{n}{r}} & \beta_1\ \beta_2\ \cdots\ \beta_{\frac{n}{r}} & \delta_1\ \cdots\ \delta_1 & \delta_2\ \cdots\ \delta_2 & \cdots & \delta_{\frac{n}{r}}\ \cdots\ \delta_{\frac{n}{r}} \\
\alpha_{\frac{n}{r}}\ \alpha_1\ \cdots\ \alpha_{\frac{n}{r}-1} & \gamma_{\frac{n}{r}}\ \cdots\ \gamma_{\frac{n}{r}} & \gamma_1\ \cdots\ \gamma_1 & \cdots & \gamma_{\frac{n}{r}-1}\ \cdots\ \gamma_{\frac{n}{r}-1} & \beta_{\frac{n}{r}}\ \beta_1\ \cdots\ \beta_{\frac{n}{r}-1} & \delta_{\frac{n}{r}}\ \cdots\ \delta_{\frac{n}{r}} & \delta_1\ \cdots\ \delta_1 & \cdots & \delta_{\frac{n}{r}-1}\ \cdots\ \delta_{\frac{n}{r}-1} \\
\vdots\ \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots & \vdots & \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots & \vdots\ \vdots\ \vdots & \vdots & \vdots\ \vdots\ \vdots \\
\alpha_2\ \alpha_3\ \cdots\ \alpha_1 & \gamma_2\ \cdots\ \gamma_2 & \gamma_3\ \cdots\ \gamma_3 & \cdots & \gamma_1\ \cdots\ \gamma_1 & \beta_2\ \beta_3\ \cdots\ \beta_1 & \delta_2\ \cdots\ \delta_2 & \delta_3\ \cdots\ \delta_3 & \cdots & \delta_1\ \cdots\ \delta_1 \\
\hline
\gamma_1\ \gamma_{\frac{n}{r}}\ \cdots\ \gamma_2 & & & & & \delta_1\ \delta_{\frac{n}{r}}\ \cdots\ \delta_2 & & & & \\
\vdots\ \vdots\ \cdots\ \vdots & & & & & \vdots\ \vdots\ \cdots\ \vdots & \sigma(v_1) & \sigma(v_2) & \cdots & \sigma(v_{\frac{n}{r}}) \\
\gamma_1\ \gamma_{\frac{n}{r}}\ \cdots\ \gamma_2 & & & & & \delta_1\ \delta_{\frac{n}{r}}\ \cdots\ \delta_2 & & & & \\
\hline
\gamma_2\ \gamma_1\ \cdots\ \gamma_3 & & & & & \delta_2\ \delta_1\ \cdots\ \delta_3 & & & & \\
\vdots\ \vdots\ \cdots\ \vdots & & & I_n & & \vdots\ \vdots\ \cdots\ \vdots & \sigma(v_{\frac{n}{r}}) & \sigma(v_1) & \cdots & \sigma(v_{\frac{n}{r}-1}) \\
\gamma_2\ \gamma_1\ \cdots\ \gamma_3 & & & & & \delta_2\ \delta_1\ \cdots\ \delta_3 & & & & \\
\hline
\vdots\ \vdots\ \cdots\ \vdots & & & & & \vdots\ \vdots\ \cdots\ \vdots & \vdots & \vdots & \ddots & \vdots \\
\hline
\gamma_{\frac{n}{r}}\ \gamma_{\frac{n}{r}-1}\ \cdots\ \gamma_1 & & & & & \delta_{\frac{n}{r}}\ \delta_{\frac{n}{r}-1}\ \cdots\ \delta_1 & & & & \\
\vdots\ \vdots\ \cdots\ \vdots & & & & & \vdots\ \vdots\ \cdots\ \vdots & \sigma(v_2) & \sigma(v_3) & \cdots & \sigma(v_1) \\
\gamma_{\frac{n}{r}}\ \gamma_{\frac{n}{r}-1}\ \cdots\ \gamma_1 & & & & & \delta_{\frac{n}{r}}\ \delta_{\frac{n}{r}-1}\ \cdots\ \delta_1 & & & &
\end{array}\right]$$

where, $\alpha_i, \beta_i, \gamma_i,$ and $\delta_i \in R$. Let the code generated by matrix M_σ be denoted by $\mathfrak{C}_\sigma$. Then the length of the code $\mathfrak{C}_\sigma$ is $2(n + \frac{n}{r})$. Now, we can prove our main result.

Lemma 4.2.1. *Let R be a finite commutative Frobenius ring with characteristic 2 and $G = \{g_1, g_2, \cdots, g_r\}$ be a finite group of order r, so that*

$$N_\sigma = \begin{pmatrix} \sigma(v_1) & \sigma(v_2) & \cdots & \sigma(v_{\frac{n}{r}}) \\ \sigma(v_{\frac{n}{r}}) & \sigma(v_1) & \cdots & \sigma(v_{\frac{n}{r}-1}) \\ \vdots & \vdots & \ldots & \vdots \\ \sigma(v_2) & \sigma(v_3) & \cdots & \sigma(v_1) \end{pmatrix},$$

where $v_1, v_2, \cdots, v_{\frac{n}{r}}$ are the elements of RG and $\sigma(v_1), \sigma(v_2), \cdots, \sigma(v_{\frac{n}{r}})$ are group-ring matrices of $n \times n$ order. Then

$$\sigma(v_k)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(v_k)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_k\\ \vdots\\ \mu_k\end{pmatrix}(k = 1, 2, \cdots, \frac{n}{r}),$$

where $\mu_1 = \sum_{g\in G} \alpha_g$, $\mu_2 = \sum_{g\in G} \beta_g$, $\cdots$, $\mu_{\frac{n}{r}} = \sum_{g\in G} \delta_g$.

Proof. *Clearly, $\sigma(v_1) = (\alpha_{g_i^{-1}g_j})_{i,j=1,\cdots,r}$, $\sigma(v_2) = (\beta_{g_i^{-1}g_j})_{i,j=1,\cdots,r}$, and $\sigma(v_{\frac{n}{r}}) = (\delta_{g_i^{-1}g_j})_{i,j=1,\cdots,r}$.*

Now, the $i-th$ element of column $\sigma(v_1)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{r} \alpha_{g_i^{-1}g_j} = \sum_{g\in G} \alpha_{g_i^{-1}g} = \sum_{g\in G} \alpha_g = \mu_1, g_i \in G, g_i^{-1} \in G,$$

and the $i-th$ element of column $\sigma(v_1)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{r} \alpha_{g_j^{-1}g_i} = \sum_{g\in G} \alpha_{g^{-1}g_i} = \sum_{g\in G} \alpha_{gg_i} = \sum_{g\in G} \alpha_g = \mu_1, g_i \in G.$$

Thus,

$$\sigma(v_1)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(v_1)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_1\\ \vdots\\ \mu_1\end{pmatrix}.$$

Similarly, the $i-th$ element of column $\sigma(v_2)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{r} \beta_{g_i^{-1}g_j} = \sum_{g\in G} \beta_{g_i^{-1}g} = \sum_{g\in G} \beta_g = \mu_2, g_i \in G, g_i^{-1} \in G,$$

and the $i-th$ element of column $\sigma(v_2)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{r} \beta_{g_j^{-1}g_i} = \sum_{g\in G} \beta_{g^{-1}g_i} = \sum_{g\in G} \beta_{gg_i} = \sum_{g\in G} \beta_g = \mu_2, g_i \in G.$$

Thus,

$$\sigma(v_2)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(v_2)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_2\\ \vdots\\ \mu_2\end{pmatrix}.$$

Continuing this way, the i−th element of column $\sigma(v_{\frac{n}{r}})\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{r}\delta_{g_i^{-1}g_j} = \sum_{g\in G}\delta_{g_i^{-1}g} = \sum_{g\in G}\delta_g = \mu_{\frac{n}{r}}, g_i \in G, g_i^{-1} \in G,$$

and the i−th element of column $\sigma(v_{\frac{n}{r}})^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{r}\delta_{g_j^{-1}g_i} = \sum_{g\in G}\delta_{g^{-1}g_i} = \sum_{g\in G}\delta_{gg_i} = \sum_{g\in G}\delta_g = \mu_{\frac{n}{r}}, g_i \in G.$$

Thus,

$$\sigma(v_{\frac{n}{r}})\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(v_{\frac{n}{r}})^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_{\frac{n}{r}}\\ \vdots\\ \mu_{\frac{n}{r}}\end{pmatrix}.$$

□

In 2019, (19, Theorem 3.1) Dougherty, Gildea, Korban, Kaya, Tylyshchak, and Yildiz introduced the concept of a single border matrix for the construction of self-dual codes from group rings. In 2019, (24, Theorem 3.2) Gildea, Taylor, Kaya, and Tylyshchak introduced the concept of a double border matrix for self-dual codes construction from group rings. In Theorem 4.2.2, we have extended these two results by introducing the concept of $\frac{n}{r}$-th border matrix and demonstrating that, under certain conditions, we can generate self-dual codes of order $2(n + \frac{n}{r})$ by a group of order r. As a result, we can construct those extremal self-dual codes that can not be attained by the technique used in (24), i.e., extremal self-dual codes of lengths 32, and 40, as shown in Table 4.5, and 4.6, respectively. By extending the concepts of (19) and (24) in Theorem 4.2.2, we can construct those extremal self-dual codes that have not been obtained in (19) and (24). In particular, we built the well-known Extended Binary Golay Code, as shown in Tables 4.1 and 4.3, Codes A_1 and B_1; the Extended QR Code, as shown in Tables 4.2 and 4.4, Codes I_2 and J_1; and various other extremal self-dual codes that are listed in Section 4.4.

Theorem 4.2.2. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order r, and $\mathfrak{C}_\sigma$ be a code generated by the matrix M_σ such that rank of a matrix M_σ is $(n+\frac{n}{r})$. Then $\mathfrak{C}_\sigma$ is a self-dual code of length $2(n+\frac{n}{r})$ if and only if*

1. $\sum_{i=1}^{\frac{n}{r}}(\alpha_i^2+\beta_i^2)+r(\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2))=0.$

2. $\alpha_1\alpha_{\frac{n}{r}}+\beta_1\beta_{\frac{n}{r}}+r(\gamma_1\gamma_{\frac{n}{r}}+\delta_1\delta_{\frac{n}{r}})+\sum_{i=2}^{n/r}(\alpha_i\alpha_{i-1})+\sum_{i=2}^{n/r}(\beta_i\beta_{i-1})+r(\sum_{i=2}^{n/r}(\gamma_i\gamma_{i-1})+\sum_{i=2}^{n/r}(\delta_i\delta_{i-1}))=0.$

3. $\alpha_1\alpha_{\frac{n}{r}-1}+\alpha_2\alpha_{\frac{n}{r}}+\beta_1\beta_{\frac{n}{r}-1}+\beta_2\beta_{\frac{n}{r}}+r(\gamma_1\gamma_{\frac{n}{r}-1}+\gamma_2\gamma_{\frac{n}{r}}+\delta_1\delta_{\frac{n}{r}-1}+\delta_2\delta_{\frac{n}{r}})+\sum_{i=3}^{n/r}(\alpha_i\alpha_{i-2})+\sum_{i=3}^{n/r}(\beta_i\beta_{i-2})+r(\sum_{i=3}^{n/r}(\gamma_i\gamma_{i-2})+\sum_{i=3}^{n/r}(\delta_i\delta_{i-2}))=0.$

4. $\sigma(\sum_{i=1}^{\frac{n}{r}}v_iv_i^*)=I_r+(\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2))circ(\underbrace{1,\cdots,1}_{r-times}).$

5. $\sigma(v_1v_{\frac{n}{r}}^*+\sum_{i=2}^{\frac{n}{r}}v_iv_{i-1}^*)=(\gamma_{\frac{n}{r}}\gamma_1+\delta_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\gamma_i\gamma_{i+1}+\delta_i\delta_{i+1}))circ(\underbrace{1,\cdots,1}_{r-times}).$

6. $\sigma(v_1v_{\frac{n}{r}-1}^*+v_2v_{\frac{n}{r}}^*+\sum_{i=3}^{\frac{n}{r}}v_iv_{i-2}^*)=(\gamma_{\frac{n}{r}}\gamma_2+\gamma_{\frac{n}{r}-1}\gamma_1+\delta_{\frac{n}{r}}\delta_2+\delta_{\frac{n}{r}-1}\delta_1+\sum_{i=1}^{\frac{n}{r}-2}(\gamma_i\gamma_{i+2}+\delta_i\delta_{i+2}))circ(\underbrace{1,\cdots,1}_{r-times}).$

7. $\sigma(v_{\frac{n}{r}}v_1^*+\sum_{i=1}^{\frac{n}{r}-1}v_iv_{i+1})=(\gamma_{\frac{n}{r}}\gamma_1+\delta_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\gamma_i\gamma_{i+1}+\delta_i\delta_{i+1}))circ(\underbrace{1,\cdots,1}_{r-times}).$

8. $\gamma_1\alpha_1+\sum_{i=0}^{\frac{n}{r}-2}(\gamma_{\frac{n}{r}-i}\alpha_{i+2})+\gamma_1+\delta_1\beta_1+\sum_{i=0}^{\frac{n}{r}-2}(\delta_{\frac{n}{r}-i}\beta_{i+2})+\sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i)=0.$

9. $\sum_{i=0}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_{i+1})+\gamma_{\frac{n}{r}}+\sum_{i=0}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_{i+1})+\mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1})=0.$

10. $\gamma_{\frac{n}{r}}\alpha_{\frac{n}{r}}+\sum_{i=1}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_i)+\gamma_{\frac{n}{r}-1}+\delta_{\frac{n}{r}}\beta_{\frac{n}{r}}+\sum_{i=1}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_i)+\mu_1\delta_{\frac{n}{r}-1}+\mu_2\delta_{\frac{n}{r}}+\sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2})=0.$

11. $\gamma_1\alpha_2+\gamma_2\alpha_1+\sum_{i=0}^{\frac{n}{r}-3}(\gamma_{\frac{n}{r}-i}\alpha_{i+3})+\gamma_2+\delta_1\beta_2+\delta_2\beta_1+\sum_{i=0}^{\frac{n}{r}-3}(\delta_{\frac{n}{r}-i}\beta_{i+3})+\mu_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1})=0.$

Proof. *Let $M_\sigma=\begin{bmatrix}M_1 & M_2 & M_3 & M_4\\ M_2^T & I_n & M_4^T & N_\sigma\end{bmatrix}$, where $M_1=circ(\alpha_1,\alpha_2,\cdots,\alpha_{\frac{n}{r}})$, $M_2=CIRC(B_1,B_2,\cdots,B_{\frac{n}{r}})$, $M_3=circ(\beta_1,\beta_2,\cdots,\beta_{\frac{n}{r}})$, $M_4=CIRC(K_1,K_2,\cdots,K_{\frac{n}{r}})$, $B_1=(\gamma_1,\cdots,\gamma_1)\in R^r$, $B_2=(\gamma_2,\cdots,\gamma_2)\in R^r$, $B_{\frac{n}{r}}=(\gamma_{\frac{n}{r}},\cdots,\gamma_{\frac{n}{r}})\in R^r$, $K_1=(\delta_1,\cdots,\delta_1)\in R^r$, $K_2=(\delta_2,\cdots,\delta_2)\in R^r$, $K_{\frac{n}{r}}=(\delta_{\frac{n}{r}},\cdots,\delta_{\frac{n}{r}})\in R^r$. Then*

$$M_\sigma M_\sigma^T=\begin{bmatrix}M_1M_1^T+M_2M_2^T+M_3M_3^T+M_4M_4^T & M_1M_2+M_2+M_3M_4+M_4N_\sigma^T\\ M_2^TM_1^T+M_2^T+M_4^TM_3^T+N_\sigma M_4^T & M_2^TM_2+I_n+M_4^TM_4+N_\sigma N_\sigma^T\end{bmatrix}.$$

Now,

$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{\frac{n}{r}}(\alpha_i^2+\beta_i^2) + r(\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)), \alpha_1\alpha_{\frac{n}{r}} + \beta_1\beta_{\frac{n}{r}} + \sum_{i=2}^{n/r}(\alpha_i\alpha_{i-1}+\beta_i\beta_{i-1}) + r(\gamma_1\gamma_{\frac{n}{r}} + \delta_1\delta_{\frac{n}{r}} + \sum_{i=2}^{n/r}(\gamma_i\gamma_{i-1}+\delta_i\delta_{i-1})), \alpha_1\alpha_{\frac{n}{r}-1} + \alpha_2\alpha_{\frac{n}{r}} + \beta_1\beta_{\frac{n}{r}-1} + \beta_2\beta_{\frac{n}{r}} + \sum_{i=3}^{n/r}(\beta_i\beta_{i-2}+\alpha_i\alpha_{i-2}) + r(\gamma_1\gamma_{\frac{n}{r}-1} + \gamma_2\gamma_{\frac{n}{r}} + \delta_1\delta_{\frac{n}{r}-1} + \delta_2\delta_{\frac{n}{r}} + \sum_{i=3}^{n/r}(\gamma_i\gamma_{i-2}+\delta_i\delta_{i-2})), \cdots, \alpha_1\alpha_{\frac{n}{r}} + \beta_1\beta_{\frac{n}{r}} + \sum_{i=2}^{n/r}(\alpha_i\alpha_{i-1}+\beta_i\beta_{i-1}) + r(\gamma_1\gamma_{\frac{n}{r}} + \delta_1\delta_{\frac{n}{r}} + \sum_{i=2}^{n/r}(\gamma_i\gamma_{i-1}+\delta_i\delta_{i-1})),$

and

$M_2^TM_2 + I_n + M_4^TM_4 + N_\sigma N_\sigma^T = circ(A, B, D, \cdots, E) + I_n + N_\sigma N_\sigma^T$ *where* $A = (\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2))circ(\underbrace{1,\cdots,1}_{r-times})$, $B = (\gamma_{\frac{n}{r}}\gamma_1 + \delta_{\frac{n}{r}}\delta_1 + \sum_{i=1}^{\frac{n}{r}-1}(\gamma_i\gamma_{i+1}+\delta_i\delta_{i+1}))circ(\underbrace{1,\cdots,1}_{r-times})$,

$D = (\gamma_{\frac{n}{r}}\gamma_2 + \gamma_{\frac{n}{r}-1}\gamma_1 + \delta_{\frac{n}{r}}\delta_2 + \delta_{\frac{n}{r}-1}\delta_1 + \sum_{i=1}^{\frac{n}{r}-2}(\gamma_i\gamma_{i+2}+\delta_i\delta_{i+2}))circ(\underbrace{1,\cdots,1}_{r-times})$,

$E = (\gamma_{\frac{n}{r}}\gamma_1 + \delta_{\frac{n}{r}}\delta_1 + \sum_{i=1}^{\frac{n}{r}-1}(\gamma_i\gamma_{i+1}+\delta_i\delta_{i+1}))circ(\underbrace{1,\cdots,1}_{r-times})$, *and* $N_\sigma N_\sigma^T = circ(F, G, H, \cdots, I)$ *where* $F = \sigma(\sum_{i=1}^{\frac{n}{r}} v_iv_i^*)$, $G = \sigma(v_1v_{\frac{n}{r}}^* + \sum_{i=2}^{\frac{n}{r}} v_iv_{i-1}^*)$, $H = \sigma(v_1v_{\frac{n}{r}-1}^* + v_2v_{\frac{n}{r}}^* + \sum_{i=3}^{\frac{n}{r}} v_iv_{i-2}^*)$, *and* $I = \sigma(v_{\frac{n}{r}}v_1^* + \sum_{i=1}^{\frac{n}{r}-1} v_iv_{i+1})$.

It follows from Lemma 4.2.1 that

$$N_\sigma M_4^T = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \cdots & \sigma(v_{\frac{n}{r}}) \\ \sigma(v_{\frac{n}{r}}) & \sigma(v_1) & \sigma(v_2) & \cdots & \sigma(v_{\frac{n}{r}-1}) \\ \sigma(v_{\frac{n}{r}-1}) & \sigma(v_{\frac{n}{r}}) & \sigma(v_1) & \cdots & \sigma(v_{\frac{n}{r}-2}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma(v_2) & \sigma(v_3) & \sigma(v_4) & \cdots & \sigma(v_1) \end{bmatrix} \begin{bmatrix} \delta_1 & \delta_{\frac{n}{r}} & \delta_{\frac{n}{r}-1} & \cdots & \delta_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \delta_1 & \delta_{\frac{n}{r}} & \delta_{\frac{n}{r}-1} & \cdots & \delta_2 \\ \delta_2 & \delta_1 & \delta_{\frac{n}{r}} & \cdots & \delta_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \delta_2 & \delta_1 & \delta_{\frac{n}{r}} & \cdots & \delta_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \delta_{\frac{n}{r}} & \delta_{\frac{n}{r}-1} & \delta_{\frac{n}{r}-2} & \cdots & \delta_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \delta_{\frac{n}{r}} & \delta_{\frac{n}{r}-1} & \delta_{\frac{n}{r}-2} & \cdots & \delta_1 \end{bmatrix} =$$

$$\begin{bmatrix}
\sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i) & \mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}) & \mu_1\delta_{\frac{n}{r}-1}+\mu_2\delta_{\frac{n}{r}}+\sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}) & \cdots & \mu_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i) & \mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}) & \mu_1\delta_{\frac{n}{r}-1}+\mu_2\delta_{\frac{n}{r}}+\sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}) & \cdots & \mu_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}) \\
\mu_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}) & \sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i) & \mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}) & \cdots & \mu_{\frac{n}{r}}\delta_2+\mu_{\frac{n}{r}-1}\delta_1+\sum_{i=1}^{\frac{n}{r}-2}(\mu_i\delta_{i+2}) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\mu_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}) & \sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i) & \mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}) & \cdots & \mu_{\frac{n}{r}}\delta_2+\mu_{\frac{n}{r}-1}\delta_1+\sum_{i=1}^{\frac{n}{r}-2}(\mu_i\delta_{i+2}) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}) & \mu_1\delta_{\frac{n}{r}-1}+\mu_2\delta_{\frac{n}{r}}+\sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}) & \cdots & \cdots & \sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
\mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}) & \mu_1\delta_{\frac{n}{r}-1}+\mu_2\delta_{\frac{n}{r}}+\sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}) & \cdots & \cdots & \sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i)
\end{bmatrix}$$

$= CIRC((\sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i))c, (\mu_1\delta_{\frac{n}{r}} + \sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}))c, (\mu_1\delta_{\frac{n}{r}-1} + \mu_2\delta_{\frac{n}{r}} + \sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}))c, \cdots, \cdots, (\mu_{\frac{n}{r}}\delta_1 + \sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}))c)$, *where* $c = \begin{bmatrix}1\\ \vdots \\ 1\end{bmatrix}_{r\times 1}$.

