T.C.
İSTANBUL UNIVERSITY
INSTITUTE OF GRADUATE STUDIES IN
SCIENCE AND ENGINEERING

Ph.D. THESIS

ON CODES OVER AN INFINITE FAMILY OF RING EXTENSION OF THE BINARY FIELD

Nesibe TÜFEKÇİ

Department of Mathematics

Mathematics Programme

Ph. D. Student transferred from Fatih University which has been closed

SUPERVISOR
Assoc. Prof. Dr. Bahattin YILDIZ

June, 2016

İSTANBUL

APPROVAL PAGE

This is to certify that I have read this thesis written by Nesibe Tüfekçi and that in my opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy in Mathematics.

Assoc. Prof. Bahattin YILDIZ
Thesis Supervisor

I certify that this thesis satisfies all the requirements as a thesis for the degree of Doctor of Philosophy in Mathematics.

F. Başar.

Prof. Feyzi BAŞAR
Head of Department

Examining Committee Members

Assoc. Prof. Bahattin YILDIZ

Assoc. Prof. Suat KARADENİZ

Assoc. Prof. Bülent KÖKLÜCE

Asst. Prof. Abidin KAYA

Asst. Prof. Gül KARADENİZ GÖZERİ

It is approved that this thesis has been written in compliance with the formatting rules laid down by the Graduate School of Sciences and Engineering.

Prof. Nurullah ARSLAN
Director

June 2016

ON CODES OVER AN INFINITE FAMILY OF RING EXTENSION OF THE BINARY FIELD

Nesibe Tüfekçi

Ph.D. Thesis – Mathematics
June 2016

Thesis Supervisor: Assoc. Prof. Bahattin YILDIZ

ABSTRACT

Codes over rings have recently been the center of interest amongst the researchers. In this thesis, we focus on codes over an infinite family of ring extension of the binary field. The rings of the form $\mathbb{F}_2+u\mathbb{F}_2+\cdots+u^k\mathbb{F}_2$ and $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ are generalized to a family of rings that we call $\mathcal{R}_{k,m}$, where $\mathcal{R}_{k,m}$ is defined to be $\mathbb{F}_2[u,v]/\left\langle u^k, v^m, uv-vu\right\rangle$.

The structural properties of the finite-commutative and characteristic 2 ring $\mathcal{R}_{k,m}$ are described. Linear codes over the ring $\mathcal{R}_{k,m}$ are defined and a Gray map that is distance preserving and more importantly orthogonality-preserving from $\mathcal{R}_{k,m}$ to $\mathbb{F}_2^{km}$ are found with the corresponding Lee weight. MacWilliams identities which give a relation between weight enumerators of a code and its dual are proved for codes over $\mathcal{R}_{k,m}$ for all the relevant weight enumerators.

Many binary self-dual codes as the Gray images of self-dual codes over $\mathcal{R}_{k,m}$ are constructed by combination of methods involving circulant matrices and extension methods. Moreover, the homogeneous weight for $\mathcal{R}_{k,m}$ was characterized using theoretical properties of the ring and an associated Gray map was found. Using this Gray map, many optimal binary codes that are divisible and self-orthogonal quasicyclic codes were obtained.

Keywords: extremal self-dual codes, Gray maps, codes over rings, MacWilliams identities, quadratic double circulant codes, homogeneous weight

İKİLİ CİSMİN HALKA GENİŞLEMESİNİN SONSUZ BİR AİLESİ ÜZERİNE TANIMLI KODLAR

Nesibe Tüfekçi

Doktora Tezi – Matematik
Haziran 2016

Tez Danışmanı: Doç. Dr. Bahattin YILDIZ

ÖZ

Son zamanlarda halkalar üzerine tanımlı kodlar araştırmacılar arasında ilgi odağı haline gelmiştir. Bu tez, ikili cismin halka genişlemesinin sonsuz bir ailesi üzerinde tanımlı kodlar üzerine bir çalışmadır. $\mathbb{F}_2+u\mathbb{F}_2+\cdots+u^k\mathbb{F}_2$ ve $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ formundaki halkalar, $\mathcal{R}_{k,m}$ olarak adlandırdığımız ve $\mathbb{F}_2[u,v]/\left\langle u^k, v^m, uv-vu\right\rangle$ şeklinde tanımladığımız bir halka ailesine genelleştirildi.

Öncelikle, sonlu, değişmeli ve karakteristiği 2 olan $\mathcal{R}_{k,m}$ halka ailesinin yapısal özellikleri belirlendi. Ayrıca, bu halka ailesi üzerinde lineer kodlar tanımlandı ve $\mathcal{R}_{k,m}$ den $\mathbb{F}_2^{km}$'e tanımlı, uzaklığı ve daha önemlisi dikliği koruyan bir Gray eşleme uygun bir Lee ağırlıkla birlikte bulundu.

Bir kodun ve dualinin ağırlık dağılımlarının arasındaki ilişkiyi veren MacWilliams özdeşlikleri $\mathcal{R}_{k,m}$ üzerine tanımlı kodların tüm ilgili ağırlık dağılımları için ispatlandı.

Devirsel matrisler ve genişleme metodlarıyla elde edilen $\mathcal{R}_{k,m}$ üzerinde tanımlı self-dual kodların ikili görüntüsü alınarak yeni ikili self-dual kodlar inşa edildi. Ayrıca, $\mathcal{R}_{k,m}$ üzerinde tanımlı kodlar için homojen ağırlık karakterize edildi ve ilişkili bir Gray eşleme bulundu. Bu Gray eşleme kullanılarak bölünebilir, kendine dik yarı devirli optimal ikili kodlar elde edildi.

Anahtar Kelimeler: ekstrem self-dual kodlar, Gray eşleme, halkalar üzerine tanımlı kodlar, MacWilliams özdeşlikleri, kuadratik 2-devirsel kodlar, homojen ağırlık

To my family

ACKNOWLEDGEMENT

I would like to thank my supervisor Assoc. Prof. Bahattin YILDIZ for his guidance, help and suggestions throughout the research and writing the thesis.

I would like to send my special thanks to Asst. Prof. Abidin KAYA due to his endless support, valuable comments and contributions. I am thankful to also Asst. Prof. İsmail Gökhan KELEBEK, Assoc. Prof. Suat KARADENİZ and Assoc. Prof. Bülent KÖKLÜCE for their encouragement and support.

I express my thanks and appreciation to my family for their understanding, motivation and patience.

Lastly, I would like to send my special thanks to TUBITAK-BIDEB due to their financial support and their kind guidance to all scientist candidates.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF SYMBOLS AND ABBREVIATIONS

SYMBOL/ABBREVIATION	
CWE	Complete weight enumerator
ω_H	Hamming weight
HWE	Hamming weight enumerator
ω_{hom}	Homogeneus weight
Rad(R)	Jacobson radical of the ring R
ω_L	Lee weight
LWE	Lee weight enumerator
QDC	Quadratic double circulant
$\mathcal{Q}_p$	Set of quadratic residues modulo p
$\mathcal{N}_p$	Set of quadratic non residues modulo p
Soc(R)	Socle of the ring R

CHAPTER 1

INTRODUCTION

Coding theory, a research area that combines applications from engineering and various branches of mathematics, is based on the problem of securely transmitting data through a noisy channel. It works for efficient and accurate transfer of information in almost all areas of communication such as compact disc recording, telephone lines and satellite communication. The influential paper “A mathematical theory of communication” published in 1948 (Shannon, 1948) by Claude Shannon, points out the beginning of mathematical point of view to coding theory.

The main objective of coding theory is getting maximal detection and even correction of errors while satisfying maximum transfer of information per unit time. Figure 1.1 illustrates the main scheme of coding theory. Significant improvements were observed in coding theory over the last fifty years. The focus of coding theorists was studying error correcting codes over finite fields in early periods, till the end of 80s, especially over the binary field $\mathbb{F}_2$. In 1994 (Hammons et al., 1994), Hammons et al. solved an old problem in coding theory related to non-linear binary codes through the ring $\mathbb{Z}_4$. In this work, they explained the seeming duality of the nonlinear binary Kerdock and Preparata codes by viewing them as Gray images of dual linear codes over the ring $\mathbb{Z}_4$. Since then, a great deal of interest has been given to codes over finite rings.

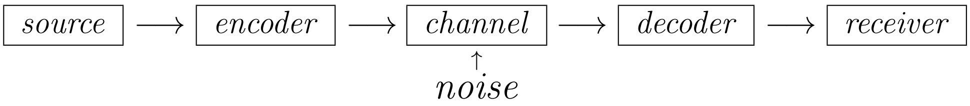

Figure 1.1 communication channel.

A great deal of interest has also been given to codes over another ring of order 4, namely $\mathbb{F}_2 + u\mathbb{F}_2$. $\mathbb{F}_2 + u\mathbb{F}_2$ is a finite chain ring like the ring $\mathbb{Z}_4$ but they have different characteristics. In (Dougherty et al., 1999) a linear Gray map was described from the ring $\mathbb{F}_2 + u\mathbb{F}_2$ to the binary field. Inspiring from this work many coding theorists focused on codes over finite chain rings which have unique forms of generating matrices. Self-dual codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$ were obtained for some lengths by Karadeniz et al (Karadeniz et al., 2014b). In 2010, this ring and its corresponding Gray map were generalized to codes over non chain and non principal ideal ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ with a linear Gray map by Yıldız and Karadeniz (Yildiz and Karadeniz, 2010a) and they have focused on self-dual codes over this ring in (Yildiz and Karadeniz, 2010b). The ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ has recently been used quite successfully to construct many good binary self-dual codes. Also cyclic codes and consta-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ have been studied in (Karadeniz and Yildiz, 2011), (Yildiz and Karadeniz, 2011). The ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ was later generalized to what is now called "$\mathcal{R}_k$", an infinite family of rings, used to build binary codes with a rich automorphism group in (Dougherty et al., 2011) and different types of codes over this ring were studied in (Dougherty et al., 2012), (Karadeniz et al., 2014a), (Karadeniz and Yildiz, 2013). This family of rings have provided an alternate method, to many existing ones, of constructing binary self-dual codes of different automorphism groups, and in many cases codes with new weight enumerators. The common theme in these works is the presence of a duality and distance preserving Gray map and the intricate structure of the ring with a high number of units that lead to large automorphism groups.

In (Wood, 1999), Wood argued that Frobenius rings are the largest class of rings for which classical theorems of MacWilliams, the extension theorem and MacWilliams identities, are valid. This has led to the belief among coding theorists that Frobenius rings are the largest class of rings to study in coding theory. Consequently, many different Frobenius rings were studied within that context for different reasons and motivations, leading to many different results. Among the oft-studied rings we can name $\mathbb{Z}_4$, $\mathbb{Z}_{p^k}$, Galois rings, finite chain rings, $\mathbb{F}_2 + v\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, R_k, etc.

In this thesis, we introduce a generalization of rings of the form $\mathbb{F}_2 + u\mathbb{F}_2 +$

$\cdots + u^k\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ to a family of rings that we denote by $\mathcal{R}_{k,m}$, where $\mathcal{R}_{k,m} = \mathbb{F}_2[u,v]/\left\langle u^k, v^m, uv - vu\right\rangle$. Note that $\mathcal{R}_{1,1} = \mathbb{F}_2$, the binary field; $\mathcal{R}_{2,1} = \mathbb{F}_2 + u\mathbb{F}_2$; $\mathcal{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and $\mathcal{R}_{k,1} = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$. We establish that this is a Frobenius, characteristic 2, family of rings that is non-chain when k and m are both greater than 1. We find a duality-preserving Gray map from $\mathcal{R}_{k,m}$ to $\mathbb{F}_2^{km}$, and using some of the common construction methods of self-dual codes we find many good binary self-dual codes as the Gray images of self-dual codes over $\mathcal{R}_{k,m}$ for suitable k and m. Furthermore, we define an alternative weight which is called the homogeneous weight for codes over $\mathcal{R}_{k,m}$ together with an associated Gray map and we get some divisible optimal binary linear codes taking homogeneous Gray images of cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$.

1.1 BASIC DEFINITIONS

We begin with some required definitions and basic facts about coding theory and refer to (Huffman and Pless, 2003), (Ling and Xing, 2004) and (MacWilliams and Sloane, 1978) for a more detailed reading.

Let F be a set of size q. The set F is said to be an *alphabet.* A *q-ary block code* of length n over F is a nonempty set C of q-ary words of length n and an element of C is called a *codeword* in C. A code over the code alphabet $\mathbb{F}_2$ is called a *binary* code. The number of codewords in C, denoted by $|C|$ is called the *size* of the code. A code of length n and size M is called an (n, M)-code.

Let $\mathbb{F}_q$ be the finite field of order q for some $q = p^m$. A *linear code* C over $\mathbb{F}_q$ of length n is a vector subspace of $\mathbb{F}_q^n$. Linear codes have been studied more than nonlinear codes because of their algebraic structure, allowing them to describe and use more easily than nonlinear codes. On the other hand, a *linear code* C of length n over a ring R is a R-submodule of R^n.

The *Hamming distance* is defined as

$$d_H(\bar{x}, \bar{y}) = |\{i|x_i \neq y_i\}|$$

where $\bar{x} = (x_1, \cdots, x_n)$ and $\bar{y} = (y_1, \cdots, y_n)$ are two words of length n over F. The *Hamming weight* ω_H of a vector is defined to be the number of nonzero coordinates and we have $d_H(x,y) = \omega_H(x-y)$. The *minimum distance* of a code C of length n is defined as

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

The *minimum Hamming weight* of C, denoted $\omega_H(C)$, is the smallest of the weights of the nonzero codewords of C and it is same with the minimum distance $d(C)$ for linear codes. A linear code C of length n and dimension k with the minimum distance d is often called an $[n,k,d]$-code. Let C be a linear code over $\mathbb{F}_q$ of length n, then the *dual* of C is the orthogonal complement of the subspace C of $\mathbb{F}_q^n$ respect to standard Euclidean inner product.

Two codes are called *equivalent* if one can be obtained from the other by a permutation. A code is called *isodual* if it is equivalent to its dual.

A *generator matrix* for a $[n,k]$- linear code C is a $k \times n$ matrix G whose rows form a basis for C and a *parity-check matrix* H of this code is a generator matrix for the dual code $C^{\perp}$.

As the focal part of this thesis, we mention self-dual codes briefly. A code C is defined as *self-orthogonal* if $C \subseteq C^{\perp}$, *self-dual* if $C = C^{\perp}$. Since they have close connection to lattices, designs and information theory, construction of self-dual codes of different lengths received a great deal of attention among coding theorists, especially binary ones(for example (Dougherty et al., 1997); (Betsumiya et al., 2003); (Bouyukliev et al., 2005); (Dontcheva., 2002)). A binary self-dual code is called *doubly even* or *Type II* if the weight of every codeword is divisible by 4, a binary self-dual code with some codeword of weight not divisible by 4 is called *singly-even* or *Type I.*

If C is a code of parameters $[n,k,d]$, then it can correct up to $\lfloor (d-1)/2 \rfloor$errors. By a good code we usually mean a code whose information rate k/n is as high as possible, with minimum distance d is also as high as possible. However, these are *conflicting* parameters, and there are numerous bounds that relate these parameters. So, finding good codes has always been one of the main questions in coding theory.

1.2 OVERVIEW OF THE DISSERTATION

In Chapter 2, the structure of the ring $\mathcal{R}_{k,m}$ with fundamental properties and linear codes over the ring are investigated. We introduce the Lee weight and the related distance-preserving Gray map, which we prove to be orthogonality-preserving as well. We verify the MacWilliams identities for the complete, Hamming and also Lee weight enumerators, for codes over $\mathcal{R}_{k,m}$.

Chapter 3 contains our different construction methods, lift, circulant matrices and extensions, to get binary self-dual codes as Gray images of self-dual codes over $\mathcal{R}_{k,m}$ for suitable k and m. We tabulate many good binary self-dual codes, including an alternate construction to the extended binary Golay code, which has many different constructions in the literature.

In Chapter 4, a new weight on $\mathcal{R}_{k,m}$, namely the homogeneous weight, is formed different from Hamming and Lee weight and the Gray-homogeneous map is constructed using first order Reed-Muller codes. We list a considerable number of optimal binary codes that are divisible with high levels of divisibility using the images of cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$ of different lengths.

The last chapter concludes the thesis with possible directions for future research in the related areas.

CHAPTER 2

LINEAR CODES OVER THE RING $\mathcal{R}_{k,m}$

In this chapter, we will study linear codes over $\mathcal{R}_{k,m}$. Primarily, we familiarize the ring $\mathcal{R}_{k,m}$ which is an infinite family of ring extension of the binary field, by describing some of their properties, which are substantial to study linear codes over this ring. For the rest of the chapter, we will define the Lee weight and the corresponding Gray map for codes over the ring $\mathcal{R}_{k,m}$. Besides these, we will give MacWilliams identities for codes over $\mathcal{R}_{k,m}$ for all the relevant weight enumerators.

2.1 THE STRUCTURE OF THE RING $\mathcal{R}_{k,m}$

The ring $\mathcal{R}_{k,m}$ is a generalization of rings of the form $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, which we shall denote by $\mathcal{R}_{k,1}$ and $\mathcal{R}_{2,2}$ respectively, from here on.

The ring $\mathcal{R}_{k,1} = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ is defined by $u^k = 0$ where $k > 0$. It is a characteristic 2 ring and has size 2^k. The following figure shows the ideal structure of this ring

$$\{0\} \subset u^{k-1}\mathcal{R}_{k,1} \subset \ldots \subset u\mathcal{R}_{k,1} \subset \mathcal{R}_{k,1}$$

Figure 2.1 The ideal lattice of the ring $\mathcal{R}_{k,1}$.

Thus, the ring $\mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$ is a principal ideal ring and it is also a finite chain ring.

The other ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which is a generalization of $\mathbb{F}_2 + u\mathbb{F}_2$ is defined in (Yildiz and Karadeniz, 2010a) as a characteristic 2 ring with 16 elements subject to the restrictions $u^2 = v^2 = 0$ and $uv = vu$. The lattice of ideals of the ring is given by the following:

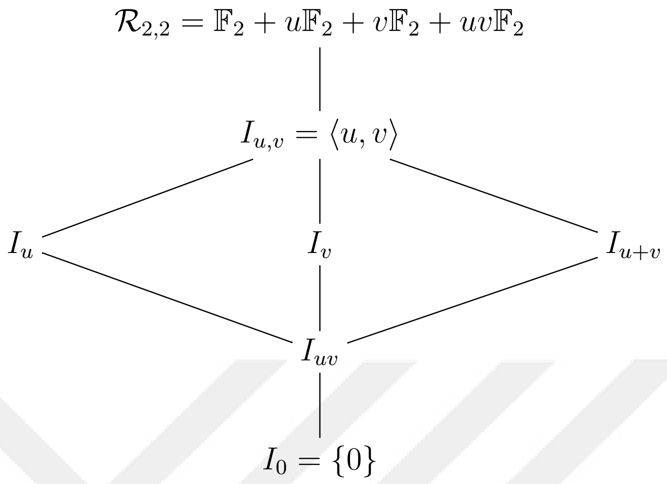
$\mathcal{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$
$I_{u,v} = \langle u, v \rangle$
I_u
I_v
I_{u+v}
I_{uv}
$I_0 = \{0\}$

Figure 2.2 The ideal lattice of the ring $\mathcal{R}_{2,2}$.

As seen in figure the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ is not a principal ideal ring and it is not a chain ring.

Now, we introduce the ring $\mathcal{R}_{k,m}$. The ring $\mathcal{R}_{k,m}$ is defined as follows for $k \geq m \geq 1$:

$$\mathcal{R}_{k,m} = \mathbb{F}_2[u,v] / \left\langle u^k, v^m, uv - vu \right\rangle .$$

$\mathcal{R}_{k,m}$ is a characteristic 2 ring of size 2^{km}. When $k = m = 1$ the ring is simply $\mathbb{F}_2$. When $k = 2, m = 1$ the ring is $\mathbb{F}_2 + u\mathbb{F}_2$ and codes over this ring have been studied quite extensively in the literature (Dougherty et al., 1999). When $k = m = 2$ the ring is $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ and codes over this ring were studied in from many different angles.

$\mathcal{R}_{k,m}$ can be viewed as an $\mathbb{F}_2-$vector space with a basis

$$\left\{u^i v^j \mid 0 \leq i \leq k-1, 0 \leq j \leq m-1\right\}.$$

Any element of $\mathcal{R}_{k,m}$ can be represented as

$$\sum_{\substack{0 \leq i \leq k-1 \\ 0 \leq j \leq m-1}} c_{ij} u^i v^j, \; c_{ij} \in \mathbb{F}_2 \tag{2.1}$$

in a unique way where, addition can be done in a natural way coordinate-wise addition and multiplication of any two elements can be defined as

$$xy{=}\sum_{\substack{0\leq r\leq k-1\\ 0\leq s\leq m-1}}\left(\sum_{\substack{i_1+i_2=r\\ j_1+j_2=s}} c_{i_1j_1}d_{i_2j_2}\right)u^rv^s.$$

for any $x=\sum_{\substack{0\leq i_1\leq k-1\\ 0\leq j_1\leq m-1}} c_{i_1j_1}u^{i_1}v^{j_1}$ and $y=\sum_{\substack{0\leq i_2\leq k-1\\ 0\leq j_2\leq m-1}} d_{i_2j_2}u^{i_2}v^{j_2}\in\mathcal{R}_{k,m}$. Note that the sum of indices in the inner sum above is done with respect to modulus k or m where suitable. $\mathcal{R}_{k,m}$ is a finite commutative ring of characteristic 2, of size 2^{km}.

Example 2.1.1. The ring $\mathcal{R}_{4,3}$ has 4096 elements. Let we take the elements $a=1+u^3+uv+u^3v$ and $b=u^3+v+uv+v^2+uv^2\in\mathcal{R}_{4,3}$ then

$$a+b=1+v+u^3v+v^2+uv^2$$

and

$$\begin{aligned} a\times b &= u^3+v+uv+v^2+uv^2+u^6+u^3v+u^4v+u^3v^2+u^4v^2+u^4v+uv^2\\ &+ u^2v^2+uv^3+u^2v^3+u^6v+u^3v^2+u^4v^2+u^3v^3+u^4v^3\\ &= u^3+v+uv+u^3v+v^2. \end{aligned}$$

One of the important structural properties is to characterize the units and non-units in $\mathcal{R}_{k,m}$. The following lemma takes care of this:

Lemma 2.1.2. An element in $\mathcal{R}_{k,m}$ of the form given in (2.1) is a unit if and only if c_{00} is 1.

Proof. Since the characteristic of the ring is 2 and $c^{2^n}=c$ for all $c\in\mathbb{F}_2$ and $n\in\mathbb{Z}_+$, we have

$$\left(\sum_{0\leq i+j\leq k+m-2} c_{ij}u^iv^j\right)^{2^n}=\sum_{0\leq i+j\leq k+m-2} c_{ij}\left(u^iv^j\right)^{2^n}.$$

If we choose n so that $2^n\geq k,m$, then the above sum becomes c_{00}. Thus, if $c_{00}=1$, this will make the element a unit, while when $c_{00}=0$, it will be a zero divisor and hence a non-unit. □

Let us denote by $\mathcal{D}(\mathcal{R}_{k,m})$, the set of non-units of $\mathcal{R}_{k,m}$ while with $\mathcal{U}(\mathcal{R}_{k,m})$ the set of units. For example, the ring $\mathcal{R}_{3,2}$ has 32 units and non-units. We can list all the non-units as:

$$\begin{aligned}\mathcal{D}(\mathcal{R}_{3,2}) &= \{0, u, u^2, u+u^2, v, v+u, v+u^2, v+u+u^2, uv, uv+u, uv+u^2,\\ &\quad uv+u+u^2, uv+v, uv+v+u, uv+v+u^2, uv+v+u+u^2, u^2v,\\ &\quad u^2v+u, u^2v+u^2, u^2v+u+u^2, u^2v+v, u^2v+v+u^2, u^2v+uv,\\ &\quad u^2v+v+u+u^2, u^2v+uv+u, u^2v+uv+u^2, u^2v+uv+u+u^2,\\ &\quad u^2v+uv+v, u^2v+uv+v+u, u^2v+uv+v+u^2, u^2v+uv+v+u+u^2\}.\end{aligned}$$

Clearly $1+x \in \mathcal{U}(\mathcal{R}_{3,2})$ for all $x \in \mathcal{D}(\mathcal{R}_{3,2})$ where $\mathcal{U}(\mathcal{R}_{3,2})$ shows the units of the ring. In $\mathcal{R}_{2,2}$ we have

$$a^2 = \begin{cases} 0, & a \text{ is non-unit,} \\ 1, & a \text{ is unit.} \end{cases}$$

This is not the case in $\mathcal{R}_{k,m}$ in general.

Lemma 2.1.3. The ring $\mathcal{R}_{k,m}$ is a local ring with unique maximal ideal $I_{u,v} = \langle u, v\rangle$. This ideal consists of all non-units and has $|I_{u,v}| = \frac{|\mathcal{R}_{k,m}|}{2}$.

Proof. $I_{u,v} = \{ur_1 + vr_2 | r_1, r_2 \in \mathcal{R}_{k,m}\}$. Clearly, $c_{00} = 0$ for all elements of $I_{u,v}$. So, all non-units are in $I_{u,v}$ from Lemma 2.1.2. Since the number of units and non-units same in $\mathcal{R}_{k,m}$ we have that the cardinality of the ideal $I_{u,v}$ is half the cardinality of ring. □

Note that when $m = 1$ the ring is $\mathcal{R}_{k,1} = \mathbb{F}_2 + u\mathbb{F}_2 + \cdots + u^{k-1}\mathbb{F}_2$. We know the ring $\mathcal{R}_{k,1}$ is a finite chain and principal ideal ring. The maximal ideal $I_{u,v}$ is not generated by a single element, so the ring $\mathcal{R}_{k,m}$ is not a principal ideal ring for $m > 1$. Let us consider ideals $I_u = \langle u\rangle$ and $I_v = \langle v\rangle$ which are contained in $I_{u,v}$ but they are not related via inclusion. That is, the ring is not a chain ring for $m > 1$. Clearly the ideal structure of the ring $\mathcal{R}_{k,m}$ is more complex for large values of k and m, which makes it hard to give a general ideal lattice. However, we would like to do this for the next case of $\mathcal{R}_{3,2}$.

Example 2.1.4. The ring $\mathcal{R}_{3,2}$ has 13 ideals. They are listed as follows:

$\mathcal{R}_{3,2}$=$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

$I_{u,v}$=$u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

$I_{u^2,v}$=$u^2\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

I_u=$u\mathbb{F}_2 + u^2\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

$I_{u^2,uv}$=$u^2\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

I_v=$v\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

I_{u^2}=$u^2\mathbb{F}_2 + u^2v\mathbb{F}_2$,

I_{uv}=$uv\mathbb{F}_2 + u^2v\mathbb{F}_2$,

I_{u^2v}=$u^2v\mathbb{F}_2$,

I_0=$\{0\}$ and

I_{u+v}=$\{0, u^2, uv, u^2 + uv, u^2v, u^2 + u^2v, uv + u^2v, u^2 + uv + u^2v,$

$u + v, u + u^2 + v, u + v + uv, u + u^2 + v + uv, u + v + u^2v, u + u^2 + v + u^2v,$

$u + v + uv + u^2v, u + u^2 + v + uv + u^2v\}$,

I_{u^2+v}=$\{0, uv, u^2v, uv + u^2v, u^2 + v, u^2 + v + uv, u^2 + v + u^2v, u^2 + v + uv + u^2v\}$,

I_{u^2+uv}=$\{0, u^2v, u^2 + uv, u^2 + uv + u^2v\}$,

Accordingly, we show the ideal lattice of the ring $\mathcal{R}_{3,2}$ in Figure 2.3:

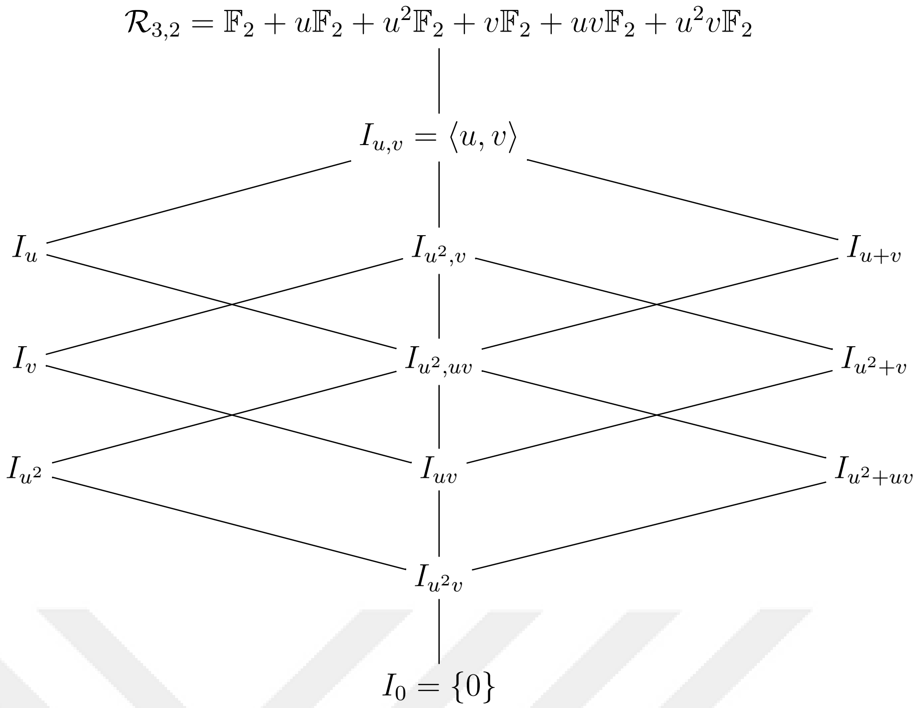
$\mathcal{R}_{3,2} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$
$I_{u,v} = \langle u, v \rangle$
I_u
$I_{u^2,v}$
I_{u+v}
I_v
$I_{u^2,uv}$
I_{u^2+v}
I_{u^2}
I_{uv}
I_{u^2+uv}
I_{u^2v}
$I_0 = \{0\}$

Figure 2.3 The ideal lattice of the ring $\mathcal{R}_{3,2}$.

Theorem 2.1.5. The ring $\mathcal{R}_{k,m}$ is a Frobenius ring.

Proof. Firstly, we give necessary definitions and following result from [Greferath and O'Sullivan, 2004]. For a finite ring R, the Jacobson radical of R which is shown by $Rad(R)$ is the intersection of all maximal left ideals of R. Note that this is the same as the intersection of all maximal right ideals of R. The left socle of R is the sum of all minimal left ideals of R and will be denoted by $soc({}_RR)$. Accordingly the right socle $soc(R_R)$ is defined as the sum of all minimal right ideals of R. Note that the left and right socles of a finite ring are two-sided ideals, which do not necessarily coincide. A finite ring is called a Frobenius ring if it satisfies any(and hence all) of the following equivalent statements for a finite ring R:

1. $R/Rad(R)$ is isomorphic to $soc({}_RR)$ as left R -modules.

2. $R/Rad(R)$ is isomorphic to $soc(R_R)$ as right R -modules.

3. $soc({}_RR)$ is left principal.

4. $soc(R_R)$ is right principal.

5. $\hat{R}$ and R are isomorphic as left R -modules.

6. $\hat{R}$ and R are isomorphic as right R -modules.

Note that $\hat{R}$ is character group of R. Since $\mathcal{R}_{k,m}$ has just one maximal ideal and just one minimal ideal $Rad(\mathcal{R}_{k,m}) = I_{u,v}$ and $Soc(\mathcal{R}_{k,m}) = I_{u^{k-1}v^{m-1}}$. Hence, one can also observe that $\mathcal{R}_{k,m}/Rad(\mathcal{R}_{k,m}) \simeq Soc(\mathcal{R}_{k,m})$. □

2.2 LINEAR CODES OVER $\mathcal{R}_{k,m}$

A linear code C of length n over $\mathcal{R}_{k,m}$ is defined in the usual terms as an $\mathcal{R}_{k,m}$-submodule of $\mathcal{R}_{k,m}^n$. Define the standard Euclidean inner product on $\mathcal{R}_{k,m}$, that is for $a = (a_1, a_2, \ldots a_n)$ and $b = (b_1, b_2, \ldots b_n) \in \mathcal{R}_{k,m}^n$, let

$$\langle a, b\rangle = \sum_{i=1}^{n} a_i b_i.$$

where the operations are performed in the ring $\mathcal{R}_{k,m}$. The duality for codes over $\mathcal{R}_{k,m}$ can then be defined naturally:

Definition 2.2.1. Let C be a linear code over $\mathcal{R}_{k,m}$ of length n, then we define the dual of C as

$$C^{\perp} := \left\{\overline{b} \in \mathcal{R}_{k,m}^n \mid \left\langle \overline{b}, \overline{a}\right\rangle = 0, \forall \overline{a} \in C\right\}.$$

Definition 2.2.2. Let C be a linear code over $\mathcal{R}_{k,m}$ of length n. C is said to be self-orthogonal if $C \subseteq C^{\perp}$, self-dual if $C = C^{\perp}$, isodual if C is equivalent to $C^{\perp}$.

Since $\mathcal{R}_{k,m}$ is a Frobenius ring, by the results in (Wood, 1999), we have the following lemma:

Lemma 2.2.3. Any linear code C over $\mathcal{R}_{k,m}^n$ satisfies $|C| . \left|C^{\perp}\right| = |\mathcal{R}_{k,m}|^n$

2.3 THE LEE WEIGHT AND THE GRAY MAP ON $\mathcal{R}_{k,m}$

In (Dougherty et al., 1999) Lee weight was defined for $\mathbb{F}_2 + u\mathbb{F}_2$ as $\omega(0) = 0$, $\omega(1) = \omega(1+u) = 1$, $\omega(u) = 2$ and a distance preserving Gray map from $(\mathbb{F}_2 + u\mathbb{F}_2)^n$

to $(\mathbb{F}_2)^n$ was defined by $\bar{a}+\bar{b}u \mapsto (\bar{a}+\bar{b},\bar{b})$. Later, in (Yildiz and Karadeniz, 2010a), the Gray map for $\mathbb{F}_2+u\mathbb{F}_2$ was generalized to $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ as

$$\begin{array}{llll} \varphi: & (\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2)^n & \to & (\mathbb{F}_2)^{4n} \\ & a+bu+cv+duv & \to & (a+b+c+d, c+d, b+d, d). \end{array} \tag{2.2}$$

Then the Lee weight was defined for any element $a+bu+cv+duv \in F_2 + u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ by $\omega_L(a+bu+cv+duv) = \omega_H(a+b+c+d, b+d, c+d, d)$ to preserve distance. Note that these maps also preserve duality besides distance. The aim of this section is to define a Lee weight for codes over the ring $\mathcal{R}_{k,m}$ and a corresponding Gray map that is distance preserving and more importantly (to study self-dual codes over $\mathcal{R}_{k,m}$) duality-preserving. In doing so, we will first define these concepts on $\mathcal{R}_{k,1}$ and then inductively extend them over to $\mathcal{R}_{k,m}$.

We define the following linear map which takes a linear code over $\mathcal{R}_{k,1}$ of length n to a binary linear code of length kn.

Definition 2.3.1. Take an element $\overline{a} = \overline{a}_0 + \overline{a}_1 u + \overline{a}_2 u^2 + \cdots + \overline{a}_{k-2}u^{k-2} + \overline{a}_{k-1}u^{k-1}$ of $(\mathcal{R}_{k,1})^n$, where $\overline{a}_i \in \mathbb{F}_2^n$. Then define the Gray map ϕ_{k1} from $(\mathcal{R}_{k,1})^n$ to $(\mathbb{F}_2)^{kn}$ as follows: when k is even let

$$\begin{aligned} \phi_{k1}(\overline{a}) = \; & (\overline{a}_0 + \overline{a}_1 + \cdots + \overline{a}_{k-2} + \overline{a}_{k-1}, \overline{a}_1 + \cdots + \overline{a}_{k-2} + \overline{a}_{k-1}, \\ & \overline{a}_1 + \cdots + \overline{a}_{k-2}, \cdots, \overline{a}_{\frac{k}{2}-1} + \overline{a}_{\frac{k}{2}} + \overline{a}_{\frac{k}{2}+1}, \overline{a}_{\frac{k}{2}-1} + \overline{a}_{\frac{k}{2}}, \overline{a}_{\frac{k}{2}}), \end{aligned}$$

and when k is odd let

$$\begin{aligned} \phi_{k1}(\overline{a}) = \; & (\overline{a}_0 + \overline{a}_1 + \cdots + \overline{a}_{k-2} + \overline{a}_{k-1}, \overline{a}_1 + \cdots + \overline{a}_{k-2} + \overline{a}_{k-1}, \\ & \overline{a}_1 + \cdots + \overline{a}_{k-2}, \cdots, \overline{a}_{\frac{k-3}{2}} + \overline{a}_{\frac{k-1}{2}} + \overline{a}_{\frac{k+1}{2}}, \overline{a}_{\frac{k-1}{2}} + \overline{a}_{\frac{k+1}{2}}, \overline{a}_{\frac{k-1}{2}}). \end{aligned}$$

To preserve distance, we define the Lee weight of an element $a = a_0 + a_1 u + \cdots + a_{k-1}u^{k-1}$ of $\mathcal{R}_{k,1}$ as $w_L(a) = w_H(\phi_{k1}(a))$ where w_H denotes the usual Hamming weight.

With these definitions, it is obvious that ϕ_{k1} is a distance preserving linear isometry from $\mathcal{R}_{k,1}^n$ with the Lee distance to $\mathbb{F}_2^{kn}$ with the Hamming distance. As pointed out earlier, we also want the map to preserve duality, which is proven in the next theorem:

Theorem 2.3.2. The Gray image of a self-dual code of length n over $\mathcal{R}_{k,1}$ is a binary self-dual code of length kn.

Proof. First, we prove that Gray images of orthogonal codewords in $\mathcal{R}_{k,1}$ are orthogonal in $\mathbb{F}_2$. That is, we shall show that

$$\langle \overline{a}, \overline{b} \rangle = 0 \Rightarrow \phi_{k1}(\overline{a}).\phi_{k1}(\overline{b}) = 0$$

for all $\overline{a}, \overline{b} \in \mathcal{R}_{k,1}^n$. Let us assume that $\overline{a} = \sum_{i=0}^{k-1} \overline{a}_i u^i$ and $\overline{b} = \sum_{j=0}^{k-1} \overline{b}_j u^j$. Then we see that

$$\langle \overline{a}, \overline{b} \rangle = 0 \Leftrightarrow \sum_{i=0}^{k-1} \overline{a}_i u^i . \sum_{j=0}^{k-1} \overline{b}_j u^j = 0 \Leftrightarrow \sum_{i+j=0}^{k-1} \overline{a}_i \overline{b}_j = 0. \tag{2.3}$$

Now, since

$$\begin{aligned} \phi_{k1}(\overline{a}\ ) &= (\sum_{i=0}^{k-1} \overline{a}_i\ , \sum_{i=1}^{k-1} \overline{a}_i\ , \sum_{i=1}^{k-2} \overline{a}_i\ , \cdots\ , \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}+1} \overline{a}_i\ , \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}} \overline{a}_i\ , \sum_{i=\frac{k}{2}}^{\frac{k}{2}} \overline{a}_i\ ), \\ \phi_{k1}(\overline{b}\ ) &= (\sum_{i=0}^{k-1} \overline{b}_i\ , \sum_{i=1}^{k-1} \overline{b}_i\ , \sum_{i=1}^{k-2} \overline{b}_i\ , \cdots\ , \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}+1} \overline{b}_i\ , \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}} \overline{b}_i\ , \sum_{i=\frac{k}{2}}^{\frac{k}{2}} \overline{b}_i\ ) \end{aligned}$$

we get, after some cancellations because of the characteristic being 2,

$$\begin{aligned} \phi_{k1}(\overline{a}).\phi_{k1}(\overline{b}) \quad &= \sum_{i=0}^{k-1} \overline{a}_i \sum_{i=0}^{k-1} \overline{b}_i + \sum_{i=1}^{k-1} \overline{a}_i \sum_{i=1}^{k-1} \overline{b}_i + \cdots \\ &+ \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}} \overline{a}_i \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}} \overline{b}_i + \sum_{i=\frac{k}{2}}^{\frac{k}{2}} \overline{a}_i \sum_{i=\frac{k}{2}}^{\frac{k}{2}} \overline{b}_i \\ &= \overline{a}_0 \sum_{i=0}^{k-1} \overline{b}_i + \overline{b}_0 \sum_{i=1}^{k-1} \overline{a}_i + \overline{a}_1 \sum_{i=1}^{k-2} \overline{b}_i + \overline{b}_1 \sum_{i=2}^{k-2} \overline{a}_i + \cdots \\ &+ \overline{a}_{\frac{k}{2}-1} \sum_{i=\frac{k}{2}-1}^{\frac{k}{2}} \overline{b}_i + \overline{b}_{\frac{k}{2}-1} \sum_{i=\frac{k}{2}}^{\frac{k}{2}} \overline{a}_i. \end{aligned}$$

One can see that this last sum is exactly equal to the right-most sum in (2.3) which is equal to 0. This shows us

$$\phi_{k1}(C^{\perp}) \subset \phi_{k1}(C)^{\perp}. \tag{2.4}$$

But, by the definition of ϕ_{k1}, $\phi_{k1}(C)$ is a binary linear code of length kn of size $|C|$. Both $\mathbb{F}_2$ and $\mathcal{R}_{k,1}$ are Frobenius, so we have

$$\left|\phi_{k1}(C^{\perp})\right| = \left|C^{\perp}\right| = \frac{\left|\mathcal{R}_{k,1}\right|^n}{|C|} = \frac{2^{kn}}{|\phi_{k1}(C)|} = \left|\phi_{k1}(C)^{\perp}\right|.$$

Combining this with (2.4), we get

$$\phi_{k1}(C^{\perp}) = \phi_{k1}(C)^{\perp}. \tag{2.5}$$

□

Because of the distance-preserving property of the Gray map we get the following important corollary:

Corollary 2.3.3. *Let C be a self-dual code over $\mathcal{R}_{k,1}$ of length n. Then $\phi_{k1}(C)$ is a binary self-dual code of length kn. Moreover the Lee weight distribution of C is the same as the Hamming weight distribution of $\phi_{k1}(C)$.*

Now since $\mathcal{R}_{k,m}$ can be viewed as an $\mathcal{R}_{k,1}-$vector space with a basis

$$\{1, v, v^2, \dots, v^{m-1}\},$$

we can write any element of $\mathcal{R}_{k,m}$ in the form $c = \sum\limits_{0 \leq i \leq m-1} c_{ki} v^i$, where $c_{ki} \in \mathcal{R}_{k,1}$. Now we can extend the Gray map easily from $\mathcal{R}_{k,1}$ to $\mathcal{R}_{k,m}$:

$$\begin{aligned} \phi_{km}(c) = \ & (\phi_{k1}(\sum_{i=0}^{m-1} \overline{c}_{ki}), \phi_{k1}(\sum_{i=1}^{m-1} \overline{c}_{ki}), \phi_{k1}(\sum_{i=1}^{m-2} \overline{c}_{ki}), \\ & \cdots, \phi_{k1}(\sum_{i=\frac{m}{2}-1}^{\frac{m}{2}+1} \overline{c}_{ki}), \phi_{k1}(\sum_{i=\frac{m}{2}-1}^{\frac{m}{2}} \overline{c}_{ki}), \phi_{k1}(\sum_{i=\frac{m}{2}}^{\frac{m}{2}} \overline{c}_{ki})). \end{aligned}$$

We note that, defining the Lee weight in the same way as the Hamming weight of the image, distance and duality-preserving properties of ϕ_{km} can be established in exactly the same way as was done for ϕ_{k1}. Thus we can extend Corollary 2.3.3 to the following important theorem which will be used in subsequent chapters:

Theorem 2.3.4. *Let C be a self-dual code over $\mathcal{R}_{k,m}$ of length n. Then $\phi_{km}(C)$ is a binary self-dual code of length kmn. Moreover the Lee weight distribution of C is the same as the Hamming weight distribution of $\phi_{km}(C)$.*

Example 2.3.5. Keeping in mind that the Gray maps ϕ_{22} and ϕ_{21} are exactly same with the Gray maps that are found before in (Dougherty et al., 1999), (Yildiz and Karadeniz, 2010a) for $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, we give as examples the Gray maps ϕ_{31} and ϕ_{32}.

$$\phi_{31}(c_1) \ = \ (c_{00} + c_{10} + c_{20}, c_{10} + c_{20}, c_{10})$$

for any element $c_1 \in \mathcal{R}_{3,1}$. Hence, we can represent all elements of $\mathcal{R}_{3,1}$ by elements of $\mathbb{F}_2^3$ as following:

$$\begin{aligned}
\phi_{31}(0) &= (000) \\
\phi_{31}(1) &= (100) \\
\phi_{31}(u) &= (111) \\
\phi_{31}(1+u) &= (011) \\
\phi_{31}(u^2) &= (110) \\
\phi_{31}(1+u^2) &= (010) \\
\phi_{31}(u+u^2) &= (001) \\
\phi_{31}(1+u+u^2) &= (101)
\end{aligned}$$

Now, we can define the Gray map ϕ_{32} for any element $c_2 = c_{00} + c_{10}u + c_{20}u^2 + c_{01}v + c_{11}uv + c_{21}u^2v \in \mathcal{R}_{3,2}$. Firstly, we rewrite the elements of $\mathcal{R}_{3,2}$ in the form $c_2 = a + bv$ where $a = c_{00} + c_{10}u + c_{20}u^2, b = c_{01} + c_{11}u + c_{21}u^2 \in \mathcal{R}_{3,1}$. Because of ϕ_{21} and ϕ_{31},

$$\begin{aligned}
\phi_{32}(c_2) &= (\phi_{31}(a+b), \phi_{31}(b)) \\
&= (\phi_{31}(c_{00} + c_{10}u + c_{20}u^2 + c_{01} + c_{11}u + c_{21}), \phi_{31}(c_{00} + c_{10}u + c_{20}u^2)) \\
&= (\phi_{31}(c_{00} + c_{01} + (c_{10} + c_{11})u + (c_{20} + c_{21})u^2), \phi_{31}(c_{00} + c_{10}u + c_{20}u^2)) \\
&= (c_{00} + c_{01} + c_{10} + c_{11} + c_{20} + c_{21}, c_{10} + c_{11} + c_{20} + c_{21}, \\
&\quad c_{10} + c_{11}, c_{00} + c_{10} + c_{20}, c_{10} + c_{20}, c_{10})
\end{aligned}$$

Accordingly, $\mathcal{R}_{3,2}$ has an element of weight 0, 5 elements of weight 1, 16 elements of weight 2, 20 elements of weight 3, 15 elements of weight 4, 6 elements of weight 5 and just one element of weight 6, as shown in following table:

Table 2.1 Lee weights of elements of $\mathcal{R}_{3,2}$.

elements of $\mathcal{R}_{3,2}$	ω_L	elements of $\mathcal{R}_{3,2}$	ω_L
0	0	u^2v	4
1	1	$1+u^2v$	3
u	3	$u+u^2v$	2
$1+u$	2	$1+u+u^2v$	4
u^2	2	u^2+u^2v	2
$1+u^2$	1	$1+u^2+u^2v$	3
$u+u^2$	1	$u+u^2+u^2v$	5
$1+u+u^2$	2	$1+u+u^2+u^2v$	4
v	2	$v+u^2v$	2
$1+v$	1	$1+v+u^2v$	3
$u+v$	3	$u+v+u^2v$	3
$1+u+v$	4	$1+u+v+u^2v$	2
u^2+v	2	u^2+v+u^2v	2
$1+u^2+v$	3	$1+u^2+u^2v$	3
$u+u^2+v$	3	$u+u^2+v+u^2v$	3
$1+u+u^2+v$	2	$1+u+u^2+v+u^2v$	4
uv	6	$uv+u^2v$	2
$1+uv$	5	$1+uv+u^2v$	3
$u+uv$	3	$u+uv+u^2v$	3
$1+u+uv$	4	$1+u+uv+u^2v$	2
u^2+uv	4	u^2+uv+u^2v	4
$1+u^2+uv$	5	$1+u^2+uv+u^2v$	3
$u+u^2+uv$	5	$u+u^2+uv+u^2v$	1
$1+u+u^2+uv$	4	$1+u+u^2+uv+u^2v$	2
$v+uv$	4	$v+uv+u^2v$	4
$1+v+uv$	5	$1+v+uv+u^2v$	3
$u+v+uv$	3	$u+v+uv+u^2v$	3
$1+u+v+uv$	2	$1+u+v+uv+u^2v$	4
u^2+v+uv	4	$u^2+v+uv+u^2v$	4
$1+u^2+v+uv$	3	$1+u^2+v+uv+u^2v$	5
$u+u^2+v+uv$	3	$u+u^2+v+uv+u^2v$	3
$1+u+u^2+v+uv$	4	$1+u+u^2+v+uv+u^2v$	2

2.4 MACWILLIAMS IDENTITIES FOR CODES OVER $\mathcal{R}_{k,m}$

The weight enumerator of a linear code C shows the number of codewords in C that have each possible weight. MacWilliams identities specify weight enumerators of dual of a code respect to weight enumerator of the code. By Jay Wood's result (Wood, 1999), MacWilliams identities hold for codes over all Frobenius rings. Since $\mathcal{R}_{k,m}$ is a Frobenius ring it has a generating character and using this we can prove MacWilliams identities for the complete weight enumerator, the Hamming weight enumerator and the Lee weight enumerator of codes over $\mathcal{R}_{k,m}$.