Additionally,

$M_2^TM_1^T + M_2^T + M_4^TM_3^T + N_\sigma M_4^T = CIRC((\gamma_1\alpha_1 + \sum_{i=0}^{\frac{n}{r}-2}(\gamma_{\frac{n}{r}-i}\alpha_{i+2}))c, (\sum_{i=0}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_{i+1}))c, (\gamma_{\frac{n}{r}}\alpha_{\frac{n}{r}} + \sum_{i=1}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_i))c, \cdots, \cdots, (\gamma_1\alpha_2 + \gamma_2\alpha_1 + \sum_{i=0}^{\frac{n}{r}-3}(\gamma_{\frac{n}{r}-i}\alpha_{i+3}))c) +$
$CIRC(\gamma_1c, \gamma_{\frac{n}{r}}c, \gamma_{\frac{n}{r}-1}c, \cdots, \cdots, \gamma_2c) + CIRC((\delta_1\beta_1 + \sum_{i=0}^{\frac{n}{r}-2}(\delta_{\frac{n}{r}-i}\beta_{i+2}))c, (\sum_{i=0}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_{i+1}))c, (\delta_{\frac{n}{r}}\beta_{\frac{n}{r}} + \sum_{i=1}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_i))c, \cdots, \cdots, (\delta_1\beta_2 + \delta_2\beta_1 + \sum_{i=0}^{\frac{n}{r}-3}(\delta_{\frac{n}{r}-i}\beta_{i+3}))c) + CIRC((\sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i))c, (\mu_1\delta_{\frac{n}{r}} + \sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}))c, (\mu_1\delta_{\frac{n}{r}-1} + \mu_2\delta_{\frac{n}{r}} + \sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}))c, \cdots, \cdots, (\mu_{\frac{n}{r}}\delta_1 + \sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}))c)$
$= CIRC((\gamma_1\alpha_1 + \sum_{i=0}^{\frac{n}{r}-2}(\gamma_{\frac{n}{r}-i}\alpha_{i+2}) + \gamma_1 + \delta_1\beta_1 + \sum_{i=0}^{\frac{n}{r}-2}(\delta_{\frac{n}{r}-i}\beta_{i+2}) + \sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i))c,$
$(\sum_{i=0}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_{i+1}) + \gamma_{\frac{n}{r}} + \sum_{i=0}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_{i+1}) + \mu_1\delta_{\frac{n}{r}} + \sum_{i=2}^{\frac{n}{r}}(\mu_i\delta_{i-1}))c, (\gamma_{\frac{n}{r}}\alpha_{\frac{n}{r}} + \sum_{i=1}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_i) + \gamma_{\frac{n}{r}-1} + \delta_{\frac{n}{r}}\beta_{\frac{n}{r}} + \sum_{i=1}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_i) + \mu_1\delta_{\frac{n}{r}-1} + \mu_2\delta_{\frac{n}{r}} + \sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2}))c, \cdots, \cdots, (\gamma_1\alpha_2 + \gamma_2\alpha_1 + \sum_{i=0}^{\frac{n}{r}-3}(\gamma_{\frac{n}{r}-i}\alpha_{i+3}) + \gamma_2 + \delta_1\beta_2 + \delta_2\beta_1 + \sum_{i=0}^{\frac{n}{r}-3}(\delta_{\frac{n}{r}-i}\beta_{i+3}) + \mu_{\frac{n}{r}}\delta_1 + \sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1}))c).$

Clearly, $M_\sigma M_\sigma^T$ *is a symmetric matrix and* $\mathfrak{C}_\sigma$ *is self-orthogonal if* $\sum_{i=1}^{\frac{n}{r}}(\alpha_i^2 + \beta_i^2) + r(\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2 + \delta_i^2)) = 0$, $\alpha_1\alpha_{\frac{n}{r}} + \beta_1\beta_{\frac{n}{r}} + r(\gamma_1\gamma_{\frac{n}{r}} + \delta_1\delta_{\frac{n}{r}}) + \sum_{i=2}^{n/r}(\alpha_i\alpha_{i-1}) + \sum_{i=2}^{n/r}(\beta_i\beta_{i-1}) + r(\sum_{i=2}^{n/r}(\gamma_i\gamma_{i-1}) + \sum_{i=2}^{n/r}(\delta_i\delta_{i-1})) = 0,$

$\alpha_1\alpha_{\frac{n}{r}-1}+\alpha_2\alpha_{\frac{n}{r}}+\beta_1\beta_{\frac{n}{r}-1}+\beta_2\beta_{\frac{n}{r}}+r(\gamma_1\gamma_{\frac{n}{r}-1}+\gamma_2\gamma_{\frac{n}{r}}+\delta_1\delta_{\frac{n}{r}-1}+\delta_2\delta_{\frac{n}{r}})+\sum_{i=3}^{n/r}(\alpha_i\alpha_{i-2})+\sum_{i=3}^{n/r}(\beta_i\beta_{i-2})+r(\sum_{i=3}^{n/r}(\gamma_i\gamma_{i-2})+\sum_{i=3}^{n/r}(\delta_i\delta_{i-2}))=0$, $\alpha_1\alpha_{\frac{n}{r}-2}+\alpha_2\alpha_{\frac{n}{r}-1}+\alpha_3\alpha_{\frac{n}{r}}+\beta_1\beta_{\frac{n}{r}-2}+\beta_2\beta_{\frac{n}{r}-1}+\beta_3\beta_{\frac{n}{r}}+r(\gamma_1\gamma_{\frac{n}{r}-2}+\gamma_2\gamma_{\frac{n}{r}-1}+\gamma_3\gamma_{\frac{n}{r}}+\delta_1\delta_{\frac{n}{r}-2}+\delta_2\delta_{\frac{n}{r}-1}+\delta_3\delta_{\frac{n}{r}})+\sum_{i=4}^{n/r}(\alpha_i\alpha_{i-3})+\sum_{i=4}^{n/r}(\beta_i\beta_{i-3})+r(\sum_{i=4}^{n/r}(\gamma_i\gamma_{i-3})+\sum_{i=4}^{n/r}(\delta_i\delta_{i-3}))=0$, $\sigma(\sum_{i=1}^{\frac{n}{r}}v_iv_i^*)=I_r+(\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2))circ(\underbrace{1,\cdots,1}_{r-times})$, $\sigma(v_1v_{\frac{n}{r}}^*+\sum_{i=2}^{\frac{n}{r}}v_iv_{i-1}^*)=(\gamma_{\frac{n}{r}}\gamma_1+\delta_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\gamma_i\gamma_{i+1}+\delta_i\delta_{i+1}))circ(\underbrace{1,\cdots,1}_{r-times})$, $\sigma(v_1v_{\frac{n}{r}-1}^*+v_2v_{\frac{n}{r}}^*+\sum_{i=3}^{\frac{n}{r}}v_iv_{i-2}^*)=(\gamma_{\frac{n}{r}}\gamma_2+\gamma_{\frac{n}{r}-1}\gamma_1+\delta_{\frac{n}{r}}\delta_2+\delta_{\frac{n}{r}-1}\delta_1+\sum_{i=1}^{\frac{n}{r}-2}(\gamma_i\gamma_{i+2}+\delta_i\delta_{i+2}))circ(\underbrace{1,\cdots,1}_{r-times})$, $\sigma(v_{\frac{n}{r}}v_1^*+\sum_{i=1}^{\frac{n}{r}-1}v_iv_{i+1})=(\gamma_{\frac{n}{r}}\gamma_1+\delta_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\gamma_i\gamma_{i+1}+\delta_i\delta_{i+1}))circ(\underbrace{1,\cdots,1}_{r-times})$,

$\gamma_1\alpha_1+\sum_{i=0}^{\frac{n}{r}-2}(\gamma_{\frac{n}{r}-i}\alpha_{i+2})+\gamma_1+\delta_1\beta_1+\sum_{i=0}^{\frac{n}{r}-2}(\delta_{\frac{n}{r}-i}\beta_{i+2})+\sum_{i=1}^{\frac{n}{r}}(\mu_i\delta_i)=0$, $\sum_{i=0}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_{i+1})+\gamma_{\frac{n}{r}}+\sum_{i=0}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_{i+1})+\mu_1\delta_{\frac{n}{r}}+\sum_{i=2}^{\frac{n}{r}}(\_i\delta_{i-1})=0$, $\gamma_{\frac{n}{r}}\alpha_{\frac{n}{r}}+\sum_{i=1}^{\frac{n}{r}-1}(\gamma_{\frac{n}{r}-i}\alpha_i)+\gamma_{\frac{n}{r}-1}+\delta_{\frac{n}{r}}\beta_{\frac{n}{r}}+\sum_{i=1}^{\frac{n}{r}-1}(\delta_{\frac{n}{r}-i}\beta_i)+\mu_1\delta_{\frac{n}{r}-1}+\mu_2\delta_{\frac{n}{r}}+\sum_{i=3}^{\frac{n}{r}}(\mu_i\delta_{i-2})=0,\cdots,$ $\gamma_1\alpha_2+\gamma_2\alpha_1+\sum_{i=0}^{\frac{n}{r}-3}(\gamma_{\frac{n}{r}-i}\alpha_{i+3})+\gamma_2+\delta_1\beta_2+\delta_2\beta_1+\sum_{i=0}^{\frac{n}{r}-3}(\delta_{\frac{n}{r}-i}\beta_{i+3})+\mu_{\frac{n}{r}}\delta_1+\sum_{i=1}^{\frac{n}{r}-1}(\mu_i\delta_{i+1})=0$.

Since the rank of the matrix M_σ is $(n+\frac{n}{r})$ and $\mathfrak{C}_\sigma$ is self-orthogonal under conditions proved above, we can say that the code $\mathfrak{C}_\sigma$ is a self-dual code if all the above conditions are satisfied. □

In Corollaries 4.2.3 and 4.2.4, we have established a relationship between the group ring element and the unitary unit and non-unit.

Corollary 4.2.3. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order r, and $\mathfrak{C}_\sigma$ be a self-dual code. Then $\sum_{i=1}^{\frac{n}{r}}v_iv_i^*\in RG$ is a unitary unit if $\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)=0$ condition is satisfied.*

Proof. *If $\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)=0$, then $\sigma(\sum_{i=1}^{\frac{n}{r}}v_iv_i^*)=I_r$. Then, $\sum_{i=1}^{\frac{n}{r}}v_iv_i^*=1$. Hence, $\sum_{i=1}^{\frac{n}{r}}v_iv_i^*\in RG$ is a unitary unit.* □

Corollary 4.2.4. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order r where (r is odd), and $\mathfrak{C}_\sigma$ be a self-dual code. Then $\sum_{i=1}^{\frac{n}{r}}v_iv_i^*\in RG$ is a non-unit if $\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)=1$ condition is satisfied.*

Proof. *If* $\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)=1$, *then* $\sigma(\sum_{i=1}^{\frac{n}{r}} v_i v_i^*) = I_r + circ(\underbrace{1,\cdots,1}_{r-times}) = circ(0,\underbrace{1,\cdots,1}_{(r-1)-times})$ *and*

$$det\begin{bmatrix}0 & 1 & \cdots & 1\\ 1 & 0 & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 1 & \cdots & 0\end{bmatrix} = (r-1)det\begin{bmatrix}1 & 1 & \cdots & 1\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix} = 0\ (if\ r\ is\ odd).$$

Therefore, $det(\sum_{i=1}^{\frac{n}{r}} v_i v_i^*) = 0$ *and* $\sum_{i=1}^{\frac{n}{r}} v_i v_i^*$ *is a non-unit by corollary 3 of (33).* □

In Corollary 4.2.5, we have established a relationship between the group ring element and the idempotent, which has not been established in (19) and (24).

Corollary 4.2.5. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order r where (r is odd), and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then* $\sum_{i=1}^{\frac{n}{r}} v_i v_i^* \in RG$ *is an idempotent if* $\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)=1$ *condition is satisfied.*

Proof. *If* $\sum_{i=1}^{\frac{n}{r}}(\gamma_i^2+\delta_i^2)=1$, *then* $\sigma(\sum_{i=1}^{\frac{n}{r}} v_i v_i^*) = I_r - circ(\underbrace{1,\cdots,1}_{r-times}) = I_r + circ(\underbrace{1,\cdots,1}_{r-times})$ *and the matrix* $circ(\underbrace{1,\cdots,1}_{r-times})$ *is an idempotent matrix. Since if T is an idempotent matrix then* $I-T$ *is also an idempotent matrix, which implies* $\sigma(\sum_{i=1}^{\frac{n}{r}} v_i v_i^*)$ *is an idempotent matrix. Hence, an element* $\sum_{i=1}^{\frac{n}{r}} v_i v_i^*$ *is an idempotent element.* □

4.3 Computational results

Now, using this new construction over the field F_2 and the ring $F_2 + uF_2$, we will design the well-known Extended Binary Golay Codes $[24, 12, 8]$, Extended Quadratic Residue Code $[48, 24, 12]$, and extremal self-dual codes of various lengths 32 and 40. We use the (54) SAGE software for all the computational results.

Algorithm:

INPUT: F_2 Field.

OUTPUT: Extremal self-dual codes.

1. Create the matrix M_σ over the field F_2 by the structure described in 4.2.

(a) Create the boundary matrices M_1, M_2, M_3, and M_4, where $M_1 = circ(\alpha_1, \alpha_2, \cdots, \alpha_{\frac{n}{r}})$, $M_2 = CIRC(B_1, B_2, \cdots, B_{\frac{n}{r}})$, $M_3 = circ(\beta_1, \beta_2, \cdots, \beta_{\frac{n}{r}})$, $M_4 = CIRC(K_1, K_2, \cdots, K_{\frac{n}{r}})$, $B_1 = (\gamma_1, \cdots, \gamma_1) \in R^r$, $B_2 = (\gamma_2, \cdots, \gamma_2) \in R^r$, $B_{\frac{n}{r}} = (\gamma_{\frac{n}{r}}, \cdots, \gamma_{\frac{n}{r}}) \in R^r$, $K_1 = (\delta_1, \cdots, \delta_1) \in R^r$, $K_2 = (\delta_2, \cdots, \delta_2) \in R^r$, $K_{\frac{n}{r}} = (\delta_{\frac{n}{r}}, \cdots, \delta_{\frac{n}{r}}) \in R^r$.

(b) Create the group ring matrices $\sigma(v_1), \sigma(v_2), \cdots, \sigma(v_{\frac{n}{r}})$ over the field F_2.

(c) Create the generator matrix M_σ of order $(\frac{n}{r}+n)\times(2(\frac{n}{r}+n))$ by using all feasible combinations of the matrices acquired in Steps 1(a) and (b).

2. Create extremal self-dual codes.

(a) Shortlist those matrices from Step 1(c) that produce self-dual codes $\mathfrak{C}_\sigma$ of length $2(\frac{n}{r} + n)$, i.e., those matrices that satisfy the condition $M_\sigma M_\sigma^T = 0$ and have rank $(\frac{n}{r} + n)$.

(b) The self-dual codes generated from the matrices shortlisted in Step 2(a) are of the parameters $\mathfrak{C}_\sigma[2(\frac{n}{r} + n), \frac{n}{r} + n, d_{min}]$, where d_{min} is the minimum distance defined as $d_{min} = min\{d(l, m)|l \neq m\}$ such that $d(l, m) = |\{i|1 \leq i \leq 2(\frac{n}{r}+n), l_i \neq m_i\}|$, where $l, m \in F_2^{2(\frac{n}{r}+n)}$ are the codewords for the code $\mathfrak{C}_\sigma$.

(c) Shortlist the extremal self-dual codes from Step 2(b) by using Theorem 4.2.2 and classifying them as Type I and Type II codes.

3. Create the matrix M_σ over the ring F_2+uF_2 by the structure described in the Section 4.2.

(a) Lift the matrix, which generates the extremal self-dual codes in Step 2(c), by lifting an element 0 of F_2 to elements 0 and u of $F_2 + uF_2$ and by lifting an element 1 of F_2 to elements 1 and $1 + u$ of $F_2 + uF_2$.

4. Create extremal self-dual codes.

(a) Select only those matrices from Step 3 that result in self-dual codes $\mathfrak{C}_\sigma$ of length $2(\frac{n}{r} + n)$ with d_L as the smallest positive Lee distance.

(b) Evaluate d_L, where d_L is defined as the Lee distance between $2(\frac{n}{r} + n)$ tuples, i.e., the sum of the Lee weights of the difference between the components of these tuples. The Lee weights of the terms $0, 1, u$, and $1 + u$ are $0, 1, 2$, and 1, respectively.

(c) Choose the matrices from Step 4(a) whose associated self-dual codes have a Lee distance d_L equal to the minimum distance of extremal self-dual codes of length $4(\frac{n}{r} + n)$, and classify these obtained self-dual codes as of Type I or Type II.

4.3.1 Construction of extremal self-dual codes of lengths 24 and 48 from C_3

We execute the above construction for $G = C_3$. By considering $n = 9$ and $r = 3$, i.e., by using triple-bordered construction, a binary extremal self-dual code with parameters $[24, 12, 6]$ and the well-known Extended Binary Golay Code is constructed over the F_2 field.

Table 4.1: Construction of Extended Binary Golay Code from $G = C_3$ over F_2

$Code(A_i)$	$(\alpha_1, \alpha_2, \alpha_3, \gamma_1, \gamma_2, \gamma_3, \beta_1, \beta_2, \beta_3, \delta_1, \delta_2, \delta_3)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$Type$
1	$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	$(1, 0, 0)$	$(0, 1, 0)$	$(0, 1, 1)$	$[24, 12, 8]_{II}$
2	$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	$(1, 0, 0)$	$(1, 0, 0)$	$(0, 0, 1)$	$[24, 12, 6]_I$

Now we will give the lift of $F_2 + uF_2$ to the codes in Table 4.1. The codes obtained are a binary extremal self-dual code with parameters $[48, 24, 10]$ and the Extended Quadratic Residue Code, as listed in Table 4.2.

Table 4.2: The extremal binary self-dual codes of length 48 obtained from the $F_2 + uF_2$ lift of A_1

$Code(I_i)$		$(\alpha_1, \alpha_2, \alpha_3, \gamma_1, \gamma_2, \gamma_3, \beta_1, \beta_2, \beta_3, \delta_1, \delta_2, \delta_3)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$Type$
1	A_1	$(1, 0, 0, 1, 1, 0, 1, u, 1, 1, 0, 0)$	$(1, 0, 0)$	$(0, u+1, u)$	$(0, 1, u+1)$	$[48, 24, 10]_I$
2	A_1	$(1, 0, 0, 1, 1, u, u+1, 0, 1, 1, 0, u)$	$(1, 0, u)$	$(0, u+1, u)$	$(0, 1, 1)$	$[48, 24, 12]_{II}$

4.3.2 Construction of extremal self-dual codes of lengths 24 and 48 from C_2

We execute the above construction for $G = C_2$. By considering $n = 8$ and $r = 2$, i.e., by using fourth-bordered construction, a binary extremal self-dual code with parameters $[24, 12, 6]$ and the well-known Extended Binary Golay Code is constructed over the F_2 field.

Table 4.3: Construction of Extended Binary Golay Code from $G = C_2$ over F_2

$Code(B_i)$	$(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\gamma_1,\gamma_2,\gamma_3,\gamma_4,\beta_1,\beta_2,\beta_3,\beta_4,\delta_1,\delta_2,\delta_3,\delta_4)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$f_{(\sigma(v_4))}$	$Type$
1	$(1,1,1,0,1,0,0,0,0,1,0,0,1,1,1,0)$	$(0,0)$	$(1,0)$	$(1,0)$	$(1,0)$	$[24,12,8]_{II}$
2	$(0,1,0,0,1,1,0,1,1,1,1,0,1,1,1,0)$	$(0,0)$	$(1,0)$	$(1,0)$	$(1,0)$	$[24,12,6]_{I}$

Now we will give the lift of $F_2 + uF_2$ to the codes in Table 4.3. The code obtained is the Extended Quadratic Residue Code, as listed in Table 4.4.

Table 4.4: The Extended Quadratic Residue Code $[48,24,12]$, obtained from the F_2+uF_2 lift of B_1

$Code(J_i)$		$(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\gamma_1,\gamma_2,\gamma_3,\gamma_4,\beta_1,\beta_2,\beta_3,\beta_4,\delta_1,\delta_2,\delta_3,\delta_4)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$f_{(\sigma(v_4))}$
1	B_1	$(1,1,1,0,1,0,0,0,0,u+1,0,0,u+1,1,u+1,u)$	$(0,u)$	$(1,0)$	$(1,0)$	$(1,0)$

4.3.3 Construction of extremal self-dual codes of length 32 from C_3

We execute the above construction for $G = C_3$. By considering $n = 12$ and $r = 3$, i.e., by using fourth-bordered construction, a binary extremal self-dual code with parameters $[32,16,8]$ of both Type I and Type II is constructed over F_2 field.

Table 4.5: Construction of extremal self-dual codes of length 32 from $G = C_3$ over F_2

$Code(D_i)$	$(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\gamma_1,\gamma_2,\gamma_3,\gamma_4,\beta_1,\beta_2,\beta_3,\beta_4,\delta_1,\delta_2,\delta_3,\delta_4)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$f_{(\sigma(v_4))}$	$Type$
1	$(0,0,0,1,0,0,1,1,1,0,0,1,1,0,1,1)$	$(0,0,0)$	$(1,0,0)$	$(1,0,0)$	$(0,1,1)$	$[32,16,8]_{I}$
2	$(0,1,0,0,0,0,1,1,1,0,0,1,1,0,0,0)$	$(0,0,0)$	$(1,0,0)$	$(1,0,0)$	$(0,1,1)$	$[32,16,8]_{II}$

4.3.4 Construction of extremal self-dual codes of length 40 from C_4

We execute the above construction for $G = C_4$. By considering $n = 16$ and $r = 4$, i.e., by using fourth-bordered construction, a binary extremal self-dual code with parameters $[40,20,8]$ of both Type I and Type II is constructed over F_2 field.