We first give a generating character for the additive group of $\mathcal{R}_{k,m}$. A character of a group G is defined as a group homomorphism from G to complex numbers. Let

$$\begin{array}{rccc} \chi: & (\mathcal{R}_{k,m},+) & \rightarrow & (\{-1,1\},.) \\ & \sum\limits_{\substack{0\leq i\leq k-1\\ 0\leq j\leq m-1}} c_{ij}u^iv^j & \mapsto & (-1)^{w_H(c)} \end{array},$$

where $c=(c_{ij})$ is the vector consisting of all the coefficients c_{ij}'s. Note that, for $a=\sum\limits_{\substack{0\leq i\leq k-1\\ 0\leq j\leq m-1}} c_{ij}u^iv^j$, $b=\sum\limits_{\substack{0\leq r\leq k-1\\ 0\leq s\leq m-1}} d_{rs}u^rv^s\in\mathcal{R}_{k,m}$, we have

$$\chi(a+b) \quad = \quad (-1)^{w_H(c+d)} \quad = \quad (-1)^{w_H(c)}.(-1)^{w_H(d)} \quad = \quad \chi(a).\chi(b),$$

where $d=(d_{rs})$ is the vector consisting of all the coefficients d_{rs}'s. Thus χ is a character.

Theorem 2.4.1. χ is a generating character for $\mathcal{R}_{k,m}$.

Proof. Since $\chi(0)=1$ and $\chi(u^{k-1}v^{m-1})=-1$, χ is non-trivial when restricted to the minimal ideal. Since every non-zero ideal contains the minimal ideal, χ is non-trivial when restricted to any non-zero ideal, showing that χ is a generating character. □

Example 2.4.2. The ring $\mathcal{R}_{4,1}$ has 16 elements. Character values of these elements can easily be observed as follows:

$$\begin{array}{llll}
\chi(0)=1 & \chi(u^2)=-1 & \chi(u^3)=-1 & \chi(u^2+u^3)=1 \\
\chi(1)=-1 & \chi(1+u^2)=1 & \chi(1+u^3)=1 & \chi(1+u^2+u^3)=-1 \\
\chi(u)=-1 & \chi(u+u^2)=1 & \chi(u+u^3)=1 & \chi(u+u^2+u^3)=-1 \\
\chi(1+u)=1 & \chi(1+u+u^2)=-1 & \chi(1+u+u^3)=-1 & \chi(1+u+u^2+u^3)=1.
\end{array}$$

Let $\mathcal{R}_{k,m} = \{g_1, g_2, \ldots, g_{2^{km}}\}$ be a labeling of the elements of the ring. The complete weight enumerator of a code C over $\mathcal{R}_{k,m}^n$ is

$$CWE_C(\overline{X}) = \sum_{\overline{c}\in C} \prod_{i=1}^{2^{km}} X_i^{n_i(\overline{c})},$$

where $\overline{X} = (X_1, X_2, \ldots, X_{2^{km}})$ and $n_i(\overline{c})$ is the number of occurrences of g_i in $\overline{c}$. Let T be the $2^{km} \times 2^{km}$ matrix such that

$$T = \begin{pmatrix} \chi(g_1g_1) & \chi(g_1g_2) & \cdots & \chi(g_1g_{2^{km}}) \\ \chi(g_2g_1) & \ddots & & \chi(g_1g_{2^{km}}) \\ \vdots & & \ddots & \vdots \\ \chi(g_{2^{km}}g_1) & \chi(g_{2^{km}}g_2) & \cdots & \chi(g_{2^{km}}g_{2^{km}}) \end{pmatrix}.$$

Then we have following theorems by (Wood, 1999):

Theorem 2.4.3. Let C be linear code over $\mathcal{R}_{k,m}$ and $C^{\perp}$ be its dual. Then we have the following identity for the complete weight enumerators:

$$CWE_{C^{\perp}}(\overline{X}) = \tfrac{1}{|C|} CWE_C(T.\overline{X}^t).$$

Here, $\overline{X}^t$ denotes the transpose of $\overline{X}$.

Putting $X_1 = x$ and $X_i = y$ for all $i \geq 2$, we obtain the MacWilliams identity for the Hamming weight enumerator:

Theorem 2.4.4.

$$HWE_{C^{\perp}}(x, y) = \tfrac{1}{|C|} HWE_C(x + (|\mathcal{R}_{k,m}| - 1)y, x - y),$$

where $HWE_C(x, y)$ is the Hamming weight enumerator of a code C over $\mathcal{R}_{k,m}^n$ given as a homogeneous polynomial as,

$$HWE_C(x, y) = \sum_{c\in C} x^{n - w_H(c)} y^{w_H(c)}.$$

Now, our goal is to describe MacWilliams identities for the Lee weight enumerators of codes over $\mathcal{R}_{k,m}$. Firstly, we define Lee weight enumerator of a code C over $\mathcal{R}_{k,m}^n$ as usual to be

$$LWE_C(z) = \sum_{\overline{c}\in C} z^{w_L(\overline{c})}$$

where $w_L(\overline{c})$ denotes the Lee weight of a codeword. Then we have the following theorem:

Theorem 2.4.5. Let C be a linear code over $\mathcal{R}_{k,m}$ of length n then

$$LWE_{C^{\perp}}(z)=\frac{1}{|C|}(1+z)^{kmn}LWE_{C}\left(\frac{1-z}{1+z}\right).$$

Proof. As we know ϕ_{km} is a distance preserving map. Therefore

$$LWE_{C^{\perp}}(z)=HWE_{\phi_{km}(C^{\perp})}(z),$$

where $HWE_C(z)$ denotes the Hamming weight enumerator of a code C. Recall that we have $\phi_{km}(C^{\perp})=\phi_{km}(C)^{\perp}$ by Theorem 2.5. So we get

$$\begin{aligned} LWE_{C^{\perp}}(z) &= HWE_{\phi_{km}(C)^{\perp}}(z)\\ &= \tfrac{1}{|\phi_{km}(C)|}(1+z)^{kmn}HWE_{\phi_{km}(C)}\left(\tfrac{1-z}{1+z}\right)\\ &= \tfrac{1}{|C|}(1+z)^{kmn}LWE_{C}\left(\tfrac{1-z}{1+z}\right), \end{aligned}$$

by the usual MacWilliams identities of binary codes. □

Example 2.4.6. Let us consider a linear code C over $\mathcal{R}_{3,2}$ of length 7, with the following generator matrix:

$$\begin{bmatrix} 0 & u^2 & u^2v & u^2v+uv & u^2v+uv & 0 & u^2\\ u^2 & 0 & u^2 & u^2v & u^2v+uv & u^2v+uv & 0\\ 0 & u^2 & 0 & u^2 & u^2v & u^2v+uv & u^2v+uv\\ uv & 0 & u^2 & 0 & u^2 & u^2v & u^2v+uv\\ uv & uv & 0 & u^2 & 0 & u^2 & u^2v\\ u^2v & uv & uv & 0 & u^2 & 0 & u^2\\ u^2 & u^2v & uv & uv & 0 & u^2 & 0 \end{bmatrix}.$$

The Gray image of this code under ϕ_{32} is a binary linear code of parameters $[42,12,8]$ and the weight distribution of the code and its dual can be obtained by MAGMA as following:

$$\begin{aligned} HWE_{\phi_{32}(C)}(z) = \quad & 1+35z^{8}+196z^{12}+763z^{16}+1414z^{20}+1197z^{24}+392z^{28}\\ & +84z^{32}+14z^{36} \end{aligned}$$

$$HWE_{\phi_{32}(C^{\perp})}(z) = \quad 1+21z^{2}+322z^{4}+3682z^{6}+3968z^{7}+36897z^{8}+\cdots$$

Clearly, the code $\phi_{32}(C^{\perp})$ is also a binary linear code of parameters $[42,30,2]$.

CHAPTER 3

SELF-DUAL CODES OVER $\mathcal{R}_{k,m}$

As we defined in the previous chapter, a linear code C over $\mathcal{R}_{k,m}$ is self orthogonal if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$. Moreover, while the dimension of a self orthogonal code of length n is at most $n/2$, the dimension of a self-dual code of length n has to be $n/2$. Useful structure of self-dual codes, make them closely connected to many research areas such as lattices, designs and information theory. Therefore, many researchers make an effort to construct good binary self-dual codes of different automorphism groups and new weight enumerators. The article (Huffman, 2005) is a survey of self-dual linear codes over the fields $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_4$ and the rings $\mathbb{Z}_4$, $\mathbb{F}_2 + u\mathbb{F}_2$, and $\mathbb{F}_2 + v\mathbb{F}_2$.

There exist some methods used to obtain self-dual codes, such as circulant constructions, Hadamard matrices, automorphism groups and extensions. We have the following upper bounds on the minimum Hamming distance for binary self-dual codes :

Theorem 3.0.1. (Conway and Sloane, 1990) Let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type I and Type II binary code of length n, respectively. Then

$$d_{II}(n) \leq 4\lfloor \frac{n}{24} \rfloor + 4$$

and

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

Self-dual codes meeting these bounds are called *extremal*. In this chapter, we construct binary self-dual codes as the Gray images of self-dual codes over $\mathcal{R}_{k,m}$ by lifts, different circulant constructions and extensions.

3.1 PROJECTIONS AND LIFTS

Recall that elements of $\mathcal{R}_{k,m}$ can be represented in the form $\sum\limits_{\substack{0\leq i\leq k-1\\0\leq j\leq m-1}} c_{ij}u^iv^j$. Now define a projection from $\mathcal{R}_{k,m}$ to $\mathbb{F}_2$.

Definition 3.1.1. Let μ be a map from $\mathcal{R}_{k,m}$ to $\mathbb{F}_2$ such that

$$\mu(\sum_{\substack{0\leq i\leq k-1\\0\leq j\leq m-1}} c_{ij}u^iv^j) = c_{00} \tag{3.1}$$

Clearly μ is an epimorphism and it is called a natural projection of $\mathcal{R}_{k,m}$ to $\mathbb{F}_2$.

Consider the projections

$$\begin{aligned} \pi_v &: R_{k,m} \to R_{k,1} \text{ defined by } v \mapsto 0,\\ \pi_u &: R_{k,1} \to \mathbb{F}_2 \text{ defined by } u \mapsto 0, \end{aligned}$$

then clearly $\pi_u \circ \pi_v$ is the projection μ.

Let C be a linear code over $\mathcal{R}_{k,m}$ and $\mu(C)$ be its projection. Then C is said to be a lift of $\mu(C)$. Our general strategy in constructing self-dual codes over $\mathcal{R}_{k,m}$ will be to lift from good binary self-dual codes. Now notice that if for $\overline{x}, \overline{y} \in \mathcal{R}_{k,m}^n$, we have $\langle \overline{x}, \overline{y}\rangle = 0$, then $x_{00} \cdot y_{00} = \mu(\overline{x}) \cdot \mu(\overline{y}) = 0$. Thus we have the following result:

Theorem 3.1.2. *Let C be a self-dual code over $\mathcal{R}_{k,m}$ of length n. Then $\mu(C)$ is a self orthogonal code over $\mathbb{F}_2$ of length n.*

Corollary 3.1.3. *If C is a free self-dual code over $\mathcal{R}_{k,m}$ of length $2n$, that is if C is generated by a matrix of the form $[I_n|A]$, then $\mu(C)$ is a binary self-dual code of length $2n$.*

The following theorem gives a bound between the minimum Lee weight of a code and the minimum Hamming weight of its projection:

Theorem 3.1.4. *Let C be a linear code over $\mathcal{R}_{k,m}$ of length n with minimum Lee weight d and $\mu(C)$ be its projection to $\mathbb{F}_2$. If d' denotes the minimum Hamming weight of $\mu(C)$, we have $d \leq 2md'$.*

Proof. Let $\overline{x}_{00} \in \mu(C)$ with $w_H(\overline{x}_{00}) = d'$. Then there exists

$$c = \overline{x}_{00} + \sum_{1\leq i+j\leq k+m-2} \overline{x}_{ij}u^iv^j \in C.$$

But then $(u^{k-1}v^{m-1})c = \overline{x_{00}}u^{k-1}v^{m-1} \in C$, because C is linear code over $\mathcal{R}_{k,m}$. Now,

$$w_L(\overline{x}_{00}u^{k-1}v^{m-1}) = w_H(\underbrace{\overline{x}_{00},\overline{x}_{00},\overline{00},\overline{x}_{00},\overline{x}_{00},\overline{00},\cdots,\overline{x}_{00},\overline{x}_{00},\overline{00}}_{m\ \text{times}\ \overline{x}_{00},\overline{x}_{00},\overline{00}})$$

where $\overline{00} = \underbrace{\overline{0},\cdots,\overline{0}}_{k-2\ \text{times}}$. That is, $w_L(u^{k-1}v^{m-1}\overline{x}_{00}) = 2md'$. This proves the theorem.

□

3.2 DOUBLE CIRCULANT,BORDERED DOUBLE CIRCULANT AND FOUR CIRCULANT CONSTRUCTIONS

In (MacWilliams and Sloane, 1978), two construction methods are described using circulant matrices. The double circulant and the bordered double circulant constructions have been used quite successfully by many researchers to obtain good self-dual binary codes. We can easily adopt these constructions over $\mathcal{R}_{k,m}$:

Definition 3.2.1. Let M be a circulant matrix over $\mathcal{R}_{k,m}$ of order n. Then the matrix $[I_n \mid M]$ generates codes over $\mathcal{R}_{k,m}$ of length $2n$. This is called the pure double circulant or double circulant construction.

Definition 3.2.2. Let M be a circulant matrix over $\mathcal{R}_{k,m}$ of order $n-1$. Then the matrix

$$\left[\begin{array}{c|cccc} & x & y & \cdots & y \\ & z & & & \\ I_n & \vdots & & M & \\ & z & & & \end{array}\right] \tag{3.2}$$

where $x, y, z \in \mathcal{R}_{k,m}$ generates codes over $\mathcal{R}_{k,m}$ of length $2n$. This is called bordered double circulant construction.

A modification on these constructions was introduced later. This construction, which is called four circulant construction in literature, was given first time in (Betsumiya et al., 2003) for self-dual codes over $\mathbb{F}_p$. In (Georgiou and Lappas, 2012) it was called as two-block circulant construction. In (Karadeniz et al., 2014b) this construction was applied to the ring $\mathbb{F}_2 + u\mathbb{F}_2$ to obtain extremal binary self-dual codes. Then following theorem can be proven in the exact same way as was done in (Karadeniz et al., 2014b):

Theorem 3.2.3. Let A and B be circulant matrices over $\mathcal{R}_{k,m}$ of length n such that $AA^t + BB^t = I_n$. Then the matrix

$$\left[I_{2n} \left| \begin{array}{cc} A & B \\ B^t & A^t \end{array} \right. \right] \tag{3.3}$$

generates self-dual codes over $\mathcal{R}_{k,m}$ of length $4n$. This is called four circulant construction.

Now, we can give binary self-dual codes of some lengths obtained from self-dual codes over $\mathcal{R}_{k,m}$ by the three circulant constructions mentioned above.

3.2.1 The General idea

The projection μ, which is defined above preserves orthogonality. Also the image of a double circulant self-dual code over $R_{k,m}$ of length n under μ must be a double circulant binary self-dual code, the image of a bordered-double circulant self-dual code over $R_{k,m}$ of length n under μ has to be a bordered-double circulant binary self-dual code and the same is true for four circulant codes as well.

So, if we want to obtain a good self-dual code over $\mathcal{R}_{k,m}$ by one of the construction methods above, we look at the projection and look for the best binary self-dual codes of the same length obtained from the same constructions. We then lift these codes over the ring $\mathcal{R}_{k,m}$ by lifting 1 to a unit in $\mathcal{R}_{k,m}$ and 0 to a non-unit in $\mathcal{R}_{k,m}$. Theorem 3.1.4 tells us exactly which binary codes to lift. Then an exhaustive search using a computer algebra reveals all the self-dual codes over $\mathcal{R}_{k,m}$ that can be obtained through these constructions. We then choose the best ones and take the Gray images to obtain good binary self-dual codes. In what follows we apply this idea to certain lengths and certain rings of the form $\mathcal{R}_{k,m}$. We only list the ones through which we have obtained extremal or near extremal binary self-dual codes. The existence of the Type II extremal code of length 72 is still an open problem. So the best known binary self-dual codes of length 72 for both Type I and Type II have parameters $[72, 36, 12]$.

3.2.2 The extended binary Golay code

The binary Golay code is probably the most well known code in the literature. It is a perfect 3-error correcting code of parameters $[23, 12, 7]$. When we extend this code by a parity check symbol we obtain the Type II extremal self-dual code of parameters $[24, 12, 8]$. This code is unique up to equivalence and is the first example of the theoretically good self-dual codes of length $24k$. Using Assmus-Mattson theorem, it also leads 5 designs with parameters $(24, 8, 1)$ and $(24, 12, 8)$. There have been many different constructions for this code in the literature. (McLoughlin and Hurley, 2008), (Peng and Farrell, 2006) are examples of these constructions. In (Karadeniz and Yildiz, 2014), the extended Golay code was constructed from what we now call $\mathcal{R}_{2,2}$.

We have been able to give a construction for the extended Golay code using bordered double circulant construction over $\mathcal{R}_{3,1}$ and $\mathcal{R}_{3,2}$. Note that because of the Gray map, these are the only ones we can use (other than $\mathcal{R}_{2,1}$ and $\mathcal{R}_{2,2}$, which have already been used before). To construct it from $\mathcal{R}_{3,1}$, we need the binary code to lift to be of parameters $[8, 4, 4]$ which is also unique. Using all possible lifts of the bordered double circulant matrix that generates the $[8, 4, 4]$-code, we were able to obtain the Golay code from $\mathcal{R}_{3,1}$ quite easily. The following matrix turns out to generate the self-dual code over $\mathcal{R}_{3,1}$ whose binary image is the extended Golay code:

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

Doing the same thing over bordered double circulant binary codes of length 4, which narrowed the search field rather considerably, we see that the following matrix generates the self-dual code over $\mathcal{R}_{3,2}$ whose binary image is the extended Golay code:

$$M' = \begin{bmatrix} 1 & 0 & u+v & 1+u+v \\ 0 & 1 & 1+u+u^2+v+uv & u+v \end{bmatrix}.$$

3.2.3 Extremal Self-Dual Codes of Length 36

Melchor and Gaborit have classified all the 41 extremal binary $[36, 18, 8]$ self-dual codes in (Melchor and Gaborit, 2008). We have obtained some of these through $\mathcal{R}_{3,1}$ and $\mathcal{R}_{3,2}$ using some of the aforementioned constructions. To be precise, we found 6 of the 41 extremal self-dual codes from the constructions mentioned above. Now, since the four circulant codes have to be of length divisible by 4, the four circulant construction was applied only to the case of $\mathcal{R}_{3,1}$, whereas the double circulant and the bordered double circulant constructions were applied to both $\mathcal{R}_{3,1}$ and $\mathcal{R}_{3,2}$. In the case of $\mathcal{R}_{3,1}$ we searched for all the good binary self-dual codes of length 12 (in this case with the parameters [12,6,4]) and then lifted them. In the case of $\mathcal{R}_{3,2}$ we lifted all the good binary self-dual codes of length 6.

After searching over all possible lifts that are self-dual and taking Gray images of these lifts we have obtained 6 non-equivalent extremal self-dual codes of length 36. Two of these codes also have been obtained taking Gray images of double circulant self-dual codes over $\mathcal{R}_{3,1}$ and $\mathcal{R}_{3,2}$ of length 12.

There are two possible weight enumerators for extended self-dual codes of length 36:

$$W_{36,1} = 1 + 225y^8 + 2016y^{10} + \cdots \tag{3.4}$$

and

$$W_{36,2} = 1 + 289y^8 + 1632y^{10} + \cdots \tag{3.5}$$

Table 3.1 Binary [36,18,8] extremal self-dual codes obtained from double circulant constructions.

Ring	First row of M	$\lvert Aut(C)\rvert$	$W_{36}(C)$
$\mathcal{R}_{3,1}$	$(u^2+u, 1, u+1, u^2+u+1, u^2+u+1, 1)$	864	$W_{36,1}$
$\mathcal{R}_{3,2}$	$(u+v, u^2+u+v, u^2v+uv+v+1)$	864	$W_{36,1}$
$\mathcal{R}_{3,1}$	$(u, 1, u+1, u^2+u+1, u^2+u+1, 1)$	12960	$W_{36,1}$
$\mathcal{R}_{3,2}$	$(u+v, u^2v+u^2+u+v, uv+1)$	12960	$W_{36,1}$

Table 3.2 Binary [36,18,8] extremal self-dual codes obtained from bordered double circulant construction over $\mathcal{R}_{3,1}$.

First row of M	(x, y, z)	$\|Aut(C)\|$	$W_{36}(C)$
$(u, 1, 1, u^2+1, u^2+1)$	$(u, u+1, u+1)$	80	$W_{36,2}$
$(u, 1, u+1, u^2+u+1, 1)$	$(u^2+u, u+1, u+1)$	240	$W_{36,1}$

Table 3.3 Binary [36,18,8] extremal self-dual codes obtained from four circulant construction over $\mathcal{R}_{3,1}$.

First row of A	First row of B	$\|Aut(C)\|$	$W_{36}(C)$
$(u, 1, u^2+1)$	$(u+1, u+1, u+1)$	96	$W_{36,1}$
$(u^2+u, 1, u^2+1)$	$(u+1, u+1, u+1)$	288	$W_{36,1}$
$(u, 1, u^2+1)$	$(u+1, u+1, u^2+u+1)$	864	$W_{36,1}$
$(u^2+u, 1, u^2+1)$	$(u+1, u+1, u^2+u+1)$	12960	$W_{36,1}$

3.2.4 Extremal Self-Dual Codes of Length 66

Extremal codes of length 66 have parameters $[66, 33, 12]$ and their possible weight enumerators are as follows:

$$W_{66,1} = 1 + (858 + 8\beta)\, y^{12} + (18678 - 24\beta)\, y^{14} + \cdots, 0 \leq \beta \leq 778, \quad (3.6)$$

$$W_{66,2} = 1 + 1690y^{12} + 7990y^{14} + \cdots \quad (3.7)$$

and

$$W_{66,3} = 1 + (858 + 8\beta)\, y^{12} + (18166 - 24\beta)\, y^{14} + \cdots, 14 \leq \beta \leq 756. \quad (3.8)$$

We have obtained 2 non-equivalent extremal binary self-dual $[66, 33, 12]$ codes from double circulant matrices over $\mathcal{R}_{3,1}$. Because of Theorem 3.1.4, we needed to search for the $[22, 11, 6]$ binary double circulant self-dual code, which we lifted to $\mathcal{R}_{3,1}$. After taking Gray images of these lifts we have obtained the following extremal binary self-dual $[66, 33, 12]$ codes, which were also obtained in (Kaya et al., 2014) by a different construction:

Table 3.4 Binary [66,33,12] extremal self-dual codes obtained from double circulant construction over $\mathcal{R}_{3,1}$

First row of A	$\lvert Aut(C)\rvert$	β in $W_{66,1}$
$(u, u, u, 1, u, u^2 + u, 1, u, 1, 1, 1)$	220	22
$(u^2 + u, u^2 + u, u^2 + u, 1, u^2 + u, u, 1, u^2 + u, 1, 1, 1)$	660	66

3.2.5 Best known Self-dual Codes of Length 72

We know that an extremal Type I code of length 72 must have a minimum distance 14 while a Type II one must have 16 as its minimum distance. But as yet the existence of these codes is an open problem. However a lot of work has gone towards classifying self-dual codes of parameters $[72, 36, 12]$ of both types, especially Type II ones. A number of singly even self-dual $[72, 36, 12]$ codes have been listed in (Kaya et al., 2014) and (Dougherty et al., 2007). In (Gulliver and Harada, 2008), (Dougherty et al., 1997), (Dontcheva., 2002), (Bouyukliev et al., 2005) a great number of doubly even self-dual $[72, 36, 12]$ codes are constructed. We have constructed a considerable number of new Type I and Type II self-dual codes of length 72 as images of self-dual codes over $\mathcal{R}_{3,1}$ and $\mathcal{R}_{3,2}$ via the double and bordered double circulant constructions. To do this, by using Theorem 3.1.4, we have had to do an exhaustive search over all possible lifts of suitable binary self-dual codes of length 24 and 12, respectively. We illustrate this method in the following example:

Example 3.2.4. Consider the binary self-dual code of the parameters $[24, 12, 6]$ obtained by pure double circulant construction. We lift the first row of the circulant matrix in its generator matrix to $\mathcal{R}_{3,1}$ as follows:

$$\begin{array}{rcccccccccccc} x = & (0, & 0, & 0, & 0, & 1, & 0, & 0, & 1, & 1, & 1, & 0, & 1) \\ & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ X = & (0, & 0, & 0, & u, & u+1, & u^2, & u^2, & 1, & u^2+u+1, & u+1, & 0, & u^2+1). \end{array}$$

Afterwards, we set the pure double circulant matrix of the form $[I_{12} \mid X]$ and we generate self-dual codes over $\mathcal{R}_{3,1}$ by MAGMA. The Gray image of this code is a binary Type I $[72,36,12]-$self-dual code with the weight enumerator $1+494y^{12}+8640y^{14}+\cdots$ and it has an automorphism group of order 48.

Using the double circulant construction over $\mathcal{R}_{3,1}$ we were able to obtain 117 non-equivalent Type I binary $[72,36,12]$-codes and 43 non-equivalent Type II binary $[72,36,12]$-codes. Using the bordered double circulant construction over $\mathcal{R}_{3,1}$ we found 27 new Type II and 36 Type I self-dual $[72,36,12]$-codes. Moreover, by using the bordered double circulant construction over $\mathcal{R}_{3,2}$, we constructed 22 new Type I $[72,36,12]$-codes and 35 new Type II $[72,36,12]$-codes. In (Kaya et al., 2014) two possible weight enumerators were given for Type I $[72,36,12]$-codes as follows:

$$\begin{aligned} W_{72,1} &= 1+2\beta y^{12}+(8640-64\gamma)y^{14}+(124281-24\beta+384\gamma)y^{16}+\cdots \\ W_{72,2} &= 1+2\beta y^{12}+(7616-64\gamma)y^{14}+(134521-24\beta+384\gamma)y^{16}+\cdots \end{aligned} \tag{3.9}$$

where β and γ are parameters.

Before proceeding with the following tables in which we list all the new Type I and Type II binary self-dual codes of parameter $[72,36,12]$, we would like to introduce a notation to shorten the elements of $\mathcal{R}_{3,2}$, that can also be used for $\mathcal{R}_{3,1}$ as well. Note that $R_{3,2}$ is an $\mathbb{F}_2$-vector space with a basis that we can take as $\{u^2v, uv, v, u^2, u, 1\}$. Any element in $\mathcal{R}_{3,2}$ corresponds to a 6-bit string over $\mathbb{F}_2$ which we can consider as a base 2 expression of a natural number. With this notation every element in $\mathcal{R}_{3,2}$ corresponds to a integer from 0 to 63. For example $uv+v+u^2+1$ corresponds to (011101) whose numerical value can be taken as 29. Taking the basis as $\{u^2, u, 1\}$ gives a numerical value from 0 to 7 to any element in $\mathcal{R}_{3,1}$.

The 76 and 41 new binary Type I $[72,36,12]$ self-dual codes that were obtained from double circulant matrices over $\mathcal{R}_{3,1}$ all have 48 and 96 respectively as the orders of their automorphism groups and the parameters for their weight enumerators in $W_{72,1}$ were given in following tables:

Table 3.5 New Type I $[72, 36, 12]$ self-dual codes obtained from double circulant matrices over $\mathcal{R}_{3,1}$,$|Aut(B_i)| = 48$.

code B_i	first row of M	β in $W_{72,1}$	γ in $W_{72,1}$
B_1	(2,2,2,4,3,4,6,1,3,5,6,7)	185	0
B_2	(0,0,0,6,3,4,4,1,7,7,0,5)	199	0
B_3	(2,0,2,0,3,6,6,3,3,1,6,5)	201	0
B_4	(4,2,2,6,1,6,0,3,5,7,2,7)	207	0
B_5	(6,2,0,2,3,6,2,3,7,3,0,7)	225	0
B_6	(0,0,2,4,3,6,4,3,3,5,6,5)	231	0
B_7	(6,0,2,0,3,6,2,3,3,1,6,5)	233	0
B_8	(0,0,0,2,3,4,4,1,7,3,0,5)	247	0
B_9	(6,2,2,4,3,4,2,1,3,5,6,7)	249	0
B_{10}	(6,2,2,6,3,4,2,1,3,7,6,7)	255	0
B_{11}	(2,2,2,6,3,4,6,1,3,7,6,7)	271	0
B_{12}	(6,2,0,4,1,4,2,1,1,5,4,7)	273	0
B_{13}	(2,2,0,4,1,4,6,1,1,5,4,7)	281	0
B_{14}	(0,2,0,6,3,6,4,3,7,7,0,7)	295	0
B_{15}	(2,0,0,0,1,6,6,3,1,1,4,5)	297	0
B_{16}	(4,2,2,2,1,6,0,3,5,3,2,7)	303	0
B_{17}	(6,0,6,4,3,2,2,3,3,1,2,1)	317	0
B_{18}	(0,2,2,6,1,6,4,3,5,7,2,7)	319	0
B_{19}	(2,0,0,6,3,4,6,1,7,7,0,5)	321	0
B_{20}	(2,2,2,2,1,6,6,3,5,3,2,7)	329	0
B_{21}	(0,0,2,0,3,2,4,3,3,5,6,1)	339	0
B_{22}	(2,0,6,0,3,2,6,3,3,5,2,1)	341	0
B_{23}	(6,2,2,6,1,6,2,3,5,7,2,7)	353	0
B_{24}	(4,0,2,4,3,2,0,3,3,1,7,1)	355	0
B_{25}	(4,2,0,6,3,6,0,3,7,7,0,7)	375	0
B_{26}	(2,0,0,2,3,4,6,1,7,3,0,5)	377	0
B_{27}	(0,2,2,2,1,6,4,3,5,3,2,7)	463	0
B_{28}	(2,0,0,3,6,1,3,3,1,4,7,5)	145	6

Table 3.5 (continued)

B_{29}	(0,6,4,3,6,3,3,7,5,6,5,7)	153	6
B_{30}	(0,4,2,1,2,7,3,5,7,4,1,3)	159	6
B_{31}	(0,4,0,3,2,3,3,7,5,2,1,7)	165	6
B_{32}	(0,2,0,1,4,5,1,1,1,6,5,1)	169	6
B_{33}	(0,0,6,1,6,3,3,5,7,0,5,7)	171	6
B_{34}	(0,2,6,1,4,3,1,1,7,6,5,7)	177	6
B_{35}	(0,0,2,1,6,1,3,5,3,0,5,5)	181	6
B_{36}	(0,2,4,3,2,1,3,7,1,2,1,5)	183	6
B_{37}	(0,6,6,3,2,5,3,7,3,6,1,1)	193	6
B_{38}	(0,0,2,3,4,1,1,3,3,4,5,5)	195	6
B_{39}	(0,2,4,3,6,3,3,7,5,2,5,7)	201	6
B_{40}	(0,0,2,1,2,3,3,5,7,0,1,7)	207	6
B_{41}	(0,0,0,1,2,7,3,5,5,0,1,3)	213	6
B_{42}	(0,0,0,3,4,1,1,3,1,4,5,5)	217	6
B_{43}	(0,4,6,1,6,3,3,5,7,4,5,7)	219	6
B_{44}	(0,0,6,3,4,7,1,3,7,4,5,3)	225	6
B_{45}	(0,6,4,3,2,1,3,7,1,6,1,5)	231	6
B_{46}	(0,4,0,1,2,7,3,5,5,4,1,3)	237	6
B_{47}	(2,0,0,1,4,1,1,5,1,0,7,5)	243	6
B_{48}	(0,2,2,3,6,1,3,7,3,2,5,5)	253	6
B_{49}	(0,0,4,3,2,7,1,3,5,4,5,3)	255	6
B_{50}	(2,0,0,3,6,5,3,3,1,4,7,1)	265	6
B_{51}	(2,0,2,3,6,1,3,3,3,4,7,5)	267	6
B_{52}	(0,0,4,3,0,1,1,3,1,4,1,5)	277	6
B_{53}	(0,0,6,3,0,1,1,3,3,4,1,5)	279	6
B_{54}	(2,0,2,3,2,7,3,3,7,4,3,3)	285	6
B_{55}	(2,0,0,3,2,7,3,3,5,4,3,3)	291	6
B_{56}	(0,2,6,1,4,7,1,1,7,6,5,3)	297	6
B_{57}	(0,2,2,3,2,3,3,7,7,2,1,7)	303	6
B_{58}	(0,0,0,1,2,3,3,5,5,0,1,7)	309	6

Table 3.5 (continued)

B_{59}	(0,6,6,3,6,3,3,7,7,6,5,7)	315	6
B_{60}	(0,0,4,1,6,3,3,5,5,0,5,7)	321	6
B_{61}	(0,0,4,3,0,5,1,3,1,4,1,1)	325	6
B_{62}	(0,0,4,1,2,1,3,5,1,0,1,5)	327	6
B_{63}	(0,0,6,3,4,3,1,3,7,4,5,7)	345	6
B_{64}	(2,0,4,3,2,5,3,3,1,4,3,1)	349	6
B_{65}	(0,2,4,1,4,3,1,1,5,6,5,7)	351	6
B_{66}	(2,0,2,3,6,5,3,3,3,4,7,1)	387	6
B_{67}	(0,0,0,3,0,7,1,3,5,4,1,3)	411	6
B_{68}	(0,2,4,1,4,7,1,1,5,6,5,3)	423	6
B_{69}	(6,2,2,2,1,6,2,3,5,3,2,7)	345	24
B_{70}	(2,2,0,6,3,6,6,3,7,7,0,7)	393	24
B_{71}	(0,0,6,4,3,2,4,3,3,1,2,1)	411	24
B_{72}	(4,0,6,0,3,2,0,3,3,5,2,1)	427	24
B_{73}	(6,0,2,0,3,2,2,3,3,5,6,1)	429	24
B_{74}	(2,0,2,4,3,6,6,3,3,5,6,5)	449	24
B_{75}	(2,0,2,4,3,2,6,3,3,1,6,1)	453	24
B_{76}	(6,2,2,0,3,4,2,1,3,1,6,7)	497	24

Table 3.6 New Type I $[72, 36, 12]$ self-dual codes obtained from double circulant matrices over $\mathcal{R}_{3,1}$,$|Aut(B_i)| = 96$.

code B_i	first row of M	β in $W_{72,1}$	γ in $W_{72,1}$
B_{77}	(0,4,2,2,1,4,4,1,5,3,2,1)	235	0
B_{78}	(0,6,2,2,1,6,4,3,5,3,2,3)	259	0
B_{79}	(4,2,0,6,3,2,0,3,7,3,0,3)	291	0
B_{80}	(4,0,0,6,3,0,0,1,7,3,0,1)	315	0
B_{81}	(0,0,2,6,1,0,4,1,5,3,2,1)	331	0
B_{82}	(4,6,0,2,3,6,0,3,7,3,0,3)	339	0
B_{83}	(2,2,0,6,3,2,6,3,7,3,0,3)	341	0
B_{84}	(0,2,2,6,1,2,4,3,5,3,2,3)	355	0

Table 3.6 (continued)

B_{85}	(2,0,2,2,1,0,6,1,5,7,2,1)	357	0
B_{86}	(4,4,0,2,3,4,0,1,7,3,0,1)	363	0
B_{87}	(6,4,0,2,3,4,2,1,7,3,0,1)	365	0
B_{88}	(0,6,0,6,3,6,4,3,7,7,0,3)	379	0
B_{89}	(6,4,0,6,3,4,2,1,7,7,0,1)	381	0
B_{90}	(2,0,2,6,1,0,6,1,5,3,2,1)	389	0
B_{91}	(0,4,2,6,1,4,4,1,5,7,2,1)	403	0
B_{92}	(2,4,0,6,3,4,6,1,7,7,0,1)	413	0
B_{93}	(0,0,0,6,3,0,4,1,7,3,0,1)	427	0
B_{94}	(2,6,0,2,3,6,6,3,7,3,0,3)	429	0
B_{95}	(4,0,0,2,3,0,0,1,7,7,0,1)	435	0
B_{96}	(4,2,0,2,3,2,0,3,7,7,0,3)	459	0
B_{97}	(6,0,0,2,3,0,2,1,7,7,0,1)	485	0
B_{98}	(0,2,0,6,3,2,4,3,7,3,0,3)	499	0
B_{99}	(4,2,2,2,1,2,0,3,5,7,2,3)	507	0
B_{100}	(2,4,2,6,1,4,6,1,5,7,2,1)	509	0
B_{101}	(0,2,2,2,1,2,4,3,5,7,2,3)	331	24
B_{102}	(6,4,2,6,1,4,2,1,5,7,2,1)	333	24
B_{103}	(4,4,0,6,3,4,0,1,7,7,0,1)	339	24
B_{104}	(0,0,2,2,1,0,4,1,5,7,2,1)	355	24
B_{105}	(2,0,0,2,3,0,6,1,7,7,0,1)	357	24
B_{106}	(4,6,0,6,3,6,0,3,7,7,0,3)	363	24
B_{107}	(6,6,2,6,1,6,2,3,5,7,2,3)	381	24
B_{108}	(4,0,2,6,1,0,0,1,5,3,2,1)	411	24
B_{109}	(0,4,0,2,3,4,4,1,7,3,0,1)	427	24
B_{110}	(6,2,0,6,3,2,2,3,7,3,0,3)	453	24
B_{111}	(4,2,2,6,1,2,0,3,5,3,2,3)	483	24
B_{112}	(0,6,0,2,3,6,4,3,7,3,0,3)	499	24
B_{113}	(6,0,0,6,3,0,2,1,7,3,0,1)	501	24
B_{114}	(2,6,2,2,1,6,6,3,5,3,2,3)	525	24

Table 3.6 (continued)

B_{115}	(2,4,2,2,1,4,6,1,5,3,2,1)	573	24
B_{116}	(6,2,0,2,3,2,2,3,7,7,0,3)	629	48
B_{117}	(2,6,2,6,1,6,6,3,5,7,2,3)	653	48

The order of the automorphism group of all the 36 new binary Type I $[72, 36, 12]$ self-dual codes that were constructed from bordered-double circulant matrices over $\mathcal{R}_{3,1}$ is 44 and their parameters in $W_{72,2}$ were given in following table:

Table 3.7 New Type I $[72, 36, 12]$ binary self-dual codes obtained from bordered double circulant matrices over $\mathcal{R}_{3,1}$,$|Aut(C_i)| = 44$.

Code C_i	first row of M	x, y, z	β in $W_{72,2}$	γ in $W_{72,2}$
C_1	(0,0,6,3,6,3,5,2,3,1,7)	(2,3,3)	88	0
C_2	(0,0,6,3,4,1,1,6,5,1,7)	(4,1,1)	89	0
C_3	(0,0,0,3,2,3,7,2,1,7,5)	(4,1,1)	111	0
C_4	(0,0,0,3,4,1,3,2,3,7,1)	(2,3,3)	132	0
C_5	(0,0,6,3,2,3,5,6,7,1,3)	(2,3,3)	154	0
C_6	(0,0,6,3,6,5,5,4,7,5,1)	(4,1,1)	155	0
C_7	(0,0,2,3,4,3,5,4,5,1,1)	(2,3,3)	165	0
C_8	(0,0,2,3,4,5,5,2,1,5,7)	(4,1,1)	177	0
C_9	(0,0,0,1,6,7,5,4,3,1,1)	(2,3,3)	187	0
C_{10}	(0,0,2,3,6,7,1,6,7,5,7)	(2,3,3)	198	0
C_{11}	(0,2,0,1,2,1,7,4,3,1,5)	(4,1,1)	199	0
C_{12}	(0,0,0,3,0,1,3,6,7,7,5)	(2,3,3)	220	0
C_{13}	(0,2,0,3,4,7,1,6,7,7,1)	(4,1,1)	221	0
C_{14}	(0,2,4,1,6,3,3,2,7,1,7)	(2,3,3)	231	0
C_{15}	(0,0,2,1,0,1,7,4,3,3,3)	(2,3,3)	242	0
C_{16}	(0,0,0,1,2,1,5,6,3,5,3)	(4,1,1)	243	0
C_{17}	(0,2,0,1,2,7,7,2,7,5,3)	(2,3,3)	253	0
C_{18}	(0,0,2,1,4,1,7,0,7,3,7)	(2,3,3)	264	0
C_{19}	(0,0,6,1,0,3,3,6,3,3,5)	(4,1,1)	265	0

Table 3.7 (continued)

C_{20}	(0,0,0,1,4,3,1,6,1,5,7)	(2,3,3)	275	0
C_{21}	(0,2,0,3,6,5,5,2,1,7,1)	(2,3,3)	286	0
C_{22}	(0,2,4,1,0,1,7,2,5,1,3)	(4,1,1)	287	0
C_{23}	(0,2,0,1,4,3,3,4,1,1,1)	(2,3,3)	297	0
C_{24}	(0,2,0,3,6,3,5,4,5,3,7)	(4,1,1)	309	0
C_{25}	(0,2,2,1,2,5,1,4,1,3,3)	(2,3,3)	319	0
C_{26}	(0,0,4,3,6,1,3,4,5,7,7)	(2,3,3)	330	0
C_{27}	(0,0,2,1,4,7,7,6,3,7,1)	(4,1,1)	331	0
C_{28}	(0,2,2,1,4,7,5,4,3,3,7)	(4,1,1)	353	0
C_{29}	(0,0,4,1,0,7,5,6,1,1,3)	(2,3,3)	363	0
C_{30}	(0,0,0,3,2,5,7,4,5,3,3)	(2,3,3)	374	0
C_{31}	(0,0,4,1,6,3,1,0,7,5,1)	(2,3,3)	385	0
C_{32}	(0,2,4,3,4,3,5,2,3,3,1)	(4,1,1)	397	0
C_{33}	(0,0,4,3,4,5,7,6,7,3,1)	(2,3,3)	418	0
C_{34}	(0,2,4,3,2,1,1,2,1,3,5)	(2,3,3)	462	0
C_{35}	(0,0,2,3,0,5,5,6,5,5,3)	(4,1,1)	573	0
C_{36}	(0,0,4,3,0,3,7,4,7,7,3)	(4,1,1)	617	0

The 22 new binary Type I $[72, 36, 12]$ self-dual codes that were obtained from bordered-double circulant matrices over $\mathcal{R}_{3,2}$ had weight enumerator of the form $W_{72,1}$. Constructions of the codes whose automorphism groups are of order 40 and 20 have been listed in following table:

Table 3.8 New Type I $[72, 36, 12]$ binary self-dual codes obtained from bordered double circulant matrices over $\mathcal{R}_{3,2}$.

Code D_i	first row of M	x, y, z	β in $W_{72,1}$	γ in $W_{72,1}$	$\lvert Aut(D_i)\rvert$
D_1	(16,1,11,43,37)	(20,49,49)	383	24	40
D_2	(16,1,27,59,37)	(20,49,49)	363	24	40
D_3	(48,1,11,43,37)	(20,17,25)	379	12	40
D_4	(48,1,27,59,37)	(20,17,25)	359	12	40
D_5	(16,1,11,43,37)	(20,17,17)	319	12	40
D_6	(56,1,27,59,5)	(28,17,17)	309	10	40
D_7	(24,17,27,59,21)	(28,17,25)	289	10	40
D_8	(24,1,11,43,5)	(28,17,25)	269	10	40
D_9	(56,17,11,43,21)	(28,17,17)	249	10	40
D_{10}	(56,49,27,59,53)	(28,17,33)	296	18	20
D_{11}	(24,17,11,43,21)	(28,17,41)	276	18	20
D_{12}	(24,33,11,43,37)	(28,17,41)	246	18	20
D_{13}	(24,49,27,59,53)	(28,17,41)	236	18	20
D_{14}	(56,1,27,59,5)	(28,17,33)	206	18	20
D_{15}	(56,1,11,43,5)	(28,17,33)	186	18	20
D_{16}	(56,17,27,59,21)	(28,17,33)	176	18	20
D_{17}	(56,1,27,59,5)	(28,17,49)	277	16	20
D_{18}	(56,1,11,43,5)	(28,17,49)	237	16	20
D_{19}	(24,1,11,43,5)	(28,17,57)	197	16	20
D_{20}	(48,1,27,59,37)	(20,17,57)	307	9	20
D_{21}	(16,1,27,59,37)	(20,17,49)	287	9	20
D_{22}	(16,1,11,43,37)	(20,17,49)	267	9	20

The possible weight enumerators for a Type II $[72, 36, 12]$ code are given in (Dougherty et al., 1997) as

$$W_{72} = 1 + (4398 + \alpha)y^{12} + (197073 - 12\alpha)y^{16} + \cdots$$

Constructions of the new Type II binary self-dual codes of the parameters $[72, 36, 12]$ obtained from circulant matrices over $\mathcal{R}_{3,1}$ and $\mathcal{R}_{3,2}$ were listed in following tables:

Table 3.9 New Type II [72,36,12] self-dual codes obtained from double circulant matrices over $\mathcal{R}_{3,1}$.

code F_i	first row of M	α in W_{72}	$\|Aut(F_i)\|$
F_1	$(2,0,4,3,6,1,3,3,5,4,7,5)$	-3996	144
F_2	$(0,6,0,3,6,3,3,7,1,6,5,7)$	-3900	48
F_3	$(0,0,6,1,2,3,3,5,3,0,1,7)$	-3888	48
F_4	$(0,6,4,3,2,3,3,7,1,6,1,7)$	-3876	48
F_5	$(0,0,2,1,2,1,3,5,7,0,1,5)$	-3852	48
F_6	$(2,0,2,3,6,7,3,3,3,4,7,3)$	-3804	48
F_7	$(0,0,6,3,4,5,1,3,7,4,5,1)$	-3768	48
F_8	$(0,0,0,1,6,3,3,5,1,0,5,7)$	-3756	48
F_9	$(0,6,0,3,2,1,3,7,5,6,1,5)$	-3744	48
F_{10}	$(0,4,4,1,2,3,3,5,1,4,1,7)$	-3732	48
F_{11}	$(0,6,2,3,2,1,3,7,7,6,1,5)$	-3708	48
F_{12}	$(2,0,0,3,6,3,3,3,1,4,7,7)$	-3696	48
F_{13}	$(0,0,6,3,4,1,1,3,7,4,5,5)$	-3672	48
F_{14}	$(0,0,4,3,4,5,1,3,5,4,5,1)$	-3660	48
F_{15}	$(0,0,4,1,6,1,3,5,5,0,5,5)$	-3624	48
F_{16}	$(2,0,2,3,6,3,3,3,3,4,7,7)$	-3612	48
F_{17}	$(0,0,0,3,4,7,1,3,1,4,5,3)$	-3600	7920
F_{18}	$(0,0,6,1,2,7,3,5,3,0,1,3)$	-3600	48
F_{19}	$(0,0,4,1,2,3,3,5,1,0,1,7)$	-3588	48
F_{20}	$(0,0,2,1,2,5,3,5,7,0,1,1)$	-3564	48
F_{21}	$(0,4,2,1,2,5,3,5,7,4,1,1)$	-3564	144

Table 3.9 (continued)

F_{22}	$(0,0,2,3,0,5,1,3,7,4,1,1)$	-3552	48
F_{23}	$(0,0,2,3,4,7,1,3,3,4,5,3)$	-3516	48
F_{24}	$(0,0,0,3,0,1,1,3,5,4,1,5)$	-3492	48
F_{25}	$(0,0,2,1,6,3,3,5,3,0,5,7)$	-3480	48
F_{26}	$(0,2,2,1,4,7,1,1,3,6,5,3)$	-3468	48
F_{27}	$(0,0,0,1,2,1,3,5,5,0,1,5)$	-3456	48
F_{28}	$(0,4,6,1,6,1,3,5,7,4,5,5)$	-3444	48
F_{29}	$(2,0,4,3,2,7,3,3,1,4,3,3)$	-3384	48
F_{30}	$(2,0,4,1,4,1,1,5,5,0,7,5)$	-3336	48
F_{31}	$(0,2,6,3,2,7,3,7,3,2,1,3)$	-3312	48
F_{32}	$(0,0,0,3,0,5,1,3,5,4,1,1)$	-3300	48
F_{33}	$(0,0,0,3,4,3,1,3,1,4,5,7)$	-3264	48
F_{34}	$(0,0,6,3,0,3,1,3,3,4,1,7)$	-3252	48
F_{35}	$(0,4,2,1,6,3,3,5,3,4,5,7)$	-3192	48
F_{36}	$(0,0,2,3,4,3,1,3,3,4,5,7)$	-3180	48
F_{37}	$(0,4,4,1,2,7,3,5,1,4,1,3)$	-3156	48
F_{38}	$(2,0,2,3,2,5,3,3,7,4,3,1)$	-3120	48
F_{39}	$(0,2,0,3,6,3,3,7,1,2,5,7)$	-3036	48
F_{40}	$(0,2,0,1,4,3,1,1,1,6,5,7)$	-3024	48
F_{41}	$(0,2,0,1,4,7,1,1,1,6,5,3)$	-2976	48
F_{42}	$(0,0,4,3,0,7,1,3,1,4,1,3)$	-2952	48
F_{43}	$(2,0,0,3,2,5,3,3,5,4,3,1)$	-2868	48

Table 3.10 New Type II [72,36,12] self-dual codes obtained from bordered double circulant matrices over $\mathcal{R}_{3,1}$.