Table 4.6: Construction of extremal self-dual code of length 40 from $G = C_4$ over F_2

$Code(G_i)$	$(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \beta_1, \beta_2, \beta_3, \beta_4, \delta_1, \delta_2, \delta_3, \delta_4)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$f_{(\sigma(v_4))}$	$Type$
1	$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	$(0, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	$[40, 20, 8]_I$
2	$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	$(0, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	$(1, 0, 0, 0)$	$[40, 20, 8]_{II}$

4.4 Conclusion

This chapter proposes a new $\frac{n}{r}$-th bordered construction of group rings to create binary linear self-dual codes. We come up with certain conditions that when this $\frac{n}{r}$-th bordered construction will generate self-dual codes. We have connected non-units, units, and idempotents with the self-dual codes. We illustrated the importance of this new $\frac{n}{r}$-th bordered construction by constructing the well-known Extended Binary Golay Code, Extended Quadratic Residue Code, and many extremal binary self-dual codes of lengths 32 and 40. We suggest two feasible directions for future research. One way is to take a group of higher order, as with the increase in order of group there is an increase in length of self-dual codes. This may potentially trigger a computational issue. The other feasible area for research can be to apply the constructions to Frobenious rings R_k for $k \geq 2$. However, this will increase the computational complexity as $|R_2| = 16$, $|R_3| = 256$, etc. i.e, with the increase in value of k, there is an increase in the cardinality of R_k.

Chapter 5

Group ring construction of $[64, 32, 12]$ Type II linear block code

---

In this chapter, we introduce the double-bordered construction of self-dual codes whose generator matrix is of the form $M = [I_n|A]$ where A is a block matrix consisting of blocks which comes from group rings and the elements in the first row cannot completely determine the block matrix A. We demonstrate that this construction is feasible for a group of order $2n$ where n is a natural number, over the Frobenius ring R_k. We show the significance of this new construction by constructing several extremal self-dual codes of lengths 20, 40, 32, *and* 64 *over the field F_2 and the ring $F_2 + uF_2$.*

5.1 Introduction

Algebraic codes and group rings have a natural relation. This strong relationship between group rings and the algebraic codes is often endorsed in the effective quest for extremal binary self-dual codes.

The work in this chapter is arranged as follows: In section 5.2.1, we have given the new construction i.e. the introduction of a double border around the generator matrix of the form $M = [I_n|A]$ where A is a block matrix consisting of blocks which comes from group rings and the elements in the first row cannot completely determine the block matrix A. Identical generator matrices are in (18) and (22). In this section, we have proved our main theorem. We specified the practicality and effectiveness of the theorem by constructing many extremal self-dual codes of various lengths in section 5.3. Finally, in section 5.4 we have given the conclusion of our work.

5.2 Main matrix construction

Now, we will outline our main construction. Let $v \in RG$, where R is a finite commutative Frobenius ring of characteristic 2, and G is a group of order n. The matrix is defined as follows

$$M_\sigma = \left[\begin{array}{cc|ccc|ccc|cc|ccc|ccc}
\beta_1 & \beta_2 & \beta_3 & \cdots & \beta_3 & \beta_4 & \cdots & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \cdots & \beta_7 & \beta_8 & \cdots & \beta_8 \\
\beta_2 & \beta_1 & \beta_4 & \cdots & \beta_4 & \beta_3 & \cdots & \beta_3 & \beta_6 & \beta_5 & \beta_8 & \cdots & \beta_8 & \beta_7 & \cdots & \beta_7 \\
\hline
\beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\
\vdots & \vdots & & I_n & & & 0 & & \vdots & \vdots & & \sigma(v_1) & & & \sigma(v_2) & \\
\beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\
\hline
\beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & & \\
\vdots & \vdots & & 0 & & & I_n & & \vdots & \vdots & & \sigma(v_2) & & & \sigma(v_3) & \\
\beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & &
\end{array}\right].$$

Let $\mathfrak{C}_\sigma$ be a code generated through the matrix M_σ. Then, the code $\mathfrak{C}_\sigma$ has length $4n + 4$.

Lemma 5.2.1. *Let R be a finite commutative Frobenius ring with characteristic 2, $G = \{g_1, g_2, \cdots, g_n\}$ be a finite group of order n such that*

$$N_\sigma = \begin{pmatrix} \sigma(v_1) & \sigma(v_2) \\ \sigma(v_2) & \sigma(v_3) \end{pmatrix},$$

where v_1, v_2, and v_3 are the elements of RG, and $\sigma(v_1)$, $\sigma(v_2)$, and $\sigma(v_3)$ are $n \times n$ group ring matrices. Then

$$\sigma(v_k)\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \sigma(v_k)^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_k \\ \vdots \\ \mu_k \end{pmatrix} (k = 1, 2, 3),$$

where $\mu_1 = \sum_{g \in G} \alpha_g$, $\mu_2 = \sum_{g \in G} \beta_g$, and $\mu_3 = \sum_{g \in G} \gamma_g$.

Proof. *Clearly, $\sigma(v_1) = (\alpha_{g_i^{-1} g_j})_{i,j=1,\cdots,n}$, $\sigma(v_2) = (\beta_{g_i^{-1} g_j})_{i,j=1,\cdots,n}$, and $\sigma(v_3) = (\gamma_{g_i^{-1} g_j})_{i,j=1,\cdots,n}$.*

Now, the $i-$th element of column $\sigma(v_1)\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ is

$$\sum_{j=1}^{n} \alpha_{g_i^{-1} g_j} = \sum_{g \in G} \alpha_{g_i^{-1} g} = \sum_{g \in G} \alpha_g = \mu_1, g_i \in G, g_i^{-1} \in G,$$

and the i−th element of column $\sigma(v_1)^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ *is*

$$\sum_{j=1}^{n} \alpha_{g_j^{-1} g_i} = \sum_{g \in G} \alpha_{g^{-1} g_i} = \sum_{g \in G} \alpha_{g g_i} = \sum_{g \in G} \alpha_g = \mu_1, g_i \in G.$$

Thus,

$$\sigma(v_1) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \sigma(v_1)^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_1 \end{pmatrix}.$$

Furthermore, the i−th element of column $\sigma(v_2) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ *is*

$$\sum_{j=1}^{n} \beta_{g_i^{-1} g_j} = \sum_{g \in G} \beta_{g_i^{-1} g} = \sum_{g \in G} \beta_g = \mu_2, g_i \in G, g_i^{-1} \in G,$$

and the i−th element of column $\sigma(v_2)^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ *is*

$$\sum_{j=1}^{n} \beta_{g_j^{-1} g_i} = \sum_{g \in G} \beta_{g^{-1} g_i} = \sum_{g \in G} \beta_{g g_i} = \sum_{g \in G} \beta_g = \mu_2, g_i \in G.$$

Thus,

$$\sigma(v_2) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \sigma(v_2)^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_2 \\ \vdots \\ \mu_2 \end{pmatrix}.$$

Similarly, the i−th element of column $\sigma(v_3) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ *is*

$$\sum_{j=1}^{n} \gamma_{g_i^{-1} g_j} = \sum_{g \in G} \gamma_{g_i^{-1} g} = \sum_{g \in G} \gamma_g = \mu_3, g_i \in G, g_i^{-1} \in G,$$

and the i−th element of column $\sigma(v_3)^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ *is*

$$\sum_{j=1}^{n} \gamma_{g_j^{-1} g_i} = \sum_{g \in G} \gamma_{g^{-1} g_i} = \sum_{g \in G} \gamma_{g g_i} = \sum_{g \in G} \gamma_g = \mu_3, g_i \in G.$$

Thus,

$$\sigma(v_3)\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \sigma(v_3)^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_3\\ \vdots\\ \mu_3\end{pmatrix}.$$

□

Theorem 5.2.2. *Let R be a finite commutative Frobenius ring of characteristic 2, $G = \{g_1, g_2, \cdots, g_n\}$ be a finite group of order n, and $\mathfrak{C}_\sigma$ be a code generated by the matrix M_σ such that rank of the matrix M_σ is $2n+2$. Then $\mathfrak{C}_\sigma$ is a self-dual code of length $4n+4$ if and only if*

Case I: *n is odd*

1. $\sum_{i=0}^{8} \beta_i = 0.$

2. $\sigma(v_1v_1^* + v_2v_2^*) = I_n + (\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2)\begin{bmatrix}1 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 1\end{bmatrix}_{n\times n}.$

3. $v_1v_2^* + v_2v_3^* = 0.$

4. $v_2v_1^* + v_3v_2^* = 0.$

5. $\sigma(v_2v_2^* + v_3v_3^*) = I_n + (\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2)\begin{bmatrix}1 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 1\end{bmatrix}_{n\times n}.$

6. $\beta_3(\beta_1 + 1) + \beta_4\beta_2 + \beta_7(\mu_1 + \beta_5) + \beta_8(\beta_6 + \mu_2) = 0.$

7. $\beta_4(\beta_1 + 1) + \beta_3\beta_2 + \beta_8(\mu_1 + \beta_5) + \beta_7(\beta_6 + \mu_2) = 0.$

8. $\beta_4(\beta_1 + 1) + \beta_3\beta_2 + \beta_7(\mu_1 + \beta_6) + \beta_8(\beta_5 + \mu_3) = 0.$

9. $\beta_3(\beta_1 + 1) + \beta_4\beta_2 + \beta_7(\mu_3 + \beta_5) + \beta_8(\beta_6 + \mu_2) = 0.$

Case II: *n is even*

1. $\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2 = 0.$

2. *Conditions 2 to 9 for this case are the same as for the case 'n is odd'.*

Proof. *Let* $M_\sigma = \begin{bmatrix}M_1 & M_2 & M_3 & M_4\\ M_2^T & I_{2n} & M_4^T & N_\sigma\end{bmatrix}$*, where* $M_1 = circ(\beta_1,\beta_2)$*,* $M_2 = CIRC(A_1, A_2)$*,* $M_3 = circ(\beta_5,\beta_6)$*,* $M_4 = CIRC(A_3, A_4)$*,* $A_1 = (\beta_3, ..., \beta_3) \in R^n$*,* $A_2 = (\beta_4, ..., \beta_4) \in R^n$*,*

$A_3 = (\beta_7, ..., \beta_7) \in R^n$, $A_4 = (\beta_8, ..., \beta_8) \in R^n$, *and* $N_\sigma = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) \\ \sigma(v_2) & \sigma(v_3) \end{bmatrix}$. *Then*

$$M_\sigma M_\sigma^T = \begin{bmatrix} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T & M_1M_2 + M_2 + M_3M_4 + M_4N_\sigma^T \\ M_2^TM_1^T + M_2^T + M_4^TM_3^T + N_\sigma M_4^T & M_2^TM_2 + I_{2n} + M_4^TM_4 + N_\sigma N_\sigma^T \end{bmatrix}.$$

Now,

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + n\beta_{i+2}^2 + \beta_{i+4}^2 + n\beta_{i+6}^2), 0).$$

Case I: *n is odd*

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+2}^2 + \beta_{i+4}^2 + \beta_{i+6}^2), 0) = circ(\sum_{i=1}^{8}\beta_i^2, 0).$$

Case II: *n is even*

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+4}^2), 0) = circ(\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2, 0).$$

and

$$M_2^TM_2 + I_{2n} + M_4^TM_4 + N_\sigma N_\sigma^T = \sum_{i=1}^{2}\beta_{i+2}^2 + \alpha_{i+6}^2 CIRC(\boldsymbol{B}, \boldsymbol{0}) + I_{2n} + N_\sigma N_\sigma^T$$

where $\boldsymbol{B} = circ(\underbrace{1, \cdots, 1}_{n-times})$, $\boldsymbol{0} = circ(\underbrace{0, \cdots, 0}_{n-times})$ *and*

$$N_\sigma N_\sigma^T = \begin{bmatrix} \sigma(v_1v_1^* + v_2v_2^*) & \sigma(v_1v_2^* + v_2v_3^*) \\ \sigma(v_2v_1^* + v_3v_2^*) & \sigma(v_2v_2^* + v_3v_3^*) \end{bmatrix}.$$

It follows from Lemma 5.2.1 that

$$N_\sigma B_4^T = \begin{bmatrix} \mu_1\beta_7 + \mu_2\beta_8 & \mu_1\beta_8 + \mu_2\beta_7 \\ \vdots & \vdots \\ \mu_1\beta_7 + \mu_2\beta_8 & \mu_1\beta_8 + \mu_2\beta_7 \\ \mu_2\beta_7 + \mu_3\beta_8 & \mu_2\beta_8 + \mu_3\beta_7 \\ \vdots & \vdots \\ \mu_2\beta_7 + \mu_3\beta_8 & \mu_2\beta_8 + \mu_3\beta_7 \end{bmatrix}.$$

Additionally, $M_2^TM_1^T + M_2^T + M_4^TM_3^T + N_\sigma M_4^T =$

$$\begin{bmatrix} \beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_6\beta_8 + \mu_1\beta_7 + \mu_2\beta_8 & \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\alpha_7 + \mu_1\beta_8 + \mu_2\beta_7 \\ \vdots & \vdots \\ \beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_6\beta_8 + \mu_1\beta_7 + \mu_2\beta_8 & \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_1\beta_8 + \mu_2\beta_7 \\ \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_2\beta_7 + \mu_3\beta_8 & \beta_4\beta_2 + \beta_3\beta_1 + \beta_3 + \beta_5\beta_7 + \beta_6\beta_8 + \mu_2\beta_8 + \mu_3\beta_7 \\ \vdots & \vdots \\ \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_6\beta_7 + \mu_2\beta_7 + \mu_3\beta_8 & \beta_4\beta_2 + \beta_3\beta_1 + \beta_3 + \beta_5\beta_7 + \beta_6\beta_8 + \mu_2\beta_8 + \mu_3\beta_7 \end{bmatrix}.$$

Clearly, $M_\sigma M_\sigma^T$ *is a symmetric matrix and* $\mathfrak{C}_\sigma$ *is self orthogonal if for* $\sum_{i=0}^{8}\beta_i = 0$, $\sigma(v_1v_1^* + v_2v_2^*) = I_n + (\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$, $v_1v_2^*+v_2v_3^* = 0$, $v_2v_1^*+v_3v_2^* = 0$, $\sigma(v_2v_2^*+v_3v_3^*) = I_n + (\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2)\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$, $\beta_3(\beta_1+1)+\beta_4\beta_2+\beta_7(\mu_1+\beta_5)+\beta_8(\beta_6+\mu_2) = 0$, $\beta_4(\beta_1+1)+\beta_3\beta_2+\beta_8(\mu_1+\beta_5)+\beta_7(\beta_6+\mu_2) = 0$, $\beta_4(\beta_1+1)+\beta_3\beta_2+\beta_7(\mu_1+\beta_6)+\beta_8(\beta_5+\mu_3) = 0$, *and* $\beta_3(\beta_1+1)+\beta_4\beta_2+\beta_7(\mu_3+\beta_5)+\beta_8(\beta_6+\mu_2) = 0$. *Since the rank of a matrix* M_σ *is* $2n+2$, *and* $\mathfrak{C}_\sigma$ *is self-orthogonal under conditions proved above, we can say that the code* $\mathfrak{C}_\sigma$ *is a self-dual code if all the conditions mentioned above are satisfied.* □

Corollary 5.2.3. *Let R be a finite commutative Frobenious ring of characteristic 2, G be a finite group of order n, and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then* $v_1v_1^* + v_2v_2^*$, $v_2v_2^* + v_3v_3^* \in RG$ *are unitary units if* $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 0$.

Proof. *If* $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 0$, *then* $\sigma(v_1v_1^*+v_2v_2^*) = \sigma(v_2v_2^*+v_3v_3^*) = I_n$ *and* $v_1v_1^*+v_2v_2^* = v_2v_2^*+v_3v_3^* = 1$. *Thus,* $v_1v_1^*+v_2v_2^*$ *and* $v_2v_2^*+v_3v_3^*$ *are unitary units.* □

Corollary 5.2.4. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n(even), and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then* $v_1v_1^*+v_2v_2^*$, $v_2v_2^*+v_3v_3^* \in RG$ *are units.*

Proof. *If n is even, then*

$$K = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}^2 = 0$$

that is K is a nilpotent matrix.
As $\sigma(v_1v_1^*+v_2v_2^*) = I_n + K$. *If k is nilpotent then* $1+k$ *is unit. Thus,* $v_1v_1^*+v_2v_2^*$ *is unit. Similarly, we can say that* $v_2v_2^*+v_3v_3^*$ *is unit.* □

Corollary 5.2.5. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then* $v_1v_1^*+v_2v_2^*$, $v_2v_2^*+v_3v_3^* \in RG$ *are non units if* $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 1$.

Proof. *If* $\beta_3^2+\beta_4^2+\beta_7^2+\beta_8^2 = 1$, *then*

$$\sigma(v_1v_1^*+v_2v_2^*) = I_n + \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{n\times n} = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}_{n\times n},$$

and

$$det(\sigma(v_1v_1^*+v_2v_2^*)) = det\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}_{n\times n} = (n-1)det\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n} = 0\,(if\ n\ is\ odd).$$

Therefore, $det(\sigma(v_1v_1^* + v_2v_2^*)) = 0$ *and* $v_1v_1^* + v_2v_2^*$ *is a non-unit by corollary 3 of (33). Similarly,* $det(\sigma(v_2v_2^* + v_3v_3^*)) = 0$ *and* $v_2v_2^* + v_3v_3^*$ *is a non-unit.* □

Corollary 5.2.6. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then* $v_1v_1^*+v_2v_2^*$, $v_2v_2^*+v_3v_3^* \in RG$ *are idempotents if* $\alpha_3^2 + \alpha_4^2 + \alpha_7^2 + \alpha_8^2 = 1$.

Proof. *If n is odd, then* $\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}^2 = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$ *that is* $\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}$ *is an idempotent matrix.*

If $\beta_3^2 + \beta_4^2 + \beta_7^2 + \beta_8^2 = 1$*, then*

$$\sigma(v_1v_1^* + v_2v_2^*) = I_n + \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n} = I_n - \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}_{n\times n}.$$

If T is an idempotent matrix, then $I - T$ *is also an idempotent matrix. Thus,* $\sigma(v_1v_1^* + v_2v_2^*)$ *is an idempotent matrix and* $v_1v_1^* + v_2v_2^*$ *is an idempotent element. Similarly, we can say that* $v_2v_2^* + v_3v_3^*$ *is an idempotent element.* □

5.3 Computational results

Now, we will design extremal self-dual codes of different lengths of $20, 32, 40, 64$ using groups of orders of $4, 7$. For all our computational calculations we have used the SAGE software (54). Algorithm:
INPUT: Field F_2.
OUTPUT: Extremal self-dual codes.

1. Generate matrices $\sigma(v_1)$, $\sigma(v_2)$, and $\sigma(v_3)$ of order $n \times n$ by a group of order n, over the field F_2.

2. Generate boundary matrices M_1, M_2, M_3, and M_4 over the Field F_2, where $M_1 = circ(\beta_1, \beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5, \beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, ..., \beta_3) \in R^n$, $A_2 = (\beta_4, ..., \beta_4) \in R^n$, $A_3 = (\beta_7, ..., \beta_7) \in R^n$, and $A_4 = (\beta_8, ..., \beta_8) \in R^n$.

3. Construct the set of generator matrices M_σ of order $(2n+2) \times (4n+4)$ having the structure mentioned in Section 5.2.1 using all the possible combinations of matrices obtained in Step 1 and Step 2.

4. From the given set of generator matrices, collect matrices that satisfy the condition $M_\sigma M_\sigma^T = 0$ and have rank $2n+2$. These matrices generate self-dual codes $\mathfrak{C}_\sigma$ with parameters $[4n+4, 2n+2, d_{min}]$, where d_{min} is the minimum distance of the code.

5. Evaluate $d_{min} = min\{d(a, b) | a \neq b\}$ for the self-dual codes that are generated from matrices collected in Step 4. Here, $d(a, b) = |\{i | 1 \leq i \leq 4n+4, a_i \neq b_i\}|$, where $a, b \in F_2^{4n+4}$ are the codewords of length $4n+4$ for the code $\mathfrak{C}_\sigma$.

6. Shortlist matrices from Step 4, whose d_{min} of its corresponding self-dual code matches the minimum distance of extremal self-dual codes of length $4n+4$. Refer to Theorem 1.1.4 for the minimum distance of extremal self-dual codes. In this step, we obtain matrices that generate the extremal self-dual codes $\mathfrak{C}_\sigma$ of length $4n+4$.

7. Classify self-dual codes constructed from the matrices obtained in Step 6 are of Type I or Type II. The binary self-dual code $\mathfrak{C}_\sigma$ is said to be of Type I and Type II if the weight of all of its codewords is divisible by two and four respectively. The weight of a codeword a is defined as $w(a) = d(a, 0)$, where $0 = (0, 0, \cdots, 0)$ is the zero vector.

8. Lift the obtained self-dual codes in Step 7, to the ring $F_2 + uF_2$, as discussed in Section 1.1.10. Generate a set of all possible lifted matrices by mapping an element 0 of F_2 to two elements 0 and u of the ring $F_2 + uF_2$ and element 1 of F_2 is mapped to elements 1 and $1+u$ of the ring $F_2 + uF_2$.

9. From the given set of uplifted matrices, collect matrices that can generate self-dual codes of length 4n+4, as done in Step 4.

10. Evaluate d_L for the self-dual codes generated from matrices collected in Step 9. Here d_L denotes a code's smallest positive Lee distance. The Lee weight of the ring $F_2 + uF_2$ elements $0, 1, u$ and $1 + u$ are $0, 1, 2$ and 1 respectively. The Lee distance between $4n + 4$ tuple is defined as the sum of Lee weights of the difference between the components of these tuples.

11. Shortlist matrices whose d_L of its corresponding self-dual code matches the minimum distance of extremal self-dual codes of length $2(4n + 4)$. In this step, we obtain matrices that can generate the self-dual codes over the ring $F_2 + uF_2$ of length $4n+4$, whose binary images are extremal self-dual codes of length $2(4n+4)$.