Code F_i	first row of M	x, y, z	α in W_{72}	$\lvert Aut(F_i\rvert$
F_{44}	$(0,2,0,3,2,1,5,2,5,7,1)$	$(6,3,3)$	-4134	132
F_{45}	$(0,0,2,3,6,3,1,2,7,5,3)$	$(6,3,3)$	-4002	44
F_{46}	$(0,2,4,1,2,1,3,4,7,5,1)$	$(0,1,1)$	-3996	44
F_{47}	$(0,0,2,3,2,3,1,6,3,5,7)$	$(6,3,3)$	-3870	44
F_{48}	$(0,0,2,3,6,5,1,4,3,1,5)$	$(0,1,1)$	-3864	44
F_{49}	$(0,0,4,1,6,7,1,4,7,5,5)$	$(6,3,3)$	-3804	44
F_{50}	$(0,0,0,3,6,1,7,4,1,3,3)$	$(6,3,3)$	-3738	44
F_{51}	$(0,0,0,1,2,5,5,2,3,5,7)$	$(0,1,1)$	-3732	44
F_{52}	$(0,0,4,1,4,3,5,6,5,1,3)$	$(6,3,3)$	-3672	44
F_{53}	$(0,0,0,3,4,5,3,6,3,7,5)$	$(6,3,3)$	-3606	44
F_{54}	$(0,0,2,3,4,1,5,6,1,5,3)$	$(0,1,1)$	-3600	44
F_{55}	$(0,0,0,1,2,3,5,4,7,1,1)$	$(6,3,3)$	-3540	44
F_{56}	$(0,0,2,1,4,5,7,4,7,3,3)$	$(6,3,3)$	-3474	44
F_{57}	$(0,0,0,1,6,5,5,6,7,5,3)$	$(0,1,1)$	-3468	44
F_{58}	$(0,0,0,1,0,7,1,6,5,5,7)$	$(6,3,3)$	-3408	44
F_{59}	$(0,2,2,1,4,5,5,6,7,7,5)$	$(6,3,3)$	-3342	132
F_{60}	$(0,0,0,3,0,5,3,2,7,7,1)$	$(6,3,3)$	-3342	44
F_{61}	$(0,0,0,3,0,3,3,4,3,3,7)$	$(0,1,1)$	-3336	44
F_{62}	$(0,0,6,3,4,3,1,4,1,5,5)$	$(6,3,3)$	-3276	44
F_{63}	$(0,2,4,3,2,5,1,6,1,3,1)$	$(6,3,3)$	-3210	44
F_{64}	$(0,0,2,1,0,3,7,6,7,7,1)$	$(0,1,1)$	-3204	44
F_{65}	$(0,2,2,1,6,1,1,4,5,3,3)$	$(6,3,3)$	-3144	44
F_{66}	$(0,0,4,3,2,5,3,4,1,7,7)$	$(6,3,3)$	-3078	44
F_{67}	$(0,0,0,3,6,7,7,2,5,7,5)$	$(0,1,1)$	-3072	44
F_{68}	$(0,2,4,3,0,1,5,4,3,7,7)$	$(6,3,3)$	-2946	44
F_{69}	$(0,2,4,1,4,5,7,2,1,1,3)$	$(0,1,1)$	-2940	44
F_{70}	$(0,0,4,3,4,7,7,4,3,7,3)$	$(0,1,1)$	-2808	44

Table 3.11 New Type II [72,36,12] self-dual codes obtained from bordered double circulant matrices over $\mathcal{R}_{3,2}$.

Code G_i	first row of M	x, y, z	α in W_{72}	$\lvert Aut(G_i)\rvert$
G_1	$(8, 17, 27, 59, 21)$	$(12, 17, 25)$	-3960	120
G_2	$(8, 33, 27, 59, 37)$	$(12, 17, 25)$	-3960	40
G_3	$(8, 1, 11, 43, 5)$	$(12, 17, 25)$	-3840	40
G_4	$(24, 1, 27, 59, 5)$	$(28, 49, 57)$	-3732	40
G_5	$(24, 17, 27, 59, 21)$	$(28, 33, 41)$	-3720	40
G_6	$(24, 1, 11, 43, 5)$	$(28, 49, 57)$	-3612	40
G_7	$(8, 1, 27, 59, 5)$	$(12, 17, 25)$	-3600	40
G_8	$(24, 17, 27, 59, 21)$	$(28, 49, 57)$	-3492	40
G_9	$(8, 33, 11, 43, 37)$	$(12, 17, 25)$	-3480	40
G_{10}	$(24, 17, 11, 43, 21)$	$(28, 49, 57)$	-3372	40
G_{11}	$(8, 49, 27, 59, 53)$	$(12, 17, 25)$	-3360	40
G_{12}	$(56, 17, 57, 43, 21)$	$(28, 49, 49)$	-3252	40
G_{13}	$(8, 17, 11, 43, 21)$	$(12, 17, 25)$	-3240	40
G_{14}	$(10, 1, 25, 29, 37)$	$(42, 11, 11)$	-3120	40
G_{15}	$(10, 1, 25, 29, 37)$	$(42, 35, 35)$	-3000	40
G_{16}	$(10, 1, 57, 61, 37)$	$(42, 11, 11)$	-2880	40
G_{17}	$(56, 33, 27, 59, 37)$	$(28, 33, 49)$	-3942	20
G_{18}	$(24, 49, 11, 43, 53)$	$(28, 33, 57)$	-3882	20
G_{19}	$(24, 1, 11, 43, 5)$	$(28, 33, 57)$	-3822	20
G_{20}	$(10, 9, 1, 37, 13)$	$(10, 11, 59)$	-3786	20
G_{21}	$(24, 17, 27, 59, 21)$	$(28, 33, 57)$	-3762	20
G_{22}	$(10, 17, 41, 45, 53)$	$(10, 11, 59)$	-3726	20
G_{23}	$(56, 1, 11, 43, 5)$	$(28, 33, 49)$	-3702	20
G_{24}	$(24, 49, 27, 59, 53)$	$(28, 33, 57)$	-3642	20
G_{25}	$(10, 9, 49, 21, 13)$	$(10, 11, 59)$	-3606	20
G_{26}	$(56, 33, 11, 43, 37)$	$(28, 33, 49)$	-3582	20
G_{27}	$(10, 1, 9, 13, 37)$	$(10, 11, 59)$	-3546	20
G_{28}	$(24, 17, 11, 43, 21)$	$(28, 33, 57)$	-3522	20

Table 3.11 (continued)

G_{29}	$(24, 33, 11, 43, 37)$	$(28, 33, 57)$	-3462	20
G_{30}	$(10, 1, 41, 45, 37)$	$(10, 11, 59)$	-3426	20
G_{31}	$(56, 49, 27, 59, 53)$	$(28, 33, 49)$	-3402	20
G_{32}	$(10, 9, 17, 53, 13)$	$(10, 11, 59)$	-3366	20
G_{33}	$(10, 25, 17, 53, 29)$	$(10, 11, 59)$	-3306	20
G_{34}	$(10, 1, 25, 29, 37)$	$(10, 11, 59)$	-3246	20
G_{35}	$(10, 9, 33, 5, 13)$	$(10, 11, 59)$	-3186	20

3.3 QUADRATIC DOUBLE CIRCULANT CODES OVER $\mathcal{R}_{k,m}$

Quadratic residue codes have been one of the interesting classes of algebraic codes. In 2002, they were generalized into quadratic double circulant (QDC) codes by Gaborit in (Gaborit, 2002) over finite fields. In (Kaya et al., 2014), Gaborit's method was extended to the rings of characteristic 2 to get extremal self-dual codes. In this section, our goal is to give some conditions to obtain self-dual codes over $\mathcal{R}_{k,m}$ using QDC construction and to find new constructions for binary self-dual codes of certain lengths.

First, we recall the notions of residues and non residues for finite fields:

Definition 3.3.1. (Ling and Xing, 2004) Let p be a prime number bigger than 2 and choose a primitive element g of $\mathbb{F}_p$ ($\mathbb{F}_p^* = \langle g \rangle = \{g, g^2, g^3, \ldots, g^{p-2}, g^{p-1} = 1\}$). A nonzero element r of $\mathbb{F}_p$ is called a quadratic residue modulo p if $r = g^{2i}$ for some integer i; otherwise, r is called a quadratic non residue modulo p. It is clear that r is quadratic non residue if $r = g^{2j-1}$ for some integer j.

We denote by $\mathcal{Q}_p$ the set of quadratic residues and by $\mathcal{N}_p$ the set of quadratic non residues.

Example 3.3.2. Consider the finite field $\mathbb{F}_{11} = \mathbb{Z}_{11}$. It is easy to check that 2 is a primitive element of $\mathbb{F}_{11}$. Thus, the nonzero quadratic residues modulo 11 are $\{2^{2i} : i = 0, 1, ...\} = \{1, 3, 4, 5, 9\}$, and the quadratic non residues modulo 11 are

$\{3^{2i-1} : i = 1, 2, ...\} = \{2, 6, 7, 8, 10\}$. So $\mathbb{Z}_{11} = \{0\} \cup \{1, 3, 4, 5, 9\} \cup \{2, 6, 7, 8, 10\} = \{0\} \cup \mathcal{Q}_{11} \cup \mathcal{N}_{11}$.

Let p be an odd prime and $Q_p(a, b, c)$ be the circulant matrix with first row r based on quadratic residues modulo p defined as $r[1] = a$, $r[i+1] = b$ if i is a quadratic residue and $r[i+1] = c$ if i is a quadratic non residue modulo p. We state the special case of the main theorem from (Gaborit, 2002) where p is an odd prime;

Theorem 3.3.3. ((Gaborit, 2002)) Let p be an odd prime and let $Q_p(a, b, c)$ be the circulant matrix with a, b and c as the elements of the ring R. If $p = 4k + 1$ then

$$\begin{aligned} & Q_p(a,b,c)\, Q_p(a,b,c)^t \\ = \; & 4Q_p\left(a^2 + 2k\left(b^2 + c^2\right), 2ab - b^2 + k\left(b + c\right)^2, 2ac - c^2 + k\left(b + c\right)^2\right). \end{aligned} \tag{3.10}$$

If $p = 4k + 3$ then

$$\begin{aligned} & Q_p(a,b,c)\, Q_p(a,b,c)^t \\ = \; & Q_p(a^2 + (2k+1)\left(b^2 + c^2\right), ab + ac + k\left(b^2 + c^2\right) + (2k+1)\, bc, \\ & ab + ac + k\left(b^2 + c^2\right) + (2k+1)\, bc). \end{aligned} \tag{3.11}$$

Definition 3.3.4. ((Gaborit, 2002)) The code generated by

$$P_p(a, b, c) = (I_p | Q_p(a, b, c))$$

over R is called a quadratic double circulant code and is denoted by $\mathcal{QDC}_p(R)(a, b, c)$.

Example 3.3.5. Consider the code $\mathcal{QDC}_5(\mathcal{R}_{2,2})(1 + v + uv, u, v)$ that is generated by

$$\left[\begin{array}{c|ccccc} & 1+v+uv & u & v & v & u \\ & u & 1+v+uv & u & v & v \\ I_5 & v & u & 1+v+uv & u & v \\ & v & v & u & 1+v+uv & u \\ & u & v & v & u & 1+v+uv \end{array}\right].$$

Self-duality of the code is easily checked by Theorem 3.3.3. Moreover, each row of the generator matrix has Lee weight 8, which means the binary image of the code is doubly-even. It is an extremal self-dual $[40, 20, 8]$ code with partial weight distribution $1 + 285z^8 + 21280z^{12} + \cdots$.

In the following, we define a special subfamily of units and non-units in $\mathcal{R}_{k,m}$;

Definition 3.3.6. An element r of $\mathcal{R}_{k,m}$ is called a *basic non-unit* if $r^2 = 0$ and a *basic unit* if $r^2 = 1$.

It is easily observed that $1+r$ is a basic unit if and only if r is a basic non-unit.

In the following theorems, we characterize families of self-dual QDC codes over $\mathcal{R}_{k,m}$:

Theorem 3.3.7. Let a be an element of $\mathcal{R}_{k,m}$ such that $a^3 = 0$ and p be a prime with $p \equiv 3 \pmod 8$ then the codes

$$\mathcal{QDC}_p\left(R_{k,m}\right)\left(a,1,a+a^2\right) \text{ and } \mathcal{QDC}_p\left(R_{k,m}\right)\left(a,1+a^2,a+a^2\right)$$

are self-dual. The constructions are called I and II, respectively.

Proof. Since $p = 8k+3$, $a^3 = 0$ and $char\left(\mathcal{R}_{k,m}\right) = 2$, by the equation 3.11 we have

$$\begin{aligned} & Q_p\left(a,1,a+a^2\right)Q_p\left(a,1,a+a^2\right)^t \\ = \; & Q_p\left(a^2+1+\left(a+a^2\right)^2, a+a\left(a+a^2\right)+\left(a+a^2\right), a+a\left(a+a^2\right)+\left(a+a^2\right)\right) \\ = \; & Q_p\left(1,0,0\right) = I_p, \end{aligned}$$

which implies that $\mathcal{QDC}_p\left(R_{k,m}\right)\left(a,1,a+a^2\right)$ is self-dual. By analogous steps $\mathcal{QDC}_p\left(R_{k,m}\right)\left(a,1+a^2,a+a^2\right)$ is also self-dual. □

The characterization of non-units given in Definition 3.3.6 can be used to construct self-dual codes as follows;

Theorem 3.3.8. Let a and b be two basic non-units in $\mathcal{R}_{k,m}$ and p be a prime. Then the code $\mathcal{QDC}_p\left(\mathcal{R}_{k,m}\right)(1+a,a,b)$ is self-dual whenever $p \equiv 1 \pmod 4$. Moreover, $\mathcal{QDC}_p\left(\mathcal{R}_{k,m}\right)(a,1+b,a)$ is self-dual if $ab = 0$ and $p \equiv 3 \pmod 8$. The constructions are named as III and IV, respectively.

Proof. Let $p = 4k+1$ be a prime, a and b be basic non-units in $\mathcal{R}_{k,m}$. Then by equation 3.10, we have

$$\begin{aligned} & Q_p\left(1+a,a,b\right)Q_p\left(1+a,a,b\right)^t \\ = \; & \begin{cases} Q_p\left((1+a)^2, a^2, b^2\right) & \text{if } k \text{ is even} \\ Q_p\left((1+a)^2, b^2, a^2\right) & \text{if } k \text{ is odd} \end{cases} \\ = \; & Q_p\left(1,0,0\right) = I_p \end{aligned}$$

Hence, the code $\mathcal{QDC}_p(\mathcal{R}_{k,m})(1+a,a,b)$ is self-dual.

Let $p=8k+3$ be a prime, a and b be basic non-units in $R_{k,m}$ with $ab=0$. Then, since $char(\mathcal{R}_{k,m})=2$, by equation 3.11 we have

$$\begin{aligned} & Q_p(a,1+b,a)\,Q_p(a,1+b,a)^T \\ = \; & Q_p(1,a(1+b)+(1+b)a,a(1+b)+(1+b)a) \\ = \; & Q_p(1,0,0)=I_p. \end{aligned}$$

Therefore, the code $\mathcal{QDC}_p(\mathcal{R}_{k,m})(a,1+b,a)$ is self-dual. □

We list some good QDC codes over $\mathcal{R}_{k,m}$ in Table 3.12.

Table 3.12 Some examples of self-dual QDC codes over $\mathcal{R}_{k,m}$.

R	p	Construction	$a,(b)$	The binary image	Comment
$\mathcal{R}_{2,1}$	5	III	$u,0$	$[20,10,4]$	extremal
$\mathcal{R}_{2,2}$	5	III	u,v	$[40,20,8]$	extremal sinly-even
$\mathcal{R}_{2,2}$	5	III	$u+uv,v$	$[40,20,8]$	extremal doubly-even
$\mathcal{R}_{2,1}$	11	I, II	u	$[44,22,8]$	extremal
$\mathcal{R}_{3,1}$	11	I	u	$[66,33,12]$	extremal
$\mathcal{R}_{3,1}$	11	II	u	$[66,33,12]$	extremal
$\mathcal{R}_{2,2}$	11	II	uv	$[88,44,12]$	singly-even
$\mathcal{R}_{2,2}$	11	IV	u,uv	$[88,44,12]$	doubly-even
$\mathcal{R}_{4,1}$	11	I	u^3	$[88,44,12]$	singly-even
$\mathcal{R}_{3,1}$	19	I	u	$[114,57,16]$	-
$\mathcal{R}_{3,2}$	11	II	$v+uv$	$[132,66,12]$	-
$\mathcal{R}_{4,1}$	19	I	u^3	$[152,76,16]$	singly-even

3.4 EXTENSION THEOREMS

Another construction method to get self-dual codes is extension method. An extremal self-dual codes of length $2n+2$ can be obtained from an extremal self-dual codes of length $2n$ by extensions. Brualdi and Pless firstly used extensions for self-dual codes in (Brualdi and Pless, 1991). Afterwards different versions of extensions were used by researchers. In (Kaya and Yildiz, 2016), extension methods described on the binary field were generalized to any ring of characteristic 2. We have applied the extensions to extremal self-dual codes constructed as binary images of self dual codes over $\mathcal{R}_{k,m}$.

3.4.1 Constructions for self-dual codes over $\mathcal{R}_{k,m}$ by λ-circulant matrices

In this section, the four circulant construction is generalized to λ-circulant matrices. Extremal singly-even binary self-dual codes of length 64 are constructed as Gray images of four circulant codes over $\mathcal{R}_{2,1}$ and $\mathcal{R}_{2,2}$. The codes are going to be used in Section 3.4.2 to construct new binary self-dual codes of lengths 66 and 68.

The possible weight enumerators of singly-even extremal self-dual codes of length 64 are characterized in (Conway and Sloane, 1990) as:

$$\begin{aligned} W_{64,1} &= 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \cdots \text{where } 14 \leq \beta \leq 104, \\ W_{64,2} &= 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \cdots \text{where } 0 \leq \beta \leq 277. \end{aligned}$$

Recently, codes with β =29, 39, 53 and 60 in $W_{64,1}$ and codes with β =51, 58 in $W_{64,2}$ are constructed in (Yankov, 2014) and a code with $\beta = 80$ in $W_{64,2}$ is constructed in (Karadeniz et al., 2014b). Together with these the existence of such codes is now known for β =14, 18, 22, 25, 29, 32, 36, 39, 44, 46, 53, 60, 64 in $W_{64,1}$ and for β =0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 21, 22, 23, 24, 25, 28, 29, 30, 32, 33, 36, 37, 38, 40, 41, 44, 48, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120, 184 in $W_{64,2}$.

Definition 3.4.1. Let $r = (r_1, r_2, \ldots, r_n)$ be an element of $(\mathcal{R}_{k,m})^n$. The λ-cyclic shift of r is defined as $\sigma_\lambda(r) = (\lambda r_n, r_1, r_2, \ldots, r_{n-1})$ where $\lambda \in \mathcal{R}_{k,m}$. A square matrix is called λ-circulant if every row is the λ-cyclic shift of the previous one.

Since λ-circulant matrices commute with each other the four circulant construction can be extended from circulant matrices to λ-circulant matrices. We have the following result:

Theorem 3.4.2. Let $\mathcal{C}$ be the linear code over $\mathcal{R}_{k,m}$ of length $4n$ generated by the four circulant matrix

$$G := \left[\begin{array}{c|cc} \multirow{2}{*}{I_{2n}} & A & B \\ & B^t & A^t \end{array}\right]$$

where A and B are λ-circulant $n \times n$ matrices over $\mathcal{R}_{k,m}$ satisfying $AA^t + BB^t = I_n$. Then the code $\mathcal{C}$ is called a λ-four circulant code over $\mathcal{R}_{k,m}$. The code $\mathcal{C}$ and its binary image are self-dual.

Four circulant codes of length 32 over $\mathcal{R}_{2,1}$ have been studied extensively in (Karadeniz et al., 2014b) and the codes with weight enumerators $\beta = 0$, 16, 32, 48 and 80 in $W_{64,2}$ were obtained. The code with the weight enumerator $\beta = 80$ in $W_{64,2}$ is the first such code in literature. For further reference we name this code as $\mathcal{C}_{64,80}$ which is the four circulant code over $\mathcal{R}_{2,1}$ with

$$r_A = (u, 0, 0, 0, u, 1, u, 1+u) \text{ and } r_B = (u, u, 0, 1, 1, 1+u, 1+u, 1+u)\,.$$

By considering $(1+u)$-four circulant codes of length 32 over $\mathcal{R}_{2,1}$ we were able to obtain the binary codes with weight enumerators for $\beta = 8k$ in $W_{64,2}$ where $0 \leq k \leq 9$. These are listed in Table 3.13.

Table 3.13 $(1+u)$-four circulant codes over $\mathcal{R}_{2,1}$.

$\mathcal{L}_i$	r_A	r_B	β in $W_{64,2}$	$\lvert Aut\,(\mathcal{L}_i)\rvert$
$\mathcal{L}_1$	$(u333uuu0)$	(11311010)	8	2^5
$\mathcal{L}_2$	$(u111000u)$	$(11333u1u)$	24	2^5
$\mathcal{L}_3$	$(u131u0uu)$	(31313030)	72	2^5
$\mathcal{L}_4$	$(33uu3110)$	$(113u00u3)$	0	2^5
$\mathcal{L}_5$	$(330u3110)$	$(1310uuu1)$	16	2^5
$\mathcal{L}_6$	$(33uu3130)$	$(331u0u01)$	32	2^5
$\mathcal{L}_7$	$(11u03130)$	$(131u0003)$	48	2^5
$\mathcal{L}_8$	$(310u113u)$	$(1330uu03)$	64	2^6
$\mathcal{L}_9$	$(u1110u3u)$	$(30u03113)$	8	2^5
$\mathcal{L}_{10}$	$(0133uu30)$	(10001113)	24	2^5
$\mathcal{L}_{11}$	$(u111001u)$	$(3u0u1311)$	40	2^5
$\mathcal{L}_{12}$	$(0133u01u)$	(10001311)	56	2^5

In order to construct extremal binary self-dual codes of length 64 as Gray images of λ-four circulant codes of length 16 over $\mathcal{R}_{2,2}$ we lift binary codes to codes over $\mathcal{R}_{2,1}$ and then lift these to codes over $\mathcal{R}_{2,2}$. Theorem 3.1.4 tells us the minimum distance of the codes to be lifted. We demonstrate this in the following example;

Example 3.4.3. Let $\mathcal{C}$ be the four circulant code of length 16 over $\mathbb{F}_2$ with $r_A = (1,0,0,0)$ and $r_B = (1,1,1,1)$. Then $\mathcal{C}$ is a singly-even $[16,8,4]$ code. The code $\mathcal{C}$ is lifted to $\mathcal{C}'$, which is the $(1+u)$-four circulant code of length 16 over $\mathcal{R}_{2,1}$ with $r'_A = (1,0,u,u)$ and $r'_B = (1,1+u,1,1+u)$. The binary image $\phi_{21}(\mathcal{C}')$ of $\mathcal{C}'$ is a self-dual $[32,16,6]$ code. Then $\mathcal{C}'$ is lifted to the $\mathcal{C}''$ that is the $(1+u+v+uv)$-four circulant code of length 16 over $\mathcal{R}_{2,2}$ with

$$r''_A = (1,0,u,u+v+uv) \text{ and } r''_B = (1+v+uv, 1+u, 1+v, 1+u+v)\,.$$

The binary code $\phi_{22}(\mathcal{C}'')$ is an extremal singly-even binary self-dual code of length 64 with weight enumerator $\beta = 0$ in $W_{64,2}$. Note that, $\pi_v\left(\mathcal{C}''\right) = \mathcal{C}'$, $\pi_u\left(\mathcal{C}'\right) = \mathcal{C}$ and $\mu\left(\mathcal{C}''\right) = \mathcal{C}$.

In order to fit the upcoming tables we use the hexadecimal number system. The one-to-one correspondence between hexadecimals and binary 4 tuples is as follows:

$$\begin{aligned} 0 &\leftrightarrow 0000,\ 1 \leftrightarrow 0001,\ 2 \leftrightarrow 0010,\ 3 \leftrightarrow 0011, \\ 4 &\leftrightarrow 0100,\ 5 \leftrightarrow 0101,\ 6 \leftrightarrow 0110,\ 7 \leftrightarrow 0111, \\ 8 &\leftrightarrow 1000,\ 9 \leftrightarrow 1001,\ A \leftrightarrow 1010,\ B \leftrightarrow 1011, \\ C &\leftrightarrow 1100,\ D \leftrightarrow 1101,\ E \leftrightarrow 1110,\ F \leftrightarrow 1111. \end{aligned}$$

To express elements of $\mathcal{R}_{2,2}$ we use the ordered basis $\{uv, v, u, 1\}$. For instance $1 + u + uv$ in $\mathcal{R}_{2,2}$ is expressed as 1011 which is B.

Table 3.14 Self-dual λ-four circulant codes over $\mathcal{R}_{2,2}$.