12. Classify self-dual codes constructed from the matrices obtained in Step 11 are of Type I or Type II.

5.3.1 Construction from cyclic group of order 4

We execute the above construction for $G = C_4$. The extremal self-dual codes of length 20 (Type I) are constructed by considering the above-defined construction over F_2 field.

Table 5.1: Self-dual codes of length 20 from C_4 over F_2

$Code(A_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$\lvert Aut(A_i)\rvert$	$Type$
1	$(1,0,1,1,1,0,0,0)$	$(1,0,0,0)$	$(0,0,0,0)$	$(1,1,1,0)$	$2^{15}\cdot 3^3\cdot 5$	$[20,10,4]_I$
2	$(1,0,1,1,1,0,0,0)$	$(1,0,0,0)$	$(1,0,1,0)$	$(1,1,0,1)$	$2^{13}\cdot 3\cdot 5$	$[20,10,4]_I$

Now we will give the lift of F_2+uF_2 on the codes of Table 5.1. The codes generated are binary extremal self-dual code with parameters $[40,20,8]$ as listed in Table 5.2.

Table 5.2: The extremal binary self-dual codes of length 40 obtained from F_2+uF_2 lift of A_1 and A_2.

$Code(I_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$Type$
1	A_1	$(1,0,1,1,1,0,0,u)$	$(1,0,0,0)$	$(0,u,u,0)$	$(1,1,1,0)$	$TypeI$
2	A_1	$(u+1,u,u+1,u+1,u+1,0,u,0)$	$(u+1,u,u,u)$	$(u,0,0,u)$	$(u+1,u+1,u+1,0)$	$TypeII$
3	A_2	$(1,0,1,1,1,0,0,u)$	$(1,0,0,0)$	$(1,0,u+1,u)$	$(1,1,u,1)$	$TypeI$
4	A_2	$(u+1,u,u+1,u+1,u+1,0,u,0)$	$(u+1,u,u,u)$	$(u+1,u,1,0)$	$(u+1,u+1,0,u+1)$	$TypeII$

5.3.2 Construction from $C_2\times C_2$ group

We execute the above construction for $G=C_2\times C_2$. The extremal self-dual codes of length 20 (Type I) are constructed by considering the above-defined construction over F_2 field.

Table 5.3: Self-dual codes of length 20 from $C_2\times C_2$ over F_2

$Code(B_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$\mathrm{f}_{(\sigma(v_1))}$	$\mathrm{f}_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$\lvert Aut(B_i)\rvert$	$Type$
1	$(1,0,1,1,1,0,0,0)$	$(0,0,1,0)$	$(0,0,0,0)$	$(0,0,0,1)$	$2^{17}\cdot 3^4\cdot 5^2\cdot 7$	$[20,10,4]_I$
2	$(1,0,1,1,1,0,0,0)$	$(0,0,1,0)$	$(0,0,1,1)$	$(0,0,0,1)$	$2^{15}\cdot 3^2$	$[20,10,4]_I$
3	$(1,0,1,1,1,0,0,0)$	$(0,0,1,0)$	$(0,0,1,1)$	$(1,1,1,0)$	$2^{13}\cdot 3\cdot 5$	$[20,10,4]_I$

Now we will give the lift of F_2+uF_2 on the codes of Table 5.3. The codes obtained are binary extremal self-dual codes with parameters $[40,20,8]$ as listed in Table 5.4.

Table 5.4: The extremal binary self-dual codes of length 40 obtained from $F_2 + uF_2$ lift of B_1, B_2, and B_3.

$Code(J_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$Type$
1	B_1	$(1,0,1,1,1,0,0,u)$	$(0,u,1,0)$	$(0,0,u,u)$	$(0,u,0,1)$	$TypeI$
2	B_1	$(u+1,u,u+1,u+1,u+1,0,u,0)$	$(u,0,u+1,0)$	$(u,u,0,0)$	$(u,0,0,u+1)$	$TypeII$
3	B_2	$(1,0,1,1,1,0,0,u)$	$(0,0,1,0)$	$(0,u,1,1)$	$(0,u,0,1)$	$TypeI$
4	B_2	$(u+1,u,u+1,u+1,u+1,0,u,0)$	$(u,u,u+1,u)$	$(u,0,u+1,u+1)$	$(u,0,0,1)$	$TypeII$
5	B_3	$(1,0,1,1,1,0,0,u)$	$(0,0,1,0)$	$(0,u,1,1)$	$(1,1,1,u)$	$TypeI$
6	B_3	$(u+1,u,u+1,u+1,u+1,0,u,0)$	$(u,u,u+1,u)$	$(u,0,u+1,u+1)$	$(u+1,u+1,u+1,0)$	$TypeII$

5.3.3 Construction from cyclic group of order 7

Finally, we execute the above-defined construction for $G = C_7$ over F_2. The extremal self-dual code of length 32 is constructed by considering the above-defined construction over F_2 field.

Table 5.5: Self-dual codes of length 32 from C_7 over F_2

$Code(D_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$\lvert Aut(D_i)\rvert$	$Type$
1	$(1,0,0,0,1,1,0,1)$	$(1,1,0,1,0,0,0)$	$(1,0,0,0,0,0,0)$	$(1,0,0,0,1,0,1)$	$2^6\cdot 3\cdot 7$	$[32,16,6]_I$

Now we will give the lift of $F_2 + uF_2$ on the codes of Table 5.5. The codes obtained are binary extremal self-dual code with parameters $[64, 32, 12]$ as listed in Table 5.6.

Table 5.6: The extremal binary self-dual codes of length 64 obtained from $F_2 + uF_2$ lift of D_1.

$Code(K_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	$f_{(\sigma(v_1))}$	$f_{(\sigma(v_2))}$	$f_{(\sigma(v_3))}$	$Type$
1	D_1	$(1,0,0,0,u+1,u+1,0,1)$	$(u+1,u+1,0,u+1,u,0,u)$	$(u+1,u,u,u,0,0,u)$	$(1,u,u,u,u+1,u,1)$	$TypeI$
2	D_1	$(1,0,0,0,u+1,u+1,u,1)$	$(u+1,u+1,0,u+1,u,0,u)$	$(u+1,u,u,u,0,0,u)$	$(1,u,u,u,u+1,u,1)$	$TypeII$

5.4 Conclusion

In this chapter, we have proposed a double-bordered construction of self-dual codes whose generator matrix is of the form $G = [I_n|A]$, where A is a block matrix consisting of blocks that come from group rings and the elements in the first row cannot completely determine the block matrix A, to create binary linear self-dual codes. We have given certain conditions that need to be fulfilled for building self-dual codes by this new construction. We have created a relationship between the self-dual codes and non-units/units of group rings and showcased the importance of this new construction by constructing several extremal binary self-dual codes of lengths 20, 40, 32, 64.

Chapter 6

Double bordered constructions of linear self-dual codes from altered four-circulant matrix over Frobenius rings

A new technique for the construction of self-dual codes is presented in this chapter. Double borders are introduced around a new, altered form of a four-circulant matrix. Using this new construction over the field F_2 and the ring $F_2 + uF_2$, and groups of orders $2, 3, 4, 5, 7,$ *and* 9*, we generate extremal binary self-dual codes of the following lengths:* $12, 20, 24, 32, 40, 48, 64,$ *and* 80.

6.1 Introduction

Self-dual codes are linear codes with strong connections to groups, designs, and lattices. The research on constructions for extremal binary self-dual codes is substantial.

In the literature, there have been some well-known construction techniques for building self-dual codes. In 1969, Chen and Karlin introduced the concept of a pure double circulant construction technique for constructing self-dual codes; see (6) and (36) for more details. In 2003, Betsumiya (3) gave the concept of the four-circulant construction. The generator matrix of the four-circulant matrix is defined as

$$M = \left[\begin{array}{cc|cc} I_n & & A & B \\ & I_n & B^T & A^T \end{array}\right],$$

where A and B are $n \times n$ circulant matrices. Then the matrix M generates the self-dual codes over the field F_2 if and only if the $AA^T + BB^T = I_n$ condition is satisfied.
In this chapter, we formulate the following modification of the four-circulant matrix: We replaced the matrix A with a reverse circulant matrix C and the matrix B with a group ring matrix, i.e., $\sigma(v_1)$. The new modified four-circulant matrix takes the form:

$$\left[\begin{array}{cc|cc} I_n & & C & \sigma(v_1) \\ & I_n & \sigma(v_1)^T & C \end{array}\right].$$

Next, we blend this new, altered version of the four-circulant matrix with the concept of double-bordered construction (24). The motivation of this chapter is to produce those extremal self-dual codes of various lengths that can not be obtained through the construction defined in (3) and (24).
The rest of the chapter is structured as follows: In Section 6.2, we present the new techniques and conditions required for constructing self-dual codes. The theoretical results are also discussed. In Section 6.3, the new way is applied to obtain numerical results: Extended Binary Golay Code, Extended Quadratic Residue Code, and extremal binary self-dual codes of the following lengths: $12, 16, 24, 32, 40, 48, 64$, and 80. We have used the SAGE (54) software for all the computer calculations. In this section, we tabulate the outcomes as well. The chapter ends with concluding remarks and recommendations for possible expansion of this work.

6.2 Main matrix construction

Now, we will outline our main construction. We define a double border around the new altered form of the four-circulant matrix, which uses reverse-circulant matrices and the idea of group rings. Let $v_1 \in RG$, where R is a finite commutative Frobenius ring of characteristic 2, and G is a group of order n. Define the following matrix:

$$M_\sigma = \left[\begin{array}{cc|ccc|ccc|cc|ccc|ccc}
\beta_1 & \beta_2 & \beta_3 & \cdots & \beta_3 & \beta_4 & \cdots & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \cdots & \beta_7 & \beta_8 & \cdots & \beta_8 \\
\beta_2 & \beta_1 & \beta_4 & \cdots & \beta_4 & \beta_3 & \cdots & \beta_3 & \beta_6 & \beta_5 & \beta_8 & \cdots & \beta_8 & \beta_7 & \cdots & \beta_7 \\
\hline
\beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\
\vdots & \vdots & & I_n & & & 0 & & \vdots & \vdots & & C & & & \sigma(v_1) & \\
\beta_3 & \beta_4 & & & & & & & \beta_7 & \beta_8 & & & & & & \\
\hline
\beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & & \\
\vdots & \vdots & & 0 & & & I_n & & \vdots & \vdots & & \sigma(v_1)^T & & & C & \\
\beta_4 & \beta_3 & & & & & & & \beta_8 & \beta_7 & & & & & &
\end{array}\right],$$

where $\beta_i \in R$, $\sigma(v_1)$ is a group-ring matrix of order n, and C is a reverse circulant matrix of order n over a ring R. Let $\mathfrak{C}_\sigma$ be a code that is generated by the matrix M_σ. Then the length of the code $\mathfrak{C}_\sigma$ is $4n+4$.

Lemma 6.2.1. *Let R be a finite commutative Frobenius ring of characteristic 2, $G = \{g_1, g_2, \cdots, g_n\}$ is a finite group of order n, and the matrix N_σ is defined as*

$$N_\sigma = \begin{pmatrix} C & \sigma(v_1) \\ \sigma(v_1)^T & C \end{pmatrix}.$$

Then

$$\sigma(v_1)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \sigma(v_1)^T\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\mu_1\\ \vdots \\ \mu_1\end{pmatrix},$$

where $\mu_1 = \sum_{g\in G} \delta_g$.
Let the sum of all components in the first row of the matrix C be represented by η. Then

$$C\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\eta\\ \vdots \\ \eta\end{pmatrix}.$$

Proof. *Consider the matrices $\sigma(v_1) = (\alpha_{g_i^{-1}g_j})_{i,j=1,\cdots,n}$ and $C = (\gamma_{ij})_{i,j=1,\cdots,n}$.*

Then the $i-th$ element of column $\sigma(v_1)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n} \alpha_{g_i^{-1}g_j} = \sum_{g\in G} \alpha_{g_i^{-1}g} = \sum_{g\in G} \alpha_g = \mu_1, g_i \in G, g_i^{-1} \in G,$$

and the $i-th$ element of column $\sigma(v_1)^T\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ is

$$\sum_{j=1}^{n} \alpha_{g_j^{-1}g_i} = \sum_{g\in G} \alpha_{g^{-1}g_i} = \sum_{g\in G} \alpha_{gg_i} = \sum_{g\in G} \alpha_g = \mu_1, g_i \in G.$$

Therefore,

$$\sigma(v_1)\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \sigma(v_1)^T\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = \begin{pmatrix}\mu_1\\ \vdots \\ \mu_1\end{pmatrix}.$$

Furthermore, the i−th element of column $C\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ *is*

$$\sum_{j=1}^{n} \gamma_{ij} = \gamma_{i1} + \gamma_{i2} + \cdots + \gamma_{in} = \eta.$$

Hence,

$$C\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\eta\\ \vdots\\ \eta\end{pmatrix}.$$

.

□

In 2003, Betsumiya (3) introduced the concept of four-circulant matrices and showed that with circulant matrices of order n, we can generate a self-dual code of order $4n$. In Theorem 6.2.2, we generalize this result by replacing matrix A with a reverse circulant matrix C and matrix B by a group ring matrix $\sigma(v_1)$. Furthermore, we extend this result by introducing a double border around this generalized form of a four-circulant matrix and proving that, under certain conditions, a group of order n can generate self-dual codes of order $4n + 4$. In 2020, Gildea (24) introduced the idea of double-bordered construction. The idea of a reverse circulant matrix is not used in their primary matrix construction. In our primary matrix, we have utilized the idea of a reverse circulant matrix. Additionally, Theorem 3.2 of (24) was only applicable to groups of order $2p$ (where p is an odd prime), but by Theorem 6.2.2, we have expanded it to cover all groups of order n. In Theorem 6.2.2, we have merged the concepts of four-circulant (3) and double border (24), which results in the generation of extremal self-codes that can not be generated individually by the methods given in (3) and (24).

Theorem 6.2.2. *Let R be a finite commutative Frobenius ring with characteristic 2, G be a finite group of order n, and $\mathfrak{C}_\sigma$ be a code generated by the matrix M_σ such that the rank of the matrix M_σ is $2n + 2$. Then $\mathfrak{C}_\sigma$ is a self-dual code of length $4n + 4$ if the following conditions are satisfied:*

Case I: *n is odd*

1. $\sum_{i=0}^{8} \beta_i = 0.$
2. $C\sigma(v_1) + \sigma(v_1)C = 0.$

3. $\sigma(v_1v_1^*) + C^2 = I_n + (\sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2)circ(\underbrace{1,\cdots,1}_{n-times})$.

4. $\beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_8\beta_6 + \eta\beta_7 + \mu_1\beta_8 = 0$.

5. $\beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_7\beta_6 + \eta\beta_8 + \mu_1\beta_7 = 0$.

Case II: *n is even*

1. $\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2 = 0$.

2. *Conditions 2 to 5 for this case are the same as for the case 'n is odd'.*

Proof. *Let* $M_\sigma = \begin{bmatrix} M_1 & M_2 & M_3 & M_4 \\ M_2^T & I_{2n} & M_4^T & N_\sigma \end{bmatrix}$, *where* $M_1 = circ(\beta_1,\beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5,\beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, ..., \beta_3) \in R^n$, $A_2 = (\beta_4, ..., \beta_4) \in R^n$, $A_3 = (\beta_7, ..., \beta_7) \in R^n$, $A_4 = (\beta_8, ..., \beta_8) \in R^n$, *and* $N_\sigma = \begin{bmatrix} C & \sigma(v_1) \\ \sigma(v_1)^T & C \end{bmatrix}$. *Then*

$$M_\sigma M_\sigma^T = \begin{bmatrix} M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T & M_1M_2 + M_2 + M_3M_4 + M_4N_\sigma^T \\ M_2^TM_1^T + M_2^T + M_4^TM_3^T + N_\sigma M_4^T & M_2^TM_2 + I_{2n} + M_4^TM_4 + N_\sigma N_\sigma^T \end{bmatrix}.$$

Now,

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + n\beta_{i+2}^2 + \beta_{i+4}^2 + n\beta_{i+6}^2), 0).$$

Case I: *n is odd*

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+2}^2 + \beta_{i+4}^2 + \beta_{i+6}^2), 0) = circ(\sum_{i=1}^{8}\beta_i^2, 0).$$

Case II: *n is even*

$$M_1M_1^T + M_2M_2^T + M_3M_3^T + M_4M_4^T = circ(\sum_{i=1}^{2}(\beta_i^2 + \beta_{i+4}^2), 0) = circ(\beta_1^2 + \beta_2^2 + \beta_5^2 + \beta_6^2, 0).$$

and

$$M_2^TM_2 + I_{2n} + M_4^TM_4 + N_\sigma N_\sigma^T = \sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2 CIRC(\boldsymbol{B}, \boldsymbol{0}) + I_{2n} + N_\sigma N_\sigma^T$$

where $\boldsymbol{B} = circ(\underbrace{1,\cdots,1}_{n-times})$, $\boldsymbol{0} = circ(\underbrace{0,\cdots,0}_{n-times})$, *and*

$$N_\sigma N_\sigma^T = \begin{bmatrix} \sigma(v_1v_1^*) + C^2 & C\sigma(v_1) + \sigma(v_1)C \\ \sigma(v_1)^TC + C\sigma(v_1)^T & \sigma(v_1^*v_1) + C^2 \end{bmatrix}.$$

Using Lemma 6.2.1, we get

$$N_\sigma M_4^T = \begin{bmatrix} \eta\beta_7 + \mu_1\beta_8 & \eta\beta_8 + \mu_1\beta_7 \\ \vdots & \vdots \\ \eta\beta_7 + \mu_1\beta_8 & \eta\beta_8 + \mu_1\beta_7 \\ \mu_1\beta_7 + \eta\beta_8 & \mu_1\beta_8 + \eta\beta_7 \\ \vdots & \vdots \\ \mu_1\beta_7 + \eta\beta_8 & \mu_1\beta_8 + \eta\beta_7 \end{bmatrix}.$$

Additionally, $M_2^T M_1^T + M_2^T + M_4^T M_3^T + N_\sigma M_4^T =$

$$\begin{bmatrix} \beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_8\beta_6 + \eta\beta_7 + \mu_1\beta_8 & \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_7\beta_6 + \eta\beta_8 + \mu_1\beta_7 \\ \vdots & \vdots \\ \beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_8\beta_6 + \eta\beta_7 + \mu_1\beta_8 & \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_7\beta_6 + \eta\beta_8 + \mu_1\beta_7 \\ \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_7\beta_6 + \mu_1\beta_7 + \eta\beta_8 & \beta_4\beta_2 + \beta_3\beta_1 + \beta_3 + \beta_7\beta_5 + \beta_8\beta_6 + \mu_1\beta_8 + \eta\beta_7 \\ \vdots & \vdots \\ \beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_7\beta_6 + \mu_1\beta_7 + \eta\beta_8 & \beta_4\beta_2 + \beta_3\beta_1 + \beta_3 + \beta_7\beta_5 + \beta_8\beta_6 + \mu_1\beta_8 + \eta\beta_7 \end{bmatrix}.$$

Clearly, $M_\sigma M_\sigma^T$ *is a symmetric matrix and* $\mathfrak{C}_\sigma$ *is self orthogonal if* $\sum_{i=0}^{8}\beta_i = 0$, $C\sigma(v_2) + \sigma(v_2)C = 0$, $\sigma(v_2v_2^*) + C^2 = I_n + (\sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2)circ(\underbrace{1, \cdots, 1}_{n-times})$, $\beta_3\beta_1 + \beta_4\beta_2 + \beta_3 + \beta_7\beta_5 + \beta_8\beta_6 + \eta\beta_7 + \mu_1\beta_8 = 0$, *and* $\beta_4\beta_1 + \beta_3\beta_2 + \beta_4 + \beta_8\beta_5 + \beta_7\beta_6 + \eta\beta_8 + \mu_1\beta_7 = 0$. *Since the rank of the matrix* M_σ *is* $2n + 2$ *and* $\mathfrak{C}_\sigma$ *is self-orthogonal. Therefore, if all the conditions mentioned above are satisfied, we can conclude that the code* $\mathfrak{C}_\sigma$ *is a self-dual code.* □

Corollary 6.2.3. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n, and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then an element* $v_1 \in RG$ *is a unitary unit if the following conditions are satisfied:*

1. $\sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2 = 0.$
2. $C^2 = 0.$

Proof. *Under the conditions* $C^2 = 0$ *and* $\sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2 = 0$, *we get* $\sigma(v_1v_1^*) = \sigma(v_1^*v_1) = I_n$. *Hence,* $v_1v_1^* = v_1^*v_1 = 1$ *and* v_1 *is a unitary unit.* □

Corollary 6.2.4. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n (odd), and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then an element* $v_1 \in RG$ *is a non-unit if the following conditions are satisfied:*

1. $\sum_{i=1}^{2}\beta_{i+2}^2 + \beta_{i+6}^2 = 1.$

2. $C^2 = 0$.

Proof. *Under the conditions* $C^2 = 0$ *and* $\sum_{i=1}^{2} \beta_{i+2}^2 + \beta_{i+6}^2 = 1$, *we get* $\sigma(v_1 v_1^*) = I_n + circ(\underbrace{1, \cdots, 1}_{n-times})$. *Evaluate,*

$$det(v_1 v_1^*) = det(circ(0, \underbrace{1, 1, \cdots, 1, 1}_{(n-1)-times})) = (n-1)det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n \times n} = 0\ (if\ n\ is\ odd).$$

Hence, $det(v_1 v_1^*) = 0$ *and* v_1 *is a non-unit by Corollary 3 of (33).* □

Corollary 6.2.5. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n, and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then an element* $v_1 \in RG$ *is a non-unit if the following conditions are satisfied:*

1. $\sum_{i=1}^{2} \beta_{i+2}^2 + \beta_{i+6}^2 = 0$.

2. $C^2 = I$.

Proof. *Under the conditions* $C^2 = I$ *and* $\sum_{i=1}^{2} \beta_{i+2}^2 + \beta_{i+6}^2 = 0$, *we get* $\sigma(v_1^* v_1) = 0$. *Hence,* v_1 *is a non-unit.* □

Corollary 6.2.6. *Let R be a finite commutative Frobenius ring of characteristic 2, G be a finite group of order n(odd), and* $\mathfrak{C}_\sigma$ *be a self-dual code. Then an element* $v_1 \in RG$ *is an idempotent if the following conditions are satisfied:*

1. $\sum_{i=1}^{2} \beta_{i+2}^2 + \beta_{i+6}^2 = 1$.

2. $C^2 = 0$.

Proof. *Since n is odd, therefore* $(circ(\underbrace{1, \cdots, 1}_{n-times}))^2 = circ(\underbrace{1, \cdots, 1}_{n-times})$, *which implies* $circ(\underbrace{1, \cdots, 1}_{n-times})$ *is an idempotent matrix.*

Under the conditions $C^2 = 0$ *and* $\sum_{i=1}^{2} \beta_{i+2}^2 + \beta_{i+6}^2 = 1$, *we get*

$$\sigma(v_1 v_1^*) = I_n + circ(\underbrace{1, \cdots, 1}_{n-times}) = I_n - circ(\underbrace{1, \cdots, 1}_{n-times})$$

where $I_n - circ(\underbrace{1, \cdots, 1}_{n-times})$ *is an idempotent matrix. Hence,* $\sigma(v_1 v_1^*)$ *is an idempotent matrix and* $v_1 v_1^*$ *is an idempotent element of RG.* □

6.3 Computational results

In this section, we search for extremal binary self-dual codes with lengths of $12, 16, 20, 24, 32, 40, 48, 64$, and 80 using our main construction over the field F_2 and the ring $F_2 + uF_2$. Specifically, C_2, C_3, C_4, C_5, C_7, and C_9 are taken into consideration as groups of orders $2, 3, 4, 5, 7$, and 9. The well-known Extended QR code and extremal self-dual codes of 64 and 80 lengths are also created using the Gray map. Our entire computational work has been done using the SAGE software (54).

Algorithm:

INPUT: Field F_2.

OUTPUT: Extremal self-dual codes.

1. Generate the matrix M_σ over the field F_2 as per the structure mentioned in Section 6.2.

   (a) Over the field F_2, create boundary matrices M_1, M_2, M_3, and M_4, where $M_1 = circ(\beta_1, \beta_2)$, $M_2 = CIRC(A_1, A_2)$, $M_3 = circ(\beta_5, \beta_6)$, $M_4 = CIRC(A_3, A_4)$, $A_1 = (\beta_3, ..., \beta_3) \in R^n$, $A_2 = (\beta_4, ..., \beta_4) \in R^n$, $A_3 = (\beta_7, ..., \beta_7) \in R^n$, and $A_4 = (\beta_8, ..., \beta_8) \in R^n$.

   (b) Over the field F_2, create $n \times n$ reverse circulant matrices C.

   (c) Over the field F_2, using group of order n create $n \times n$ group ring matrix $\sigma(v)$.

   (d) Over the field F_2, using all the possible combinations of matrices obtained in Steps 1(a), (b), and (c), creates $(2n + 2) \times (4n + 4)$ generator matrices M_σ.

2. Generate extremal self-dual codes.

   (a) From Step 1, shortlist matrices of rank $2n + 2$ that satisfy the condition $M_\sigma M_\sigma^T = 0$, i.e., those matrices that produce self-dual codes $\mathfrak{C}_\sigma[4n + 4, 2n + 2, d_{min}]$, where d_{min} is the minimum distance of the code.

(b) Calculate $d_{min} = min\{d(a,b)|a \neq b\}$ for $\mathfrak{C}_\sigma$. Here, $d(a,b) = |\{i|1 \leq i \leq 4n+4, a_i \neq b_i\}|$, where $a, b \in F_2^{4n+4}$ are the codewords for the code $\mathfrak{C}_\sigma$.

(c) Select those matrices from Step 2(a) whose corresponding self-dual codes have a minimum distance d_{min} that coincides with the minimum distance of extremal self-dual codes of length $4n+4$.

(d) Identify whether the obtained self-dual codes are of Type I or Type II.

3. Generate the matrix M_σ over the ring $F_2 + uF_2$ as per the structure mentioned in the Section 6.2.

(a) Lift the matrices obtained in Step 2(c) by mapping an element 0 of F_2 to two elements 0 and u of the ring $F_2 + uF_2$ and an element 1 of F_2 to two elements 1 and $1+u$ of the ring $F_2 + uF_2$.

4. Generate extremal self-dual codes

(a) Shortlist those matrices from Step 3, that produce self-dual codes $\mathfrak{C}_\sigma$ of length $4n+4$, with d_L as the smallest positive Lee distance of a code.

(b) Calculate d_L. The Lee distance between $4n+4$ tuple is defined as the sum of Lee weights of the difference between the components of these tuples.

(c) Select those matrices from Step 4(a) whose corresponding self-dual codes have a Lee distance d_L that coincides with the minimum distance of extremal self-dual codes of length $2(4n+4)$.

(d) Identify whether the obtained self-dual codes are of Type I or Type II.

6.3.1 Construction from cyclic group of order 2

Here, using the main construction and the cyclic group of order 2 over the binary field F_2, we obtain an extremal self-dual code with parameters $[12, 6, 4]$.

Table 6.1: Extremal self-dual code of length 12 from C_2 over F_2

$Code(A_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$\|Aut(A_i)\|$	$Type$
1	$(1,0,1,1,0,1,0,0)$	$(1,0)$	$(0,0)$	$2^9 \cdot 3^2 \cdot 5$	$[12,6,4]_I$

By lifting the code of Table 6.1 over the ring $F_2 + uF_2$, we obtain an extremal self-dual code of length 24.

Table 6.2: Extremal self-dual code of length 12 from C_2 over $F_2 + uF_2$, whose binary image is an extremal self-dual codes of length 24

$Code(I_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$Type$
1	A_1	$(1,u,1,u+1,0,u+1,0,u)$	$(1,0)$	$(0,u)$	$[24,12,8]_{II}$

6.3.2 Construction from cyclic group of order 3

Here, using the main construction and the cyclic group of order 3 over the binary field F_2, we obtain extremal self-dual codes with parameters $[16, 8, 4]$.

Table 6.3: Extremal self-dual codes of length 16 from C_3 over F_2

$Code(B_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$\|Aut(B_i)\|$	$Type$
1	$(1,0,1,1,0,0,0,1)$	$(1,0,1)$	$(0,0,0)$	$2^{13} \cdot 3^2$	$[16,8,4]_I$
2	$(0,1,1,1,1,0,0,0)$	$(1,0,0)$	$(0,0,0)$	$2^{14} \cdot 3^2 \cdot 5 \cdot 7$	$[16,8,4]_{II}$

By lifting the code of Table 6.3 over the ring $F_2 + uF_2$, we obtain extremal self-dual codes of length 32.

Table 6.4: Extremal self-dual codes of length 16 from C_3 over $F_2 + uF_2$, whose binary images are extremal self-dual codes of length 32

$Code(J_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$Type$
1	B_1	$(1,0,u+1,1,0,0,0,1)$	$(1,0,1)$	$(0,u,u)$	$[32,16,8]_I$
2	B_1	$(1,0,1,u+1,0,0,u,u+1)$	$(1,0,1)$	$(0,u,u)$	$[32,16,8]_{II}$
3	B_2	$(0,u+1,1,u+1,u+1,u,0,u)$	$(u+1,u,u)$	$(0,u,u)$	$[32,16,8]_I$
4	B_2	$(0,1,u+1,u+1,u+1,u,0,u)$	$(1,0,0)$	$(u,0,0)$	$[32,16,8]_{II}$

6.3.3 Construction from cyclic group of order 4

Here, using the main construction and the cyclic group of order 4 over the binary field F_2, we obtain an extremal self-dual code with parameters $[20,10,4]$.

Table 6.5: Extremal self-dual codes of length 20 from C_4 over F_2

$Code(D_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$\lvert Aut(D_i)\rvert$	$Type$
1	$(0,1,0,0,1,0,1,1)$	$(1,0,0,0)$	$(0,0,0,0)$	$2^{17}\cdot 3^4\cdot 5^2\cdot 7$	$[20,10,4]_I$

By lifting the code of Table 6.5 over the ring F_2+uF_2, we obtain extremal self-dual codes of length 40.

Table 6.6: Extremal self-dual codes of length 20 from C_4 over $F_2 + uF_2$, whose binary images are extremal self-dual codes of length 40

$Code(K_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$Type$
1	D_1	$(0,1,u,0,1,0,u+1,u+1)$	$(1,0,0,0)$	$(0,0,u,0)$	$[40,20,8]_I$
2	D_1	$(0,1,u,0,u+1,u,1,1)$	$(1,0,0,0)$	$(0,0,u,0)$	$[40,20,8]_{II}$

6.3.4 Construction from cyclic group of order 5

Here, using the main construction and the cyclic group of order 5 over the binary field F_2, we obtain an extremal self-dual code with parameters $[24,12,6]$ and the Extended Binary Golay Code, i.e., $[24,12,8]$.

Table 6.7: Extremal self-dual codes of length 24 from C_5 over F_2

$Code(G_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$\lvert Aut(G_i)\rvert$	$Type$
1	$(0,1,0,0,0,0,1,0)$	$(0,1,0,0,1)$	$(0,0,1,1,0)$	$2^{10}\cdot 3^3\cdot 5$	$[24,12,6]_I$
2	$(0,1,1,1,0,0,1,0)$	$(0,1,0,1,0)$	$(0,0,1,1,0)$	$2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23$	$[24,12,8]_{II}$

By lifting the code of Table 6.7 over the ring $F_2 + uF_2$, we obtain the well-known Extened Quadratic Residue Code.

Table 6.8: Extremal self-dual code of length 24 from C_2 over $F_2 + uF_2$, whose binary image is an extremal self-dual codes of length 48

$Code(L_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$Type$
1	G_2	$(0,1,u+1,1,0,u,u+1,u)$	$(0,1,u,1,0)$	$(0,u,1,1,u)$	$[48,24,12]_{II}$

6.3.5 Construction from cyclic group of order 7

Here, using the main construction and the cyclic group of order 7 over the binary field F_2, we obtain an extremal self-dual code with parameters $[32,16,8]$.

Table 6.9: Extremal self-dual code of length 32 from C_7 over F_2

$Code(H_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$\lvert Aut(H_i)\rvert$	$Type$
1	$(1,0,1,1,1,1,0,1)$	$(1,1,0,1,0,0,0)$	$(1,0,0,0,0,0,0)$	$2^{15}\cdot 3^2\cdot 5\cdot 7$	$[32,16,8]_{II}$

By lifting the code of Table 6.9 over the ring $F_2 + uF_2$, we obtain extremal self-dual codes of length 64.

Table 6.10: Extremal self-dual codes of length 32 from C_7 over $F_2 + uF_2$, whose binary images are extremal self-dual codes of length 64

$Code(M_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$Type$
1	H_1	$(1,0,1,1,1,1,u,1)$	$(1,1,0,1,0,0,0)$	$(1,0,0,u,u,0,0)$	$[64,32,12]_I$
2	H_1	$(1,0,1,1,1,1,0,1)$	$(1,1,0,1,0,0,0)$	$(1,0,0,u,u,0,0)$	$[64,32,12]_{II}$

6.3.6 Construction from cyclic group of order 9

Here, using the main construction and the cyclic group of order 9 over the binary field F_2, we obtain extremal self-dual codes with parameters $[40,20,8]$.

Table 6.11: Extremal self-dual codes of length 40 from C_9 over F_2

$Code(O_i)$	$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$\|Aut(O_i)\|$	$Type$
1	$(1,0,1,1,1,1,0,1)$	$(1,0,1,0,1,0,0,0,0)$	$(0,1,1,0,1,0,0,0,0)$	$2^2\cdot3^2$	$[40,20,8]_I$
2	$(1,0,0,0,1,1,0,1)$	$(1,0,1,0,1,0,0,0,0)$	$(0,1,1,0,1,0,0,0,0)$	$2^3\cdot3\cdot5\cdot19$	$[40,20,8]_{II}$

By lifting the code of Table 6.11 over the ring $F_2 + uF_2$, we obtain extremal self-dual codes of length 80.

Table 6.12: Extremal self-dual codes of length 40 from C_9 over $F_2 + uF_2$, whose binary images are extremal self-dual codes of length 80

$Code(N_i)$		$(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7,\beta_8)$	f_C	$f_{(\sigma(v_1))}$	$Type$
1	O_2	$(1,0,0,0,1,u+1,u,1)$	$(1,0,1,0,1,0,0,0,0)$	$(0,1,1,0,u+1,0,0,u,u)$	$[80,40,14]_I$
2	O_2	$(1,0,0,u,1,u+1,u,1)$	$(1,0,1,0,1,0,0,0,0)$	$(0,1,1,0,u+1,0,0,u,u)$	$[80,40,14]_{II}$

6.4 Conclusion

We have a new construction for the generation of extremal self-dual codes by using the concept of borders around a new, altered form of the four-circulant matrix. We show the importance of this new technique by generating extremal binary self-dual codes of numerous lengths: $12,16,20,32,40$. More significantly, we constructed the unique Extended Binary Golay Code search for which began in (2), (17), and (43), the unique Extended Quadratic Residue Code search for which is done in (17), (28), and (29), and the extremal self-dual codes of higher lengths, i.e., 64 and 80. With the self-dual codes, we develop a connection between unitary units/non-units and idempotents. One of the future scopes would be to apply this new construction to numerous other families of rings and groups.

Chapter 7

$*$-Semiclean rings and its application in construction of LCD and self-orthogonal abelian codes

In this chapter, we introduce a new class of ring, which is the $*$-version of the semiclean ring, i.e., the $*$-semiclean ring. A $*$-ring is $*$-semiclean if each element is the sum of a $*$-periodic element and a unit. In this chapter, many properties of $*$-semiclean rings are discussed. It is proved that if $p \in P(R)$ such that pRp and $(1-p)R(1-p)$ are $*$-semiclean rings, then R is also a $*$-semiclean ring. As a result, the matrix ring $M_n(R)$ over a $*$-semiclean ring is $*$-semiclean. A characterization that when the group rings RC_r and RG are $*$-semiclean is done, where R is a finite commutative local ring, C_r is a cyclic group of order r, and G is a locally finite abelian group. We have also found sufficient conditions when the group rings RC_3, RC_4, RQ_8, and RQ_{2n} are $*$-semiclean, where R is a commutative local ring. We have also demonstrated that the group ring $\mathbb{Z}_2D_6$ is a $*$-semiclean ring (which is not a $*$-clean ring). We have characterized the $*$-semicleanness of F_qG in terms of LCD and self-orthogonal abelian codes under the classic involution, where F_q is a finite field with q elements and G is a finite abelian group.

7.1 Introduction

A ring R is called clean if every element of R can be expressed as sum of an idempotent and a unit. In literature, a lot of work is done on this class of ring; see (46), (56), and (59) for more details on it. A ring R is called $*$-clean if every element of R can be expressed as the sum of a projection and a unit. See (7), (10), (21), (31), (39), (53), and (55) for more details on it. So far, much work has been done on the ∗-clean ring, but the ∗-semiclean ring has yet to be discovered. The motivation of the chapter is to find out about the ∗ concept in the semiclean ring.

A ∗-semiclean ring is the subclass of a semiclean ring and properly contains the class of a ∗-clean ring. A ring R is a ∗-ring (or ring with involution) if there is an operation $* : R \to R$ such that

$$(a+b)^* = a^* + b^*, \quad (ab)^* = b^* a^*, \quad (a^*)^* = a$$

for all $a, b \in R$. An element p of a ∗-ring R is known as a projection if $p^* = p = p^2$, i.e., p is a self-adjoint idempotent. An element a of a ∗-ring R is called ∗-periodic if there exists a positive integer $n > 1$ such that $a^n = p$, where p is a projection. A ∗-ring R is called ∗-semiclean if each element of R is sum of a ∗-periodic element and a unit. Both local and ∗-clean rings are clearly ∗-semiclean, and a ∗-semiclean ring is semiclean.

Section 7.2 looks at the various basic properties of ∗-periodic elements. In Section 7.3, we obtain multiple properties of ∗-semiclean rings. Moreover, examples of semiclean rings that are not ∗-semiclean and ∗-semiclean rings that are not ∗-clean are provided. In Section 7.4, the matrix extension of the ∗-semiclean rings is done. In Section 7.5, we investigate when a group ring RG is ∗-semiclean. We provide a characterization that when the group rings RC_r and RG are ∗-semiclean, where R is a finite commutative local ring, C_r is a cyclic group of order r, and G is a locally finite abelian group. We obtain several sufficient conditions for the group ring RG to be ∗-semiclean, where R is a commutative local ring and G is one of the groups C_i, $i = 3, 4$ (cyclic group of order 3 and 4), Q_8 (quaternion group of order 8), and Q_{2n} (generalized quaternion group). As a result, numerous examples of ∗-rings that are ∗-semiclean but not ∗-clean have been discovered. Also, we have shown that the group ring $\mathbb{Z}_2 D_6$ is ∗-semiclean but not ∗-clean. In Section 7.6, we have established a relationship between the ∗-semicleanness of the group ring $F_q G$ with the LCD and self-orthogonal codes. An LCD code (linear code with complementary dual) is a linear code $\mathfrak{C}$ satisfying the condition $\mathfrak{C} \cap \mathfrak{C}^\perp = \{0\}$, where

$$\mathfrak{C}^\perp = \{y \in F_q G | < z, y >= 0 \ \forall z \in \mathfrak{C}\}.$$

A self-orthogonal code is a linear code $\mathfrak{C}$ that satisfies the condition $\mathfrak{C} \subset \mathfrak{C}^\perp$. Data storage, telecommunication, consumer electronics, and cryptography all use LCD codes extensively. Self-orthogonal codes are extensively used in communication and information sharing. We cite, for example, (1), (5), and (40) for more data and information on LCD and self-orthogonal coding.

In the chapter, the ring R represents an associative ring with unity. The terms $J(R)$, $U(R)$, $I(R)$, $N(R)$, $Pri^*(R)$, and $P(R)$ represent the Jacobson radical, the group of all units, the set of all idempotents, the set of all nilpotents, the set of all $*$-periodic elements, and the set of projections of a ring R, respectively. For a group ring RG, the classical (or standard) involution $* : RG \to RG$ is given by $(\sum_{g\in G} \alpha_g g)^* = \sum_{g\in G} \alpha_g g^{-1}$; see (50, Proposition 3.2.11) for more details. Also, for a ring R, the ring homomorphism $\varepsilon : RG \to R$ defined by $\sum_{g\in G} \alpha_g g = \sum_{g\in G} \alpha_g$ is known as the augmentation mapping of RG. Moreover, the terms $\mathbb{Z}_p$, $\mathbb{Z}_{(p)}$, and $\mathbb{Z}$ represent the ring of integers modulo p, the localization of $\mathbb{Z}$ at the prime ideal generated by p, and the ring of integers, respectively.

7.2 $*$-Periodic elements

Some properties of $*$-periodic elements are given in this section.

Definition 7.2.1. *Let R be a $*$-ring. An element $x \in R$ is called $*$-periodic if $x^k = x^l$ (where, l and k are positive integers, $l \neq k$) such that $x^{l(k-l)} = p$, where $p \in P(R)$.*

Theorem 7.2.2. *Let R be a $*$-ring and $x \in R$. Then the following statements are equivalent:*

1. *There exists $n \in \mathbb{N}$ such that $x^n = p$, where $p \in P(R)$.*
2. *There exists an integer $n \geq 2$ such that $x = f + a$, where $f^n = f$ and $f^{n-1} = p$, with $p \in P(R)$, $a \in N(R)$, and $xf = fx$.*
3. *x is a $*$-periodic element.*

Proof. *1. $\Rightarrow$ 2. Since $x^n = p = p^2 = x^{2n}$, which implies $x^n = x^{2n}$ for some $n \in \mathbb{N}$. Rewrite an element x as $x = x^{n+1} + (x - x^{n+1})$ where $(x^{n+1})^{n+1} = x^{n+1}$ (since $(x^{n+1})^{n+1} = (x^n \cdot x)^{n+1} = (px)^{n+1} = px^{n+1} = px = x^n \cdot x = x^{n+1}$) and $(x^{n+1})^n = p$. Also, $(x - x^{n+1})^n = x^n(1 - x^n)^n = p(1 - p)^n = p(1 - p) = 0$, i.e., $x - x^{n+1} \in N(R)$.*
2. $\Rightarrow$ 3. It follows from (11, Lemma 4.3, Definition 4.4).
3. $\Rightarrow$ 1. By Definition 7.2.1, we can say there exist distinct positive integers l and k such that $x^{l(k-l)} = p$, where $p \in P(R)$. Since $l(k-l) \in \mathbb{N}$, therefore, there exists $n = l(k-l) \in \mathbb{N}$ such that $x^n = p$. □

Let R be a $*$-ring. According to (8, Proposition 2.1), (10, Theorem 3.2), and (10, Theorem 3.6), $x \in R$ is a strongly-π-$*$-regular element if and only if there exists an integer $n \geq 1$ such that $x^n = pu = up$, where $p \in P(R)$ and $u \in U(R)$.

Theorem 7.2.3. *Let R be a $*$-ring and $x \in R$. Then the following statements are equivalent:*

1. *x is $*$-periodic element.*

2. *x is strongly-π-$*$-regular element, with $u = 1 \in U(R)$.*

Proof. *1. $\Rightarrow$ 2. From Theorem 7.2.2, we get $x^n = p = p \cdot 1$, where $p \in P(R)$ and $1 \in U(R)$; therefore, x satisfies the condition of being strongly-π-$*$-regular with $u = 1 \in U(R)$.*
2. $\Rightarrow$ 1. As x is a strongly-π-$*$-regular element, there exists an integer $n \geq 1$ such that $x^n = pu$. Since $u = 1$, which implies $x^n = p$, then by Theorem 7.2.2, x is $*$-periodic element. □

The following concept is based on the above.

Definition 7.2.4. *Let R be a $*$-ring. An element $x \in R$ is called $*$-periodic if it satisfies the conditions given in Theorem 7.2.2 or Theorem 7.2.3.*

Let R be a $*$-ring. According to (55), an element $x \in R$ is called (strongly) $*$-clean if it can be expressed as $x = p + u$, where $p \in P(R)$ and $u \in U(R)$, with $(pu = up)$.