$\mathcal{M}_i$	λ	r_A	r_B	β in $W_{64,2}$	$\lvert Aut\,(\mathcal{M}_i)\rvert$
$\mathcal{M}_1$	3	$(F, 0, E, 2)$	$(7, 5, 3, D)$	0	2^5
$\mathcal{M}_2$	3	$(7, 0, C, A)$	$(F, F, 9, 5)$	16	2^5
$\mathcal{M}_3$	3	$(3, 0, D, 4)$	$(E, 3, F, B)$	48	2^5
$\mathcal{M}_4$	7	$(B, 0, 1, C)$	$(9, B, 1, 2)$	5	2^3
$\mathcal{M}_5$	7	$(B, 0, 1, 4)$	$(A, 7, 5, F)$	8	2^4
$\mathcal{M}_6$	7	$(3, 0, 7, A)$	$(B, C, D, 9)$	9	2^3
$\mathcal{M}_7$	7	$(7, 0, 5, C)$	$(1, 3, 2, 5)$	12	2^4
$\mathcal{M}_8$	7	$(D, 0, F, C)$	$(F, 1, 7, A)$	13	2^3
$\mathcal{M}_9$	7	$(B, 0, 1, C)$	$(A, 5, 5, D)$	16	2^5
$\mathcal{M}_{10}$	7	$(B, 0, F, A)$	$(B, C, D, 7)$	17	2^3
$\mathcal{M}_{11}$	7	$(7, 0, 5, C)$	$(2, 7, 5, F)$	24	2^4
$\mathcal{M}_{12}$	F	$(1, 0, 2, E)$	$(D, 3, 5, 7)$	0	2^5
$\mathcal{M}_{13}$	F	$(C, 0, 3, 6)$	$(1, B, 7, 1)$	16	2^5
$\mathcal{M}_{14}$	F	$(F, 0, B, A)$	$(F, B, 4, 5)$	48	2^5
$\mathcal{M}_{15}$	B	$(9, 0, F, C)$	$(B, 6, 9, 3)$	5	2^3
$\mathcal{M}_{16}$	B	$(D, 0, 3, C)$	$(6, B, 5, 3)$	8	2^4
$\mathcal{M}_{17}$	B	$(5, 0, B, 4)$	$(7, 6, D, 9)$	9	2^3
$\mathcal{M}_{18}$	B	$(5, 0, 1, E)$	$(9, 9, C, B)$	12	2^4
$\mathcal{M}_{19}$	B	$(D, 0, 1, 6)$	$(F, 1, 7, C)$	13	2^3
$\mathcal{M}_{20}$	B	$(5, 0, B, C)$	$(E, D, F, 5)$	16	2^3
$\mathcal{M}_{21}$	B	$(B, 0, 5, C)$	$(7, E, D, 7)$	17	2^3
$\mathcal{M}_{22}$	B	$(D, 0, 3, 4)$	$(E, 9, 3, 1)$	24	2^4

Remark 3.4.4. In order to construct the codes in Table 3.13 the binary four circulant codes are lifted to $\mathcal{R}_{2,1}$. Similarly, to construct the codes in Table 3.14 the binary four circulant codes are lifted to $\mathcal{R}_{2,1}$ and then to $\mathcal{R}_{2,2}$. This reduces the search field remarkably from $2^{32} = 4294967296$ to $2^{16} = 65536$.

3.4.2 New binary self-dual codes by extensions

We are able to construct new binary self-dual codes from old. Firstly, we take the images of self-dual codes over $\mathcal{R}_{k,m}$ of length n under duality preserving Gray map $\phi_{k,m}$ and we get binary self-dual codes of length kmn. Afterwards, applying the extension methods to generator matrices of these codes we obtain self dual-codes of length $kmn+2$. On the other hand, we also consider the $\mathcal{R}_{k,1}$ extensions. The ring $\mathcal{R}_{k,m}$ can be considered as an extension of $\mathcal{R}_{k,1}$ and the Gray map φ_u from $\mathcal{R}_{k,m}$ to $\mathcal{R}_{k,1}$ can be defined rearranging ϕ_{km}. So that, we apply extension methods to φ_u-image of codes over $\mathcal{R}_{k,m}$ of length n as well as the codes over $\mathcal{R}_{k,1}$. Then we get codes over $\mathcal{R}_{k,1}$ of length $mn+2$. Finally, we take the Gray images of these new codes under $\phi_{k,1}$ and we obtain binary self-dual codes of length $k(mn+2)$.

There exists different versions of extensions previously applied, for some of these we refer to (Kim, 2001), (Dougherty et al., 2010) and (Kaya and Yildiz, 2016). The following extension theorems hold for any commutative Frobenius ring R of characteristic 2.

Theorem 3.4.5. (Dougherty et al., 2010)Let $\mathcal{C}$ be a self-dual code over R of length n and $G=(r_i)$ be a $k \times n$ generator matrix for $\mathcal{C}$, where r_i is the i-th row of G, $1 \leq i \leq k$. Let c be a unit in R such that $c^2=1$ and X be a vector in R^n with $\langle X, X\rangle = 1$. Let $y_i = \langle r_i, X\rangle$ for $1 \leq i \leq k$. Then the following matrix

$$\left(\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array}\right),$$

generates a self-dual code $\mathcal{C}'$ over R of length $n+2$.

A more specific extension method which can be applied to generator matrices in standard form is as follows:

Theorem 3.4.6. (Kaya and Yildiz, 2016) Let $\mathcal{C}$ be a self-dual code generated by

$G = (I_n|A)$ over R. If the sum of the elements in i-th row of A is r_i then the matrix:

$$G^* = \left(\begin{array}{cc|cccccc} 1 & 0 & x_1 & \dots & x_n & 1 & \dots & 1 \\ \hline y_1 & cy_1 & & & & & & \\ \vdots & \vdots & & I_n & & & A & \\ y_n & cy_n & & & & & & \end{array}\right),$$

where $y_i = x_i + r_i$, c is a unit with $c^2 = 1$, $X = (x_1, \dots, x_n)$ and $\langle X, X \rangle = 1 + n$, generates a self-dual code $\mathcal{C}^*$ over R.

By applying the extensions for self-dual codes to the codes constructed in Section 3.4.1 we were able to obtain new binary self-dual codes of lengths 66 and 68. More precisely, 11 new codes of length 66 and 34 new codes of length 68 were constructed.

3.4.3 $\mathbb{F}_2$-extensions

The Gray images of the codes in tables 3.13 and 3.14 are extremal singly-even self-dual binary codes of length 64. In this section, we search for extremal binary self-dual codes of length 66 by applying Theorem 3.4.5. Eleven new codes were obtained.

A self-dual $[66, 33, 12]$-code has a weight enumerator in one of the following forms (Dougherty et al., 1997)

$$\begin{aligned} W_{66,1} &= 1 + (858 + 8\beta)\, y^{12} + (18678 - 24\beta)\, y^{14} + \cdots \text{ where } 0 \leq \beta \leq 778, \\ W_{66,2} &= 1 + 1690y^{12} + 7990y^{14} + \cdots \\ \text{and } W_{66,3} &= 1 + (858 + 8\beta)\, y^{12} + (18166 - 24\beta)\, y^{14} + \cdots \text{ where } 14 \leq \beta \leq 756, \end{aligned}$$

Recently, five new codes in $W_{66,1}$ are constructed in (Karadeniz et al., 2014b). For a list of known codes in The codes β =0, 1, 2, 3, 5, 6, 8, …, 11, 14, …, 18, 20, …, 54, 56, 59, 60, 62, …, 69, 71, …, 74, 76, 77, 78, 80, 83, 84, 86, 87, 92, 94 $W_{66,1}$. For a list of known codes in $W_{66,3}$ we refer to (Karadeniz and Yildiz, 2013).

We construct the codes with weight enumerators β =19, 61, 75, 79, 81, 82, 85, 88, 89, 90 and 100 in $W_{66,1}$. The extension in Theorem 3.4.5 is applied to the binary images of the codes constructed in Section 3.4.1 to obtain the new codes. The results are given in Table 3.15 where $\mathbf{1^{32}}$ denotes 32 successive 1s in X.

Table 3.15 New extremal binary self-dual codes with weight enumerators in $W_{66,1}$ by Theorem 3.4.5. (11 codes)

$\mathcal{L}_i$	The extension vector X	β in $W_{66,1}$
$\mathcal{M}_{17}$	10101010111001110010001101110010$\mathbf{1}^{\mathbf{32}}$	19
$\mathcal{M}_3$	11001100001011100111100101011111$\mathbf{1}^{\mathbf{32}}$	61
$\mathcal{L}_8$	10001011111111011011010110100100$\mathbf{1}^{\mathbf{32}}$	75
$\mathcal{L}_8$	00010101001111110101110111100101 01111001110010000111111001100000	79
$\mathcal{L}_3$	01100110100001001100000110100000 01001101100110110111110101111001	81
$\mathcal{L}_8$	01010110111110101100011010100111 00010101100101110100110101101001	82
$\mathcal{L}_3$	00111101100000000111010010101001 00100000111000001111100011000101 00	85
$\mathcal{C}_{64,80}$	11100000101011010111100100110110$\mathbf{1}^{\mathbf{32}}$	88
$\mathcal{C}_{64,80}$	10100100001110101110100111000001$\mathbf{1}^{\mathbf{32}}$	89
$\mathcal{C}_{64,80}$	00011111110111101111001110001011$\mathbf{1}^{\mathbf{32}}$	90
$\mathcal{C}_{64,80}$	11100001100000000000100001001101$\mathbf{1}^{\mathbf{32}}$	100

3.4.4 $\mathcal{R}_{2,1}$-extensions

In this section, we obtain new extremal binary self-dual codes by considering $\mathcal{R}_{2,1}$-extensions of the codes constructed in the previous section. The ring $\mathcal{R}_{2,2}$ can be considered as an extension of $\mathcal{R}_{2,1}$. Throughout this section, φ_u is the Gray map from $\mathcal{R}_{2,2}$ to $\mathcal{R}_{2,1}$ defined as $\varphi_u\left(a+bv\right)=\left(b,a+b\right)$ where $a,b\in\mathcal{R}_{2,1}$. We consider the extensions of the codes in Table 3.13 as well as the Gray images of the codes in Table 3.14 under φ_u. 39 new extremal binary self-dual codes of length 68 are obtained as the binary images of the extensions.

The weight enumerator of an extremal binary self-dual code of length 68 is characterized in (Dougherty et al., 1997) as follows:

$$\begin{aligned} W_{68,1} &= 1 + (442 + 4\beta)\, y^{12} + (10864 - 8\beta)\, y^{14} + \cdots \ , 104 \leq \beta \leq 1358, \\ W_{68,2} &= 1 + (442 + 4\beta)\, y^{12} + (14960 - 8\beta - 256\gamma)\, y^{14} + \cdots \end{aligned}$$

where $0 \leq \gamma \leq 11$ and $14\gamma \leq \beta \leq 1870 - 32\gamma$. Tsai et al. constructed new extremal self-dual binary codes of lengths 66 and 68 in (Tsai et al., 2008). Recently, 3 codes with previously unknown weight enumerators in $W_{68,1}$ were constructed in (Kaya and Yildiz, 2014). Together with the codes obtained in (Tsai et al., 2008), (Kaya and Yildiz, 2014) the existence of codes in $W_{68,1}$ are known for β =104, 117, 120, 122, 123, 125, ..., 168, 170, ..., 232, 234, 235, 236, 241, 255, 257, ..., 269, 302, 328, ..., 336, 338, 339, 345, 347, 355, 401.

We obtain a code with a weight enumerator $\beta = 169$ in $W_{68,1}$.

First codes with $\gamma = 4$ and $\gamma = 6$ in $W_{68,2}$ are constructed in (Karadeniz and Yildiz, 2013b). Recently, new codes in $W_{68,2}$ are obtained in (Kaya and Yildiz, 2016), (Kaya et al., 2015) and (Kaya and Yildiz, 2014) together with these, codes exists for $W_{68,2}$ when

$$\begin{aligned} \gamma &= 0,\ \beta = 44, ..., 154 \text{ or } \beta \in \{2m | m = 19,\ 20,\ 88,\ 102,\ 119,\ 136 \text{ or } 78 \leq m \leq 86\}\,; \\ \gamma &= 1,\ \beta = 49, 57, 59, ..., 160 \text{ or } \beta \in \{2m | m = 27,\ 28,\ 29,\ 95,\ 96 \text{ or } 81 \leq m \leq 89\}\,; \\ \gamma &= 2,\ \beta = 65, 68, 69, 71, 77, 81, 159 \text{ or } \beta \in \{2m | 37 \leq m \leq 68,\ 70 \leq m \leq 81\} \text{ or} \\ \beta &\in \{2m+1 | 42 \leq m \leq 69,\ 71 \leq m \leq 77\}\,; \\ \gamma &= 3,\ \beta = 101, 117, 123, 127, 133, 137, 141, 145, 147, 149, 153, 159, 193 \text{ or} \\ \beta &\in \{2m | m = 44, 45, 48, 50, 51, 52, 54, ..., 58, 61, 63, ..., 66, 68, ..., \\ & \quad 72, 74, 77, ..., 81, 88, 94, 98\}; \\ \gamma &= 4,\ \beta \in \{2m | m = 51,\ 55,\ 58,\ 60,\ 61,\ 62,\ 64{,}65,\ 67,\ ...,\ 71,\ 75,\ ...,\ 78,\ 80\} \text{ and} \\ \gamma &= 6 \text{ with } \beta \in \{2m | m = 69,\ 77,\ 78,\ 79,\ 81,\ 88\}\,. \end{aligned}$$

In this section, we construct the codes with weight enumerators in $W_{68,2}$ for $\gamma = 0$ and $\beta = 178$; $\gamma = 1$ and $\beta = 180$; $\gamma = 2$ and β =60, 62, 64, 66, 70, 72, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 186; $\gamma = 3$ and β =94, 107, 118, 120, 156, 168, 172, 180; $\gamma = 4$ and β =98, 104, 108, 112, 174, 194.

By considering $\mathcal{R}_{2,1}$-extensions of codes in Table 3.13 with respect to Theorem

3.4.6 we were able to obtain 14 new extremal binary self-dual codes, which are listed in Table 3.16.

Table 3.16 New codes in $W_{68,2}$ by Theorem 3.4.6 on $\mathcal{R}_{2,1}$ (14 codes).

$\mathcal{L}_i$	X	c	γ	β
$\mathcal{L}_4$	$(1313uu0133130u11)$	$1+u$	2	60
$\mathcal{L}_4$	$(1131uu011133u011)$	1	2	62
$\mathcal{L}_4$	$(0001u11uu3110300)$	1	2	64
$\mathcal{L}_4$	$(00u1u130u111u1u0)$	$1+u$	2	66
$\mathcal{L}_4$	$(uuu30330013101uu)$	$1+u$	2	70
$\mathcal{L}_4$	$(u0u1u13uu333u3u0)$	$1+u$	2	72
$\mathcal{L}_3$	$(u3000uu33u31u031)$	1	2	166
$\mathcal{L}_3$	$(u1u0u0u11u31uu13)$	$1+u$	2	170
$\mathcal{L}_3$	$(03u0u00330310u31)$	$1+u$	2	172
$\mathcal{L}_3$	$(u1uuu0u11u31u013)$	$1+u$	2	174
$\mathcal{L}_3$	$(01000u0110310013)$	$1+u$	2	176
$\mathcal{L}_3$	$(011300u031111313)$	1	3	156
$\mathcal{L}_3$	$(3u131011301u0u10)$	$1+u$	3	172
$\mathcal{L}_3$	$(103130333010u010)$	$1+u$	3	180

Example 3.4.7. Let $\mathcal{C}$ be the code obtained by applying Theorem 3.4.5 for $\varphi_u(M_4)$ over $\mathcal{R}_{2,1}$ with

$$X = (u, 1+u, 0, 0, 0, 1+u, 0, 0, 1, u, 0, 1, u, u, 1+u, 0, 1111111111111111)$$

and $c = 1+u$ then the binary image of the extension is an extremal binary self-dual code of length 68 with a weight enumerator $\beta = 169$ in $W_{68,1}$. The code $\mathcal{C}$ is the first extremal binary self-dual code with this weight enumerator.

Theorem 3.4.5 is applied to codes in Table 3.13 and $\mathcal{R}_{2,1}$-images of codes in Table 3.14. 24 new extremal binary self-dual codes of length 68 are obtained as Gray images of the extensions. Similar to the Section 3.4.1 lifts can be applied to the extensions. If X is a possible extension vector for a free self-dual code $\mathcal{C}$ over $\mathcal{R}_{2,1}$ then $\pi_u(X)$ is an extension vector for $\pi_u(\mathcal{C})$. In order to extend $\mathcal{C}$ we may lift an extension vector for $\pi_u(\mathcal{C})$. Theorem 3.1.4 gives an idea on which extension vectors to lift. For instance, a possible extension vector for the binary code $\pi_u(\varphi_u(M_{12}))$ is (00010111001100110000001000110011). By considering the lifts of this vector we were able to obtain new codes with weight enumerators corresponding to rare parameters $\gamma = 4$ and $\beta = 86$, 96 and 98. Those are listed in Table 3.17. Considering lifts reduces the workload remarkably from 4^{32} to 2^{32}.

Table 3.17 New codes in $W_{68,2}$ by Theorem 3.4.5 on $\mathcal{R}_{2,1}$ (24 codes).

Code	X	c	γ	β
$\mathcal{L}_3$	$(31u1u11133u10u113u10u33013010111)$	$1+u$	0	178
$\mathcal{L}_3$	$(10u1u033uu3u00u03101010uu10u3u0u)$	1	1	180
$\mathcal{L}_{12}$	$(11330u11u1103101u3u3101u31uu33u)$	1	2	164
$\mathcal{L}_8$	$(0uuu0011113u13u01303113033311003)$	1	2	168
$\mathcal{L}_8$	$(00000031313033u031u3333u33311003)$	$1+u$	2	178
$\mathcal{L}_8$	$(u0uuu033111033uu1301113u13331uu1)$	1	2	180
$\mathcal{L}_8$	$(u0u00011313u31u011u1113u33313u01)$	1	2	182
$\mathcal{L}_3$	$(u3uuu33uu10uu00103010u001u030u13)$	$1+u$	2	186
$\varphi_u(M_{12})$	$(13331031u0u1133u1111111111111111)$	1	3	94
$\varphi_u(M_4)$	$(11u301u33u0133u3u1u3u0uu010330uu)$	1	3	107
$\varphi_u(M_{12})$	$(11333u3100u1133u1331133313313133)$	$1+u$	3	118
$\varphi_u(M_{17})$	$(1310u30u33010000111111111111111 1)$	$1+u$	3	120
$\mathcal{L}_3$	$(uuu310u11u3u00u1uuu303u3u3u13333)$	1	3	164
$\mathcal{L}_3$	$(uu031u03103u0u01u00103u3u1u13111)$	$1+u$	3	166
$\mathcal{L}_3$	$(uuu11u031u3u0u01u003u3u303u31131)$	$1+u$	3	168
$\mathcal{L}_3$	$(u0031003301uuuu3u001u103u3u31331)$	$1+u$	3	174
$\varphi_u(M_{12})$	$(000101330011uu330u000u1u0011uu33)$	$1+u$	4	86
$\varphi_u(M_{12})$	$(uu01u1110u33u033uu0u003u0u31u013)$	$1+u$	4	96
$\varphi_u(M_{12})$	$(0001u3130u31uu1100uuuu1uu0130u31)$	$1+u$	4	98
$\varphi_u(M_{12})$	$(u3u3u1110u3310u31111111111111111)$	1	4	104
$\varphi_u(M_{12})$	$(u3010333003110031331133333113313)$	1	4	108
$\varphi_u(M_{12})$	$(u1u10313001110u33313331111331111)$	1	4	112
$\mathcal{L}_8$	$(00u00u33111u130011u31130111310u3)$	$1+u$	4	174
$\mathcal{L}_8$	$(u300033003u0uuu10303000u1uu10u31)$	1	4	194

Remark 3.4.8. The binary generator matrices of the new extremal binary self-dual codes of lengths 66 and 68 that are constructed in tables 3.15, 3.16 and 3.17 are available online at (Kaya and Tüfekçi, 2015).

CHAPTER 4

DIVISIBLE BINARY CODES FROM GRAY-HOMOGENEOUS MAPS OF CODES OVER $\mathcal{R}_{k,m}$

The homogeneous weight was introduced for codes over rings as an alternative to the Hamming weight. In this chapter, we consider the homogeneous weight on the ring family $\mathcal{R}_{k,m}$. Using the generating character characterization of the homogeneous weight we find a form for the homogeneous weight on $\mathcal{R}_{k,m}$. We then assign a value to the average weight γ, giving algebraic and combinatorial justifications. We construct the Gray-homogeneous map using Reed-Muller codes. Using the images of cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$ of different lengths with suitable k, m we are able to construct many optimal binary codes that are divisible with high levels of divisibility. The codes we have obtained are also quasicyclic with high indices and they are all self-orthogonal when $km \geq 4$. Thus we obtain many optimal, self-orthogonal quasicyclic binary codes, which have been shown to be of importance in (Townsend and Weldon, 1967), for their connection to difference sets and their near-BCH performance.

Recall that by $\mathcal{U}(\mathcal{R}_{k,m})$, we denote the units of $\mathcal{R}_{k,m}$ and by $\mathcal{D}(\mathcal{R}_{k,m})$, the set of non-units in $\mathcal{R}_{k,m}$. Moreover, we observe that $|\mathcal{U}(\mathcal{R}_{k,m})| = |\mathcal{D}(\mathcal{R}_{k,m})| = \frac{|\mathcal{R}_{k,m}|}{2}$ and that $\mathcal{U}(\mathcal{R}_{k,m}) = 1 + \mathcal{D}(\mathcal{R}_{k,m})$.

As a Frobenius ring, $\mathcal{R}_{k,m}$ has a generating character. It was shown in Chapter 2 that the generating character of $\mathcal{R}_{k,m}$ is given by

$$\begin{array}{cccc} \chi: & (\mathcal{R}_{k,m}, +) & \rightarrow & (\{-1, 1\}, .) \\ & \sum\limits_{\substack{0\leq i\leq k-1 \\ 0\leq j\leq m-1}} c_{ij} u^i v^j & \mapsto & (-1)^{w_H(c)} \end{array} ,$$

where $c = (c_{ij})$ is the binary vector consisting of all the coefficients c_{ij}'s of a typical element in $\mathcal{R}_{k,m}$, and $w_H(c)$ denotes the Hamming weight of c.

4.1 THE HOMOGENEOUS WEIGHT AND CORRESPONDING GRAY MAP ON $\mathcal{R}_{k,m}$

Homogeneous weights were first introduced in 1997 by Heise and Constantinescu in (Constantinescu and Heise, 1997). The theoretical work on the homogeneous weight and its form for frobenius rings can be found in such works as (Constantinescu and Heise, 1997), (Greferath and OSullivan, 2004) and (Honold, 2001). Different characterizations for the homogeneous weight on frobenius rings were given in these works. The Mobius function or the generating character of the ring seem to be the prevalent tools used in these constructions. The homogeneous weight is defined with two conditions for arbitrary finite rings as follows in (Greferath and OSullivan, 2004):

Definition 4.1.1. A real valued function ω on the finite ring R is called a (left) homogeneous weight if $\omega(0) = 0$ and the following is true:

(H1) For all $x, y \in R, Rx = Ry$ implies $\omega(x) = \omega(y)$ holds.

(H2) There exists a real number γ such that

$$\sum_{y \in Rx} \omega(y) = \gamma\, |Rx| \text{ for all } x \in R \backslash \{0\}$$

It has been shown that all Frobenius rings are equipped with a homogeneous weight. Different characterizations of the homogeneous weight for Frobenius rings have been given. Some of these use the Mobius function, and some use the generating character of Frobenius rings. We will use the following proposition from (Honold, 2001), which describes the homogeneous weight in terms of the generating character of the ring:

Proposition 4.1.2. (Honold, 2001) The homogeneous weight function for a finite ring R with generating character χ is of the form

$$\begin{array}{rccl} \omega: & R & \to & \mathbb{R} \\ & x & \mapsto & \gamma \left[1 - \frac{1}{|R^\times|} \sum\limits_{\rho \in R^\times} \chi(x\rho) \right], \end{array} \tag{4.1}$$

where $R^\times$, represents the group of units of R.

The γ that appears in the weight function is also called the average weight and further satisfies the following proeprty:

Proposition 4.1.3. (Honold, 2001) Let I be either a left or a right ideal of a finite Frobenius ring R, and let $y \in R$. Then $\sum\limits_{r \in I+y} \omega(r) = \gamma\,|I|$.