Lemma 7.2.5. *Every $*$-periodic element is strongly-$*$-clean.*

Proof. *Let x be a $*$-periodic element. By Theorem 7.2.2, an integer $n \geq 1$ exists, and $p \in P(R)$, such that $x^n = p$. Clearly, $1 - p = f$ is a projection. If we prove that $u = x - (1 - p)$ is a unit, then it will complete the proof. Define*

$$v = x^{n-1}p - (1 + x + \cdots + x^{n-1})(1 - p).$$

Rewrite the term u as $u = xp - (1 - x)(1 - p)$. Evaluate the term uv, we have

$$\begin{aligned} uv &= (xp - (1 - x)(1 - p))(x^{n-1}p - (1 + x + \cdots + x^{n-1})(1 - p)) \\ &= x^n p + (1 - x)(1 + x + \cdots + x^{n-1})(1 - p) \\ &= p + (1 - x^n)(1 - p) \\ &= 1. \end{aligned}$$

Clearly, $uv = vu$. Therefore, we get $uv = vu = 1$, which implies u is a unit with inverse v. Hence, $x = f + u$, where $f \in P(R)$ and $u \in U(R)$. Clearly, $fu = a + p - ap - 1 = uf$. Hence, element x is strongly $*$-clean. □

7.3 $*$-Semiclean rings

Let R be a $*$-ring. In 2003, Y. Ye introduced the class of semiclean rings (58). The notion of $*$-semiclean rings can be perceived as a $*$-versions of the semiclean ring. In this section, the definition and properties of $*$-semiclean rings are given.

Definition 7.3.1. *A $*$-ring R is $*$-semiclean if every element in it can be written as the sum of a $*$-periodic element and a unit.*

Proposition 7.3.2. *A $*$-ring R is $*$-semiclean if it is semiclean, and every idempotent is a projection.*

Corollary 7.3.3. *The group ring $\mathbb{Z}_{(p)}C_3$, where C_3 is a cyclic group of order 3, is $*$-semiclean for every prime p.*

Proof. *(58, Theorem 3.1) states that the group ring $\mathbb{Z}_{(p)}C_3$ is semiclean, and (58, proposition 3.1) tells us that the only idempotents of the group ring $\mathbb{Z}_{(p)}C_3$ are 0, 1, $\frac{1}{3}+\frac{1}{3}a+\frac{1}{3}a^2$ and $\frac{2}{3}-\frac{1}{3}a-\frac{1}{3}a^2$. Since 0^* is 0, 1^* is 1, $(\frac{1}{3}+\frac{1}{3}a+\frac{1}{3}a^2)^*$ is $\frac{1}{3}+\frac{1}{3}a+\frac{1}{3}a^2$, and $(\frac{2}{3}-\frac{1}{3}a-\frac{1}{3}a^2)^*$ is $\frac{2}{3}-\frac{1}{3}a-\frac{1}{3}a^2$, this implies that every idempotent is a projection. Hence, by Proposition 7.3.2, $\mathbb{Z}_{(p)}C_3$ is $*$-semiclean for every prime p.* □

We obtain the following relations between the classes of rings:

$$\begin{array}{ccccccc} *\text{-periodic} & \Rightarrow & \text{strongly-}\pi\text{-}*\text{-regular} & \Rightarrow & *\text{-clean} & \Rightarrow & *\text{-semiclean} \\ \Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\ \text{periodic} & \Rightarrow & \text{strongly-}\pi\text{-regular} & \Rightarrow & \text{clean} & \Rightarrow & \text{semiclean} \end{array}$$

The examples given below show that the above relations are irreversible.

Example 7.3.4. *1. Let $R = \left\{\begin{bmatrix}0&0\\0&0\end{bmatrix},\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&1\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&1\end{bmatrix}\right\}$ (where $0,1\in\mathbb{Z}_2$) be a commutative ring under the usual addition and multiplication. Clearly, the ring R is semiclean. Now, define a map $*: R\to R$ such that $\begin{bmatrix}x&y\\z&w\end{bmatrix}^* = \begin{bmatrix}x+y&y\\x+y+z+w&y+w\end{bmatrix}$. The only way of representing the element $\begin{bmatrix}1&1\\0&0\end{bmatrix}$ as sum of the periodic and the unit is $\begin{bmatrix}0&1\\0&1\end{bmatrix}+\begin{bmatrix}1&0\\0&1\end{bmatrix}$, but $\begin{bmatrix}0&1\\0&1\end{bmatrix}\notin Pri^*(R)$. Hence, it is not $*$-semiclean.*

2. *By Corollary 7.3.3, the group ring $\mathbb{Z}_{(7)}C_3$, where C_3 is a cyclic group of order 3, generated by a, is $*$-semiclean. However, the element $2+3a$ of $\mathbb{Z}_{(7)}C_3$ is not clean. Thus, the group ring $\mathbb{Z}_{(7)}C_3$ is not $*$-clean.*

3. *The ring F_3C_8 is finite; therefore, it is clean, but by (53, Example 3.12), it is not $*$-clean.*

4. *Let $R = \mathbb{Z}_5 \bigoplus \mathbb{Z}_5$ be a ring. Define an involution map $* : R \to R$ such that $(a,b)^* = (b,a)$. The ring R is strongly-π-regular, but it is not strongly-π-$*$-regular as idempotents do not coincide with projections.*

5. *The ring $R = F_{7^2}C_8$ is finite, so it is periodic, but by (53, Example 3.10), it is not $*$-clean, and thus according to Lemma 7.2.5, it is not $*$-periodic.*

Theorem 7.3.5. *Let R be a $*$-ring, with $2 \in U(R)$. Then R is semiclean, and every unit is self-adjoint, i.e., $v^* = v$ for all $v \in U(R)$ if and only if R is $*$-semiclean and $* = 1_R$.*

Proof. $\Rightarrow$ *Let $a \in R$. Then, by Definition 7.3.1, we have $a = f + v$, where $f^{2n} = f^n$ and $v \in U(R)$. Observe that $(1-2f^n)^2 = 1$. Because every unit of R is self-adjoint, $2f^{n*} = 2f^n$. As a result, $2(f^{n*} - f^n) = 0$. Because $2 \in U(R)$, $f^{n*} = f^n$, implying that an element $a \in R$ is $*$-semiclean. Because $f \in R$ is periodic, and every periodic is clean, so $f = f' + v'$, where $f' \in I(R)$ and $v' \in U(R)$. Observe that $(1-2f')^2 = 1$. Because every unit of R is self-adjoint, $2f'^* = 2f'$. As a result, $2(f'^* - f') = 0$. Because $2 \in U(R)$, $f'^* = f'$, implying that $f^* = f$. Hence, $a^* = a$, so $* = 1_R$.*
$\Leftarrow$ *Obvious.* □

If an element x is self-adjoint square root of 1, it fulfills the conditions $x^2 = 1$ and $x^* = x$.
Every element of a $*$-clean ring in which 2 is invertible is shown to have sum of no more than 2 units by Jian Cui and Zhou Wang (10). We extended this finding to $*$-semiclean rings using Theorem 7.3.6 and demonstrated that each element of a $*$-semiclean ring can be expressed as sum of three units.

Theorem 7.3.6. *Let R be a $*$-semiclean ring with $2 \in U(R)$. Then every element of R is sum of a self-adjoint square root of 1 and two units.*

Proof. *Let $a \in R$. Then $\frac{a+1}{2} = f + v$, where $f \in Pri^*(R)$ and $v \in U(R)$. Because $f \in Pri^*(R)$, $f^n = f^{2n}$, and $f^n = p = p^*$. According to Lemma 7.2.5, $f = f' + v'$, where $f' = (1-p) \in P(R)$ and $v' \in U(R)$. Thus, $a = (2-2p) - 1 + 2v' + 2v = (1-2p) + 2v' + 2v$, where $(1-2p)^* = 1-2p$ and $(1-2p)^2 = 1$, with $2v', 2v \in U(R)$.* □

An ideal I of a $*$-ring R is called $*$-invariant if $I^* \subseteq I$. Lemma 7.3.7 extends an involution $*$ of R to the factor ring R/I, which is still denoted by $*$.

Lemma 7.3.7. *Let R be $*$-semiclean and I be $*$-invariant ideal. Then the ring R/I is $*$-semiclean. In particular, the ring $R/J(R)$ is $*$-semiclean.*

Proof. *By (58, Proposition 2.1), the homomorphic image of semiclean is semiclean. Also, the homomorphic image of projection is projection. Thus, the result holds. Since an ideal $J(R)$ is $*$-invariant, therefore, $R/J(R)$ is $*$-semiclean.* □

Every polynomial ring over a commutative ring is not $*$-semiclean, as shown in Example 7.3.8.

Example 7.3.8. *Let R be a commutative ring. Then the polynomial ring $R[x]$ is not $*$-semiclean.*

Proof. *By (58, Example 3.2), the polynomial ring $R[x]$ is never semiclean. Hence, for any involution $*$, the ring $R[x]$ is not $*$-semiclean.* □

Let R be a $*$-ring and $R[[x]]$ be a power series ring. Then on $R[[x]]$, an induced involution $*$ is defined as $(\sum_{i=0}^{\infty} \alpha_i x^i)^* = \sum_{i=0}^{\infty} \alpha_i^* x^i$. In 2003, Yuanqing Ye (58) proved that the ring $R[[x]]$ is semiclean if and only if R is semiclean. This result has been extended to $*$-semiclean by Proposition 7.3.9.

Proposition 7.3.9. *The ring $R[[x]]$ is $*$-semiclean if and only if R is $*$-semiclean.*

Proof. $\Rightarrow$ *Let $R[[x]]$ be $*$-semiclean. Because $R \cong R[[x]]/(x)$ and (x) is a $*$- invariant ideal of $R[[x]]$, R is $*$-semiclean according to Lemma 7.3.7.*
$\Leftarrow$ *Let R be $*$-semiclean and $g(x) = \sum_{i=0}^{\infty} \alpha_i x^i \in R[[x]]$. If $\alpha_0 = f + v$, where $f \in Pri^*(R)$ and $v \in U(R)$, then $g(x) = f + (v + \sum_{i=1}^{\infty} \alpha_i x^i)$, where $f \in Pri^*(R) \subseteq Pri^*(R[[x]])$ and $v + \sum_{i=1}^{\infty} \alpha_i x^i \in U(R[[x]])$. As a result, $g(x) \in R[[x]]$ is $*$-semiclean.* □

Every $*$-clean ring is a $*$-semiclean ring, but the converse is not true. By Theorem 7.3.10, we demonstrate that, under certain conditions, the converse will also hold.

Theorem 7.3.10. *Let R be a torsion free ring, and $z \in R$ such that $z = b + v$, where $b \in Pri^*(R)$ and $v \in U(R)$. If $v = \pm 1$, then z is $*$-clean.*

Proof. *Case I: Let $v = 1$*
Rewrite an element $z \in R$ as $z = b + 1$, $b^k = b^l$ (where, l and k are positive integers such that $l > k$), and $b^{k(l-k)} = p = p^* \in P(R)$.
We have $(z-1)^k = (z-1)^l$ because $b^k = b^l$, which implies that $(1-z)^{2k} = (1-z)^{2l}$ and

$(1-z)^{2k(2l-2k)} = p$. *As a result,* $1-z$ *is* $*$*-periodic, and thus, according to Lemma 7.2.5, an element* $1-z$ *is* $*$*-clean, i.e.,* $1-z = f+u$, *where* $f = (1-p) \in P(R)$, *and* $u \in U(R)$. *To put it simply,* $z = p + u'$, *where* $p \in P(R)$ *and* $u' = -u \in U(R)$.

Case II: Let $v = -1$
Then an element $z \in R$ *is rewritten as* $z = b - 1$.

1. *Let* $b = b^n$ *(where, n is a positive integer such that* $n > 1$*).*
   Then $z = b^{n-1} + (-1 + b - b^{n-1})$. *Because* $b \in Pri^*(R)$ *and* $b = b^n$, *an element* $b^{n-1} \in P(R)$. *An element* $-1 + b - b^{n-1}$ *is a unit in R, with the inverse* $(2^{n-1} - 1 + 2^{n-3}b + 2^{n-4}b^2 + \cdots + b^{n-2} + (1-2^{n-2})b^{n-1})(1-2^{n-1})^{-1} \in R$. *Hence,* $z = b - 1$ *is* $*$*-clean.*

2. *Let* $b^k = b^l$ *(where, l and k are positive integers such that* $l > k$*).*
   Then $z = b^{k(l-k)} + (-1 + b - b^{k(l-k)})$. *Because* $b \in Pri^*(R)$ *and* $b^k = b^l$, *an element* $b^{k(l-k)} \in P(R)$. *An element* $-1 + b - b^{k(l-k)}$ *is a unit in R. Hence,* $z = b - 1$ *is* $*$*-clean.*

□

7.4 Matrix extension of ∗-semiclean rings

If R is a $*$-ring, then $M_n(R)$ the ring of $n \times n$ matrices over R inherit the natural involution from R: if $A = (a_{ij})$, then A^* is the transpose of (a^*_{ij}). In 2010, Lia Vaš (55) proved that if both pRp and $(1-p)R(1-p)$ are $*$-clean rings (here p is a projection), then R is $*$-clean. As a result, the $M_n(R)$ (ring of $n \times n$ matrices over R) is $*$-clean. This result has been extended to $*$-semiclean rings in this section.

Lemma 7.4.1. *If* pRp *and* $(1-p)R(1-p)$ *are both* $*$*-semiclean, where* $p \in P(R)$, *then R is also* $*$*-semiclean.*

Proof. *For each* $p \in R$, *write* $1 - p = \overline{p}$. *Apply the Pierce decomposition of the ring R:*

$$R = \begin{bmatrix} pRp & pR\overline{p} \\ \overline{p}Rp & \overline{p}R\overline{p} \end{bmatrix}.$$

Let $M = \begin{bmatrix} m & n \\ o & q \end{bmatrix} \in R$. *Thus,* $m = a + u$, *where* $a \in Pri^*(pRp)$ *such that* $a^{k_1} = a^{l_1}$ *(where,* l_1 *and* k_1 *are possitive integers such that* $l_1 > k_1$*) and u is a unit in pRp with inverse* u_1. *Then,* $q - nu_1o \in \overline{p}R\overline{p}$. *So* $q - ou_1n = b + v$, *where* $b \in Pri^*(\overline{p}R\overline{p})$ *such that* $b^{k_2} = b^{l_2}$ *(where,*

l_2 and k_2 are possitive integers such that $l_2 > k_2$) and v is a unit in $\overline{p}R\overline{p}$ with inverse v_1. Thus,

$$M = \begin{bmatrix} a+u & n \\ o & b+v+nu_1o \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} u & n \\ o & v+ou_1n \end{bmatrix}.$$

To show: $\begin{bmatrix} u & n \\ o & v+ou_1n \end{bmatrix}$ *is unit in R.*

Compute, $\begin{bmatrix} p & 0 \\ -ou_1 & \overline{p} \end{bmatrix}\begin{bmatrix} u & n \\ o & v+ou_1n \end{bmatrix}\begin{bmatrix} p & -u_1n \\ 0 & \overline{p} \end{bmatrix} = \begin{bmatrix} u & n \\ 0 & v \end{bmatrix}\begin{bmatrix} p & -u_1n \\ 0 & \overline{p} \end{bmatrix} = \begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}$. *Since the matrices* $\begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}$, $\begin{bmatrix} p & 0 \\ -ou_1 & \overline{p} \end{bmatrix}$, *and* $\begin{bmatrix} p & -u_1n \\ 0 & \overline{p} \end{bmatrix}$ *are units in* $\begin{bmatrix} pRp & pR\overline{p} \\ \overline{p}Rp & \overline{p}R\overline{p} \end{bmatrix}$, *therefore,* $\begin{bmatrix} u & n \\ o & v+ou_1n \end{bmatrix}$ *is unit in R.*

To show: $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ *is ∗-periodic, i.e.,* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^k = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^l$ *and* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^{k(l-k)} \in P(R)$ *(where, l and k are the possitive integer such that $l > k$).*

Without loss of generality, let $k_2 \geqslant k_1$.

$a^{k_1} = a^{l_1} = a^{(l_1-k_1)+k_1} = a^{s(l_1-k_1)+k_1}$,

$b^{k_2} = b^{l_2} = b^{(l_2-k_2)+k_2} = b^{s(l_2-k_2)+k_2}$, *and*

$a^{k_2} = a^{k_1+(k_2-k_1)} = a^{s(l_1-k_1)+k_2}$.

Let $k = k_2$ and $l = (l_1-k_1)(l_2-k_2)+k_2$. Then $a^k = a^l$ and $b^k = b^l$.

Thus, $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^k = \begin{bmatrix} a^k & 0 \\ 0 & b^k \end{bmatrix} = \begin{bmatrix} a^l & 0 \\ 0 & b^l \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^l$. *Hence,* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ *is periodic.*

As $a \in Pri^*(pRp)$ and $a^k = a^l$. Thus, $a^{k(l-k)} = p_1$, where $p_1 \in P(pRp)$.

Similarly, $b \in Pri^*(\overline{p}R\overline{p})$ and $b^k = b^l$. Thus, $b^{k(l-k)} = 1 - p_2$, where $p_2 \in P(\overline{p}R\overline{p})$.

Compute, $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^{k(l-k)} = \begin{bmatrix} a^{k(l-k)} & 0 \\ 0 & b^{k(l-k)} \end{bmatrix} = \begin{bmatrix} p_1 & 0 \\ 0 & 1-p_2 \end{bmatrix} \in P(R)$.

This proves that matrix M is ∗-semiclean. Therefore, R is ∗-semiclean. □

By Lemma 7.4.1, and an inductive argument, the next result holds.

Theorem 7.4.2. *If $p_1, p_2, \cdots, p_n$ are orthogonal projections with $1 = p_1 + p_2 + \cdots + p_n$, and p_iRp_i is ∗-semiclean for each i, then R is ∗-semiclean.*

The following two conclusions follow directly from Theorem 7.4.2.

Corollary 7.4.3. *If R is ∗-semiclean, then so is $M_n(R)$.*

Corollary 7.4.4. *If* $N = N_1 \bigoplus N_2 \bigoplus \cdots \bigoplus N_n$ *are modules and* $End(N_i)$ *is* $*$*-semiclean for each i, then* $End(N)$ *is* $*$*-semiclean.*

7.5 $*$-Semiclean group rings

In this section, we obtain several results pertaining to commutative and non-commutative $*$-semiclean group rings. Throughout this section, we are considering standard involution on the group ring RG.

Theorem 7.5.1. *If* RG *is a* $*$*-semiclean ring, then so is* $((R/J(R))G$.

Proof. *Define a map* $\Psi : RG \to (R/J(R))G$ *as* $\Psi(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \Psi(\alpha_g)g$, $\Psi(\alpha_g) = \alpha_g + J(R)$. *Note that* Ψ *is an onto map. The map* Ψ *preserves an involution* $*$ *as* $\Psi(\sum_{g\in G} \alpha_g g)^* = (\Psi(\sum_{g\in G} \alpha_g g))^*$. *Let* $\overline{x} \in (R/J(R))G$. *Since* Ψ *is an onto map, there exists an element* $x \in RG$, *which is defined as* $x = f + u$, *where* $f \in Pri^*(RG)$ *and* $u \in U(RG)$. *So,* $\overline{x} = \Psi(f) + \Psi(u)$, *where* $\Psi(f) \in Pri^*((R/J(R))G)$ *and* $\Psi(u) \in U((R/J(R))G)$. *Hence,* $((R/J(R))G$ *is a* $*$*-semiclean ring.* □

7.5.1 Abelian group rings

In 2015 (21), Gao, Chen, and Li found out that when the group rings RC_3, RC_4, RS_3 and RQ_8 are $*$-clean, where R is a commutative local ring. In this section, we have extended this result to $*$-semiclean rings. As a consequence, many examples of group rings that are $*$-semiclean but not $*$-clean have been obtained. In Theorem 7.5.7 and 7.5.8, a characterization that when the group rings RC_r and RG are $*$-semiclean is obtained (respectively). Here, R is a finite commutative local ring, C_r is a cyclic group of order r, and G is a locally finite abelian group.

Proposition 7.5.2. *(45) If* R *is local,* G *is a locally finite p-group, and* $p \in J(R)$*, then the group ring* RG *is local.*

We now investigate when RC_3 is $*$-semiclean.

In 2015 (21), Gao, Chen, and Li investigated the group rings RC_3 and $\mathbb{Z}_pC_3$ and proved that if $(-3)^{\frac{p-1}{2}} \equiv 1(mod\ p)$, then the group ring $\mathbb{Z}_pC_3$ is not $*$-clean; however, Theorem 7.5.3(3) demonstrates that it is $*$-semiclean. Furthermore, in Theorem 7.5.3(2), we relaxed the requirement that RC_3 be clean, allowing us to broaden the class of rings (rings that are $*$-semiclean but not $*$-clean are obtained). One such example is $\mathbb{Z}_{(7)}C_3$, which is explained below.

Theorem 7.5.3. *Let R be a commutative local ring and $G = C_3 = \langle x \rangle$ be a cyclic group of order 3.*

1. *If $3 \notin U(R)$, then RC_3 is $*$-semiclean.*
2. *If $3 \in U(R)$ and the equation $z^2 + z + 1 = 0$ has no solutions in R, then the ring RC_3 is $*$-semiclean.*
3. *If $2 \in U(R)$, then RC_3 is $*$-semiclean if RC_3 is clean and $U(RC_3)$ is a torsion group.*

Proof. 1. *Since $3 \in J(R)$, by Proposition 7.5.2, RC_3 is local. Hence, RC_3 is a $*$-semiclean.*

2. *According to (37, Theorem 2.7), the ring RC_3 is a semiclean ring. By (21, Theorem 2.4), if the equation $z^2 + z + 1 = 0$ has no solution in R, then every idempotent of the ring RC_3 is a projection. Hence, by Proposition 7.3.2, the ring RC_3 is a $*$-semiclean ring.*

3. *If RC_3 is clean and $2 \in U(RC_3)$, then by (57, Proposition 2.5), RC_3 is a 2-good ring. If an element $a \in RC_3$, then there exist $u_1, u_2 \in U(RC_3)$ such that $a = u_1 + u_2$, according to the definition of a 2-good ring. Because $U(RC_3)$ is a torsion group, there exists $m \in \mathbb{N}$ such that $u_1^m = 1 = 1^*$, implying that $u_1 \in Pri^*(RC_3)$ and $u_2 \in U(RC_3)$. Thus, element a is $*$-semiclean. Since a is an arbitary element of RC_3, therefore, every element of RC_3 is $*$-semiclean. Hence, RC_3 is a $*$-semiclean ring.*

□

The examples given below are the direct consequences of Theorem 7.5.3.

Example 7.5.4. 1. *By Theorem 7.5.3(1), the ring $\mathbb{Z}_3C_3$ is $*$-semiclean.*

2. *The ring $\mathbb{Z}_{(7)}C_3$ is $*$-semiclean because the equation $z^2 + z + 1 = 0$ has no solution in $\mathbb{Z}_{(7)}$, but it is not $*$-clean because, according to (46), $\mathbb{Z}_{(p)}C_3$ is clean if and only if $p \not\equiv 1(mod 3)$.*

3. *By (59, Corollary 19), we can say that $\mathbb{Z}_pC_3$, where $p > 2$ is prime, is clean. Also, as $2 \in U(\mathbb{Z}_pC_3)$, by Theorem 7.5.3(3), we conclude $\mathbb{Z}_pC_3$ is $*$-semiclean, but by (21, Example 2.7), for $p > 3$, if $(-3)^{\frac{p-1}{2}} \equiv 1(mod\ p)$, it is not $*$-clean.*

We now investigate when RC_4 is $*$-semiclean.

In 2015 (21), Gao, Chen, and Li investigated the group rings RC_4 and $\mathbb{Z}_pC_4$, and proved that if $p \equiv 1(mod\ 4)$, then the group ring $\mathbb{Z}_pC_4$ is not ∗-clean; however, Theorem 7.5.5(2b) demonstrates that it is ∗-semiclean. Furthermore, in Theorem 7.5.5(2a), we relaxed the requirement that RC_4 be clean, allowing us to broaden the class of rings (rings that are ∗-semiclean but not ∗-clean are obtained). One such example is $\mathbb{Z}_{(5)}C_4$, which is explained below.

Theorem 7.5.5. *Let R be a commutative local ring and $G = C_4 = \langle x \rangle$ be a cyclic group of order 4.*

1. *If $2 \notin U(R)$, then RC_4 is ∗-semiclean.*
2. *If $2 \in U(R)$, then RC_4 is ∗-semiclean if any of the condition given below is satisfied.*
   (a) *The equation $z^2 + 1 = 0$ has no solutions in R.*
   (b) *RC_4 is clean and $U(RC_4)$ is torsion group.*

Proof. 1. *Since $2 \in J(R)$, by Proposition 7.5.2, RC_4 is local. Hence, RC_4 is a ∗-semiclean.*

2. (a) *According to (37, Theorem 2.7), the ring RC_4 is a semiclean ring. By (21, Theorem 2.10), if the equation $z^2 + 1 = 0$ has no solution in R, then every idempotent of the ring RC_4 is a projection. Hence, by Proposition 7.3.2, the ring RC_4 is a ∗-semiclean ring.*
   (b) *The proof is similar to the proof of Theorem 7.5.3(3).*

□

The examples given below are the direct consequences of Theorem 7.5.5.

Example 7.5.6. 1. *The ring $\mathbb{Z}_{(5)}C_4$ is ∗-semiclean because the equation $z^2+1 = 0$ has no solution in $\mathbb{Z}_{(5)}$, but it is not ∗-clean because, according to (46), $\mathbb{Z}_{(5)}C_4$ is not clean.*

2. *By (59, Corollary 19), we can say that $\mathbb{Z}_pC_4$, where $p > 2$ is prime, is clean. Also, as $2 \in U(\mathbb{Z}_pC_4)$, by Theorem 7.5.5(2b), we conclude $\mathbb{Z}_pC_4$ is ∗-semiclean, but by (21, Corollary 2.11), for $p \equiv 1 \pmod 4$, $\mathbb{Z}_pC_4$ is not ∗-clean.*

By using Theorem 7.5.7 and Theorem 7.5.8, we can find various other examples of ∗-semiclean rings that are not ∗-clean. Some of them are listed in Example 7.5.9.

Theorem 7.5.7. *Let R be a finite commutative local ring.*

1. *If $2 \in U(R)$ and $C_r = \langle x \rangle$ is a cyclic group of order r, then RC_r is ∗-semiclean.*

2. *If $2 \in J(R)$, $C_r = \langle x \rangle$ is a cyclic group of order $r = 2^s t$ $(s \geq 0)$, where $2 \nmid t$, and γ is the cyclic permutation on the set $J = \{1, 2, \cdots, t-1\}$ defined as $\gamma : J \to J$ by $j \to 2j(\text{mod } t)$, then RC_r is $*$-semiclean.*

Proof. 1. *Let $x \in RC_r$. The group ring RC_r is periodic because it is finite. Thus, according to (58, Lemma 5.1), RC_r is clean. Furthermore, $2 \in U(R)$. Thus, by (57, Proposition 2.5), RC_r is a 2-good ring, i.e., $x = u_1 + u_2$, where $u_1, u_2 \in U(RC_r)$. As RC_r is periodic, according to (8, Proposition 2.3), $U(RC_r)$ is a torsion group. Because $u_1 \in U(RC_r)$, there exists $n \in \mathbb{N}$ such that $u_1^n = 1 = 1^*$. Thus, $u_1 \in Pri^*(RC_r)$ and $u_2 \in U(RC_r)$. As a result, an element x meets the condition of being $*$-semiclean. Hence, RC_r is $*$-semiclean.*

2. *Let $s \geq 1$. Then $C_r \cong C_{2^s} \times C_t$. Thus, $RC_r \cong (RC_{2^s})C_t$, where $C_t = \langle x \rangle$ is a cyclic group of order t. By (45, Theorem), $R' = RC_{2^s}$ is the local ring. Since $(R/J(R))$ is a field of char $= 2$ and $(R/J(R))C_{2^s} \to (R'/J(R'))$ is ring epimorphism, therefore, $(R'/J(R'))$ is also a field of char $= 2$. Let $a = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1}x^{t-1}$ be an idempotent element of $(R'/J(R'))C_t$. Because $2 = 0$ and $x^t = 1$, it follows that $a^2 = a_0^2 + a_{\gamma(1)}x^{\gamma(1)} + \cdots a_{\gamma(t-1)}x^{\gamma(t-1)}$. Because γ is the cyclic permutation on the set $J = \{1, 2, \cdots, t-1\}$, therefore, $a_0^2 = a_0$ and $a_1^2 = a_1 = a_2 = \cdots = a_{t-1}$. So the idempotents of $(R'/J(R'))C_t$ are $0,\ 1,\ 1 + x + \cdots + x^{t-1}$, and $x + x^2 + \cdots + x^{t-1}$. Because $0^* = 0$, $1^* = 1$, $(1 + x + \cdots + x^{t-1})^* = 1 + x + \cdots + x^{t-1}$ and $(x + x^2 + \cdots + x^{t-1})^* = x + x^2 + \cdots + x^{t-1}$, implying that $(R'/J(R'))C_t$ has four idempotents, all of which are projections. Now, because C_t is a locally finite group, $J(R')C_t \subseteq J(R'C_t)$. As the $(char(R'/J(R')), t) = 1$, therefore, $(R'/J(R'))C_t$ is semisimple, implying that $R'J(C_t) = J(R'C_t)$. Therefore, we get $(R'/J(R'))C_t \cong R'C_t/J(R')C_t = R'C_t/J(R'C_t)$. Thus, the factor ring $R'C_t/J(R'C_t) = \overline{R'C_t}$ will also have only four idempotents : $\overline{0},\ \overline{1},\ \overline{1} + \overline{x} + \cdots + \overline{x}^{t-1}$, and $\overline{x} + \overline{x}^2 + \cdots + \overline{x}^{t-1}$, all of which are projections. Since the order of the ring $\overline{R'C_t}$ is finite, $\overline{R'C_t}$ is clean. Thus, $\overline{R'C_t}$ is $*$-clean, i.e., for each $\overline{a} \in \overline{R'C_t}$, there exists $\overline{p} \in P(\overline{R'C_t})$ and $\overline{u} \in U(\overline{R'C_t})$, such that $\overline{a} = \overline{p} + \overline{u}$. Moreover, in $R'C_t$ the elements $m_1 = 0$, $m_2 = 1$, $m_3 = t^{-1}(1 + x + \cdots + x^{t-1})$, and $m_4 = t^{-1}((t-1) - x - x^2 - \cdots - x^{t-1})$ are projections such that $\overline{m_1} = \overline{0}$, $\overline{m_2} = \overline{1}$, $\overline{m_3} = \overline{1} + \overline{x} + \cdots + \overline{x}^{t-1}$, and $\overline{m_4} = \overline{x} + \overline{x^2} + \cdots + \overline{x}^{t-1}$. Which implies there exists a $n_1 = p \in P(R'C_t)$ such that $\overline{n_1} = \overline{p}$ for $\overline{p} \in P(\overline{R'C_t})$. There is also $n_2 = u \in U(R'C_t)$ such that $\overline{n_2} = \overline{u}$ for $\overline{u} \in U(\overline{R'C_t})$. Thus, there exists an element $n_3 = p + u \in R'C_t$ such that $\overline{n_3} = \overline{p} + \overline{u}$ for $\overline{p} + \overline{u} \in \overline{R'C_t}$. Then $\overline{n_3} = \overline{a}$, i.e., $a - n_3 \in J(R'C_t)$. Since R' is finite, R' is an artinian ring, which implies $J(R')$ is nilpotent. Thus, $J(R')C_t$ is nil-ideal. By (38, Corollary 4.3), $J(R')C_t$ is nilpotent. Since $J(R'C_t) = J(R')C_t$, the ideal $J(R'C_t)$ is*

also nilpotent. Since $a - n_3 \in J(R^{'}C_t)$, therefore, $a - n_3 = a - (p + u) = k$ for some $k \in J(R^{'}C_t)$. Simplifying it, we get $a = p + u + k$, where $p \in P(R^{'}C_t)$, $u \in U(R^{'}C_t)$, and $k \in J(R^{'}C_t)$. Thus, $a = p + v$, where $p \in P(R^{'}C_t)$ and $v = (u + k) \in U(R^{'}C_t)$. As a result, an element a meets the condition of being $*$-clean. Hence, $RC_r = R^{'}C_t$ is $*$-clean. Thus, RC_r is $*$-semiclean.

□

Theorem 7.5.8. *Let R be a finite commutative local ring and G be a locally finite abelian group.*

1. *If $2 \in U(R)$, then RG is $*$-semiclean.*
2. *If $2 \in J(R)$ and G is a locally finite 2-group, then RG is $*$-semiclean.*
3. *If $2 \in J(R)$ with $R/J(R) \cong \mathbb{F}_2$ and exponent of G is r, where r is an odd positive integer, and a $q \in \mathbb{N}$ exists such that $2^q \equiv -1(mod\ r)$, then RG is $*$-semiclean.*

Proof. 1. *Let $x \in RG$. Since G is a locally finite abelian group, there exists a finite subgroup H such that $x \in RH$. The rest of the proof is similar to that of Theorem 7.5.7(1).*

2. *Since $2 \in J(R)$, by Proposition 7.5.2, RG is local. Hence, RG is $*$-semiclean.*

3. *We will first show that the group ring $\overline{RG^{'}}$ is $*$-clean for any arbitary finite abelian group, say $G^{'}$ (with odd exponent say r) such that $2^q \equiv -1(mod\ r)$ for some $q \in \mathbb{N}$. Let $a = x_1 + x_2 + \cdots + x_t$ be the idempotent element of $(R/J(R))G^{'}$, where $x_i \in G^{'}$ for $i = 1$ to t. Then $(x_1 + x_2 + \cdots + x_t)^2 = x_1^2 + x_2^2 + \cdots + x_t^2 = x_1 + x_2 + \cdots + x_t$. Thus, $\{x_1, x_2, \cdots, x_t\} = \{x_1^2, x_2^2, \cdots, x_t^2\}$. Furthermore, if $x \in \{x_1, x_2, \cdots, x_t\}$, then $x^{2^k} \in \{x_1, x_2, \cdots, x_t\}$ for some $k \in \mathbb{N}$. Thus, an element x can be rewritten as $x = (x_{k_1} + x_{k_1}^2 + \cdots + x_{k_1}^{2^{m_1}}) + \cdots + (x_{k_j} + x_{k_j}^2 + \cdots + x_{k_j}^{2^{m_j}})$. Here the elements x_{k_i} are distinct and m_i's are the smallest positive integers such that $x_{k_i}^{2^{m_i+1}} = x_{k_i}$. Evaluating x^*, we have $x^* = (x_{k_1}^{-1} + x_{k_1}^{-2} + \cdots + x_{k_1}^{-2^{m_1}}) + \cdots + (x_{k_j}^{-1} + x_{k_j}^{-2} + \cdots + x_{k_j}^{-2^{m_j}})$. Since, for some $q \in \mathbb{N}$, we have $2^q \equiv -1(mod\ p)$, thus, clearly $a^* = a$, i.e., every idempotent of $(R/J(R))G^{'}$ is a projection. Now, as the order of $(R/J(R))G^{'}$ is finite, it is a clean ring. As a result, the ring $(R/J(R))G^{'}$ is $*$-clean. Now, as G is a locally finite group, therefore, $J(R)G^{'} \subseteq J(RG^{'})$. Since order of every element of $G^{'}$ is invertible in $(R/J(R))$, therefore, $(R/J(R))G^{'}$ is semisimple. Thus, $J(R)G^{'} = J(RG^{'})$. Therefore, we get $(R/J(R))G^{'} \cong RG^{'}/J(RG^{'})$. Thus, every idempotent of $RG^{'}/J(RG^{'})$ is a projection. Being the ring $RG^{'}/J(RG^{'}) = \overline{RG^{'}}$ of finite order, it is a clean ring. Thus, it is a $*$-clean ring.*

Let $z \in RG$. Since G is a locally finite abelian group, there exists a finite abelian subgroup H such that $z \in RH$. For $l_1 = z \in RH$, there exists a $\overline{z} \in \overline{RH}$ such that $\overline{l_1} = \overline{z}$. Because $\overline{z} \in \overline{RH}$, and because, as explained above, the group ring $\overline{RH}$ is a $*$-clean, there exists $\overline{p} \in P(\overline{RH})$ and $\overline{u} \in U(\overline{RH})$, such that $\overline{z} = \overline{p} + \overline{u}$. Because $J(RH)$ is the $*$-invariant nil ideal of a $*$-ring RH, there exists a $n_1 = p \in P(RH)$ such that $\overline{n_1} = \overline{p}$ for $\overline{p} \in P(\overline{RH})$. There is also $n_2 = u \in U(RH)$ such that $\overline{n_2} = \overline{u}$ for $\overline{u} \in U(\overline{RH})$. Thus, there exists an element $n_3 = p + u \in RH$ such that $\overline{n_3} = \overline{p} + \overline{u}$ for $\overline{p} + \overline{u} \in \overline{RH}$. Thus, $\overline{n_3} = \overline{z}$, i.e., $z - n_3 \in J(RH)$. Also, the ideal $J(RH)$ is nilpotent. Since $z - n_3 \in J(RH)$, $z - n_3 = z - (p + u) = k$ for some $k \in J(RH)$. Simplifying it, we get $z = p + u + k$, where $p \in P(RH)$, $u \in U(RH)$, and $k \in J(RH)$. Thus, $z = p + v$, where $p \in P(RH)$, and $v = (u + k) \in U(RH)$. As a result, element z meets the condition of being $*$-clean. Hence, RH is $*$-clean. Thus, RH is $*$-semiclean, which implies RG is $*$-semiclean.

□

The examples given below are the direct consequences of Theorem 7.5.7 and Theorem 7.5.8. These are $*$-semiclean but not $*$-clean group rings.

Example 7.5.9. *1. The ring F_3C_8 is $*$-semiclean, but by (53, Example 3.12), it is not $*$-clean.*

2. The ring $F_7(C_4 \times C_8)$ is $*$-semiclean, but by (53, Example 3.10(1)), it is not $*$-clean.

3. The ring F_3C_{35} is $*$-semiclean, but by (31, Example 3.3), it is not $*$-clean.

7.5.2 Non-abelian group rings

In this section, we investigate when a non-abelian group ring RG is $*$-semi-clean, where R is a commutative local ring and G is Q_8, Q_{2n}, D_{2n}, and D_6.

Quaternion group Q_8

The group ring $\mathbb{Z}_pQ_8$ was studied by Gao in (21), and it was shown that it is not $*$-clean; however, by Theorem 7.5.10, we obtain that it is $*$-semiclean.

Theorem 7.5.10. *Let R be a commutative local ring and $G = Q_8 = \langle x, y | x^4 = 1, x^2 = y^2, yx = x^{-1}y \rangle$ be a quaternion group of order 8.*

1. If $2 \notin U(R)$, then RQ_8 is $*$-semiclean.

2. If $2 \in U(R)$, RQ_8 is clean and $U(RQ_8)$ is a torsion group, then RQ_8 is $*$-semiclean.

Proof. *1. As R is local, Q_8 is a finite 2-group, and $2 \in J(R)$, therefore, by Proposition 7.5.2, RQ_8 is local. Thus, RQ_8 is a $*$-semiclean ring.*

2. The proof is similar to the proof of Theorem 7.5.3(3).

□

The example given below is the direct consequence of Theorem 7.5.10.

Example 7.5.11. *The ring $\mathbb{Z}_p Q_8$ (where $p > 2$ is prime) is clean. Furthermore, because $2 \in U(\mathbb{Z}_p Q_8)$, we can conclude from Theorem 7.5.10(2) that $\mathbb{Z}_p Q_8$ is $*$-semi-clean. However, according to (21, Example 3.9), $\mathbb{Z}_p Q_8$ is not $*$-clean.*

Generalized quaternion group Q_{2n} and Dihedral group D_{2n}

The group ring $F_q Q_{2n}$ was studied by Hongdi Huang in (30) and it was shown that if $4|n$ and $gcd(q, 2n) = 1$, then it is not $*$-clean; however, by Theorem 7.5.12, we obtain that it is $*$-semiclean.

Theorem 7.5.12. *Let R be a finite commutative local ring and $G = Q_{2n} = \langle x, y | x^4 = 1, y^{\frac{n}{2}} = x^2, y^x = y^{-1} \rangle$ be the generalised quaternion group of order $2n$ or $G = D_{2n} =< x, y | y^n = x^2 = 1, xyx^{-1} = y^{-1} >$ be the dihedral group of order $2n$.*

1. If $2 \in U(R)$, then RQ_{2n} and RD_{2n} are $*$-semiclean.

2. If $2 \in J(R)$, then RQ_{2n} and RD_{2n} (where n is a power of 2) are $*$-semiclean.

Proof. *1. The proof is similar to the proof of Theorem 7.5.7(1).*

2. As R is local, Q_{2n} and D_{2n} are finite 2-groups, and $2 \in J(R)$, therefore, by Proposition 7.5.2, RQ_{2n} and RD_{2n} are local. Thus, RQ_{2n} and RD_{2n} are $*$-semiclean rings.

□

The example below is the direct consequence of Theorem 7.5.12.

Example 7.5.13. *The ring $F_q Q_{2n}$ (where $gcd(q, 2) = 1$) is clean. Furthermore, because $2 \in U(F_q Q_{2n})$, we can conclude from Theorem 7.5.12(1) that $F_q Q_{2n}$ is $*$-semi-clean. However, according to (30, Theorem 4.7), $F_q Q_{2n}$ is not $*$-clean if $4|n$ and $gcd(q, 2n) = 1$.*

In 2015 (21), Gao, Chen, and Li investigated the group ring $\mathbb{Z}_2 D_6$, and proved that it is not $*$-clean; however, Example 7.5.14 demonstrates that it is $*$-semiclean. To prove $\mathbb{Z}_2 D_6$ is $*$-semiclean, we have shown that every element is written as sum of a $*$-periodic element and a unit. To check this, we first represented every element of $\mathbb{Z}_2 D_6$ in a matrix, and by using the SAGE (54) software obtain units, $*$-periodic elements. We then checked whether every element of $\mathbb{Z}_2D_6$ can be written as sum of a ∗-periodic element and unit of it. By (33), the matrix representation $\sigma(v)$ of an element $v = \alpha_0+\alpha_1y+\alpha_2y^2+\alpha_3x+\alpha_4yx+\alpha_5y^2x \in RD_6$, where $D_6 = \langle x, y | y^3 = x^2 = 1, xyx^{-1} = y^{-1}\rangle$ is a dihedral group of order 6, as given by $\sigma(v) = \begin{bmatrix} A & B \\ B^T & A^T \end{bmatrix}$, where $A = circ\begin{bmatrix}\alpha_0 & \alpha_1 & \alpha_2\end{bmatrix}$ and $B = circ\begin{bmatrix}\alpha_3 & \alpha_4 & \alpha_5\end{bmatrix}$. The codes for this are given below.