Applying Proposition 4.1.2 to the ring $\mathcal{R}_{k,m}$, we can obtain a form for the homogeneous weight for codes over the ring $\mathcal{R}_{k,m}$:

Theorem 4.1.4. The homogeneous weight for the ring $\mathcal{R}_{k,m}$ is of the form

$$\omega_{hom}(x) \begin{cases} 0 & x = 0, \\ 2\gamma, & x = u^{k-1}v^{m-1}, \\ \gamma, & otherwise. \end{cases}$$

Proof. Firstly, we put 0 in Equation 4.1 instead of x recalling that $\chi(0) = 1$ and $|\mathcal{U}(\mathcal{R}_{k,m})| = 2^{km-1}$, then we have:

$$\omega_{hom}(0) = \gamma \left[1 - \tfrac{1}{2^{km-1}} \sum_{\rho \in \mathcal{U}(\mathcal{R}_{k,m})} 1 \right] = 0.$$

Next, note that

$$u^{k-1}v^{m-1}\rho = u^{k-1}v^{m-1}$$

for all $\rho \in \mathcal{U}(\mathcal{R}_{k,m})$ and so we have $\chi(u^{k-1}v^{m-1}\rho) = (-1)$ for all $\rho \in \mathcal{U}(\mathcal{R}_{k,m})$. Putting $u^{k-1}v^{m-1}$ into Equation 4.1 we see that we have

$$\omega_{hom}(u^{k-1}v^{m-1}) = \gamma \left[1 - \tfrac{1}{2^{km-1}} \sum_{\rho \in \mathcal{U}(\mathcal{R}_{k,m})} (-1) \right] = 2\gamma.$$

Finally, for any element x in $\mathcal{R}_{k,m}$ such that $x \neq 0, u^{k-1}v^{m-1}$, since χ is a non-trivial when restricted to any non-zero ideal, we have

$$\sum_{\alpha \in \mathcal{R}_{k,m}} \chi(\alpha x) = 0. \tag{4.2}$$

On the other hand, since $1 + \alpha \in \mathcal{D}(\mathcal{R}_{k,m})$ while $\alpha \in \mathcal{U}(\mathcal{R}_{k,m})$ and $\chi((\alpha+1)x) = \chi(\alpha x + x) = \chi(\alpha x)\chi(x)$, we rewrite the sum 4.2 as follows:

$$\begin{aligned} 0 &= \sum_{\alpha \in \mathcal{R}_{k,m}} \chi(\alpha x) \\ &= \sum_{\alpha \in \mathcal{U}(\mathcal{R}_{k,m})} \chi(\alpha x) + \sum_{\alpha \in \mathcal{U}(\mathcal{R}_{k,m})} \chi(\alpha x)\chi(x) \\ &= (1 + \chi(x)) \sum_{\alpha \in \mathcal{U}(\mathcal{R}_{k,m})} \chi(\alpha x) \end{aligned}$$

Let us call the sum:

$$F(x) = \sum_{\alpha \in \mathcal{U}(\mathcal{R}_{k,m})} \chi(\alpha x).$$

While α runs through all the units of $\mathcal{R}_{k,m}$ and $\alpha\beta$ is also for all $\beta \in \mathcal{U}(\mathcal{R}_{k,m})$, we easily have $F(x) = F(\beta x)$. So, the Equation 4.1 can be written as

$$(1 + \chi(\alpha x))F(x) = 0, \forall \alpha \in \mathcal{U}(\mathcal{R}_{k,m}).$$

Now, assume that $\chi(\alpha x) = -1$ for all $\alpha \in \mathcal{U}(\mathcal{R}_{k,m})$. But, then we must have $\chi(\beta x) = 1$ for all $\beta \in \mathcal{D}(\mathcal{R}_{k,m})$. Since $x \neq u^{k-1}v^{m-1}$ and $\alpha x \neq u^{k-1}v^{m-1}$ for any $\alpha \in \mathcal{U}(\mathcal{R}_{k,m})$, we must have $\beta x = u^{k-1}v^{m-1}$ for some $\beta \in \mathcal{D}(\mathcal{R}_{k,m})$ because of the ideal generated by x must contain $u^{k-1}v^{m-1}$. But this is a contradiction since $\chi(u^{k-1}v^{m-1}) = -1$. That is,

$$\sum_{\alpha \in \mathcal{U}(\mathcal{R}_{k,m})} \chi(\alpha x) = 0.$$

Thus we obtain

$$\omega_{hom}(x) = \gamma \left[1 - \tfrac{1}{2^{km-1}} 0\right] = \gamma$$

for all $x \neq 0, u^{k-1}v^{m-1}$. □

In most works related to the homogeneous weight, the average weight γ is unassigned. Having settled the form of the homogeneous weight, we now want to choose a specific value for γ so that we can find a distance preserving isometry from $\mathcal{R}_{k,m}$ to $\mathbb{F}_2^s$ for a suitable s. We will call this map the Gray-homogeneous map. We recall some of the work done in this direction. An inductive algebraic construction of a distance preserving Gray map was given by Yildiz from Galois rings with the homogeneous distance to the field of prime size with the Hamming distance in (Yildiz, 2006) as well as a combinatorial construction of the Gray map for Galois rings by using Affine geometries in (Yildiz, 2009). Later, projective geometries $PG_n(q)$ were used to construct the Gray map for linear codes over a family of Frobenius rings in (Pasa and Yildiz, 2014). Considering the hyperplanes and projective spaces, the work in (Pasa and Yildiz, 2014) suggests the use of the projective geometry $PG_{km-1}(\mathbb{F}_2)$ in our work. This requires the s to be 2^{km-1}. However, as was later done in (Yildiz and Kelebek, 2014), the first order Reed-Muller codes seem to give us a more constructive method of finding this map.

We recall that the first order Reed-Muller codes $RM(1,m)$ are a family of binary linear codes of parameters $[2^m, m+1, 2^{m-1}]$, defined for each positive integer m. The important property of the first order Reed-Muller codes is that there is one codeword with weight 2^m and all the other non-zero codewords have weight 2^{m-1}. Because of the structure of the homogeneous weight, it is clear that first order Reed-Muller codes can be used to construct the Gray map. Since $|\mathcal{R}_{k,m}| = 2^{km}$, we clearly need $RM(1,s)$ where $s+1 = km$. Thus, to define a distance preserving Gray map for the homogeneous weight on $\mathcal{R}_{k,m}$ we use the first order Reed-Muller codes $RM(1, km-1)$, of length 2^{km-1}. This coincides with length of the image suggested in (Pasa and Yildiz, 2014), which adds an added motivation for the choice of γ for us. Thus we choose $\gamma = 2^{km-2}$. This means that for us, the homogeneous weight will have the following form:

$$\omega_{hom}(x) \begin{cases} 0 & \text{if } x = 0, \\ 2^{km-1} & \text{if } x = u^{k-1}v^{m-1}, \\ 2^{km-2} & \textit{otherwise.} \end{cases}$$

Now, in order to define the Gray-homogeneous map on $\mathcal{R}_{k,m}$, we first note that $\mathcal{R}_{k,m}$ can be viewed as an $\mathbb{F}_2$-vector space with a basis

$$\beta = \{1, u, \ldots, u^{k-1}, v, \ldots, v^{m-1}, uv, \ldots, u^{k-1}v^{m-1}\}.$$

$RM(1, 2^{km} - 1)$ has exactly km basis elements, which are binary vectors of length 2^{km-1}, including $(1,1,\ldots,1)$. So, we first let ϕ_{hom} map elements of the minimal ideal $I_{u^{k-1}v^{m-1}}$ to the two elements of $RM(1, km-1)$, given by $(0,0,\ldots,0)$ and $(1,1,\ldots,1)$, respectively. The remaining elements of the basis are mapped to basic generators of $RM(1, km-1)$ except $(1,1,\ldots,1)$. Taking all the possible linear combinations, we extend the map ϕ_{hom} to $\mathcal{R}_{k,m}$. The map is then extended in the natural way $\mathcal{R}^n_{k,m}$:

$$\begin{aligned} \phi_{hom}: \quad (\mathcal{R}_{k,m})^n \quad & \rightarrow \quad \mathbb{F}_2^{(2^{km-1})n} \\ \sum_{\substack{0 \le i \le k-1 \\ 0 \le j \le m-1}} \bar{c}_{ij} u^i v^j \quad & \mapsto \quad \sum_{\substack{0 \le i \le k-1 \\ 0 \le j \le m-1}} \bar{c}_{ij} \phi_{hom}(u^i v^j). \end{aligned} \tag{4.3}$$

The properties of the Reed-Muller codes then result in the following:

Theorem 4.1.5. ϕ_{hom} is a distance preserving isometry from ($\mathcal{R}_{k,m}^{n}$, homogeneous distance) to ($\mathbb{F}_2^{2^{km-1}n}$, Hamming distance). Thus if C is a linear code over $\mathcal{R}_{k,m}$ of length n and minimum homogeneous weight d, then $\phi_{hom}(C)$ is a binary linear code of length $2^{km-1}n$, and minimum Hamming weight d. Moreover, the Homogeneous weight distribution of C is the same as the Hamming weight distribution of $\phi_{hom}(C)$.

We finish this section with a few examples:
The homogeneous weight for $\mathcal{R}_{2,1} = \mathbb{F} + u\mathbb{F}_2$ coincides with the Lee weight defined on $\mathbb{F}_2 + u\mathbb{F}_2$ and the Gray-homogeneous map also coincides with the usual Gray map for $\mathbb{F}_2 + u\mathbb{F}_2$, that is well-known in the literature.

Example 4.1.6. Let us consider $\mathcal{R}_{3,1} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. The homogeneous weight then is found to be

$$\omega_{hom}(x) \begin{cases} 0 & \text{if } x = 0, \\ 4 & \text{if } x = u^2, \\ 2 & \textit{otherwise.} \end{cases}$$

The Gray-homogeneous map is described on the basis elements as $\phi_{hom}(u^2) = (1,1,1,1)$, $\phi_{hom}(u) = (1,1,0,0)$, $\phi_{hom}(1) = (1,0,1,0)$. The map is then extended to $\mathcal{R}_{3,1}$ by taking the $\mathbb{F}_2$-linear combinations as follows:

$$\begin{array}{ll} \phi_{hom}(0) = (0,0,0,0) & \phi_{hom}(1+u) = \phi_{hom}(1) + \phi_{hom}(u) = (0,1,1,0) \\ \phi_{hom}(1) = (1,0,1,0) & \phi_{hom}(1+u^2) = \phi_{hom}(1) + \phi_{hom}(u^2) = (0,1,0,1) \\ \phi_{hom}(u) = (1,1,0,0) & \phi_{hom}(u+u^2) = \phi_{hom}(u) + \phi_{hom}(u^2) = (0,0,1,1) \\ \phi_{hom}(u^2) = (1,1,1,1) & \phi_{hom}(1+u+u^2) = \phi_{hom}(1+u) + \phi_{hom}(u^2) = (1,0,0,1) \end{array}$$

Consequently we have

$$\phi_{hom}(a + bu + cu^2) = (a+b+c, b+c, a+c, c), \quad a, b, c \in \mathbb{F}_2.$$

Example 4.1.7. Let us consider $\mathcal{R}_{3,2} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + u^2v\mathbb{F}_2$. By the similar way, the homogeneous weight of u^2v found to be 32 in the ring $\mathcal{R}_{3,2}$ and other non-zero elements of $\mathcal{R}_{3,2}$ have homogeneous weight of 16. Then the basis elements of $\mathcal{R}_{3,2}$ are mapped to basic generators of $RM(1,5)$ as follows:

$$\begin{aligned}
\phi_{hom}(u^2v) &= (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)\\
\phi_{hom}(uv) &= (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)\\
\phi_{hom}(v) &= (1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)\\
\phi_{hom}(u^2) &= (1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,0)\\
\phi_{hom}(u) &= (1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0)\\
\phi_{hom}(1) &= (1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1,0).
\end{aligned}$$

So, the Gray-homogenous map for the ring $\mathcal{R}_{3,2}$ is obtained by taking the $\mathbb{F}_2-$linear combinations as follows:

$$\begin{aligned}
&\phi_{hom}(a_1 + a_2u + a_3u^2 + b_1v + b_2uv + b_3u^2v) = (a_1 + a_2 + a_3 + b_1 + b_2 + b_3,\\
&a_2 + a_3 + b_1 + b_2 + b_3, a_1 + a_3 + b_1 + b_2 + b_3, a_3 + b_1 + b_2 + b_3,\\
&a_1 + a_2 + b_1 + b_2 + b_3, a_2 + b_1 + b_2 + b_3, a_1 + b_1 + b_2 + b_3, b_1 + b_2 + b_3,\\
&a_1 + a_2 + a_3 + b_2 + b_3, a_2 + a_3 + b_2 + b_3, a_1 + a_3 + b_2 + b_3, a_3 + b_2 + b_3,\\
&a_1 + a_2 + b_2 + b_3, a_2 + b_2 + b_3, a_1 + b_2 + b_3, b_2 + b_3,\\
&a_1 + a_2 + a_3 + b_1 + b_3, a_2 + a_3 + b_1 + b_3, a_1 + a_3 + b_1 + b_3, a_3 + b_1 + b_3,\\
&a_1 + a_2 + b_1 + b_3, a_2 + b_1 + b_3, a_1 + b_1 + b_3, b_1 + b_3,\\
&a_1 + a_2 + a_3 + b_3, a_2 + a_3 + b_3, a_1 + a_3 + b_3, a_3 + b_3,\\
&a_1 + a_2 + b_3, a_2 + b_3, a_1 + b_3, b_3), \quad a_i, b_i \in \mathbb{F}_2
\end{aligned}$$

The Gray-homogeneous map for the ring $\mathcal{R}_{k,m}$ when $m \geq 2$ is not practical because of large length.

4.2 DIVISIBLE CODES OVER $\mathcal{R}_{k,m}$

Divisible codes were first introduced by Ward in 1981 in (Ward, 1981).

Definition 4.2.1. A code is divisible if the weights of all the codewords have a common divisor $\Delta > 1$.

The replicated code, constructed by repeating each coordinate of a selected code a certain number of times is the simplest divisible code. Moreover, Ward proved that a divisible code is equivalent to a Δ-fold replicated code if the divisor Δ of the code is relatively prime to the field characteristic in (Ward, 1981).

Definition 4.2.2. A divisible code is said to be of *"level e"*, if the greatest divisor of weights of codewords in C equals p^e for some integer $e \geq 1$.

Reed-Muller codes are also an example of divisible codes, by the following theorem in (MacWilliams and Sloane, 1978):

Theorem 4.2.3. The weight of every codeword in $RM(r,m)$ is divisible by $2^{[(m-1)/r]}$.

Because of the homogeneous weight on $\mathcal{R}_{k,m}$ we can easily observe the following:

Theorem 4.2.4. Any linear code C over $\mathcal{R}_{k,m}$ is homogeneous-divisible with $\Delta \geq \gamma$. In particular with our choice of γ, we see that if C is a linear code over $\mathcal{R}_{k,m}$ of length n, then $\phi_{hom}(C)$ is a divisible binary code of length $2^{km-1}n$ with $\Delta \geq 2^{km-2}$.

It is well known that binary linear divisible codes with $\Delta = 2^k$, $k \geq 2$ are also self-orthogonal. Thus we have the following corollary:

Corollary 4.2.5. Let C be any linear code over $\mathcal{R}_{k,m}$. Then $\phi_{hom}(C)$ is a binary self-orthogonal linear code if $km \geq 4$.

In what follows, we will search for binary divisible codes with various divisors from the Gray-homogeneous images of cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$ of some lengths. Because of the increased size of the rings, we will mostly consider the rings $\mathcal{R}_{3,1}$, $\mathcal{R}_{4,1}$ and $\mathcal{R}_{5,1}$. For these rings, the Gray homogeneous maps are given as follows:

$$\phi_{hom}(x) = \quad (a_1 + a_2 + a_3, a_2 + a_3, a_1 + a_3, a_3)$$

for $x = a_1 + a_2 u + a_3 u^2 \in \mathcal{R}_{3,1}$ which is given above,

$$\begin{aligned}\phi_{hom}(y) = \quad & (a_1 + a_2 + a_3 + a_4, a_2 + a_3 + a_4, a_1 + a_3 + a_4, \\ & a_3 + a_4, a_1 + a_2 + a_4, a_2 + a_4, a_1 + a_4, a_4)\end{aligned}$$

for $y = a_1 + a_2 u + a_3 u^2 + a_4 u^3 \in \mathcal{R}_{4,1}$ and

$$\begin{aligned}\phi_{hom}(z) = \quad & (a_1 + a_2 + a_3 + a_4 + a_5, a_2 + a_3 + a_4 + a_5, a_3 + a_4 + a_5, \\ & a_1 + a_3 + a_4 + a_5, a_1 + a_2 + a_4 + a_5, a_2 + a_4 + a_5, \\ & a_1 + a_4 + a_5, a_4 + a_5, a_1 + a_2 + a_3 + a_5, a_2 + a_3 + a_5, \\ & a_1 + a_3 + a_5, a_3 + a_5, a_1 + a_2 + a_5, a_2 + a_5, a_1 + a_5, a_5)\end{aligned}$$

for $z = a_1 + a_2 u + a_3 u^2 + a_4 u^3 + a_5 u^4 \in \mathcal{R}_{5,1}$. The examples that we give are mainly optimal.

4.2.1 Divisible Cyclic Codes Over $\mathcal{R}_{k,m}$

Recall that a linear code C of length n over $\mathcal{R}_{k,m}$ is a cyclic code if $\tau(\bar{c}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ for all $\bar{c} = (c_0, c_1 \ldots, c_{n-1}) \in C$, where τ is the cyclic shift. Considering the polynomial correspondence

$$\begin{array}{rlcl} \pi : & (\mathcal{R}_{k,m})^n & \rightarrow & \mathcal{R}_{k,m}[x] \\ & \bar{c} = (c_0, c_1 \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} \end{array}$$

The cyclic shift corresponds to multiplying by x modulo $x^n - 1$. Thus it is clear that a code C of length n over $\mathcal{R}_{k,m}$ is cyclic if and only if $\pi(C)$ is an ideal in the ring $\mathcal{R}_{k,m}[x]/(x^n - 1)$. There are a lot of results concerning the structural properties of cyclic codes over rings, in particular over finite chain rings. The rings that we consider for the purposes in this section, $\mathcal{R}_{3,1}$, $\mathcal{R}_{4,1}$ being finite chain, we are not going to go into the theoretical aspects of cyclic codes. Instead we will demonstrate how some one-generator cyclic codes over these rings lead to optimal divisible binary linear codes under the Gray-homogeneous map.

Theorem 4.2.6. The Gray-homogeneous image of a cyclic code over $\mathcal{R}_{k,m}$ is a 2^{km-1}-quasicyclic binary code.

Proof. Let $\bar{c} \in \mathcal{R}_{k,m}^n$. Then

$$\phi_{hom} \circ \tau(\bar{c}) = \quad (\phi_{hom}(c_{n-1}), \phi_{hom}(c_0), \ldots, \phi_{hom}(c_{n-2})) \tag{4.4}$$

on the other hand

$$\phi_{hom}(\bar{c}) = \quad (\phi_{hom}(c_0), \ldots, \phi_{hom}(c_{n-2}), \phi_{hom}(c_{n-1})) \tag{4.5}$$

where each $\phi_{hom}(c_i)$ is of length 2^{km-1}. Hence we obtain equation 4.4 applying the cyclic shift 2^{km-1} times to equation 4.5. That is,

$$\tau^{2^{km-1}} \circ \phi_{hom}(\bar{c}) = \quad (\phi_{hom}(c_{n-1}), \phi_{hom}(c_0), \ldots, \phi_{hom}(c_{n-2})).$$

Hence we obtain:

$$\phi_{hom} \circ \tau(\bar{c}) = \quad \tau^{2^{km-1}} \circ \phi_{hom}(\bar{c}). \tag{4.6}$$

Let C be a cyclic code over $\mathcal{R}_{k,m}$, then we know $\tau(C) = C$. Thus,

$$\phi_{hom}(\tau(C)) = \phi_{hom}(C). \tag{4.7}$$

Applying the Equation 4.6 to 4.7 we get:

$$\phi_{hom}(C) = \phi_{hom}(\tau(C)) = \tau^{2^{km-1}} \circ \phi_{hom}(C).$$

□

The binary codes that we have constructed have the additional property that they are 4-quasicyclic or 8-quasicyclic according as we are on the ring $\mathcal{R}_{3,1}$ or $\mathcal{R}_{4,1}$.

Table 4.1 Divisible cyclic codes over $\mathcal{R}_{3,1}$ of length n and the binary images.

n	$g(x)$	$\phi_{hom}(\langle g(x) \rangle)$	Δ	*level*
3	$u^2x + u^2x^2$	$[12, 2, 8]$	8	3
3	$1 + x^2$	$[12, 3, 6]$	6	1
4	$ux + u^2x^2 + ux^3$	$[16, 4, 8]$	8	3
4	$1 + x + x^2 + (1 + u^2)x^3$	$[16, 5, 8]$	8	3
4	$x + ux^2 + (u + 1)x^3$	$[16, 6, 6]$	2	1
4	$x^2 + x^3$	$[16, 9, 4]$	2	1
4	x^3	$[16, 12, 2]$	2	1
5	$x^3 + x^4$	$[20, 12, 4]$	2	1
5	$x^3 + (1 + u^2)x^4$	$[20, 13, 4]$	2	1
6	$ux + ux^2 + u^2x^3 + ux^4 + (u + u^2)x^5$	$[24, 4, 12]$	4	2
6	$x^4 + x^5$	$[24, 15, 4]$	2	1
6	$x^4 + (1 + u)x^5$	$[24, 16, 4]$	2	1
7	$u^2x^2 + u^2x^4 + u^2x^5 + u^2x^6$	$[28, 3, 16]$	16	4
7	$1 + x + x^2 + (1 + u^2)x^3 + x^4 + (1 + u^2)x^5 + (1 + u^2)x^6$	$[28, 6, 12]$	2	1
7	$x^2 + x^4 + (1 + u^2)x^5 + (1 + u^2)x^6$	$[28, 12, 8]$	4	2
7	$x^5 + (1 + u^2)x^6$	$[28, 19, 4]$	2	1
8	$x^3 + ux^5 + ux^6 + x^7$	$[32, 14, 8]$	2	1
8	$x^4 + x^5 + (1 + u)x^6 + (1 + u + u^2)x^7$	$[32, 15, 8]$	2	1

Table 4.2 Divisible cyclic codes over $\mathcal{R}_{4,1}$ of length n and the binary images.

n	$g(x)$	$\phi_{hom}(\langle g(x)\rangle)$	Δ	*level*
2	$u+ux$	$[16,3,8]$	8	3
3	$u^3x+u^3x^2$	$[24,2,16]$	16	4
3	$x+x^2$	$[24,8,8]$	4	2
3	$x+(1+u^3)x^2$	$[24,9,8]$	4	2
4	$u^2x+u^3x^2+u^2x^3$	$[32,4,16]$	16	4
4	$1+x+(1+u^3)x^2+(1+u^3)x^3$	$[32,5,16]$	16	4
4	$1+x+x^2+(1+u^3)x^3$	$[32,6,16]$	16	4
6	$u^3x+u^3x^2+u^3x^4+u^3x^5$	$[48,2,32]$	32	5
6	$u^2x+u^2x^2+u^3x^3+u^2x^4+(u^2+u^3)x^5$	$[48,4,24]$	8	3

Remark 4.2.7. All the binary codes given in the above tables are optimal or best known codes, meaning that they either attain upper bounds or have the best known minimum distance according to (Grassl, 2007). The codes given in Table 4.2 have the additional property that they are all self-orthogonal quasicyclic codes of the best possible parameters.

4.2.2 Divisible constacyclic codes over $\mathcal{R}_{k,m}$

Constacyclic codes are a natural generalization of cyclic codes. For a unit $\alpha \in R$, a constacyclic shift on R^n is given by $\tau_\alpha(c_0, c_1, \ldots, c_{n-1}) = (\alpha c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. A code C over R is said to be α-constacyclic if it is invariant under the α-constacyclic shift, i.e., $\tau_\alpha(C) = C$. In exactly the same way as the cyclic codes, constacylic codes are also endowed with an algebraic structure. More precisely, $\alpha-$constacyclic codes over R are in one-to-one correspondence with ideals in the quoient ring $R[x]/(x^n-\alpha)$. Structural properties of constacyclic codes over different alphabets have been studied quite extensively in the literature. In (Karadeniz and Yildiz, 2011), Karadeniz and Yildiz studied $(1+v)$-constacyclic codes over $\mathcal{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. It is well known that if R is a ring of characteristic 2, and $\alpha \in R$ satisfies $\alpha^2 = 1$, then α-constacyclic codes over R of odd lengths are also cyclic. In $\mathcal{R}_{2,2}$ as well as in the latter generalizations R_k, (Yildiz and Kelebek, 2014), every unit in the ring satisfies this property. So, constacyclic codes over these rings of odd lengths are just cyclic. However, the cases that we look at, namely in $\mathcal{R}_{3,1}$, $\mathcal{R}_{4,1}$ and $\mathcal{R}_{5,1}$ this is not true. If we take $\alpha = 1 + u$, then $(1 + u)^2 \neq 1$ in the rings mentioned above. Thus, the constacyclic codes we study are in general different than cyclic codes.

In what follows, we have listed some examples of one-generator $(1+u)$-constacyclic codes over $\mathcal{R}_{k,m}$ and their homogeneous Gray images, which turn out to be divisible, optimal and in some cases self-orthogonal:

Table 4.3 Divisible $(1 + u)$-constacyclic codes over $\mathcal{R}_{k,1}$ of length n and the binary images.

$\mathcal{R}_{k,1}$	n	generator of the code	$\phi_{hom}(\langle g(x)\rangle)$	Δ	*level*
$\mathcal{R}_{3,1}$	6	$(0, u^2, u^2, 0, u^2, u^2)$	$[24, 2, 16]$	16	4
$\mathcal{R}_{3,1}$	6	$(0, 0, 0, 1, u, 1)$	$[24, 15, 4]$	2	1
$\mathcal{R}_{3,1}$	7	$(0, 0, u^2, 0, u^2, u^2, u^2)$	$[28, 3, 16]$	16	4
$\mathcal{R}_{3,1}$	7	$(1, u + 1, 1, u + 1, 1, u^2 + u + 1, u^2 + 1)$	$[28, 6, 12]$	2	1
$\mathcal{R}_{3,1}$	7	$(0, 0, 1, 0, 1, u + 1, 1)$	$[28, 12, 8]$	4	2
$\mathcal{R}_{3,1}$	7	$(0, 0, 0, 0, 0, 1, u^2 + u + 1)$	$[28, 19, 4]$	2	1
$\mathcal{R}_{3,1}$	9	$(0, u^2, u^2, 0, u^2, u^2, 0, u^2, u^2)$	$[36, 2, 24]$	24	
$\mathcal{R}_{4,1}$	2	(u^2, u^2)	$[16, 3, 8]$	8	3
$\mathcal{R}_{4,1}$	3	$(0, 1, u + 1)$	$[24, 8, 8]$	4	2
$\mathcal{R}_{4,1}$	3	$(0, 1, u^3 + u + 1)$	$[24, 9, 8]$	4	2
$\mathcal{R}_{4,1}$	5	$(1, u^3 + u^2 + u + 1, u^2 + 1, u + 1, 1)$	$[40, 4, 20]$	20	
$\mathcal{R}_{4,1}$	7	$(0, 0, u^3, 0, u^3, u^3, u^3)$	$[56, 3, 32]$	32	5
$\mathcal{R}_{5,1}$	3	$(0, u^4, u^4)$	$[48, 2, 32]$	32	5
$\mathcal{R}_{5,1}$	3	$(u, u^2 + u, u^3 + u)$	$[48, 4, 24]$	24	
$\mathcal{R}_{5,1}$	3	$(1, 1 + u + u^4, 1 + u^2)$	$[48, 5, 24]$	24	
$\mathcal{R}_{5,1}$	5	$(1, u^3 + u^2 + u + 1, u^4 + u^2 + 1, u + 1, u^4 + 1)$	$[80, 5, 40]$	40	

Remark 4.2.8. If C is an α-constacyclic code over $\mathcal{R}_{k,m}$, then $\phi_{hom}(C)$ might not be a 2^{km-1}-quasicyclic binary code, however it can easily be shown that $\phi_{hom}(C)$ is equivalent to a 2^{km-1}-quasicyclic binary code. Thus all the codes given in the above table are equivalent to binary quasicyclic codes and they are also self-orthogonal when $\Delta \geq 4$.

4.2.3 Some results on divisible quasicyclic codes over $\mathcal{R}_{k,m}$

Quasicyclic codes are another generalization of cyclic codes and have generated a lot of interest. They have algebraic structure and they also satisfy a modified version of the Gilbert-Varshamov bound. Many optimal good binary codes are quasicyclic. A lot of good codes have been constructed using quasicyclic codes over different alphabets, such as (Aydin et al., 2013) and (Chen, 1994). A definition can be given from (MacWilliams and Sloane, 1978):

Definition 4.2.9. A code C of length n is called $\ell-$quasicyclic if $\ell | n$ and $\tau^{\ell}(C) = C$.

Note that when $\ell = 1$, 1-quasicyclic codes are just cyclic codes. Structurally, the generator matrix of a t generator $\ell-$quasicyclic code can be shown to be of the following form:

$$\begin{bmatrix} C_{11} & C_{12} & \dots & C_{1,\ell} \\ C_{21} & C_{22} & \dots & C_{2,\ell} \\ \vdots & \vdots & \vdots & \vdots \\ C_{t,1} & C_{t,2} & \dots & C_{t,\ell} \end{bmatrix}$$

where C_{ij} are $m \times m$ circulant matrices. In such a case, the length n of the $\ell-$quasicyclic code C is $m \times \ell$. We refer to (Townsend and Weldon, 1967) and (Chen, 1994) for more information on quasicyclic codes.

We have searched through one generator ℓ-quasicyclic codes over $\mathcal{R}_{k,m}$ to get divisible codes of various lengths. We have listed in the following table, divisible, optimal binary codes obtained as the ϕ_{hom}-images of quasi cyclic codes over $\mathcal{R}_{k,m}$:

Table 4.4 Divisible ℓ-quasicyclic codes over $\mathcal{R}_{k,1}$ and the binary images.

$\mathcal{R}_{k,1}$	ℓ	generator of the code	$\phi_{hom}(\langle g(x)\rangle)$	Δ	*level*
$\mathcal{R}_{3,1}$	3	$(0,1,1,0,1,1+u^2,u,u,u^2)$	$[36,2,24]$	24	
	3	$(0,u,u,0,u,u^2+u,u,u,u^2)$	$[36,5,16]$	4	2
	3	$(0,1,1,0,u,u,1,u^2,u^2+1)$	$[36,6,16]$	4	2
	3	$(0,1,1,0,1,u^2+1,u,u,u^2)$	$[36,7,16]$	4	2
	3	$(1,1,u^2+1,u^2+1,1,1,u^2+1,u^2+1,1,1,u^2+1,u^2+1)$	$[48,4,24]$	24	
	3	$(0,u,u^2,u^2+u,1,1,u^2+1,u^2+1,1,u+1,1,u+1)$	$[48,5,24]$	8	3
	2	$(0,1,1,u^2,1,u^2+1,u^2+u,1,u^2+u+1,u,1,u+1)$	$[48,6,24]$	8	3
	2	$(0,0,0,u,u,0,u^2,u,u,u^2)$	$[40,8,16]$	8	3
	3	$(1,1,1,1,u^2+1,1,1,1,u^2+1,u^2+1,1,1,u^2+1,1,u^2+1)$	$[60,7,28]$	2	1
	3	$(0,0,0,1,1,0,u,1,u,1,1,u+1,u^2,1,u^2+u+1)$	$[60,12,24]$	4	2
$\mathcal{R}_{4,1}$	2	$(1,1,u^3+1,u^3+1,1,1,u^3+1,u^3+1)$	$[64,5,32]$	32	5
	2	$(1,1,1,u^3+1,1,1,1,u^3+1)$	$[64,6,32]$	32	5
	2	$(1,1,u^2+1,u^3+u^2+1,1,1,u^3+u^2+1,u^2+1)$	$[64,7,32]$	32	5
	3	$(1,1,u^3+1,1,1,u^3+1,1,1,u^3+1)$	$[72,5,36]$	12	
	3	$(1,1,1,u^3+1,1,1,1,u^3+1,1,1,1,u^3+1)$	$[96,6,48]$	48	

Remark 4.2.10. It can easily be shown that the Gray-homogeneous image of an ℓ-quasicyclic code is a $(2^{km-1}\ell)$-quasicyclic binary code. So, the binary codes constructed above are all $(2^{km-1}\ell)$-quasicyclic for the appropriate values of ℓ, k, m. In all but one of the cases they are self-orthogonal as well. Thus almost all the codes given in the above table are optimal self-orthogonal quasicyclic codes.

4.2.4 Griesmer Codes

The Griesmer bound, introduced in (Griesmer, 1960) is one of the many bounds that exist for codes, and can be stated as follows: For a linear $[n,k,d]$-code over $\mathbb{F}_q$, we have

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil, \tag{4.8}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. Linear codes meeting this bound are called Griesmer Codes.

Let us consider a one generator cyclic code C_{km} of length n over $\mathcal{R}_{k,m}$ with the generator vector $(1,1,\dots,1)$. This is actually the repetition code. It is clear to see that the Gray-homogeneous image of this code is a binary linear code of the parameters $[2^{km-1}n, km, 2^{km-2}n]$. Thus, the images of this code are binary divisible codes with divisor $2^{km-2}n$. We may construct many optimal linear codes, which otherwise may have complicated constructions, in a relatively easier way from C_{km}. As an illustration of this idea, consider, the Gray-homogeneous images of C_{51} and C_{32} of length n. These will be binary codes of parameters $[16n, 5, 8n]$ and $[32n, 6, 16n]$, respectively. According to (Grassl, 2007), these codes are all optimal when $1 \leq n \leq 8$.

We finish this section by noticing that $\phi_{hom}(C_{km})$s are Griesmer codes, when $n = 1$, for all k and m.

Theorem 4.2.11. The binary linear code $\phi_{hom}(C_{km})$ is a Griesmer code for $n = 1$, and for all k, m.

Proof. When $n = 1$, $\phi_{hom}(C_{km})$ is a km-dimensional linear code with minimum distance 2^{km-2}. Calculating the Griesmer lower bound according to 4.8, we see that the lower bound must be

$$\begin{aligned}\sum_{i=0}^{km-1} \lceil \frac{d}{2^i} \rceil &= \lceil \frac{2^{km-2}}{2^0} \rceil + \lceil \frac{2^{km-2}}{2^1} \rceil + \cdots + \lceil \frac{2^{km-2}}{2^{km-2}} \rceil + \lceil \frac{2^{km-2}}{2^{km-1}} \rceil \\ &= 2^{km-2} + 2^{km-3} + \cdots + 1 + 1 \\ &= (2^{km-1} - 1) + 1 = 2^{km-1},\end{aligned}$$

which is precisely the length of $\phi_{hom}(C_{km})$, when $n = 1$. □

CHAPTER 5

CONCLUSION

Codes over rings have been an integral part of Algebraic Coding Theory over the recent years. The increased activity around this topic is justified by many interesting results obtained through codes over rings as well as many applications. With an intricate algebraic structure compared to fields, they sometimes fill the gaps caused by the restrictive nature of fields. Recent years have shown for example, that many new extremal binary self-dual codes have been found through codes over rings of characteristic 2. These codes were not found using the classical construction methods over the fields oft-applied previously. What started with an $\mathbb{Z}_4$-duality of certain non-linear binary codes has now led to an avalanche of works in this area. The many different applications suggest that this interest in this area will continue to be one of the focal parts for coding theorists in the future. Because of Wood's studies in this field, Frobenius rings have been the center of attention in codes over rings. In fact, looking over the literature, we see that many of the works consider finite, commutative Frobenius rings, and in some cases, local Frobenius rings are considered. This choice is justified because of many nice properties of these rings. The existence of a generating character, which can be found without much difficulty, allows one to consider MacWilliams identities and in our case for example, allows one to characterize the homogeneous weights.

The Hamming weight is not a focal weight for codes over rings. Instead many different weights have been suggested. The Lee weight, the Euclidean weight and the homogeneous weight are amongst these. The common theme in working with codes over rings has been as follows: describe the ring explicitly through its units, non units and ideals. Define a weight (Lee, Homogeneous etc.) with associated Gray maps that map codes over the ring to codes over the ambient residue field of the ring. Thus consider different aspects of coding theory within this context.

In this thesis, we followed the some script for the ring that we described as $\mathcal{R}_{k,m}$. $\mathcal{R}_{k,m}$ is a generalization of some oft-studied rings in the literature over the recent years. The characteristic is 2, and it is a family of finite-commutative, local Frobenius rings but are not (usually) finite chain or principal ideal rings. These rings are endowed with an orthogonality-preserving, linear bijective Gray map to the binary field, which allows us to work on self-dual codes. Defining the Lee weight in terms of this Gray map and using the construction methods such as the double circulant, bordered double circulant, four circulant constructions and also using extension methods we obtained extremal binary self-dual codes of lengths 36, 64, 66, 68 and 72, and gave a different construction for Golay code. We also used quadratic circulant matrices to obtain extremal binary self-dual codes of lengths 20, 40, 44 and 66.

The first main part of the thesis being the applications to self-dual codes. We focused on the homogeneous weight in the second main part. After a characterization of the homogeneous weight using the generating character, we were able to find a linear, distance preserving Gray map using first order Reed-Muller codes. The binary images of codes over $\mathcal{R}_{k,m}$ under the Gray-homogeneous map have many interesting desirable properties, such as being divisible with high levels of divisibility and being self-orthogonal. Considering cyclic and quasicyclic codes over $\mathcal{R}_{k,m}$, we were able to get many optimal binary codes that are divisible, self-orthogonal quasicyclic codes. self-orthogonal quasicyclic codes, being of importance in communications, we find a further justification of working on codes over $\mathcal{R}_{k,m}$ with respect to the homogeneous weight. The results of the thesis show that, the ring family $\mathcal{R}_{k,m}$ is a relevant ambient space for codes over rings. The fruitful results obtained in extremal binary self-dual codes as well as self-orthogonal quasicyclic codes suggest that further explorations are possible. Possible connections to such recently introduced subjects as skew cyclic codes DNA codes can be explored as part of future work on the subject.

Another comment that we would like to make is about Frobenius rings. The main attraction of Frobenius rings for coding theorists is that they possess a generating character and consequently the MacWilliams identities hold for codes over such rings. It is our belief that non-Frobenius rings may also be considered for different aspects of coding theory as long as the concept of duality, generating character and MacWilliams identities do not come into the picture. With almost nothing in the literature about codes over such rings, the end results and the justification must be well described before such work can be undertaken. But we suggest this as a possible direction for future research.

REFERENCES

Aydin, N., Karadeniz, S., and Yildiz, B., "Some new binary quasi-cyclic codes from codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", *Appl. Algebr. Eng. Comm.*, Vol. 24, pp. 355–367, 2013.

Betsumiya, K., Georgiou, S., Gulliver, T.A., Harada, M., and Koukouvinos, C., "On self-dual codes over some prime fields", *Discrete Math.*, Vol. 262, No. 1, pp. 37–58, 2003.

Bouyukliev, I., Fack, V., and Winne, J., "Hadamard matrices of order 36 and double-even self-dual $[72, 36, 12]$ codes", *Eurocomb* 2005*,DMTCS proc.*, Vol. , pp. 93–98, 2005.

Brualdi, R.A. and Pless, V.S., "Weight enumerators of self-dual codes", *IEEE Trans. Inform. Theory*, Vol. 37, pp. 1222–1225, 1991.

Chen, Z., "Six new binary quasi-cyclic codes", *IEEE Trans. Inform. Theory*, Vol. 40, No. 5, pp. 1666–1667, 1994.

Constantinescu, I. and Heise, W., "A Metric for codes over residue class rings of integers", *Problemy Peredachi Informatsii*, Vol. 33, No. 3, pp. 22–28, 1997.

Conway, J.H. and Sloane, N.J.A., "A new upper bound on the minimal distance of self-dual codes", *IEEE Trans. Inform. Theory*, Vol. 36, No. 6, pp. 1319–1333, 1990.

Dontcheva., R., "New binary self-dual $[70, 35, 12]$ and binary $[72, 36, 12]$ self-dual doubly-even codes", *Serdica Math. J.*, Vol. 27, pp. 287–302, 2002.

Dougherty, S.T., Gaborit, P., Harada, M., and Solé, P., "Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$", *IEEE Trans. Inform. Theory*, Vol. 45, pp. 32–45, 1999.

Dougherty, S.T., Gulliver, T.A., and Harada, M., "Extremal binary self-dual codes", *IEEE Trans. Inf. Theory*, Vol. 43, No. 6, pp. 2036–2047, 1997.

Dougherty, S.T., Karadeniz, S., and Yildiz, B., "Cyclic codes over R_k", *Des. Codes and Crypt.*, Vol. 63, pp. 113–126, 2012.

Dougherty, S.T., Kim, J.L., Kulosman, H., and Liu, H., "Self-dual codes over commutative Frobenius rings", *Finite Fields Appl.*, Vol. 16, pp. 14–26, 2010.

Dougherty, S.T., Kim, J.L., and Sole, P., "Double circulant codes from two class association schemes", *Adv. Math. Commun.*, Vol. 1, No. 1, pp. 45–64, 2007.

Dougherty, S.T., Yildiz, B., and Karadeniz, S., “Codes over R_k, Gray Maps and their Binary Images”, *Finite Fields Appl.*, Vol. 17, pp. 205–219, 2011.

Gaborit, P., “Quadratic double circulant codes over fields”, *Journal of Combinatorial Theory Series A*, Vol. 97, No. 1, pp. 85–107, 2002.

Georgiou, S.D. and Lappas, E., “Self-dual codes from circulant matrices”, *Des. Codes Cryptogr.*, Vol. 64, pp. 129–141, 2012.

Grassl, M., “Bounds on the minimum distance of linear codes and quantum codes”, Online available at http://www.codetables.de2007, Accessed on 2015-12-01.

Greferath, M. and OSullivan, M.E., “On bounds for codes over Frobenius rings under homogeneous weights”, *Discrete Mathematics*, Vol. 289, pp. 11–24, 2004.

Griesmer, J.H., “A bound for error correcting codes”, *IBM J. Res. Dev.*, Vol. 4, pp. 532–542, 1960.

Gulliver, T.A. and Harada, M., “On double circulant doubly even self-dual $[72, 36, 12]$ codes and their neighbors”, *Australasian Journal of Combinatorics*, Vol. 40, pp. 137–144, 2008.

Hammons, A.R., Kumar, V., Calderbank, A.R., Sloane, N.J.A., and Sole, P., “The $\mathbb{Z}_4$ - linearity of Kerdock, Preparata, Goethals and related codes”, *IEEE Trans. Inform. Theory*, Vol. 40, pp. 301–319, 1994.

Honold, T., “A Characterization of finite Frobenius rings”, *Arch. Math.(Basel)*, Vol. 76, pp. 406–415, 2001.

Huffman, W.C., “On the classification and enumeration of self-dual codes”, *Finite Fields and Their Applications*, Vol. 11, pp. 451–490, 2005.

Huffman, W.C. and Pless, V., *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

Karadeniz, S., Dougherty, S.T., and Yildiz, B., “Constructing formally self-dual codes over $\mathcal{R}_k$”, *Discrete Applied Mathematics*, Vol. 167, No. 1, pp. 188–196, 2014a.

Karadeniz, S. and Yildiz, B., “$(1+v)$-constacylic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$”, *Journal of the Franklin Institute*, Vol. 348, pp. 2625–2632, 2011.

Karadeniz, S. and Yildiz, B., “New extremal binary self-dual codes of length 66 as extensions of self-dual codes over R_k”, *J. Franklin Inst.*, Vol. 350, No. 8, pp. 1963–1973, 2013.

Karadeniz, S. and Yildiz, B., “A New Construction for the Extended Binary Golay Code”, *Appl. Math. Inf. Science*, Vol. 8, No. 1, pp. 69–72, 2014.

Karadeniz, S., Yildiz, B., and Aydin, N., “Extremal binary self-dual codes of lengths 64 and 66 from four circulant constructions over $\mathbb{F}_2+u\mathbb{F}_2$”, *FILOMAT*, Vol. 28, No. 5, pp. 937–945, 2014b.

Kaya, A. and Tüfekçi, N., "Binary generator matrices of new extremal self-dual binary codes of lengths 66 and 68", available online at http://www.fatih.edu.tr/˜akaya/newbinary66-68.html2015.

Kaya, A. and Yildiz, B., "New extremal binary self-dual codes of length 68", *JA-CODESMATH*, Vol. 1, No. 1, pp. 29–39, 2014.

Kaya, A. and Yildiz, B., "Various constructions for self-dual codes over rings and new binary self-dual codes", *Discrete Mathematics*, Vol. 339, pp. 460–469, 2016.

Kaya, A., Yildiz, B., and Siap, I., "New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$", *Finite Fields Appl.*, Vol. 29, pp. 160–177, 2014.

Kaya, A., Yildiz, B., and Siap, I., "New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of quadratic double circulant codes over $\mathbb{F}_4$", *Finite Fields and Their Applications*, Vol. 35, pp. 318–329, 2015.

Kim, J.L., "New extremal self-dual codes of lengts $36, 38$ and 58", *IEEE Trans. Inf. Theory*, Vol. 47, No. 1, pp. 386–393, 2001.

Ling, S. and Xing, C., *Coding Theory: A First Course*, Cambridge University Press, 2004.

MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, 2nd Edition, North-holland Publishing Company, 1978.

McLoughlin, I. and Hurley, T., "A Group ring construction of the extended binary Golay code", *IEEE Trans. Infrom. Theory*, Vol. 54, pp. 4381–4383, 2008.

Melchor, C.A. and Gaborit, P., "On the Classification of Extremal $[36, 18, 8]$ Binary Self-Dual Codes", *IEEE Trans. Inform. Theory*, Vol. 54, No. 10, pp. 4743–4750, 2008.

Pasa, A. and Yildiz, B., "Constructing Gray maps from combinatorial geometries", *Commun. Fac. Sci. Univ. Ank. Serie A1*, Vol. 63, pp. 147–161, 2014.

Peng, X. and Farrell, P., "On construction of the $(24, 12, 8)$ Golay codes", *IEEE Trans. Inform. Theory*, Vol. 52, pp. 3669–3675, 2006.

Shannon, C.E., "A mathematical theory of communication", *Bell System Tech. J.*, Vol. 27, pp. 379–423, 1948.

Townsend, R.L. and Weldon, E., "Self-orthogonal quasi-cyclic codes", *IEEE Trans. Inform. Theory*, Vol. 13, No. 2, pp. 183–195, 1967.

Tsai, H.P., Shih, P.Y., Wuh, R.Y., Su, W.K., and Chen, C.H., "Construction of self-dual codes", *IEEE Trans.Inform. Theory*, Vol. 54, pp. 3826–3831, 2008.

Ward, H.N., "Divisible codes", *Arch. Math.*, Vol. 36, pp. 485–499, 1981.

Wood, J., "Duality for modules over finite rings and applications to coding theory", *Am. J. Math.*, Vol. 121, pp. 555–575, 1999.

Yankov, N., "Self-dual $[62, 31, 12]$ and $[64, 32, 12]$ codes with an automorphism of order 7", *Adv. Math. Commun.*, Vol. 8, No. 1, pp. 73–81, 2014.

Yildiz, B., *Weight enumerators and Gray maps of linear codes over rings*, Ph.D. Thesis, California Institute of Technology, 2006.

Yildiz, B., "A Combinatorial construction of the Gray map over Galois rings", *Discrete Mathematics*, Vol. 309, pp. 3408–3412, 2009.

Yildiz, B. and Karadeniz, S., "Linear Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", *Des. Codes Crypt.*, Vol. 54, pp. 61–81, 2010a.

Yildiz, B. and Karadeniz, S., "Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", *J. Franklin Inst.*, Vol. 347, pp. 1888–1894, 2010b.

Yildiz, B. and Karadeniz, S., "Cyclic Codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", *Des. Codes Crypt.*, Vol. 58, , 2011.

Yildiz, B. and Kelebek, I.G., "The homogeneous weight for $\mathcal{R}_k$, related Gray map and new binary quasicyclic codes", *ArXiv: 1504.04111*, Vol. , , 2014.

APPENDIX A

DECLARATION STATEMENT FOR THE ORIGINALITY OF THE THESIS, FURTHER STUDIES AND PUBLICATIONS FROM THESIS WORK

A.1 DECLARATION STATEMENT FOR THE ORIGINALITY OF THE THESIS

I hereby declare that this thesis comprises my original work. No material in this thesis has been previously published and written by another person, except where due reference is made in the text of the thesis. I further declare that this thesis contains no material which has been submitted for a degree or diploma or other qualifications at any other university.

Signature:
Date:

A.2 PUBLICATIONS FROM THESIS WORK

1. N. Tüfekçi, B. Yıldız, "On codes over $\mathcal{R}_{k,m}$ and constructions for new binary self-dual codes", to appear in Mathematica Slovaca.

2. A. Kaya, N. Tüfekçi, "New extremal binary self-dual codes of lengths 66 and 68 from codes over $\mathcal{R}_{k,m}$", to appear in Bulletin of the Korean Mathematical Society

3. B. Yıldız, N. Tüfekçi, "Optimal, divisible binary codes from gray-homogeneous images of codes over $\mathcal{R}_{k,m}$", to appear in European Journal of Pure and Applied Mathematics.

CURRICULUM VITAE

CONTACT INFORMATION

Nesibe TÜFEKÇİ
Email: nesibe_tufekci@hotmail.com

EDUCATION

Fatih University, Graduate School of Sciences and Engineering, Istanbul, Turkey
Doctor of Philosophy in Mathematics
June 2016
Thesis Title: On codes over an infinite family of ring extension of the binary field

Fatih University, Graduate School of Sciences and Engineering, Istanbul, Turkey
Master of Science in Mathematics
June 2012
Thesis Title: Characterization of $\mathcal{U}_1(\mathbb{Z}\mathbf{C}_\mathbf{n}^+)$ for $n \leq 24$

Fatih University, İstanbul, Turkey
Bachelor of Science in Mathematics
June 2010

Private Yavuz Selim High School, Kütahya, Turkey
June 2006

PROFESSIONAL EXPERIENCE

- Scholarship Assistant, Fatih University, December 2012–July 2015

PUBLICATIONS

Academic Journals

1. N. Tüfekçi, B. Yıldız, “On codes over $\mathcal{R}_{k,m}$ and constructions for new binary self-dual codes”, to appear in Mathematica Slovaca.

2. A. Kaya, N. Tüfekçi, “New extremal binary self-dual codes of lengths 66 and 68 from codes over $\mathcal{R}_{k,m}$”, to appear in Bulletin of the Korean Mathematical Society.

3. B. Yıldız, N. Tüfekçi, “Optimal, divisible binary codes from gray-homogeneous images of codes over $\mathcal{R}_{k,m}$”, to appear in European Journal of Pure and Applied Mathematics.

4. B. Köklüce, N. Tüfekçi, “Characterization of $V(\mathbb{Z}\mathbf{C}_{\mathbf{n}}^{+})$ of rank $\rho \leq 4$”, Miskolc Mathematical Notes, vol. 15, pp. 571-584 (2015).

Conference Proceedings

1. N. Tüfekçi, B. Köklüce, “Characterization of $\mathcal{U}_1\mathbb{Z}\mathbf{C}_{\mathbf{n}}^{+})$ for $n \leq 15$”, International conference on Applied Analysis and Algebra, Proceedings of International conference on Applied Analysis and Algebra, İstanbul-Türkiye, (2012).

2. T. Bilgin, N. Tüfekçi, “On the Involutions of Antihomomorphisms of Dihedral Groups”, Algerian-Turkish International Days on Mathematics 2013, İstanbul-Türkiye, (2013).

3. N. Tüfekçi, B. Yıldız, “On codes over an infinite family of ring extension of the binary field and constructions for new binary self-dual codes”, Karatekin Mathematics Days 2014, International Mathematics Symposium, Çankırı-Türkiye, (2014).