Example 7.5.14. *Consider the ring $\mathbb{Z}_2D_6$. The group of all units of $\mathbb{Z}_2D_6$ is* $U(\mathbb{Z}_2D_6) = \{x, yx, y^2x, 1, y+y^2+x+yx+y^2x, 1+y+y^2+x+yx, 1+y+y^2+x+y^2x, 1+y+y^2+yx+y^2x, y, y^2, 1+y+x+yx+y^2x, 1+y^2+x+yx+y^2x\}$. *The set of all ∗-peridic elements of $\mathbb{Z}_2D_6$ is* $Pri^*(\mathbb{Z}_2D_6) = \{0, x, yx, x+yx, y^2x, x+y^2x, yx+y^2x, x+yx+y^2x, 1, 1+x, 1+yx, 1+x+yx, 1+y^2x, 1+x+y^2x, 1+yx+y^2x, 1+x+yx+y^2x, y, y+x+yx+y^2x, 1+y, 1+y+x+yx+y^2x, y^2, y^2+x+yx+y^2x, 1+y^2, 1+y^2+x+yx+y^2x, y+y^2, y+y^2+x, y+y^2+yx, y+y^2+x+yx, y+y^2+y^2x, y+y^2+x+y^2x, y+y^2+yx+y^2x, y+y^2+x+yx+y^2x, 1+y+y^2, 1+y+y^2+x, 1+y+y^2+yx, 1+y+y^2+x+yx, 1+y+y^2+y^2x, 1+y+y^2+x+y^2x, 1+y+y^2+yx+y^2x, 1+y+y^2+x+yx+y^2x\}$. *Every element of $\mathbb{Z}_2D_6$ can be written as the sum of a ∗-periodic element and a unit. Thus, we can say that the group ring $\mathbb{Z}_2D_6$ is ∗-semiclean, but by (21, Theorem 3.4), it is not ∗-clean.*

Code for the construction of a matrix representation of $\mathbb{Z}_2D_6$.

```
Type = Integer(3)
Field = GF(Integer(2))
Vector = Field*Type
CM = [matrix.circulant(a) for a in Vector]
Length = len(CM)
Matrices_64 = []
for x in range(Length):
for y in range(Length):
CB = block_matrix(Integer(2),Integer(2),[CM[x],CM[y],CM[y].T,CM[x].T])
Matrices_64.append(CB)
```

Code to find the units of $\mathbb{Z}_2D_6$.

```
Elements = Field*Integer(1)
Zero = Elements[Integer(0)][Integer(0)]
One = Elements[Integer(1)][Integer(0)]
```

```
Identity_row = [One,Zero,Zero,Zero,Zero,Zero]
Identity_Matrix = matrix.circulant(Identity_row)
Matrices_Unit = []
List_Matrices_64 = list(range(len(Matrices_64)))
for x in List_Matrices_64:
y = x
while y <=List_Matrices_64[len(List_Matrices_64)-Integer(1)]:
if y not in List_Matrices_64:
y = y+Integer(1)
else:
mul_r = Matrices_64[x]*Matrices_64[y]
if mul_r == Identity_Matrix:
mul_r_rev = Matrices_64[y]*Matrices_64[x]
if mul_r_rev == Identity_Matrix:
Matrices_Unit.append(x)
Matrices_Unit.append(y)
break
y = y+Integer(1)
```

Code to find the ∗-periodic element of $\mathbb{Z}_2 D_6$.

```
Zero_row = [Zero for x in range(Integer(6))]
Zero_Matrix = matrix.circulant(Zero_row)
Zero_row_3 = [Zero for x in range(Integer(3))]
One_row_3 = [One for x in range(Integer(3))]
Combination_row_3 = [Zero,One,One]
Zero_matrix_3 = matrix.circulant(Zero_row_3)
One_matrix_3 = matrix.circulant(One_row_3)
Comb_matrix_3 = matrix.circulant(Combination_row_3)
Projection1 =
block_matrix(2,2,[One_matrix_3,Zero_matrix_3,Zero_matrix_3,One_matrix_3])
Projection2 =
block_matrix(2,2,[Comb_matrix_3,Zero_matrix_3,Zero_matrix_3,Comb_matrix_3])
Matrices_StrPeriodic = []
N = Integer(1000000)

for x in range(len(Matrices_64)):
res = Matrices_64[x]
```

```
i = Integer(1)
while i <=N:
res = res*Matrices_64[x]
if res == Identity_Matrix or res == Zero_Matrix
or res == Projection1 or res == Projection2 :
Matrices_StrPeriodic.append([x,i+Integer(1)])
break
i = i+Integer(1)
```

Code to check whether every element of $\mathbb{Z}_2D_6$ can be written as the sum of ∗-periodic element and unit of it.

```
Matrices_Star_Semiclean = []
Star_Semiclean_map = []
StarPeriodic_Set = set(x[Integer(0)] for x in Matrices_StrPeriodic)
Unit_set = set(Matrices_Unit)

for x in StarPeriodic_Set:
for y in Unit_set:
res = Matrices_64[x]+Matrices_64[y]
if res in Matrices_64:
index = Matrices_64.index(res)
if index not in Matrices_Star_Semiclean:
Matrices_Star_Semiclean.append(index)
Star_Semiclean_map.append([x,y,index])
```

7.6 The relationship between the ∗-semicleanness of the group ring F_qG and coding theory

Consider the finite field with q elements, say F_q, and the finite abelian group with exponent n, say G, such that $(q, n) = 1$. In this section, a relationship between abelian group codes in F_qG and the ∗-semicleanness (with the classical involution ∗) of the ring F_qG is developed. Let $\bar{F}$ represent the algebraic closure of F. Let $\hat{G}$ represent the group that consists of all characters of G over F, defined as,

$$\hat{G} = \{\phi | \phi : G \to \bar{F} \text{ a homomorphism}\}$$

Also $|G| = |\hat{G}|$. For each $\phi \in \hat{G}$, we define

$$f_\phi = \frac{1}{|G|}\sum_{g\in G}\phi(g)g,$$

which is an element in $\bar{F}G$.
Clearly, an element f_ϕ satisfies the following properties:

1. $f_\phi^2 = f_\phi$, for any $\phi \in \hat{G}$.

2. $f_\phi f_\chi = 0$, for any $\phi, \chi \in \hat{G}$ with $\phi \neq \chi$.

3. $\sum_{\phi\in\hat{G}} f_\phi$.

Consequently, the set

$$K = \{f_\phi | \phi \in \hat{G}\}$$

includes each and every primitive idempotent of $\bar{F}G$.
Now using the set K we will construct the primitive idempotent of FG. Let $\phi \in \hat{G}$ be a fixed element of order d in $\hat{G}$ and w_d be defined as a d-th primitive root of unity over F. Then $f_\phi \in F(w_d)G$. More simply, we define it as

$$Tr_\phi(f_\phi) = Tr_{F(w_d)/F(f_\phi)}$$

Consider the following lemma.

Lemma 7.6.1. *(27) Let $\phi \in \hat{G}$. Then we have $Tr_\phi(f_\phi)$ is a primitive idempotent in FG. Moreover, the set*

$$F := \{Tr_\phi(f_\phi) | \phi \in \hat{G})\}$$

contains exactly all primitive idempotents of FG.

Lemma 7.6.2. *(27, Proposition 4.2) Let $\phi \in \hat{G}$ be an element of order d in $\hat{G}$ and $\mathfrak{C}_\phi$ be an abelian code generated by $Tr_\phi(f_\phi)$ in F_qG. Then we get:*

1. *$\mathfrak{C}_\phi$ is an LCD abelian code if and only if there exists $t \in N$ such that $q^t \equiv -1($ mod $d)$.*

2. *$\mathfrak{C}_\phi$ is a self-orthogonal code if and only if there exists no $t \in N$ such that $q^t \equiv -1($ mod $d)$.*

By Theorem 7.6.3, we are able to characterize LCD abelian codes and self-orthogonal abelian codes with the $*$-semicleanness of a ring. In 2021, (27) Dongchun Han and Hanbin Zhang showed that if all abelian group codes of F_qG are self-orthogonal abelian codes, then F_qG cannot be a $*$-clean ring. By Theorem 7.6.3, we are able to show that in this case, the ring F_qG will be a $*$-semiclean ring. Examples of the same are given below in Example 7.6.4.

Theorem 7.6.3. *Let F_q be a finite field of order q, G be a finite abelian group with exponent n with $(q, n) = 1$, and $\mathfrak{C}_\phi$ be the abelian code generated by $Tr_\phi(f_\phi)$ in F_qG.*

1. *If $q \neq 2$, then*
   (a) *If there exist $t \in N$ such that $q^t \equiv -1(mod\ n)$, then F_qG is $*$-semiclean if and only if all abelian group codes are LCD abelian codes in F_qG.*
   (b) *If there exist no $t \in N$ such that $q^t \equiv -1(mod\ n)$, then F_qG is $*$-semiclean if and only if all abelian group codes are self-orthogonal abelian codes in F_qG.*
2. *If $q = 2$, and G is a finite 2-group then*
   (a) *If there exist $t \in N$ such that $q^t \equiv -1(mod\ n)$, then F_qG is $*$-semiclean if and only if all abelian group codes are LCD abelian codes in F_qG.*
   (b) *If there exist no $t \in N$ such that $q^t \equiv -1(mod\ n)$, then F_qG is $*$-semiclean if and only if all abelian group codes are self-orthogonal abelian codes in F_qG.*
3. *If $q = 2$ such that there exist $t \in N$ such that $q^t \equiv -1(mod\ n)$, then F_qG is $*$-semiclean if and only if all abelian group codes are LCD abelian codes in F_qG.*

Proof. 1. (a) $\Rightarrow$ Follows from Lemma 7.6.2(1).
$\Leftarrow$ Since every abelian group code is an LCD abelian codes in F_qG, from (27, Theorem 4.2), we can say that the ring F_qG is $*$-clean. Since, every $*$-clean ring is a $*$-semiclean ring. The result follows.

(b) $\Rightarrow$ Follows from Lemma 7.6.2(2).
$\Leftarrow$ Follows from Theorem 7.5.8(1).

2. (a) $\Rightarrow$Follows from Lemma 7.6.2(1).
$\Leftarrow$ Since every abelian group codes are LCD abelian codes in F_qG, from (27, Theorem 4.2), we can say that the ring F_qG is $*$-clean. Since, every $*$-clean ring is a $*$-semiclean ring. The result follows.

(b) $\Rightarrow$ Follows from Lemma 7.6.2(2).
$\Leftarrow$ Since $q = 2$, therefore $2 \in J(F_q)$, by Proposition 7.5.2, F_qG is local. Since every local ring is a $*$-semiclean ring, F_qG is also $*$-semiclean.

3. $\Rightarrow$Follows from Lemma 7.6.2(1).
$\Leftarrow$ Follows from Theorem 7.5.8(3).

□

In Example 7.6.4, we have given examples of group rings that are not $*$-clean but are $*$-semiclean rings such that all their abelian group codes are self-orthogonal abelian codes.

Example 7.6.4. 1. *Consider the group ring* F_3C_8*. Since there is no* $t \in \mathbb{N}$ *such that* $3^t \equiv -1(mod\ 8)$*, by Lemma 7.6.2, all its abelian group codes are self-orthogonal abelian codes. By Theorem 7.6.3,* F_3C_8 *is* $*$*-semiclean. Also by (53, Example 3.12), it is not* $*$*-clean.*

2. *Consider the group ring* F_3C_{35}*. Since there is no* $t \in \mathbb{N}$ *such that* $3^t \equiv -1(mod\ 35)$*, by Lemma 7.6.2, all its abelian group codes are self-orthogonal abelian codes. By Theorem 7.6.3,* F_3C_{35} *is* $*$*-semiclean.*

7.7 Conclusion

In this chapter, we have developed a new class of ring that is $*$-semiclean ring and build a relationship between the $*$-semicleanness of a ring with the LCD and self-orthogonal abelian codes.

References

[1] Berman, S. D. (1967). Semisimple cyclic and Abelian codes. II. Cybernetics, 3(3), 17-23.

[2] Bernhardt, F., Landrock, P., & Manz, O. (1990). The extended Golay codes considered as ideals. Journal of Combinatorial Theory, Series A, 55(2), 235-246.

[3] Betsumiya, K., Georgiou, S., Gulliver, T. A., Harada, M., & Koukouvinos, C. (2003). On self-dual codes over some prime fields. Discrete Mathematics, 262(1-3), 37-58.

[4] Blahut, R. E. (2003). Algebraic codes for data transmission. Cambridge university press.

[5] Boripan, A., Jitman, S., & Udomkavanich, P. (2018). Characterization and enumeration of complementary dual abelian codes. Journal of Applied Mathematics and Computing, 58, 527-544.

[6] Chen, C. L., Peterson, W. W., & Weldon Jr, E. J. (1969). Some results on quasi-cyclic codes. Information and Control, 15(5), 407-423.

[7] Chen, J., & Cui, J. (2013). Two questions of L. Vas on $*$-clean rings. Bulletin of the Australian Mathematical Society, 88(3), 499-505.

[8] Chin, A. (2004). A note on strongly π-regular rings. Acta Mathematica Hungarica, 102(4), 337-342.

[9] Creedon, L., & Gildea, J. (2009). Unitary Units of The Group Algebra $\mathbb{F}_{2^k}Q_8$. arXiv preprint arXiv:0905.4644.

[10] Cui, J., & Wang, Z. (2015). A note on strongly-$*$-clean rings. Journal of the Korean Mathematical Society, 52(4), 839-851.

[11] Cui, J., & Danchev, P. (2020). Some new characterizations of periodic rings. Journal of Algebra and Its Applications, 19(12), 2050235.

[12] Dougherty, S. T., Gaborit, P., Harada, M., & Solé, P. (1999). Type II codes over $F_2 + uF_2$. IEEE Transactions on Information Theory, 45(1), 32-45.

[13] Dougherty, S. T., Kim, J. L., Kulosman, H., & Liu, H. (2010). Self-dual codes over commutative Frobenius rings. Finite Fields and Their Applications, 16(1), 14-26.

[14] Dougherty, S. T., Yildiz, B., & Karadeniz, S. (2011). Codes over R_k, Gray maps and their binary images. Finite Fields and Their Applications, 17(3), 205-219.

[15] Dougherty, S. T., Yildiz, B., & Karadeniz, S. (2013). Self-Dual Codes over R_k and Binary Self-Dual Codes. European Journal of Pure and Applied Mathematics, 6(1), 89-106.

[16] Dougherty, S. T. (2017). Algebraic coding theory over finite commutative rings. Springer International Publishing.

[17] Dougherty, S. T., Gildea, J., Taylor, R., & Tylyshchak, A. (2018). Group rings, G-codes and constructions of self-dual and formally self-dual codes. Designs, Codes and Cryptography, 86, 2115-2138.

[18] Dougherty, S., Gildea, J., Kaya, A., & Korban, A. (2019). Composite constructions of self-dual codes from group rings and new extremal self-dual binary codes of length 68.

[19] Dougherty, S. T., Gildea, J., Korban, A., Kaya, A., Tylyshchak, A., & Yildiz, B. (2019). Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes. Finite Fields and Their Applications, 57, 108-127.

[20] Gallian, J. A. (2021). Contemporary abstract algebra. Chapman and Hall/CRC.

[21] Gao, Y., Chen, J., & Li, Y. (2015). Some $*$-clean group rings. Algebra Colloquium, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, and Suzhou University, 22(1), 169-180.

[22] Gildea, J., Kaya, A., Taylor, R., & Yildiz, B. (2018). Constructions for self-dual codes induced from group rings. Finite Fields and Their Applications, 51, 71-92.

[23] Gildea, J., Kaya, A., Korban, A., & Yildiz, B. (2020). Constructing self-dual codes from group rings and reverse circulant matrices.

[24] Gildea, J., Taylor, R., Kaya, A., & Tylyshchak, A. (2020). Double bordered constructions of self-dual codes from group rings over Frobenius rings. Cryptography and Communications, 12, 769-784.

[25] Gulliver, T. A., & Harada, M. (1997). Classification of extremal double circulant formally self-dual even codes. Designs, Codes and Cryptography, 11, 25-35.

[26] Gulliver, T. A., & Harada, M. (2008). On doubly circulant doubly even self-dual [72, 36, 12] codes and their neighbors. Australasian Journal of Combinatorics, 40, 137.

[27] Han, D., & Zhang, H. (2021). On $*$-clean group rings over finite fields. Finite Fields and Their Applications, 73, 101863.

[28] Houghten, S. K., Lam, C. W., Thiel, L. H., & Parker, J. A. (2003). The extended quadratic residue code is the only $[48, 24, 12]$ self-dual doubly-even code. IEEE Transactions on Information Theory, 49(1), 53-59.

[29] Houghton, S., Lam, C., & Thiel, L. (1994). Construction of [48, 24, 12] doubly-even self-dual codes. Congressus Numerantium, 41-54.

[30] Huang, H., Li, Y., & Tang, G. (2016). On $*$-clean non-commutative group rings. Journal of Algebra and Its Applications, 15(08), 1650150.

[31] Huang, H., Li, Y., & Yuan, P. (2016). On $*$-clean group rings II. Communications in Algebra, 44(7), 3171-3181.

[32] Huffman, W. C., & Pless, V. (2010). Fundamentals of error-correcting codes. Cambridge university press.

[33] Hurley, T. (2006). Group rings and rings of matrices. Int. J. Pure Appl. Math, 31(3), 319-335.

[34] Hurley, P., & Hurley, T. (2009). Codes from zero-divisors and units in group rings. International Journal of Information and Coding Theory, 1(1), 57-87.

[35] Hurley, P., & Hurley, T. (2010). Block codes from matrix and group rings. In Selected Topics in Information and Coding Theory (pp. 159-194).

[36] Karlin, M. (1969). New binary coding results by circulants. IEEE Transactions on Information Theory, 15(1), 81-92.

[37] Klingler, L., Loper, K. A., McGovern, W. W., & Toeniskoetter, M. (2021). Semiclean group rings. Journal of Pure and Applied Algebra, 225(11), 106744.

[38] Lam, T. Y. (1991). A first course in noncommutative rings (Vol. 131, pp. New-York). New York: Springer-verlag.

[39] Li, Y., Parmenter, M. M., & Yuan, P. (2015). On $*$-clean group rings. Journal of Algebra and Its Applications, 14(01), 1550004.

[40] Li, F., Yue, Q., & Wu, Y. (2019). LCD and Self-Orthogonal Group Codes in a Finite Abelian p-Group Algebra. IEEE Transactions on Information Theory, 66(5), 2717-2728.

[41] Mac Lane, S., & Birkhoff, G. (1999). Algebra (Vol. 330). American Mathematical Soc.

[42] MacWilliams, F. J., Odlyzko, A. M., Sloane, N. J., & Ward, H. N. (1978). Self-dual codes over GF (4). Journal of Combinatorial Theory, Series A, 25(3), 288-318.

[43] McLoughlin, I., & Hurley, T. (2008). A group ring construction of the extended binary Golay code. IEEE transactions on information theory, 54(9), 4381-4383.

[44] McLoughlin, I. (2012). A group ring construction of the $[48, 24, 12]$ Type II linear block code. Designs, Codes and Cryptography, 63, 29-41.

[45] Nicholson, W. K. (1972). Local group rings. Canadian Mathematical Bulletin, 15(1), 137-138.

[46] Immormino, N. A., & McGovern, W. W. (2014). Examples of clean commutative group rings. Journal of Algebra, 405, 168-178.

[47] O'Neill, H. T. (2017). Group Algebras and Their Applications.

[48] Piper, F. C. (1987). A first course in coding theory (Oxford Applied Mathematics and Computing Series).

[49] Rains, E. M. (1998). Shadow bounds for self-dual codes. IEEE Transactions on Information Theory, 44(1), 134-139.

[50] Sehgal, S. K., & Milies, C. P. (2002). An introduction to group rings. Kluwer Academic Publishers.

[51] Shi, M., Sok, L., Solé, P., & Çalkavur, S. (2018). Self-dual codes and orthogonal matrices over large finite fields. Finite Fields and their Applications, 54, 297-314.

[52] Shi, M., Qian, L., & Solé, P. (2018). On self-dual negacirculant codes of index two and four. Designs, Codes and Cryptography, 86, 2485-2494.

[53] Tang, G., Wu, Y., & Li, Y. (2017). $*$-Cleanness of finite group rings. Communications in Algebra, 45(10), 4190-4195.

[54] The SAGE Group, SAGE: Mathematical software, version 2.10, http://www.sagemath.org/

[55] Vaš, L. (2010). $*$-Clean rings; some clean and almost clean Baer $*$-rings and von Neumann algebras. Journal of Algebra, 324(12), 3388-3400.

[56] Wang, Z., & Chen, J. L. (2009). 2-clean rings. Canadian Mathematical Bulletin, 52(1), 145-153.

[57] Wang, Y., & Ren, Y. (2013). 2-good rings and their extensions. Bulletin of the Korean Mathematical Society, 50(5), 1711-1723.

[58] Ye, Y. (2003). Semiclean rings. Communications in Algebra, 31(11), 5609-5625.

[59] Zhou, Y. (2010). On clean group rings. In Advances in ring theory (pp. 335-345). Birkhäuser Basel.

List of Publications

1. Shefali Gupta, Dinesh Udar. $*$-Semiclean Rings. *Turkish Journal of Mathematics*, 47(5), 1406-1422, (2022). https://doi.org/10.55730/1300-0098.3437 **(SCIE, Impact Factor 1)**.

2. Shefali Gupta, Dinesh Udar. An Altered Group Ring Construction of the $[24, 12, 8]$ and $[48, 24, 12]$ Type II Linear Block Code. *Bulletin of the Korean Mathematical Society*, 60(3), 829-844, (2023). 10.4134/BKMS.b220378 **(SCIE, Impact Factor 0.5)**.

3. Shefali Gupta, Dinesh Udar. Self-dual and modified codes over Q_8 group ring. *Emerging Advancements in Mathematical Sciences, Nova Science Publishers*, 1-22, (2022). **(SCOPUS)**.

4. Shefali Gupta, Dinesh Udar. New construction of Extremal Self-Dual Binary Codes of length 64. (Communicated).

5. Dinesh Udar, Shefali Gupta. Double bordered constructions of linear self-dual codes from altered four-circulant matrix over Frobenius rings. (Communicated).

6. Dinesh Udar, Shefali Gupta. $\frac{n}{r}$-th bordered constructions of self-dual codes from Group rings over Frobenius rings. (Communicated).

Papers presented in International Conferences

1. Self-dual and Modified Codes Over Q_8 Group Ring; 5^{th} *International Conference on Recent Advances in Mathematical Sciences and its Applications* (RAMSA-2021), Jaypee Institute of Information Technology, Noida, India, December 2-4, 2021.

2. Bordered Four Circulant for Self-dual Codes from Group Rings; *International Conference on Graphs, Networks and Combinatorics* (ICGNC-2023), Ramanujan College, Delhi, India, January 10-12, 2023.

3. Application of $*$-Semiclean ring in construction of LCD abelian codes and self-orthogonal abelian codes; *1st International Mathematics Conclave 2023* (IMC-2023), Sastra University, Kerala, India, November 23-25, 2023.